idn cadernos

CIBERSEGURANÇA E POLÍTICAS PÚBLICAS

ANÁLISE COMPARADA DOS CASOS CHILENO E PORTUGUÊS

JOÃO BARBAS E CAROLINA SANCHO

idn Instituto da Defesa Nacional

nº 29

Cibersegurança e Políticas Públicas

Análise comparada dos casos chileno e português

João Barbas e Carolina Sancho

Instituto da Defesa Nacional
e
Academia Nacional de Estudios Políticos
y Estratégicos de Chile

Lisboa
Julho de 2018

Instituto da Defesa Nacional

Os Cadernos do IDN resultam do trabalho de investigação residente e não residente promovido pelo Instituto da Defesa Nacional. Os temas abordados contribuem para o enriquecimento do debate sobre questões nacionais e internacionais.
As perspetivas são da responsabilidade dos autores não refletindo uma posição institucional do Instituto da Defesa Nacional sobre as mesmas.

Diretor
Vitor Rodrigues Viana

Coordenador Editorial
Alexandre Carriço

Núcleo de Edições
António Baranita

Capa
Nuno Fonseca/nfdesign

Propriedade, Edição e Design Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Composição, Impressão e Distribuição
EUROPRESS – Indústria Gráfica
Rua João Saraiva, 10-A – 1700-249 Lisboa – Portugal
Tel.: 218 494 141/43 Fax.: 218 492 061 E-mail: geral@europress.pt www.europress.pt

ISSN 1647-9068
ISBN: 978-972-27-1994-0
Depósito Legal 344513/12
Tiragem 150 exemplares

João Barbas. Coronel de Artilharia. Licenciado Ciências Militares e em Engenharia de Sistemas Decisionais. Mestre em Administração e Gestão de Empresas (MBA) com especialização em Gestão da Informação. Possui ainda uma pós-graduação em Investigação Operacional e Análise de Sistemas. Subdiretor do Curso de Defesa Nacional, Coordenador do Curso de Cibersegurança e Gestão de Crises no Ciberespaço e Assessor de Estudos do Instituto da Defesa Nacional de Portugal. Colabora com a Academia Militar como docente da unidade curricular "Tecnologias de Informação e Plataformas Internet" do Mestrado em Guerra de Informação e com o Instituto Politécnico de Setúbal como docente das unidades curriculares "Informática" e "Ética e Segurança da Informação".

Carolina Sancho. Doctora en Conflictos, Seguridad y Solidaridad, Universidad de Zaragoza en España. Magíster en Ciencia Política, Universidad de Chile. Licenciada en Gobierno y Gestión Pública y Administradora Pública, Universidad de Chile. Ha sido profesora en diversas Universidades chilenas en diferentes cátedras, entre ellas, la Escuela de Gobierno y Gestión Pública de Universidad de Chile en las asignaturas de "Análisis de conflictos internacionales actuales", "Teoría del Estado" y "Gobierno y gestión del Estado". Ha sido profesora titular y Jefa de Diplomados en Academia Nacional de Estudios Políticos y Estratégicos (ANEPE).

Resumo

Este estudo analisa as políticas de cibersegurança do Chile e Portugal e identifica os seus principais elementos e desafios. Começa por apresentar uma abordagem conceptual e contextual do ciberespaço, nomeadamente as suas principais caraterísticas e tendências, ameaças e riscos. No âmbito da cooperação multilateral, são abordados os principais fóruns em que o Chile e/ou Portugal participam – *i.e.* Organização das Nações Unidas (ONU), União Europeia (UE), Organização do Tratado do Atlântico Norte (OTAN) e Organização dos Estados Americanos (OEA) – cujos instrumentos normativos ou posição oficial refletem os consensos alcançados e influenciam as respetivas políticas nacionais no domínio em apreço.

O estudo carateriza fatores mínimos – conceitos, legislação especializada, arquitetura de cibersegurança, cooperação, cultura e políticas públicas – bem como outros elementos a considerar numa política nacional de cibersegurança. As políticas de cibersegurança de cada um dos países são estudadas individualmente e analisadas comparativamente à luz de cada fator mínimo.

Abstract

The study analyzes the cybersecurity policies of Chile and Portugal, identifying its main elements and challenges. Initially, presents a conceptual and contextual approach to cyberspace, its main characteristics and trends, threats and risks. In the context of multilateral cooperation, are introduced the main forums in which Chile and/or Portugal participate: the United Nations (UN), the European Union (EU), the North Atlantic Treaty Organization (NATO) and the Organization of American States (OAS), whose normative instruments or official positions reflect the consensus reached and influence their respective national policies in this area.

The research characterizes the minimum factors – concepts, specialized legislation, cybersecurity architecture, cooperation, culture and public policies – and other elements to be considered in a national cybersecurity policy. The cybersecurity policies of both countries are studied individually and analyzed comparatively under each minimum factor.

Preâmbulo

No âmbito da XVII Conferência de Diretores de Colégios de Defesa Ibero-Americanos ocorrida no Rio de Janeiro em outubro de 2016, foi manifestado o interesse e acordada a realização de um projeto de investigação conjunto no âmbito da cibersegurança entre a *Academia Nacional de Estudios Políticos y Estratégicos* (ANEPE) do Chile e o Instituto da Defesa Nacional (IDN) de Portugal.

O projeto decorre da importância que ambas as instituições colocam no estudo e aprofundamento da análise das temáticas associadas ao ciberespaço, que contribuem e condicionam as sociedades chilena e portuguesa, inseridas em hemisférios e quadros regionais próprios e com níveis de maturidade tecnológicas eventualmente diferenciadas.

O estudo, que agora se apresenta, foi realizado ao longo de 2017, por um investigador de cada uma das instituições, utilizando extensivamente as capacidades das plataformas de comunicação digital disponíveis atualmente.

Para a realização deste projeto, os investigadores socorreram-se exclusivamente de fontes de informação públicas de cada um dos respetivos países assim como das instituições e fóruns internacionais em que participam, nomeadamente, Organização das Nações Unidas (ONU), União Europeia (UE), Organização do Tratado do Atlântico Norte (OTAN) e Organização dos Estados Americanos (OEA).

Este estudo analítico e comparativo não se circunscreve exclusivamente à cibersegurança mas aborda igualmente a ciberdefesa e demais domínios e/ou temas afins, que contribuem para a capacidade de resiliência cibernética de cada um dos países e o seu desenvolvimento económico e social.

Por motivos de fidelidade aos documentos que serviram de suporte ao estudo, este é apresentado nas línguas maternas de cada um dos investigadores, nas partes que cada um redigiu.

ÍNDICE

Resumo / Abstract 5

Preâmbulo 7

Índice de Tabelas e Figuras 13

Introducción 15

Capítulo I: Aproximación Conceptual y Contextualización 18
1. El Ciberespacio: Nuevo Dominio para el Desarrollo del Hombre 18
   1.1. Principales Características y Tendencias 19
   1.2. Amenazas y Riesgos en el Ciberespacio 22
2. La Ciberseguridad como Condición para el Normal Uso del Ciberespacio 29

Capítulo II: Cooperación Multilateral 32
1. Organización de Naciones Unidas 32
2. União Europeia 37
   2.1. Estratégia Global da União Europeia 37
   2.2. Estratégia da UE para a Cibersegurança 39
   2.3. Regulamento Geral de Proteção de Dados 45
   2.4. Proteção das Infraestruturas de Informação Críticas 47
3. Organização do Tratado do Atlântico Norte 49
4. Organización de Estados Americanos 51

Capítulo III: Factores Mínimos a Considerar en una Política Nacional de Ciberseguridad 56
1. Aproximación Conceptual 56
2. Legislación Especializada 56
3. Arquitectura de Ciberseguridad 57
4. Cooperación Internacional 57
   4.1. La Conferencia Global del Ciberespacio 58
   4.2. La Conferencia de Meridian 59
   4.3. Convenio de Budapest 60
   4.4. Manual de Tallin 62
5. Cultura de Ciberseguridad 62
6. Política Pública en Ciberseguridad 62

Capítulo IV: Outros Elementos Essenciais a Considerar numa Política de Cibersegurança 64

1. Abordagem Concetual 64
   1.1. Conhecimento 64
   1.2. Conhecimento Organizacional 66
   1.3. Aprendizagem Organizacional 68
   1.4. Melhoria Contínua 70
   1.5. Lições Aprendidas 72
   1.6. Continuidade de Negócio 74
   1.7. Resiliência Cibernética 75
   1.8. "Ciber-higiene" 76
   1.9. Governação 77
   1.10. Planeamento de Longo Prazo 78
   1.11. Recrutamento, Formação e Retenção de Talentos 79

Capítulo V: Políticas Nacionais de Cibersegurança/Políticas Nacionales de Ciberseguridad 80

1. Caso de Chile 80
   1.1. Aproximación Conceptual 81
   1.2. Legislación Especializada 84
   1.3. Arquitectura de Ciberseguridad 87
      1.3.1. Los Principales Organismos Técnicos 91
   1.4. Cooperación Internacional 91
   1.5. Cultura de Ciberseguridad 93
   1.6. Política Pública en Ciberseguridad 97
      1.6.1. Políticas Integradas Complementarias en Materia Digital 100
2. Caso de Portugal 101
   2.1. Aproximação Conceptual 101
   2.2. Legislação Especializada 102
      2.2.1. Conceito Estratégico de Defesa Nacional 102
      2.2.2. Lei do Cibercrime 103
      2.2.3. Estratégia Nacional de Combate ao Terrorismo 103
      2.2.4. Outra Legislação 103
   2.3. Arquitectura de Cibersegurança 104
      2.3.1. Centro Nacional de Cibersegurança 104
      2.3.2. Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica 105
      2.3.3. Conselho Superior de Segurança do Ciberespaço 107

2.3.4. Despacho n.º 7456/2017 de 24 agosto da MPMA 107
2.3.5. Centro de Ciberdefesa 108
2.3.6. Rede Nacional de CSIRT 109
2.4. Cooperação Internacional 110
2.5. Cultura de Cibersegurança 111
2.6. Política Pública em Cibersegurança 115
2.6.1. Estratégia Nacional de Segurança do Ciberespaço 115
2.6.2. Orientação Política para a Ciberdefesa 116
2.6.3. O Programa do XXI Governo Constitucional 118

Capítulo VI: Análise Comparada dos Países 120
1. Aproximação Conceptual 120
2. Legislação Especializada 120
3. Arquitetura de Cibersegurança 120
4. Cooperação Internacional 121
5. Cultura de Cibersegurança 121
6. Política Pública de Cibersegurança 122

Capítulo VI: Conclusiones 123

Referências 127

Anexo A: Estrutura da Convenção de Budapeste 140
Anexo B: Estrutura do Manual de Tallinn 2.0 141
Anexo C: Outra legislação portuguesa aplicável 142
Anexo D: Iniciativas e ações de sensibilização 144
Anexo E: Programas de Formação Superior em Cibersegurança 145

INDÍCE DE TABELAS E FIGURAS

Tabla 1	Resumen de Estado de Riesgo del Ciberespacio	25
Tabla 2	Las Principales Familias de *Malware* de 2014	27
Tabla 3	Principales Resoluciones de ONU sobre Ciberseguridad	33
Tabla 4	Principales Publicaciones de UIT sobre Ciberseguridad	36
Tabela 5	Infraestruturas Essenciais	48
Tabla 6	Principales Leyes que Abordan Aspectos Específicos sobre Ciberseguridad en Chile	85
Tabla 7	Principales Decretos que Abordan Aspectos Específicos sobre Ciberseguridad en Chile	87
Tabla 8	Instituciones que Intervienen en Ciberseguridad en Chile	88
Tabla 9	Objetivos y Metas de la PNCS Chilena	97
Tabela 10	Conceitos empregues na *Lei do Cibercrime*	102
Tabela 11	Competências do Centro Nacional de Cibersegurança	105
Tabela 12	Competências da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica	106
Tabela 13	Objetivos do Conselho Superior de Segurança do Ciberespaço	107
Tabela 14	Missão e Atribuições da Direção de Comunicações e Sistemas de Informação	108
Tabela 15	Atribuições da Direção de Comunicações e Sistemas de Informação no Âmbito da Ciberdefesa	108
Tabela 16	Atribuições da Direção de Comunicações e Sistemas de Informação no Âmbito da Ciberdefesa Setorial da Defesa Nacional	109
Tabela 17	Objetivos da Rede Nacional de CSIRT	110
Tabela 18	Principais Contributos da ENISA	111
Tabela 19	*Cyber Security Breaches*	113
Tabela 20	Estratégia Nacional de Segurança do Ciberespaço	116
Tabela 21	Linhas Orientadoras para a Ciberdefesa Nacional	118

Figura 1	Desarrollo Global de TIC entre 2001-2017*	20
Figura 2	Acceso a las TIC Según el Estado de Desarrollo, 2017	21
Figura 3	Cuenta AP Intervenida	23
Figura 4	Impacto en *DOW Jones*	23
Figura 5	Principales Aspectos Promovidos por la Agenda Global de Ciberseguridad de la UIT	35
Figura 6	Dimensões do Conhecimento	65
Figura 7	Modelo SECI	65
Figura 8	Espiral da Criação do Conhecimento Organizacional	67
Figura 9	Tipos de Aprendizagem	69
Figura 10	Campaña Ciudadanía Digital e Internet Segura	94
Figura 11	Rede Nacional de CSIRT	109

Introducción

Esta investigación se efectúa en el marco del convenio de cooperación entre la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) de Chile y el Instituto da Defensa Nacional (IDN) de Portugal que promueve la cooperación académica entre ambas instituciones y fomenta la investigación conjunta para una mejor comprensión de temas vinculados con la seguridad y defensa, como con la realidad de ambos países.

En esta ocasión el tema seleccionado ha sido la ciberseguridad. En efecto, el ciberespacio y su seguridad es una materia de creciente interés en los países, al menos por tres motivos:

Su creciente uso por personas, organizaciones privadas e instituciones públicas a nivel nacional e internacional, en los diferentes ámbitos de la actividad que realizan, sea social política o económica, entre otras.

Su relevancia desde una perspectiva de seguridad, debido a que el ciberespacio como dimensión en la que se efectúan comunicaciones, acciones, interacciones y transacciones entre personas, organizaciones privadas e instituciones públicas, requiere contar con condiciones mínimas que garanticen por un lado la continuidad del servicio de acceso al ciberespacio, como también, la confiabilidad, disponibilidad e integridad de la información que circula por éste.

Su sensibilidad en un enfoque de defensa, toda vez que, es necesario contar con una capacidad liderada desde el Estado, para responder frente a incidentes en el ciberespacio que afecten la seguridad en su uso y muy especialmente para proteger la infraestructura crítica vinculada al ciberespacio, la infraestructura crítica de la información.

Las tres situaciones expuestas están vigentes tanto en Chile como en Portugal y ello ha justificado la preocupación de sus gobiernos para formular una política pública en ciberseguridad. En efecto, si entendemos una política pública como una "intervención del Estado, expresada en una decisión o conjunto de decisiones de una autoridad pública, que considera un análisis técnico – racional para un tema determinado y una finalidad específica, que sigue un procedimiento formal, todo lo cual se da en el contexto de un intenso proceso político de confrontación y articulación de intereses"[1], podemos considerar que la formulación de una política pública de ciberseguridad ha sido una necesidad imperiosa. Revisaremos este planteamiento con relación a la ciberseguridad para constatar el modo en que ambos se vinculan.

Tal como señala el autor, una política pública se vincula a un problema público, que muchas veces se visibiliza por medio de necesidades de personas o agrupaciones del sector privado o público, desde el nivel local, nacional o internacional. Aplicado al tema de la ciberseguridad, el problema o necesidad proviene de los riesgos en el ciberespacio que pueden ser resultado de amenazas o vulnerabilidades, manifestándose como inciden-

1 Olavarría, M., 2007. *Conceptos Básicos en el Análisis de Políticas Públicas*. Documentos de Trabajo N.º 11, Diciembre. INAP-Instituto de Asuntos Públicos Departamento de Gobierno y Gestión Pública, Universidad de Chile, pp. 92. Disponible en Repositorio Académico de la Universidad de Chile: http://repositorio.uchile.cl/bitstream/handle/2250/123548/Conceptos_%20Basicos_Politicas_Publicas.pdf?sequence=1

tes que en su máxima expresión puede tratarse de un ataque a infraestructura crítica para afectar las actividades más sensibles del país y con ello afectar el orden y la seguridad pública e inclusive la seguridad nacional, como ocurrió en Estonia en 2007, por ejemplo.

Debido a que este problema público, afecta a la comunidad en forma transversal y compromete áreas de responsabilidad exclusivas del Estado, como el orden y la seguridad pública y la seguridad nacional, justifican que sea éste quien lidere la respuesta. Enfrentar el tema tiende a expresarse por medio de una política pública de la cual pueden derivarse otras políticas públicas y/o conectase con otras relacionadas, potenciando así la respuesta que se desea dar.

La consideración técnica – racional del tema implica hacer un diagnóstico del problema a que es necesario abordar. En este sentido, para el caso de la ciberseguridad, ¿qué puede afectarla y con qué objetivo? Una primera aproximación a este asunto permite identificar una diversidad de situaciones que pueden afectar el adecuado funcionamiento del ciberespacio y distinguir al menos tres objetivos. Mientras los incidentes que afecten la ciberseguridad pueden ser originados por[2]: ataques patrocinados por otros Estados; ataques patrocinados por sector privado; terroristas, extremismo político o ideológico; hacktivistas; crimen organizado; ataques de perfil bajo; ataques de personal con accesos privilegiados, los blancos pueden ser el gobierno, el sector privado y/o los ciudadanos. Adicionalmente, para efecto de una mejor comprensión es posible clasificar los peligros en el ciberespacio como: ciberdelito, ciberespionaje, ciberterrorismo e inclusive ciberguerra[3].

El diagnóstico es el insumo que permite identificar líneas de acción para responder a las demandas ciudadanas y/o el problema público detectado, siendo frecuente a partir de la descripción realizada la consideración de planteamientos en términos de actualizar y crear leyes y normas que regulen el uso del ciberespacio según protocolos de seguridad de acuerdo a estándares internacionales y sancionen las prácticas que atenten contra los derechos de las personas, su libertad (en sistemas políticos democráticos), su bienestar y sus bienes o patrimonio. En este contexto, la cooperación internacional resulta clave para el intercambio de información como para una respuesta instantánea frente a ilícitos transnacionales. Otras líneas de acción frecuentemente consideradas por los gobiernos son la promoción de la educación para la ciberseguridad y la creación de una institucionalidad que la gestione la seguridad en el ciberespacio.

Finalmente, ese "creciente proceso de confrontación y articulación de intereses", se realiza en el ejecutivo entre los distintos organismos involucrados en la ciberseguridad, siendo frecuente constatar que diversos ministerios desde diferentes aristas tienen atribuciones y competencia en la materia. Junto a lo indicado, se adiciona el mismo proceso desde el legislativo, sea para discutir leyes, aprobar el presupuesto o apoyar la firma de acuerdos internacionales.

---

2 Torres, M., 2013. Ciberguerra. *In* Javier Jordán, coordinador, *Manual de Estudios Estratégicos y Seguridad Internacional*. Madrid: Plaza y Valdés Editores, pp. 329-348.

3 Nye, J., 2012. Ciberguerra y Ciberpaz. *Project Syndicate*, Apr 10. Disponible en https://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish?barrier=accesspaylog

Estos antecedentes avalan la formulación de políticas nacionales de ciberseguridad. En esta investigación se analiza el caso chileno y portugués, a partir de los cuales es efectuado un análisis comparado con la finalidad e identificar similitudes, diferencias y buenas prácticas.

La metodología a ocupar para el desarrollo de la investigación es la investigación bibliográfica, la revisión de libros y revistas especializados, el análisis de documentos oficiales a nivel nacional e internacional y la consulta a experto cuando ello ha sido necesario. Asimismo, los investigadores se han especializado en el tema. En efecto, han participado en diversas publicaciones académicas y expuesto en diferentes instancias sobre el tema. El tipo de investigación efectuada es de tipo cualitativa, exploratoria y descriptiva.

El objetivo de esta investigación es "describir factores mínimos a contemplar en una política nacional de ciberseguridad para el caso de Chile y Portugal, estableciendo similitudes, diferencias y desafíos en cada caso, actualmente (año 2018)".

Los objetivos específicos son:

(1) Conceptualizar los principales términos usados en la investigación (al menos ciberseguridad y ciberdefensa);
(2) Identificar factores mínimos a considerar en una política nacional de ciberseguridad, explicando en que consiste cada uno de ellos;
(3) Caracterizar la situación de Chile y Portugal con relación a cada factor identificado, estableciendo los desafíos nacionales en la matéria;
(4) Comparar el caso de Chile y Portugal con relación a los factores mínimos de una política de ciberseguridad.

El esquema de desarrollo de este trabajo contempla seis partes. La primera, corresponde a una aproximación conceptual y contextualización del tema de la ciberseguridad. La segunda, aborda el tema de la seguridad en el ciberespacio desde la perspectiva de la cooperación internacional. La tercera, identifica los factores mínimos a considerar en una política de ciberseguridad. La cuarta, describe elementos adicionales esenciales en una política de ciberseguridad. La quinta, analiza el caso chileno y el portugués. Finalmente, el capítulo sexto desarrolla un análisis comparado de cada uno de los casos estudiados en el capítulo anterior.

CAPÍTULO I
Aproximación Conceptual y Contextualización

1. El Ciberespacio: Nuevo Dominio para el Desarrollo del Hombre

El ciberespacio es producto de la revolución en las TIC y una de sus principales consecuencias, el fenómeno de la globalización, entendido como un "proceso o (serie de procesos) que engloba una transformación en la organización especial de las relaciones y transacciones sociales"[4] que puede ser "evaluada en función de su alcance, intensidad, velocidad y repercusión, y que genera flujos y redes transcontinentales o interregionales de actividad, interacción y ejercicio del poder"[5], ha producido un cambio en las relaciones sociales reconfigurando las relaciones de poder. Por ejemplo, desde una perspectiva estatal, el poder del Estado se modifica en cuanto cede cuotas de poder a nivel supranacional y/o internacional y también a nivel local. Sin embargo, ello no implica que pierda importancia o vigencia. Al contrario, se refuerza su relevancia por cuanto es el articulador de las diferentes relaciones entre actores locales, nacionales, internacionales y transnacionales.

Este cambio en las relaciones sociales genera consecuencias que estamos permanentemente descubriendo y periódicamente plantea dilemas y paradojas. En efecto, se ha planteado que actualmente estamos frente a la "Cuarta Revolución Industrial"[6], en la cual se constatan cambios "tan profundos que, desde la perspectiva de la historia humana, nunca ha habido una época de mayor potencial o peligro"[7]. En efecto, tres motivos que permitirían argumentar la magnitud del cambio detectado, que justificaría darle la cualidad de revolucionario:

"*Velocidad*: Al contrario que las anteriores revoluciones industriales, ésta está evolucionando a un ritmo exponencial, más que lineal. Este es el resultado del mundo polifacético y profundamente interconectado en que vivimos, y del hecho de que la nueva tecnología engendra, a su vez, tecnología más nueva y más poderosa"[8].

"*Amplitud y profundidad*: Se basa en la revolución digital y combina múltiples tecnologías que están llevando a cambios de paradigma sin precedentes en la economía, los negocios, la sociedad y las personas. No sólo está cambiando el 'qué' y el 'cómo' hacer las cosas, sino el 'quienes somos'"[9].

"*Impacto de los sistemas*: Se trata de la transformación de sistemas complejos entre (y dentro de) los países, las empresas, las industrias y la sociedad en su conjunto"[10].

Este cambio que inclusive es entendido como una revolución requiere para su mejor comprensión con contextualización del ambiente en que se genera, es decir, la descrip-

4 Held, D. *et al*., 2002. *Transformaciones globales. Política, economía y cultura.* México: Oxford University Press.
5 *Ibidem.*
6 Schwab, K., 2017. *La cuarta revolución industrial.* Buenos Aires: Debate.
7 *Ibidem.*
8 *Ibidem.*
9 *Ibidem.*
10 *Ibidem.*

ción de algunas de sus principales características y tendencias, las cuales son descritas a continuación en este capítulo.

1.1. Principales Características y Tendencias[11]

El acceso creciente a las TIC ha influido en lo que algunos han denominado un nuevo momento en la historia del hombre caracterizado – entre otros aspectos – por la desaparición de la distinción entre distancia y tiempo. En este sentido, recordemos que hace más de una década Manuel Castells en su obra de tres tomos denominada "La era de la información" nos proponía la existencia de un nuevo paradigma llamado la "Era Informacional", por cuanto se trataba de "un nuevo modo de desarrollo informacional"[12] en donde la "fuente de la productividad estriba en la tecnología de la generación del conocimiento, el procesamiento de la información y la comunicación de símbolos"[13].

Ello puede constatarse, por ejemplo, cuando recibimos y enviamos un correo electrónico, situación en la cual a través de una única acción estamos generando, procesando y comunicando símbolos. En efecto, tal como indica Kissinger "lo nuevo en nuestra época es el promedio del cambio del poder informático y la penetración de la tecnología de la información en todas las esferas de la existencia"[14]. Otro ejemplo se relaciona con la creciente valoración de las bases datos. En efecto, la profesora titular de la Universidad Politécnica de Madrid y experta en big data, Ernestina Menasalvas afirma:

> "(…) algunos dicen que los datos son el nuevo petróleo del siglo XXI y ya se dice que el data scientist será la profesión más demandada en las próximas décadas. Son especialistas que se van a demandar en todos los países y en todos los sectores. Será un proceso similar al que ocurrió en la década de los 60 con la automatización. Además, a día de hoy no hay tanta gente formada en este campo. Por otro lado, la tecnología de datos no hace más que avanzar, cada vez hay más datos y cada vez está más generalizada. Ahora recibimos datos de manera continua y en tiempo real y tenemos que conseguir ordenarlos y analizarlos a tiempo"[15].

De acuerdo a Castells (1999)[16], es posible advertir algunas características de este nuevo paradigma de desarrollo, su tendencia a ser integrador, complejo e interconectado. Ello se explica porque son tecnologías que actúan sobre la información, cuentan con una alta capacidad para penetrar y modificar la vida cotidiana de las personas, presentando

11 El desarrollo de este tema fue previamente abordado en Sancho, C., 2016. Ciberespacio bien público mundial en tiempos de globalización: política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI. *In* José Cimar Rodrigues Pinto, org., *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional*. XVII Conferência de Diretores de Colégios de Defesa Ibero-Americanos 2016.

12 Castells, M., 1999. *La era de la información: Economía, Sociedad y cultura. Volumen II: El poder de la identidad*. México: Siglo XXI Editores.

13 *Ibidem*.

14 Kissinger, H., 2016. *Orden Mundial*. Madrid: Debate.

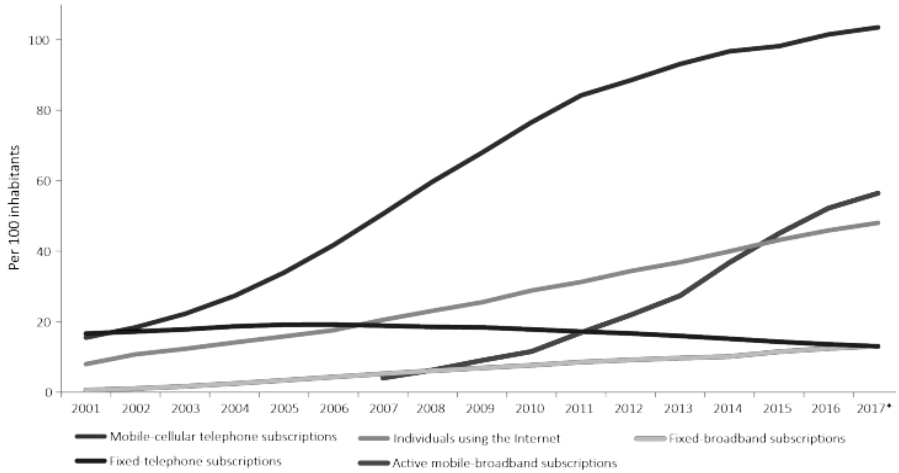
15 Villamediana, M., 2015. Los datos son el nuevo petróleo del siglo XXI. *EuroXpress*, 1 de julio. Disponible en http://www.euroxpress.es/noticias/los-datos-son-el-nuevo-petroleo-del-siglo-xxi [Consult. 15/9/2017].

16 Castells, M., 1999. *La era de la información: Economía, Sociedad y cultura. Volumen II: El poder de la identidad*. México: Siglo XXI Editores.

una creciente convergencia, debido a que se trata de distintas tecnologías específicas que actúan en un mismo sistema integrado. Todo lo cual ha generado una nueva estructura social denominada RED y a través de éstas un modo de gestión del poder más descentralizado en comparación con las tradicionales organizaciones estructuradas en distintos niveles de jerarquía.

Ello puede observarse en los denominados "teléfonos inteligentes" o "*Smartphone"*, que ofrecen diferentes tecnologías antes en disponibles de diversos aparatos o de difícil acceso. Por ejemplo, tienen desde un despertador pasando por un cronómetro hasta un GPS, como también, comunicación instantánea con cualquier lugar del mundo donde exista similar tecnología. Aplicaciones como *Skype*, *Whatsapp* o *Messenger* ilustran esta idea. De esta manera, "los efectos de la revolución se extienden a todos los niveles de organización humana. Los individuos que usan *smartphones* (…) hoy poseen información y capacidades analíticas superiores a muchas agencias de inteligencia de una generación atrás"[17]. Además esta tecnología presenta una creciente penetración mundial, de acuerdo a lo indicado por la UIT, tal como se ilustra en la figura 1.

Figura 1 – Desarrollo Global de TIC entre 2001-2017*



Notes: * ITU estimate.

Fuente: ITU (2017).

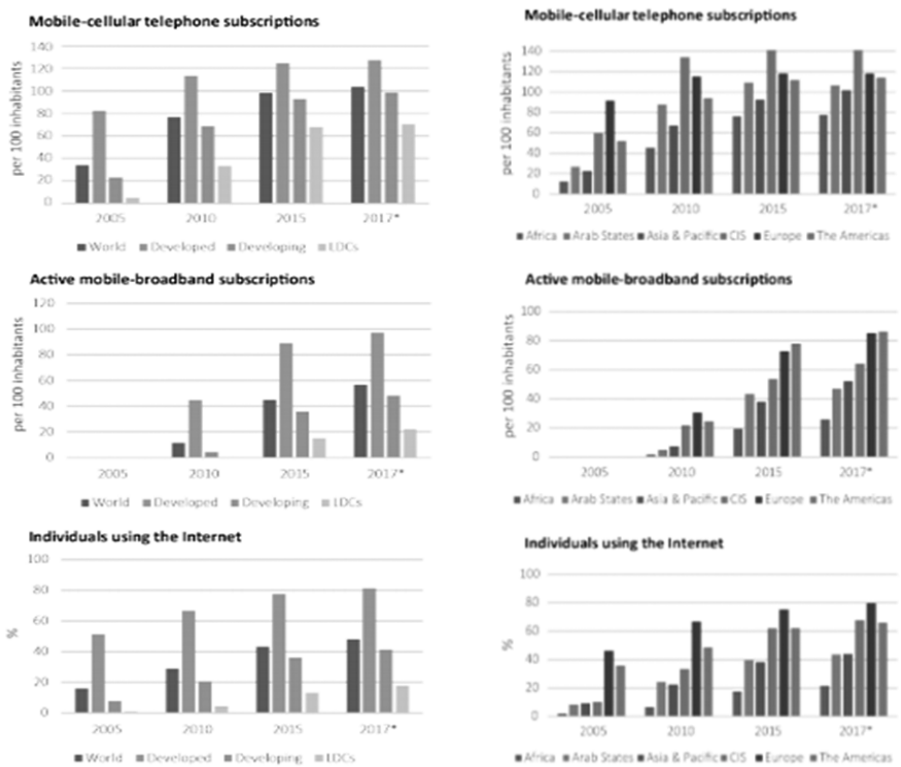
Esta tendencia ha siso sostenida a lo largo de los últimos años. En efecto, ya en 2015 el Director de la Oficina de Desarrollo de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), en el informe "Medición de la Sociedad de la Información 2015", señalaba que:

17 Kissinger, H., 2016. *Orden Mundial.* Madrid: Debate.

> "La proporción de la población mundial cubierta por las redes móviles y celulares es ahora de más del 95%, mientras que el número de abonados a telefonía móvil celular se ha incrementado de 2.200 millones en 2005 a unos 7.100 millones en 2015 (…) El número de abonados a la banda ancha móvil en todo el mundo ha crecido, de 800 millones en 2010, a unos 3.500 millones en 2015, al mismo tiempo que la cifra de abonados de banda ancha fija ha aumentado mucho más lentamente, a unos 800 millones en la actualidad. El número de usuarios de Internet también ha crecido rápidamente, y actualmente se estima en más del 40% de la población mundial".

Sin embargo, las regiones no están igualmente globalizadas. Considerando que el grado de globalización medido en función del nivel de acceso a las TIC puede ser cuantificado, el informe "Medición de la Sociedad de la Información 2017"[18] permite constatar las diferencias en el acceso a las tecnologías de la información en diferentes zonas del mundo, tal como se ilustra en la figura 2.

Figura 2 – Acceso a las TIC Según el Estado de Desarrollo, 2017



Fuente: ITU (2017).

18 International Telecommunication Union (ITU), 2017. *Measuring the Information Society Report 2017*. Volume 1. Geneva. Disponible en http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf. [Consult. 17 de Noviembre de 2017].

No obstante, aun cuando se reconoce la existencia de una brecha en el desarrollo digital de los países, el ciberespacio se continúa desarrollando y los Estados, de acuerdo a sus posibilidades, participan de ello. Una de las importantes tendencias en este ambiente es el "*big data*", entendido como:

> "Conjuntos de datos cuyo volumen, variedad y velocidad superan los correspondientes a los conjuntos de datos habituales. Su aparición denota adelantos tecnológicos que permiten captar, almacenar y procesar cantidades de datos cada vez mayores de diferentes fuentes de datos. De hecho, una de las tendencias primordiales que fomenta el surgimiento de "big data" es la "conversión en datos" y la digitalización masivas, también de actividad humana, en "árboles" o "huellas" digitales. En un mundo cada vez más digitalizado, los "big data" se generan de forma digital a partir de diversas fuentes, entre ellas registros administrativos (por ejemplo antecedentes bancarios o historiales clínicos electrónicos), transacciones comerciales entre dos entidades (como, por ejemplo, compras en línea o transacciones con tarjeta de crédito), sensores y dispositivos de localización (por ejemplo teléfonos móviles o dispositivos GPS) y actividades de los usuarios en Internet (entre ellas búsquedas y contenidos de los medios sociales)"[19].

Las principales características de los "*big data*"[20] son: velocidad, debido a la rapidez con la que se generan y analizan los datos; variedad, contienen diferentes tipos y formas de datos, incluidos grandes volúmenes de datos no estructurados; valor, debido al desarrollo socioeconómico potencial de los "*big data*"; veracidad, dada por el nivel de calidad, exactitud e incertidumbre de los datos y las fuentes de datos y; volumen, pues son cantidades ingentes de datos generados a través de la "conversión en datos".

De esta manera, las cualidades de los "*big data*" encierran grandes posibilidades de mejorar la puntualidad e integridad de las estadísticas oficiales. Por ejemplo, para formular políticas a favor del desarrollo social y económico[21]. En efecto, los diversos usos dados a la información en el ciberespacio facilitan una serie de acciones que antiguamente requerían más tiempo y dinero.

1.2. Amenazas y Riesgos en el Ciberespacio[22]

Junto a los beneficios que brinda el ciberespacio, es posible también encontrar su lado oscuro representado por los peligros que han sido detectados. Por ejemplo, el Informe de Riesgos Mundiales 2013 elaborado por el Foro Económico Mundial (FEM) advirtió sobre el peligro de los "incendios digitales en un mundo hiperconectado". Con ello se refería a las consecuencias sociales – e inclusive políticas – que puede generar la información falsa difundida en internet, resultado de un error humano o una acción deliberada, siendo esta última la que genera mayores desafíos desde la perspectiva de la

19 Unión Internacional de Telecomunicaciones (UIT), 2014. Informe sobre Medición de la Sociedad de la Información 2014. Resumen Ejecutivo. *UIT*, Ginebra. Disponible en https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS_2014_Exec-sum-S.pdf

20 *Ibidem.*

21 *Ibidem.*

22 El desarrollo de este tema fue previamente abordado en Sancho (2016).

seguridad de la información en el ciberespacio. Ejemplo de ello pudo observarse cuando las autoridades de EE.UU., los medios de comunicación, el mercado bursátil y la opinión pública mundial durante algunos minutos fueron sorprendidos con la noticia publicada en el twitter de la agencia Associated Press (AP) que indicaba: "Dos explosiones en la Casa Blanca y el Presidente Obama herido" (figura 3), la cual correspondió a difusión de información falsa resultado de un hackeo a la cuenta de twitter de la agencia Associated Press (AP). No obstante, hubo consecuencias inmediatas, como por ejemplo la baja en las acciones, según lo reflejó ese día el índice del *DOW Jones* (figura 4).

Figura 3 – Cuenta AP Intervenida

Figura 4 – Impacto en *DOW Jones*

Fuente: Saiz (2013).

Actualmente una creciente cantidad de países identifican los ataques cibernéticos como un peligro tanto o más importante que los ataques terroristas para la seguridad nacional y los entienden como una amenaza seria a la seguridad del país desde una perspectiva política, económica, social y tecnológica.

En este sentido, James Clapper, ex Director de la Oficina de Inteligencia Nacional, en una exposición ante el Comité de Inteligencia del Senado con motivo del informe anual sobre los peligros para la seguridad de EE.UU., abordó uno de los problemas que enfrentan en seguridad cibernética señalando que "en algunos casos, el mundo está aplicando tecnologías digitales con mayor rapidez que nuestra capacidad para entender las implicaciones que se puedan derivar para nuestra seguridad y para tratar de mitigar los nuevos riesgos"[23].

De esta manera, es posible reconocer la vulnerabilidad de los sistemas de información cibernéticos y la importancia de contar con niveles mínimos de seguridad en la gestión de la información digital, es decir, en su generación, almacenamiento y distribución. Asimismo, nos recuerda la variedad de posibles amenazas que estos sistemas pueden ser objeto, por ejemplo: hackeo; ataques distribuidos por denegación de servicio (DDoS); robo de información y los diferentes tipos de virus que pueden afectar al sistema de información digital, entre otros.

23 Saiz, E., 2013. Los ciberataques sustituyen al terrorismo como primera amenaza a Estados Unidos. *El País*, 13 MAR, Washington. Disponible en http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html

Recordemos que "los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos"[24]. Además, no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas. En este contexto la ciberseguridad adquiere preponderancia, pues deja en evidencia que el desarrollo de las tecnologías de la información – software y hardware –, debe ir acompañado de un similar desarrollo de protección a la información que es procesada por estas tecnologías. Ello se refuerza al observar una síntesis del "estado de riesgo en el ciberespacio"[25], que sistematiza los diversos tipos de amenazas detectados y los clasifica en diferentes niveles de riesgo, tal como se indica en tabla 1.

Agrava esta situación la detección de los denominados "*Malware*", es decir, *software* maliciosos que ya han causado daño en países alertándonos del peligro que hay tras su actuar. De acuerdo a un reporte de la empresa de seguridad informática Kaspersky, los *malware* pueden agruparse "en amenazas conocidas (70%), amenazas desconocidas (29%) y amenazas sofisticadas (1%)"[26], estas últimas denominadas también como "*Advanced Persistent Threats*" (APT) o "Amenazas Avanzadas Permamentes" y son particularmente peligrosas porque se trata de "ataques polivalentes, continuados y dirigidos. Diseñados para introducirse en una red, merodear de forma invisible y recopilar datos confidenciales, una vez introducidos pueden pasar desapercibidos durante años"[27].

Para ilustrar su modo de funcionamiento y posibles daños que pueden generar se hará referencia a tres de ellos: *Darkhotel, Flame y Stuxnet*. El primero es descrito en un reporte de Kaspersky:

> "Una APT conocida como "Darkhotel" utilizó el Wi-Fi en hoteles de lujo para robar los datos de los huéspedes durante siete años antes de que se descubriera. Esta fue especialmente interesante, ya que tenía un objetivo muy específico (los altos ejecutivos y directores ejecutivos) e ilustraba de forma muy clara el reto que se presenta a la seguridad de IT cuando los endpoints [terminales] (portátiles y tablets empresariales) operan fuera del perímetro de seguridad de la red de la empresa"[28].

24 Candau, J., 2010. Estrategias Nacionales de Ciberseguridad. Ciberterrorismo. *Cuadernos de Estrategia* 149, Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Diciembre. Instituto Español de Estudios Estratégicos, Ministerio de Defensa. Disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. [Consult. 15/9/2017].

25 Spanish Cyber Security Institute (SCSI), 2012. La Ciberseguridad Nacional, un compromiso de todos. *Instituto Español de Ciberseguridad*. Disponible en https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf

26 Karpersky Lab, 2015. *Los riesgos futuros: Protéjase*. Disponible en http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf [Consult. 15/9/2017].

27 *Ibidem.*

28 *Ibidem.*

Tabla 1 – Resumen de Estado de Riesgo del Ciberespacio

Autoría	Objetivos		
	Gobierno	**Sector Privado**	**Ciudadanos**
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Privados	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de internet; infección con malware; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de datos personales
Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	
Ataques de personal con accesos privilegiados (Insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	

Impacto	Alto
	Medio
	Bajo

Fuente: SCSI (2012).

En el caso de *Flame*, este fue detectado en 2010, aun cuando se sospecha que ya en 2006 estaba operando en los sistemas informáticos. Tiene la capacidad de que al infectar el sistema comienza a realizar una compleja serie de operaciones, incluyendo espiar en el tráfico de internet, tomar imágenes de pantallas de computador, grabar conversaciones, interceptar teclados y demás[29], explicó Vitaly Kamluk, experto en *malware* de la empresa Kaspersky. Entre los países afectados se encuentran Irán, Israel, Sudán, Siria, Líbano, Arabia Saudita y Egipto.

Por su parte, el gusano informático *Stuxnet* presenta un mayor riesgo por cuanto espía y reprograma sistemas industriales, particularmente los SCADA (Supervisión, Control y Adquisición de Datos)[30], además cuenta con capacidad para afectar instalaciones industriales. En Irán, fue usado para afectar incluso infraestructura nuclear entre 2009 y 2010, donde atacó en forma reiterada cinco plantas a lo largo de 10 meses, según un análisis realizado por Symantec. Actualmente es considerado el primer virus para afectar sistemas industriales.

Junto a lo indicado, es posible constatar la proliferación de estos "*malware*" tal como se indica en el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas[31] donde son identificados los principales *malware* detectados en 2014, tal como se indica a continuación en la tabla 2.

Bajo un enfoque de la seguridad interior, los ciberdelitos también forman parte de los riesgos y amenazas en el ciberespacio. Muchas veces se trata de delitos que históricamente se han realizado y que ahora utilizan el ciberespacio para su realización. Por ejemplo, la venta de drogas a través de páginas de internet de difícil acceso (*deepweb*); estafas por medio de la clonación de tarjetas bancarias y; secuestro, pero ahora de cuentas de correo o aparatos electrónicos con acceso a internet (computadores, *tablets* o teléfonos inteligentes) los cuales son infectados con un tipo de virus informático que bloquea mails, ordenadores o teléfonos y exige dinero para el retorno de archivos[32] lo que se conoce como *ransomware*.

Se adiciona a lo indicado, que los tradicionales activistas también han encontrado un espacio para manifestarse. De este modo, los ciberhacktivistas han promovido sus causas por internet y para obtener la visibilidad necesaria han hackeado diversas páginas, ejemplo emblemático de ello ha sido *Anonymus*.

29 UNAM, 2012. Karpesky habla sobre el virus Flame. *UNAM,* 01-Jun-2012. Disponible en http://www.seguridad.unam.mx/noticia/?noti=377 [Consult. 17/9/2017].

30 Anabalón, J. y. Donders, E., 2014. Una revisión de ciberdefensa de infraestructura crítica. *Estudios de Seguridad y Defensa*, n.º 3, jun., pp. 131-164. Disponible en http://esd.anepe.cl/wp-content/uploads/2014/11/art5.pdf [Consult.17/9/2017].

31 Organización de los Estados Americanos (OEA), 2015a. *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. OEA, Abril de 2015, Secretaría de Seguridad Multidimensional de la OEA/Trend Micro. Disponible en https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf.

32 BBC, 2016. Así secuestraron mi teléfono los piratas informáticos. *BBC Mundo*, 4 de marzo. Disponible en http://www.bbc.com/mundo/noticias/2016/03/160304_tecnologia_telefono_smartphone_secuestro_il [Consult. 17/9/2017].

Tabla 2 – Las Principales Familias de *Malware* de 2014

Familia de Malware	Descripción
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente.
DUNIHI	Esta familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla manualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/ Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes.
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afecta.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosas, que van desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectado
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Fuente: Organización de los Estados Americanos (2015a).

No obstante, dada su estructura en red y anonimato en la acción y discurso, para la autoridad es muy difícil poder identificarlos y monitorearlos cuando sus acciones afectan el orden público[33].

33 Abad, J., 2015. Anonymus declara la guerra al ISIS: quiénes son y qué han conseguido. *El País*, 18 NOV, Madrid. Disponible en http://tecnologia.elpais.com/tecnologia/2015/11/17/actualidad/1447752730_293113.html [Consult. 17/9/2017].

Por este motivo es necesario dimensionar adecuadamente estas amenazas, perspectiva en la cual el profesor Nye nos orienta señalando:

> "Si bien se suele considerar al llamado "hacktivismo" de grupos ideológicos esencialmente como un fastidio molesto en esta etapa, siguen existiendo cuatro categorías importantes de ciberataques a la seguridad nacional, cada uno de ellos con un horizonte temporal diferente: la ciberguerra y el espionaje económico están en gran medida asociados con los estados, mientras que el delito cibernético y el ciberterrorismo están básicamente asociados con actores no estatales. Para Estados Unidos, los costos más elevados hoy en día surgen del espionaje y del delito, pero en la próxima década aproximadamente, la guerra y el terrorismo podrían convertirse en mayores amenazas de lo que son hoy"[34].

Entre los riesgos en el uso del ciberespacio, destaca la posibilidad de explotar la vulnerabilidad que genera la insuficiente protección de información sensible que se encuentre en formato electrónico. La filtración de información, particularmente desde los Servicios de Inteligencia – lo que constituye un problema de contrainteligência – puede afectar la seguridad de los países. Situaciones recientes, asociadas al clásico problema de la protección de la información sensible para evitar fugas y difusión no deseada de ella, han alcanzado alta visibilidad y recuerdan que el problema está vigente. Por ejemplo, algunas situaciones en los EE.UU. han generado repercusiones más allá de sus fronteras en diferentes continentes. Se trata de los casos protagonizados por el soldado Manning y el ex funcionario de la Agencia Nacional de Seguridad (NSA) Edward Snowden. Ambos accedieron a información secreta del Departamento de Defensa de EE.UU. y la difundieron a la opinión pública por medio de *Wikileaks*, produciendo problemas diplomáticos y de seguridad al gobierno norteamericano. En opinión del general Michael Hayden, Director de la Agencia Central de Inteligencia (CIA) y de la NSA durante el período de dos presidentes de Estados Unidos (Bill Clinton y George W. Bush), los documentos filtrados por Snowden han sido "la destrucción de secretos legítimos de Estados Unidos más grande de la historia de mi país (…) casi mil objetivos de inteligencia extranjeros han cambiado su comportamiento basándose en las revelaciones de Snowden"[35].

En síntesis, podemos afirmar que la mayor parte de las amenazas en el ciberespacio son transnacionales y se caracterizan por ser: flexibles (presentan una estructura horizontal), ambiguas (su arquitectura es difusa), globales (su ámbito de acción es transnacional) y versátiles (son capaces readaptarse al entorno). Asimismo, es importante tener presente que el ciberespacio puede ser un medio o un objetivo para la realización de ilícitos. En el primer caso se trata especialmente de prácticas delictuales con un daño limitado a personas, organizaciones o instituciones. En el segundo, la probabilidad de generar importantes daños a la infraestructura crítica del país (energía, comunicaciones, transporte, sistema

34 Nye, J. 2012. Ciberguerra y Ciberpaz. *Project Syndicate,* Apr 10. Disponible en https://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish?barrier=accesspaylog

35 Ximenéz, P., 2016. Michael Hayden: "Me preocupa que Trump pueda ser presidente". *El País*, 8 MAR, Los Ángeles. Disponible en http://internacional.elpais.com/internacional/2016/03/04/actualidad/1457076618_844331.html [Consult. 17/9/2017].

financiero, sanitario, de alimentación, entre otros) puede convertirse en un problema de seguridad nacional.

Recientes incidentes en el ciberespacio, ha dejado en evidencia la vigencia de la vulnerabilidad de los sistemas críticos de sistemas información. En efecto, hospitales en U. K[36], redes informáticas en Europa, América Latina y Asia fueron cerradas[37], gran cantidad de organizaciones, empresas y personas se vieron de diverso modo afectadas por el virus *WannaCry* que mutaba[38], dificultando encontrar el modo de detenerlo, quedando en evidencia las consecuencias de acciones como no colocar los parches[39] de seguridad en los sistemas informáticos que lo requieran.

2. La Ciberseguridad como Condición para el Normal Uso del Ciberespacio[40]

El ciberespacio presenta tanto fortalezas y oportunidades que es necesario potenciar, como debilidades y vulnerabilidades, que se requiere prevenir o neutralizar. Ante esta situación la ciberseguridad puede entenderse como una condición que requiere ser brindada para promover el uso del ciberespacio y evitar que incidentes, ciberataques, ciberdelitos entre otros, generen desconfianza en su uso. En esta perspectiva la ciberseguridad es un medio que permite alcanzar un objetivo y en ningún caso debe entenderse como un fin en si mismo.

La existencia de amenazas, riesgos y vulnerabilidades en el ciberespacio genera al menos dos desafíos. Por un lado, desarrollar una capacidad para prevenir y/o detectar oportunamente la ocurrencia de un ciberincidente e identificar su origen. Por otro, garantizar que la información virtual cumpla con los requisitos de: disponibilidad, integridad, oportunidad, confiabilidad, interoperabilidad robustez, trazabilidad, resiliencia y seguridad. Ambos deben estar contenidos en una política pública de ciberseguridad cuya existencia es responsabilidad de las máximas autoridades políticas del país y, en el caso de Chile, es una tarea en la cual aún se está trabajando, toda vez que ello va en particular beneficio de los ciudadanos debido a que "grandes organizaciones podrían tal vez, dotarse de una seguridad cibernética eficaz, pero las personas individuales y los grupos reducidos difícilmente podrían hallarse en condiciones de alcanzar tal objetivo"[41].

---

36 Guimón, P., 2017. Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero, *El País*, 12 May, Londres. Disponible en https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html [Consult. 17/9/2017]

37 Infobae, 2017. Ciberataque mundial impacta a instituciones estatales y privadas en "una dimensión nunca antes vista". *Infobae*. Disponible en http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/.

38 Palazuelos, F., 2017. China descubre una nueva mutación del virus responsable del ciberataque mundial. *El País*, 15 May, Pekin/Madrid. Disponible en https://elpais.com/tecnologia/2017/05/15/actualidad/1494835268_125044.html

39 BBC, 2017. Virus WannaCry: ¿corre peligro mi computadora? *BBC Mundo*. Redaccion, 12 de Mayo. Disponible en http://www.bbc.com/mundo/noticias-39904811

40 El desarrollo de este tema fue previamente abordado en Sancho (2016).

41 Laqueur, W., 2015. La guerra cibernética ("juegos de guerra"). *Vanguardia dossier*, N.º 54, pp. 6-15.

Ofrecer un mínimo de seguridad en el ciberespacio obliga a buscar respuesta a preguntas del tipo ¿cuáles son los desafíos que enfrentamos en el ciberespacio desde una perspectiva de seguridad? La respuesta obliga a identificar lo que es necesario proteger, es decir, "la información e infraestructura crítica" que podemos definirla como "aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad, o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros"[42].

En este ámbito, para lograr proteger la información crítica de un país implica considerar a diversos servicios y organizaciones estratégicas, lo cual obliga a convocar a actores de diversa naturaleza, provenientes de la administración civil del Estado y a las Fuerzas Armadas y de Orden y Seguridad, junto a variados estamentos dentro de la sociedad civil, quienes deben garantizar que esa información cumpla con las siguientes características: disponibilidad, integridad, oportunidad, confiabilidad, interoperabilidad, seguridad.

De acuerdo a lo indicado, la búsqueda de la seguridad en el ciberespacio requiere enfrentar desafíos nacionales e internacionales. Entre los nacionales cabe destacar al menos los siguientes:

(1) Formulación de una política pública de ciberseguridad, expresada en una Estrategia o Política Nacional de Ciberseguridad
(2) Creación de autoridades nacionales en materia de ciberseguridad y de una arquitectura del sistema de ciberseguridad nacional que contemple la participación de las principales entidades vinculadas al tema.
(3) Implementación de Centros especializados y coordinados en monitoreo, alarma y respuesta frente a ciberincidentes (CSIRT: Centro de Respuesta a Incidentes de Seguridad Informática/Computer Security and Incidente Response Team.
(4) Organización de entidades tipo CLCERT Grupo Chileno de Respuesta a Incidentes de Seguridad Computacional/Chilean Computer Emergency Response Team.
(5) Contemplar directrices que consideren, entre otros múltiples aspectos:
(6) Legislación específica y actualizada sobre el tema.
(7) Mejora de la capacidad de coordinación interagencial.
(8) Capacidad operacional para combatir el cibercrimen.
(9) Aspectos mínimos en la formulación de protocolos de ciberseguridad.
(10) Promover una cultura de ciberseguridad.
(11) Desarrollar recursos industriales y tecnológicos para la ciberseguridad.
(12) Disponer de planes para enfrentar ciberincidentes que contemplen acciones de prevención, respuesta, mitigación y ciberresiliencia.

42 del Moral Torres, A., 2010. *Cooperación Policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal.* ARI 50/2010, 17/03/2010, Real Instituto Elcano. Disponible en https://www.files.ethz.ch/isn/122470/ARI50-2010_cooperacion_policial_UE_inteligencia_criminal.pdf

Respecto a los desafíos internacionales, resultan de especial relevancia:

(1) Cooperación internacional ante ciberincidentes.
(2) Establecer estándares comunes en materia de ciberseguridad.
(3) Generación de instancias compartidas de formación profesional y de investigación académica en estas materias.
(4) Participación en foros multilaterales como son y la Conferencia Global del Ciberespacio, entre otros.

No obstante, es relevante considerar que estas medidas buscan reducir la vulnerabilidad del ciberespacio debido a que frente a la interrogante "¿Un lugar 100% seguro y privado, donde nadie pueda acceder a tus datos?"[43], la respuesta probablemente sería "Seguro que existe: en Siberia. Allá no hay teléfonos, conectividad, electricidad ni nada. Es por lejos el lugar más seguro que conozco", en opinión del experto Eugene Kaspersky.

43 Alaluf, A., 2013. Tecnología: La ciberseguridad de Mr. K. *Qué Pasa*, Agosto 15. Disponible en http://www.quepasa.cl/articulo/tecnologia/2013/08/23-12457-9-tecnologia-la-ciberseguridad-de-mr-k.shtml/

CAPÍTULO II
Cooperación Multilateral

Foros y acuerdos internacionales como instrumentos para regular el uso del ciberespacio y enfrentar los riesgos a la seguridad que en este se producen.

1. Organización de Naciones Unidas

Para abordar el tema de la ciberseguridad, la Organización de Naciones Unidas (ONU) dispone de organizaciones especializadas que realizan un tratamiento respecto de distintas dimensiones que afectan a la seguridad cibernética, a través de la emisión de informes técnicos y programas de diversa índole que permiten apoyar a los países para reforzar sus mecanismos de protección del ciberespacio. Dichas organizaciones, abogan por la necesidad de fortalecer las relaciones de cooperación multilateral como herramienta para hacer frente a la naturaleza de global de las amenazas a la ciberseguridad[44].

Una de ellas corresponde a la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés), organización que aborda distintos tópicos tales como corrupción, prevención del crimen, tráfico de drogas, lavado de dinero y tráfico de drogas entre otros. En este contexto, la evolución que presenta el crimen transnacional ha posicionado al cibercrimen como una de las materias que afectan a la seguridad global[45] y UNODC la ha incorporado como una tema específico a abordar[46].

De esta manera UNODC, se enfoca en promover la creación de capacidad sostenible y a largo plazo en contra la ciberdelincuencia, a través del apoyo a la acción y estructura nacional. De manera más específica, la UNODC a partir de su experiencia especializada en los sistemas de justicia penal, entregan asistencia técnica en materia de creación de capacidad, prevención y sensibilización, además de la cooperación internacional, recopilación de datos, investigación y análisis sobre cibercrimen[47].

Para abordar la complejidad del ciberdelito, la UNODC dispone de programas como reuniones para acordar, diseñar e implementar medidas que vayan a favor de la protección cibernética. El Programa Global contra el Cibercrimen, en conformidad con la resolución 65/230 de la Asamblea General, junto con la resolución 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, está encargado de ayudar a los distintos Estados miembro en la lucha contra los delitos que dicen relación con el ciberespacio, a través de la constante capacitación y asistencia técnica[48]. Para ello, el Programa se enfoca

44 Naciones Unidas, 2012. La UIT pide reforzar la ciberseguridad. *Noticias ONU*, 31 Mayo. Disponible en http://www.un.org/spanish/News/story.asp?newsID=23582#.Wd_gFVvWzcc

45 United Nations Office on Drugs and Crime (UNODC). *Cybercrime*. [website] Disponible en https://www.unodc.org/unodc/es/cybercrime/index.html.

46 Al respecto ver UNODC. *Cybercrime*. [website] Disponible en https://www.unodc.org/unodc/es/cybercrime/index.html.

47 *Ibidem*.

48 *Ibidem*.

específicamente en aquellos países en desarrollo para responder de forma flexible a sus necesidades y de esa forma, apoyarlos en la prevención y el combate del delito cibernético. En efecto, el Programa se enfoca en América Central, África Oriental, Medio Oriente y Norte de África, el Sudeste Asiático y el Pacífico, en base a tres objetivos[49]. El primero de ellos tiene relación con el aumento de la eficiencia y la eficacia en la investigación, enjuiciamiento e imputación del cibercrimen, especialmente el abuso y explotación sexual infantil en línea, enmarcados en una perspectiva de Derechos Humanos. En segundo lugar, el Programa busca entregar respuestas eficientes y eficaces que sean sostenibles a largo plazo por parte de los gobiernos contra la ciberdelincuencia, lo que incluiría mecanismos de coordinación nacional, recopilación de datos y la creación de marcos legales efectivos. Por último, el fortalecimiento de instancias de comunicación tanto a nivel nacional como internacional, entre el gobierno, quienes aplican la ley y el sector privado[50].

Finalmente, la ONU ha publicado una serie de resoluciones y manuales que buscan complementar los esfuerzos realizados en materia de ciberseguridad y son sistematizados[51] en la tabla 3.

Tabla 3 – Principales Resoluciones de ONU sobre Ciberseguridad

Resoluciones de la Asamblea General	Resoluciones de Ecosoc (Consejo Económico y Social)	Documentos y Publicaciones de UNODC	Manuales
Resolución aprobada por la Asamblea General A/RES/55/63 del 22 de Enero de 2001 sobre la lucha contra la utilización de la tecnología de la información con fines delictivos	ECOSOC Resolución 2004/26 del 21 de Julio de 2004 sobre cooperación internacional para prevenir, investigar, enjuiciar y castigar el fraude, la utilización delictiva y la falsificación de identidad y delitos afines	UNODC Core Group of Experts on Identity Related Crime	Manual de las Naciones Unidas sobre la prevención y control de los delitos relacionados con los sistemas de cómputo de 1994
Resolución aprobada por la Asamblea General A/RES/56/121 del 23 de Enero de 2002 sobre la lucha contra la utilización de la tecnología de la información con fines delictivos	ECOSOC Resolución 2004/42 del 21 de Julio de 2004 sobre la venta de drogas ilícitas a través de internet	Notas de la Quinta Reunión del Grupo de Expertos sobre Delitos relacionados con la Identidad, Viena, Austria, 6-8 de Diciembre de 2010	

CONTINUA NA PÁGINA SEGUINTE →

49 *Ibidem.*

50 *Ibidem.*

51 Resoluciones clasificadas por organismo internacional y año. Ver Ciberdelincuencia.Org [Website]. Disponible en http://ciberdelincuencia.org/fuentes/resoluciones.php

Resoluciones de la Asamblea General	Resoluciones de Ecosoc (Consejo Económico y Social)	Documentos y Publicaciones de UNODC	Manuales
Resolución aprobada por la Asamblea General A/RES/57/239 del 31 de Enero de 2003 sobre la creación de una cultura global de la ciberseguridad	ECOSOC Resolución 2007/20 del 26 de Julio de 2007 sobre cooperación internacional para impedir, investigar, enjuiciar y castigar el fraude económico y los delitos de usurpación de identidad conexos	UNODC, "The Globalization of Crime. A Transnational Organized Crime Threat Assesment" (Chapter 10 Cybercrime), (2010)	
Resolución aprobada por la Asamblea General A/RES/58/199 de 30 de Enero de 2004 sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales			

Fuente: Elaboración propia según página ONU (2017).

Otra de las organizaciones internacionales que ha participado activamente en materia de ciberseguridad es la Unión Internacional de Telecomunicaciones (UIT). Esta organización, se encarga de fomentar la cooperación internacional, además de la prestación de asistencia técnica, creación, desarrollo y perfeccionamiento de redes y equipos de telecomunicación junto con tecnologías de la información y telecomunicación (TIC) en países en desarrollo.

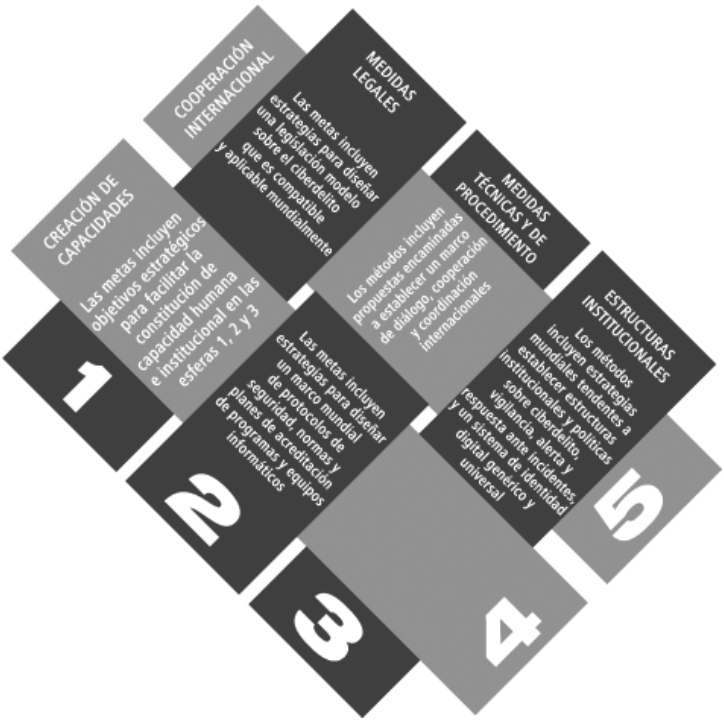
Especial referencia merece la "Agenda sobre Ciberseguridad Global", la cual fue "lanzada en 2007 por el Dr. Hamadoun I. Touré, Secretario General de la UIT, es un marco de cooperación internacional destinado a mejorar la seguridad y la confianza en la sociedad de la información"[52] que ha encontrado apoyo en destacados líderes internacionales y se orienta a ayudar a los países en la promoción de la ciberseguridad. Esta agenda contempla la promoción de cinco aspectos que requieren ser promovidos en materia de ciberseguridad: medidas legales, medidas técnicas y de procedimiento, estructuras internacionales, creación de capacidades y cooperación internacional, tal como se ilustra en la figura 5.

Entre las acciones desarrolladas por la UIT destaca la creación de un "Centro de respuesta global" el cual "colaborará con asociados de los sectores público, privado y

52 Al respecto ver en la página web de la Unión Internacional de Telecomunicaciones (UIT), s.d.. La Agenda sobre Ciberseguridad Global. UIT. Disponible en https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html

académico, ofrecerá a la comunidad mundial un "Sistema de alerta temprana de red" (NEWS, *Network Early-Warning System*) constantemente disponible y en tiempo real que ayudará a identificar las amenazas y proporcionaría orientaciones sobre las medidas que se han de tomar. También dará a los Estados Miembros de la UIT acceso a instrumentos y sistemas especializados tales como la recientemente desarrollada "Plataforma de aplicación colaborativa electrónicamente segura para expertos" (ESCAPE, *Electronically Secure Collaborative Application Platform for Experts*), con la cual expertos de varios países podrán aunar recursos y colaborar a distancia en un entorno seguro, y que dispone de una base de datos completa y evolutiva de recursos esenciales de todo el mundo a los que se puede recurrir en caso de crisis. La UIT aportará conocimientos granjeados en sus investigaciones sobre la ciberseguridad, así como su experiencia en la creación de plataformas de colaboración en línea"[53].

Figura 5 – Principales Aspectos Promovidos por la Agenda Global de Ciberseguridad de la UIT



Fuente: ITU (2017).

53 Unión Internacional de Telecomunicaciones (UIT), s.d.. La Agenda sobre Ciberseguridad Global. *UIT*. Disponible en https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html

Junto a los mecanismos que desarrolla la UIT para posicionar una agenda y cultura de ciberseguridad, es posible reconocer herramientas como la creación de estrategias nacionales que sean capaces de responder a los riesgos y necesidades que representa la creciente interconectividad e interdependencia que las redes han generado a nivel global. Para ello, se generan guías de referencia que permitan la comprensión del propósito, contenido y alcance de una estrategia nacional de ciberseguridad, además de los mecanismos necesarios para generarla[54]. Considerando que no basta con la generación de una estrategia para afrontar los diversos desafíos que la seguridad cibernética, si no existen los mecanismos legales que respalden a dicha estrategia. Por ello la UIT se encarga además de brindar asesoría personalizada para la creación de capacidad respecto de la legislación atingente en materia de ciberseguridad a más de cincuenta países del globo[55].

Dentro de las publicaciones y programas que genera la UIT, es posible encontrar el Índice Mundial de Ciberseguridad, cuyo objetivo radica en impulsar el tema de la seguridad cibernética y así posicionarlo hasta el primer plano de las agendas nacionales[56] y el Programa CIRT, enfocado en la creación de equipos de respuesta a incidentes, siendo 102 los que actualmente se encuentran vigentes[57]. Con lo anterior, al igual que Naciones Unidas, la UIT ha emitido una serie de resoluciones, folletos, lineamientos y reportes que dan cuenta de la situación actual en materia de ciberseguridad[58] como se sistematiza en la tabla 4.

Tabla 4 – Principales Publicaciones de UIT sobre Ciberseguridad

Resoluciones	Folletos	Lineamientos	Reportes
UIT WTSA Resolución 58: Fomentar la creación de equipos nacionales de respuesta a incidencias de cómputo, especialmente para los países en desarrollo (Johannesburgo Octubre de 2008)	Cybersecurity Brochure	UIT, "El Ciberdelito: Guía para los Países en Desarrollo", Abril de 2009	Global Strategic Report (2008)
UIT WTSA Resolución 52: Reduciendo y Combatiendo Spam (Johannesburgo Octubre de 2008)		Entendiendo el Cibercrimen: Una Guía para los Países en Desarrollo (Mayo de 2009)	IUT. Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar (2015)

CONTINUA NA PÁGINA SEGUINTE →

54 International Telecommunication Union (ITU), s.d.a. National Strategies. *ITU*. Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

55 International Telecommunication Union (ITU), s.d.b. Legal Measures. *ITU*. Disponible en https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx

56 International Telecommunication Union (ITU), 2015. Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar. ITU Informe, Abril de 2015. Disponible en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf.

57 International Telecommunication Union (ITU), s.d.c. CIRT Programe. *ITU*. Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.

58 Ciberdelincuencia.Org [Website]. Disponible en http://ciberdelincuencia.org/fuentes/resoluciones.php

Resoluciones	Folletos	Lineamientos	Reportes
UIT WTSA Resolución 50: Ciberseguridad (Johannesburgo Octubre de 2008)		ITU Toolkit for Cybercrime Legislation (Mayo de 2009)	
UIT Resolución 149 Estudio de definiciones y terminología relacionada a brindar confianza y seguridad en el uso de las tecnologías de información y comunicaciones. (Antalya 2006)		Guía de Ciberseguridad para los Países en Desarrollo	
UIT Resolución 130 Fortaleciendo el Rol de la UIT en brindar confianza y seguridad en el uso de las tecnologías de información y comunicaciones. (Antalya 2006)			
UIT Resolución 45: Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluyendo el combate al spam (Doha 12 de Abril de 2006)			
ITU WTSA Resolución 50: Ciberseguridad (Florianpolis, 2004).			
ITU WTSA Resolución 51: Combatiendo el spam (Florianpolis, 2004)			

Fuente: Elaboración propia según página UIT (2017).

2. União Europeia

A UE dispõe de um extenso quadro normativo nos domínios da cibersegurança e ciberdefesa, supletivo e/ou enquadrador das políticas e capacidades nacionais e das instituições europeias envolvendo nomeadamente, a Estratégia Global da União Europeia, a Estratégia de Cibersegurança da União Europeia, Proteção das Infraestruturas de Informação Críticas, as decisões dos Conselhos Europeus, a Política-Quadro da Ciberdefesa da União Europeia (EU Cyber Defence Policy Framework), a Diretiva de Segurança das Redes e da Informação (NIS) e o Regulamento Geral sobre a Proteção de Dados (RGPD).

2.1. Estratégia Global da União Europeia

A *Estratégia Global da União Europeia* (European External Action Service, 2016) realça a indissociabilidade entre os interesses e os valores da UE. A "paz e segurança", "prosperidade", "democracia" e uma "ordem mundial assente em regras" continuam a representar os interesses vitais subjacentes à ação externa da União, sendo que a prosperidade depende da circulação de informação de forma livre e segura através da internet, supor-

tada pela "revolução digital". O documento enuncia quatro princípios fundamentais subjacentes à Estratégia – unidade, empenhamento, responsabilidade e parcerias – e identifica cinco prioridades da ação externa[59].

No domínio da prioridade "Segurança da União", o terrorismo, as ameaças híbridas[60], a volatilidade económica, as alterações climáticas e a insegurança energética são consideradas ameaças fundamentais que requerem um "adequado nível de ambição e de autonomia estratégica" para promoção da paz e garantia da segurança dentro e fora das fronteiras da UE, a concretizar e intensificar através de cinco linhas de ação estratégicas[61].

No âmbito da linha de ação "Segurança e Defesa" – integrada na prioridade "A Segurança da União" –, os Estados-membros são instados a concretizarem os "compromissos de assistência mútua e solidariedade consagrados nos tratados", enquanto a UE manifesta a sua intenção de reforçar a cooperação com os seus parceiros, nomeadamente com a NATO, e a assistência aos Estados-membros, entre outros, nos domínios da investigação, tecnologias de defesa e cooperação multinacional.

No plano da "Luta contra o Terrorismo", a estratégia pretende incentivar a partilha de informação[62] e cooperação entre os serviços de informações dos Estados-membros e agências da UE, o apoio da UE aos Estados-membros na sua rápida recuperação, em caso de atentado, através de medidas no âmbito da segurança do aprovisionamento, proteção das infraestruturas críticas e reforço de um quadro voluntário de gestão de crises cibernéticas.

As instituições da União Europeia tencionam reforçar a sua "Cibersegurança" através de meios próprios e auxiliar os Estados-membros na proteção contra as ciberameaças, através do reforço de capacidades tecnológicas que permitam reduzir as ameaças, aumentar a resiliência das infraestruturas críticas, redes e serviços e diminuir a cibercriminalidade. Nesse sentido, a UE preconiza a promoção de Sistemas e Tecnologias de Informação e Comunicação (TIC) inovadoras, que permitam assegurar a disponibilidade[63] e a integridade[64] dos dados[65], assim como a garantia da segurança do "espaço digital" (cibe-

59 A segurança da União, resiliência do Estado e da sociedade a leste e a sul, uma abordagem integrada dos conflitos, ordens regionais de cooperação e governação mundial para o século XXI.

60 "Hybrid warfare can be more easily characterised than defined as a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces". European External Action Service, 2015. *Food-for-thought paper "Countering Hybrid Threats"*. EEAS(2015) 731, 13 May. Disponível em: http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.

61 Segurança e defesa, luta contra o terrorismo, cibersegurança, segurança energética e comunicação estratégica.

62 Nomeadamente através de alertas sobre extremismo violento, redes terroristas e combatentes terroristas estrangeiros, bem como o acompanhamento e a supressão de conteúdos ilegais dos *media*.

63 Por definição "disponibilidade" representa a "(…) Property of being accessible and usable upon demand by an authorized entity". International Organization for Standardization (ISO), *2016b. ISO/IEC 27000:2016, Information security management systems: Overview and vocabulary*. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

64 Por definição, a "integridade" dos dados representa a "Property of accuracy and completeness". *Ibidem*.

65 A confidencialidade, integridade, disponibilidade e autenticidade são características básicas da segurança da informação.

respaço) europeu, através de políticas de armazenagem de dados e a certificação de produtos e serviços digitais. Tal requererá a integração das questões cibernéticas em todos os domínios de intervenção (políticas), o reforço da cibersegurança das missões e operações da Política Comum de Segurança e Defesa (PCSD) e a expansão do desenvolvimento de plataformas de cooperação.

A UE tenciona apoiar a cooperação política, operacional e técnica entre os Estados-membros no domínio cibernético, na análise e gestão das consequências das crises cibernéticas e promoção da partilha de informação (avaliação das ameaças) entre as estruturas da UE e as instituições competentes dos Estados-membros, e o reforço da cooperação com os seus principais parceiros, nomeadamente EUA e NATO. A abordagem da UE valorizará o estabelecimento de parcerias público-privadas e a cooperação e partilha de informação entre Estados-membros, instituições, setor privado e a sociedade civil visando a promoção de uma cultura de cibersegurança e resiliência.

A prioridade "Resiliência do Estado e da Sociedade a Leste e a Sul da UE" estabelece a promoção da resiliência, enquanto "capacidade de os Estados e as sociedades se reformarem, enfrentando e superando desse modo as crises internas e externas" (European External Action Service, 2016), das regiões circundantes da UE através de quatro linhas de ação estratégicas, e a intenção de apoiar os "Estados frágeis" no desenvolvimento de capacidades, nomeadamente de cibersegurança.

A prioridade "Ordens Regionais de Cooperação"[66] preconiza na sua linha de ação *Um Atlântico Mais Coeso,* a intenção de aprofundar a parceria com a NATO através da coordenação do desenvolvimento de capacidades de defesa e exercícios que favoreçam o combate das ameaças híbridas e ciberameaças e a cooperação com os EUA e o Canadá, em iniciativas no âmbito da gestão de crises, combate ao terrorismo e cibersegurança.

Através da prioridade "Governação Mundial para o Século XXI" o documento reflete sobre a necessidade de normas internacionais globais e meios para forçar a sua adoção por forma a proteger os interesses vitais – paz, segurança, prosperidade e democracia – da UE, no quadro do Direito Internacional e da Carta das Nações Unidas.

Visando a proteção das infraestruturas e informação digital críticas europeias, pretende intervir ativamente no ciberespaço através da ciberdiplomacia e parcerias, nomeadamente na promoção da internet livre e segura, defesa de um comportamento responsável dos Estados com base no Direito Internacional, governação digital multilateral e um quadro mundial de cooperação no domínio da cibersegurança.

2.2. Estratégia da UE para a Cibersegurança

A *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (European Commission, 2013) propõe medidas que permitem melhorar o desempenho da União através da intervenção das instituições europeias, Estados-membros e indústria, numa visão articulada em cinco prioridades fundamentais: (1) resiliência cibernética; (2) redução drástica da criminalidade cibernética; (3) política e capacidades de ciberdefesa no

66 Contempla uma combinação de relações bilaterais, sub-regionais, regionais e inter-regionais.

âmbito da PCSD; (4) recursos industriais e tecnológicos para a cibersegurança; (5) política internacional coerente em matéria de ciberespaço para a UE e promoção dos valores fundamentais da UE[67].

A resiliência cibernética requer que as instituições do setor público e as empresas do setor privado dos Estados-membros cooperem de forma efetiva e desenvolvam capacidades específicas, podendo a UE apoiar na limitação dos riscos e ameaças cibernéticas transfronteiriças e coordenação em situações de emergência cibernética. A estratégia reconhece, contudo, a existência de limitadas capacidades, recursos e processos exigidos na prevenção, deteção e resolução de incidentes cibernéticos na UE, vulnerabilidades que importa obviar.

Complementarmente, a Diretiva-Quadro para as Comunicações Eletrónicas[68] estabelece o dever das empresas, que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, tomarem "medidas técnicas e organizacionais apropriadas para gerir adequadamente os riscos para a segurança das redes e serviços", garantir a "integridade das suas redes, assegurando assim a continuidade do fornecimento dos serviços que utilizam essas redes" e notificar a autoridade reguladora nacional competente – Autoridade Nacional de Comunicações (ANACOM) – de "qualquer violação da segurança ou perda da integridade que tenha tido um impacto significativo no funcionamento das redes ou serviços" (European Parliament, 2009).

A *Política de Segurança das Redes e da Informação*, mais conhecida por Diretiva NIS-Network Information Security (European Parliament, 2016a), enuncia um conjunto de medidas para prevenir incidentes cibernéticos na Europa, nomeadamente:

67 A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos Direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias, Art.º 2.º, do Tratado da UE. European Union, 2016. Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. *Official Journal of the European Union*, C 202, Volume 59, 7 June 2016. Disponível em http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG. Segundo a Estratégia de Cibersegurança da UE, "(…) devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico". European Commission, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN(2013) 1 final, 7.2.2013, Brussels, High Representative of the European Union for Foreign Affairs and Security Policy. Disponível em European Union External Affairs, Archives: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

68 European Parliament and Council of the European Union, 2002. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). *Official Journal of the European Union*, L108, EN, 24.4.2002. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=EN; alterada pela European Parliament and Council of the European Union, 2009. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance). *Official Journal of the European Union*, L337, EN, 18.12.2009. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140&from=EN.

(1) O estabelecimento de requisitos nacionais mínimos e comuns para a segurança das redes e da informação, visando obrigar os Estados-membros a: (a) designar as autoridades nacionais competentes em matéria de Segurança das Redes e da Informação (SRI); (b) criar uma CERT[69]; (c) e adotar uma estratégia nacional para a SRI e um plano nacional de cooperação para a SRI.
(2) A criação do CERT-EU[70] de modo permanente para dar resposta a emergências informáticas e de segurança dos sistemas informáticos das instituições, agências e organismos da UE.
(3) A criação de mecanismos de prevenção, deteção, atenuação e resposta, permitindo a partilha de informação e assistência mútua entre as autoridades nacionais competentes no domínio da SRI.
(4) A melhoria da preparação e empenhamento do setor privado, através do desenvolvimento de uma adequada cultura de cibersegurança, capacidades técnicas próprias de resiliência cibernética, adequada gestão dos riscos e partilha das "melhores práticas".

Esta diretiva pretende ainda que as empresas privadas responsáveis por um extenso conjunto de infraestruturas críticas[71] avaliem os riscos de cibersegurança que enfrentam, assegurem a fiabilidade e resiliência das respetivas redes e sistemas de informação através de uma adequada gestão de risco e partilhem informação com as autoridades nacionais competentes em matéria de SRI. A UE sugere ainda a cooperação informal e voluntária entre os setores público e privado, para reforçar os níveis de segurança e o intercâmbio de informações e melhores práticas[72].

Na prioridade relativa à criminalidade cibernética, a coordenação e colaboração das autoridades policiais dos diversos Estados-membros são consideradas essenciais e enunciadas três linhas de ação fundamentais: (1) legislação rigorosa e eficaz; (2) meios operacionais acrescidos para combater a cibercriminalidade; (3) melhor coordenação.

No plano legislativo, a estratégia recomenda a produção de legislação rigorosa e eficaz e a ratificação da *Convenção do Conselho da Europa sobre Cibercriminalidade* (Council of

69 Computer Emergency Response Teams "CERT (…) is a name and a registered service mark. (…) of Carnegie Mellon University. CERT Coordination Center (CC) was the first computer security incident response team (CSIRT). When referring to incident response teams, use the general term CSIRT and not the registered mark CERT". West-Brown, M. J. *et al.*, 2003. *Handbook for Computer Security Incident Response Teams* (CSIRTs). Disponível em http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.

70 Estabelecido em 2012, Computer Emergency Response Team (CERT-EU). [Website] Disponível em https://cert.europa.eu/cert/plainedition/en/cert_about.html.

71 Energia, transportes, banca, bolsas de valores, *enablers* de serviços essenciais da internet e administração pública.

72 A cooperação entre o setor público e setor privado é considerada essencial, uma vez que a maioria das redes e dos sistemas de informação são explorados pelo setor privado. European Parliament and Council of the European Union, 2016a. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L194, EN, 19.7.2016. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Europe, 2001a; 2001b; 2001c), com caráter vinculativo, aos Estados-membros que ainda o não fizeram. Nesse sentido, Portugal já ratificou a referida convenção e aprovou a *Lei do Cibercrime*, tendo transposto para a ordem jurídica interna a *Decisão-Quadro n.º 2005/222/JAI*, do Conselho da União Europeia, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação, e adaptado o direito interno à mesma (Assembleia da República, 2009). Entretanto, a UE já adotou legislação relativa à cibercriminalidade e à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil (European Parliament, 2011) e sobre ataques a sistemas de informação[73].

Quanto aos meios operacionais requeridos para combater a cibercriminalidade, a estratégia reconhece as limitações dos Estados-membros, pelo que a Comissão pretende:

(1) Apoiar os Estados-membros na identificação das lacunas e no reforço da sua capacidade para investigar e combater a cibercriminalidade através do Internal Security Fund (European Commission, 2016).
(2) Apoiar a articulação entre a investigação e as universidades, os agentes policiais/judiciais e o setor privado.
(3) Coordenar os esforços para identificar as melhores práticas e técnicas disponíveis para combater a cibercriminalidade – *e.g.* ferramentas forenses ou análise das ameaças.
(4) Cooperar com o Centro Europeu da Cibercriminalidade (EC3) para harmonizar as abordagens políticas com as melhores práticas operacionais.

No âmbito da linha de ação "Uma melhor coordenação a nível da UE", pretende-se facilitar a adoção de uma abordagem coordenada e colaborativa, entre as autoridades policiais e judiciais, setores público e privado da União e internacionais, envolvendo a Europol (EC3), Academia Europeia de Polícia (CEPOL) e o EUROJUST[74].

Na prioridade associada à ciberdefesa no âmbito da Política Comum de Segurança e Defesa, a estratégia enfatiza a concentração das capacidades de deteção e resposta às ameaças cibernéticas sofisticadas por forma a assegurar a resiliência dos Sistemas de Informação e Comunicação (SIC) que apoiam as políticas de defesa e os interesses no domínio da segurança dos Estados-membros. A UE entende ainda existirem benefícios do reforço da cooperação civil-militar, apoiada por Investigação e Desenvolvimento (I&D) e cooperação intergovernamental com o setor privado e as universidades. Para reforçar a resiliência das infraestruturas críticas governamentais, da defesa e outras infraestruturas de informação comuns, a UE pretende aprofundar a cooperação com a NATO evitando a duplicação de capacidades.

---

73 European Parliament and Council of the European Union, 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union*, L218, EN, 14.8.2013. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN. De referir que a Diretiva-Quadro substituída tinha sido transposta para a ordem jurídica interna através da Lei n.º 109/2009 de 15 de Setembro, Lei do Cibercrime.

74 European Union's Judicial Cooperation Unit (EUROJUST). [Website] Disponível em: http://www.eurojust.europa.eu

A estratégia enuncia um conjunto de ações a patrocinar pela Alta Representante (European External Action Service, 2016a), para as quais solicita o apoio dos Estados-membros e da EDA, nomeadamente: (1) a avaliação dos requisitos operacionais de ciberdefesa; (2) o desenvolvimento de capacidades e tecnologias; (3) o desenvolvimento o quadro político de ciberdefesa (gestão dos riscos, análise das ameaças e partilha de informação); (4) o estabelecimento de um programa de formação e exercícios de ciberdefesa; (5) o diálogo e coordenação civil-militar[75]; (6) a cooperação internacional com a NATO, e outras organizações internacionais e centros de excelência multinacionais.

A prioridade associada ao desenvolvimento de Recursos Industriais e Tecnológicos para a cibersegurança decorre da perceção de riscos de dependência tecnológica e segurança, pelo recurso a produtos e serviços de TIC e segurança produzidos maioritariamente fora da UE. A estratégia considera fundamental que os componentes de *hardware* e *software*, produzidos na UE e em países terceiros utilizados em serviços e infraestruturas críticas e dispositivos móveis, sejam confiáveis, seguros e permitam garantir a proteção dos dados pessoais. As linhas de ação a prosseguir englobam: (1) a promoção de um mercado único dos produtos de cibersegurança; (2) e a promoção de investimentos em I&D e em inovação.

A promoção de um mercado único de produtos de "cibersegurança" contribuirá para elevar o nível global da segurança da UE, pela incorporação requisitos de segurança em toda a cadeia de valor dos produtos TIC utilizados na Europa (fabricantes de equipamentos e *software* e fornecedores de serviços), pretendendo-se adotar medidas nos seguintes domínios:

(1) Procura de produtos de alta segurança no mercado europeu;
(2) Gestão dos riscos e a adoção de normas e soluções de segurança;
(3) Sistemas de certificação da UE e internacionais;
(4) Adoção de abordagens coerentes entre os Estados-membros;
(5) Criação de normas de segurança;
(6) Sistemas de certificação voluntários no domínio da computação em nuvem;
(7) Proteção de dados pessoais;
(8) Segurança da cadeia de abastecimento, em especial nos setores económicos críticos – sistemas de controlo industrial, infraestruturas energéticas e de transportes.

A estratégia antecipa que o investimento em I&D favorecerá a indústria europeia, o desenvolvimento do mercado interno e a redução da dependência da Europa de tecnologias de países fora do espaço da UE, pelo que deverá estar orientado para: (1) obviar as limitações de segurança das TIC; (2) antecipar soluções para os problemas de segurança do futuro; (3) tomar em consideração a constante evolução dos requisitos dos utilizadores; (4) tirar partido das tecnologias de duplo-uso[76]; (5) apoiar o desenvolvimento da criptografia.

75 Intercâmbio de boas práticas, o intercâmbio de informações, o alerta precoce, a resposta a incidentes, a avaliação dos riscos, a sensibilização e a atribuição de prioridade à cibersegurança.

76 Civil e militar (*dual use*).

A estratégia:

(1) Incentiva os Estados-membros a: (a) estimularem o desenvolvimento e implementação de especificações de segurança nos produtos e serviços TIC, como boa prática na contratação pública; (b) envolverem as empresas e universidades no desenvolvimento e coordenação das soluções.

(2) Suscita a cooperação: (a) da EUROPOL e ENISA na identificação das novas tendências da cibercriminalidade e da segurança cibernética, e na identificação de requisitos que suportem o desenvolvimento de ferramentas e tecnologias digitais forenses; (b) e dos setores públicos e privados e do setor dos seguros, no desenvolvimento de métricas de cálculo de prémios de risco que favoreçam o investimento em segurança.

A política e o envolvimento internacional da UE relativamente ao ciberespaço é pautada pelos valores fundamentais[77] e privilegia:

(1) A abertura e liberdade da internet;
(2) O estabelecimento de normas de conduta;
(3) A aplicação do direito internacional no ciberespaço;
(4) A promoção da redução da clivagem digital;
(5) A construção de uma capacidade cibersegurança.

Esta prioridade enuncia duas linhas de ação fundamentais:

(6) Integrar as questões do ciberespaço nas relações externas da UE e na PESC;
(7) Reforçar as capacidades de cibersegurança e a resiliência das infraestruturas de informação em países terceiros.

A estratégia sugere, aos vários atores envolvidos – Comissão, Alta Representante e Estados-membros –, uma política que promova um maior empenhamento e o reforço das relações com os principais parceiros[78] e organizações internacionais[79], bem como com a sociedade civil e o setor privado. A acessibilidade à internet favorece as reformas democráticas, pelo que, os progressos alcançados no domínio da conectividade não devem ser contraditados pela censura ou vigilância dos Estados.

A UE apoiará a definição de normas de conduta e medidas para o ciberespaço que promovam a confiança, a transparência e a redução do risco de mal-entendidos entre Estados, sem contudo promover novos instrumentos jurídicos internacionais. Para a União, as obrigações legais consagradas no Pacto Internacional sobre os Direitos Civis e Políticos (United Nations, 1966b), a Convenção Europeia dos Direitos do Homem (1950) e a Carta dos Direitos Fundamentais da União Europeia (2000) são aplicáveis e devem ser igualmente respeitadas no espaço virtual. No combate à cibercriminalidade, a Convenção de Budapeste de 2001 é considerada como base para o direito interno e a cooperação internacional neste domínio. Em caso de escalada de conflitos armados,

77 Dignidade humana, a liberdade, a democracia, a igualdade, o Estado de Direito e o respeito pelos direitos fundamentais.

78 Grupo de Trabalho UE-EUA para a Cibersegurança e a Cibercriminalidade.

79 O Conselho da Europa, a OCDE, a ONU, a OSCE, a NATO, a UA, a ASEAN e a OEA.

deverá ser aplicado o Direito Internacional Humanitário (Deyra, 2001) e, eventualmente, a legislação sobre os Direitos do Homem[80].

O reforço das capacidades de cibersegurança e a resiliência das infraestruturas de informação em países terceiros beneficia da cooperação internacional que consagre, nomeadamente, o intercâmbio de melhores práticas, a partilha de informação, exercícios de alerta precoce e de gestão conjunta de incidentes, etc. Para a consecução deste objetivo, a UE pretende reforçar as redes de cooperação entre os governos e o setor privado que visam a proteção das infraestruturas críticas da informação.

A estratégia enuncia ainda um extenso conjunto de iniciativas da Comissão e da Alta Representante, em cooperação com os Estados-membros nos âmbito da:

(1) Proteção dos direitos fundamentais;
(2) Apoio ao desenvolvimento de capacidades no acesso à informação, prevenção e combate de acontecimentos acidentais, cibercriminalidade e ciberterrorismo;
(3) Capacitação em cibersegurança;
(4) Proteção de infraestruturas de informação críticas;
(5) Cooperação entre as autoridades competentes em matéria de SRI.

2.3. Regulamento Geral de Proteção de Dados

O *Regulamento Geral de Proteção de Dados* (RGPD) (European Parliament, 2016b) passará a ser aplicado diretamente a partir de 25 de maio de 2018, substituindo a atual diretiva comunitária[81] e a *Lei de Proteção de Dados Pessoais*[82] em Portugal. Enquanto regulamento, "tem caráter geral, é vinculativo em todos os seus elementos e diretamente apli-

80 A Lei Internacional de Direitos Humanos é constituída pela Declaração Universal dos Direitos do Homem, United Nations (UN), 1948. Universal Declaration of Human Rights. *UN*. Disponível em. http://www.un.org/en/universal-declaration-human-rights/. Pacto Internacional dos Direitos Civis e Políticos, United Nations (UN), 1976. International Covenant on Civil and Political Rights. Adopted by the General Assembly of the United Nations on 19 December 1966, *UN*, Treaty Series, vol. 999, No. 14668. Disponível em https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Pacto Internacional dos Direitos Económicos United Nations (UN), 1966a. International Covenant on Economic, Social and Cultural Rights. *UN*, Treaty Series, Vol. 993, New York, 16 December. Disponível em: https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/iv-3.en.pdf; United Nations (UN), 1966b. *International Covenant on Economic, Social and Cultural Rights*. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A of 16 December 1966 (XXI) entry into force 3 January 1976, in accordance with article 27, UN. Disponível em http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf

81 European Parliament and Council of the European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, No L 281, EN, 23.11.95. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

82 *Lei n.º 67/98* de 26 outubro. Assembleia da República, 1998. Lei n.º 67/98 de 26 Outubro. Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva no. 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). *Diário da República*, I Série-A, N.º 247, pp. 5536-5546. Disponível em https://dre.pt/application/conteudo/239857.

cável" pelos particulares, Estados-membros, instituições da União, não devendo ser "objeto de um ato nacional de transposição" (European Parliament, 2017).

O RGPD introduz mudanças significativas com impacto diferenciado na vida das organizações, consoante a sua natureza, área de atividade, dimensão e tipo processamento de dados pessoais realizados (CNPD, 2017), nomeadamente:

(1) Devem ser respeitados os princípios gerais relativos ao tratamento de dados pessoais[83] e os princípios de proteção de dados[84] desde a sua conceção e por defeito.

(2) É exigida a fundamentação legal para o tratamento de dados[85] e estabelecida a possibilidade de ser apresentada queixa junto das autoridades de controlo nacionais – em Portugal, a CNPD[86].

(3) Os direitos dos sujeitos titulares dos dados são expandidos[87], alargada a noção de consentimento e introduzidas novas condições para a sua obtenção, em especial no caso de menores ou dos seus representantes legais, assim como os tipos de categorias especiais[88] de dados que passaram a ser consideradas dados sensíveis[89].

(4) O regulamento realça a figura do encarregado da proteção de dados (DPO), detalhando a sua designação, posição e funções e a necessidade de ser assegurada a sua independência no desempenho das suas funções e atribuições. A avaliação do nível de segurança deve ter em consideração os riscos decorrentes do tratamento dos dados[90], assim como a divulgação ou o acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

---

83 Licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; e integridade e confidencialidade (n.º 1, Art.º 5.º do RGPD).

84 " (…) a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas;" alínea d) do n.º 2, Art.º 47.º do RGPD).

85 Prazo de conservação, informação detalhada sobre transferências internacionais, a necessidade de uma maior transparência e clareza na informação prestada aos cidadãos, em especial quando dirigida a crianças.

86 Art.º 51.º, European Parliament and Council of the European Union, 2016b. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal of the European Union*, L 119, EN, 4.5.2016. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=PT [Consult. 4/6/2017]

87 No direito à limitação do tratamento, portabilidade e eliminação dos dados (direito ao esquecimento).

88 " (…) dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." (Art.º 9.º RGPD).

89 European Comission, 2011. *Article 29 Data Protection Working Party. Advice paper on special categories of data ("sensitive data")*. Justice and Consumers. Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

90 Pela sua eventual destruição, perda e alteração acidentais ou ilícitas.

2.4. Proteção das Infraestruturas de Informação Críticas

A comunicação *Proteção das infraestruturas críticas no âmbito da luta contra o terrorismo* (Commission of the European Communities, 2004)[91] caracteriza o conceito de "infraestrutura crítica"[92] e estabelece critérios[93] que permitem considerar como "crítica" uma infraestrutura ou um determinado elemento de uma infraestrutura.

As conclusões do Conselho em matéria de "prevenção, de preparação para intervir e de capacidade de resposta a atentados terroristas" e o "Programa de solidariedade da União Europeia respeitante às consequências das ameaças e dos atentados terroristas", adotado pelo Conselho em Dezembro de 2004, apoiaram a intenção da Comissão de propor um Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC) e a criação pela Comissão Europeia de uma Rede de Alerta para as Infraestruturas Críticas (RAIC).

Em novembro de 2005, a Comissão Europeia adotou um *Livro Verde* sobre um Programa Europeu de Proteção de Infraestruturas Críticas em que expôs as opções políticas com vista ao estabelecimento pela Comissão do PEPIC e da RAIC.

As conclusões do Conselho Justiça e Assuntos Internos (JAI) de dezembro de 2005 sobre a proteção das infraestruturas críticas apelam à Comissão Europeia para apresentar uma proposta de PEPIC.

A presente comunicação estabelece os princípios, processos e instrumentos propostos para a aplicação do PEPIC. Esta aplicação será, se for caso disso, complementada por comunicações sectoriais específicas que estabelecerão a abordagem da Comissão em relação a determinados sectores das infraestruturas críticas.

---

91 Estratégia global de proteção das infraestruturas críticas solicitada pelo Conselho Europeu de Junho de 2004, apresentando uma perspetiva geral das ações a desenvolver pela Comissão em matéria de proteção das infraestruturas críticas e reforço de outros instrumentos já existentes.

92 " (…) instalações físicas e de tecnologia de informação, redes, serviços e bens, os quais, se forem interrompidos ou destruídos, provocarão um sério impacto na saúde, na proteção, na segurança ou no bem-estar económico dos cidadãos ou ainda no funcionamento efetivo dos governos nos Estados-Membros. As infraestruturas críticas abarcam vários sectores da economia, incluindo o sector bancário e financeiro, os transportes e a distribuição, a energia, os serviços públicos, a saúde, o abastecimento alimentar e as comunicações, bem como certos serviços administrativos de base. Alguns elementos essenciais destes sectores não são "infraestruturas" propriamente ditas, mas, de facto, redes ou cadeias de abastecimento que asseguram a entrega de um produto ou a prestação de um serviço essencial". Commission of the European Communities, 2004. *Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism,* COM(2004) 702 final, 20.10.2004, Brussels. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN.

93 Alcance, magnitude e efeitos no tempo, *Ibidem*.

Tabela 5 – Infraestruturas Essenciais

• Instalações e redes de energia (por exemplo, energia elétrica, produção de petróleo e gás, instalações de armazenamento e refinarias, sistema de transmissão e distribuição);
• Tecnologia da informação e comunicação (por exemplo, telecomunicações, sistemas de radiodifusão, programas e equipamentos informáticos e redes, incluindo a internet);
• Finanças (por exemplo, catividades bancárias, valores mobiliários e investimento);
• Cuidados de saúde (por exemplo, hospitais, centros de assistência médica e bancos de sangue, laboratórios e empresas farmacêuticas, serviços de busca e de primeiros socorros, serviços de urgência);
• Alimentação (por exemplo, segurança, alimentar meios de produção, distribuição por grosso e indústria alimentar);
• Água (por exemplo, barragens, armazenamento, tratamento e redes);
• Transportes (por exemplo, aeroportos, portos, instalações intermodais, redes ferroviárias e redes de transporte de massa, sistemas de controlo de tráfego);
• Produção, armazenamento e transporte de mercadorias perigosas (por exemplo, materiais químicos, biológicos, radiológicos e nucleares);
• Administração (por exemplo, serviços de base, instalações, redes de informação, bens, sítios e monumentos de importância nacional).

Fonte: Commission of the European Communities (2004)

Na sequência do *Livro Verde* da Comissão Europeia sobre a Proteção de Infraestruturas Críticas a comunicação "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência" relativa à Proteção das Infraestruturas de Informação Críticas (Commission of the European Communities, 2009)[94] enfatiza:

(1) A importância da cibersegurança e da proteção das infraestruturas de informação críticas para a confiança dos cidadãos e das empresas na internet e demais redes, e para a "Agenda Digital para a Europa";
(2) A globalização dos desafios e a importância da cooperação entre os Estados-membros e o setor privado, ao nível nacional, europeu e internacional;
(3) A necessidade de envolvimento de todos os interessados na coordenação das iniciativas para prevenir, detetar, mitigar e reagir a todos os tipos de incidentes, mesmo naturais;
(4) A promoção de princípios orientadores para a resiliência e a estabilidade da internet;
(5) A materialização de parcerias estratégicas internacionais e esforços coordenados nas instâncias internacionais;

94 Ver também Commission of the European Communities, 2009. *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Critical Information Infrastructure Protection. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",* COM(2009) 149 final, 30.03.2009, Brussels. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&from=EN.

(6) A melhoria da preparação da UE através do estabelecimento de CERT nas instituições europeias.

3. Organização do Tratado do Atlântico Norte

A proteção dos Sistemas de Informação e Comunicação foi desde sempre um elemento essencial da NATO. A defesa cibernética porém, apenas foi inserida na agenda política da Aliança na Cimeira de Praga[95] em 2002 e reiterada na Cimeira de Riga[96] em 2006.

Na sequência dos ataques cibernéticos contra as instituições públicas e privadas da Estónia em abril e maio de 2007, os Ministros de Defesa dos Estados-membros da Aliança[97], manifestaram a sua preocupação, nomeadamente com a "extensão e a natureza dos ataques" e realçaram:

> "Eles foram sustentados; eles foram coordenados; eles estavam concentrados; eles foram contra uma infraestrutura de informação pública da Estónia. Eles tiveram implicações claras na segurança nacional e economia da Estónia" (NATO, 2007).

Foi ainda consensual a necessidade de um "trabalho urgente" no aumento da capacidade de proteção contra ataques cibernéticos dos sistemas de informação críticos da Aliança, de que decorreram a aprovação da Política de Ciberdefesa na NATO (dezembro de 2007)[98] e o Conceito de Ciberdefesa da NATO[99] (fevereiro de 2008).

O conflito entre a Rússia e a Geórgia no Verão de 2008 demonstrou que os ataques cibernéticos – *e.g.* ataques DDoS[100] – tinham potencial para se tornarem um componente importante da guerra convencional, tendo os mesmos, pela primeira vez na história, antecedido e coincidido com um conflito armado.[101]

Na sequência da Cimeira de Lisboa[102] em 2010 a NATO adotou um novo Conceito Estratégico[103] e decidiu desenvolver uma nova Política de Defesa Cibernética (Ciberde-

95 NATO, 2002. *Prague Summit Declaration*. Disponível em http://www.nato.int/cps/ic/natohq/official_texts_19552.htm?. NATO, 2006a. *Prague Summit*. Disponível em: http://www.nato.int/docu/comm/2002/0211-prague/index.htm.

96 NATO, 2006b. *Riga Summit Declaration*. Disponível em: http://www.nato.int/docu/pr/2006/p06-150e.htm.

97 NATO, 2007. Press briefing by the NATO Spokesman, James Appathurai on the Meetings of NATO Defence Ministers on 14 and 15 June 2007. *NATO*. Disponível em NATO, Online Library: http://www.nato.int/docu/speech/2007/s070614g.html

98 NATO Policy on Cyber Defence.

99 NATO Cyber Defence Concept.

100 Digital Attack Map, 2013. *What is a DDoS Attack?*. Disponível em: http://www.digitalattackmap.com/understanding-ddos/.

101 Markoff, J., 2008. Before the Gunfire, Cyberattacks. *The New York Times*, August 12. Disponível em http://www.nytimes.com/2008/08/13/technology/13cyber.html

102 NATO, 2010a. *Lisbon Summit Declaration*. Disponível em http://www.nato.int/cps/en/natohq/official_texts_68828.htm

103 NATO, 2010b. *Active Engagement, Moderne Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010, Brussels, NATO Public Diplomacy Division. NATO, Strategic Concept 2010: Disponível em https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

fesa) e o correspondente plano de ação. Esta segunda Política de Defesa Cibernética da NATO[104] foi aprovada em junho de 2011 pelo Conselho do Atlântico Norte[105]. Posteriormente, em abril de 2012, iniciou-se a integração da Ciberdefesa no Processo de Planeamento da NATO[106] e os requisitos de defesa cibernética identificados e priorizados através do referido processo.

Na Cimeira de Chicago[107] foram reafirmados os compromissos no âmbito da ciberdefesa firmados anteriormente na Cimeira de Lisboa e feita referência ao Conceito[108], à Política[109] e ao Plano de Ação de Ciberdefesa da NATO adotados em 2011 e em fase de implementação, às capacidades existentes, nomeadamente ao NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC) e à proteção centralizada de todas as redes e utilizadores da NATO. Em julho de 2012, foi estabelecida a NATO Communications and Information Agency (NCIA)[110] como parte da reforma das agências da NATO.

Em fevereiro de 2014, os ministros de defesa aliados decidiram desenvolver uma nova política de defesa cibernética, mais adequada em matéria de defesa coletiva, assistência aos Aliados, governança simplificada, considerações legais e relações com a indústria.

Na Cimeira de Gales[111] em setembro 2014, os Aliados reconheceram que as ameaças e ataques cibernéticos continuarão a ser progressivamente mais comuns, sofisticados e prejudiciais. Nesse sentido, foi aprovada uma nova política de defesa cibernética (Enhanced Cyber Defence Policy) e aprovaram um novo plano de ação que, juntamente com a política, contribui para o cumprimento das principais tarefas da Aliança.

A referida política reafirma os princípios da "indivisibilidade da segurança aliada e da prevenção, deteção, resiliência, recuperação e defesa". A declaração final da Cimeira lembra ainda que a responsabilidade fundamental da defesa cibernética da NATO é defender suas próprias redes e que a assistência aos Aliados deve ser abordada de acordo com o espírito de solidariedade, enfatizando a responsabilidade dos Aliados em desenvolver as capacidades relevantes para a proteção das suas redes nacionais. A política aprovada reconhece a aplicação do direito internacional no ciberespaço, incluindo o Direito Internacional Humanitário e a Carta das Nações Unidas.

104 NATO, 2011. *Defending the networks: The NATO Policy on Cyber Defence*. Disponível em http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

105 North Atlantic Council (NAC).

106 NATO, 2014a. *The NATO Defence Planning Process*. Disponível em http://www.nato.int/cps/en/natohq/topics_49202.html.

107 NATO, 2012. *Chicago Summit Declaration*. Disponível em http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en.

108 NATO Cyber Defence Concept. MC 0571/1, Military Concept on Cyber Defence

109 PO (2014)0358, Enhanced NATO Policy on Cyber Defence, 27 May 2014.

110 NATO, 2014b. NATO Communications and Information Agency. *NCI Agency*. Disponível em https://www.ncia.nato.int.

111 NATO, 2014. *Wales Summit Declaration*. Disponível em https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

Relativamente à decisão sobre se um ataque cibernético levaria à invocação do Artigo 5[112], os aliados declararam que a mesma seria tomada pelo Conselho do Atlântico Norte[113] (NAC), caso a caso.

4. Organización de Estados Americanos

La Organización de Estados Americanos (OEA) ha considerado como una de las principales prioridades para el Hemisferio la consolidación de una estrategia de protección y resguardo en materia de seguridad cibernética, que sea capaz de abordar los múltiples y diversos desafíos que la revolución digital ha puesto frente a la comunidad global, tomando en consideración el crecimiento del uso de internet, junto con el aumento de los ciberataques a infraestructuras digitales, cuyas consecuencias podrían afectar la infraestructura crítica de un país, así como también podría comprometer la provisión de servicios esenciales para la comunidad[114]. En ese sentido y para proteger a los países de las Américas contra la amenaza del ciberdelito, la OEA en su rol de promotor de derechos, se ha comprometido con el fortalecimiento de las capacidades de los países de la región para proteger a las personas, economías e infraestructura crítica[115].

El reconocimiento de la necesidad de adoptar una estrategia que fuera capaz de hacerse cargo de la seguridad digital para combatir el crimen cibernético, además de aumentar la resiliencia cibernética de los Estados como un tema prioritario y que tiene directa relación con el desarrollo económico y social, además de la efectiva gobernanza democrática, la seguridad nacional, como también de la seguridad de los ciudadanos[116], fue aprobada en la cuarta sesión plenaria, celebrada el 8 de junio del año 2004 ante la asamblea general de la Organización de los Estados Americanos, con la resolución AG/RES. 2040, bajo el título de "*Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*". Posteriormente, durante la celebración de la Sexta Sesión Plenaria celebrada el 7 de abril de 2017, se emitió una resolución (CICTE/RES.1/17) presentada por las delegaciones de Chile, Colombia, Perú, Costa Rica, Canadá, Guatemala y México para el

112 NATO. 2017a. *Collective Defence – Article 5*. Disponível em https://www.nato.int/cps/ic/natohq/topics_110496.htm.

113 NATO, 2017b. *North Atlantic Council (NAC)*. Disponível em https://www.nato.int/cps/ic/natohq/topics_49763.htm

114 Organización de los Estados Americanos (OEA), 2015a. Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. *OEA*, Abril de 2015, Secretaría de Seguridad Multidimensional de la OEA/Trend Micro, Washington. Disponible en https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf.

115 Banco Interamericano de Desarrollo (BID), 2016. BID y OEA instan a América Latina y el Caribe a mayores esfuerzos en ciberseguridad. *BID*, Marzo 14, Comunicados de Prensa. Disponible en http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html

116 Organización de los Estados Americanos (OEA), 2014. Tendencias de Seguridad Cibernética en América Latina y el Caribe. OEA, Junio, Secretaría de Seguridad Multidimensional de la OEA, Washington. Disponible en https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf.

"Establecimiento de un grupo de trabajo sobre medidas de fomento de cooperación y confianza en el ciberespacio".

Con ello, la OEA busca posicionar una agenda de seguridad digital que sea capaz de comprometer a los Estados de la región para que sean capaces de acordar distintas medidas, detectar amenazas y vulnerabilidades que afectan a un alto número de usuarios, tanto del sector público como privado, además de identificar oportunidades de cooperación y de manera mancomunada, articular una estrategia integral que permita proteger la infraestructura de la información, adoptando para ello un enfoque internacional y multidisciplinario[117].

Junto a lo indicado, la OEA ha impulsado una serie de iniciativas que buscan fortalecer la cooperación multilateral y la creación de capacidad en materia de seguridad cibernética. Sin embargo, se ha reconocido que existe una escasez en términos de literatura asociada a la ciberseguridad tanto en América Latina como el Caribe[118], lo que ha constituido un serio obstáculo para la materialización de los objetivos propuestos por la OEA en materia de seguridad digital. En ese sentido, para hacer frente a esta dificultad y posicionar e impulsar la efectiva adopción de una agenda de seguridad cibernética, ha diseñado, elaborado y difundido numerosos documentos de carácter técnico entre los distintos Estados de las Américas, como mecanismo para poner a disposición de los Estados información que sea de utilidad en la formulación de políticas en materia de ciberseguridad, colaborando de este modo con su toma de decisiones en una perspectiva integral.

En efecto, es posible encontrar diversos informes que dan cuenta del estado actual de los distintos países miembros en relación al grado de desarrollo que han alcanzado sus mecanismos de ciberseguridad al interior de sus fronteras. Junto con lo anterior, se proponen estrategias para abordar los distintos escenarios que van surgiendo, además de las nuevas amenazas que aparecen con el avance de la tecnología y el uso de los dispositivos electrónicos en diversos ámbitos. Un ejemplo de ello tiene que ver con las distintas metodologías de respuesta a incidentes (IRM, por sus siglas en inglés) que va desde la respuesta frente a la infección de gusanos, hasta lineamientos para manejar incidentes de infracción de marcas registradas[119]. Cada metodología propone seis pasos para manejar incidentes de seguridad[120], que son: Preparación, Identificación, Contención, Remedio, Recuperación, Repercusiones.

---

117 Organización de los Estados Americanos (OEA), 2004. Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética, AG/RES. 2004 (XXXIV-O/04). Aprobada en la cuarta sesión plenaria, celebrada el 8 de junio. Disponible en https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf

118 Banco Interamericano de Desarrollo (BID) e Organización de los Estados Americanos (OEA), 2016. *Ciberseguridad* ¿Estamos preparados *en América Latina y el Caribe?* Informe Ciberseguridad 2016, BID/OEA, Observatorio de la Ciberseguridad en América Latina y el Caribe. Disponible en https://publications.iadb.org/handle/11319/7449.

119 Organización de los Estados Americanos (OEA), 2017a. Seguridad Cibernética. *OEA*. Disponible en https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx

120 Organización de Estados Americanos (OEA), 2015a. *Respuesta a incidentes de infracción de marcas registradas*. IRM 15. Disponible en https://www.sites.oas.org/cyber/Documents/Metodolog%C3%ADa%20de%20Respuesta%20a%20Incidentes%20(IRMs)%20IRM15-InfraccionMarcaRegistrada-OEA.pdf.

Con lo anterior, la OEA aborda el tema de la ciberseguridad a través de distintos mandatos que contribuyen con los objetivos de la Estrategia Integral de Seguridad Cibernética. Entre ellos podemos encontrar, en primer lugar, Reunión de Ministros de Justicia y Procuradores Generales de las Américas (REMJA), quienes a través de su grupo de expertos en cibercrimen, buscan asegurar que los Estados miembros de la OEA cuenten con los instrumentos legales y jurídicos necesarios para proteger a los usuarios de internet y las redes de información[121]. En segundo lugar, se encuentra la Comisión Interamericana de Telecomunicaciones (CITEL), cuyo objetivo se basa en la creación de estándares, identificación de aspectos técnicos, además de la promoción de una cultura de concienciación en materia de seguridad cibernética[122]. Por último, el Comité Interamericano contra el Terrorismo (CICTE), cuya misión corresponde a la promoción y el desarrollo de la cooperación entre los distintos Estados miembros para prevenir, combatir y eliminar el terrorismo, a partir de los principios de la Carta de la Organización de Estados Americanos, con la Convención Interamericana contra el Terrorismo y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional, junto con el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados[123].

De esta manera, el CICTE articula sus acciones en base a cinco programas para responder a su misión institucional, estos son: Controles Fronterizos, Cooperación internacional y Alianzas, Asistencia Legislativa y Lucha Contra el Financiamiento del Terrorismo, Fortalecimiento de Estrategias sobre Amenazas Terroristas Emergentes y Protección de Infraestructura Crítica[124]. En este último programa, el CICTE busca potenciar la creación de capacidad de los Estados miembros, empleando para ello un enfoque integral en el tratamiento de esta dimensión de la seguridad global, reconociendo simultáneamente que la seguridad cibernética depende tanto de la responsabilidad nacional y regional, como también de un gran abanico de entidades públicas y privadas, cuyos esfuerzos se enfocan en asegurar el ciberespacio a través del trabajo en ámbitos políticos y técnicos[125].

La labor del CICTE en materia de ciberseguridad se resume en tres dimensiones:

(1) Apoyar a los Estados miembros de la OEA en sus esfuerzos para la creación de Equipos de respuesta a Incidentes (CSIRT, por sus siglas en inglés), en concordancia con los requerimientos de la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética.

121 Contreras, B., 2009. *Esfuerzos del CICTE-OEA para fortalecer la Seguridad Cibernética en las Américas*. OEA, Secretaría de Seguridad Multidimensional, Comité Interamericano contra el Terrorismo (CICTE). Disponible en https://www.itu.int/ITU-D/cyb/events/2009/santo-domingo/docs/CONTRERAS-CICTE-overview-nov-09.pdf

122 *Ibidem*.

123 Organización de los Estados Americanos (OEA), 2017b. Comité Interamericano contra el Terrorismo. Misión. *OEA*. Disponible en http://www.oas.org/es/sms/cicte/acerca_nosotros_mision.asp.

124 Organización de los Estados Americanos (OEA), 2017c. Comité Interamericano contra el Terrorismo. Programas. *OEA*. Disponible en http://www.oas.org/es/sms/cicte/programas.asp.

125 Organización de los Estados Americanos (OEA), 2017a. Seguridad Cibernética. *OEA*. Disponible en https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx

(2) Contribuir y promover la creación de una red hemisférica 24/7 de CSIRT que posean la capacidad y el mandato de difundir correcta y rápidamente información relacionada con la ciberseguridad.
(3) Fomento de una cultura de ciberseguridad que sea capaz de disuadir el uso indebido de internet y de los sistemas de desarrollo de redes de información caracterizadas por su confianza y fiabilidad (Contreras, 2009, p. 6).

Junto a lo indicado, el CICTE ha desarrollado un Programa de Seguridad Cibernética, de carácter regional, cuyo objetivo se enfoca en el fortalecimiento de la seguridad y protección de la infraestructura de información crítica del Hemisferio, a partir del reconocimiento de la necesidad de cooperación multilateral. En ese sentido, el Programa se articula en torno a siete puntos:

(1) Participación de la sociedad Civil y del Sector Privado: Asociación entre la OEA con diferentes grupos, compañías y organizaciones sin fines de lucro para trabajar colaborativamente en materia de ciberseguridad.
(2) Crear Conciencia: Ante la tendencia del aumento de la conexión y el uso de internet en diversos ámbitos, se reconoce la necesidad de desarrollar políticas que sean capaces de contribuir en la creación de conciencia por parte de todos quienes utilizan la red, respecto de los mecanismos de seguridad cibernética y así difundir los riesgos y medidas necesarias para un funcionamiento sostenible.
(3) Desarrollo de estrategias nacionales: Apoyar en el establecimiento de estrategias a nivel nacional permite generar perspectiva en torno al tema, además de establecer responsabilidades y coordinación entre las distintas partes interesadas, además de la creación de diversos mecanismos de respuesta ante situaciones que pudiesen afectar la seguridad cibernética.
(4) Brindar capacitación: Tomando en consideración el permanente desarrollo de las tecnologías de internet, es necesario mantenerse constantemente actualizado en lo que a ello respecta. La capacitación técnica ha demostrado ser un mecanismo útil y exitoso para la mejora de la seguridad cibernética a nivel nacional y regional. En este sentido la OEA realiza actividades por si misma con los países en forma bilateral o multilateral, como también, junto a otras entidades como por ejemplo el Bando Interamericano del Desarrollo (BID). Ilustra estas prácticas el encuentro realizado durante Septiembre en Montevideo (Uruguay) donde junto a una jornada de capacitación para expertos y formuladores de políticas de los países que componen la OEA, se realizó conjuntamente con BID el Foro de Ciberseguridad de las Américas. Con estas actividades además de colaborar en la formación especializada en temas de ciberseguridad se va constituyendo una comunidad de ciberseguridad en el Hemisferio[126].
(5) Ejercicios de gestión de crisis: Además de lo anterior, la OEA ha generado meca-

126 Al respecto ver Organización de los Estados Americanos (OEA), 2017. Seguridad Cibernética. Simposio de la OEA en Ciberseguridad para la Región de las Américas. *OEA*. Disponible en https://www.sites.oas.org/cyber/ES/Paginas/Events/eventsdet.aspx?docid=93.

nismos de simulación de control de crisis, lo que permite a los Estados miembros ejercitar su capacidad de manejo de este tipo de situaciones de acuerdo a sus propias necesidades, lo que a su vez fortalece la colaboración técnica entre diversos países para hacer frente a las amenazas.

(6) Misiones de asistencia técnica: La OEA asiste a los países miembros a través de visitas, revisiones de las diversas políticas en materia de ciberseguridad, además de presentaciones de autoridades locales para, posteriormente, brindar recomendaciones expertas.

(7) Compartir información y experiencia: Para ello, la OEA trabaja en la creación de una red de Equipos de Respuesta a Incidentes entre distintas autoridades nacionales y otras relacionadas con la ciberseguridad para facilitar la comunicación y el flujo de información en tiempo real[127].

127 Organización de los Estados Americanos (OEA), 2015a. *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. OEA, Abril de 2015, Secretaría de Seguridad Multidimensional de la OEA/Trend Micro, Washington, pp. 3-4. Disponible en https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

CAPÍTULO III
Factores Mínimos a Considerar en una Política Nacional de Ciberseguridad

Una política nacional en su condición de política pública, contempla diversas etapas en su desarrollo que en términos sintéticos pueden resumirse en: formulación, ejecución, evaluación y retroalimentación. En este contexto, una adecuada formulación de una política desde el Estado es condición necesaria más no suficiente para su éxito.

En el marco de la política de ciberseguridad han sido considerados seis factores mínimos a desarrollar en esta política pública. Este capítulo identifica y explica brevemente cada factor y en el capítulo V se describe en modo en que se presentan estos factores tanto en el caso de chileno como el portugués, a partir de la revisión de las políticas nacionales en la materia en cada país.

1. Aproximación Conceptual

La aproximación conceptual para una política pública se refiere a los conceptos centrales del tema que son definidos para un adecuado y compartido entendimiento de éstos por los diferentes actores, muchas veces de diversas instituciones y variadas organizaciones. Frecuentemente ello está contenido en documentos públicos que establecen directrices en la materia y muchas veces plantean definiciones mínimas de conceptos claves.

Por ejemplo, en el caso de una política nacional de ciberseguridad resulta esencial establecer a nivel nacional y teniendo en consideración los estándares internacionales que se entenderá por: ciberseguridad, ciberdelito o cibercrimen, ciberdefensa, entre otros.

Junto a lo indicado, también a modo de ejemplo, se encuentran las cualidades que debe tener la información y/o los sistemas de información en el ciberespacio, las que muchas veces se encuentran relacionadas con: disponibilidad, integridad, oportunidad, confiabilidad, interoperabilidad, robustez, trazabilidad, resiliencia y seguridad.

Se justifica lo señalado debido a que es recurrente la confusión conceptual o la existencia de diversas formas de entender un problema o concepto. Por ejemplo, frecuentemente ello ha se ha detectado en el caso de la noción de ciberseguridad y resiliencia cibernética.

2. Legislación Especializada

En el marco de la acción del Estado su capacidad regulatoria es clave para establecer las autorizaciones y limitaciones para hacer o evitar desarrollar. Diversos documentos legales como Leyes, Convenios internacionales, decretos y reglamentos forman parte de la política pública y son una forma en que se manifiesta la voluntad del legislador y/o del poder ejecutivo en materias específicas.

En materia de ciberseguridad a nivel internacional los Convenios internacionales y a nivel nacional leyes, decretos y reglamentos son los principales documentos que componen la legislación en materia de ciberseguridad. En ocasiones los compromisos internacionales adquiridos generan el desafío de adaptar legislación nacional por existir vacíos o

actualizaciones que deben ser incorporadas en leyes nacionales desfasadas en el tiempo en una materia que evoluciona con mayor rapidez que el Estado en rol de regulador del uso del ciberespacio y responsable último de la seguridad en este ambiente.

3. Arquitectura de Ciberseguridad

El diseño en el marco del cual se relacionan los organismos involucrados en la ciberseguridad de un país, el modo en que se relacionan y las funciones asignadas a cada un o de ellos, es lo que permite identificar la arquitectura de ciberseguridad de un país. En efecto, se refiere a los organismos y entidades nacionales o sectoriales que componen el sistema de ciberseguridad nacional y la interacción que existe entre ellos.

La experiencia en el tema condicionará la madurez de la arquitectura, que además se va fortaleciendo en la medida que a los largo del tiempo va enfrentado incidentes críticos en el ciberespacio que constituyen problema de seguridad para el país o alguna(s) de su(s) infraestructura(s) crítica(s).

4. Cooperación Internacional

La cooperación en materia de ciberseguridad es necesaria pues ningún país por si solo puede lograr la seguridad del ciberespacio correspondiente a su área de responsabilidad. En este contexto, la cooperación internacional es una herramienta clave si se tiene en consideración que el ciberespacio no tiene fronteras y por extensión tampoco en el caso de muchos de los incidentes a la seguridad que ocurren en este ambiente. El modo en que se realiza la cooperación puede ser de diferentes tipos. En efecto, la cooperación en este tema puede manifestar de muchas maneras, por ejemplo, de acuerdos a criterios de:

(1) Formalidad: puede ser formal o informal, es decir, se realiza en el marco de un convenio institucionalizado entre dos entidades o por medio de p personas de entidades diferentes que están dispuestas a intercambiar información por voluntad propia sin un convenio que las respalde en la acción;
(2) Cantidad de actores que participan: puede ser bilateral o multilateral, es decir, si hay dos o más actores respectivamente quienes participan en el intercambio de información;
(3) Territorialidad de entidades involucradas: puede ser nacional o internacional, es decir, si los organismos que participan del intercambio de información son exclusivamente de un país o el intercambio permite la inclusión de entidades de diferentes países.

En materia de cooperación internacional en ciberseguridad, además de los organismos multilaterales señalados en otro capítulo, es posible destacar por su creciente importancia de acuerdo a su nivel de convocatoria y las materias que abordan algunos foros internacionales y un tratado internacional, el Convenio de Budapest.

En efecto, los foros internacionales como mecanismos de discusión e intercambio de conocimiento a nivel multilateral se encargan de ofrecer instancias de encuentro a distintos países para tratar temas relativos a ciberseguridad, como por ejemplo, cuáles son

las herramientas y asuntos contingentes que es necesario tratar. Así, se constituyen como una instancia colaborativa en la que diversos actores tanto del sector público como privado pueden realizar sus aportes y así contribuir en el fortalecimiento de la seguridad cibernética. Por su relevancia y nivel de convocatoria, a continuación se describen dos foros internacionales que abordan el tema de la seguridad en el ciberespacio.

4.1. La Conferencia Global del Ciberespacio

Es un evento global que goza de un alto prestigio. Tanto líderes mundiales, como formuladores de políticas, expertos de la industria y centros de pensamiento, entre otros, se reúnen para discutir sobre temas y desafíos para un óptimo uso del ciberespacio a nivel global. Así el lanzamiento de la Conferencia Global del Ciberespacio (GCCS) fue con miras a establecer directrices de consenso internacional respecto del comportamiento en el ciberespacio. Asimismo, busca crear un diálogo más inclusivo y orientado a todos aquellos quienes participan y utilizan internet, como por ejemplo gobiernos, industria y sociedad civil[128].

Fue durante el año 2011, en la ciudad de Londres donde tomó lugar por primera vez la GCCS, la que contó con la presencia de más de setecientos delegados mundiales y que sirvió para definir las reglas y orientaciones para las próximas ediciones. La segunda conferencia fue organizada el siguiente año en Budapest, cuyo enfoque trataba sobre sobre la relación existente entre la seguridad y los derechos de internet. En esta ocasión asistieron alrededor de setecientos delegados de todo el mundo y más de sesenta países. En el año 2013, la conferencia se llevó a cabo en la ciudad de Seúl y sus temas fueron se orientaron en el ciberespacio abierto y seguro. En esta oportunidad, el número de delegados que participaron de esta actividad alcanzó la cifra de 1600. Posteriormente, en 2015, el evento fue realizado en la ciudad de la Haya. Nuevamente, el número de delegados asistentes a la conferencia creció, llegando a un total de 1800 aproximadamente, mientras que alrededor de cien países participaron en la actividad[129].

Como es posible apreciar, la magnitud de la conferencia ha ido en notable aumento, considerando que cada año, la cantidad de delgados participantes ha crecido, e incluso se ha duplicado en comparación con la asistencia inicial. Por otra parte, la participación oficial de distintos países también se ha hecho patente, por lo que se podría esperar que, en relación a la evidencia señalada, esta tendencia se replique para el presente año (2017), cuando la conferencia tome lugar en India en el mes de noviembre.

Los objetivos de la GCCS 2017 se relacionan con la promoción de la importancia de la inclusión y de los derechos humanos en la política cibernética mundial, orientándose a defender un ciberespacio abierto e interoperable. De esta forma se busca colaborar en la formulación de compromisos políticos respecto a las iniciativas de creación de capacidad para abordar las brechas existentes, además de brindar ayuda a los distintos países y

128 Global Conference on Cyber Space (GCCS), 2017. *Global Conference on Cyber Space. About GCCS*. Disponible en https://gccs2017.in/about.

129 *Ibidem*.

desarrollar soluciones sobre seguridad cibernética capaces de reconocer debidamente la importancia del sector privado y de la comunidad técnica, configurándose de este modo una plataforma multisectorial[130].

A partir de lo anterior, es posible desprender cuatro subcategorías que guiarán el desarrollo temático de la conferencia:

(1) Crecimiento: recientemente el ciberespacio ha surgido como un diferenciador crítico para el progreso social y económico. Con más de 3.5 billones de usuarios a nivel global, el ciberespacio brinda oportunidades tanto a los individuos, pequeñas y grandes compañías en el diseño de sus modelos de negocio para lograr mayor eficiencia y alcance. La GCCS, se constituye como una plataforma multisectorial que reúne tanto a líderes de la industria, como también, nuevas compañías y formuladores de políticas para compartir ideas y perspectivas respecto a esta temática, además de ser una oportunidad para todos quienes participan, de ser testigos de las nuevas innovaciones en productos y servicios digitales.

(2) Inclusión Digital: una sociedad inclusiva con igualdad de oportunidades es el núcleo del valor democrático. En ese sentido, las tecnologías digitales ofrecen nuevos caminos para hacer a la sociedad mucho más inclusiva. Ejemplos de ello corresponden al desarrollo de software de reconocimiento de voz, el software de texto a voz, ayuda visual o de audio digital herramientas que colaboran en programas de inclusión social.

(3) Seguridad: la ciberseguridad y los incidentes cibernéticas constituyen la principal preocupación para la infraestructura crítica de los países, como por ejemplo las telecomunicaciones, banca y energía entre otras. Esta situación se agrava, tal como se ha observado, por los recientes ciberataques que dejaron en evidencia las vulnerabilidades de los países y los desafíos que impone la digitalización.

(4) Diplomacia: considerando la mayor interconexión mundial y que la naturaleza de los desafíos ha ido cambiando, es necesario que los gobiernos diseñen nuevas medidas para el uso del ciberespacio para alcanzar los objetivos de la cooperación internacional y el desarrollo. De esta manera, la diplomacia cibernética redefine las relaciones diplomáticas entre los Estados, organizaciones internacionales y otros organismos[131].

4.2. La Conferencia de Meridian

La primera Conferencia de Meridian fue organizada en el Reino Unido en 2005 posteriormente se han efectuado en diversos países como: Hungría, Suecia, Singapur, Estados Unidos de América, Taiwán, Qatar, Alemania, Argentina, Japón, España y México (2016)[132]. Cada año, un país distinto realiza la Conferencia, con la finalidad de rotar la conferencia a diferentes regiones para aumentar la participación en la Comunidad Meri-

130 *Ibidem*.

131 *Ibidem*.

132 Meridian, 2017. *How Meridian work. About Meridian*. Disponible en https://meridian2017.atlassian.net/wiki/spaces/TS1/pages/1671371/About+Meridian.

dian. Junto a lo indicado, "la participación en el proceso de Meridian está abierta a todos los países/economías y está dirigida a los altos responsables de las políticas gubernamentales que participan en cuestiones relacionadas con el CIIP. Todos los países/economías están invitados a participar en el Proceso de Meridian, y se les anima a asistir a la Conferencia Meridian anual"[133].

El objetivo del Proceso de Meridian que nació en la primera conferencia de Meridian en Reino Unido, es "intercambiar ideas e iniciar acciones para la cooperación de organismos gubernamentales en cuestiones de Protección de la Infraestructura de Información Crítica (CIIP) a nivel mundial. Explora los beneficios y oportunidades de cooperación entre gobiernos y brinda la oportunidad de compartir mejores prácticas de todo el mundo"[134]. Asimismo, "busca crear una comunidad de altos funcionarios gubernamentales en CIIP mediante el fomento de la colaboración en curso"[135], reconociendo que solo mediante el trabajo conjunto es posible progresar en el logro de las "metas y objetivos nacionales de CIIP"[136]. En 2017 esta Conferencia se realiza en Oslo, Noruega.

De acuerdo a lo expuesto, Meridian se basa en los siguientes principios fundamentales:

(1) La Comunidad Meridian, como la conferencia y el Directorio están abiertos a todos los países y economías.
(2) Meridian está abierto a los formuladores de políticas gubernamentales interesados en la protección de información de la infraestructura crítica.
(3) Meridian busca el fomento de la colaboración internacional sobre cuestiones relacionadas con CIIP a partir del mutuo acuerdo entre gobiernos.
(4) La conferencia anual de Meridian brinda un foro confidencial entre los delegados gubernamentales de manera de promover una discusión abierta libre de presiones de carácter comercial[137].

4.3. Convenio de Budapest[138]

En noviembre del año 2001, se llevó a cabo la Convención de Budapest que abordó el tratamiento del cibercrimen, teniendo en consideración las implicancias que esta forma de delito tiene a nivel global, dado que no reconoce límites y fronteras nacionales, por lo que goza de un amplio alcance, además de eludir los mecanismos de regulación y legislación a nivel local[139].

Esta convención constituye la culminación de un esfuerzo que había comenzado hace años atrás, donde se hizo patente que las tecnologías de la computación podían ser

133 *Ibidem*.
134 *Ibidem*.
135 *Ibidem*.
136 *Ibidem*.
137 Meridian, 2017. [Website] Disponible en https://www.meridianprocess.org/.
138 Ver estrutura da Convenção de Budapeste em Anexo A.
139 Brenner, S., 2012. La Convención sobre el Cibercrimen del Consejo de Europa. *Revista chilena de Derecho y Tecnología* n.º 1. Disponible en http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629.

utilizadas de diferentes formas en la realización de actividades no deseadas, como aquellas que se manifestaban en forma de delitos transnacionales, donde dichas tecnologías eran utilizadas para comer ilícitos, entre ellos el fraude o el acoso[140]. Ello justificaba la necesidad de contar con un acuerdo internacional en materia de ciberdelito, siendo el Convenio de Budapest sobre ciberdelincuencia el "primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos, como la búsqueda de redes de computadoras e intercepción. Su objetivo principal, es perseguir una política criminal común dirigida a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de legislación apropiada y el fomento de la cooperación internacional"[141], en cual fue elaborad en el marco del Consejo de Europa en 2001 y está abierto a la adhesión de cualquier país en el mundo, previa solicitud de invitación a suscribirlo.

En el preámbulo del convenio que se materializó en el Convenio, se señala que en virtud del objetivo perseguido por el Consejo de Europa de lograr aumentar la cohesión y cooperación entre sus diversos miembros, han reconocido la necesidad de generar un política que sea común a sus miembros en lo que respecta a la ciberdelincuencia y así proteger a la sociedad, a partir de la configuración de una legislación apropiada y la constante mejora de la cooperación internacional. Esto, tomando en cuenta los cambios que ha traído consigo los crecientes y profundos cambios que ha producido la digitalización, además de la convergencia y globalización de carácter permanente de las redes cibernéticas[142].

Dentro de los objetivos del convenio, es posible apreciar que estos se orientan en la prevención de actos que pongan en riesgo la confidencialidad, integridad y disponibilidad de sistemas, redes y datos de carácter informático, además del abuso de estos recursos. En ese sentido, buscan la tipificación de estos actos como constitutivos de delito, además de la asunción de determinados poderes que sean suficientes y capaces de luchar contra estos ilícitos permitiendo su detección, investigación y sanción a nivel nacional como internacional. A su vez, buscan garantizar la protección de los recursos digitales en un marco de derechos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades fundamentales del año 1950, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas del año 1966 y otros tratados en materia de derechos humanos, de forma tal que sea posible equilibrar los intereses de la acción de carácter penal con el respeto a los derechos humanos[143].

---

140 *Ibidem*.

141 Council of Europe, 2001a. *Convention on Cybercrime*. Details of Treaty No.185, 23/11/2001, Budapest. Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

142 Council of Europe, 2001b. *Convenio sobre la ciberdelincuencia*. Serie de Tratados Europeos nº185, 23.11.2001, Budapest. Disponible en http://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

143 *Ibidem*.

4.4. Manual de Tallin[144]

O *Manual de Tallin* é um documento não vinculativo sobre a aplicabilidade da lei internacional na resolução de conflitos cibernéticos, *i.e* o *jus ad bellum*[145] e o *jus in bello*[146], desenvolvido por especialistas independentes a convite do Centro de Excelência de Ciberdefesa Cooperativa da NATO (CCDCOE) em Tallinn. O manual não representa as opiniões do CCDCOE, dos Estados patrocinadores do referido Centro de Excelência ou da NATO. A primeira versão (1.0)[147] foi publicada em 2013 e a segunda (2.0) em 2017.

A análise apresentada no *Manual de Tallin 2.0* baseia-se no entendimento de que a lei internacional se aplica às operações cibernéticas conduzidas e dirigidas contra Estados. Os eventos cibernéticos não ocorrem num vácuo legal, pelo que os Estados possuem direitos e obrigações de acordo com o direito internacional. O manual aborda uma ampla gama de princípios e regimes de direito internacional que regulam eventos no espaço cibernético incluindo princípios gerais de direito internacional, como a soberania, diligência e as diversas bases para o exercício da jurisdição. A lei da responsabilidade do Estado é examinada detalhadamente, assim como examinados vários regimes especializados de direito internacional no contexto das operações cibernéticas, incluindo os direitos humanos, o direito do ar e do espaço, o direito do mar e o direito diplomático e consular.

5. Cultura de Ciberseguridad

Corresponde a la manera en que es entendida la ciberseguridad por parte de toda la población, como el modo en que ella es enseñada y la forma en que son formados los especialistas en ciberseguridad. Asimismo, la forma en que son reclutados los expertos en la materia, forma parte de la cultura de ciberseguridad de un país. Por este motivo, se hará especial referencia al significado de la cultura de ciberseguridad, como también, al desafío del reclutamiento de expertos en estas materias por parte de las organizaciones.

6. Política Pública en Ciberseguridad

Se habla de política pública de ciberseguridad porque efectivamente se trata de una "intervención del Estado, expresada en una decisión o conjunto de decisiones de una autoridad pública, que considera un análisis técnico – racional para un tema determinado y una finalidad específica, que sigue un procedimiento formal, todo lo cual se da en el contexto de un intenso proceso político de confrontación y articulación de intereses"[148]. En efecto, ante el creciente uso del ciberespacio y frente a los diversos incidentes de

144 Ver estrutura do Manual de Tallin em Anexo B.

145 Congrega os critérios a verificar antes de iniciar-se um conflito armado de forma justa *i.e* as condições em que é legítimo entrar em guerra.

146 Direito Internacional Humanitário que regula a conduta aceitável em conflitos armados.

147 Schmitt, M. N., ed., 2013. *Tallinn Manual on the International Law Applicable to Cyber warfare*. Cambridge: Cambridge University Press. Disponible en https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

148 Olavarría, M., 2007. *Conceptos Básicos en el Análisis de Políticas Públicas*. Documentos de Trabajo N.º 11, Diciembre. INAP-Instituto de Asuntos Públicos Departamento de Gobierno y Gestión Pública, Universidad de Chile, p. 92. Disponible en Repositorio Académico de la Universidad de Chile: http://repositorio.uchile.cl/bitstream/handle/2250/123548/Conceptos_%20Basicos_Politicas_Publicas.pdf?sequence=1

seguridad que han afectado su normal funcionamiento y ello ha sido especialmente peligroso cuando se ha tratado de infraestructura crítica de la información, han sido las máximas autoridades nacionales las que han plateando la elaboración de una política nacional de ciberseguridad.

En el camino para concretar este objetivo, han participado diversos actores del Estado, la sociedad civil, el sector privado y la academia donde por medio del dialogo y la negociación se ha conseguido elaborar documentos que contienen las directrices de los países en materia de ciberseguridad, los objetivos, metas a alcanzar y desafíos a enfrentar, pero ante todo, buscando la unidad entre actores diversos con responsabilidad en la material al poner a disposición de todos ellos un documento único sobre el tema.

Desde una perspectiva del sector privado, una política nacional de ciberseguridad es también relevante pues para estas organizaciones.

CAPÍTULO IV
Outros Elementos Essenciais a Considerar numa Política de Cibersegurança

Neste capítulo apresentamos um conjunto de temas identificados de forma consistente em normas internacionais, projetos de investigação e publicações ou que sendo enunciadas nas políticas e estratégias de cibersegurança, não são muitas vezes apresentadas de forma abrangente.

1. Abordagem Concetual

1.1. Conhecimento

> "O desenvolvimento do conhecimento no sentido mais amplo da palavra (conscientização, educação, inovação) é necessário para garantir que todos os atores possam assumir suas responsabilidades e beneficiarem otimamente das oportunidades oferecidas pela digitalização." (Government of The Nederlands, 2013).

> "A segurança do ciberespaço pressupõe o conhecimento das ameaças e das vulnerabilidades existentes. Este conhecimento é essencial para a realização de análise de risco, com vista a uma melhor aplicação dos meios e recursos disponíveis para o tratamento dos riscos, bem como para a identificação das lacunas a colmatar" (PCM, 2015b).

A grande maioria das Estratégias de Cibersegurança analisadas realçam a importância do conhecimento no domínio cibernético e das TIC. A Cibersegurança e Ciberdefesa são domínios tecnológicos avançados que requerem recursos humanos qualificados e processos organizacionais eficientes e como tal, políticas ativas de criação de conhecimento individual, coletivo e organizacional, sob pena da sua ausência aumentar o risco – aos seus vários níveis estratégico, operacional e tático – e os encargos na criação e sustentação de capacidades de defesa cibernética. Importa pois compreender quais os principais fatores envolvidos na aquisição do conhecimento em geral.

Nonaka e Takeuchi (1995) definiram "conhecimento" como uma "convicção verdadeira e justificada" e propuseram uma teoria para explicar a criação de conhecimento organizacional como "a capacidade de uma empresa como um todo para criar novos conhecimentos, disseminá-los em toda a organização, e incorporá-los em produtos, serviços e sistemas."

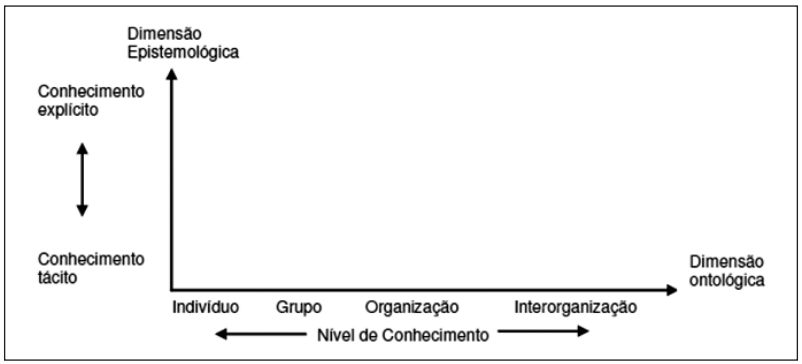
Estes autores consideraram que o conhecimento é inicialmente criado pelas pessoas, tornando-se "conhecimento organizacional" através de um processo evolutivo com duas dimensões: epistemológica (natureza e validade) e ontológica (nível de interação social).

No plano epistemológico, os autores reconhecem dois tipos de conhecimento[149], tácito e explícito. O conhecimento explícito ou codificado pode ser transmitido numa linguagem formal e sistemática, partilhada sob a forma de dados, sendo relativamente fácil o seu processamento, transferência e armazenagem. O conhecimento tácito envolve elementos cognitivos e técnicos (Nonaka, 1994) e possui uma qualidade pessoal que difi-

149 Anteriormente teorizado por Polanyi (1996).

culta a sua formalização e comunicação, estando intimamente ligado à experiência – *i.e.*, ação, contexto, rotinas, ideais, valores e emoções.

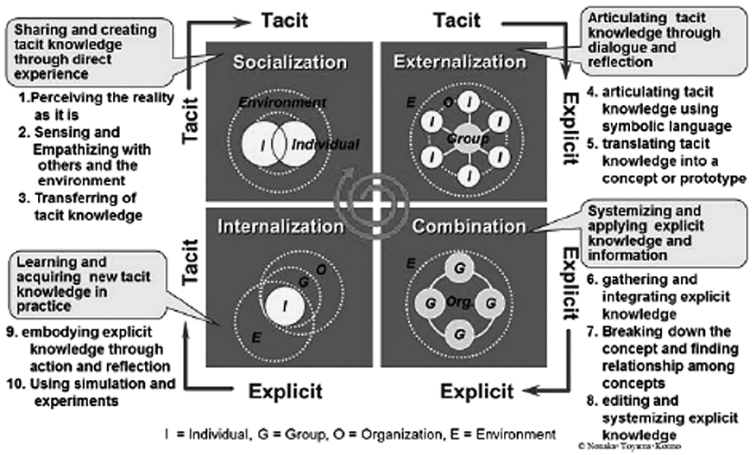
Figura 6 – Dimensões do Conhecimento



Fonte: Adaptado Nonaka e Takeuchi (1995).

A dimensão epistemológica corresponde à conversão interativa entre o conhecimento tácito e o conhecimento explícito. A dimensão ontológica diz respeito ao indivíduo na cadeia de valor, atravessando diferentes níveis de agregação e ampliando as fronteiras organizacionais. Segundo Nonaka (1994), a dimensão ontológica é fundamental pois as pessoas são indispensáveis à criação do conhecimento. A criação de conhecimento deveria ser entendida como um processo organizacional que amplifica o conhecimento criado individualmente pelas pessoas.

Figura 7 – Modelo SECI



Fonte: Adaptado de Nonaka, Toyama e Konno (2000).

As duas dimensões da criação do conhecimento – epistemológica e ontológica – formam uma espiral com quatro padrões de interação entre conhecimento tácito e explícito. Tendo como pressuposto que o conhecimento é criado através da conversão ou interação entre estes dois tipos de conhecimento, Nonaka (1994) descreveu quatro formas distintas de conversão de conhecimento: socialização, externalização, combinação e internalização. Na socialização, a criação de "conhecimento tácito" decorre da partilha de experiências, requerendo a interação entre as pessoas, mas podendo ser realizada sem o uso de linguagem, como o desenvolvimento de competências pelos aprendizes.

A combinação é a forma mais habitual de aquisição de conhecimento e envolve processos sociais na conversão de diversas formas de "conhecimento explícito" das pessoas em outras formas mais complexas e sistematizadas de "conhecimento explícito", permitindo a criação e partilha de novo conhecimento com outros elementos da organização. Esta interação pode ser facilitada através de diversos mecanismos de interação – *e.g.* sistemas de informação, redes de comunicação, redes sociais, portais, etc..

Quando o "conhecimento tácito" é tornado explícito através da externalização, o conhecimento é "cristalizado" (Nonaka, 1994) permitindo a sua partilha e tornando-se ponto de partida para novo conhecimento.

A conversão de "conhecimento explícito" em "conhecimento tácito" designa-se internalização e possui algumas semelhanças à tradicional noção de aprendizagem através da prática. O conhecimento internalizado torna-se "conhecimento tácito" do individuo podendo dar origem a uma nova espiral de conhecimento quando partilhado com outros indivíduos através de "socialização".

A compreensão das dinâmicas associadas à aquisição de conhecimento individual e coletivo são essenciais para qualquer domínio do saber e por maioria de razão para o Ciberespaço, cuja génese recente e permanente evolução obriga à aquisição de novos conhecimentos e adaptação de processos e comportamentos ajustados ao novo ambiente comunicacional, com reflexo nas políticas públicas e privadas.

1.2. Conhecimento Organizacional

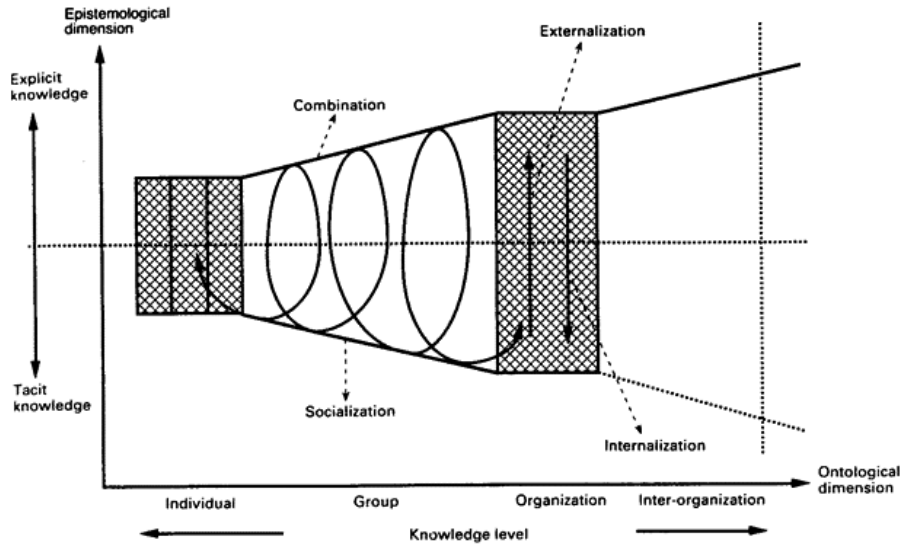
As organizações requerem não só que os seus colaboradores possuam conhecimentos e competências adequadas às suas atribuições mas que elas mesmas disponham de um conjunto diversificado de conhecimentos indispensáveis ao funcionamento dos seus processos e à conformidade de produtos e serviços. Tal foi reconhecido pela introdução do conceito de Conhecimento Organizacional na Norma ISO2015:1015 (Sistemas de Gestão da Qualidade – Requisitos).

Apesar de todas formas de conversão poderem criar conhecimento independentemente, Nonaka (1994) defendeu que a criação de "conhecimento organizacional" decorre da sua interação dinâmica e ocorre apenas quando as referidas formas são geridas pelas organizações de forma cíclica e contínua, numa "espiral de conhecimento".

Apesar do "conhecimento tácito" individual poder estar no centro do processo de criação de conhecimento, os seus maiores benefícios decorrem na sua externalização e amplificação. A espiral criada pela interação dos quatro modos de conversão de conheci-

mento através dos quais o conhecimento pode ser convertido de um tipo de conhecimento para outro, carateriza uma teoria[150] que também explica como o conhecimento individual é "amplificado" para toda a organização promovendo o conhecimento organizacional.

Figura 8 – Espiral da Criação do Conhecimento Organizacional



Fonte: Nonaka (1994).

As interações entre conhecimento tácito e conhecimento explícito tendem a aumentar em escala e velocidade à medida que mais atores (internos e próximos) são envolvidos. Desse modo, a criação de conhecimento organizacional poderia ser vista como um processo em espiral ascendente, com o seu foco deslocando-se progressivamente do nível individual, para o coletivo (grupo), organização e eventualmente entre organizações.

A criação de "conhecimento organizacional" inicia-se ao nível do "individuo" pela acumulação de "conhecimento tácito" obtido através da experiência, cuja qualidade depende da sua diversidade, grau de correlação[151] e "conhecimento da experiência". A qualidade do "conhecimento explícito" é influenciada pelo "conhecimento da racionalidade" que descreve a capacidade racional de refletir sobre a experiência adquirida.

O processo de criação do conhecimento organizacional ocorre ao nível do grupo, mas, para tal, as organizações precisam oferecer as condições necessárias, ou seja, contextos organizacionais que facilitem as atividades do grupo, a criação e a acumulação de conhecimento.

150 Também conhecida por SECI – Socialização, Externalização, Combinação e Internalização. Ver Argyris, C., 2006. *Reasons and Rationalizations: The Limits to Organizational Knowledge*. Oxford: Oxford University Press.

151 Também designada *high-quality experience*. Ver Nonaka (1994).

Nonaka, Toyama e Konno (2000) expandiram o anterior modelo propondo um modelo de criação de conhecimento baseado em três elementos:

(1) O processo SECI: criação de conhecimento através de socialização, externalização, combinação e internalização;
(2) O contexto partilhado de criação de conhecimento: "*ba*" (palavra japonesa para "lugar");
(3) Os ativos ou recursos do conhecimento (Nonaka, Toyama e Konno, 2000): *inputs*, *outputs* e "moderadores" do processo de criação de conhecimento. Segundo este modelo, o processo de criação de conhecimento é uma espiral que resulta da externalização destes três elementos.

Nonaka, Toyama e Konno (2000) definiram ativos (ou recursos) de conhecimento como "recursos específicos das empresas que são indispensáveis para criar valor" e consideram que representam os "*inputs*, *outputs* e fatores de mediação do processo de criação de conhecimento". A criação de novo conhecimento decorre dos ativos de conhecimento existentes através do processo SECI que ocorre num determinado contexto de interação. O conhecimento então criado integra-se nos ativos de conhecimento da organização e constitui a base de uma nova espiral de criação de conhecimento organizacional.

O conhecimento organizacional é um conhecimento específico de cada organização, adquirido através da experiência, utilizado e partilhado para alcançar os objetivos da organização. O conhecimento organizacional pode basear-se em: fontes internas – por exemplo, propriedade intelectual, experimentação, lições aprendidas com falhas e projetos bem-sucedidos, registo e partilha de conhecimento e experiência não-documentadas, resultados de melhorias em processos, produtos e serviços; fontes externas – por exemplo, normas, academia, conferências, conhecimento adquirido através de clientes, fornecedores ou concorrentes. A importância do conhecimento organizacional para a cibersegurança é reconhecida por Trim e Lee (2014).

1.3. Aprendizagem Organizacional

A capacidade de aprender das organizações é essencial em qualquer setor de atividade, área funcional e nível estrutural e, por maioria de razão, numa qualquer capacidade de cibersegurança, permitindo deduzir ensinamentos da análise da informação própria ou facultada por terceiros e incorporar o conhecimento adquirido nos processos e procedimentos internos. Porém, nem sempre as politicas publicas refletem esta preocupação.

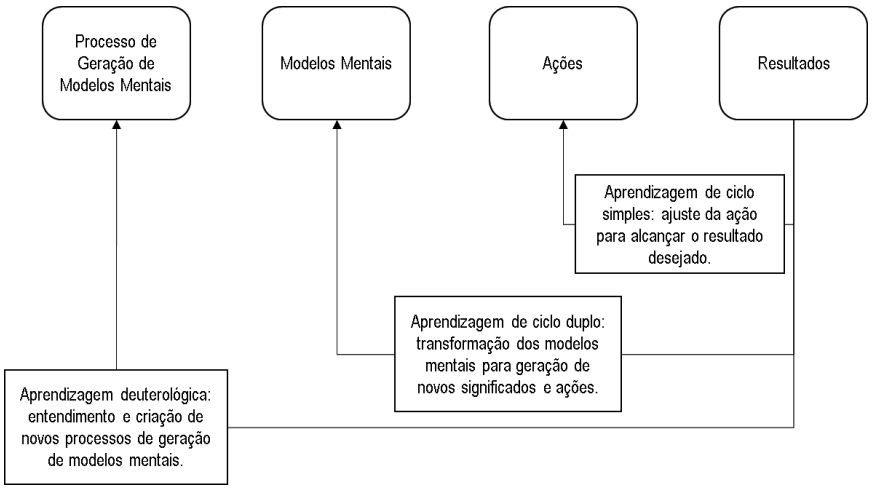
A ideia de que as organizações podiam aprender e manter o conhecimento ao longo do tempo foi inicialmente apresentado por Cyert e March (1963) realçando que através dos processos de aprendizagem organizacional as empresas se adaptavam ao ambiente envolvente e aprendiam através da experiência.

Fiol e Lyles (1985) definiram aprendizagem organizacional como "(…) o processo de melhoria das ações através de melhor conhecimento e compreensão" e Hedberg (1981) referiu que apesar da sua importância para as organizações, esta não resulta da mera soma das aprendizagens individuais. Segundo Argyris e Schön (1978), a "aprendiza-

gem organizacional" envolve a "deteção e correção de erros" e enunciaram três tipos de aprendizagem: ciclo simples, ciclo duplo e deuterológica.

A aprendizagem de ciclo [*feedback*] simples – *single-loop learning* (SLL) – tem por base o trabalho de Bateson (1972) que considera como aprendizagem a capacidade de uma qualquer organização se manter estável perante um contexto de mudança. Neste tipo de aprendizagem, o ciclo de *feedback* faz a ligação entre os resultados das ações observadas com as estratégias e pressupostos das organizações, de que resulta o seu eventual ajustamento de forma a manter a performance dentro dos parâmetros adequados às "normas em vigor" – qualidade, vendas, performance, etc. –, que permanecem inalteradas.

Figura 9 – Tipos de Aprendizagem



Fonte: Probst e Buchel (1994).

A aprendizagem organizacional ocorre quando os indivíduos, enquanto "agentes da aprendizagem" organizacional, detetam uma concordância ou divergência dos resultados com a expetativa, confirmando ou infirmando a teoria. No caso de divergência estes passam da deteção do erro para a sua correção, devendo:

(1) Descobrir a origem dos erros;
(2) Criar novas estratégias baseadas em novos pressupostos por forma a corrigir o erro e avaliar e generalizar os resultados da nova ação;
(3) Integrar as conclusões[152] na "memória organizacional" que influenciará a ação futura. Se tal não ocorrer, os indivíduos podem ter aprendido mas não a organização.

152 "discoveries, inventions, and evaluations". Ver Argyris, C. e Schön, D. A., 1978. *Organizational Learning: A theory of action perspective*: Addison-Wesley Publishing Company.

Em conclusão, foco do "ciclo de *feedback* simples" da OL é a eficácia[153]. A aprendizagem individual é uma condição necessária mas insuficiente para a aprendizagem organizacional e requer que o resultado da mesma seja incorporada na organização.

A aprendizagem de ciclo [*feedback*] duplo – *double-loop learning* (DLL) – ocorre quando o ciclo de aprendizagem organizacional requer a modificação das normas de referência. A incompatibilidade dos requisitos da organização é inicialmente expressa através de conflitos entre os seus membros ou grupos. Quando a aprendizagem ocorre resulta um processo de investigação (ou análise) através do qual os grupos se confrontam e resolvem o conflito emergente. A organização é um meio para transformar requisitos incompatíveis em conflitos interpessoais e intergrupais. A resposta a esses conflitos pode ocorrer de vários modos apesar nem todos considerados de aprendizagem de ciclo duplo (DLL).

A aprendizagem de ciclo duplo designa a análise organizacional que soluciona normas incompatíveis através de novas prioridades e pesos ou da sua reestruturação, assim como estratégias e pressupostos associados. Os indivíduos resolvem os conflitos interpessoais e intergrupais, decorrentes da manifestação de incompatibilidade de requisitos, através de uma nova compreensão dos requisitos conflituantes, suas fontes, condições e consequências.

A aprendizagem deuterológica[154] ocorre quando os membros de uma organização aprendem a aprender a partir dos outros contextos de aprendizagem de SLL e DLL anteriores, através da reflexão e análise sobre os mesmos. Da identificação dos elementos facilitadores ou inibidores da aprendizagem são criadas novas estratégias de aprendizagem e promovem a sua avaliação e adoção. Os resultados são incorporados pelos indivíduos e refletem-se na prática de aprendizagem organizacional.

Em síntese, uma qualquer capacidade de cibersegurança requer e forma explicita a integração dos três processos de aprendizagem nos processos de gestão que lhe estão subjacentes. A sua inexistência favorece a repetição dos erros e/ou o não reconhecimento de boas práticas e desse modo favorecendo a ineficiência.

1.4. Melhoria Contínua

> "Sendo a digitalização um dos principais componentes dos serviços públicos e do funcionamento da sociedade, o governo enfatiza a necessidade de melhorias constantes na segurança cibernética e da informação" (Government of Denmark, 2015).

Segundo Bhuiyan e Baghel (2005, p. 762) as origens da melhoria contínua remontam ao séc. XIX e às iniciativas empresariais que, com a participação dos seus colaboradores, visavam a introdução de mudanças nas organizações. No final desse século e início do

153 "(…) how best to achieve existing goals and objectives and how best to keep organizational performance within the range specified by existing norms." *Idem*.

154 No original "*deutero-learning*". Discurso do defensor oficioso nos tribunais de Atenas, na Grécia antiga, após o discurso do acusado. "deuterologia". Dicionário Priberam da Língua Portuguesa 2008-2013, disponível em http://www.priberam.pt/dlpo/deuterologia.

séc. XX foi dada uma maior atenção à adoção de métodos científicos[155] na gestão para resolver problemas de produção (otimização). Durante a Segunda Guerra Mundial o governo dos EUA criou o programa "*Training Within Industry*" para melhorar a produção industrial que incluía técnicas de melhoria contínua, mais tarde adotadas e expandidas pela indústria Japonesa – *e.g. Kaisen,* palavra japonesa para melhoria continua.

Segundo o The Chartered Quality Institute[156] a melhoria contínua é "um tipo de mudança que está focada no aumento da eficácia e/ou eficiência de uma organização para cumprir a sua política e objetivos". Para Bhuiyan e Baghel (2005, p. 761) a melhoria contínua reflete uma "cultura de melhoria sustentada visando a eliminação de desperdícios".

Boer, Berger, Champna e Gertsen (2000) descrevem a melhoria contínua como um processo planeado, sistematizado e organizado que visa modificar as práticas existentes e desse modo melhorar o desempenho da organização. Esta definição aparenta refletir uma abordagem estruturada *top-down,* contestada por outros autores que consideram essencial o envolvimento de todos os colaboradores na concretização das iniciativas de melhoria.

Para Michela, Noori e Jha (1996)[157] o foco da melhoria contínua não é a mudança mas a avaliação dos resultados da mudança de modo a permitir uma atuação fundamentada que permita melhorar o processo.

A melhoria contínua aplica-se quer ao setor público quer ao setor privado, confrontados com a necessidade de "fazer mais com menos" (Fryer, Antony e Douglas, 2007). Segundo estes autores, a necessidade de melhoria contínua no setor privado decorre, nomeadamente, da crescente competição e regulamentação dos mercados e das expetativas de aumento da qualidade dos produtos e serviços fornecidos, enquanto no setor público resulta da necessidade de melhoria de processos que satisfaçam progressivamente mais cidadãos, permitam reduzir custos e minimizar erros.

Os possíveis benefícios da melhoria contínua são segundo Cole (2001) são nomeadamente:

(1) Maximização dos resultados e a possibilidade de concretizar mudanças extensas na sequência de múltiplos pequenos sucessos concorrentes;
(2) Incremento da aprendizagem (individual e organizacional) decorrente de uma maior aceitação de alterações em que os próprios participam;
(3) Promoção do conhecimento e aprendizagem através da disseminação dos pequenos sucessos da organização;

155 Durante a Segunda Guerra Mundial os Aliados viram-se confrontados com um conjunto de problemas de natureza logística, tática ou estratégica, de grande complexidade. Para apoiar a sua resolução através do método científico, um conjunto de cientistas (matemáticos, físicos e engenheiros) desenvolveram modelos matemáticos que lhes permitiam perceber os problemas, ensaiar e avaliar hipóteses de forma a encontrar soluções otimizadas que suportassem o processo de decisão. Esse novo corpo metodológico permitiu a individualização da Investigação Operacional – *Operational Research* (Reino Unido) ou *Operations Research* (EUA). No pós-guerra, alguns dos métodos matemáticos então desenvolvidos para aplicação militar foram progressivamente introduzidos na indústria, pelo que nos EUA a Investigação Operacional é também conhecida por *Management Science*.

156 The Chartered Quality Institute (CQI). [Website] Disponível em http://www.thecqi.org/

157 Citado por Fryer, K.; Antony, J. e Douglas, A., 2007. Critical success factors of continuous improvement in the public sector: A literature review and some key findings. *The TQM magazine*, 19(5), pp. 497-517.

A experiência com a adoção de métodos de gestão científicos e a necessidade de aumentar a escala da sua implementação fomentou o desenvolvimento de diversas metodologias de melhoria contínua, das quais se realça o "*lean thinking*"[158], "*six sigma*"[159], "*lean six sigma*"[160], *kaizen*[161], 5S e PDCA (Bhuiyan e Baghel, 2005; Santos, 2013), que tal como as normas da ISO, ISACA e NIST têm em comum o método PDCA.

O ciclo PDCA (*Plan-Do-Check-Act*) ou *"ciclo de Deming"*[162] é um método iterativo de gestão para a melhoria contínua e controle de processos e produtos baseado no método científico, que permite desenvolver o pensamento crítico, aumentar a eficiência e competitividade.

Neste ciclo são definidos os objetivos para um determinado processo/produto para o qual se pretende obter melhoria (*Plan*); implementado o que foi planeado (*Do*); verificado se os objetivos foram alcançados (*Check*) *i.e.* se a melhoria foi implementada; e identificados os fatores de sucesso ou fracasso de modo a influenciar um novo processo de planeamento visando definir novas ações de melhoria (*Act*).

Um outro modelo muitas vezes referido indistintamente é o ciclo OODA – *Observe; Orient; Decide; Act* – ou ciclo de *Boyd*, desenvolvido na década de 1970 pelo Coronel John Boyd tendo por base a análise de combates aéreos. Apesar de desenvolvido para aplicação militar, este método pode ser aplicado igualmente a situações empresariais ou competitivas.

O ciclo PDCA é uma abordagem analítica que utiliza dados internos da organização para análise e decisão de progresso, cuja verificação permite confirmar ou rejeitar a hipótese suscitada pela análise. O OODA é igualmente uma abordagem analítica que a partir da observação de um ambiente externo (ou envolvente) complexo e sujeito a imprevisibilidade permite sintetizar um plano de ação e orientar o processo de decisão da entidade ou organização para a ação.

Os dois modelos com estrutura em ciclo iterativo são compatíveis e complementares, apesar de possuírem diferenças importantes. As normas internacionais (ISO, ISACA e NIST) adotam o PDCA como método de melhoria contínua dos processos internos, que por sua vez requerem a identificação e implementação de lições cujos processos pressupõem o OODA – *e.g.* processo de Lições Aprendidas da NATO.

1.5. Lições Aprendidas

As Lições Aprendidas são práticas comuns de Gestão do Conhecimento[163], através das quais as organizações procuram acelerar a aprendizagem individual e organizacional

158 Womack, J. P. e Jones, D. T., 2003. *Lean thinking: banish waste and create wealth in your corporation*. New York: Free Press, p. 396.

159 Linderman, K.; Schroeder, R.G.; Zaheer, S. e Choo, A. S, 2003. Six Sigma: A goal-theoretic perspective. *Journal of Operations Management*, 2(6), pp. 220-235.

160 George, M. L., 2002. *Lean Six Sigma*. McGraw-Hill.

161 Kato, I. e Smalley, A., 2011. *Toyota Kaizen Methods: Six Steps to Improvement*. New York: Productivity Press.

162 Divulgado por Edwards Deming e baseado nos estudos de Walter A. Shewart.

163 McInerney, C. e Koenig, M. E. D., 2011. *Knowledge Management Processes in Organizations: Theoretical Foundations and Examples of Practice*. New York: Morgan & Claypool Publishers.

a partir da experiência e preencher a lacuna entre a norma (processos padrão)[164] e a realidade e desse modo alcançar melhorias, desenvolver novos produtos, etc..

As Lições aprendidas têm subjacente uma abordagem formal para a aprendizagem, permitindo que indivíduos e organizações possam reduzir o risco da repetição de erros e aumentar a probabilidade de repetição de sucessos. No contexto militar, isso pode significar nomeadamente, a redução do risco operacional, maior eficiência de custos e melhoria da eficiência operacional.

Aprender através da experiência é uma das mais básicas atividades humanas. Mas se aprender é uma atividade natural, por que motivo é tão dificil a aprendizagem nas organizações? A criação de conhecimento individual ou organizacional, são atividades complexas, nomeadamente pelo contexto da aprendizagem, implicações culturais e organizacionais.

Secchi, Ciaschi e Spence (1999) definem Lição Aprendida como:

> "(…) Um conhecimento ou compreensão adquirido pela experiência. A experiência pode ser positiva, como num teste ou missão bem-sucedida, ou negativa, como em caso de acidente ou falha. Os êxitos também são considerados fontes de lições aprendidas. (...) deve ser significativa por ter um impacto real ou presumido nas operações; válido na medida em que é factual e tecnicamente correta; e aplicável na medida em que identifica um projeto, processo ou decisão específica que reduz ou elimina o potencial de falha e acidente, ou reforça um resultado positivo".

Esta definição de Lição Aprendida realça um conjunto de elementos extremamente importantes e que importa referir:

(1) Forma de conhecimento – *i.e* "competência" conforme modelo KSAO[165];
(2) Resulta de experiência, enquanto fonte de "conhecimento tácito"[166] ou "conhecimento explícito" internalizado[167] , positivo ou negativo;
(3) Significativa, baseada em evidência, tecnicamente correta e aplicável, o que implica "análise" decorrente da comparação entre a "realidade" e a "norma" conforme aprendizagem organizacional[168].

Para Lo e Fong (2010) as Lições Aprendidas permitem que sejam tomadas decisões fundamentadas não seguindo regras cegamente e permitido compreender as razões em que os seus antecessores se fundamentaram basearam para fazer opções e tomar decisões. Esta abordagem tem certamente ligações com os processos de aprendizagem organizacional propostos por Argyris e Schön (1978).

A obtenção ou criação de novos conhecimentos através de Lições Aprendidas em contexto organizacional exige que estas sejam efetivamente aprendidas (*i.e.* implementadas), o que significa introduzir mudanças nos processos da organização como resultado

164 Argyris, C. e Schön, D. A., 1978. *Organizational Learning: A theory of action perspective*. Addison-Wesley Publishing Company.

165 Mendes, J. S. e Sarmento, M., 2009. A Importância da Gestão de Competências nas Organizações. *Economia & Empresa*, N.º 9, pp. 114-139.

166 Polanyi, M., 1996. *The Tacit Dimension*. London: Routledge & Kegan Paul.

167 Nonaka, I., Toyama, R. e Konno, N., 2000. SECI, *Ba* and Leadership: a Unified Model of Dynamic Knowledge Creation. *Long Range Planning,* 33(1), pp. 5-34.

168 Argyris, C. e Schön, D. A., 1978. *Organizational Learning: A theory of action perspective*: Addison-Wesley Publishing Company.

do novo conhecimento, isto é que sejam incorporadas na "memória organizacional", tal como nos tipos de Aprendizagem Organizacional[169].

A capacidade e motivação de cada indivíduo em aprender e mudar – *i.e.* empenhamento, que é igualmente uma condição indispensável para a aquisição de "conhecimento tácito" – traduz o sucesso da capacidade de Lições Aprendidas e promove a melhoria contínua da organização.

1.6. Continuidade de Negócio

De acordo com a norma ISO/IEC 22301[170], continuidade de negócio[171] é a capacidade de uma qualquer organização, na sequência de um incidente disruptivo, continuar a fornecer produtos ou serviços em níveis aceitáveis predefinidos.[172]

O desafio da continuidade de negócio ultrapassa a mera preparação de planos de emergência ou a adoção de estratégias de gestão de catástrofes, que antecipem e minimizem as consequências de perturbações naturais, acidentais ou intencionais.

As organizações requerem processos pró-ativos, abrangentes e sistemáticos de prevenção, proteção, preparação, mitigação, e resposta para a continuidade do negócio e sua recuperação[173]. As ameaças exigem processos contínuos, que garantam a sustentabilidade das atividades essenciais de uma organização antes, durante e depois de um evento disruptivo. A capacidade de recuperação de uma organização após um desastre está intimamente ligada ao planeamento da continuidade de negócio antes do desastre através de planos de continuidade de negócio – *Business Continuity Plans* (BCP).

De acordo com o Business Continuity Institute (2016) a continuidade de negócio visa a construção e melhoria da "resiliência" da organização, pressupondo a identificação dos produtos e serviços essenciais e "atividades mais urgentes que as sustentam", a elaboração de planos e estratégias que permitam continuar as operações que lhe estão associadas e favorecer uma rápida recuperação face a qualquer tipo de interrupção independentemente da sua dimensão ou causa.

Segundo Watters (2014), a continuidade de negócio é simultaneamente uma disciplina e um processo. Enquanto disciplina, engloba: (1) O planeamento da continuidade de negócio, visando a preparação para um incidente; (2) A continuidade do serviço, visando a configuração, manutenção e teste das soluções tecnológicas que suportam a continuidade do negócio; e a (3) Gestão de crises, enquanto processo a adotar para responder a eventos que o *business as usual* não permite enfrentar. Enquanto processo ou ciclo de vida, descreve como uma qualquer organização deve garantir que atividades críticas são realizadas independentemente da ocorrência de acontecimentos inusitados.

---

169 *Ibidem.*

170 International Organization for Standardization (ISO). 2016a. ISO 22301:2012. Disponível em https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

171 Na língua inglesa designada *Business Continuity*.

172 International Organization for Standardization (ISO) 2012. *I*SO 22301:2012. Disponível em https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

173 St-Germain, R. *et al.*, 2012. *White Paper on Societal security: Business Continuity Management Systems*. Disponível em: www.pecb.org/iso22301

1.7. Resiliência Cibernética

Muitas pessoas acreditam que a cibersegurança ou segurança cibernética é algo que se pode adquirir incrementalmente como uma mercadoria. Outros acreditam a cibersegurança se refere exclusivamente a questões técnicas, como a utilização de *passwords* ou a instalação de *firewalls* para proteger uma rede de computadores. Ainda assim, outros acreditam que se trata de uma capacidade técnica e administrativa da exclusiva responsabilidade dos profissionais de TI.

A cibersegurança não é apenas uma questão técnica, mas um imperativo das organizações que implica gerir riscos visando a continuidade do negócio, protegendo os investimentos e os ativos, mantendo a reputação e vantagem competitiva. Para lidar com a multiplicidade de potenciais ameaças, requer uma abordagem sistémica e multidisciplinar que permita gerir o risco, nomeadamente, através da adoção da norma ISO 22301.

Randall (2015) exorta para a necessidade de serem aprendidas das lições do ataque à Sony Pictures em 2014, sugerindo a inclusão de cenários de ataque cibernético nos planos de continuidade de negócio e recuperação tecnológica. Este autor dá ainda nota de uma atualização do FFIEC[174] para o setor dos serviços financeiros dos EUA, que pela primeira vez inclui estratégias de mitigação de risco que promovem um aumento da resiliência cibernética face à escalada de ataques contra a indústria. O seu anexo J[175] reforça a responsabilidade da organização no apoio à gestão dos riscos dos ISP[176], nomeadamente que decorrem de *malware*, ameaças internas, destruição ou corrupção de dados ou sistemas e quebra de infraestruturas de comunicações tais como ataques DDoS[177].

De igual modo, as orientações[178] publicadas para a resiliência cibernética das instituições financeiras – Financial Market Infrastructures (FMI) – descrevem cinco categorias de gestão de risco primárias e três componentes fundamentais a considerar na estrutura de resiliência cibernética das infraestruturas financeiras. As categorias de gestão de risco são: governança; identificação; proteção; deteção; e resposta e recuperação. As componentes fundamentais são: testes; consciência situacional (*situational awareness*); aprendizagem e evolução. Para alcançar a desejada resiliência das infraestruturas financeiras é requerida uma abordagem integrada e sinergias nos investimentos associados.

Na componente aprendizagem e evolução é realçada a importância da implementação de um quadro de resiliência cibernética adaptativa e evolutiva, que permita identificar,

174 FFIEC, 2015b. *Federal Financial Institutions Examination Council*. Disponível em https://www.ffiec.gov/about.htm

175 FFIEC, 2015a. *Appendix J: Strengthening the Resilience of Outsourced Technology Services*. Disponível em: http://tinyurl.com/ntpr9ch.

176 Internet Service Providers.

177 Ataque de negação de serviço ou Denial of Service Attack (DDoS). "A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information" Digital Attack Map, 2016. *What is a DDoS Attack?*. Disponível em: http://www.digitalattackmap.com/understanding-ddos/.

178 Bank for International Settlements (BIS) e International Organization of Securities Commissions (IOSCO), 2016. *Guidance on cyber resilience for financial market infrastructures*. BIS/IOSCO, June 2016, pp. 32. Disponível em https://www.bis.org/cpmi/publ/d146.pdf

avaliar e gerir as ameaças e vulnerabilidades de segurança, visando a salvaguarda dos sistemas, estando subdividida em "*continuous learning*" e "*cyber resilience benchmaking*".

As referidas orientações relativas à resiliência cibernética das infraestruturas financeiras aproximam-se assim da norma ISO 22301 requerendo nomeadamente, a implementação de uma capacidade de Lições Aprendidas que promova a recolha nomeadamente de observações sobre eventos – *e.g.* intrusões ou tentativas, violações dados, *malware*, etc. –, exercícios ou planos; a análise da informação e identificação de ações corretivas ou boas práticas, monitorização da implementação dos planos de ação corretiva, validação e difusão de lições.

1.8. "Ciber-higiene"

A expressão higiene cibernética ou ciber-higiene foi utilizado pela primeira vez por Vinton Cerf (2000):

> "A maioria das vulnerabilidades advém daqueles que usam internet, empresas, governos, instituições académicas e indivíduos, mas que não praticam o que eu chamo de boa higiene cibernética".

A ciber-higiene está associada à adoção de práticas que visam reduzir as vulnerabilidade das TIC podendo definir-se como as " (…) práticas fundamentais geralmente necessárias para estabelecer e manter a segurança de qualquer sistema de TI" (Commission on Enhancing National Cybersecurity, 2016).

A ciber-higiene desempenha um papel crítico em toda a UE na proteção das empresas e fornece as bases para a proteção das infraestruturas e dos dados dos clientes das quais as empresas dependem. Esta importância é reconhecida na União Europeia, na medida em que quase todos os Estados-membros desenvolveram uma estratégia nacional de segurança cibernética que visa melhorar e melhorar a forma como as organizações se protegem das ameaças cibernéticas (ENISA, 2016). De acordo com o referido estudo da European Union Agency for Network and Information Security (ENISA), na Europa existem três programas publicos de ciber-higiene: Bélgica, França e Reino Unido.

As recomendações para proteção dos computadores pessoais dos utilizadores incluem normalmente o uso de senhas de autenticação fortes (complexas) alteradas com frequência e não escritas, atualização do sistema operativo, acesso remoto – Remote Desktop Protocol (RDP) – desabilitado, *software* de antivírus e antispyware instalado e atualizado, proteção do *browser* e dos respetivos *add-ons*, utilização de *firewall*, verificação de anexos dos emails, proteção da rede *wifi*, *backup* de dados importantes, etc. (U.S. Department of Homeland Security, 2016)

As recomendações relacionadas à higiene cibernética para administradores de sistemas informáticos incluem, mas não estão limitadas à segmentação de redes, definição de perfis de utilizador com delimitação de permissões de acesso a recursos de informação, aplicação de regras autenticação com senha fortes, instalação e configuração de *firewalls* de acordo com as melhores práticas, *software* de proteção antivírus e antispam instalado corretamente e atualizado, manutenção atualizada de todos os sistemas operativos garantindo que todos os *patches* de *firmware* e *software* estejam instalados, remoção de *software* não autorizado, etc.

1.9. Governação

"A complexidade e a abrangência dos desafios da segurança do ciberespaço requerem uma liderança e governação forte e transversal (…)." (PCM, 2015b).

"A correlação entre segurança, liberdade e benefícios socioeconomicos (…) é um equilíbrio dinâmico (…) entre todas as partes interessadas, tanto nacionais como internacionais. Para isso, precisamos de um modelo de governança[179] claro" (Government of The Nederlands, 2013).

A implementação da política de segurança cibernética na Letónia envolve uma ampla gama abrangente de partes interessadas; portanto, é necessário criar um modelo efetivo de governança de segurança cibernética." (Government of Latvia, 2013).

A governação das capacidades de cibersegurança e ciberdefesa à escala nacional e transnacional é essencial para a resiliência cibernética. A informação, recurso último a proteger pela segurança cibernética, é um bem fundamental para todas as organizações, para os negócios e as pessoas, assim como os processos que lhe estão associados (criação, utilização, retenção, disponibilização/exposição e destruição), e as tecnologias que os suportam. Além desses processos, podem existir outros não motivados ou controlados pela própria organização, decorrentes de ação mal-intencionada ou erro, originando informação "não utilizável" ou a exposição da mesma.

Normalmente, as organizações procuram:

(1) Assegurar a manutenção da informação que suporta os processos de decisão;
(2) Gerar valor para o negócio através dos investimentos em tecnologia;
(3) Alcançar excelência operacional através da aplicação fiável e eficaz da tecnologia;
(4) Manter o risco induzido pelas TI num nível aceitável;
(5) Otimizar os custos da tecnologia e dos serviços de TI.

Gerar valor para o negócio e para as partes interessadas (*stakeholders*) através de TI requer:

(1) A boa governação e gestão da Informação e dos ativos tecnológicos subjacentes;
(2) A necessidade de encarar – por parte das administrações, gestão de topo e gestão intermédia – as TI como qualquer outra parte importante do negócio;
(3) A necessidade de conformidade com requisitos legais, regulatórios e contratuais relacionados com a utilização da informação e da tecnologia;
(4) Um quadro normativo (*framework)* abrangente que suporte as organizações na realização dos seus objetivos e na entrega de valor através de uma efetiva governação e gestão das tecnologias corporativas.

Para apoiar as organizações na governação e gestão das TI, foram desenvolvidas diversas metodologias das quais destacamos o COBIT 5 (Governance of Entreprise IT),

179 Refere-se às regras, processos e comportamentos através dos quais os interesses são articulados, os recursos são geridos e o poder é exercido na sociedade. Comissão das Comunidades Europeias, 2003. *Comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu. Governança e Desenvolvimento.* COM(2003) 615 final, 20.10.2003, Bruxelas. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52003DC0615&from=PT

ITIL (Information Technology Infrastructure Library) e BS7799 (British Standard). O ITIL foi concebido como uma estrutura de gestão de serviços para apoiar a compreensão da forma como são apoiados os processos e entregue os serviços. O COBIT (Control Objectives for Information and Related Technology) foi criado como um modelo de governança de TI, inicialmente com um foco em auditoria, com objetivos de controlo e práticas de controlo sobre como esse processo se deve se comportar. A norma do Reino Unido BS7799[180] para a Segurança da Informação é composta por 3 partes e tem vido a ser integrada e/ou alinhada com as normas da ISO[181].

A ISO 17799 descreve os controlos de segurança, mas não em como integrá-los nos processos de negócio. A ITIL concentra-se nos processos de TI e não em segurança, enquanto a COBIT se concentra em controlos e métricas, não tanto na segurança. A COBIT diz "o que" se deve fazer, enquanto a ITIL diz "como" se deve fazer, pelo que utilizadas conjuntamente constituem um modelo extremamente poderoso na gestão de processos.

Estas metodologias ou normas não estão em concorrência mútua, podendo e devendo ser usadas conjuntamente. A COBIT pode ser usada para determinar se as necessidades da empresa (incluindo segurança) estão sendo devidamente atendidas pelas TI. A ISO 17799 pode ser usada para determinar e melhorar a postura de segurança da empresa, e a ITIL pode ser usada para melhorar os processos de TI para atingir os objetivos da empresa (incluindo segurança).

1.10. Planeamento de Longo Prazo

Uma das maiores dificuldades na conceção e planeamento de um sistema de segurança cibernética (cibersegurança ou ciberdefesa) decorre da sua complexidade, pelo volume dos recursos envolvidos (humanos, organizacionais, materiais e financeiros, etc.) numa perspetiva de médio e longo prazo e em interação com múltiplos atores.

A análise do custo total de propriedade (TCO)[182] tem o seu foco na identificação dos custos diretos e indiretos associados aos investimentos no domínio das TIC, podendo ser um precioso auxiliar na conceção de um novo sistema na medida em que tem em consideração cada uma das fases do respetivo ciclo de vida. Porém, o TCO não tem em con-

180 A BS7799-1 com as melhores práticas da gestão da segurança da informação foi adotada pela ISO através da norma ISO/IEC 17799 (*Information Technology – Code of practice for information security management*) e posteriormente (2007) integrada na série de normas ISO 27000 como ISO/IEC 27002. A BS7799-2 (*Information Security Management Systems – Specification with guidance for use*, publicada em 1999) abordava como implementar um sistema de Gestão da Segurança da Informação (ISMS), que mais tarde se tornou ISO / IEC 27001. A BS7799-3 (*Information security management systems –- guidelines for information security risk management*), publicada em 2005, cobre a área de gestão e análise de risco e está alinhada com a ISO/IEC 27001.

181 International Organization for Standardization (ISO). [Website] Disponível em www.iso.org.

182 Total cost of ownership: "(…) comprehensive assessment of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses" Gartner, 2017. Total Cost of Ownership (TCO). *Gartner*. Disponível em http://www.gartner.com/it-glossary/total-cost-of-ownership-tco.

sideração outros elementos não tecnológicos e/ou não quantificáveis financeiramente essenciais para a concretização de um sistema "complexo".

A Research and Technology Organization (RTO)/NATO definiu o conceito de Planeamento de Defesa de Longo Prazo[183] (LTDP) exigindo um diálogo contínuo entre os *long-term planners* e os *policy makers*. A RTO/NATO (2003) identifica diversas possíveis abordagens[184] das quais se realça o Planeamento baseado em Capacidades.

Este método envolve uma análise funcional das possíveis operações futuras, da qual resulta não um sistema de armamento concreto ou sistema de forças, mas uma descrição das tarefas que a estruturas de forças deve ser capaz de se realizar expresso em termos de capacidades. Essas tarefas, que consubstanciam as capacidades, são caraterizadas em termos de linhas de desenvolvimento (doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade)[185].

1.11. Recrutamento, Formação e Retenção de Talentos

> "Ampliar e ampliar o recrutamento de talentos, programas avançados de pesquisa e treinamento em segurança cibernética em cooperação com universidades e centros especializados (Linha de Ação 6, Conhecimento, Competencias e I&D)." (Government of Spain, 2013).

Segundo o Center for Strategic and International Studies (2016) não existem profissionais de segurança cibernética suficientes para defender adequadamente as redes informáticas, pelo que os países e as empresas devem agir rapidamente, recrutando, melhorando a educação e a diversificação da força de trabalho, promovendo oportunidades de treino, melhorando as tecnologias de segurança e de recolha de dados. Todavia, as Estratégias de Cibersegurança não refletem esta realidade.

A formação e qualificação de recursos humanos em segurança cibernética é muito exigente, longa e onerosa, exigindo avultados investimentos em equipamentos, treino e certificação, cujo retorno só é possível se for possível assegurar os recursos humanos qualificados numa perspetiva de médio e longo prazo.

De acordo com AlienVault (2016), melhores salários e benefícios, treino e certificação, trabalho flexível, mais desafiante e excitante e uma melhor cultura de trabalho foram identificadas como razões para decidir mudar de emprego. As conclusões desse estudo realçam ainda a importância da localização e cultura da equipa e empresa, não se devendo assumir que são idênticas. Formação, qualificação, recrutamento e retenção de talentos são fundamentais para a segurança do ciberespaço.

---

183 Long Term Defence Planning: processo que estuda possíveis ambientes operacionais futuros e desenvolve um plano para melhor adaptar a organização de defesa a esses ambientes de acordo com um conjunto de restrições, nomeadamente financeiros. RTO/NATO, 2003. *Handbook on Long Term Defence Planning*.

184 Top-Down Planning, Resource-constrained Planning, Technology Optimism, Risk Avoidance, Incremental Planning, Historical Extension, Capability-based Planning, Scenario-based Planning e Threat-based Planning. *Ibidem*.

185 DOTMLPF-I.

CAPÍTULO V
Políticas Nacionales de Ciberseguridad

1. Caso de Chile

La formulación de la Política Nacional de Ciberseguridad en el año 2017 es resultado de un trabajo que comienza en 2014 y contempla un diagnóstico sobre el tema, el cual identifica varias situaciones en el país que coinciden con tendencias internacionales y corresponden a: importancia de las tecnologías que permiten el uso del ciberespacio; creciente uso de internet; incremento de la incorporación de tecnologías emergentes ("Big data", "internet de las cosas", "automatización cibernético de procesos", "uso de sistemas SCADA"); aumento de incidentes en el ciberespacio caracterizados por crecientes amenazas detectadas y ataques cada vez más sofisticados; brechas de seguridad que no sólo afectan infraestructuras y capacidades, sino también los derechos de las personas; carencia de una cultura que prácticas de ciberseguridad; en forma masiva en la población; y ausencia de una política integral de ciberseguridad. Son fundamentalmente estos elementos los que permiten entender los principales aspectos contenidos en la Política Nacional de Ciberseguridad elaborada en el marco del Comité Interministerial de Ciberseguridad (CICS) en el cual participa:

(1) Subsecretaría de Interior y Seguridad Pública;
(2) Subsecretaría de Defensa Nacional;
(3) Subsecretaría de Relaciones Exteriores;
(4) Subsecretaría de Justicia;
(5) Subsecretaría General de la Presidencia;
(6) Subsecretaría de Telecomunicaciones;
(7) Subsecretaría de Economía;
(8) Subsecretaría de Hacienda y;
(9) Agencia Nacional de Inteligencia.

El CICS fue creado con el Decreto 533 del Ministerio del Interior y Seguridad Pública, el 27 de Abril de 2015, siendo cinco los considerando que justifican su creación y corresponden a:

> "1. Que el desarrollo y la masificación en el uso de las tecnologías de información y comunicaciones conlleva riesgos asociados que afectan los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de Chile, a nivel nacional e internacional.
> 2. Estos riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave a la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados, o, incluso, por sujetos individuales.
> 3. Que el programa de gobierno de la Presidenta Michelle Bachelet 2014-2018 contempla el desarrollo de una estrategia de seguridad digital que proteja a los usuarios privados y públicos.

4. Que corresponde al Ministerio del Interior y Seguridad Pública la coordinación, implementación y evaluación de las políticas, planes y programas en materia de seguridad pública, para lo cual puede solicitar la colaboración de los demás organismos que integran la Administración del Estado, propendiendo a la unidad de acción
5. Que corresponde al Ministerio de Defensa Nacional proponer y evaluar la política de defensa y efectuar el análisis político y estratégico de la apreciación de los riesgos y amenazas para el país en el ámbito de su seguridad exterior"[186].

La revisión de la Política Nacional de Ciberseguridad difundida el 27 de abril del 2017 por la Presidente de la República, Sra. Michelle Bachelet Jeria, desde la perspectiva de los factores de política pública a considerar en materia de ciberseguridad permite conocer el modo en que cada uno de los factores identificados se encuentran descritos en el caso de Chile.

1.1. Aproximación Conceptual

En el ámbito del ciberespacio se reconoce la existencia de diversos fenómenos. Uno de ellos es la necesidad de brindar seguridad. Para precisar la naturaleza de los fenómenos que se manifiestan en el ciberespacio asociados a la seguridad ha sido necesario formular definiciones que perta homologar conceptos que sirva para una mejor comunicación comunicación entre las diversas instituciones involucradas en la prevención, enfrentamiento o mitigación de ellos, como asimismo, para compartir un común entendimiento de la naturaleza del concepto al cual se hace referencia.

En este sentido, en el documento "Bases para una Política Nacional de Ciberseguridad" del año 2015 se incluyó un glosario con los principales términos ocupados en materia de ciberseguridad y que se detalla a continuación[187]:

(1) Ciberespacio: es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

(2) Ciberseguridad: es tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición. En un documento posterior de mayor rango que establecido que el concepto es definido como "aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición."[188], constatándose continuidad en la aproximación conceptual a los términos.

186 Decreto 533 del Ministerio del Interior y Seguridad Pública, el 27 de Abril de 2015. Disponible en https://www.leychile.cl/Navegar?idNorma=1079608.

187 Ministerio del Interior y Seguridad Pública/Ministerio de Defensa Nacional, 2015. *Bases para una Política Nacional de Ciberseguridad.* Gobierno de Chile. Disponible en http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf.

188 Ministerio del Interior, 2015. Decreto num. 533, artículo séptimo. Crea Comité Interministerial sobre Ciberseguridad. Chile. Disponible en https://www.leychile.cl/Navegar?idNorma=1079608.

(3) Ciberconflicto: es la expresión de intereses contrapuestos, entre dos o más partes, en relación a temas, intereses o valores que se manifiestan en el ciberespacio.
(4) Ciberataque: es una expresión del ciberconflicto consistente en acciones hostiles desarrolladas en el ciberespacio con el objetivo de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica, componente lógico o interacciones de éste y pueden tener distintos niveles según su duración, frecuencia y daño generado.
(5) Ciberdefensa: el término posee dos acepciones – (a) en un sentido amplio, son acciones contempladas en el marco de una política nacional de ciberseguridad orientadas a proteger el ciberespacio ante cualquier acción que pueda dañarlo; (b) en un sentido restringido, es el conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio, de acuerdo con sus atribuciones constitucionales y legales.
(6) Cibercrimen: son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos.
(7) Componentes lógicos de la información: los componentes lógicos de la información corresponden a la capa abstracta de datos que fluyen a través de las infraestructuras físicas de la información. Son componentes lógicos de la información, todos los programas computacionales, los protocolos técnicos de transmisión y almacenamiento de datos en todas sus capas, y en general todas las infraestructuras lógicas que sustentan las interacciones humanas en el ciberespacio.
(8) Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
(9) Dato informático: toda representación de hechos, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
(10) Delito informático: comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos.
(11) Incidente informático: evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.
(12) Infraestructura crítica de la información: las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

Posteriormente estos conceptos son complementados y ampliados en el marco de la Política Nacional de Ciberseguridad del año 2017, cuando se hace referencia a las fuentes y tipos de riesgos y amenazas en el ciberespacio, que son identificados como[189]:

(1) Incidentes internos: fugas involuntarias de información, interrupción accidental de sistemas informáticos, u otros incidentes involuntarios que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
(2) Desastres naturales o fuerza mayor: terremotos, inundaciones u otros desastres que puedan afectar al ciberespacio, debido a la destrucción de infraestructuras físicas esenciales para la disponibilidad de la información.
(3) Actividades de espionaje y vigilancia llevadas a cabo por actores estatales: conductas que afectan la confidencialidad de la información, mediante su sustracción con fines políticos o estratégicos. En particular, destacan acciones utilizando herramientas sofisticadas conocidas como APT (amenazas avanzadas persistentes), que a su vez pueden valerse de vulnerabilidades informáticas no publicadas de las tecnologías en uso.
(4) Ataques de denegación de servicio y denegación distribuida de servicios (DOS y DDOS): consisten en la sobrecarga intencional de servicios que se proveen en un sistema informático, que puede ser conducida desde un punto de la red o distribuirse para coordinar el ataque desde varios puntos, muchas veces mediante dispositivos infectados con programas maliciosos, con el fin de cumplir dicho propósito.
(5) Cibercrimen: actividades criminales cometidas contra componentes del ciberespacio (acceso no autorizado, sabotaje de información, robo de información, secuestro de información o ransomware o empleando herramientas del ciberespacio como medio de comisión phishing, pharming, fraudes virtuales, y otros relacionados).
(6) Ataques a infraestructuras críticas mediante el ciberespacio: la alteración en el funcionamiento de infraestructuras críticas (físicas o de la información) realizada por medios electrónicos. Por ejemplo: disrupción masiva de sistemas financieros, intervención de servicios básicos, daños físicos a infraestructuras físicas, y otros relacionados.

En síntesis, es posible afirmar que durante desde el período 2014 en adelante se producido un incremento en la conceptualización de términos especializados en materia de ciberseguridad, los cuales requieren de una amplia difusión para la incorporación en el trabajo de las entidades especializadas en el tema, sean públicas, privadas, académicas y de la sociedad civil. Asimismo, es necesario profundizar este esfuerzo, toda vez que lo efectuado a la fecha constituye una aproximación que ha buscado estandarizar nociones mínimas sobre ciberseguridad.

189 Gobierno de Chile, 2017. *Política Nacional de Ciberseguridad*. Disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

1.2. Legislación Especializada

Tal como se indica en la Política Nacional de Ciberseguridad (PNCS) (PNCS, 2017, pp. 30-32), son diversas las normas que regulan los aspectos específicos de la ciberseguridad en Chile. La principal norma es la Constitución Política de la República del año 1980, cuyo contenido presenta artículos específicos que se vinculan con el tema y corresponden a Constitución Política de la República:

(1) Artículo 8º, relativo a la transparencia pública.
(2) Artículo 19º, que contempla un catálogo de derechos fundamentales donde son especialmente relevantes: Nº2, igualdad ante la ley; Nº3 y 7, relativos al debido proceso y seguridad individual; Nº4 y 5, sobre protección de la vida privada e inviolabilidad de las comunicaciones; Nº12, que garantiza la libertad de expresión y de información; y Nº24 y 25, relativos a la propiedad y libertad de creación.
(3) Artículo 24º, que otorga a quien ejerza la Presidncia de la República la autoridad para conservar el orden público en el interior y la seguridad externa de la República, además de las normas que regulan las facultades de otros poderes y órganos del Estado.
(4) Artículo 39º y siguiente, que regulan situaciones específicas que afectan el normal desenvolvimiento del Estado.

Junto a esta norma fundamental, son diversas las leyes que se vinculan con el tema regulan aspectos específicos de la ciberseguridad, a continuación se presentan en forma sistematizada en la tabla 6 y siguientes.

Tabla 6 – Principales Leyes que Abordan Aspectos Específicos sobre Ciberseguridad en Chile

Ley	Contenido
Código Procesal Penal	Se encarga de regular el proceso tanto de investigación como de juicio criminal en Chile. Así entonces, está encargado de realizar cualquier investigación que tenga que ver con ciberdelitos, que sea impulsada al interior del país. Además se ocupa de regular un conjunto de medidas de carácter intrusivo, las cuales pueden afectar la vida privada o la inviolabilidad de las comunicaciones entre sus destinatarios y, por consiguiente, afectar la confidencialidad de la información. Es por ello, que la ley entrega determinadas exigencias a este respecto, además de la necesidad de contar con una resolución específica que autorice el ejercicio de estas medidas.
Ley Nº19.913	Referida a la creación de la unidad de análisis financiero y a la modificación de ciertas disposiciones referidas específicamente al lavado y blanqueo de activos. En ese sentido, se encarga de regular algunas medidas de investigación y de vigilancia, al igual que en el Código Procesal Penal, son capaces de afectar la vida privada y/o la inviolabilidad de las comunicaciones entre sus destinatarios. En consecuencia, se afecta la confidencialidad de la información, por lo que también en este caso se necesita de una resolución de carácter judicial que permita la ejecución de estas prácticas.
D.L. Nº211, Ley de Defensa de la Libre Competencia	Al igual que en el caso anterior, esta ley se encarga de autorizar aquellas prácticas de carácter intrusivo en determinados casos y que se regulan de la misma forma ya señalada.
Ley Nº19.974	Esta ley se refiere al Sistema de Inteligencia del Estado y la creación de la Agencia Nacional de Inteligencia, en el ámbito de la recolección de datos de inteligencia. Dicha ley norma la práctica de los procedimientos de carácter especial acerca de la obtención de información, que para llevarse a cabo necesitan de una orden judicial previamente emitida, además de una serie de otros resguardos legales encargados de limitar la obtención y el uso de dicha información.
Código Penal	Instrumento que tipifica la mayoría de los delitos en el país, además de la descripción de determinadas conductas y las penalidades que traen aparejadas. En el ámbito de la seguridad cibernética, este instrumento señala aquellas conductas que es posible realizar a través del ciberespacio o que puedan afectar sus elementos constitutivos, por lo que posee gran importancia en lo que atañe al diseño de políticas y la lucha contra el cibercrimen.
Código de Justicia Militar	Contiene las disposiciones que dicen relación con delitos perpetrados por militares o durante tiempos de guerra. Así, señala delitos relacionados con el espionaje y la revelación de información con carácter de reservado a terceros y que apunta a la protección de la seguridad a nivel nacional.
Ley Nº19.233	Hace referencia a la tipificación de acciones penales relacionadas a la informática. En el marco de los ciberdelitos, se presenta una subcategoría relacionada a la perturbación de los componentes lógicos del ciberespacio, como por ejemplo programas de computación, sistemas informáticos, bases de datos, entre otros. Dichas perturbaciones se clasifican como delitos informáticos. En esta ley se señalan las acciones penales específicas en contra del acceso no autorizado, sustracción y destrucción de sistemas informáticos.

CONTINUA NA PÁGINA SEGUINTE →

Ley	Contenido
Ley Nº20.009	Referida al Extravío, robo o hurto de tarjetas de crédito y débito.
Ley Nº18.168	Corresponde a la ley general de telecomunicaciones. Se regulan las telecomunicaciones al interior del país, que son aquellas que brindan infraestructuras físicas y lógicas para el desarrollo del ciberespacio a nivel nacional. En su contenido, se hace referencia a la protección, confidencialidad e integridad de la información a través de la tipificación de delitos, como por ejemplo, la interceptación no autorizada, contenido en el artículo Nº36 en sus letras b y c. Junto con lo anterior, se destacan dos modificaciones que atañen a la Ley Nº20.453, acerca del principio de neutralidad en la red para los usuarios y consumidores de internet. Dicho principio regula la gestión de la red que puede utilizar un proveedor de servicios de internet, además de establecer deberes de confidencialidad. En segundo lugar, la Ley Nº20.478 acerca de la recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones, que se materializó posterior al terremoto en Chile durante el año 2010 y que establece medidas que permiten mantener normal desarrollo de las telecomunicaciones a nivel país y, por consiguiente, la disponibilidad de la información contenida en el ciberespacio.
Ley Nº19.799	Se refiere a los documentos y firma electrónica, además de los servicios que certifican tales firmas. En esta ley se regula la utilización de documentos electrónicos al interior del país y, con ello, los mecanismos que aseguran tanto la integridad como la confidencialidad de la información, a través de la utilización de herramientas de firma digital, además de un sistema que asegura el correcto funcionamiento de quienes proveen tales servicios.
Ley Nº20.285	Corresponde a la Ley sobre acceso a la información pública. Aquí se señalan las actividades que debe realizar el Estado para la generación de un régimen de transparencia. El estado posee obligaciones de transparencia activa, que se lleva a cabo a través de la página web de cada organismo público, y de transparencia pasiva, que es aquella que se materializa a través de la solicitud de datos por parte de cualquier persona a dichos organismos, siempre y cuando tal solicitud no afecte otros derechos o intereses que son reconocidos por esta ley.
Ley Nº19.628	Sobre las disposiciones acerca de la protección a la vida privada. En esta ley se señalan los principios y derechos que dicen relación con el manejo de datos de carácter personal al interior del país y que puede exigir el titular de datos personales a quien los administre. Además se establecen reglas de aplicación general para la gestión de datos personales a nivel de sector público y privado, respecto de la confidencialidad de la información.

Fuente: Elaboración propia a partir de la PNCS 2017.

Tabla 7 – Principales Decretos que Abordan Aspectos Específicos sobre Ciberseguridad en Chile

Decreto	Año	Contenido
D.S. Nº83	2005	Sobre las disposiciones técnicas para los órganos de la administración del Estado acerca de la seguridad y confidencialidad de los documentos electrónicos. En este decreto se desarrolla lo establecido por la Ley Nº19.799 donde se fijan las normas técnicas relativas a la administración pública, sobre la seguridad y confidencialidad de los documentos electrónicos, y sus infraestructuras de la información a partir de los estándares señalados en la norma ISO 27.000, y a su vez estableciendo medidas administrativas como la creación de comités de seguridad de las informaciones respecto de cada servicio público. Este decreto es complementado con el D.S. 93 del año 2006, donde se aprueban las normas relativas a la adopción de medidas orientadas a minimizar los efectos de carácter perjudicial que generan mensajes electrónicos masivos no solicitados y que han sido recibidos en las casillas electrónicas de los órganos de la administración del Estado y de sus funcionarios.
D.S. Nº1.299	2004	Se refiere a las disposiciones que se encargan de regular la Red de conectividad del Estado, administrado por parte del Ministerio del Interior, donde se establecen los requerimientos y estándares tecnológicos para la integración a dicha red de instituciones públicas. En este decreto se consolida un recurso de intranet llamado Red de conectividad del Estado, donde podrán conectarse una serie de ministerios y organismos públicos, centralizando así el acceso a internet. Para ello se debe cumplir con determinados estándares técnicos de seguridad que sean acorde a los estándares con tenidos en el IEEE e ISO.
D.S. Nº1	2015	Esta norma de carácter técnico aprueba los sistemas y sitios web de los órganos de la administración del Estado, donde se regulan las condiciones sobre confidencialidad, disponibilidad y acceso a la información contenida en estos sitios, siendo todas indispensables para la seguridad en el ciberespacio.
D.S. Nº533	2015	Establece la creación de un comité de carácter interministerial sobre seguridad cibernética, cuyo objetivo corresponde a la preparación de una propuesta de política nacional sobre ciberseguridad.

Fuente: Elaboración propia a partir de la PNCS (2017).

En síntesis, existe una legislación especializada que aborda el tema de la ciberseguridad en Chile. No obstante, parte de ella requiere actualización debido a que desde la fecha en que fueron creadas hasta la actualidad se han producidos cambios no contemplados en el marco regulatorio hecho en su momento. Asimismo, en los ultimos años se ha hecho un esfuerzo por regular aspectos no abordados previamente en materia de ciberseguridad.

1.3. Arquitectura de Ciberseguridad

En el marco de la Política Nacional de Ciberseguridad (PNCS), es posible identificar las instituciones que intervienen en ciberseguridad en Chile[190] son las cuales son indicadas en forma sistematizada en la tabla 8.

190 Gobierno de Chile, 2017. *Política Nacional de Ciberseguridad*. Disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Tabla 8 – Instituciones que Intervienen en Ciberseguridad en Chile

Institución	Entidad	Rol	Misión
Ministerio del Interior y Seguridad Pública	Subsecretaría del Interior	- Preventivo - Formulador de Política Pública	- La misión del Ministerio tiene está referida con el resguardo de la seguridad pública al interior del país. En ese sentido, se encarga de coordinar, evaluar y controlar la ejecución de los planes de carácter intersectorial relacionados con la prevención y el control de la delincuencia, de acuerdo con el Artículo 1 de la Ley Nº20.502. Entre ellos podemos encontrar los que se refieren a ciberdelitos, por lo que se establecen políticas públicas que buscan prevenirlos, enfrentarlos y sancionarlos. El responsable de generar estrategias para el combate al cibercrimen corresponde al Departamento de crimen organizado.
	Subsecretaría del Interior	- Preventivo - Reactivo - Formulador de política pública	- A partir del D.S. Nº5996 del año 1999, el Ministerio del Interior y Seguridad Pública se encarga de implementar y operar, por medio de la división de Informática, la Red de Conectividad del Estado (RCE). En adición a este decreto, el D.S. Nº1299 del año 2004, permite a esta institución la publicación de las normas oficiales de la República sobre temas relativos a la seguridad de la información y el establecimiento de normas, políticas y estándares de seguridad lógica que obligatoriamente tendrán que cumplir los órganos públicos que participan de la RCE (que constituye una herramienta de apoyo a la ciberseguridad gubernamental), la que está habilitada para consultar sobre materias técnicas a cualquier institución del Estado. Además la RCE junto con "proveer una red confiable y segura para las comunicaciones del Estado, en la cual todos los Ministerios y Servicios Públicos podrán comunicarse entre ellos y tener acceso a internet, su coordinación, administración y supervisión corresponden a la División de Informática del Ministerio del Interior y Seguridad Pública"[191], siendo de este modo el CSIRT chileno.
	Policía de Investigaciones (PDI): Brigada Investigadora del Cibercrimen	- Preventivo - Investigativo	- Se encarga de investigar los ilícitos de acuerdo a las disposiciones del Ministerio Público, en este caso los ciberdelitos.
	Carabineros: Departamento OS 9	- Preventivo - Investigativo	- Se encargan del orden y seguridad pública. La alteración de estos se debe prevenir e investigar, como los ciberdelitos, por ejemplo.
	Agencia Nacional de Inteligencia	- Preventivo	- A partir de la Ley 19.974 que se encarga de regular su funcionamiento, se encarga de proponer normas y procedimientos de protección relacionados con los sistemas de información crítica del Estado.

191 "Misión RCE". Gobierno de Chile. Disponible en https://www.csirt.gob.cl/mision_rce.html.

Institución	Entidad	Rol	Misión
Ministerio de Defensa Nacional	Subsecretaría de Defensa	- Formulador de política	- Esta institución se encarga de crear y mantener actualizada la planificación de carácter primario y las políticas necesarias para enfrentar los diversos desafíos que la ciberseguridad presenta a la Defensa a nivel nacional, además de asegurar la correspondencia entre ésta y la planificación secundaria.
	Estado Mayor Conjunto y Fuerzas Armadas (FFAA)	- Preventivo - Reactivo	- Las FFAA están a cargo de resguardar su infraestructura de la información, además de ayudar en las tareas referentes a la ciberseguridad que se relacionen con la seguridad nacional y el sistema nacional de inteligencia. - El Estado Mayor Conjunto, es la institución encargada del trabajo y asesoría permanente del Ministro de Defensa Nacional, en relación a aquellos temas sobre la preparación y utilización de las Fuerzas Armadas. También está a cargo de la elaboración y mantenimiento de la actualización de la planificación secundaria de la Defensa, así como también de otros quehaceres atingentes a la seguridad cibernética del país. - Las FFAA se encargan de los planes institucionales y operativos correspondientes, a partir de la planificación realizada.
Ministerio de Transportes y Telecomunica-ciones	Subsecretaría de Telecomunica-ciones	- Preventivo - Formulador de políticas públicas	- Está a cargo de la implementación de la Ley 20.478, relativa a la recuperación y continuidad del sistema público de telecomunicaciones en situaciones de emergencia y condiciones críticas. Lo anterior se materializa a través del decreto N°60 del año 2012, el cual establece el Reglamento para la interoperabilidad y difusión de mensajería de alerta, así como también de la declaración y protección de la infraestructura crítica de telecomunicaciones e información relativa a las fallas de carácter significativo en los sistemas de telecomunicación. Junto con lo anterior, esta institución está encargada de la fiscalización del respeto al principio de neutralidad de la red contenido en la Ley 20.453.
Ministerio de Economía, Fomento y Turismo		- Formulador de política pública.	- Este ministerio se encarga de promover la competencia y modernización a nivel de estructura productiva del país, iniciativa privada y la acción eficiente de los mercados. Junto con lo anterior, se encarga de la innovación y la consolidación de la inserción a nivel internacional de la economía nacional. Es por ello que la ciberseguridad es un elemento de desarrollo nacional que se considera en la Agenda de Productividad, Innovación y Crecimiento.
Ministerio de Justicia y Derechos Humanos		- Formulador de política pública - Modernizador del sistema de Justicia.	- Se encarga de la promoción de normas y políticas públicas destinadas a facilitar el acceso y protección de los derechos fundamentales de las personas junto con su seguridad. En ese sentido, esta institución se encarga de la constante actualización y ajuste de las leyes a partir de los desafíos que establece el desarrollo tecnológico.

CONTINUA NA PÁGINA SEGUINTE →

Institución	Entidad	Rol	Misión
Ministerio de Relaciones Exteriores	Dirección de Seguridad Internacional y Humana (DISIN)	- Articulador en la comunidad internacional - Coordinador internacional de la política de ciberseguridad.	- Se encarga de identificar, coordinar y promover tanto la posición como los intereses del país ante la comunidad internacional en relación a la seguridad cibernética. A su vez se encarga de coordinar y promover la participación del país en organismos y foros especializados de carácter internacional, como por ejemplo Meridian, Octopus, OEA, UNASUR, UIT, IGF, grupos expertos de la ONU, entre otros. Junto con lo anterior, fomenta las relaciones bilaterales en este tema.
Ministerio Secretaría General de la Presidencia	Unidad de Modernización del Estado	- Formulador de política - Desarrollo Digital.	- Tiene como misión acercar el Estado a las personas, y en ese marco se encarga de desarrollar la modernización del estado y el Gobierno digital.
	NIC Chile	- Órgano técnico. - Administrador.	- Esta organización se encarga de la administración del registro de nombres de dominio.CL, además de manipular la tecnología que permite a dichos nombres funcionar de forma segura y eficiente, para que de esta forma las personas, instituciones y empresas puedan identificarse en internet.
	CLCert	- Órgano académico, punto de contacto con CERT internacionales y con FIRST.	- Los principales objetivos de esta entidad corresponden a: a) entregar en forma oportuna y sistemática la información respecto a vulnerabilidades de seguridad y amenazas. b) difundir y poner a disposición de la comunidad aquella información que permita prevenir y resolver los incidentes que afectan a la seguridad. c) Educar a las personas en general sobre temas de seguridad, a partir de la promoción de políticas que permiten su implementación.
Instituto Nacional de Normalización		- Órgano técnico - Normalizador de estándares - Acreditador	- Es un organismo de carácter técnico en temas sobre Infraestructura de la calidad, que en el marco de la ciberseguridad se relacionan con las normas ISO/IEC 27000.
Ministerio Público		- Dirigir la persecución penal. - Ejercer la acción penal pública.	- Organismo autónomo que se encarga de dirigir la investigación de delitos, así como también llevar a los imputados a los tribunales y en caso de proceder, entregar protección a las víctimas y a los testigos.
Poder Judicial		- Conocer, resolver y hacer cumplir lo juzgado en causas civiles y penales.	- En el ámbito de la ciberseguridad, los jueces pueden autorizar diligencias de carácter intrusivo, además de controlar la legalidad de la investigación penal y decidir de las causas penales, lo que incluye a los ciberdelitos.

Fuente: Política Nacional de Ciberseguridad (2017b)

1.3.1. Los Principales Organismos Técnicos

RCE: el cual se encarga de la "publicación de las normas oficiales de la República sobre temas relativos a la seguridad de la información y el establecimiento de normas, políticas y estándares de seguridad lógica que obligatoriamente tendrán que cumplir los órganos públicos que participan de la RCE (que constituye una herramienta de apoyo a la ciberseguridad gubernamental), la que está habilitada para consultar sobre materias técnicas a cualquier institución del Estado" (PNCS, 2017), junto con "proveer una red confiable y segura para las comunicaciones del Estado, en la cual todos los Ministerios y Servicios Públicos podrán comunicarse entre ellos y tener acceso a internet, su coordinación, administración y supervisión corresponden a la División de Informática del Ministerio del Interior y Seguridad Pública"[192], siendo de este modo el CSIRT chileno.

CLCERT (de carácter académico) – "grupo dedicado al monitoreo y análisis de los problemas de seguridad de los sistemas computacionales en Chile, y a la generación tanto del conocimiento como el recurso humano especializado para asegurar dichos sistemas."(CLCERT, 2017).

NIC Chile – instituição dedicada ao registo de domínios na internet (NIC Chile, 2017).

En síntesis, son diferentes las instituciones públicas con atribuciones y competencia en aspectos específicos vinculados al tema de la ciberseguridad. En este contexto, la coordinación interagencial es clave y una manera de facilitarlo es con un leguaje compartido, que se facilita por medio de una aproximación conceptual unificada. Sin embargo, está pendiente la creación de una institucionalidad que centralice las principales responsabilidades en la materia y constituye un desafío contemplado en la PNCS 2017.

1.4. Cooperación Internacional

Debido a que ningún país por si solo puede lograr niveles mínimos de ciberseguridad sin contemplar la ayuda internacional ante incidentes transnacionales en el ciberespacio. En este contexto, Chile no es la excepción. En efecto, la cooperación internacional en ciberseguridad es un tema que se ha analizado desde el año 2009, fecha en que se crea la "Comisión de Trabajo Interministerial Conducente a la Adhesión de Chile a la Convención sobre Ciberdelitos del Consejo de Europa", decisión evaluada en forma positiva por el gobierno y recientemente en 2017 luego de una serie de consultas a diferentes instituciones del Estado se ha decidido suscribir este Convenio internacional.

La relevancia que adquiere la cooperación internacional en materia de ciberseguridad explica la decisión de considerar la formulación de una como una "Política internacional para el ciberespacio" como componente de las "Políticas integradas complementarias en materia digital" junto a la "Agenda Digital 2020" y la "Política nacional de ciberdefensa". En este sentido, la "Política internacional para el ciberespacio" se orienta la elaboración de una estrategia sobre el tema por parte del Ministerio de Relaciones Exteriores que contemple una "visión país sobre la gobernanza de internet". Asimismo, en la PNCS 2017 son incorporadas varias metas relacionadas con este tema y corresponden a:

192 "Misión RCE". Gobierno de Chile. Disponible en https://www.csirt.gob.cl/mision_rce.html.

(1) Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región.
(2) Avanzar en el establecimiento de mecanismos bilaterales de trabajo, diseñando agendas e implementando instancias de consultas políticas transversales con países afines.
(3) Elaborar un documento de política internacional de Chile sobre el ciberespacio y ciberseguridad.
(4) Establecimiento de un grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio.
(5) Propiciar el intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas.
(6) Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales.
(7) Adherir e implementar la Convención sobre Ciberdelitos del Consejo de Europa.
(8) Apoyar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando posibilidades de apoyo.

Junto a lo indicado, Chile participa en diferentes instancias internacionales que abordan el tema de la ciberseguridad. A nivel mundial está presente en Nacionales Unidas, donde asiste a las reuniones que se efectúan en UNODC y la UIT. A nivel hemisférico está presente en la OEA y participa en las reuniones del REMJA y el CICTE. Especial referencia tiene esta última entidad e la cual Chile preside durante el período 2016 – 2017, desde promovió la XVI Declaración CICTE denominada "Fortalecimiento de la Cooperación y del Desarrollo en la Seguridad Cibernética y la Lucha contra el Terrorismo en las Américas". Asimismo, colabora en las diversas encuestas, cuestionarios y estudios que son efectuados en el marco de los organismos multilaterales indicados.

Otra instancia multilateral en la que Chile participa que ha incorporado el tema de la ciberdefensa y con ello implícitamente el tema de la ciberseguridad es la Unión de Naciones Suramericanas (UNASUR) a través de su entidad especializada el Centro de Estudios Estratégicos de Defensa (CEED) que actúa según los mandatos que emanan del Consejo de Defensa Suramericano (CDS). En efecto, en el Plan de Trabajo 2017 se contempla el tema de la ciberdefensa como línea de investigación.

También la participación internacional de Chile en materia de Ciberseguridad, contempla la asistencia a foros especializados sobre el tema como la Conferencia Global del Ciberespacio y la Conferencia de Meridian, con la finalidad de ser parte del debate global en los diversos temas relacionados con el ciberespacio y su seguridad. Asimismo, Chile ha sido sede de capacitación internacional sobre el Manual Tallin, organizado por la OEA.

De esta manera, es posible afirmar que la participación internacional de Chile en materias de ciberseguridad es formal y principalmente a nivel multilateral, efectuándose a través de diferentes instancias que existen actualmente en materia de ciberseguridad:

organismos gubernamentales multilaterales (OEA; ONU y organismos especializados de estas), foros específicos sobre la materia CGCS y Conferencia de Meridian, como también, suscribiendo tratado internacionales y capacitándose en la aplicación del derecho internacional en el ciberespacio.

En síntesis, se participa en diferentes instancias internacionales en materia de ciberseguridad, las cuales son de variada naturaleza, como por ejemplo: organismos multilaterales, foros, convenciones, encuentros entre otros. De esta manera, es posible conocer los estándares internacionales en los distintos temas relacionados con la ciberseguridad. Asimismo, es una oportunidad para compartir nuestra experiencia en el tema, conocer las lecciones aprendidas de quienes tienen mayor trayectoria y apoyar a quienes se inician en el camino. Además, esta participación múltiple permite promover nuestros intereses en el tema y construir alianzas que permitan defenderlos. Constituye un desafío dar continuidad a esta participación y poder liderar aquellas materias que consideramos claves en el tema de ciberseguridad.

1.5. Cultura de Ciberseguridad

La seguridad en el ciberespacio es un tema reciente como problema y desafíos que se enfrentan los países y su incorporación como asunto en la agenda pública de los gobiernos es tema de los últimos años. En este contexto, el estudio de la ciberseguridad por parte de la población es escaso. Se han encontrado como el problema en la medida que han sido usuarios vulnerables de sistemas virtuales. El caso de Chile no es la excepción. La mayor parte de la población no cuenta con formación mínima de hábitos saludables en el uso del ciberespacio y las principales aplicaciones que ofrece. En este contexto y como manera de responder a la necesidad de que las personas sean responsables cunado hacen uso del ciberespacio y muy especialmente internet, instituciones publicas han promovido campañas de concientización en la población sobre riesgos en el ciberespacio y modo de prevenirlo. En este sentido, tanto la Subsecretaría del Interior junto a otras entidades, se han encargado de informar a la población por medio de su página web de prácticas recomendadas como seguras al hacer uso del ciberespacio. Por ejemplo, se ha desarrollado una campaña de prevención de clonación de tarjetas, indicando de que se trata este ilícito y como puede evitarse. También la página institucional de la Policía de Investigaciones de Chile (PDI), cuenta con el link cibercrimen donde se dan indicaciones mínimas de seguridad para evitar ser víctima de tradicionales delitos en el ciberespacio como robo de claves. Asimismo, Carabineros de Chile en el marco del Programa "Internet Segura.cl".

Especial referencia merece la campaña "Decálogo por una Ciudadanía Digital e Internet Segura" en la cual participan entidades públicas y privadas (Subsecretaría de Telecomunicaciones, Ministerio de Educación, Carabineros de Chile y Asociación de telefonía móvil) y apoyadas por la Subsecretaría del Interior, busca que las personas internalicen 10 medidas que permiten una navegación más segura, las cuales se indican en la figura Nº 11.

Figura 10 – Campaña Ciudadanía Digital e Internet Segura

Fuente: Ministerio del Interior y Seguridad Pública de Chile (2017).

En efecto, ha sido el incremento del cibercrimen uno de los principales estímulos en la preocupación de las instituciones públicas y privadas relacionadas con el tema, para promover una cultura de ciberseguridad por parte los usuarios para evitar algunos delitos como el fraude, acoso sexual o en gaño a través del ciberespacio. Ello ha llevado a trabajos conjuntos entre organizaciones públicas y del sistema financiero para informar a los ciudadanos de este tipo de ilícitos.

El estudio de este tema en colegios y universidades es escaso y depende de la voluntad de sus autoridades, pues no existe obligación en los currículos y hay carencia de suficientes especialistas de la materia para contar con un experto en cada centro educacional.

Una mayor antigüedad en el estudio de la materia se encuentra en los centros de estudios superiores que enseñan informática, donde se aborda el tema de la programación y los riesgos y vulnerabilidades en el desarrollo de procesos y sistemas informáticos y de software. Estos especialistas son escasos según la necesidad de estos profesionales, existiendo una alta demanda por este tipo de expertos.

A nivel universitario, en facultades de ingeniería y derecho se ha impulsado el estudio de la ciberseguridad, cada uno en su propio ámbito de conocimiento. En este contexto, por ejemplo la Universidad de Chile en el departamento de Ciencias de la Computación de la facultad de Ingeniería, cuenta desde hace varios años con una línea de formación en seguridad informática en el marco del cual se realizan cursos sobre seguridad cibernética. A contar de este año la facultad de Derecho de la misma Universidad imparte un Diploma de postítulo en Ciberseguridad y Ciberdefensa. Por su parte, la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) desde hace 5 años aborda el tema de la ciberseguridad en el marco de la cátedra de inteligencia, asignando horas de clases para abordar el tema en los diferentes programas académicos que son realizados (pregrado, post-

grado, postitulo y Diplomado), contemplando en 2018 impartir un Diplomado en Ciberseguridad. De esta manera, es posible constatar que aun cuando una formación estructurada en el tema es reciente, cada vez se incrementan las instancias para promover una cultura de ciberseguridad.

En el marco de la PNCS se han contemplado varias metas que permiten avanzar en este tema. En efecto, se trata de 15 metas de un total de 41, es decir, un 36 % de ellas contribuye a la promoción de una cultura de ciberseguridad y corresponden a:

(1) Generar primer punto de difusión de información para el ciudadano sobre Ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet.
(2) Instaurar el mes de la Ciberseguridad en octubre de cada año, promoviendo y consolidando actividades de sensibilización en todos los niveles. Además, en Febrero participar en el día internet segura.
(3) Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género.
(4) Generar guías de buenas prácticas para la ciudadanía y el sector público.
(5) Conformar una mesa intersectorial para fomentar la formación en ciberseguridad en todos los niveles y estamentos del sector educativo.
(6) Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión.
(7) Incorporación de Seguridad en Internet en programas específicos de MINEDUC, reforzando la iniciativa ENLACES.
(8) Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras)
(9) Actualizar DTO 5996 y DS 1299 en coherencia con modificación del DS 83, estableciendo requisitos para acceder a la red (autoevaluación, curso online) y la obligación de reportar incidentes por parte de organismos públicos.
(10) Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales.
(11) Incorporar estándares de ciberseguridad a los proveedores del Estado, exigiendo requisitos específicos para proveedores TIC, y analizando otros para el resto de los proveedores.
(12) Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos.
(13) Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales
(14) Fomentar el patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad.

(15) Promover el desarrollo de capital humano avanzado en asuntos de Ciberseguridad en los distintos ámbitos técnico-profesionales.

En el caso chileno, el incremento en el uso del ciberespacio se constata por ejemplo en "los accesos a internet han crecido en un 45,3%, en el último bienio, pasando de 52,2 accesos por cada 100 habitantes a inicios de 2014, a 73,8 accesos por cada 100 habitantes en marzo de 2016. La economía digital nacional, en tanto, creció en torno al 11% en el último bienio, pasando de 34.127 millones de dólares en 2014 a 39.485 millones de dólares en 2015"[193]. En este contexto, adquiere relevancia la promoción de una cultura de ciberseguridad que desde una perspectiva histórica en el caso nacional ha sido un tema de especialistas y se ha abordado en instancias específicas entre expertos. No obstante, el incremento en el uso del ciberespacio y la necesidad que ello entre confianza en su seguridad, ha estimulado la generación de una masificación de la cultura de ciberseguridad, es decir, que los actores involucrados en el uso de ciberespacio entiendan y hagan como propias prácticas que permitan no exponer datos que gestionan en el ciberespacio.

De esta manera, la promoción de una cultura de ciberseguridad cobra creciente importancia en Chile, observándose la incorporación del tema en la agenda pública a nivel de ciudadanía, sector privado, sector público y academia. Ejemplo de ello puede encontrarse en diversas medidas contempladas en la PNCS 2017 que están orientadas a los diversos actores involucrados en el tema. En efecto, se convierte en condición necesaria más no suficiente para que el uso del ciberespacio no sólo sea conveniente sino también confiable para los ciudadanos, organizaciones, empresas e instituciones públicas con respecto al funcionamiento de éste, como asimismo, el resguardo de los datos e información generados, almacenados y transmitidos. En este contexto, la prevención, alerta y gestión de incidentes es responsabilidad tanto de quienes proveen servicios en este ambiente, los que fiscalizan su funcionamiento, como también de los usuarios, siendo imperiosa la formación y capacitación de ellos en este tema, promoviendo de este modo una creciente cultura de ciberseguridad. Explicándose de este modo la incorporación del tema en la PNCS 2017 y en las prácticas promovidas por el gobierno durante este período a través de diversas campañas de sensibilización según se ha indicado.

En síntesis, debido al incremento en el uso del ciberespacio y el aumento en la cantidad de usuarios en internet hay mayor vulnerabilidad a que las personas sean víctimas de ilícitos en el ciberespacio. Para prevenirlos, existen diversas buenas prácticas que es necesario sean adoptadas en la ciudadanía junto con una mayor sensibilización de los peligros a los que pueden estar expuestas las personas al usar el ciberespacio. Por este motivo, diferentes acciones orientadas a sensibilizar y capacitar se han desarrollado por parte de la autoridad a distintos públicos objetivos, las cuales también tienen una proyección futura según se indica en la PNCS. Constituye un desafío mantener, profundizar y adaptar este esfuerzo a las nuevas necesidades que se vayan detectando en términos de enseñar a un buen uso del ciberespacio y difundir los peligros a los que están expuestas las personas.

193 Bachelet, M., 2017. *Política Nacional de Ciberseguridad*. Gobierno de Chile. Disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

1.6. Política Pública en Ciberseguridad

La Política Nacional de Ciberseguridad (PNCS), principal documento sobre el tema, establece "los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2023, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente". Esta política se fundamente en la necesidad de resguardar la seguridad de las personas en el ciberespacio; proteger la seguridad del país y; gestionar los riesgos del ciberespacio. La PNCS chilena tiene dos ejes principales: "una política de Estado, diseñada con objetivos orientados al año 2022, y una agenda de medidas específicas, que serán implementadas entre los años 2017 y 2018", en la tabla 9 se indican tanto los objetivos como las metas asociadas.

Tabla 9 – Objetivos y Metas de la PNCS Chilena

Objetivos de política para el 2022	Medidas de política pública para 2017 – 2018 asociada	Entidades involucradas[194]
El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.	(1) Preparar y enviar al Congreso Nacional un proyecto de Ley sobre ciberseguridad, para consolidar institucionalidad y manejo de incidentes de seguridad informática en el país. (2) Actualizar el DS 83 sobre seguridad de la información del Estado, con miras a la adopción de estándares renovados y a un modelo de control de su cumplimiento efectivo. (3) Añadir una dimensión de ciberseguridad a la preparación y gestión de contratos de concesión de obra pública. (4) Creación de un grupo de trabajo que establezca un marco normativo y de obligaciones para las infraestructuras críticas en Chile, desde un enfoque de gestión de riesgos. (5) Creación de una norma técnica para el desarrollo o contratación de software en el Estado, acorde a estándares de desarrollo seguro. (6) Creación de una plataforma para agregar información sobre incidentes de ciberseguridad. (7) Decretar coordinadamente requisitos actualizados de seguridad para sectores económicos regulados. (8) Identificar un set mínimo de riesgos para las infraestructuras críticas de la información. (9) Implementar una matriz estandarizada para reportes de incidencias en materia de ciberseguridad. (10) Incorporar la dimensión de ciberseguridad en el sistema nacional de emergencias. (11) Preparación de normativa que establezca mecanismos seguros de intercambio de información en el Gobierno, entre autoridades de alto nivel y otros funcionarios que manejen información reservada o secreta.	-MISP -MINDEF -MINHACIENDA (CICS supervisor de la medida, Dirección Chilecompra) -MINSEGPRES -MOP (Dirección de concesiones) -CSIRT -MTT -Superintendencias -ANI -MINREL -MINECON

CONTINUA NA PÁGINA SEGUINTE →

194 Las siglas utilizadas en el cuadro corresponden a: CSIRT: equipo de seguridad de la Red de Conectividad del Estado; CICS: Comité Interministerial sobre Ciberseguridad; MISP: Ministerio del Interior y Seguridad Pública; MTT: Ministerio de Transportes y Telecomunicaciones; MINDEF: Ministerio de Defensa Nacional; MINHACIENDA: Ministerio de Hacienda; ANI: Agencia Nacional de Inteligencia; MINJUSTICIA: Ministerio de Justicia y Derechos Humanos; MINSEGPRES: Ministerio Secretaría General de la Presidencia; MOP: Ministerio de Obras Públicas; MINEDUC: Ministerio de Educación; MINREL: Ministerio de Relaciones Exteriores; MSGG: Ministerio Secretaria General de Gobierno; MINECON: Ministerio de Economía, Fomento y Turismo.

Objetivos de política para el 2022	Medidas de política pública para 2017 – 2018 asociada	Entidades involucradas[194]
	(12) Preparación de un estudio sobre la resiliencia de las redes de telecomunicaciones en Chile, proponiendo medidas para mejorar la misma en el ámbito público y privado. (13) Tramitar nueva ley de datos personales, con facultades a un órgano específico que pueda imponer requisitos de seguridad y de notificación de filtraciones de datos. (14) Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras) (15) Actualizar DTO 5996 y DS 1299 en coherencia con modificación del DS 83, estableciendo requisitos para acceder a la red (autoevaluación, curso online) y la obligación de reportar incidentes por parte de organismos públicos. (16) Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales. (17) Incorporar estándares de ciberseguridad a los proveedores del Estado, exigiendo requisitos específicos para proveedores TIC, y analizando otros para el resto de los proveedores.	
El Estado velará por los derechos de las personas en el ciberespacio.	(1) Actualizar normativa sobre delitos informáticos. (2) Diseñar e implementar una matriz estandarizada de denuncias de ciberdelitos. (3) Promover el fortalecimiento de las capacidades de investigación y análisis forense relacionadas con el ciberdelito. (4) Tramitar nueva ley de datos personales, con facultades a un órgano específico que pueda imponer requisitos de seguridad y de notificación de filtraciones de datos. (5) Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras) (6) Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos. (7) Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales. (8) Adherir e implementar la Convención sobre Ciberdelitos del Consejo de Europa.	-MISP (con policías y ANI) -MINJUSTICIA -MINREL -CICS -MINISTERIO PÚBLICO
Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.	(1) Generar primer punto de difusión de información para el ciudadano sobre Ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet. (2) Instaurar el mes de la Ciberseguridad en octubre de cada año, promoviendo y consolidando actividades de sensibilización en todos los niveles. Además, de en Febrero participar en el día internet segura. (3) Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género. (4) Generar guías de buenas prácticas para la ciudadanía y el sector público. (5) Conformar una mesa intersectorial para fomentar la formación en ciberseguridad en todos los niveles y estamentos del sector educativo.	

Objetivos de política para el 2022	Medidas de política pública para 2017 – 2018 asociada	Entidades involucradas[194]
	(6) Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión. (7) Incorporación de Seguridad en internet en programas específicos de MINEDUC, reforzando la iniciativa ENLACES. (8) Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras) (9) Actualizar DTO 5996 y DS 1299 en coherencia con modificación del DS 83, estableciendo requisitos para acceder a la red (autoevaluación, curso online) y la obligación de reportar incidentes por parte de organismos públicos. (10) Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales. (11) Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos. (12) Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales. (13) Fomentar el patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad. (14) Promover el desarrollo de capital humano avanzado en asuntos de Ciberseguridad en los distintos ámbitos técnico-profesionales.	-MISP -MSGG (CICS supervisor de la medida) -CICS -MINEDUC -MINECON (Mesa Capital Humano) -MDS (Senama) -CSIRT -MINREL -CORFO -Actores del mundo público, privado y académico.
El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.	(1) Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región. (2) Avanzar en el establecimiento de mecanismos bilaterales de trabajo, diseñando agendas e implementando instancias de consultas políticas transversales con países afines. (3) Elaborar un documento de política internacional de Chile sobre el ciberespacio y ciberseguridad. (4) Establecimiento de un grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio. (5) Propiciar el intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas. (6) Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales. (7) Apoyar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando posibilidades de apoyo.	-MINREL -MISP -MINJUSTICIA -MINISTERIO PÚBLICO -MINECON

CONTINUA NA PÁGINA SEGUINTE →

Objetivos de política para el 2022	Medidas de política pública para 2017 – 2018 asociada	Entidades involucradas[194]
El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.	(1) Analizar la regulación y aplicación del régimen vigente de compras públicas respecto a apoyo productivo e intereses nacionales estratégicos. (2) Realizar estudios tanto de caracterización de la industria de ciberseguridad (oferta), como de acceso y uso de ciberseguridad en el país (demanda), con el objeto de orientar programas especiales para impulsar la industria de ciberseguridad nacional, en sectores definidos. (3) Estudio de incentivos tributarios, subsidios o mecanismos de I+D+i para desarrollo y adopción de estándares de ciberseguridad. (4) Incorporar estándares de ciberseguridad a los proveedores del Estado, exigiendo requisitos específicos para proveedores TIC, y analizando otros para el resto de los proveedores. Medida Nº39 (5) Fomentar el patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad. (6) Promover el desarrollo de capital humano avanzado en asuntos de Ciberseguridad en los distintos ámbitos técnico-profesionales. (7) Apoyar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando posibilidades de apoyo.	-MINHACIENDA (Dirección Chilecompra) -MISP -MINDEF -CORFO -CICS -MINECON (Mesa de capital humano) -MINREL (Prochile)

Fuente: Política Nacional de Ciberseguridad (2017b).

1.6.1. Políticas Integradas Complementarias en Materia Digital

La PNCS se complementa con otras políticas públicas en desarrollo, las cuales corresponden a:

(1) Agenda Digital 2020: La Agenda Digital 2020 orienta el avance hacia el desarrollo digital del país, a través de la definición de objetivos de mediano plazo, líneas de acción y medidas concretas. Presentada el segundo semestre del año 2015, busca que el uso masivo de las tecnologías se convierta en un mecanismo para disminuir las desigualdades, facilitando la apertura de más y mejores oportunidades de desarrollo, y apoyar al respeto de los derechos de toda la ciudadanía. En la Agenda existe una medida específica (Nº25) que apunta a la elaboración de una estrategia de ciberseguridad, la cual se conecta con la PNCS.

(2) Asimismo, diversas medidas de la Agenda potencian y complementan la PNCS, entre las que destacan el impulso otorgado a una nueva Ley de Protección de datos personales, el resguardo a los derechos de los consumidores en internet, el desarrollo de un Plan Nacional de Infraestructura de Telecomunicaciones, el perfeccionamiento de la normativa sobre firma electrónica, entre otras.

(3) Política Nacional de Ciberdefensa: Debido a que las redes y sistemas de información de la Defensa Nacional componen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía del país, junto a las atribuciones constitucionales y legales de la Defensa Nacional, constituyen los antecedentes que justifican la elaboración por parte del Ministerio de Defensa Nacional, durante el

año 2017 de políticas específicas de ciberdefensa, que contemplen las definiciones políticas respecto a la protección de las redes, y la forma en que las capacidades de la Defensa Nacional colaborarían en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país.

(4) Política Internacional para el Ciberespacio: Uno de los objetivos de alto nivel de la PNCS se vincula con con la cooperación y relaciones internacionales en torno a la ciberseguridad en un ambiente de globalización. No obstante, resulta fundamental que estos objetivos sean conectados con otros tales como el desarrollo, los derechos humanos, la defensa y otros relacionados, para consolidarlos e integrarlos en la política exterior chilena. Por este motivo, la PNCS contempla una medida específica relacionada con la formulación de una estrategia en estos temas por p del Ministerio de Relaciones Exteriores. Ello es consistente y da inicio la ejecución de la medida Nº11 de la Agenda Digital 2020, referida a generar una visión país sobre gobernanza de internet.

De esta manera, es posible constar la concatenación de tres políticas diferentes pero vinculadas entre si y con objetivos que desde diferentes ámbitos de competencia y acción se refuerza, complementan y potencian, en el marco de una voluntad única del Estado tendiente a contar con niveles de ciberseguridad según estándares internacionales que permitan el respecto a los derechos de las personas y el desarrollo del país, sus ciudadanos, organizaciones y empresas.

En síntesis, existe una política de ciberseguridad recientemente formulada cuyo principal desafíos es tanto dar cumplimiento a las metas propuestas, como dar continuidad en el mediano y largo plazo al esfuerzo que se ha realizado, considerando un enfoque supra-partidario en el tema.

2. Caso de Portugal

A arquitetura de segurança cibernética em Portugal decorre de um conjunto de capacidades públicas e privadas, nacionais e de parceiros internacionais no âmbito de relações multilaterais (ONU, UE e NATO) e de bilaterais com outros Estados e empresas multinacionais, e do respetivo enquadramento normativo.

2.1. Aproximação Conceptual

Em Portugal, existem diversos glossários de termos técnicos e científicos utilizados nos domínios das TIC e do ciberespaço compilados e disponibilizados por instituições públicas e organizações não-governamentais de interesse público através da web, tais como:

(1) Centro Nacional de Cibersegurança (CNCS);
(2) Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI);
(3) AFCEA Portugal (2013).

Todavia, a *Lei do Cibercrime* apresenta um conjunto de definições para o seu âmbito de aplicação e que mimetizam a Convenção de Budapeste.

Tabela 10 – Conceitos Empregues na *Lei do Cibercrime*

Sistema informático	Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;
Dados informáticos	Qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;
Dados de tráfego	Os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;
Fornecedor de serviço	Qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;
Interceção	O acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;
Topografia	Uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;
Produto semicondutor	A forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.
Ciberespaço	O ciberespaço transpõe a vida real para um mundo virtual, com características únicas que impõem novas formas de interação e de relacionamento.

Fonte: Adaptado de Assembleia da República (2009).

2.2. Legislação Especializada

2.2.1. Conceito Estratégico de Defesa Nacional

O *Conceito Estratégico de Defesa Nacional 2013* (Governo de Portugal, 2013) refere-se aos potenciais efeitos dos ataques cibernéticos e identifica: o ciberterrorismo e a cibercriminalidade como "ameaças e riscos prioritários", que podem afetar as infraestruturas críticas e estruturas tecnológicas que suportam a organização social e económica nacional; a criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN); e o levantamento da capacidade de ciberdefesa nacional.

2.2.2. Lei do Cibercrime

A *Lei n.º 109/2009*, de 15 de Setembro, aprova a *Lei do Cibercrime*, transpondo para a ordem jurídica interna a *Decisão Quadro n.º 2005/222/JAI*, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à *Convenção sobre Cibercrime do Conselho da Europa*.

2.2.3. Estratégia Nacional de Combate ao Terrorismo

A *Estratégia Nacional de Combate ao Terrorismo* (PCM, 2015a) tem como pressuposto o "(…) compromisso de combate ao terrorismo em todas as suas manifestações, e tem como objetivos estratégicos: detetar, prevenir, proteger, perseguir e responder". As linhas de ação associadas a cada objetivo estratégico enunciam um conjunto de iniciativas extremamente relevantes para os domínios da cibersegurança, ciberdefesa e áreas conexas que importa realçar, nomeadamente:

(1) Partilha da informação entre as forças e serviços de segurança ou outras entidades, no âmbito das respetivas competências, ao nível nacional, europeu e internacional;
(2) Consciencialização dos operadores públicos e privados quanto à natureza crítica da segurança informática;
(3) Cooperação entre todos os setores da sociedade civil quanto à radicalização e recrutamento para o terrorismo;
(4) Remoção ou bloqueio de conteúdos de apologia da violência e do terrorismo acessíveis na internet;
(5) Identificação de infraestruturas críticas, em todos os setores de atividade económica e social e desenvolvimento do "Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas";
(6) Implementação do "Plano de Ação Nacional para a Proteção contra as Ciberameaças";
(7) Avaliação periódica das vulnerabilidades das infraestruturas essenciais, nacionais e europeias, para transportes e energia;
(8) Avaliação das vulnerabilidades dos sistemas de informação críticos e acompanhamento das medidas de correção adotadas face a ciberataques;
(9) Reforço da colaboração e articulação entre os vários intervenientes e responsáveis nas áreas da cibersegurança, ciberespionagem, ciberdefesa e ciberterrorismo;
(10) Operacionalização de um efetivo sistema nacional de gestão de crises;
(11) Exercitação de procedimentos e mecanismos de interoperabilidade que favoreçam a resposta a ocorrências terroristas, incluindo sistemas de informação críticos face a ciberataques.

2.2.4. Outra Legislação

Existe ainda outra legislação conexa, com interesse para uma melhor compreensão do quadro normativo da cibersegurança, cujo detalhe se apresenta em Anexo A, e que aborda, nomeadamente:

(1) Critérios, normas técnicas e medidas indispensáveis a garantir a segurança de informações;
(2) Instruções e normas para a segurança nacional;
(3) Interoperabilidade:
    (a) Regulamento Nacional de Interoperabilidade Digital;
    (b) Condições e procedimentos de interoperabilidade para Sistemas de Informação de polícia criminal;
    (c) Interoperabilidade dos sistemas eletrónicos de portagem rodoviária na Comunidade;
(4) Regimes jurídicos:
    (a) Corrupção passiva para a prática de ato ilícito;
    (b) Violação do segredo de Estado;
    (c) Ficheiros informáticos da Polícia Judiciária;
    (d) Ficheiros informáticos dos Institutos de Medicina Legal;
    (e) Documentos electrónicos e da assinatura digital;
(5) Sociedade Digital:
    (a) Sistema de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas;
    (b) Sistema Público de Autenticação Chave Móvel Digital;
    (c) Plataformas eletrónicas de contratação pública.

2.3. Arquitectura de Cibersegurança

2.3.1. Centro Nacional de Cibersegurança

Na sequência da constituição da Comissão Instaladora do Centro Nacional de Cibersegurança e dos trabalhos por ela desenvolvidos, foi aprovada pelo governo a criação do Centro Nacional de Cibersegurança (CNCS) (PCM, 2012) temporariamente inserido na estrutura do Gabinete Nacional de Segurança (GNS), tendo por missão: "contribuir para que Portugal use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional" (PCM, 2014). As competências do CNCS são as seguintes:

Tabela 11 – Competências do Centro Nacional de Cibersegurança

• Exercer os poderes de autoridade nacional competente em matéria de Cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais.
• Assegurar a produção de referenciais normativos em matéria de Cibersegurança.
• Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de Cibersegurança e ciberataques.
• Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e dos Operadores de serviços essenciais e Prestadores de serviços digitais.
• Promover a formação e a qualificação de recursos humanos na área da Cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de Cibersegurança.
• Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da Cibersegurança.
• Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da Cibersegurança.
• Coordenar a cooperação internacional em matérias da Cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;
• Coordenar a transposição da *Diretiva (UE) n.º 2016/1148* do Parlamento Europeu e do Conselho, de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, para o ordenamento jurídico interno;
• Assegurar o planeamento da utilização do ciberespaço em situação de crise ou de conflito armado, no âmbito do planeamento civil de emergência.

Fonte: Presidência do Conselho de Ministros (2015b).

2.3.2. Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) instituída pelo *Decreto-Lei n.º 81/2016* é uma unidade operacional especializada na Polícia Judiciária, típica de uma Polícia Científica, que permite recolher informação (*Cyber-intelligence*) em tempo útil e a deteção precoce de ataques digitais, assim como a compreensão da intenção criminosa associada ao uso, comercialização e disseminação de programas maliciosos.

A UNC3T permite ainda reforçar o ajustamento com as estruturas europeias e internacionais de informação e contrainformação criminal – *e.g.* EUROPOL e INTERPOL –, tendo em vista a luta eficaz contra o cibercrime assente na recolha e partilha de informações criminais

Esta unidade da Polícia Judiciária é fundamentada no modelo adotado pelo European Cybercrime Center (EC3) da EUROPOL, tendo como vetores fundamentais de atuação o abuso sexual de crianças através da internet, a fraude com os cartões e outros meios de pagamento eletrónico e virtuais, a criminalidade informática pura e a criminalidade praticada com recurso a meios informáticos.

A UNC3T tem as seguintes competências:

Tabela 12 – Competências da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

(1) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na *Lei nº 109/2009*, de 15 de Setembro;

(2) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, designadamente:
   (a) Na *Lei de Proteção de Dados Pessoais*;
   (b) No *Código dos Direitos de Autor e Direitos Conexos*, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços;

(3) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes:
   (a) Contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistemas informático;
   (b) De devassa por meio da informática;
   (c) De burla informática e nas comunicações;
   (d) Relativos à interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais;
   (e) De espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente.

(4) Elaborar e manter atualizado o Plano Nacional da Polícia Judiciária para a Prevenção e o Combate ao Cibercrime, nomeadamente, em articulação com o Centro Nacional de Cibersegurança;

(5) Assegurar o regular funcionamento de um grupo consultivo informal para debate e aconselhamento estratégico, formativo, jurídico, técnico e científico de questões relacionadas com o cibercrime, com a criminalidade tecnológica e a cibersegurança;

(6) Assegurar a colaboração e participação direta na formação inicial e contínua sobre cibercrime aos quadros do pessoal de investigação criminal e de apoio da Polícia Judiciária, designadamente, nas áreas da segurança da informação e da cibersegurança.

(7) Na UNC3T e sob a dependência da sua direção é criada uma equipa técnica e de investigação digital com as seguintes funções:
   (a) Otimizar e gerir as infraestruturas e meios tecnológicos atribuídos à Unidade;
   (b) Apoiar e assessorar nos planos técnico, tecnológico e jurídico, o pessoal de investigação criminal nas suas investigações;
   (c) Testar e desenvolver ferramentas específicas para a investigação do cibercrime, da criminalidade tecnológica e da decifragem de dados;
   (d) Recolher, tratar e difundir dados relativos a ciber-intelligence para apoio às investigações, à cooperação policial internacional e à prevenção de atos de cibercrime;
   (e) Desenvolver ações de contrainformação criminal;
   (f) Dar apoio em ações de carácter técnico para a recolha de prova digital, nomeadamente, ações encobertas e interceção de dados;
   (g) Apoiar investigações que exijam conhecimentos técnicos especializados, nomeadamente, redes de anonimização, mercados virtuais, moedas virtuais, análise de programas maliciosos.

Fonte: Adaptado de Governo de Portugal (2016).

2.3.3. Conselho Superior de Segurança do Ciberespaço

O Conselho Superior de Segurança do Ciberespaço (CSSC)[195] foi institucionalizado pela *Resolução do Conselho de Ministros n.º 115/2017* de 24 de agosto na sequência da *Estratégia Nacional de Segurança do Ciberespaço* (ENSC) (PCM, 2015b) tendo por missão "assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da ENSC e da respetiva revisão".

Este documento reconhece a necessidade de coordenação político-estratégica e de uma "abordagem transversal e integradora das variadas sensibilidades, necessidades e capacidades dos diversos setores" com responsabilidades pela segurança do ciberespaço nacional, além de reiterar o "dever de notificação de incidentes de Cibersegurança" pelas entidades públicas e operadores de infraestruturas críticas, visando a melhoria da coordenação operacional e avaliação situacional.

Tabela 13 – Objetivos do Conselho Superior de Segurança do Ciberespaço

(1) Assegurar a coordenação político-estratégica para a segurança do ciberespaço;
(2) Verificar a implementação da ENSC;
(3) Propor a revisão e elaborar a ENSC;
(4) Pronunciar –se sobre a ENSC previamente à sua submissão para aprovação;
(5) Elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da ENSC
(6) Propor ao Primeiro-Ministro, ou ao membro do Governo em quem aquele delegar, a aprovação de decisões de caráter programático relacionadas com a definição e execução da ENSC;
(7) Responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem aquele delegar, no âmbito da sua missão.

Fonte: Presidência do Conselho de Ministros (2017).

2.3.4. Despacho n.º 7456/2017 de 24 agosto da Ministra da Presidência e da Modernização Administrativa

Este despacho determina a criação de um Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação do *Regulamento Geral de Proteção de Dados* (RGPD) em Portugal e competindo-lhe em especial:

(1) Realizar uma consulta pública (até 30 de setembro de 2017);
(2) Identificar as regras de segurança no tratamento de dados pessoais decorrentes do RGPD;
(3) Apresentar alternativas de arquitetura institucional requeridas pelo RGPD;
(4) Apresentar um anteprojeto de lei (até 31 de dezembro de 2017).

195 "Funciona na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar". Presidência do Conselho de Ministros (PCM), 2017. Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço", *Resolução do Conselho de Ministros n.º 115/2017*.

2.3.5 Centro de Ciberdefesa

A Direção de Comunicações e Sistemas de Informação (DIRCSI) do Estado-Maior General das Forças Armadas (EMGFA) tem por missão e atribuições (tabela 14).

Tabela 14 – Missão e Atribuições da Direção de Comunicações e Sistemas de Informação

(1) No âmbito da Ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas
(2) No âmbito da Cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional
(3) Assegurar e participar na representação nacional nos organismos nacionais e internacionais de defesa, no âmbito dos sistemas de informação de comando e controlo, de comunicações, de segurança da informação, guerra eletrónica e Ciberdefesa
(4) Garantir o conhecimento das capacidades, limitações, tecnologias e interoperabilidade dos organismos e operadores civis de telecomunicações, tendo em vista a sua eventual utilização em situações de exceção ou guerra
(5) Apoiar os órgãos do EMGFA nas áreas de comunicações e sistemas de informação
(6) Assegurar a gestão, a manutenção e operação dos sistemas criptográficos em utilização pelas Forças Armadas
(7) Exercer a autoridade técnica no âmbito das comunicações, dos sistemas de informação, guerra eletrónica, Ciberdefesa e segurança da informação, no âmbito das Forças Armadas.

Fonte: Ministério da Defesa Nacional (2013).

No âmbito da ciberdefesa a DIRCSI/EMGFA prossegue também as seguintes atribuições (tabela 15):

Tabela 15 – Atribuições da Direção de Comunicações e Sistemas de Informação no Âmbito da Ciberdefesa

(1) Assumir a direção e coordenação da capacidade nacional de Ciberdefesa;
(2) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a Ciberdefesa;
(3) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço;
(4) Assegurar a coordenação e o trabalho colaborativo e integrado com os Núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA;
(5) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com o Centro Nacional de Cibersegurança e os CIRC nacionais e internacionais;
(6) Contribuir para as Operações de Informação, na vertente Computer Network Operations;
(7) Manter atualizada uma carta de situação do ciberespaço, situation awareness, no domínio das Forças Armadas;
(8) Planear, propor e organizar um programa de exercícios para obtenção de treino.

Fonte: Ministério da Defesa Nacional (2013).

A DIRCSI, no âmbito da cibersegurança setorial da defesa nacional, prossegue ainda as seguintes atribuições (tabela 16).

Tabela 16 – Atribuições da Direção de Comunicações e Sistemas de Informação no Âmbito da Ciberdefesa Setorial da Defesa Nacional

(1) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a cibersegurança setorial da defesa nacional;
(2) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço, no âmbito da cibersegurança setorial da defesa nacional;
(3) Assegurar a coordenação e o trabalho colaborativo e integrado com os CIRC do universo da defesa nacional;
(4) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com os CIRC nacionais e internacionais, de forma articulada com as competências de coordenação da cooperação nacional e internacional do Centro Nacional de Cibersegurança;
(5) Cooperar com as estruturas nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.

Fonte: Ministério da Defesa Nacional (2013).

2.3.6. Rede Nacional de CSIRT

Figura 11 – Rede Nacional de CSIRT

Fonte: Rede Nacional CSIRT (2017).

A Rede Nacional de CSIRT é um "*forum* de excelência para a partilha de informação de carácter operacional" que tem como principais objetivos (tabela 17).

Tabela 17 – Objetivos da Rede Nacional de CSIRT

(1) Estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;
(2) Criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contra-medidas pró-activas e reactivas;
(3) Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;

2.4. Cooperação Internacional

A importância da cooperação nacional no âmbito da cibersegurança, seja entre instituições públicas e privadas, sociedade civil e militares, indústria, academia, etc., e internacional, nos plano bilateral e multilateral, é realçada praticamente por todos os atores e em todos os fóruns e documentos de política e estratégia deste domínio.

O Centro Nacional de Cibersegurança[196] refere que "a segurança e defesa do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais", requerendo "uma abordagem em rede", em que a "cooperação nacional e internacional nos diversos domínios de atuação é da maior importância."

No âmbito da conferência organizada pela Comissão Parlamentar de Defesa Nacional sobre a temática "Ciberdefesa: o desafio do século XXI", o Chefe do Estado-Maior General das Forças Armadas (CEMGFA) (Lusa, 2017) defendeu a "necessidade absoluta" de uma cooperação "estreita e ágil" entre os serviços do Estado com responsabilidades na `ciberdefesa´ e `cibersegurança´ e a " (…) necessidade absoluta de criação de mecanismos de cooperação estreitos, ágeis e operacionais entre todas as entidades com responsabilidades nesta matéria que atravessa fronteiras nacionais, mas também transpõe fronteiras institucionais e de competências".

Relativamente à cooperação entre o Centro de Ciberdefesa, na esfera das Forças Armadas, e o Centro Nacional de Cibersegurança, com competências no âmbito da Administração Interna, *i.e.* cooperação civil-militar, afirmou ainda existirem "evidentes as complementaridades", defendendo ser indispensável "uma estreita colaboração e interoperabilidade" entre as duas estruturas, mas também uma cooperação com "forças e serviços de segurança, entidades judiciárias, entidades públicas e privadas e academia".

Essa cooperação pode concretizar-se de múltiplas formas, nomeadamente através da ciberdiplomacia, partilha ou troca de informação – ex. *intelligence*, lições, melhores práticas, normas, etc. – ou recursos – *e.g.* recursos humanos ou tecnológicos –, promoção ou realização de projetos conjuntos, etc..

Em outubro de 2013, Portugal assumiu a liderança de um Projeto Multinacional de "Smart Defense" da NATO, na área da Educação e Treino em ciberdefesa (MN CD E&T). Este projeto tem como objetivo criar uma Plataforma de Coordenação da E&T em Ciberdefesa e desenvolver novas iniciativas, destinadas a preencher as lacunas existentes contribuindo para o desenvolvimento e a interoperabilidade das capacidades de ciberdefesa.

196 CNCS, 2017a. *Centro Nacional de Cibersegurança*. Disponível em: https://www.cncs.gov.pt.

Em simultâneo, Portugal conjuntamente com França, lidera o *European Union Military Training Group – Cyber Defence Discipline*, visando desenvolver uma abordagem similar ao projeto MN CD E&T na União Europeia.

A ENISA constitui-se como uma "plataforma europeia" para o intercâmbio e partilha de informação nomeadamente entre os Estados-membros da UE, apoiando políticas e governança, facilitando a colaboração transfronteiriça e contribuindo para a preparação e partilha de conhecimento (Helmbrecht *et al.*, 2013). A tabela 18 apresenta os principais contributos da ENISA no âmbito da cooperação.

Tabela 18 – Principais Contributos da European Union Agency for Network and Information Security (ENISA)

(1) Identification and analysis of emerging trends and threats
(2) Publishing network and information security risks and challenges
(3) Early warning and response
(4) Cybersecurity strategies and capacity building
(5) Critical information infrastructure protection
(6) Incident Reporting in the EU
(7) Supporting adequate and consistent policy implementation
(8) Supporting actors in other communities (for example, industry, law enforcement and academia) in actions against cybercrime
(9) Supporting the European Commission and the Member States in international cooperation
(10) Encouraging structured information exchange
(11) Building communities
(12) Promoting private public partnerships (PPPs) in the area of cybersecurity

Fonte: Helmbrecht *et al.* (2013).

2.5. Cultura de Cibersegurança

As organizações públicas e privadas estão sujeitas a um meio envolvente[197] exigente e competitivo e a relações de poder interno com diversos grupos de interesse[198] que lhe exigem um ritmo de adaptação cada vez mais acelerado na busca da excelência. As dificuldades enfrentadas nessa adaptação requerem não só o planeamento, implementação e monitorização da mudança organizacional, mas também a análise da influência da cultura organizacional e das relações de poder.

A cibersegurança[199] não é apenas uma questão técnica, mas um imperativo das organizações, que implica gerir riscos visando a continuidade do negócio, protegendo os

197 Com múltiplas dimensões, nomeadamente, política, económica, social, tecnológica, segurança, etc.

198 Tais como acionistas, dirigentes, trabalhadores, prestadores de serviços, etc.

199 "Conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de risco, ações, treino, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos da organização e dos utilizadores" International Technology Union (ITU), 2016. *Definition of cybersecurity*. Disponível em http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

investimentos e os ativos, mantendo a reputação e vantagem competitiva. A multiplicidade de potenciais ameaças e atores, externos e internos, requer uma abordagem sistémica e multidisciplinar e a atuação no domínio da cultura organizacional.

A necessidade de desenvolver uma cultura cibersegurança alicerçada em competências[200] e favorecida através da sensibilização é enunciada em diversas estratégias.

> "O objetivo final do governo é criar uma cultura de segurança cibernética em que os Canadianos estejam conscientes das ameaças e das medidas que podem tomar para garantir o uso seguro do ciberespaço. Criar tal consciência exigirá um esforço sustentado ao longo de vários anos. O esforço deve começar agora." (Government of Canada, 2010).

> "Sensibilizar os cidadãos, os profissionais e as empresas sobre a importância da Cibersegurança e o uso responsável das novas tecnologias e dos serviços da Sociedade da Informação." Linha de Ação 7 (Cultura de Cibersegurança) – (Government of Spain, 2013).

> Eixo 4 (Educação, sensibilização e prevenção) reconhece a associa o sucesso da segurança do ciberespaço com a promoção de uma cultura de segurança que "proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização dos sistemas de informação" (PCM, 2015b).

> Objetivo 4 ("Construiremos uma base de conhecimento, habilidades e capacidades flexíveis no Reino Unido, apoiando todos os nossos objetivos."); Linha de ação "Construindo capacidades": "Construir uma cultura que entenda os riscos e permita que as pessoas usem o ciberespaço e melhorem as capacidades de segurança cibernética em todos os níveis" (UK HM Government, 2011).

Uma cultura de segurança moderna deve favorecer a autonomia dos seus colaboradores na forma como trabalham, dentro ou fora da rede corporativa. No presente, esses trabalhadores utilizam qualquer dispositivo que esteja ao seu alcance para realizar as suas tarefas da forma mais fácil, mesmo utilizando equipamentos não controlados pela respetiva organização – *e.g.* portáteis, *tablets* ou *smartphones*.

Porém, a utilização de equipamentos pessoais de forma não controlada são uma ameaça à segurança, com consequências na eventual perda de informação, introdução de malware e vírus na rede corporativa, etc. Mas, em sentido oposto, uma cultura organizacional exclusivamente baseada na adoção de práticas restritivas pode tornar uma organização mais vulnerável.

De acordo com um inquérito anual sobre incidentes cibernéticos realizados no Reino Unido, expresso na tabela 19.

---

200 As competências dependem do conhecimento (*knowledge*), habilidades (*skills*) e capacidades (*abilities)* e como tal intimamente ligadas à aprendizagem individual e organizacionais. Mendes, J. S. e Sarmento, M., 2009. A Importância da Gestão de Competências nas Organizações. *Economia & Empresa* N.º 9, pp. 114-139. Lisboa: Universidade Lusíada Editora. Disponível em http://revistas.lis.ulusiada.pt/index.php/lee/article/view/850/927

Tabela 19 – *Cyber Security Breaches*

(1) Dois terços das grandes organizações reconheceram ter sofrido penetrações não maliciosas ou acidentais;
(2) O roubo ou a divulgação não autorizada de informação classificada e o ataque ou acesso não autorizado por outsiders foram duas dos principais tipos de incidentes;
(3) As tecnologias melhoraram a colaboração, a comunicação (internet e email) e a produtividade das organizações, mas suscitaram a ocorrência de violações com origem nos seus próprios colaboradores;
(4) O erro humano inadvertido, a falta de sensibilização do pessoal, e fragilidades no processo de seleção são fatores que contribuem significativamente para estes incidentes.

Fonte: Adaptado de Gov.UK (2015, 2016).

Para lidar com esta situação as organizações em Portugal têm investido em programas de treino, sensibilização e educação, indiciando uma preocupação efetiva com esta vulnerabilidade. Na ausência de informação nacional similar ao referido relatório e atento às conclusões do mesmo, em que fatores acidentais suscitam a maioria das violações de segurança da informação, realça-se a interrogação suscitada sobre a necessidade de promoção de uma cultura de segurança.

Criar uma cultura de segurança dentro de uma empresa exige fundamentalmente treino e sensibilização. Os Chief Information Officers (CIO) e os Chief Information Security Officers (CISO) devem assegurar que todos os colaboradores da organização estejam conscientes das potenciais ameaças que podem enfrentar, por exemplo através de uma mensagem de correio eletrónico, da partilha de *passwords* ou do acesso a redes não-seguras.

Segundo Ismail (2017) a principal finalidade de uma cultura de segurança é "implementar a mudança e ser aceite por todos os envolvidos" de acordo com as melhores práticas e permitindo identificar a sua influência nos produtos e serviços que o negócio oferece, de acordo com o seu próprio ciclo de vida, requerendo investimento e desenvolvimento. Esta cultura de segurança cibernética envolve múltiplas ferramentas[201] e requer um ambiente favorável à consciência do risco, em que os colaboradores se sintam confortáveis ao reportar atividades incomuns ou suspeitas[202].

Este autor sugere um conjunto de processos internos que permitem garantir o desenvolvimento da cultura de segurança, tais como:

(1) Consciencialização de segurança cibernética e estabelecimento de procedimentos de segurança organizacional no processo de recrutamento e treino inicial;
(2) Conhecimento, por parte de todos os colaboradores, dos riscos cibernéticos e das medidas de proteção em vigor;
(3) Implementação efetiva de medidas de salvaguarda que permitam obviar qualquer evento;

201 Nomeadamente, o treino de consciencialização de segurança, cartazes, treino online, jogos online e fóruns de discussão. Ismail, N., 2017. The importance of creating a cyber security culture. *Information Age*, 8 April. Disponível em http://www.information-age.com/importance-creating-cyber-security-culture-123465778/.

202 Citando Rashmi Knowles, chief security architect, RSA. Disponível em https://www.rsa.com.

(4) Investigação forense completa após qualquer incidente contido;
(5) Envolvimento dos colaboradores;
(6) Clara identificação do que é proibido e porquê;
(7) Recompensa das boas práticas de segurança;
(8) Envolvimento dos parceiros e prestadores de serviços por forma a obviar qualquer fragilidade.

Em Portugal, diversas instituições públicas e privadas têm promovido iniciativas de educação, formação, treino e sensibilização ou mesmo comerciais que contribuem para o desenvolvimento de uma cultura de cibersegurança, de que destacamos[203]:

(1) Curso de Cibersegurança e Gestão de Crises no Ciberespaço
O curso tem por finalidade " (…) contribuir para a sensibilização e formação de quadros intermédios e superiores das estruturas do Estado e da sociedade civil, bem como de elementos com potencial para o desempenho de funções relevantes no futuro, habilitando-os a intervir em questões relacionadas com situações de crise no ciberespaço." (IDN, 2017).
(2) Exercício Cyber Perseu (Exército Português)
O Exercício CP17 tem por finalidade "exercitar e avaliar a capacidade de resposta do Exército, face à ocorrência de ciberataques de âmbito nacional ou internacional que ponham em causa a obtenção da superioridade de Informação das Forças Terrestres e a consolidação do levantamento da Capacidade Nacional de Ciberdefesa" (Exército Português, 2017)
Todavia participam igualmente neste exercício, outras entidades públicas e privadas, que utilizam o "core" do cenário e incidentes para exercitar os seus processos de decisão e atuação internos.
(3) MN CD E&T Nacional
O objetivo deste projeto é criar uma Plataforma de Coordenação da Educação e Treino em Ciberdefesa (ponto de coordenação central para uma rede de atividades de Educação e Treino) e desenvolver / proporcionar novas iniciativas, destinadas a preencher as lacunas de Educação e Treino em Ciberdefesa existentes ao nível da NATO e das Nações (MNCDET Project Team, 2017)
(4) Curso de Planeamento de Operações de Ciberdefesa
Trata-se de um "(…) curso de especialização que visa habilitar, os alunos que nele participam, com os conhecimentos teóricos e técnicos necessários para o desempenho de tarefas no âmbito das operações no ciberespaço, em funções de Estado-Maior de forças nacionais e internacionais." (IUM, 2017)
(5) *Cyber Days* (C-Days)
"*Focused on developing a strong Cybersecurity culture, C-Days 2017 brings together citizens, Public Administration, Industry and Academia to discuss and present cybersecurity at strategic, operational and technical level*" (CNCS, 2017a).

203 Ver lista global no Anexo D.

(6) Curso Geral de Cibersegurança:
Contribuir para a sensibilização, educação e literacia em todas as questões que caracterizam, moldam, influenciam e conduzem ao estado-da-arte atual da Cibersegurança e do Ciberespaço (CNCS, 2017b).

(7) NetVivaeSegura
Iniciativa da revista Deco Proteste e da Google que tem como objetivo promover uma maior segurança na internet e sensibilizar para a importância de proteger a privacidade do utilizador na rede (DECO, 2017).

(8) Programa Internet Mais Segura
Projeto da responsabilidade de um consórcio coordenado pela Fundação para a Ciência e Tecnologia (FCT), e que também envolve a Direção Geral da Educação (DGE) do Ministério da Educação, a Fundação para a Computação Científica Nacional (FCCN), Instituto Português do Desporto e Juventude (IPDJ), e a Microsoft Portugal (Internet Segura, 2017).

(9) Programas de Formação Avançada (Mestrados e Pós-Graduações)
Diversas universidades e Institutos Politécnicos têm oferecido programas avançados ao nível Mestrado e Pós-Graduação na área da cibersegurança e domínios afins (ver Anexo E).

2.6. Política Pública em Cibersegurança

2.6.1. Estratégia Nacional de Segurança do Ciberespaço

A *Estratégia Nacional de Segurança do Ciberespaço* (ENSC) (PCM, 2015b) tem o seu preâmbulo alinhado com as visões e tendências enunciadas nos documentos de referência da União Europeia para a Cibersegurança e os relatórios *Global Risks* do Fórum Económico Mundial, e faz referência a um conjunto de elementos que importam realçar:

(1) A segurança ciberespaço como espaço de soberania e prioridade nacional;
(2) A dependência das Tecnologias de Informação e Comunicação (TIC) para realização de "funções vitais" e o reconhecimento dos riscos para a sociedade das suas vulnerabilidades;
(3) A necessidade de reduzir as fragilidades da segurança das redes e da informação e de aumentar a resiliência das infraestruturas críticas;
(4) O impacto do ativismo religioso, criminal ou terrorismo nas infraestruturas vitais de informação;
(5) A necessidade de um sistema eficaz de gestão de crises e coordenação da resposta operacional;
(6) A potenciação da criminalidade sexual e a sua dimensão transnacional através da internet;
(7) As múltiplas facetas do "cibercrime" nomeadamente fraude bancária e usurpação de identidade;
(8) O *hacktivismo* político através do "desvio e revelação de informação", "sabotagem informática" e a "espionagem de Estado e industrial";
(9) A indispensabilidade de cooperação nacional, europeia e internacional.

A Estratégia tem como finalidade "aprofundar a segurança das redes e da informação", enquanto condição indispensável à segurança e defesa das "infraestruturas críticas" e "serviços vitais de informação"[204] por forma a "potenciar uma utilização livre, segura e eficiente do ciberespaço". É igualmente a reconhecida a importância da liberdade no acesso às TIC e em particular à internet para a sociedade em geral e à segurança e eficiência na comunicação e transações eletrónicas, caraterísticas essenciais para a atividade económica. O seu âmbito é abrangente e procura dar resposta às necessidades dos cidadãos, empresas, setor público e privado.

A Estratégia pressupõe um conjunto de princípios[205] (gerais) e pilares – subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização – e desenvolve-se em quatro objetivos estratégicos, com uma orientação geral e específica, refletidos em seis eixos de intervenção, integrando medidas concretas e linhas de ação.

Tabela 20 – Estratégia Nacional de Segurança do Ciberespaço

(1) Objetivos Estratégicos
(a) Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
(b) Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
(c) Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;
(d) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.
(2) Eixos de Intervenção
(a) Eixo 1 – Estrutura de segurança do ciberespaço;
(b) Eixo 2 – Combate ao cibercrime;
(c) Eixo 3 – Proteção do ciberespaço e das infraestruturas;
(d) Eixo 4 – Educação, sensibilização e prevenção;
(e) Eixo 5 – Investigação e desenvolvimento;
(f) Eixo 6 – Cooperação

Fonte: Presidência do Conselho de Ministros (2015b) e Barbas (2016).

2.6.2. Orientação Política para a Ciberdefesa

O ciberespaço é considerado um novo domínio operacional onde podem ser conduzidas operações militares indispensáveis às Forças Armadas para o seu Comando e Controlo e atuar potenciais ameaças à Defesa Nacional.

204 O conceito de "serviços vitais de informação" não é caraterizado no documento.

205 " (…) nos princípios gerais da soberania do Estado, das linhas gerais da Estratégia da União Europeia para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade" Presidência do Conselho de Ministros (PCM), 2015b. Resolução do Conselho de Ministros n.º 36/2015. *Diário da República*, 1.ª Série, N.º 113, 12 de junho. Disponível em http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html

A "Orientação para a Política de Ciberdefesa" assemelha-se a uma "Estratégia Nacional para a Ciberdefesa" e visa definir os objetivos, estabelecer as linhas orientadoras dos esforços a desenvolver e promover, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa.

As linhas de ação da Política de Ciberdefesa Nacional têm como pressupostos: (1) a importância do Ciberespaço na afirmação da Soberania Nacional e na defesa de valores e interesses; (2) a dependência das Forças Armadas do Ciberespaço na condução de operações militares; (3) a segurança dos Sistemas de Informação e Comunicações (SIC) e o valor da informação corporativa; (4) o desenvolvimento tecnológico articulado com Planeamento de Defesa; (5) a articulação das iniciativas com a OTAN e a União Europeia; (6) a colaboração entre a Defesa e a comunidade académica, os setores público e privado e a base industrial de defesa.

Os princípios que lhe estão subjacentes são, nomeadamente:

(1) A prevenção, deteção, contenção e alerta;
(2) A proporcionalidade da resposta à ameaça;
(3) O reforço da segurança dos SIC[206] críticos;
(4) A defesa cooperativa das Infraestruturas de Informação Críticas (IIC) e a exigência de uma abordagem conjunta[207] e cooperativa[208];
(5) A potenciação das capacidades técnicas associadas à cibersegurança;
(6) A complementaridade da ciberdefesa na gestão do risco operacional[209] das IIC através da criptografia, segurança da informação, segurança física e do pessoal;
(7) Capacidades de recolha e análise de informação no ciberespaço;
(8) O apoio jurídico à condução das operações;
(9) O recrutamento e retenção de recursos humanos qualificados pelas Forças Armadas.

Os objetivos estratégicos para a ciberdefesa são:

(1) Garantir a proteção, a resiliência e a segurança das redes e dos SIC da defesa nacional contra ciberataques;
(2) Assegurar a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional;
(3) Contribuir de forma cooperativa para a cibersegurança nacional.

206 Entendemos que a designação "SIC críticos" utilizada no texto da *Orientação Política para a Ciberdefesa* deve ser entendida como Infraestruturas de Informação Críticas (IIC), designação normalmente utilizada na bibliografia de referência sobre o ciberespaço.

207 Envolvendo mais de um Ramo das Forças Armadas.

208 Apesar de não ser explícito, entendemos tratar-se de uma abordagem cooperativa nos planos bilateral e multilateral (UE, NATO, ONU).

209 Conjunto de práticas e procedimentos que permitem assegurar a confidencialidade, integridade e disponibilidade da informação. Sewall, B., 2009. *Confidentiality, Integrity & Availability*. Disponível em http://ishandbook.bsewall.com/risk/Methodology/CIA.html.

Tabela 21 – Linhas Orientadoras para a Ciberdefesa Nacional

(1) [Estabelecer] Estrutura de [Comando e Controlo da] Ciberdefesa Nacional
(a) Órgão com caráter de orientação estratégica-militar das atividades de Ciberdefesa;
(b) Capacidade militar de resposta operacional a ciberataques e a incidentes informáticos;
(2) Planeamento de Defesa Militar
(a) Integração da criação da Capacidade de Ciberdefesa nos processos de Planeamento Nacional[210], da NATO[211] e da UE[212].
(3) Capacidade para conduzir Operações Militares em Redes de Computadores
(a) Implementação de capacidades para conduzir todo o espectro de operações no ciberespaço (defensivas, de exploração e ofensivas).
(4) Reforço da Capacidade de Informações no Ciberespaço
(a) Produção de conhecimento situacional e recolha de informação.
(5) Partilha da Informação de Ciberdefesa
(a) Implementação de sistemas de "partilha de informação" e de "alerta imediato"[213].
(b) Estratégia de ciência e tecnologia para a Ciberdefesa.
(6) Sensibilização, Formação e Exercícios
(a) Sensibilização de utilizadores dos SIC;
(b) Formação e qualificação de peritos em ameaças cibernéticas e operações em redes de computadores;
(c) Treino em ambientes degradados;
(d) Participação em exercícios nacionais e internacionais de ciberdefesa;
(e) Centralização da formação e treino em ciberdefesa
(f) Constituição de um polo de excelência em ciberdefesa;
(7) Aquisições e Cadeia de Reabastecimento – Gestão de Risco
(a) Adoção de requisitos de gestão de risco visando reduzir risco com *software* ou do *hardware*.

Fonte: Barbas (2016).

2.6.3. O Programa do XXI Governo Constitucional

O Programa do Governo (PCM, 2015a) tem como linhas de orientação ou medidas no âmbito do ciberespaço:

(1) Defesa Nacional. Reforço do combate ao ciberterrorismo, através do Centro de Ciberdefesa e pela cooperação e articulação internacional no combate ao cibercrime;

(2) Segurança interna e política criminal:

210 Processo de Planeamento de Defesa Militar.

211 NATO Defence Planning Process (NDPP). Fleischer, P., 2015. NATO Defence Planning Process. Implications for Defence Posture. *Securitologia* N.º 1, pp. 103-114. Disponível em http://tinyurl.com/j65uvjp.

212 Capability Defence Plan (CDP).

213 Em colaboração com a rede nacional de serviços de resposta a incidentes de segurança informática (CSIRT), instituições privadas, universidades e organizações internacionais (NATO e UE).

(3) O estabelecimento de orientações estratégicas de segurança interna em resposta aos principais riscos e ameaças internas e externas, nomeadamente o cibercrime;
(4) A ampliação das responsabilidades e meios do Centro Nacional de Cibersegurança, preservando a segurança das infraestruturas e os direitos fundamentais, designadamente a privacidade, em articulação com as estruturas homólogas do setor da defesa nacional.
(5) A melhoria das capacidades da Polícia Judiciária, nomeadamente no combate à cibercriminalidade.
(6) A referência ao papel das Forças Armadas na luta contra as ameaças à segurança coletiva, em especial à cibercriminalidade.

CAPÍTULO VI
Análise Comparada dos Países

1. Aproximação Concetual

O documento *Bases para una Política Nacional de Ciberseguridad* do Chile apresenta um conjunto de definições dos termos mais utilizados no âmbito da cibersegurança. Em Portugal, a *Lei do Cibercrime* (Governo de Portugal, 2009) apresenta um conjunto de definições para os termos utilizados na mesma, mapeando a Convenção de Budapeste (Council of Europe, 2001a; 2001b; 2001c) ratificada por Portugal (Assembleia da República, 2009). Existem ainda glossários de termos técnicos e científicos utilizados nos domínios das TIC e do ciberespaço compilados e disponibilizados por instituições públicas e organizações não-governamentais de interesse público através da web, tais como os do Centro Nacional de Cibersegurança (CNCS); Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) e AFCEA Portugal (2013).

Em ambiente académico – por exemplo, em teses e projetos de investigação – é habitual a explicitação dos principais conceitos utilizados. Tal é menos frequente em legislação, podendo a sua ausência acarretar dificuldades na sua compreensão, enquanto a sua inserção favorecer a sua obsolescência, principalmente em domínios ainda em processo de maturação.

2. Legislação Especializada

Ambos os países possuem legislação especializada e diferenciada, sobre múltiplos temas conexos com a cibersegurança, tal como no âmbito dos serviços de informações, investigação criminal, proteção de dados pessoais, etc. No caso chileno, em geral, foram tomadas em consideração orientações internacionais na formulação da legislação nacional, que nalguns casos enfrentam o desafio da sua atualização. No caso de Portugal, a arquitetura normativa da cibersegurança (estratégias, legislação, etc.) está articulada – *e.g. Lei do Cibercrime* – ou decorre de cooperação multilateral – *e.g. Regulamento Geral de Proteção de Dados* – no âmbito da União Europeia e da NATO.

Em qualquer dos casos, entende-se que a legislação identificada em ambos os países com relevância para a cibersegurança, se encontra num processo de evolução e maturação permanente, para ir de encontro às oportunidades e desafios da Sociedade da Informação e do aprofundamento do mercado digital.

3. Arquitetura de Cibersegurança

A *Política Nacional de Cibersegurança* do Chile consagra um extenso conjunto de entidades com responsabilidades no domínio desta política pública, e nalguns casos, mapeando outra legislação específica e conexa.

Neste caso é possível identificar o Ministério do Interior e Segurança Pública, Ministério da Defesa Nacional, Ministério de Transportes e Telecomunicações, Ministério da Economia, Fomento e Turismo, Ministério da Justiça e Direitos Humanos, Ministério das Relações Exteriores e Ministério Secretaria Geral da Presidência. Apesar de aparente-

mente faltar uma estrutura coordenadora das diversas entidades dependentes do executivo com responsabilidades neste âmbito, em 2015 foi criado o Comité Interministerial de Cibersegurança (CIC) com o objetivo de "propor uma política nacional de cibersegurança e apoiar a coordenação de ações, planos e programas dos diferentes atores institucionais" e tendo como atribuições, nomeadamente: (1) assessorar a Presidência da República; (2) identificar as ameaças, propor ações de mitigação e monitorizar a sua implementação; (3) Propor medidas de coordenação entre os atores dos setores público e privado.

No caso de Portugal, o Centro Nacional de Cibersegurança (CNCS) foi criado em 2014 (PCM, 2014), tendo integrado as competências técnicas do CERT.PT da FCCN de carater académico que tinha estado na génese da utilização da internet em Portugal em meados dos anos 90. O Conselho Superior de Segurança do Ciberespaço (CSSC) recentemente institucionalizado em Portugal pretende, nomeadamente, "assegurar a coordenação político-estratégica para a segurança do ciberespaço". A Rede Nacional CSIRT que congrega 31 CSIRT é um *forum* de partilha de informação de carácter operacional indispensável à capacidade de reação a incidentes cibernéticos.

Neste factor de comparação constata-se que os países possuem entidades similares, apesar de uma arquitetura de Cibersegurança em distintos estádios de maturidade. No Chile, o CLCERT de caráter académico assemelha-se porventura ao CERT.PT anterior à sua integração no CNCS, i.e. ainda na sua ligação à FCCN, não existindo ainda uma estrutura similar ao Centro Nacional de Cibersegurança. Em contrapartida, o Comité Interministerial de Cibersegurança (CIC) do Chile, foi constituido (2015) antes da promulgação da Política de Cibersegurança do Chile (PNCS) em 2017 e visando desenvolver a mesma, enquanto em Portugal, a criação do CSSC (2017) foi concretizado apenas após a promulgação da Estratégia Nacional de Segurança do Ciberespaço de 2015.

4. Cooperação Internacional

Ambos os países reconhecem a importância da cooperação internacional nas suas políticas públicas no domínio do Ciberespaço e participam ativamente em diversas iniciativas no plano multilateral no âmbito da ONU. No caso de Portugal também na União Europeia e NATO e o caso chileno na OEA. Ambos países participam em fóruns internacionais como a Conferência Global do Ciberespaço e Conferência de Medelin.

Portugal lidera a participação em projetos de Educação e Treino de caráter cibernético na NATO/OTAN e União Europeia, enquanto o Chile trabalha com a OEA em termos de treino e capacitação. O *Manual de Tallinn* é utilizado como manual de referência para lidar com temas/situações ligadas ao Direito Internacional no Ciberespaço.

5. Cultura de Cibersegurança

O Chile e Portugal têm desenvolvido um extenso conjunto de iniciativas no domínio da cultura de cibersegurança, nomeadamente nos domínios da educação, formação, treino, sensibilização, etc., através de instituições públicas, academia, empresas, organizações não-governamentais e sociedade civil em geral. Todavia, a alteração de hábitos com-

portamentais e de mentalidade na forma como se utilizam as TIC e a internet diariamente por instituições públicas ou privadas e cidadãos, exige um esforço duradouro e de longo-prazo, que deverá ser acompanhado por iniciativas que permitam aferir a eficiência e eficácia das mesmas, i.e. se os comportamentos de risco têm tendência a reduzirem-se de forma consistente.

Tal como com as campanhas de segurança rodoviárias visando a redução da sinistralidade, não bastam boas intenções.

6. Política Pública de Cibersegurança

O Chile e Portugal dispõem de políticas públicas para a área da cibersegurança, respetivamente a *Política Nacional de Ciberseguridad* e a *Estratégia Nacional de Segurança do Ciberespaço* (PCM, 2015b). Embora promulgados em tempos diferentes, mas próximos, ambos os países possuem documentos de orientação política para abordar a segurança cibernetica numa perspectiva de política pública.

Ambos os países tem ainda preocupações com a orientação política da ciberdefesa, que no caso de Portugal deu origem à publicação da *Orientação para a Política de Ciberdefesa* e no caso do Chile suscita a criação, em breve, da *Politica Nacional de Ciberdefesa*. Embora em momentos diferentes mas próximos, ambos os países produziram documentos de orientação política para abordar a segurança cibernética numa perspectiva de política pública.

A implementação de uma política pública neste domínio enfrenta ainda desafios que importa enunciar, nomeadamente: (1) na aquisição e disseminação de conhecimento específico; (2) mudança de mentalidades que potencie a melhoria contínua e a aprendizagem individual e coletiva, nomeadamente através de capacidades de lições aprendidas; (3) a governação e cooperação público-privada; (4) a adoção de metodologias de planeamento que permitam implementar e rentabilizar as indispensáveis capacidades de defesa cibernética; (5) o recrutamento e retenção de recursos humanos qualificados.

Em resumo, ambos os países consideraram os seis fatores no âmbito da sua política de segurança cibernética. No entanto, existem semelhanças e diferenças na forma como cada fator se desenvolveu a nível nacional.

CAPÍTULO VI
Conclusiones

La existencia de un nuevo dominio o ambiente denominado ciberespacio, puesto a disposición de la sociedad ha tenido como resultado un creciente uso en la población, incorporándose en las diferentes dimensiones de la vida humana tanto a nivel individual como colectivo. En forma paralela se han aparecido peligros de diverso tipo que pueden afectar su uso seguro, siendo necesario contemplar la "ciberseguridad" como una condición necesaria más no suficiente para promover su uso en forma confiable y masivo en la comunidad. Debido a que ello es un problema público al afectar toda la población, una perspectiva de política pública constituye un modo recomendable de abordar este tema. En este contexto, desde Naciones Unidas se ha hecho un importante esfuerzo para entregar herramientas que orienten a los países, especialmente a través de su organismo especializado la Unión Internacional de Telecomunicaciones, difundiendo informes que abordan diversos aspectos del ciberespacio y la ciberseguridad.-

En el caso de Chile y Portugal a nivel internacional se participa en la UIT y a nivel nacional han generado políticas públicas en materia de ciberseguridad con la finalidad de promover la disponibilidad, integridad y confiabilidad de la información virtual, considerando estándares internacionales en la materia.

Una primera etapa para abordar a nivel nacional la ciberseguridad, ha sido la construcción de aproximaciones conceptuales mínimas y compartidas para abordar un tema especializado cuyo tratamiento requiere de profesionales de diferente origen que trabajan en organizaciones distintas. En efecto, términos como "ciberespacio" y "ciberseguridad" han requerido ser definidos como requisito para formular políticas y a través de ellas explicitar principios orientadores, como también, establecer objetivos, metas e instituciones.

La revisión de la experiencia de Chile y Portugal, permite plantear una aproximación conceptual sobre ciberespacio y ciberseguridad. La ciberseguridad puede entenderse como un ambiente o dominio con características específicas compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior cuya interacción ha generado una nueva forma de relacionarse a nivel individual y colectivo. La ciberseguridad constituye una necesidad de este nuevo ambiente que se constituye en condición necesaria más no suficiente para permitir su uso confiable. Se caracteriza por ser un medio para alcanzar un fin y desde una perspectiva estatal se manifiesta en una serie de políticas nacionales que considerando diversos factores, buscan evitar que un ciberincidente afecte la vida de las personas, su patrimonio, la estabilidad institucional y/o la soberanía nacional. En este contexto, especial relevancia tiene que la información virtual no pierda sus cualidades de disponibilidad, integridad y confidencialidad, como también, que la infraestructura crítica de la información no tenga daños que impidan su normal funcionamiento.

Por este motivo, las políticas públicas específicas en el tema, que se manifiestan por medio de la Política Nacional de Ciberseguridad en el caso chileno y una estrategia de

seguridad del Ciberespacio en el caso portugués constituyen instrumentos claves para orientar el modo a abordar este tema al entregar las directrices para enfrentarlo, con la finalidad de evitar los peligros en el uso del ciberespacio que originados por amenazas externas y/o vulnerabilidades propias, pueden causar riesgos de origen diverso, manifestándose en forma variada y buscando como objetivo alcanzar diferentes efectos que perturben el normal funcionamiento del ciberespacio.

Aunque las políticas para abordar el tema presentan diferencias, es posible identificar factores comunes en ambas, las cuales corresponden a: marco conceptual; legislación especializada; arquitectura de ciberseguridad; cooperación internacional; cultura de ciberseguridad; y política pública en ciberseguridad.

En el caso chileno, la formulación de una política nacional de ciberseguridad ha sido un trabajo de años que se ha concretado en la presentación de la PNCS el primer semestre de 2017. En este documento queda consignado el compromiso chileno con objetivos y medidas que permitirán contar con un ciberespacio libre, abierto, seguro y resiliente para responder a la necesidad de resguardar la seguridad de las personas en el ciberespacio, proteger la seguridad del país y gestionar los riesgos del ciberespacio. En este contexto el gobierno chileno ha elaborado una serie de definiciones especializadas para facilitar el trabajo interagencial sobre el tema. También ha planteado la necesidad de actualizar el marco normativo sobre delitos en el ciberespacio y la necesidad de generar las normativas que falten en materia de regulación en el uso del ciberespacio. Asimismo, se constata la existencia de una arquitectura de ciberseguridad que contempla a entidades de diversos ministerios, destacando un CSIRT nacional ubicado en el Ministerio del Interior. Esta arquitectura requiere una nueva institucionalidad, la cual está contemplada en el marco de la PNCS. La cooperación internacional ha sido considerada como un aspecto clave en la ciberseguridad, promoviéndose la participación en diferentes instancias multilaterales que abordan el tema como la ONU y la OEA. Además se ha considerado la participación en foros internacionales como la CGCS y MERIDIAN, entre otros. Junto a lo indicado, se ha contemplado la firma de la Convención de Budapest y la capacitación en el derecho internacional aplicado al ciberespacio (Manual de Tallin). Atendiendo a la importancia de que la población cuente con buenas prácticas en ciberseguridad se ha considerado la promoción de una cultura de ciberseguridad que a través de diferentes instancias se informe a los distintos grupos de la sociedad de conductas de riesgo en el ciberespacio y la manera de prevenirlas. Además se ha establecido el mes de octubre como el mes de la ciberseguridad, instando a que se realicen actividades sobre el tema a nivel de instituciones como de campañas públicas. La política pública chilena en materia de ciberseguridad junto al documento PNCS se complementa con otras políticas en desarrollo, las cuales corresponden a la Agenda 2020, la Política Nacional de Ciberdefensa y la Política Nacional del Ciberespacio, cada una de ellas a cargo de diferentes ministerios (Economía, Defensa y Relaciones Exteriores, respectivamente), quedando en evidencia la importancia de la coordinación interagencial en materia de ciberseguridad.

En el caso de Portugal, desde hace años se avanza en una política de ciberseguridad, contando en el año 2009 con una aproximación conceptual mínima de términos especia-

lizados. Respecto a la legislación especializada, el Concepto Estratégico de Defensa Nacional se encuentra creado por Ley se refiere a los efectos de los ataques cibernéticos, identificando el ciberterrorismo y la cibercriminalidad como amenazas y riesgos prioritarios por su capacidad de afectar las infraestructuras críticas del país. Además tiene una Ley de Cibercrimen aprobada en 2009 junto a una variada normativa que regula diversos aspectos asociados a la ciberseguridad como por ejemplo: centro de datos, la interoperabilidad digital, entre otros. Con relación a la arquitectura de ciberseguridad, existe un Centro Nacional de Ciberseguridad creado en 2014, con la misión de contribuir en el uso del ciberespacio en forma segura, por medio de la mejora continua y la cooperación internacional. Para el cumplimiento de esta misión se entregan atribuciones y competencias específicas que lo convierten en un organismo especializado y coordinador de los diferentes organismos vinculados al tema a nivel nacional e internacional. Junto a este organismo hay otras entidades gubernamentales especializadas con responsabilidades en el ámbito de la ciberseguridad como la Unidad Nacional de Combate al Crimen y la Criminalidad Tecnológica, el Consejo Superior de Seguridad del Ciberespacio y el Centro de Ciberdefensa, entre otros. Además cuenta con un CSIRT nacional. La cooperación internacional se considera como necesaria y relevante. Contempla la participación en diferentes instancias internacionales como por ejemplo, la ONU y la adopcion de las directrices emanadas de la UE y la OTAN en materia de ciberseguridad. La cultura de ciberseguridad es considerada como factor clave para promover prácticas deseadas en ciberseguridad en diferentes sectores de la población, a través de iniciativas de formación, sensibilización y divulgación.

La Estrategia de Seguridad en el Ciberespacio, desarrollada en 2015, es el documento de política pública que establece las directrices para la ciberseguridad nacional. Su finalidad es profundizar la seguridad de las redes y de la información considerado como condición para la seguridad y defensa de las infraestructuras críticas y servicios vitales de información, lo que permitiría potenciar el uso libre, seguro y eficiente del ciberespacio. Su alcance es amplio y busca responder a las necesidades de los ciudadanos, las empresas, el sector público y el privado. Asimismo, esta estrategia plantea un conjunto de principios generales, objetivos estratégicos y ejes de intervención que integran medidas y líneas de acción. Ademas en el ámbito de las políticas públicas, hay que tener en cuenta la Orientación política para la Ciberdefesa y el programa del XXI Gobierno Constitucional, que consideró esta cuestión en su agenda.

Al revisar el caso de chileno y de Portugal es posible constatar similitudes con relación a contar con una aproximación oficial de términos especializados que contribuyen a un trabajo interagencial del tema. Ambos países cuentan con una política pública que además de establecer una base conceptual mínima, contempla documentos que explicitan las directrices, objetivos y medidas que se desea alcanzar en el tema. En el marco de esta política destaca la cooperación internacional que se expresa en la participación en instituciones, foros y convenios multilaterales especializados (coincidiendo ambos en la firma de la Convención de Budapest, entre otros), junto a la promoción de una cultura de ciberseguridad como elementos claves para sensibilizar a la población en buenas prácticas

para el uso del ciberespacio. Aunque con políticas diferentes ambos presentan políticas asociadas a la de ciberseguridad. Asimismo, es posible encontrar una legislación especializada que regula el funcionamiento y uso del ciberespacio, como también, busca perseguir los incidentes que pueden ocurrir en éste resultado de amenazas y vulnerabilidades propias de este ambiente. En los dos países hay una arquitectura de ciberseguridad que relaciona a diversos organismos nacionales vinculados al tema desde su especificidad.

En cuanto a las diferencias, se constata que el trabajo en los documentos oficiales especializados en el tema ha sido en tiempos cercanos pero diferentes. Por ejemplo, mientras la Estrategia Nacional de Seguridad en el Ciberespacio de Portugal fue promulgada en 2015, la Política Nacional de Ciberseguridad chilena se promulgó en 2017. Asimismo, es posible apreciar que el nivel de compromisos internacionales suscritos condicionará el nivel de autonomía para desarrollar esta política. Por ejemplo en el caso de Portugal, las directrices emanadas por la UE entregan lineamientos a considerar a nivel nacional esta política. A diferencia en el caso chileno, las recomendaciones de OEA aunque también orientan en la formulación de la política, no son obligatorias su incorporación en los documentos nacionales sino orientadoras. Este mismo factor influye en las legislaciones nacionales sobre el tema. La arquitectura de ciberseguridad es diferente en ambos países, presentando solo el caso de Portugal un organismo con capacidad de coordinar a nivel nacional e internacional el tema. Aunque ambos países tienen definiciones especializadas son diferentes entre ambos pero no son discrepantes.

En síntesis, las similitudes permiten una interlocución válida para abordar el tema desde una perspectiva bilateral y las diferencias responden a realidades, una madurez institucional distinta y exigencias internacionales diferentes. En este sentido, es posible desarrollar un trabajo compartido en el tema de ciberseguridad desde una perspectiva de política pública pues los enfoques nacionales sobre el tema son coincidentes. Por ejemplo, en materia de formación, capacitación y pasantías en la el tema.

Referências

Abad, J., 2015. Anonymus declara la guerra al ISIS: quiénes son y qué han conseguido. *El País* [Em linha], 18 NOV, 21:13 CET, Madrid. Disponible en http://tecnologia.elpais.com/tecnologia/2015/11/17/actualidad/1447752730_293113.html [Consult. 17/9/2017].

AFCEA Portugal, 2013. Glossário do Ciberespaço. *AFCEA Portugal* [Em linha]. Disponível em: http://www.afceaportugal.pt/2013/eventos/GlossarioCiberespaco__v2_27Set.pdf.

Alaluf, A., 2013. Tecnología: La ciberseguridad de Mr. K. *Qué Pasa* [Em linha], Agosto 15. Disponível em: http://www.quepasa.cl/articulo/tecnologia/2013/08/23-12457-9-tecnologia-la-ciberseguridad-de-mr-k.shtml/ [Consult. 17/9/2017].

Alien Vault, 2016. *Blood on HR's Floor – The Challenge of Retaining Skilled IT Security Professionals*. Alien Vault [Em linha]. Disponível em: https://www.alienvault.com/docs/whitepapers/blood-on-hrs-floor.pdf [Consult.7/9/2017].

Anabalón, J. y. Donders E., 2014. Una revisión de ciberdefensa de infraestructura crítica. *Estudios de Seguridad y Defensa* [Em linha], n.º 3, jun., pp. 131-164. Disponible en http://esd.anepe.cl/wp-content/uploads/2014/11/art5.pdf [Consult.17/9/2017].

Argyris, C., ed., 2006. *Reasons and Rationalizations: The Limits to Organizational Knowledge*: Oxford: OUP.

Argyris, C. e Schön, D. A., 1978. *Organizational Learning: A theory of action perspective*. Addison-Wesley.

Assembleia da Républica, 2017. Conferência "Ciberdefesa: o Desafio do Século XXI", 24 de maio, Comissão de Defesa Nacional. Disponível em: https://www.parlamento.pt/sites/COM/Paginas/DetalheNoticia.aspx?BID=8182 [Consult. 13/9/2017].

Assembleia da República, 2009a. Lei n.º 109/2009 de 15 de Setembro. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. *Dário da República*, 1.ª Série, N.º 179, de 15 de Setembro, pp. 6319-6325. Disponível em: https://dre.pt/application/file/a/489631 [Consult. 2/6/2017].

Assembleia da República, 2009b. Resolução da Assembleia da República n.º 88/2009. Aprova a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001, *Diário da República* [Em linha], 1.ª Série, N.º 179, 15 de Setembro. Disponível em: http://data.dre.pt/eli/resolassrep/88/2009/09/15/p/dre/pt/html [Consult. 2/6/2017].

Assembleia da República, 1998. Lei n.º 67/98 de 26 Outubro. Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.o 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). *Diário da República*, I Série-A, N.º 247, pp. 5536-5546 Disponível em: https://dre.pt/application/conteudo/239857 [Consult. 13/06/2017].

Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI). *Glossário da Sociedade de Informação*. [Website] Disponível em: http://www.apdsi.pt/Actividades_2005/Glossario/glossario.html

Bachelet, M., 2017. *Política Nacional de Ciberseguridad*. Gobierno de Chile. Disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Banco Interamericano de Desarrollo (BID), 2016. BID y OEA instan a América Latina y el Caribe a mayores esfuerzos en ciberseguridad. *BID* [Em linha], Marzo 14, Comunicados de Pren-

sa. Disponible en http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html

Banco Interamericano de Desarrollo (BID) e Organización de los Estados Americanos (OEA), 2016. *Ciberseguridad* ¿Estamos preparados *en América Latina y el Caribe?* Informe Ciberseguridad 2016, Observatorio de la Ciberseguridad en América Latina y el Caribe. Disponible en https://publications.iadb.org/handle/11319/7449

Bank for International Settlements (BIS) e International Organization of Securities Commissions (IOSCO), 2016. *Guidance on cyber resilience for financial market infrastructures*. BIS/IOSCO, June 2016, pp. 32. [Em linha] Disponível em: https://www.bis.org/cpmi/publ/d146.pdf [Consult. 30/1/2018].

Barbas, J., 2016. Contributo para o Estudo da Cibersegurança em Portugal. *In* José Cimar Rodrigues Pinto, org., *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional*. XVII Conferência de Diretores de Colégios de Defesa Ibero-Americanos 2016. Rio de Janeiro: Escola Superior de Guerra, pp. 228-264. Disponible en http://www.asociacioncolegiosdefensaiberoamericanos.org/acdibero/LibrosReunionesDirectores/LIBRO+XVII+CONFERENCIA+-+CIBERDEFESA+E+CIBEREGURAN%C3%87A+NOVAS+AMEA%C3%87AS+%C3%80+SEGUR....pdf

Bateson, G. 1972. *Steps to an Ecology of Mind*. New York: Ballantine. [Em linha] Disponível em: http://www.edtechpost.ca/readings/Gregory%20Bateson%20-%20Ecology%20of%20Mind.pdf

BBC, 2017. Virus WannaCry: ¿corre peligro mi computadora? *BBC Mundo* [Em linha], Redaccion, 12 de Mayo. Disponível em: http://www.bbc.com/mundo/noticias-39904811 [Consult. 17/9/2017].

BBC, 2016. Así secuestraron mi teléfono los piratas informáticos. *BBC Mundo* [Em linha], 4 de marzo. Disponible en http://www.bbc.com/mundo/noticias/2016/03/160304_tecnologia_telefono_smartphone_secuestro_il [Consult. 17/9/2017].

Bhuiyan, N. e Baghel, A., 2005. An overview of continuous improvement: from the past to the present. *Management Decision* 43(5) 761-771.

Boer, H., Berger, A., Champna, R. e Gertsen, F., eds., 2000. *CI Changes: From Suggestion Box to Organisational Learning. Continuous Improvement in Europe and Australia*. Aldershot: Ashgate Publishing.

Business Continuity Institute (BCI). [Website]. Disponível em: http://www.thebci.org/ [Consult. 30 Maio 2016].

Candau, J., 2010. Estrategias Nacionales de Ciberseguridad. Ciberterrorismo. *Cuadernos de Estrategia* 149 [Em linha]. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Diciembre. Instituto Español de Estudios Estratégicos, Ministerio de Defensa. Disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. [Consult. 15/9/2017].

Castells, M. 1999. *La era de la información: Economía, Sociedad y cultura. Volumen II: El poder de la identidad*. México: Siglo XXI Editores.

Center for Strategic and International Studies (CSIS), 2016. *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*. Report [PDF]. Washington, CSIS. Disponível em McAfee: https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf [Consult. 7/9/2017].

Centro Nacional de Cibersegurança (CNCS), 2017a. *Centro Nacional de Cibersegurança* [Em linha]. Disponível em: https://www.cncs.gov.pt [Consult. 13/9/2017].

Centro Nacional de Cibersegurança (CNCS), 2017b. *Curso Geral de Cibersegurança* [Em linha]. Disponível em: https://www.cncs.gov.pt/atividades/oferta-formativa/curso-geral-de-ciberseguranca/ [Consult. 24/11/2017].

Centro Nacional de Cibersegurança (CNCS). *Glossário* [Website]. Disponível em: https://www.cncs.gov.pt/recursos/glossario/.

Cerf, V. G., 2000. *Statement of Dr. Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology MCI WorldCom, For the Joint Economic Committee*. February 23. [Em linha] Disponível em: https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm [Consult. 13/11/2017].

Ciberdelincuencia.Org. [Website] Disponible en http://ciberdelincuencia.org/fuentes/resoluciones.php

CLCERT, 2017. *Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile* [Em linha]. Disponível em: https://www.clcert.cl/.

Cole, R., 2001. From continuous improvement to continuous innovation. *Quality Management Journal* 8(4) pp. 7-20.

Comissão das Comunidades Europeias, 2003. *Comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu. Governança e Desenvolvimento.* COM(2003) 615 final, 20.10.2003, Bruxelas. Disponível em EUR-Lex: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52003DC0615&from=PT [Consult. 14/11/2017].

Comissão Nacional de Proteção de Dados (CNPD), 2017. 10 Medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados. *CNPD* [Em linha], 28 de janeiro. Disponível em: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf [Consult. 28 Janeiro 2017].

Commission of the European Communities, 2009. *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Critical Information Infrastructure Protection. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*. COM(2009) 149 final, 30.03.2009, Brussels. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&from=EN [Consult. 2/6/2017].

Commission of the European Communities, 2006. *Communication from the Commission on a European Programme for Critical Infrastructure Protection.* COM(2006) 786 final, 12.12.2006, Brussels. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN [Consult. 2/6/2017].

Commission of the European Communities, 2004. *Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism.* COM(2004) 702 final, 20.10.2004, Brussels. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN [Consult. 11/8/2017].

Commission on Enhancing National Cybersecurity, 2016. *Report on Securing and Growing the Digital Economy*. December 1, National Institute of Standards and Technology (NIST), US Department of Commerce. [Em linha] Disponível em: https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf [Consult. 13/11/2017].

Computer Emergency Response Team (CERT-EU). [Website] Disponível em: https://cert.europa.eu/cert/plainedition/en/cert_about.html.

Contreras, B., 2009. *Esfuerzos del CICTE-OEA para fortalecerla Seguridad Cibernética en las Américas*. OEA, Secretaría de Seguridad Multidimensional, Comité Interamericano contra el Terrorismo (CICTE). Disponible en https://www.itu.int/ITU-D/cyb/events/2009/santo-domingo/docs/CONTRERAS-CICTE-overview-nov-09.pdf

Council of Europe, 2001a. *Convention on Cybercrime*. Details of Treaty No.185, 23/11/2001, Budapest. Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe, 2001b. Convenio sobre la ciberdelincuencia. Serie de Tratados Europeos nº185, 23.11.2001, Budapest. Disponible en http://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Council of Europe, 2001c. *Convention on Cybercrime.* European Treaty Series, No. 185, 23.11.2001, Budapest. Disponível em Council of Europe, Treaty Office: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 [Consult. 12/1/2017].

Council of Europe, 1950. *Convenção Europeia dos Direitos do Homem,* European Court of Human Rights/ Council of Europe, Strasbourg. [Em linha] Disponível em: http://www.echr.coe.int/documents/convention_por.pdf [Consult. 05/01/2017].

Cyert, R. M. e March, J. G., 1963. *A behavioral theory of the firm.* Englewood Cliffs, NJ, USA: Prentice-Hall.

Danish Government, 2015. *The Danish Cyber and Information Security Strategy*. Ministry of Finance. [Em linha] Disponível em https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy.

del Moral Torres, A., 2010. *Cooperación Policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal.* ARI 50/2010, 17/03/2010, Real Instituto Elcano. [Em linha] Disponível em: https://www.files.ethz.ch/isn/122470/ARI50-2010_cooperacion_policial_UE_inteligencia_criminal.pdf [Consult.17/9/2017].

Digital Attack Map, 2013. What is a DDoS Attack? *Digital Attack Map* [Em linha]. Disponível em: http://www.digitalattackmap.com/understanding-ddos/.

European Commission, 2016. Security, Borders, Police. *Migration and Home Affairs* [Em linha]. Disponível em: https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties_en [Consult. 23/1/2017].

European Commission, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN(2013) 1 final, 7.2.2013, Brussels, High Representative of the European Union for Foreign Affairs and Security Policy. Disponível em European Union External Affairs, Archives: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [Consult. 9/1/2015].

European Comission, 2013. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN(2013) 1 final, 7.2.2013, Brussels. Disponível em EEAS, Archives: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [Consult. 9 January 2015].

European Comission, 2011. *Article 29 Data Protection Working Party. Advice paper on special categories of data ("sensitive data").* Justice and Consumers. [Em linha] Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [Consult. 10/8/2017].

European Economic and Social Committee, 2010. Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"', COM(2009) 149 final (2010/C 255/18). *Official Journal of the European Union,* C 255/98 EN, 22.9.2010. Disponível em EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009AE1948&from=EN [Consult. 4/6/2017].

European External Action Service, 2016. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy.* EEAS [Em linha], June. Disponível em European Union External Action, Archives: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf [Consult. 4/6/2017].

European External Action Service, 2015. *Food-for-thought paper "Countering Hybrid Threats".* EEAS(2015) 731, 13 May, Council of the European Union. [Em linha] Disponível em: http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf [Consult. 4/6/2017].

European Parliament, 2017. *As Fontes e o Âmbito de Aplicação do Direito da União Europeia*. Fichas técnicas sobre a União Europeia. Disponível em European Parliament: http://www.europarl.europa.eu/ftu/pdf/pt/FTU_1.2.1.pdf.

European Parliament and Council of the European Union, 2016a. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal of the European Union*, L 119, EN, 4.5.2016. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en [Consult. 10/1/2017].

European Parliament and Council of the European Union, 2016b. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194, EN, 19.7.2016. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN [Consult. 4/6/2017].

European Parliament and Council of the European Union, 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union*, L 218, EN, 14.8.2013. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN [Consult. 2/6/2017].

European Parliament and Council of the European Union, 2009. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance) *Official Journal of the European Union,* L 337, EN, 18.12.2009. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140&from=EN [Consult. 2/6/2017].

European Parliament and Council of the European Union, 2002. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). *Official Journal of the European Union,* L 108, EN, 24.4.2002. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=EN [Consult. 2/6/2017].

European Parliament and Council of the European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, No L 281, EN, 23.11.95. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

European Union, 2016. *Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union*. Official Journal of the European Union, C 202, Volume 59, 7 June 2016. Disponível em EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG [Consult. 13/6/2016].

European Union Agency for Network and Information Security (ENISA), 2016. Review of Cyber Hygiene practices. *ENISA* [Em linha], December, Heraklion. Disponível em: https://www.enisa.europa.eu/publications/cyber-hygiene [Consult. 13/11/2017].

European Union Agency for Network and Information Security (ENISA). [Website] Disponível em: https://www.enisa.europa.eu/.

European Union's Judicial Cooperation Unit (EUROJUST). [Website] Disponível em: http://www.eurojust.europa.eu [Consult. 25/4/2016].

Evenbrite, 2017. Innovation Meets Cybersecurity: The Public-Private Cooperation Challenge. *Evenbrite* [Em linha], Conferência, 4.ª feira, 8 de novembro, COTEC Portugal/CNCS/Conselho da Diáspora Portuguesa/Univ. of Maryland Baltimore County. Disponível em: https://www.eventbrite.pt/e/bilhetes-innovation-meets-cybersecurity-the-public-private-cooperation-challenge-37647205806# [Consult. 24/11/2017].

Exército Português, 2017. Exército testa segurança informática. *Exército Português* [Em linha], Initial Planning Conference (IPC), CIBER PERSEU 17 (CP17), 18 de maio. Disponível em: https://www.exercito.pt/pt/informa%C3%A7%C3%A3o-p%C3%BAblica/not%C3%ADcias/207 [Consult. 24/11/2017].

Federal Financial Institutions Examination Council (FFIEC), 2015a. Appendix J: Strengthening the Resilience of Outsourced Technology Services. Background and Purpose. *FFIEC* [Em linha]. Disponível em: http://tinyurl.com/ntpr9ch.

Federal Financial Institutions Examination Council (FFIEC), 2015b. About the FFIEC. [Website] Disponível em: https://www.ffiec.gov/about.htm [Consult. 13 Abril 2016].

Fiol, C. M. e Lyles, M. A., 1985. Organizational Learning. The Academy of Management Review [Em linha], Vol. 10, No. 4 (Oct., 1985), pp. 803-813.

Fleischer, P., 2015. NATO Defence Planning Process. Implications for Defence Posture. *Securitologia* [Em linha], N.º 1, pp. 103-114. Disponível em: http://tinyurl.com/j65uvjp.

Fryer, K., Antony, J. e Douglas, A., 2007. Critical success factors of continuous improvement in the public sector: A literature review and some key findings. *The TQM magazine* 19(5) pp. 497-517.

Gartner, 2017. Total Cost of Ownership (TCO). *Gartner* [Em linha]. Disponível em: http://www.gartner.com/it-glossary/total-cost-of-ownership-tco [Consult. 7/9/2017].

George, M. L., 2002. *Lean Six Sigma*. McGraw-Hill.

Global Conference on Cyber Space (GCCS), 2017. Global Conference on Cyber Space. About GCCS. Disponible en https://gccs2017.in/about

Gobierno de Chile, 2017. *Política Nacional de Ciberseguridad*. Disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Gov.UK, 2016. *Cyber Security Breaches Survey 2016*. Department for Digital, Culture, Media & Sport. May, London. [Em linha] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016.

Gov.UK, 2015. *Information Security Breaches Survey 2015*. Department for Business, Innovation and Skils. London. [Em linha] Disponível em: https://assets.publishing.service.gov.uk/government/uplo-

ads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

Government of Latvia 2013. *Cyber Security Strategy of Latvia 2014-2018*. [Em linha] Disponível em https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

Government of The Nederlands, 2013. *National Cyber Security Strategy 2. From awareness to capability*. National Coordinator for Security and Counterterrorism. [Em linha] Disponível em https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf.

Governo de Portugal, 2013. *Conceito Estratégico de Defesa Nacional 2013*. Aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril. Disponível em IDN: https://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf

Guimón, P., 2017. Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero. *El País* [Em linha], 12 May, 23:11 CEST, Londres. Disponível em: https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html [Consult. 17/9/2017].

Hedberg, B., 1981. How organizations learn and unlearn? *In* Paul C. Nystrom e William H. Starbuck, eds., *Handbook of organizational design*. Vol. 2: Remodelling Organizations and their Environments. Oxford: Oxford University Press, pp. 8-27.

Held, D. *et al*., 2002. *Transformaciones globales. Política, economía y cultura*. México: Oxford University Press.

Helmbrecht, U. *et al*., 2013. *Cybersecurity cooperation: Defending the digital frontline* [PDF]. European Union Agency for Network and Information Security (ENISA), Science and Technology Park of Crete (ITE), October, Heraklion. [Em linha] Disponível em: https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline [Consult. 13/9/2017].

Infobae, 2017. Ciberataque mundial impacta a instituciones estatales y privadas en "una dimensión nunca antes vista". *Infobae* [Em linha]. Disponible en http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/. [Consult. 17/9/2017].

Instituto da Defesa Nacional (IDN), 2017. *Curso de Cibersegurança e Gestão de Crises no Ciberespaço (CGCiber)*. IDN [Em linha]. Disponível em: http://www.idn.gov.pt/index.php?mod=1004&area=1600 [Consult. 24/11/2107].

Instituto Universitário Militar (IUM), 2017. Curso de Planeamento de Operações de Ciberdefesa (CPOCIBER). *IUM* [Em linha]. Disponível em: https://www.ium.pt/s/index.php/pt/cursos/cursos-de-especializacao/curso-de-planeamento-de-operacoes-de-ciberdefesa-cpociber [Consult. 24/11/2017].

International Organization for Standardization (ISO), 2012. ISO 22301 2012. Societal security – Business continuity management systems – Requirements. *ISO* [Em linha]. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

International Organization for Standardization (ISO), 2016a. ISO 22301 2012. *ISO* [Em linha]. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en [Consult. 2 abril 2016].

International Organization for Standardization (ISO), 2016b. ISO/IEC 27000 *2016,* Information security management systems: Overview and vocabulary. *ISO* [Em linha]. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en [Consult. 9/10/2016].

International Organization for Standardization (ISO). [Website] Disponível em: www.iso.org

International Telecommunication Union (ITU), 2017. *Measuring the Information Society Report 2017*. Volume 1, ITU, Geneva. [Em linha] Disponible en http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf. [Consult. 17 de Noviembre de

2017].

International Telecommunication Union (ITU), 2016. Definition of cybersecurity. *ITU* [Em linha] Disponível em: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

International Telecommunication Union (ITU), 2015. Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar. *ITU* [Em linha]. Informe, Abril de 2015, Oficina de Desarrollo de las Telecomunicaciones, Ginebra. Disponible en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

International Telecommunication Union (ITU), s.d.a. National Strategies. *ITU* [Em linha]. Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

International Telecommunication Union (ITU), s.d.b. Legal Measures. *ITU* [Em linha]. Disponible en https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx

International Telecommunication Union (ITU), s.d.c. CIRT Programe. *ITU* [Em linha]. Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx

Internet Segura, 2017. Sobre o Projeto Internet Segura. *Internet Segura* [Em linha]. Disponível em: http://www.internetsegura.pt/projecto [Consult. 24/11/2017].

Ismail, N., 2017. The importance of creating a cyber security culture. *information age* [Em linha], 8 April. Disponível em: http://www.information-age.com/importance-creating-cyber-security-culture-123465778/ [Consult. 11/9/2017].

Karpersky Lab, 2015. *Los riesgos futuros: Protéjase*. [Em linha] Disponible en http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf [Consult. 15/9/2017].

Kato, I. e Smalley, A., 2012. *Toyota Kaizen Methods: Six Steps to Improvement* [e-book]. New York: Productivity Press.

Kissinger, H., 2016. *Orden Mundial*. Madrid: Debate.

Laqueur, W., 2015. La guerra cibernética ("juegos de guerra"). *Vanguardia dossier,* Nº 54, pp. 6-15.

Linderman, K. *et al.*, 2003. Six Sigma: A goal-theoretic perspective. *Journal of Operations Management*. 21(2), pp. 193-203.

Lo, T. K. M. e Fong, P. S. W., 2010. Enhancing Quality of Lessons Learned: Evaluating Knowledge Management Practices in Project Management. *In* P. Barrett *et al.,* eds., *Information and Knowledge Management in Building: Proceedings of the 18th CIB World Building Congress*. CIB General Secretariat, pp. 173-178.

Lusa, 2017. Chefe do EMGFA adverte para necessidade absoluta de cooperação para proteger 'ciberespaço'. *Diário de Notícias* [Em linha], 13:12, 24 de maio. Disponível em: http://www.dn.pt/lusa/interior/chefe-do-emgfa-adverte-para-necessidade-absoluta-de-cooperacao-paraproteger-ciberespaco-8503215.html [Consult. 13/9/2017].

Markoff, J., 2008. Before the Gunfire, Cyberattacks. *The New York Times* [Em linha], August 12. Disponível em: http://www.nytimes.com/2008/08/13/technology/13cyber.html [Consult. 25/9/2017].

McInerney, C. e Koenig, M. E. D., 2011. Knowledge Management (KM) Processes in Organizations: Theoretical Foundations and Examples of Practice. *Synthesis Lectures on Information Concepts, Retrieval, and Services*, 3(1), January, pp. 1-96. Morgan & Claypool Publishers.

Mendes, J. S. e Sarmento, M., 2009. A Importância da Gestão de Competências nas Organizações. *Economia & Empresa* [Em linha], N.º 9, pp. 114-139. Lisboa: Universidade Lusíada Editora. Disponível em: http://revistas.lis.ulusiada.pt/index.php/lee/article/view/850/927

Meridian, 2017. [Website] Disponible en https://www.meridianprocess.org/

Meridian, 2017. *How Meridian work. About Meridian*. Disponible en https://meridian2017.atlassian.net/wiki/spaces/TS1/pages/1671371/About+Meridian

Michela, J. L., Noori, H. e Jha, S., 1996. The dynamics of continuous improvement. *International Journal of Quality Science*, 1(1) pp. 19-47.

Ministério da Defesa Nacional (MDN), 2013. Despacho n.º 13692/2013 de 11 de outobro de 2013, Gabinete do Ministro. *Diário da República* [Em linha], II Série, N.º 208, 28 de outubro de 2013.

Ministerio del Interior y Seguridad Pública/Ministerio de Defensa Nacional, 2015. *Bases para una Política Nacional de Ciberseguridad*. Gobierno de Chile. Disponible en http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

MNCDET Project Team, 2017. *Multinational Cyber Defence Education and Training Project (MN CD E&T)*. [Em linha] Disponível em: http://www.mncdet-pt.net/ [Consult. 24/11/2017].

Naciones Unidas, 2012. La UIT pide reforzar la ciberseguridad. *Noticias ONU* [Em linha], 31 Mayo. Disponible en http://www.un.org/spanish/News/story.asp?newsID=23582#.Wd_gFVvWzcc

NATO, 2017a. Collective defence – Article 5. *NATO* [Em linha]. Disponível em: https://www.nato.int/cps/ic/natohq/topics_110496.htm [Consult. 11/11/2017].

NATO, 2017b. North Atlantic Council (NAC). *NATO* [Em linha]. Disponível em: https://www.nato.int/cps/ic/natohq/topics_49763.htm [Consult. 25/11/2017].

NATO, 2014. *Wales Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. *NATO* [Em linha], Press Release (2014) 120. Disponível em NATO, Official texts: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm [Consult. 11/11/2017].

NATO, 2014a. The NATO Defence Planning Process. *NATO* [Em linha]. Disponível em: http://www.nato.int/cps/en/natohq/topics_49202.htm [Consult. 12 Abril].

NATO, 2014b. NATO Communications and Information Agency. *NCI Agency* [Em linha]. Disponível em: https://www.ncia.nato.int.

NATO, 2012. *Chicago Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. *NATO* [Em linha], Press Release (2012) 062. Disponível em NATO, Official texts: http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en [Consult. 25/9/2017].

NATO, 2011. Defending the networks: The NATO Policy on Cyber Defence. *NATO* [Em linha] Disponível em: http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819--policy-cyberdefence.pdf [Consult. 5/9/2017].

NATO, 2010a. *Lisbon Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon. *NATO* [Em linha]. Disponível NATO, Official texts: em: http://www.nato.int/cps/en/natohq/official_texts_68828.htm

NATO, 2010b. *Active Engagement, Moderne Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010, Brussels, NATO Public Diplomacy Division. Disponível em: NATO, Strategic Concept 2010: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO, 2007. Press briefing by the NATO Spokesman, James Appathurai on the Meetings of NATO Defence Ministers on 14 and 15 June 2007. *NATO* [Em linha]. Disponível em NATO, Online Library: http://www.nato.int/docu/speech/2007/s070614g.html [Consult. 25/9/2017].

NATO, 2006. *Riga Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006. *NATO* [Em linha], Press Release (2006) 150. Disponível em NATO, Online Library: https://www.nato.int/docu/pr/2006/p06-150e.htm

NATO, 2003. *Handbook on Long Term Defence Planning*. RTO Technical Report 69, RTO/NATO, April. Disponível em http://www.ibrarian.net/navon/paper/NORTH_ATLANTIC_TREATY_ORGANISATION.pdf?paperid=18906814 [Consult. 7/9/2017].

NATO, 2002. Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic. *NATO* [Em linha], Press Release (2002) 127. Disponível em NATO, Official texts: http://www.nato.int/cps/ic/natohq/official_texts_19552.htm? [Consult. 24/9/2017].

NIC Chile, 2017. Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. [Website] Disponível em: https://www.nic.cl/.

Nonaka, I., 1995. The knowledge-creating company. *Harvard business review classics*, V, p. 59. Boston, Mass., Harvard Business Press.

Nonaka, I., 1994. A Dynamic Theory of Organizational Knowledge Creation. *Organization Science,* 5(1) pp. 14-27.

Nonaka, I., Toyama, R. e Konno, N., 2000. SECI, *Ba* and Leadership: a Unified Model of Dynamic Knowledge Creation. *Long Range Planning,* 33(1), pp. 5-34.

Nye, J. 2012. Ciberguerra y Ciberpaz. *Project Syndicate* [Em Linha], Apr 10. Disponible en https://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish?barrier=accesspaylog

Olavarría, M., 2007. *Conceptos Básicos en el Análisis de Políticas Públicas*. Documentos de Trabajo N.º 11, Diciembre. INAP-Instituto de Asuntos Públicos Departamento de Gobierno y Gestión Pública, Universidad de Chile, pp. 92. [Em linha] Disponível em Repositorio Académico de la Universidad de Chile: http://repositorio.uchile.cl/bitstream/handle/2250/123548/Conceptos_%20Basicos_Politicas_Publicas.pdf?sequence=1 [Consult. 15/9/2017].

Organización de los Estados Americanos (OEA), 2017a. Seguridad Cibernética. *OEA* [Em linha]. Disponible en https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx

Organización de los Estados Americanos (OEA), 2017b. Comité Interamericano contra el Terrorismo. Misión. *OEA* [Em linha]. Disponible en http://www.oas.org/es/sms/cicte/acerca_nosotros_mision.asp

Organización de los Estados Americanos (OEA), 2017c. Comité Interamericano contra el Terrorismo. Programas. *OEA* [Em linha]. Disponible en http://www.oas.org/es/sms/cicte/programas.asp

Organización de los Estados Americanos (OEA), 2015a. *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. OEA [Em linha], Abril de 2015, Secretaría de Seguridad Multidimensional de la OEA/Trend Micro, Washington. Disponible en https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Organización de los Estados Americanos (OEA), 2015b. Respuesta a incidentes de infracción de marcas registradas. IRM 15. Disponible en https://www.sites.oas.org/cyber/Documents/Metodolog%C3%ADa%20de%20Respuesta%20a%20Incidentes%20(IRMs)%20IRM15-InfraccionMarcaRegistrada-OEA.pdf

Organización de los Estados Americanos (OEA), 2014. *Tendencias de Seguridad Cibernética en América Latina y el Caribe. Estados Unidos*. OEA [Em linha], Junio, Secretaría de Seguridad Multidimensional

de la OEA, Washington. Disponible en https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Organización de los Estados Americanos (OEA), 2004. *Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética*, AG/RES. 2004 (XXXIV-O/04). Aprobada en la cuarta sesión plenaria, celebrada el 8 de junio. Disponible en https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf

Palazuelos, F., 2017. China descubre una nueva mutación del virus responsable del ciberataque mundial. *El País* [Em linha]. 15 May, 16:13 CEST, Pekin/Madrid. Disponível em: https://elpais.com/tecnologia/2017/05/15/actualidad/1494835268_125044.html [Consult. 17/9/2017].

Parlamento Europeu e Conselho da União Europeia, 2011. Directiva 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho. *Jornal Oficial da União Europeia*, L 335, PT, 17.12.2011. Disponível em EUR-Lex: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=PT [Consult. 2/6/2017].

Polanyi, M., 1996. *The Tacit Dimension*. London: Routledge & Kegan Paul.

Presidência do Conselho de Ministros (PCM), 2017. Resolução do Conselho de Ministros n.º 115/2017. *Diário da República*, 1.ª Série, N.º 163, 24 de agosto. Disponível em: http://data.dre.pt/eli/resolconsmin/115/2017/08/24/p/dre/pt/html.

Presidência do Conselho de Ministros (PCM), 2015a. Resolução do Conselho de Ministros n.º 7-A/2015. *Diário da República*, 1.ª série, N.º 36, 20 de fevereiro. Disponível em https://dre.pt/application/conteudo/66567251

Presidência do Conselho de Ministros (PCM), 2015b. Resolução do Conselho de Ministros n.º 36/2015. *Diário da República*, 1.ª Série, N.º 113, 12 de junho. Disponível em: http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html

Presidência do Conselho de Ministros (PCM), 2014. Decreto-Lei N.º 69/2014 de 9 de maio. *Diário da República*, 1.ª Série, N.º 89, 9 de maio de 2014. Disponível em: https://dre.pt/application/conteudo/25343754

Presidência do Conselho de Ministros (PCM), 2012. Resolução do Conselho de Ministros n.º 42/2012. *Diário da República*, 1.ª série, N.º 74, 13 de abril. Disponível em: https://dre.pt/application/dir/pdf1s/2012/04/07400/0192501926.pdf

Probst, G. e Buchel, B., 1994. *Organisationales Lernen*. Gabler.

Randall, R., 2015. *Cyber Security Considerations for Your Business Continuity Plan*. [Em linha] Disponível em: http://blog.integratelecom.com/cyber-security-considerations-for-your-business-continuity-plan/ [Consult. 13 Abril 2016].

Rede Nacional CSIRT, 2017. [Website] Disponível em: http://www.redecsirt.pt/.

Saiz, E., 2013. Los ciberataques sustituyen al terrorismo como primera amenaza a Estados Unidos. *El País* [Em linha], 13 MAR, 17:00 CET, Washington. Disponível em: http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html

Sancho, C., 2016. Ciberespacio bien público mundial en tiempos de globalización: política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI. *In* José Cimar Rodrigues Pinto, Org., *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional*. XVII

Conferência de Diretores de Colégios de Defesa Ibero-Americanos 2016. Rio de Janeiro: Escola Superior de Guerra, pp. 41-79. Disponible en http://www.asociacioncolegiosdefensaiberoamericanos.org/acdibero/LibrosReunionesDirectores/LIBRO+XVII+CONFERENCIA+-+CIBERDEFESA+E+CIBEREGURAN%C3%87A+NOVAS+AMEA%C3%87AS+%C3%80+SEGUR....pdf

Santos, D., 2013. *Metodologia de Melhoria Contínua na Gestão de Projetos*. [PDF] Dissertação de Mestrado, Faculdade de Engenharia da Universidade do Porto.

Schmitt, M., ed., 2013. *Tallinn Manual on the International Law Applicable to Cyber warfare*. Cambridge University Press.

Schwab, K., 2017. *La cuarta revolución industrial*. Buenos Aires: Debate.

Secchi, P., Ciaschi, R. e Spence, D., 1999. A Concept for an ESA Lessons Learned System. *In* P. Secchi, ed., *Proceedings of Alerts and LL: An Effective way to prevent failures and problems (Tech. Rep. WPP-167)*. The Netherlands: ESTEC, Noordwijk.

Serviços Partilhados do Ministério da Saúde (SPMS), 2017. 3rd eHealth Security Conference: Protecting the Hospital of the Future, 15 de novembro, Lisboa, aud. da FMD/Univ. de Lisboa. *Ministério da Saúde* [Em linha]. Disponível em: http://spms.min-saude.pt/events/3rd-enisa-ehealth-cyber-security-conference/ [Consult. 24/11/2017].

Sewall, B., 2009. *Confidentiality, Integrity & Availability*. [Em linha] Disponível em: http://ishandbook.bsewall.com/risk/Methodology/CIA.html [Consult. 30 Abril 2016].

Spanish Cyber Security Institute (SCSI), 2012. La Ciberseguridad Nacional, un compromiso de todos. *Instituto Español de Ciberseguridad* [Em linha]. Disponible en https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf

St-Germain, R. *et al*., s.d.. ISO 22301 Societal Security Business Continuity Management Systems. *White Paper*, PECB University. [Em linha] Disponível em: http://zih.hr/sites/zih.hr/files/cr-collections/3/iso22301_bcm.pdf.

The Chartered Quality Institute (CQI). [Website] Disponível em: http://www.thecqi.org/.

Torres, M., 2013. Ciberguerra. *In* Javier Jordán, coordinador, *Manual de Estudios Estratégicos y Seguridad Internacional*. Madrid: Plaza y Valdés Editores, pp. 329-348.

Trim, P. R. J. e Lee, Y.-I., 2014. *Cyber security management : a governance, risk and compliance framework*, 1st Edition. London: Routledge.

U. S. Department of Homeland Security, 2016. *Cyber Hygiene & Cyber Security Recommendations* [PDF], October 5. Disponível em https://ohioauditor.gov/cybersecurity/CYBER%20HYGIENE.PDF [Consult.13/11/2017].

União Europeia, 2000. Carta dos Direitos Fundamentais da União Europeia. *Jornal Oficial das Comunidades Europeias*, C 364/1 PT, 18.12.2000. Parlamento Europeu, Conselho Europeu e Comissão Europeia. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf [Consult. 12/1/2017].

Unión Internacional de Telecomunicaciones (UIT), 2014. Informe sobre Medición de la Sociedad de la Información 2014. Resumen Ejecutivo. *UIT* [Em linha], Ginebra. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS_2014_Exec-sum-S.pdf [Consult. 15/9/2017].

Unión Internacional de Telecomunicaciones (UIT), s.d.. La Agenda sobre Ciberseguridad Global. *UIT* [Em linha]. Disponible en https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html

United Nations (UN), 1976. *International Covenant on Civil and Political Rights*. Adopted by the General Assembly of the United Nations on 19 December 1966, UN [Em linha], Treaty Series, vol. 999, No. 14668. Disponível em: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf [Consult. 13/6/2017].

United Nations (UN), 1966a. *International Covenant on Economic, Social and Cultural Rights*. UN [Em linha], Treaty Series, vol. 993, New York, 16 December. Disponível em: https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/iv-3.en.pdf

United Nations (UN), 1966b. *International Covenant on Economic, Social and Cultural Rights*. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A of 16 December 1966 (XXI) entry into force 3 January 1976, in accordance with article 27, UN. [Em linha] Disponível em: http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf [Consult. 13/6/2017].

United Nations (UN), 1948. *Universal Declaration of Human Rights*. *UN* [Em linha]. Disponível em: http://www.un.org/en/universal-declaration-human-rights/ [Consult. 13/6/2017].

United Nations Office on Drugs and Crime (UNODC). Cybercrime. [website] Disponible en https://www.unodc.org/unodc/es/cybercrime/index.html

Universidad Nacional Autónoma de México (UNAM), 2012. Karpesky habla sobre el virus Flame. *UNAM* [Em linha], 01-Jun-2012. Disponible en http://www.seguridad.unam.mx/noticia/?noti=377 [Consult. 17/9/2017].

Villamediana, M., 2015. Los datos son el nuevo petróleo del siglo XXI. *EuroXpress* [Em linha], 1 de julio. Disponível em: http://www.euroxpress.es/noticias/los-datos-son-el-nuevo-petroleo-del-siglo-xxi [Consult. 15/9/2017].

Watters, J., 2014. *Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference*. [s.l.] Apress.

West-Brown, M. J. *et al.,* 2003. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. 2nd Edition. Pittsburgh: Software Engineering Institute/Carnegie Mellon University. [Em linha] Disponível em: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf [Consult. 2/6/2017].

Womack, J. P. e Jones, D. T., 2003. *Lean thinking: banish waste and create wealth in your corporation*. 2nd Edition, Revised and Updated. New York: Free Press, pp. 396.

Ximenéz, P., 2016. Michael Hayden: "Me preocupa que Trump pueda ser presidente". *El País* [Em linha], 8 MAR, 00:12 CET, Los Ángeles. Disponible en http://internacional.elpais.com/internacional/2016/03/04/actualidad/1457076618_844331.html [Consult. 17/9/2017].

Anexo A: Estrutura da Convenção de Budapeste

(1) Chapter I – Use of terms
(2) Article 1 – Definitions
(3) Chapter II – Measures to be taken at the national level
(4) Section 1 – Substantive criminal law
(5) Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems
(6) Article 2 – Illegal access
(7) Article 3 – Illegal interception
(8) Article 4 – Data interference
(9) Article 5 – System interference
(10) Article 6 – Misuse of devices
(11) Title 2 – Computer-related offences
(12) Article 7 – Computer-related forgery
(13) Article 8 – Computer-related fraud
(14) Title 3 – Content-related offences
(15) Article 9 – Offences related to child pornography
(16) Title 4 – Offences related to infringements of copyright and related rights
(17) Article 10 – Offences related to infringements of copyright and related rights
(18) Title 5 – Ancillary liability and sanctions
(19) Article 11 – Attempt and aiding or abetting
(20) Article 12 – Corporate liability
(21) Article 13 – Sanctions and measures
(22) Section 2 – Procedural law
(23) Title 1 – Common provisions
(24) Article 14 – Scope of procedural provisions
(25) Article 15 – Conditions and safeguards
(26) Title 2 – Expedited preservation of stored computer data
(27) Article 16 – Expedited preservation of stored computer data
(28) Article 17 – Expedited preservation and partial disclosure of traffic data
(29) Title 3 – Production order
(30) Article 18 – Production order
(31) Title 4 – Search and seizure of stored computer data
(32) Article 19 – Search and seizure of stored computer data
(33) Title 5 – Real-time collection of computer data
(34) Article 20 – Real-time collection of traffic data
(35) Article 21 – Interception of content data
(36) Section 3 – Jurisdiction
(37) Article 22 – Jurisdiction
(38) Chapter III – International co-operation
(39) Section 1 – General principles
(40) Title 1 – General principles relating to international co-operation
(41) Article 23 – General principles relating to international co-operation
(42) Title 2 – Principles relating to extradition
(43) Article 24 – Extradition
(44) Article 25 – General principles relating to mutual assistance
(45) Article 26 – Spontaneous information
(46) Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
(47) Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
(48) Article 28 – Confidentiality and limitation on use
(49) Section 2 – Specific provisions
(50) Title 1 – Mutual assistance regarding provisional measures
(51) Article 29 – Expedited preservation of stored computer data
(52) Article 30 – Expedited disclosure of preserved traffic data
(53) Title 2 – Mutual assistance regarding investigative powers
(54) Article 31 – Mutual assistance regarding accessing of stored computer data
(55) Article 32 – Trans-border access to stored computer data with consent or where publicly available
(56) Article 33 – Mutual assistance regarding the real-time collection of traffic data
(57) Article 34 – Mutual assistance regarding the interception of content data
(58) Title 3 – 24/7 Network
(59) Article 35 – 24/7 Network
(60) Chapter IV – Final provisions
(61) Article 36 – Signature and entry into force
(62) Article 37 – Accession to the Convention
(63) Article 38 – Territorial application
(64) Article 39 – Effects of the Convention
(65) Article 40 – Declarations
(66) Article 41 – Federal clause
(67) Article 42 – Reservations
(68) Article 43 – Status and withdrawal of reservations
(69) Article 44 – Amendments
(70) Article 45 – Settlement of disputes
(71) Article 46 – Consultations of the Parties
(72) Article 47 – Denunciation
(73) Article 48 – Notification

Anexo B: Estrutura do Manual de Tallinn 2.0

Part I. General International Law and Cyberspace:
1. Sovereignty
2. Due diligence
3. Jurisdiction
4. Law of international responsibility
5. Cyber operations not per se regulated by international law
6. International human rights law
7. Diplomatic and consular law
8. Law of the sea
9. Air law
10. Space law
11. International telecommunication law

Part II. International Peace and Security and Cyber Activities:
12. Peaceful settlement
13. Prohibition of intervention
14. The use of force
15. Collective security

Part III. The Law of Cyber Armed Conflict:
16. The law of armed conflict generally
17. Conduct of hostilities
18. Certain persons, objects and activities
19. Occupation
20. Neutrality

Anexo C: Outra Legislação Portuguesa Aplicável

- *Resolução do Conselho de Ministros n.º 47/88*, de 5 de novembro, que aprova os critérios, normas técnicas e medidas indispensáveis a garantir a segurança de informações processadas, necessários ao funcionamento do Centro de Dados do Serviço de Informações de Segurança (SIS)
- *Resolução do Conselho de Ministros n.º 50/88*, de 3 de dezembro, que aprova as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1).
- *Resolução do Conselho de Ministros n.º 37/89*, de 24 de outubro, que aprova as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação (SEGNAC 2).
- *Resolução do Conselho de Ministros n.º 5/90*, de 28 de fevereiro, que aprova as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática (SEGNAC 4).
- *Resolução do Conselho de Ministros n.º 13/93*, de 6 de março, que altera a RCM n.º 50/88, de 3 de dezembro.
- *Resolução do Conselho de Ministros n.º 16/94*, de 22 de março, que aprova as instruções para a segurança nacional, segurança das telecomunicações (SEGNAC 3).
- *Resolução do Conselho de Ministros n.º 91/2012*, de 8 de novembro, que aprova o Regulamento Nacional de Interoperabilidade Digital.
- *Lei n.º 36/2003*, de 22 de agosto, que estabelece normas de execução da decisão do Conselho da União Europeia que cria a EUROJUST, a fim de reforçar a luta contra as formas graves de criminalidade, e regula o estatuto e competências do respetivo membro nacional.
- *Código de Justiça Militar,* aprovado pela *Lei n.º 100/2003*, de 15 de novembro e revisto – Art.º 36.º, sobre corrupção passiva para a prática de ato ilícito.
- *Lei n.º 30/2007,* de 6 de agosto, que transpõe para a ordem jurídica interna a *Diretiva n.º 2004/52/CE*, do Parlamento Europeu e do Conselho, de 29 de Abril, relativa à interoperabilidade dos sistemas eletrónicos de portagem rodoviária na Comunidade, tendo em vista a implementação do serviço eletrónico europeu de portagem.
- *Lei n.º 49/2009*, de 5 de agosto, que regula as condições de acesso e exercício das atividades de comércio e indústria de bens e tecnologias militares.
- *Lei n.º 38/2015,* de 11 de maio, que altera a *Lei n.º 73/2009*, de 12 de agosto, que estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos órgãos de polícia criminal, e segunda alteração à *Lei n.º 49/2008*, de 27 de agosto, que aprova a *Lei de Organização da Investigação Criminal*
- *Lei n.º 73/2009*, de 12 de agosto, que estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos órgãos de polícia criminal.
- *Lei n.º 20/2014*, de 15 de abril, que procede à primeira alteração à *Lei n.º 36/2003*, de 22 de agosto.
- *Lei n.º 37/2014*, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na internet da Administração Pública denominado Chave Móvel Digital

- *Lei n.º 96/2015*, de 17 de agosto, que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública.
- *Lei n.º 103/2015*, de 24 de agosto criou, na Polícia Judiciária, uma unidade nacional, a Unidade Nacional de Investigação da Criminalidade Informática.
- *Código Penal,* aprovado pelo *Decreto-Lei n.º 48/95*, de 15 de março – Art.º 383.º, que estabelece o regime jurídico da violação do segredo de Estado por funcionário.
- *Decreto-Lei n.º 352/99*, de 3 de setembro, que estabelece o regime jurídico dos ficheiros informáticos da Polícia Judiciária
- *Decreto-Lei n.º 395/99*, de 13 de outubro, que estabelece o regime jurídico dos ficheiros informáticos dos Institutos de Medicina Legal de Lisboa, Porto e Coimbra.
- *Decreto-Lei n.º 62/2003*, de 3 de abril, altera o *Decreto-Lei n.º 290-D/99*, de 2 de Agosto, que aprova o regime jurídico dos documentos eletrónicos e da assinatura digital
- *Decreto-Lei n.º 116-A/2006*, de 16 de junho, que procede à criação do Sistema de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas e designa a ANS como autoridade credenciadora nacional (republicado).
- *Decreto-Lei n.º 62/2009*, de 10 de março, que procede à primeira alteração ao *Decreto-Lei n.º 7/2004*, de 7 de Janeiro, que transpõe para a ordem jurídica nacional a *Diretiva n.º 2000/31/CE*, do Parlamento Europeu e do Conselho, de 8 de Junho, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno.
- *Portaria n.º 8-A/2001*, de 3 de janeiro, que altera a *Portaria n.º 1178-E/2000*, de 15 de dezembro que determina que as peças processuais a apresentar em suporte digital devam sê-lo em disquete de 3,5" ou em CD-ROM
- *Decreto Regulamentar n.º 25/2004*, de 15 de julho, que regulamenta o *Decreto-Lei n.º 290-D/99*, de 2 de agosto, que aprova o regime jurídico dos documentos eletrónicos e da assinatura digital
- *Portaria n.º 469/2009*, de 5 de maio, que estabelece os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado.
- *Portaria n.º 1109/2009*, de 25 de setembro, que determina o suporte informático para os actos e processos de registo civil e regulamenta a reconstituição de actos e processos de registo.
- *Portaria n.º 189/2014*, de 23 e setembro, que procede à regulamentação necessária ao desenvolvimento da Chave Móvel Digital
- *Portaria n.º 286/2017*, de 28 de setembro, que define os modelos oficiais e exclusivos do cartão de cidadão, os elementos de segurança física que o compõem, os requisitos técnicos e de segurança a observar na captação da imagem facial e das impressões digitais do titular do pedido e ainda as medidas concretas de inclusão de cidadãos com necessidades especiais na sociedade de informação, a observar na disponibilização do serviço de apoio ao cidadão

Anexo D: Iniciativas e Ações de Sensibilização

Iniciativa	Promotor	Tipo	Finalidade
Curso de Cibersegurança e Gestão de Crises no Ciberespaço	IDN	Formação	Formação e Sensibilização
Exercício Cyber Perseu	Exército	Exercício	Sensibilização e Treino
MN CD E&T Nacional	Exército	Projeto	Requisitos de E&T
Curso de Curso de Planeamento de Operações de Ciberdefesa	IUM	Formação	Sensibilização e Treino
C-Days	CNCS	Conferência	Sensibilização
Curso Geral de Cibersegurança	CNCS	Formação	Formação e Sensibilização
Innovation Meets Cybersecurity: The Public-Private Cooperation Challenge	COTEC Portugal CNCS	Conferência	Sensibilização
"3rd eHealth Security Conference – Proteção do Hospital do Futuro"	SMPS	Conferência	Formação e Sensibilização
Competências em Cibersegurança	CNCS	Conferência	
RGPD – Regulamento Europeu de Proteção de Dados	CNCS	Conferência	Sensibilização
Mês Europeu da Cibersegurança	CNCS	Conferência	Sensibilização
Girls in ICT	CNCS	Conferência	Sensibilização
"Segurança da Informação e do Ciberespaço: Contributos para a Cibersegurança e Ciberdefesa de Portugal"	IDN	Seminário	Sensibilização
"Gerir a Segurança e a Privacidade na Transformação Digital	AFCEA	Conferência	Sensibilização
Cidades Inteligentes e Ciber Resiliência	AFCEA	Seminário	Sensibilização
Cybersecurity *Forum* 2017	AFCEA	Seminário	Sensibilização
Conferência Internacional sobre Cibersegurança	AFCEA	Conferência	Sensibilização
NetVivaeSegura	DECO & Google	Projeto	Sensibilização
Projeto InternetSegura	FCT DGE IPDJ PT Microsoft	Projeto	Sensibilização
Programa Crianças na Internet	GNR	Website	Sensibilização

Anexo E: Programas de Formação Superior em Cibersegurança

Curso	Instituições
• Mestrado em Cibersegurança e Informática Forense	• IPLeiria
• Curso de Pós-Graduação em Cibersegurança	• Universidade Europeia
• Mestrado em Segurança de Informação e Direito no Ciberespaço	• Escola Naval • Instituto Superior Técnico / ULisboa • Faculdade de Direito / ULisboa
• Mestrado em Segurança Informática	• Universidade do Porto
• Curso de Pós-Graduação em Cibersegurança e Ciberdefesa	• Academia Militar • Universidade do Minho
• Master em Cibersegurança	• IMF Business School
• Mestrado em Segurança Informática • Curso de Pós-Graduação em Segurança Informática	• Universidade de Coimbra
• Pós-graduação Cibersegurança e Inteligência Competitiva	• Universidade Lusófona

Índice de IDN Cadernos Publicados

III SÉRIE		
2018	28	Contributos para uma Estratégia Nacional de Ciberdefesa
2017	27	Economia da Defesa Nacional
	26	Novo Século, Novas Guerras Assimétricas? Origem, Dinâmica e Resposta a Conflitos não-Convencionais
	25	II Seminário IDN Jovem
	24	Geopolitics of Energy and Energy Security
	23	I Seminário IDN Jovem
	22	Entering the First World War
2016	21	Os Parlamentos Nacionais como Atores Dessecuritizadores do Espaço de Liberdade, Segurança e Justiça da União Europeia: O Caso da Proteção de Dados
	20	América do Sul: uma Visão Geopolítica
2015	19	A Centralidade do Atlântico: Portugal e o Futuro da Ordem Internacional
	18	Uma Pequena Potência é uma Potência? O Papel e a Resiliência das Pequenas e Médias Potências na Grande Guerra de 1914-1918
	17	As Ásias, a Europa e os Atlânticos sob o Signo da Energia: Horizonte 2030
	16	O Referencial Energético de Gás Natural Euro-Russo e a Anunciada Revolução do *Shale Gas*
2014	15	A Diplomacia Militar da China: Tipologia, Objetivos e Desafios
	14	Geopolítica e Geoestratégia da Federação Russa: a Força da Vontade, a Arte do Possível
	13	Memória do IDN
2013	12	Estratégia da Informação e Segurança no Ciberespaço
	11	Gender Violence in Armed Conflicts
	10	As Revoltas Árabes e a Democracia no Mundo
	9	Uma Estratégia Global para Portugal numa Europa em Crise
2012	8	Contributo para uma "Estratégia Abrangente" de Gestão de Crises
	7	Os Livros Brancos da Defesa da República Popular da China, 1998-2010: Uma desconstrução do Discurso e das Perceções de (in)Segurança
2011	6	A Arquitetura de Segurança e Defesa da Comunidade dos Países de Língua Portuguesa
	5	O Futuro da Comunidade de Segurança Transatlântica
	4	Segurança Nacional e Estratégias Energéticas de Portugal e de Espanha
	3	As Relações Energéticas entre Portugal e a Nigéria: Riscos e Oportunidades
2010	2	Dinâmicas Migratórias e Riscos de Segurança em Portugal
	1	Acerca de "Terrorismo" e de "Terrorismos"

II SÉRIE		
2009	4	O Poder Aéreo na Transformação da Defesa O Programa de Investigação e Tecnologia em Veículos Aéreos Autónomos Não-Tripulados da Academia da Força Aérea
	3	Conhecer o Islão
2008	2	Cibersegurança Segurança e Insegurança das Infra-Estruturas de Informação e Comunicação Organizacionais
	1	Conflito e Transformação da Defesa A OTAN no Afeganistão e os Desafios de uma Organização Internacional na Contra-subversão O Conflito na Geórgia

I SÉRIE		
2007	5	Conselho de Segurança das Nações Unidas Modelos de Reforma Institucional
	4	A Estratégia face aos Estudos para a Paz e aos Estudos de Segurança. Um Ensaio desde a Escola Estratégica Portuguesa
2006	3	Fronteiras Prescritivas da Aliança Atlântica Entre o Normativo e o Funcional
	2	Os Casos do Kosovo e do Iraque na Política Externa de Tony Blair
	1	O Crime Organizado Transnacional na Europa: Origens, Práticas e Consequências

idn cadernos

CIBERSEGURANÇA E POLÍTICAS PÚBLICAS

Este estudo, resultado de uma parceria entre o IDN e a ANEPE, analisa as políticas de cibersegurança de Portugal e Chile, identificando os seus principais elementos e desafios. Apresenta uma abordagem conceptual e contextual do ciberespaço, nomeadamente as suas principais caraterísticas e tendências, ameaças e riscos. No âmbito da cooperação multilateral, são analisados os principais fóruns em que o Chile e/ou Portugal participam, cujos instrumentos normativos refletem os consensos alcançados e influenciam as respetivas políticas nacionais no domínio da cibersegurança.

Caracterizam-se ainda fatores mínimos – conceitos, legislação especializada, arquitetura de cibersegurança, cooperação, cultura e políticas públicas – a considerar numa política nacional de cibersegurança. As políticas de cibersegurança de cada um dos países são estudadas individualmente e analisadas comparativamente à luz de cada fator mínimo.

idn Instituto da Defesa Nacional

ISSN 1647-9068
00029
9 771647 906000