ACADEMIA NACIONAL DE ESTUDIOS POLÍTICOS Y ESTRATÉGICOS

La Ciberseguridad y Protección de Datos Personales para las Fuerzas Armadas de Chile

Por

CAP (EJÉRCITO DE CHILE) SERGIO MIRANDA AGUAYO

Monografía Final presentada al programa de Pregrado de la Academia Nacional de Estudios Políticos y Estratégicos para optar al grado académico de Licenciado en Seguridad y Defensa**.**

Profesor tutor: Carolina Sancho Hirane

Noviembre, 2023

RESUMEN

Este informe titulado "La Ciberseguridad y Protección de Datos Personales para las Fuerzas Armadas de Chile", postula que la Política Nacional de Ciberseguridad (de las cuales se desprenden otras políticas), junto a las regulaciones y estándares internacionales en esta materia deben ser aplicadas en las Fuerzas Armadas, entendiendo que el avance de la tecnología ha traído beneficios para las organizaciones, pero también una serie de riesgos que debe ser mitigados. Es así, como la presente investigación analiza las principales normas, proyectos de ley y estándares internacionales relativos a ciberseguridad y protección de datos personales, describiendo el impacto que esta tiene para las Fuerzas Armadas de Chile desde una perspectiva organizacional, para finalmente establecer los desafíos que esto implica, pudiendo de esta forma sugerir buenas prácticas asociadas a estos desafíos.

SUMMARY

"Cybersecurity and Protection of Personal Data for the Armed Forces of Chile", postulates that the National Cybersecurity Policy (from which other policies emerge), together with the regulations and international standards in this matter, must be applied in the Armed Forces, understanding that the advancement of technology has brought benefits to organizations, but also a series of risks that must be mitigated. This is how this research analyzes the main regulations, bills and international standards related to cybersecurity and protection of personal data, describing the impact that this has for the Chilean Armed Forces from an organizational perspective, to finally establish the challenges that this implies, thus being able to suggest good practices associated with these challenges.

INTRODUCCIÓN

La presente investigación realiza un análisis de la Política Nacional de Ciberseguridad (de la cual se desprenden otras políticas y documentos de importancia), junto a las regulaciones y estándares en materia de ciberseguridad, con especial atención en la protección de datos personales, para describir el impacto que esto tiene en las Fuerzas Armadas chilenas desde el punto de vista organizacional, estableciendo algunos desafíos que esto implica y las buenas prácticas asociadas a estos.

El avance de la tecnología ha tenido diversos impactos positivos en todos los ámbitos de la sociedad, los cuales han generados "transformaciones relevantes también en los usos y

miradas de la ciudadanía"[1]. Sin embargo, el uso de nuevas tecnologías trae aparejado una serie de riesgos, frente a los cuales es menester generar mecanismos que permitan aminorar su impacto, señalando que este nuevo dominio concebido como el ciberespacio generan problemas como la "ambigüedad que ofrece este medio para posibles elementos hostiles, y el amplio ámbito sobre el que se producen sus efectos, que sobrepasan las fronteras físicas y los mecanismos institucionales"[2]. Es por ello, que la ciberseguridad y su énfasis para efectos de este estudio en la protección de datos personales se presentan como una condición que debe ser alcanzada, para que las interacciones en el ciberespacio sean con la menor cantidad de riesgos posibles. Lo señalado anteriormente, presenta una serie de medidas que buscan generar un ambiente seguro, con pleno respeto a las garantías de las personas, entendiendo que "la privacidad es nuestro modo de vendarle los ojos al sistema para que nos trate con imparcialidad y justicia"[3]. Frente a esto, las Fuerzas Armadas desde el punto de vista organizacional no pueden estar ajenas a esta regulación, debiendo adoptar sus políticas y procedimientos a estos, teniendo presente que, en Chile, al igual que en Europa y numerosos países, existe legislación en materia de ciberseguridad y protección de datos personales, la que está radicada principal pero no únicamente en la Política Nacional de Ciberseguridad y la Ley N.º 19.628[4].

De esta manera, la investigación plantea como objetivo general, analizar la Política Nacional de Ciberseguridad (con las políticas y documentos que se irradian a partir de ella), regulaciones y estándares internacionales en materia de ciberseguridad y protección de datos personales, vigentes en Chile. Para el desarrollo de la investigación se proponen tres objetivos específicos, los cuales son: en primer lugar a describir la Política Nacional de Ciberseguridad, las regulaciones y estándares internacionales vigentes en la materia. En segundo lugar, se describirá el impacto que lo anteriormente señalado tiene para las Fuerzas Armadas de Chile desde el punto de vista organizacional y finalmente en tercer lugar se busca establecer los desafíos que esto implica, sugiriendo buenas prácticas asociadas a esta materia.

A raíz de lo anteriormente expuesto, se ha escogido bibliografía pertinente a la investigación, clasificándose en políticas públicas, regulaciones (tanto vigentes, como en proyectos de ley), estándares internacionales, así como literatura nacional y extranjera.

1- CIBERSEGURIDAD Y POLÍTICA PÚBLICA

En los últimos años, la administración del Estado ha generado instancias en las cuales ha buscado hacerse cargo del fenómeno de la ciberseguridad y la protección de datos personales, entendiendo por una parte el impacto que está generando en el mundo y observando por otra, el desarrollo que los otros Estados y entes internacionales están impulsando en esta materia,

[1] MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA. 2017. Política Nacional de Ciberseguridad. Disponible en: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%c3%adtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y .
[2] GARCÍA VÁSQUEZ, Borja. 2021. "El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra". Revista Chilena de Derecho y Tecnología. Santiago, (10) p. 44.
[3] VÉLIZ, Carissa. 2021. "Privacidad es poder. Datos, vigilancia y libertad en la era digital". Penguin Random House Grupo Editorial. Mexico. (1). p. 236.
[4] REUSSER MONSÁLVEZ, Carlos. 2021. "Derecho al olvido. La protección de datos personales como límites a las libertades informativas". DER Ediciones. Chile. (2). p.196.

que se traducen por ejemplo en el desarrollo de regulaciones, creación de entes especializados en esta materia, desarrollo de profesionales y adopción de una cultura en este campo.

De esta forma, se describen a continuación la Política Nacional de Ciberseguridad, junto a otras políticas e instrumentos que se desprenden de ella relativas a ciberseguridad y protección de datos personales.

Política Nacional de Ciberseguridad

Bajo la premisa de que Chile, debía "ponerse al día en materia de seguridad porque cualquier error o ataque exitoso puede vulnerar el bienestar y los derechos de chilenas y chilenos, afectar intereses particulares y comunes, afectar servicios críticos para el funcionamiento del país[5]", se dictó en el año 2017 la Política Nacional de Ciberseguridad, como un instrumento orientado a establecer parámetros que permitan un ciberespacio[6] seguro, junto con combatir la ciberdelincuencia, fomentando la concientización en esta materia, para comprender este fenómeno y disminuir la ignorancia que ha operado por años.

Es así, como a la fecha de esta política, el país contaba con una gobernanza dispersa en materia de ciberseguridad, junto con una normativa legal pionera en su época, pero hoy abiertamente desactualizada en comparación a los estándares internacionales actualmente vigentes, como lo es el Reglamento General de Protección de Datos, imperante en la Unión Europea[7].

La política a su vez define un concepto importante, como es el de la infraestructura crítica de la información, señalando que "comprende 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 seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado[8]".

En esta misma línea, la política permitió la creación de un CSIRT (por sus siglas en inglés), a cargo de la prevención, monitoreo, gestión y respuesta a incidentes de seguridad de la información a nivel nacional[9]. Este órgano vino a reemplazar a la red de conectividad del Estado, produciéndose de esta forma una transición y una modernización en cuanto a institucionalidad.

La política también manifestó la importancia de la protección de los datos personales de la ciudadanía, de parte de los organismos públicos y privados de la nación, reforzando una cultura de ciberseguridad. Esta cultura trae aparejado la sensibilización de sus aspectos más relevantes y la formación que debe existir para preparar no sólo a la población civil, sino

[5] MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA, op. Cit. (2017).p.5.
[6] La política, definió al Ciberespacio como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren.
[7] Su nombre real es REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
[8] MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA, op. Cit. (2017).p.16.
[9] Ibídem.

también a profesionales capacitados que puedan abordar los desafíos que esta materia trae consigo.

Otro aspecto relevante de esta política fue impulsar la institucionalidad en materia de ciberseguridad[10], mediante el compromiso de generar un proyecto de ley que aborde esto, entendiendo el aporte de las capacidades de la Defensa Nacional a formación de un ciberespacio libre, abierto, seguro y resiliente para el país[11], es que se comprometió también a la redacción de una Política Nacional de Ciberdefensa, ambos puntos se hablaran más adelante.

Finalmente, el 2023 el gobierno de Chile elaboró una nueva Política Nacional de Ciberseguridad, sin embargo, a la fecha esta no ha sido publicada para proceder a su análisis[12].

1.1- OTROS DOCUMENTOS VINCULADOS A LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

A) Libro de la Defensa Nacional 2017

El libro de la Defensa Nacional de Chile del año 2017, constituyó un documento con diversos desafíos para este sector, sin embargo, para los efectos del presente estudio interesa los compromisos que se adoptaron en materia de ciberseguridad, toda vez que este libro buscó materializar la primera política nacional de ciberdefensa (compromiso inserto en la Política Nacional de Ciberseguridad) considerando los impactos que el uso de la tecnología estaba teniendo, sumado a la noción de ciberespacio como otro flanco en el cual se deben tomar los resguardos necesarios por todas las actividades que allí ocurren, tanto de carácter lícito como ilícito. Es importante destacar que este documento declara que "la Defensa Nacional debe generar nuevas capacidades para proteger la confidencialidad, integridad y disponibilidad de la información, con el objeto de proteger a las personas y a sus intereses, tanto en territorio nacional como en el exterior", lo cual expone la preocupación de las Fuerzas Armadas sobre estos tópicos los cuales no habían sido abordados en el libro de la defensa anterior del año 2010, el cual sólo hacía mención al ciberespacio como un "nuevo concepto dentro de la noción de campo de batalla"[13], sin ahondar en otros contenidos o políticas complementarias, como tampoco esgrimir esfuerzos en resguardar la información que transita al interior del sector defensa, como un activo vital para el desarrollo de sus operaciones. Ahora bien, la ciberseguridad y la protección de datos personales ni siquiera fueron mencionados en lo absoluto en los libros de defensa de Chile en los años 2002 y 1997.

[10] La política destaca que las funciones de este organismo serán la gestión de relaciones interinstitucionales, gestión de incidentes, funcionamiento como punto de contacto nacional e internacional en este ámbito, función comunicacional, función normativa técnica y asesora en normativa general, función de seguimiento y evaluación de medidas.
[11] Ibíd.
[12] (30 de mayo de 2023). Gobierno presentó su propuesta de nueva Política Nacional de Ciberseguridad. *CSIRT.* Disponible en https://www.csirt.gob.cl/noticias/gobierno-presento-su-nueva-politica-nacional-de-ciberseguridad/
[13] MINISTERIO DE DEFENSA NACIONAL. 2010. Libro de la Defensa Nacional de Chile. Disponible en: https://www.resdal.org/ultimos-documentos/libro-blanco-chile-2010.html p.176.

B) Política Nacional de Ciberdefensa.

Como una respuesta a los lineamientos de la Política Nacional de Ciberseguridad, el Ministerio de Defensa aprobó en el año 2017, la Política de Ciberdefensa, la cual se erigió como "la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa[14]".

Esta política, destaca la importancia que tiene para la nación el ciberespacio, el cual merece protección al igual que los espacios marítimos, terrestre y aéreo. En síntesis, el ciberespacio como concepto da cuenta de la existencia de un nuevo dominio, dimensión o ambiente que es usado en forma creciente por personas, organizaciones, empresas, gobiernos e instituciones las cuales se ven transformadas al incorporarlo en su gestión[15]. Con este instrumento, Chile reconoce que los ambientes digitales, son igualmente expresión de la soberanía, motivo por el cual merece la protección de los órganos de la administración del Estado, entre ellos los organismos de las Fuerzas Armadas.

Además, la Política de Ciberdefensa señaló que "El Ministerio de Defensa Nacional promoverá el desarrollo de una industria que sirva a los objetivos estratégicos para la Defensa Nacional, y que le permita mantener un adecuado nivel de independencia y soberanía tecnológica[16]", destacando así la importancia que para el sector defensa tiene el desarrollo tecnológico. Adicionalmente, el documento señala que "El Estado de Chile considera que un ciberataque puede llegar a ser tan dañino como un ataque armado[17]", pudiendo ejercer su derecho a la legítima defensa y debiendo establecer mecanismos de cooperación internacional.

Es importante resaltar, que la presente política estableció el desarrollo de capacidades en materia de defensa nacional, para lo cual identificó diferentes requerimientos[18], ahora bien, a raíz de esto, se adoptaron compromisos de reorganización orgánica como lo fueron la creación de los CSIRT para cada una de las Fuerzas Armadas.

Por último, en cuanto a los instrumentos que se deberán generar a raíz de esta política, es preciso destacar la adecuación del derecho internacional humanitario y del derecho internacional de los conflictos armados al ciberespacio, junto la preparación doctrinaria por parte de las Fuerzas Armadas y la inversión de cada uno de los organismos que las componen en cuanto al gasto asociado a ciberseguridad, debiendo considerarlos en la planificación de sus presupuestos anuales.

---

[14] BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2017. Decreto Nª 3 que Aprueba Política de Ciberdefensa. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf. p. 1.

[15] SANCHO HIRANE, Carolina. 2018. Ciberinteligencia: Contextualización, Aproximación conceptual, Características y Desafíos. Cuaderno de Trabajo (1), 1-32. Disponible en: https://www.publicacionesanepe.cl/index.php/cdt/article/view/911/580. P.7.

[16] Ibíd.

[17] Ibíd.

[18] Ibíd.

C) Política de Defensa Nacional

El año 2020, el ejecutivo estimó que los libros de defensa que se venían publicando desde el año 1997, debían avanzar a una política, la cual manifiesta que su objetivo es que se "reafirma y actualiza los fundamentos expresados en anteriores Libros de la Defensa, como también avanza en conceptos y orientaciones necesarias para la conducción política de la Defensa[19]".

Es importante destacar, que mediante esta política las Fuerzas Armadas comprenden que su actuar no es ajeno a los desafíos que imponen los avances de las tecnologías, reconociendo los déficits regulatorios que tenemos en la materia, lo que incrementa las posibilidades de ser vulnerables ante un ciberataque, con las perniciosas consecuencias que esto puede traer para la seguridad de la población y del país en su conjunto.

Tomando en consideración los postulados de la política nacional de ciberseguridad y la política de ciberdefensa es que el documento plantea el desafío del sector defensa para "mantenerse a la vanguardia en las tecnologías, procedimientos, equipamiento y capacitación del capital humano responsable de la ciberdefensa, para contribuir de manera decisiva al esfuerzo de ciberseguridad del país[20]", adoptando una actitud proactiva contra las amenazas que se presentan en esta área.

Finalmente, para el desarrollo de las capacidades estratégicas del país, la Política de Defensa Nacional, hace alusión a capacidades en ciberdefensa, considerándolo como un tópico de alta relevancia, requiriendo por ende un aumento de la ciberseguridad tanto de la infraestructura crítica de las Fuerzas Armadas, como del Estado en general, el desarrollo de ciberoperaciones, la formación de capital humano "tanto especializado, como en los niveles de toma de decisiones"[21], avanzar en la adecuación de las organizaciones, la generación de doctrinas, entre otras.

D) Política Nacional de Inteligencia Artificial

Elaborar recomendaciones de política pública en materia de inteligencia artificial no es una tarea sencilla, porque es una tecnología que está en constante desarrollo, y porque un mal diseño de políticas públicas puede perjudicar seriamente el desarrollo del país en esta materia[22], no obstante, el año 2021, también fue importante en materia de producción de instrumentos asociados a los contenidos que se han abordado en el presente estudio, toda vez que el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, publicó la Política Nacional de Inteligencia Artificial (en adelante "IA") como un esfuerzo político por visualizar la preponderancia que esta tecnología va a generar en el desarrollo del país, esbozando compromisos para incorporar a la IA en diversos sectores, generando a su vez alianzas con otras políticas estatales.

---

[19] MINISTERIO DE DEFENSA NACIONAL. 2020. Política de Defensa Nacional de Chile 2020. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defensa.cl/wp-content/uploads/2023/06/POL%C3%8DTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf p.7.
[20] Ibíd.
[21] Ibíd.
[22] ARAYA PAZ, Carlos. 2020. Desafíos legales de la inteligencia artificial en Chile. Revista Chilena De Derecho Y Tecnología, 9(2), 257–290. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/54489/64369. p.281.

Esta política, pone de manifiesto la brecha profesional que existe en Chile en materia de tecnologías, de las cuales las Fuerzas Armadas no se encuentran ajenas. Sin ir más lejos, el documento señala que "el escenario actual en Chile es tal que existen marcadas brechas en capacidad y talentos en todos los niveles para áreas relacionadas con la transformación digital[23]".

La ciberseguridad y ciberdefensa también es motivo de estudio para esta política, manifestando inclusive que "Un ciberataque puede llegar a ser tan efectivo y perjudicial como un ataque armado, y más aún ante posibles usos bélicos de estos sistemas automatizados[24]". Con este enunciado, la política se encarga de señalar los aportes que podría realizar la inteligencia artificial a esta área "tanto en acciones de legítima defensa, como efectos de disuasión y manejo de crisis"[25], lo cual implica tener a la vista los riesgos e implicancias que esta tecnología puede traer aparejado.

Es por ello, que este documento promueve que las próximas políticas públicas en materia de ciberseguridad y ciberdefensa, contemplen a la Inteligencia Artificial como un factor de relevancia.

Además, se propone que la inteligencia artificial sea una herramienta que contribuya a enfrentar los ataques informáticos, los cuales se han incrementado exponencialmente en los últimos años, no estando ajenos las Fuerzas Armadas, en especial si se piensa en el ataque informático sufrido por el Estado Mayor Conjunto el año 2022[26] y el Ejército de Chile el año 2023[27].

E) Construyendo la Ciberseguridad en Chile

Cómo último documento para ser analizado, la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación, a través de la Mesa de Ciberseguridad dependiente del Senado de Chile, elaboró el año 2023 el documento titulado "Construyendo la Ciberseguridad en Chile".

En la elaboración de este documento, se ahondó sobre lo ya avanzado, proponiendo nuevos caminos para que sean considerados tanto "por el poder ejecutivo, como por el legislativo, dando así un fuerte un impulso al desarrollo de la ciberseguridad nacional"[28].

---

[23] MINISTERIO DE CIENCIA, TECNOLOGÍA, CONOCIMIENTO E INNOVACIÓN. 2021. Política Nacional de Inteligencia Artificial. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf. p.24.

[24] Ibíd.

[25] Ibíd.

[26] GONZÁLEZ, C. (23 de septiembre de 2022). Cerca de 400 mil correos filtrados, contenido estratégico y sumarios administrativos: Lo que se sabe del hackeo al EMCO. *EMOL*. https://www.emol.com/noticias/Nacional/2022/09/23/1073631/detalles-hackeo-masivo-emco.html.

[27] GONZÁLEZ, A. (29 de mayo de 2023). Ejército de Chile sufre ataque informático en su red interna. *BiobioChile*. Disponible en: https://www.biobiochile.cl/noticias/nacional/chile/2023/05/29/ejercito-de-chile-sufre-ataque-informatico-en-su-red-interna.shtml.

[28] BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Construyendo la Ciberseguridad en Chile. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/89176/3/Construyendo_la_Ciberseguridad_en_Chile.pdf. p. 9.

Dentro de los aportes del presente documento, se encuentran diversas propuestas tendientes a una mejor institucionalidad en materia de ciberseguridad que permita aunar los esfuerzos públicos y privados que permitan la colaboración de los múltiples sectores de este ecosistema, junto con propulsar un sistema de gobernanza que actúe coordinadamente y que defina roles y responsabilidades robustas asociadas a los desafíos que impone la ciberseguridad y la protección de datos personales. A lo anterior, se suman los esfuerzos en fomentar la formación de profesionales especializados en la materia, que cuenten con los incentivos necesarios y que aporten a combatir tanto la higiene informática, como la analfabetización, de la cual el país acaece. A su vez, se requiere una asignación de recursos consciente y eficiente, que permita una adecuada inversión en estas materias, comprendiendo la importancia de estos activos para el desarrollo del país, puesto que a la fecha aún "muchos ven la ciberseguridad como un gasto, y no una inversión que permite no sólo cuidar sus activos, sino defenderse de un potencial daño reputacional"[29].

Es necesario, recalcar el aporte de este documento para que se generen instancias que impulsen el talento humano en ciberseguridad, reconociendo la amplia brecha que se distingue en este sector. Señala el documento que "Humanos intervienen en toda la cadena de la ciberseguridad, desde el diseño de sistemas y programas (software) seguros, la implementación de tecnología como los cortafuegos o los sistemas de detección y prevención de ataques, la repuesta a incidentes y el análisis forense, hasta la gestión de crisis con la comunicación y otras acciones asociadas[30]".

Una propuesta interesante del documento es crear en Chile una unidad equivalente al Estonian Defence League's Cyber Unit[31] que agrupa miembros especialistas en ciberseguridad tanto públicos como privados, para la defensa del ciberespacio.

Continuando con el análisis, se destaca la importancia de la protección y seguridad de los servicios esenciales e infraestructura crítica, factor donde las Fuerzas Armadas deben participar, coordinadamente con el sector público y privado en ciberejercicios, como asimismo en la cooperación que debe existir entre los diversos CSIRTs, incluido los de las Fuerzas Armadas por separado y en su conjunto.

Se plantea como desafío para el sector Defensa combatir la amenaza de la desinformación, debido al impacto que puede tener en las operaciones militares. Sobre este punto, el documento expone que "Se requiere que las FF.AA. y de Orden y Seguridad, mantengan capacidades para enfrentar estas nuevas dimensiones del conflicto, las que pueden servir como potenciadoras de una fuerza militar en operaciones convencionales, pero también actuar como una variable independiente en operaciones militares distintas a la guerra[32]". Siguiendo esta línea, se señala que se requiere una actualización doctrinaria al interior de las Fuerzas Armadas, que pueda hacerse cargo de esta amenaza, estableciendo lineamientos coherentes. Ergo, la falta de preparación, conocimientos, capacitación provoca una severa deficiencia y retraso en comparación con los países más avanzados en esta materia, los cuales "están empleando la estrategia de defensa cibernética activa para defender sus activos críticos

[29] Ibíd.
[30] Ibíd.
[31] Ibíd.
[32] Ibíd.

y neutralizar las amenazas"[33], mientras que las Fuerzas Armadas de Chile emplean un enfoque reactivo del problema, debiendo evolucionar a una defensa proactiva.

Luego de sus 7 capítulos, el documento propone finalmente la conformación de un "Foro Nacional de Ciberseguridad, que convoque de manera organizada a expertos y expertas a fin de canalizar inquietudes e iniciativas sobre la materia, y que esté radicada en el Senado de Chile"[34].

De esta manera, se espera que las Fuerzas Armadas aporten capital humano para que forme parte de este órgano consultivo, de manera de contribuir a la generación de ideas e instancias que permitan una ciberseguridad robusta para el país.

1.2- NORMATIVA

En el ámbito de la ciberseguridad y la protección de datos personales, el país cuenta con regulación en esta materia, no obstante, esta se encuentra desfasada o es incipiente, en comparación a los estándares internacionales que imperan en la materia.

A modo de ejemplo, en la década de los 90, Chile marcaba un hito al ser el primer país de Latinoamérica en tener la primera ley de protección de datos personales, la cual en la actualidad es "incapaz de hacer frente a las necesidades actuales surgidas de los avances tecnológicos y la capacidad de procesar grandes volúmenes de datos en forma automatizada"[35].

Para conocer que ha pasado desde aquella primera normativa, a las necesidades legislativas que este fenómeno requiere y necesita, se describen a continuación las principales normativas en la materia, junto con los actuales proyectos de ley en discusión, que buscan darle una vuelta al paradigma de obsolescencia e inexistencia legal, imperante en esta área.

A) Constitución Política de la República

La Carta fundamental, reguló a través de la Ley N.º 21.096 el derecho a la protección de datos personales, incorporándolo en el capítulo tercero "de los Derechos y Deberes Constitucionales", en específico su artículo 19 N° 4[36], amparado a su vez dentro del catálogo de derechos fundamentales tutelados por el recurso de protección[37]. Lo señalado anteriormente, incorporó de manera reciente al artículo 19 N.°4 un componente que no estaba considerado, el cual es la protección de datos personales, señalando que "el tratamiento y

[33] Ibid.
[34] Ibid.
[35] BORDACHAR BENOIT, Michelle. 2022. ¿Cómo y quiénes cuidan nuestros datos? Legislaciones vigentes en países Latinoamericanos (en línea). En: *DerechosDigitales*. Disponible en: https://www.derechosdigitales.org/17759/dia-de-la-proteccion-de-los-datos-personales/.
[36] El artículo en concreto señala que la Constitución asegura a todas las personas "4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley."
[37] CONTRERAS VÁSQUEZ, Pablo. 2020. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Revista Estudios Constitucionales, 18(2), 87-120. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.cl/pdf/estconst/v18n2/0718-5200-estconst-18-02-87.pdf. p.112. En relación al recurso de protección, la decisión de reconocer explícitamente el derecho a la autodeterminación informativa en el art. 19 No. 4 de la Constitución tenía entre otros objetivos el de asegurar su tutela a través de la acción o recurso de protección, establecido en el art. 20 de la Constitución.

protección de estos datos se efectuará en la forma y condiciones que determine la ley", recalcando la urgencia que existe en la actualidad de contar con una norma actualizada que operativice el mandato constitucional. Ahora bien, la ciberseguridad en sí, no tiene una regulación constitucional concreta, como lo señalado anteriormente. Sin embargo, el fallido borrador constitucional del año 2022 intentó regular el "Derecho a la seguridad informática[38]", el cual señalaba elementos concretos de esta área.

De esta forma, la Constitución Política de la República otorga actualmente en Chile al dominio legal, la regulación y el tratamiento de los datos personales, como veremos a continuación.

B) Ley N.º 19.628

Como señalamos anteriormente, la normativa de protección de datos personales en Chile data de 1999, llevó por nombre "sobre protección de la vida privada" lo que en la práctica no ocurre, "sino que establece reglas relativas al mercado de los datos personales, especialmente el tratamiento de los datos de carácter económico, bancarios y comercial (morosidades), cuyo principal gestor en esa época era la empresa DICOM"[39].

Siendo este su origen, las múltiples modificaciones sobre esta normativa, han seguido orientadas al ámbito financiero y comercial, sin ser a la fecha una respuesta efectiva a las actuales necesidades que una sociedad inmersa en la tecnología exige, por lo que mientras que la mayoría de los países occidentales (como los países de Unión Europea que se rigen por el RGPD, Estados Unidos, México, Ecuador, Argentina, Perú y Costa Rica por nombrar algunos)[40] avanzan en la defensa del derecho a la privacidad y a la protección de datos personales, Chile sigue con una ley que tiene más de 20 años.

Ahora bien, debido a la antigüedad de esta ley y la falta de modificaciones sustanciales, esta ha quedado desactualizada en cuanto a derechos, principios, autoridades, obligaciones, procedimientos y mecanismos sancionatorios, toda vez que existe en la actualidad el Reglamento General de Protección de Datos Personales (o RGPD por sus siglas en español) que no sólo fue una revolución en esta materia, sino que también ha servido de inspiración para los países no europeos.

Es por esta razón, que actualmente se discute en el Congreso una modificación sustancial a lo actualmente regulado, recaídos sobre los boletines Nºs 11.144-07 y 11.092-07.

Este proyecto incorpora tópicos relevantes entre los que se encuentran:

Contiene un capítulo relativo al tratamiento de datos personales por parte de los Órganos de la Administración del Estado (entre ellos las Fuerzas Armadas)[41]; Se establece un régimen de tratamiento de datos especial, para los datos relacionados directamente con la Defensa

[38] La propuesta señalaba que "Todas las personas, individual y colectivamente, tienen el derecho a la protección y promoción de la seguridad informática. El Estado y los particulares deberán adoptar las medidas idóneas y necesarias que garanticen la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan los sistemas informáticos que administren, salvo los casos expresamente señalados por la ley".
[39] DONOSO ABARCA, Lorena y REUSSER MONSÁLVEZ, Carlos. 2022. La protección de los datos personales en Chile. Santiago. Der Ediciones. ISBN: 978-956-405-122-2. p.13.
[40] BORDACHAR BENOIT, Michelle. op. Cit. (2022).
[41] Titulo IV del proyecto de ley.

Nacional[42]; Regula la transferencia internacional de datos personales[43]; Se crea la Agencia de Protección de Datos Personales; Se aumentan considerablemente las sanciones para los infractores en materia de protección de datos personales[44] y Se contempla la posibilidad de establecer voluntariamente un modelo de cumplimiento el cual deberá designar un delegado de protección de datos personales[45].

De esta manera, a la fecha el proyecto se encuentra en tercer trámite constitucional ante el senado y no existe previsión de su avance, sin perjuicio de la urgencia y relevancia que esta materia ha tomado en los últimos años.

C) Ley 21.459

Este cuerpo legal, vino a reemplazar a la ley N.° 19.233, que databa del año 1993, la cual tenía nula aplicación, debido a que a la época de su concepción no existía el avance tecnológico, principalmente asociado al internet con el que contamos el día de hoy, por lo que los tipos penales eran indeterminados, lo que dificultaba su persecución e investigación.

De esta forma, se incorporan 7 nuevos tipos penales[46], los cuales por su relevancia forman a la vez parte de los delitos bases de la Ley N.º 20.393, debiendo ser incorporados en los modelos de prevención de delitos de las organizaciones.

Adicionalmente, esta normativa busca adaptarse al Convenio de Budapest sobre ciberdelincuencia, del cual Chile es adherente, el cual "es el primer instrumento internacional que se hizo cargo de la necesidad de cooperación entre estados frente a la utilización ilícita del ciberespacio"[47].

D) Decreto N.º 273

Como una respuesta a las obligaciones que impuso la entrada en vigor de la ley de delitos informáticos, se dictó el 2022 el Decreto N.º 273 que estableció la obligación de reportar incidentes de ciberseguridad. "Todas las instituciones por más precavidas y diligentes que sean son objeto de ciberataques y también de sufrir ciberincidentes, sin embargo, lo importante en una democracia es que la sociedad cuente con la información suficiente para saber si hubo o no alguna acción u omisión de la autoridad que propiciara ese ciberataque o ciberincidente"[48].

[42] Artículo 24°, letra b) del proyecto de ley.
[43] Artículo 27° del proyecto de ley.
[44] Artículo 35° del proyecto de ley.
[45] Artículo 49º del proyecto de ley.
[46] Se incorporan los delitos de Ataque a la integridad de un sistema informático, Acceso ilícito, Interceptación ilícita, Ataque a la integridad de los datos informáticos, Falsificación informática, Receptación de datos informáticos, Fraude informáticos y Abuso de dispositivos.
[47] MINISTERIO DE DEFENSA NACIONAL. op.cit. 2017, p. 157.
[48] LUZ ÁLVAREZ, Clara. 2023. Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes en instituciones públicas. Revista Chilena De Derecho Y Tecnología, 11(2), 183–210. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/65502/72154 .p.192

Con esta regulación, los jefes de servicio de los órganos públicos deben comunicar los incidentes de ciberseguridad que les afecten al CSIRT dependiente del Ministerio del Interior, no pudiendo exceder del plazo de 3 horas desde la constatación del suceso.

E) Ley 21.180

En el año 2019, se publicó en el Diario Oficial la Ley de Transformación Digital del Estado que viene a modificar la forma en que desarrollan los procedimientos administrativos al interior de la Administración del Estado, otorgando "mayor certeza, seguridad y velocidad en la entrega de servicios a las personas, junto con una mayor transparencia de los procesos y actuaciones del Estado en su relación con los ciudadanos"[49].

Esta modificación, no ha estado exenta de dificultades para las entidades públicas, lo que ha obligado a aplazar los plazos de implementación de esta regulación, teniendo como plazo fatal, el 31 de diciembre del año 2027[50]. Las Fuerzas Armadas no están exentas de estos plazos y tienen el desafío de modernizar sus sistemas de aquí a los próximos 4 años.

Esta ley, estableció una serie de reglamentos serían dictados posterior a su establecimiento sobre diversos tópicos de la regulación. Además, a través de reglamento se comprometió la elaboración de una serie de normas técnicas que precisarían la aplicación de este cuerpo legal.

Dichas normas técnicas se publicaron en agosto del 2023, y la primera de estas normas, según su artículo primero tiene por objeto definir los estándares y establecer las directrices técnicas sobre seguridad de la información y ciberseguridad, que deberán cumplir los órganos de la Administración del Estado para resguardar la confidencialidad, integridad, disponibilidad de la información y la infraestructura informática, de las plataformas electrónicas que sustentan sus procedimientos administrativos.

En concreto, esta norma técnica establece la obligación de los órganos de la Administración del Estado de elaborar una política de seguridad de la información y ciberseguridad[51].

F) Proyecto de Ley de Marco de Ciberseguridad

Actualmente, se encuentra en discusión el proyecto de ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, cuyo mensaje señala que "Para el adecuado funcionamiento de la ciberseguridad en el país, es necesario gestionar los riesgos

[49] Información extraída del sitio web https://digital.gob.cl/transformacion-digital/ley-de-transformacion-digital/#:~:text=El%20%C3%BAltimo%20de%20ellos%20fue,9%20de%20junio%20de%202022.
[50] El aplazamiento fue en virtud de la Ley N.° 21.464 del año 2022.
[51] El artículo 5° de la Norma Técnica precisó que el objetivo de la política era establecer las directrices generales en materia de seguridad de la información y ciberseguridad dentro del órgano, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan. Asimismo, deberá contener la visión estratégica del respectivo órgano de la Administración del Estado respecto de la seguridad de la información y ciberseguridad. La Política tendrá como objetivo, además, velar por la preservación, confidencialidad, integridad y disponibilidad de la información, considerando estándares de seguridad de la información y la privacidad como parte del diseño inicial.

e implementar los más exigentes estándares que otorguen confianza y seguridad, en las instituciones públicas como privadas[52]".

La elaboración de esta ley es parte de los compromisos de la Política Nacional de Ciberseguridad, la cual busca crear las condiciones necesarias para institucionalizar esta materia a nivel nacional, con un marco regulatorio que imponga obligaciones para las organizaciones públicas y privadas, basadas en la colaboración por un ciberespacio más seguro.

Entre las principales innovaciones de este proyecto, se encuentra la creación de la Agencia Nacional de Ciberseguridad, que será el órgano encargado de fiscalizar y regular las directrices en materia de ciberseguridad, generando las instancias de coordinación necesaria para la protección de los intereses nacionales.

Este proyecto, también busca regular tanto la infraestructura crítica de la información y los sectores que serán considerados prestadores de servicios esenciales, que por ende manejan infraestructura crítica. A estos servicios, se les impondrán una serie de obligaciones y deberes de y resolución de incidentes.

Se propone la creación del Registro Nacional de Incidentes de Ciberseguridad, a cargo de la Agencia Nacional de Ciberseguridad.

También, se propone la creación de un CSIRT nacional que reemplace al actual y que coordine tanto con los diversos CSIRT sectoriales, como con los CSIRT internacionales.

Adicionalmente, el proyecto busca la creación de un CSIRT de gobierno y CSIRT para el sector Defensa, el cual es perteneciente al Estado Mayor Conjunto del Ministerio de Defensa Nacional, "es responsable de la coordinación y protección de la infraestructura de la información calificada como crítica del sector defensa"[53]. El proyecto, le encomienda al Ministerio de Defensa Nacional la elaboración de un reglamento que precise los contenidos de esta obligación.

Actualmente, el proyecto se encuentra en segundo trámite constitucional en la Cámara de Diputados, donde se han incorporado indicaciones al proyecto, de manera tal que no existe previsibilidad de su pronta publicación en el Diario Oficial.

1.3- ESTÁNDARES INTERNACIONALES

Sumado a las políticas y las regulaciones, existen estándares y buenas prácticas que, sin ser obligatorias, sirven como una importante guía a las organizaciones para contar con mejores herramientas en materia de protección y datos personales.

Actualmente, los niveles de dependencia que poseen las organizaciones con la información, los sistemas que la gestionan, la infraestructura que la soporta y el personal técnico que la opera es cada vez mayor, requiriendo implementar diversos sistemas de gestión al interior de las TICs para poder alcanzar sus objetivos. Es así, como diversas necesidades de gestión

[52] SENADO. 2022. Proyecto de Ley: Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.
[53] Ibíd.

surgen al interior de las organizaciones desde las TICs y normativas que le son aplicables, lo cual genera la necesidad de implementar mecanismos que posibiliten el gobierno de TICs, la gestión de servicios TI, la gestión del desarrollo y calidad de software, gestionar la seguridad de la información, la ciberseguridad, la continuidad del negocio, los incidentes de seguridad de la información, entre otros[54].

Para los efectos de este estudio, se hará un resumen de las principales normas ISO[55] que tienen bastante utilidad en las organizaciones comprometidas con la ciberseguridad.

A) ISO 27.001: Es un estándar que permite en las organizaciones tanto públicas como privadas, la implementación de un Sistema de Gestión de Seguridad de la Información (en adelante "SGSI"). "El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos"[56].

B) ISO 27.701: Esta norma, se presenta como una extensión de la ISO 27.001, centrándose en los datos de carácter personal que son tratados por las organizaciones, pasando de un SGSI a un Sistema de Gestión de Privacidad de la Información (en adelante "SGPI").

C) ISO 29.100: Es un marco de gestión, que en base a 11 principios propone la protección de los datos personales de la organización, asociado a las tecnologías de la información y comunicación.

D) ISO 22.301: Permite el establecimiento de un Sistema de Gestión de Continuidad del Negocio, "para asegurar que una organización pueda continuar operando durante y después de situaciones de crisis, como desastres naturales, ciberataques, pandemias, conflictos armados o cualquier otra situación que pueda interrumpir sus actividades"[57].

---

[54] LOBOS DE MEDINA, Carlos: Una estructura común en las normas ISOs que definen Sistemas de Gestión en el ámbito de las TICs. En: LinkdIn. Disponible en: https://www.linkedin.com/pulse/una-estructura-com%C3%BAn-en-las-normas-isos-que-definen-lobos-de-medina?utm_source=share&utm_medium=member_android&utm_campaign=share_via

[55] 2020. ¿Qué son las normas ISO y para qué sirven?. En: ProChile (en línea). Disponible en: https://centrodeayuda.prochile.gob.cl/hc/es-419/articles/360047722114--Qu%C3%A9-son-las-normas-ISO-y-para-qu%C3%A9-sirven-#:~:text=La%20%E2%80%9COrganizaci%C3%B3n%20Internacional%20de%20Normalizaci%C3%B3n,mayor%20eficiencia%20y%20rentabilidad%20econ%C3%B3mica. La "Organización Internacional de Normalización" o ISO, es el organismo encargado de promover el desarrollo de normas internacionales, tanto de productos como de servicios, a través de la estandarización de normas voluntarias que se usan en las empresas para su mayor eficiencia y rentabilidad económica. La normalización ofrece importantes ventajas, tanto para el fabricante de un producto o prestador de un servicio, como para los consumidores o usuarios, principalmente para mejorar la adaptación de los productos, procesos y servicios a los propósitos para los cuales fueron diseñados, además de prevenir obstáculos técnicos al comercio y facilitar la cooperación tecnológica.

[56] UNE. ISO 27001, *Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos*. España, 2017. p.13.

[57] 2023. ¿Qué es la norma ISO 22301 y para qué sirve?. En: GlobalSuiteSolutions (en línea). Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-22301-y-para-que-sirve/

E) ISO 31.700: Este estándar, está íntimamente relacionado con la regulación del proyecto de ley sobre protección de datos personales en Chile, al generar buenas prácticas asociadas a la privacidad desde el diseño, la cual permite que las organizaciones consideren durante todo el ciclo de vida de un producto o servicio, los datos personales de las personas naturales que pudieren verse afectado.

F) ISO 27.035: Este marco, se enfoca en la gestión de información de incidentes de la seguridad, motivo por el cual se convierte en un aliado para las organizaciones en el reporte y gestión de respuesta oportuna a los incidentes que pueden ocurrir en un SGSI cuando los controles fallan. Por ende, este documento es de relevancia, sobre todo en base a las obligaciones de reporte que establece el Decreto N.º 273 y la futura ley marco de ciberseguridad.

Para finalizar estos estándares no son excluyentes, pudiendo complementarse según los objetivos del ente implementador.

2- POLÍTICA PÚBLICA DE CIBERSEGURIDAD Y SU IMPACTO EN LAS FF.AA CHILENAS

Surge la interrogante, de cómo esta batería de instrumentos han impactado a las Fuerzas Armadas y como ha sido su recibimiento e implementación. Es por ello, que corresponde dar cuenta de los desafíos que las Fuerzas Armadas deben enfrentar en estructura organizacional, teniendo en cuenta que los cambios regulatorios avanzan conforme la tecnología también lo hace, de manera tal que el sector defensa no puede estar ajeno al cambio.

Dicho esto, los desafíos se centran en 3 elementos organizacionales, a saber, estructura, procesos y personal.

A) Estructuras

El diseño organizacional "es el proceso de construir y adaptar continuamente la estructura de la organización para que alcance sus objetivos y estrategias"[58]. Esto obliga a las Fuerzas Armadas, a regular internamente la ciberseguridad en sus estructuras, estando al debe en esta materia, no generando organismos suficientes que se hagan cargo de este contenido.

El surgimiento de instituciones como los CSIRT propio de cada rama de las Fuerzas Armadas, sumado al futuro CSIRT Defensa que será dependiente del Estado Mayor Conjunto, ha impuesto nuevas responsabilidades para las instituciones quienes deberán organizar a su personal conforme a estas necesidades.

A su vez, la figura voluntaria del Delegado de Protección de Datos Personales y del Oficial de Seguridad de la Información, adolece de adecuar las estructuras, para abrir paso a figuras autónomas e independientes al interior de las Fuerzas Armadas, misión que no será fácil de

[58] CHIAVENATO, I. 2009. Comportamiento Organizcional, la dinámica del éxito en las organizaciones. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gob.mx/cms/uploads/attachment/file/335680/Comportamiento_organizacional._La_dina_mica_en_las_organizaciones..pdf. p.112.

conseguir, si consideramos el carácter jerarquizado, obediente y no deliberante que caracteriza a la defensa nacional.

Por el carácter mecanicista de las Fuerzas Armadas[59], una estructura en equipo se presenta como un apoyo a la cadena vertical de mando, pudiendo distribuir las tareas a realizar, dividiendo así las responsabilidades asociadas al control, modernizando el actuar, generando eficiencia y eficacia.

B) Procesos

Los procesos operan en primer lugar sobre la base de la integración, que "permite coordinar las diferentes partes de una organización para crear unidad entre personas y grupos"[60]. En segundo lugar, operan sobre la diferenciación, la cual "consiste en dividir el trabajo en una organización y se relaciona con la especialización de los órganos y las personas"[61].

Sobre esta definición, la ciberseguridad y la protección de los datos personales impacta en las Fuerzas Armadas, puesto que deberán regular internamente las exigencias y compromisos analizados en el presente estudio.

Se debe promover una cultura de ciberdefensa al interior de todas las Fuerzas Armadas, que que incluya tópicos que la sociedad hoy en día demanda, como lo son la perspectiva de género por ejemplo[62]. Para este cometido, serán de apoyo el desarrollo de políticas, manuales, reglamentos y cartillas, para adoptar los procesos de la organización a estos importante cambios.

En este aspecto, cobra relevancia la Política de Seguridad de la Información que deberán elaborar las Fuerzas Armadas, conforme a las exigencias de la Norma Técnica N.º 7, donde se deberán regular roles y responsabilidades, sumado al cumplimiento de las funciones de identificación, protección, detección, respuesta y recuperación.

Adicionalmente, la regulación existente plantearía la elaboración de modelos de cumplimiento. El primero de ellos, dice relación con el modelo de prevención del delito que cada rama de las Fuerzas Armadas puede elaborar para hacer frente a los delitos bases regulados en la Ley N.º 20.393, entre los que deben ser considerados los tipos penales que incorporó la Ley N.º 21.459. El segundo modelo de cumplimiento es el de carácter voluntario que plantea el proyecto de ley de protección de datos personales, el cual también obliga

[59] Se consideran como características de las organizaciones mecanicistas: Estructura organizacional jerárquica, piramidal, vertical y compleja. Departamentos funcionales y especializados. Órganos definitivos y permanentes. Cadena de mando rígida. Comunicaciones verticales y formales Cultura organizacional conservadora, basada en tradiciones, reglas y procedimientos. Aplicación continua de soluciones rutinarias y estandarizadas. Enfoque en esquemas preestablecidos de organización y métodos.
[60] CHIAVENATO. cit. 2009, p. 94.
[61] Ibíd.
[62] El informe Ciberseguridad y Género del año 2023, del Centro de Estudios en Derecho Informático de la Universidad de Chile, recomienda que se debe"Incorporar la perspectiva de género en las políticas de ciberseguridad. Para ello es necesario: i) definir qué se debe entender por enfoque de género, ii) contemplar medidas concretas para promover la perspectiva de género, iii) monitorear el impacto del género en las amenazas de ciberseguridad, y iv) analizar los datos disponibles y crear políticas focalizadas acorde a los resultados de las investigaciones.

ajustar los procesos internos para la creación de sistemas de denuncia, gestión de incidentes de seguridad, elaboración de matrices de riesgo y evaluaciones de impacto.

En este mismo sentido, los estándares ISO que analizamos con anterioridad siempre traen aparejado la confección de instrumentos o políticas que acompañen los procesos estratégicos de las organizaciones.

Finalmente, la ley de transformación digital del Estado ha puesto un cronómetro hasta el momento ineludible, de modo tal que las Fuerzas Armadas tienen hasta el año 2027, para adoptar sus procesos al camino de la digitalización. Esto implica, ir cumpliendo con las normas técnicas que se han dictado al efecto, junto con los aportes que los estándares ISO pueden generar en el desarrollo de estrategias.

C) Personas

Las Fuerzas Armadas deben medir el impacto que el avance de la tecnología está teniendo en su personal e impulsar tanto medidas de ciberhigiene, como aquellas tendientes a enfrentar el analfabetismo digital.

Para lo anterior, se necesitan indicadores que permitan medir el nivel de conocimiento del personal de las Fuerzas Armadas en los conceptos de ciberseguridad y protección de datos personales.

Determinadas las brechas en estos conocimientos, será labor de los órganos directivos que se hayan seleccionado conforme a las exigencias de las políticas, regulaciones y estándares ya analizados, elaborar planes de capacitación y concientización del personal.

Además de los conocimientos para la formación del personal, existe el desafío de dotar de autonomía a personal que se caracteriza por un carácter jerarquizado, obediente y no deliberante, sobre todo en la figura del Delegado de Protección de Datos, la del Oficial de Cumplimiento y la del Oficial de Seguridad de la Información.

Teniendo en consideración, que el error humano es la principal causa de los problemas de ciberseguridad[63], es que es suma urgencia superar las brechas de desconocimiento, capacitando al personal, generando la cultura organizacional que se requiere para reducir los ciberincidentes al interior de las Fuerzas Armadas.

En este contexto, las Fuerzas Armadas también el desafío de combatir las brechas de género y en específico, las brechas que se producen en materia de los contenidos abordados en el presente estudio, puesto que, si ya la participación de las mujeres es relativamente baja en temas de TIC, en ciberseguridad es escasa[64]. Ahora bien, el reciente informe de ciberseguridad y género evidenció que “en América Latina y el Caribe solo Argentina, Chile,

[63] DI PAULA AMBRISSI, R (31 de octubre de 2022). El error humano es la principal causa de los problemas de ciberseguridad, revela un estudio. *Cointelegraph*. Disponible en: https://es.cointelegraph.com/news/human-error-leading-cause-of-cybersecurity-problems-study-reveals.
[64] HERRERA CARPINTERO, Paloma. 2020. El enfoque de género en la Política Nacional de Ciberseguridad de Chile. Revista Chilena De Derecho Y Tecnología, 9(1), 5–32. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679 .p.9.

Colombia y Ecuador incluyen el enfoque de género de forma expresa en sus políticas de ciberseguridad"[65].

3- CIBERSEGURIDAD, DESAFÍOS Y BUENAS PRÁCTICAS APLICADO EN LAS FFAA CHILENAS

Una vez mencionado los desafíos que adolecen las Fuerzas Armadas, es preciso señalar algunas recomendaciones para mitigar los impactos de lo ya analizado y evidenciado. Para este punto, se propone el siguiente decálogo de medidas:

En primer lugar, las Fuerzas Armadas deberán contar con la asignación de recursos necesarios para poder de manera consciente y responsable los cambios que ciberseguridad y la protección de datos personales traen aparejados.

Estos recursos, deben permitir el financiamiento de los planes de capacitación y formación, junto con la contratación de personal con conocimientos suficientes para liderar los procesos de transformación asociado a estas materias. Asociado a este punto, una adecuada inyección de recursos podría estimular el desarrollo I+D en estas temáticas, pudiendo las Fuerzas Armadas innovar con desarrollos propios, como aplicaciones, herramientas que usen inteligencia artificial y sandbox regulatorios[66]. Lo anterior, considerando que, en el futuro, "el liderazgo mundial se medirá en el desarrollo que cada país haya alcanzado en las tecnologías asociadas a la 4ta revolución industrial"[67], lo cual impacta de manera directa al sector defensa.

En segundo lugar, debido a la especialidad de estos contenidos, se podría evaluar el desarrollo de especialidades secundarias o certificaciones especiales al interior de las Fuerzas Armadas, que permitan motivar al personal a concientizar y capacitarse en ciberseguridad, entendiendo que "formar o instruir cibersoldados debiese tener la misma importancia que entrenar pilotos de combate o tanquistas"[68].

En tercer lugar, se considera que las figuras analizadas del Delegado de Protección de Datos, Oficial de Cumplimiento y Oficial de Seguridad de la Información deben ser independientes y autónomas, con facultades suficientes para tomar decisiones, asesorar y reportar a las autoridades correspondientes cuando correspondan, máxime si consideramos que el Delegado de Protección de Datos, tendrá la importante labor de ser el punto de contacto con

---

[65] OLIVARES ROJAS, Daniela y ARRIAGADA ALVARADO, Valentina. 2023. CIBERSEGURIDAD Y GÉNERO La perspectiva de género en las políticas de ciberseguridad en América Latina y el Caribe. *Centro de Estudios en Derecho Informático*. p.47.

[66] ARAYA. cit. 2020, p. 284.El objetivo de estas cajas es minimizar la incertidumbre respecto de la normativa aplicable a algún producto o servicio, pues permite a las empresas con modelos de negocios innovadores en fase de desarrollo, conocer y adecuarse a la regulación de forma gradual y anticipada, y al regulador, entender de mejor manera el funcionamiento de una nueva tecnología.

[67] LODEIRO ENCINA, Andrea. 2018. Cuarta revolución industrial y sus implicancias en los ámbitos de seguridad y defensa. *Cuadernos de Trabajo* (15), 1-19. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://anepe.cl/wp-content/uploads/2020/11/Cuaderno-de-Trabajo-N%C2%B015-2018.pdf. p.6.

[68] BRIONES RIVEROS, Daniela, 2020. Expectativa v/s Realidad; ciberseguridad en américa latina. En: *Estudios Estratégicos* (en línea). Disponible en: https://www.dropbox.com/sh/qjtsx0boi4iibyh/AABaN_mcpvOYSBjgCkC3DwZva/2019%20y%202020?dl=0&preview=NL_CESIM_39.pdf&subfolder_nav_tracking=1.p.6.

la futura Agencia Nacional de Protección de Datos, organismo sobre el que existen altas expectativas, donde se espera que sea una entidad con verdadero poder y no una mera espectadora de las circunstancias[69].

En cuarto lugar, la ciberseguridad y protección de datos personales deben contar con alta publicidad y una estrategia comunicacional que permitan difundir adecuadamente estos contenidos al interior de las Fuerzas Armadas, de manera que esto no se traduzca en la elaboración de políticas y recomendaciones intrascendentes que no produzcan impacto alguno en los miembros de la defensa nacional.

En quinto lugar, se requiere generar incentivos de coordinación y cooperación entre las diversas ramas de las Fuerzas Armadas, incluyendo al Estado Mayor Conjunto, toda vez que los ciberataques requieren ser abordados de manera colectiva, generando sinergias que permitan cumplir con las funciones de Identificación, protección, detección, respuesta y recuperación.

En sexto lugar, se podría ahondar en la posibilidad de constituir una reserva de expertos en ciberseguridad, a los cuales las Fuerzas Armadas puedas recurrir para los diversos fines asociados a este cometido.

En sexto lugar, es altamente recomendable que las Fuerzas Armadas puedan obtener certificaciones de los estándares ISO, en especial la certificación de la ISO 27.001 de manera que las Fuerzas Armadas, puedan certificar su Sistema de Gestión de Seguridad de la Información.

En séptimo lugar, se debe tomar en consideración el principio de privacidad desde el diseño, de manera que todos los procesos y estructuras que deban ser modificados o desarrollados en virtud de los análisis ya realizados, tomen en cuenta desde el principio la privacidad de los datos de las personas involucradas.

En octavo lugar, se debe continuar innovando y profundizando los objetivos dispuestos por las Política de Ciberdefensa, en especial, materializar los desafíos que las Fuerzas Armadas tienen de cara al ciberterrorismo[70].

Finalmente, no se debe perder de vista, que más que proteger datos, lo que se protege son las personas[71], lo que debe ser un factor diferenciador a la hora de actuar[72]. Las Fuerzas

---

[69] VERGARA, Manuel. 2017. Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. Revista Chilena De Derecho Y Tecnología, 6(2), 135–152. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/45822/50556. p.150.

[70] MAYER LUX, Laura. 2018. Defining Ciberterrorism. Revista Chilena De Derecho Y Tecnología, 7(2), 5–25. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51028/54675 .p.6. The concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks.

[71] PEDUTO, Eduardo. 2013. Cuando protegemos datos protegemos personas. En: *Observatorio Iberoamericano de Protección de Datos* (en línea). Disponible: https://oiprodat.com/2013/05/03/cuando-protegemos-datos-protegemos-personas/.

[72] MARTABIT TELLECHEA, Pía. 2019. Atribución en el ciberespacio: piedra tope en el derecho internacional. *Cuaderno de Trabajo.*(14), 1-18. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-

Armadas, como Órganos de la Administración del Estado, tienen el deber de garantizar el orden institucional de la República, estando dentro de este concepto el respeto a los derechos fundamentales, como es el derecho a la protección de datos personales, amparado en nuestra carta magna. Por este motivo, el tratamiento de los datos personales de los miembros de las Fuerzas Armadas, así como otros que se traten en virtud de sus funciones, deben ser de manera responsable, informada, contando con una base de licitud reconocida, junto con mecanismos que permitan el ejercicio de sus derechos, sumado a la disposición de medidas técnicas y organizativas que recojan sólo los datos estrictamente necesarios para los fines que se han recolectado, de lo contrario, la falta de resguardo por parte de las Fuerzas Armadas, pueden decantar en una falta de servicio, la cual será alegada por los afectados antes las instancias judiciales y administrativas correspondientes[73].

Conclusiones

A la luz de todo lo anteriormente expuesto, el presente estudio constata que las políticas, regulaciones y estándares en materia de ciberseguridad y protección de datos personales requieren un involucramiento directo de las Fuerzas Armadas, ya sea por la obligatoriedad de ciertos contenidos para el sector defensa, como por la necesidad de mantenerse actualizados ante la revolución tecnológica, comprendiendo los riesgos asociados y las mejores prácticas para mitigar los impactos negativos que un incidente de seguridad o una filtración masiva de datos personales puede provocar para las instituciones.

De esta manera, se describió la política pública que rige actualmente en esta materia (a la espera de su actualización), junto con los documentos vinculados a esta, sumado a las regulaciones y estándares internacionales que ofrecen buenas prácticas para que la ciberseguridad logre el estándar de cumplimiento deseado en aras de permitir un acceso seguro y consciente al ciberespacio por parte de las Fuerzas Armadas chilenas, como lo son por ejemplo la incorporación de una nueva institucionalidad, como lo son la Agencia Nacional de Ciberseguridad y la Agencia de Protección de Datos Personales, la inclusión de la privacidad desde el diseño como principio orientador y la implementación de políticas de sistemas de implementación de seguridad de la información.

A su vez, la exposición del impacto organizacional ha logrado visibilizar la necesidad de darle importancia a estos contenidos, comprendiendo los desafíos que esto genera para las instituciones y el largo camino que aún queda por recorrer, como lo son por ejemplo la inversión que deberá realizar en esta área, la preparación del personal, la modificación de

Trabajo-N%C2%B014-2019-1.pdf. p. 16. Es necesario determinar en primeria instancia que cualquier régimen jurídico que se establezca debe de tener el foco del objeto a asegurar es el individuo civil y sus derechos y libertades humanas establecidas por la Carta de Derechos Humanos de la Organización de las Naciones Unidas, respetando los principios liberales.

[73] JARA FUENTEALBA, Natalia y JORQUERA CRUZ, Antonia. La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. Revista Chilena De Derecho Y Tecnología, 10(1), 201–230. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/58776/67520. p.226. Desde este punto de vista, el Estado será responsable por los daños causados a aquellos usuarios de servicios públicos por un ciberataque cuando el servicio en cuestión no haya adoptado las medidas de ciberseguridad consideradas estándar en la industria informática, lo que, a su vez, variará en función del tipo de información almacenada y tratada en los sistemas del respectivo servicio y su atractivo para ser blanco de ciberataques.

estructuras, junto con la implementación de una cultura de ciberseguridad a nivel organizacional.

Posteriormente, el decálogo planteado pone de manifiesto buenas prácticas que pueden ser tomadas en consideración para enfrentar los desafíos e impactos ya abordados, sirviendo de herramienta para los desarrollos internos que deban implementarse, destacando las yo abordados planes de capacitación para el personal, desarrollo de especialidades secundarias, la creación de una reserva de profesionales en ciberseguridad y la obtención de certificaciones ISO, como lo son la ISO 27.001, por citar ejemplos.

Finalmente, existe la oportunidad de aprovechar que las normativas que generarán la mayor cantidad de modificaciones se encuentran aún en tramitación legislativa, sumado a que la Ley de Transformación Digital del Estado aún tiene plazo para su total implementación, razón por la cual las Fuerzas Armadas aún están a tiempo de seguir ajustando sus estructuras, procesos y personal a los desafíos ya esbozados.

Listado Bibliográfico

AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO (BOE). 2016. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf .

ALVARÉZ VALENZUELA, Daniel. 2018. Ciberseguridad en América Latina y Ciberdefensa en Chile. Revista Chilena De Derecho Y Tecnología, 7(1), 1–2. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416/53050.

ARAYA PAZ, Carlos. 2020. Desafíos legales de la inteligencia artificial en Chile. Revista Chilena De Derecho Y Tecnología, 9(2), 257–290. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/54489/64369. p.281.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 1999. *Ley N°19.628, Sobre Protección de la Vida Privada*. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2020-08-26.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2017. Decreto Nª 3 que Aprueba Política de Ciberdefensa. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.° 7 que Establece norma técnica de seguridad de la información y ciberseguridad conforme la ley Nº 21.180. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361371.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.° 8 que Establece Norma Técnica de Notificaciones. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361372.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.° 9 que Establece Norma Técnica de Autenticación. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361373.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.º 10 que Establece Norma Técnica de Documentos y Expedientes Electrónicos para la gestión de procedimientos administrativos. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361374.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.º 11 que Establece Norma Técnica de Calidad y Funcionamiento de las Plataformas Electrónicas que sustentan procedimientos administrativos en los órganos de la Administración del Estado. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361375.pdf.

BIBLIOTECA DEL CONGRESO NACIONAL (BCN). 2023. Decreto N.º 12 que Establece Norma técnica de interoperabilidad. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361376.pdf.

BORDACHAR BENOIT, Michelle. 2022. ¿Cómo y quiénes cuidan nuestros datos? Legislaciones vigentes en países Latinoamericanos (en línea). En: *DerechosDigitales*. Disponible en: https://www.derechosdigitales.org/17759/dia-de-la-proteccion-de-los-datos-personales/.

BORDACHAR BENOIT, Michelle. 2022. Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO. Revista Chilena De Derecho Y Tecnología, 11(1), 395–412. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/67205/70914.

BRIONES RIVEROS, Daniela, 2020. Expectativa v/s Realidad; ciberseguridad en américa latina. En: *Estudios Estratégicos* (en línea). Disponible en: https://www.dropbox.com/sh/qjtsx0boi4iibyh/AABaN_mcpvOYSBjgCkC3DwZva/2019%20y%202020?dl=0&preview=NL_CESIM_39.pdf&subfolder_nav_tracking=1.

CHIAVENATO, I. 2009. Comportamiento Organizcional, la dinámica del éxito en las organizaciones. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gob.mx/cms/uploads/attachment/file/335680/Comportamiento_organizacional._La_dina_mica_en_las_organizaciones..pdf.

CNIL. 2022. Practical Guide GDPR for Data Protection Officers. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf.

CONTRERAS VÁSQUEZ, Pablo. 2020. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Revista Estudios Constitucionales, 18(2), 87-120. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.cl/pdf/estconst/v18n2/0718-5200-estconst-18-02-87.pdf.

CONTRERAS VÁSQUEZ, Pablo. BORDACHAR BENOIT, Michelle. y . ORTÍZ MESÍAS, Leonardo. 2022. *Privacidad y protección de datos personales*. Santiago. DER Ediciones. ISBN: 978-956-405-037-9.

DI PAULA AMBRISSI, R (31 de octubre de 2022). El error humano es la principal causa de los problemas de ciberseguridad, revela un estudio. *Cointelegraph*. Disponible en:

https://es.cointelegraph.com/news/human-error-leading-cause-of-cybersecurity-problems-study-reveals.

DONOSO ABARCA, Lorena y REUSSER MONSÁLVEZ, Carlos. 2022. La protección de los datos personales en Chile. Santiago. Der Ediciones. ISBN: 978-956-405-122-2.

FERNANDEZ, R. (26 de mayo de 2023). Ranking de sanciones económicas impuestas en Europa por delitos contra la protección de datos personales conforme al GDPR hasta mayo de 2023. *Statista.* Disponible en: https://es.statista.com/estadisticas/1386869/gdpr-mayores-multas-por-violaciones-de-datos-personales-en-europa/

GARCÍA VÁSQUEZ, Borja. 2021. El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra. Revista Chilena De Derecho Y Tecnología, Vol. 10. (2). 43-68.

GONZÁLEZ, A. (29 de mayo de 2023). Ejército de Chile sufre ataque informático en su red interna. *BiobioChile*. Disponible en: https://www.biobiochile.cl/noticias/nacional/chile/2023/05/29/ejercito-de-chile-sufre-ataque-informatico-en-su-red-interna.shtml.

GONZÁLEZ, C. (23 de septiembre de 2022). Cerca de 400 mil correos filtrados, contenido estratégico y sumarios administrativos: Lo que se sabe del hackeo al EMCO. *EMOL.* https://www.emol.com/noticias/Nacional/2022/09/23/1073631/detalles-hackeo-masivo-emco.html.

HERRERA CARPINTERO, Paloma. 2020. El enfoque de género en la Política Nacional de Ciberseguridad de Chile. Revista Chilena De Derecho Y Tecnología, 9(1), 5–32. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679.

JARA FUENTEALBA, Natalia y JORQUERA CRUZ, Antonia. La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. Revista Chilena De Derecho Y Tecnología, 10(1), 201–230. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/58776/67520.

LOBOS DE MEDINA, Carlos: *Una estructura común en las normas ISOs que definen Sistemas de Gestión en el ámbito de las TICs*. En: LinkdIn. Disponible en: https://www.linkedin.com/pulse/una-estructura-com%C3%BAn-en-las-normas-isos-que-definen-lobos-de-medina?utm_source=share&utm_medium=member_android&utm_campaign=share_via.

LODEIRO ENCINA, Andrea. 2018. Cuarta revolución industrial y sus implicancias en los ámbitos de seguridad y defensa. *Cuadernos de Trabajo* (15), 1-19. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://anepe.cl/wp-content/uploads/2020/11/Cuaderno-de-Trabajo-N%C2%B015-2018.pdf.

LUZ ÁLVAREZ, Clara. 2023. Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes en instituciones públicas. Revista Chilena De Derecho Y Tecnología, 11(2), 183–210. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/65502/72154 .

MARTABIT TELLECHEA, Pía. 2019. Atribución en el ciberespacio: piedra tope en el derecho internacional. *Cuaderno de Trabajo.*(14), 1-18. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N%C2%B014-2019-1.pdf.

MARRERO TRUJILLO, Leocadio. 2023. Disponible en: https://www.linkedin.com/posts/leocadio-marrero_implementador-l%C3%ADder-iso-31700-privacy-by-activity-7048645337300819968-3Kit/?originalSubdomain=cl.

MAYER LUX, Laura. 2018. Defining Ciberterrorism. Revista Chilena De Derecho Y Tecnología, 7(2), 5–25. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51028/54675 .p.6. The concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks.

MINISTERIO DE CIENCIA, TECNOLOGÍA, CONOCIMIENTO E INNOVACIÓN. 2021. Política Nacional de Inteligencia Artificial. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c 760ae7686e2c/documento_politica_ia_digital_.pdf.

MINISTERIO DE DEFENSA NACIONAL. 2017. *Libro de la defensa nacional de Chile*. Disponible en: https://www.defensa.cl/media/LibroDefensa.pdf .

MINISTERIO DE DEFENSA NACIONAL. 2020. Política de Defensa Nacional de Chile 2020. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defensa.cl/wp-content/uploads/2023/06/POL%C3%8DTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA. 2017. *Política Nacional de Ciberseguridad*. Disponible en: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%c3%adtica%20 Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y .

OLIVARES ROJAS, Daniela y ARRIAGADA ALVARADO, Valentina. 2023. CIBERSEGURIDAD Y GÉNERO La perspectiva de género en las políticas de ciberseguridad en América Latina y el Caribe. *Centro de Estudios en Derecho Informático*.

PEDUTO, Eduardo. 2013. Cuando protegemos datos protegemos personas. En: *Observatorio Iberoamericano de Protección de Datos* (en línea). Disponible: https://oiprodat.com/2013/05/03/cuando-protegemos-datos-protegemos-personas/.

PÉREZ COLOMÉ, J y AYUSO, S. (22 de mayo de 2023). Irlanda impone a Meta una multa de 1.200 millones de euros, la mayor sanción europea por infracción de privacidad. *ElPaís.* Disponible en: https://elpais.com/tecnologia/2023-05-22/irlanda-impone-a-

meta-una-multa-de-1200-millones-de-euros-la-mayor-sancion-europea-por-infraccion-de-privacidad.html.

REUSSER MONÁRDEZ, C. 2021. *Derecho al olvido: La protección de datos personales como límite a las libertades informativas*. Santiago: DER Ediciones. (2) ISBN: 978-956-9959-95-0

SANCHO HIRANE, Carolina. 2018. Ciberinteligencia: Contextualización, Aproximación conceptual, Características y Desafíos. Cuaderno de Trabajo (1), 1-32. Disponible en: https://www.publicacionesanepe.cl/index.php/cdt/article/view/911/580.

SENADO. 2017. Proyecto de Ley: Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

SENADO. 2022. Proyecto de Ley: Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

SENADO. (2 de abril de 2022). *Protección y tratamiento de datos personales: claves de la modernización en trámite*. Senado. Disponible en https://www.senado.cl/proteccion-y-tratamiento-de-datos-personales-claves-de-la-modernizacion.

VÉLIZ, C. 2021. Privacidad es poder: Datos, vigilancia y libertad en la era digital. Mexico: Penguin Random House Grupo Editorial. ISBN: 978-607-380-902-3.

VERGARA, Manuel. 2017. Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. Revista Chilena De Derecho Y Tecnología, 6(2), 135–152. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/45822/50556.