Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

Aportes a la ciberseguridad y la gestión de las Infraestructuras Críticas de la Información en Argentina (2011-2019)

AUTORA: ABOG. AGOSTINA TAVERNA

DIRECTOR: DR. JULIO CÉSAR SPOTA

CO-DIRECTOR: MG. RODRIGO CÁRDENAS HOLIK

JUNIO 2021

Dedicatoria

A mis padres, quienes desde siempre me transmitieron los valores más importantes en un individuo, incluido el amor por mi país.

Agradecimientos

A los directores de la maestría, Dr. Roberto Uzal y Esp. Ing. Carlos Federico Amaya, por la oportunidad académica en un entorno multidisciplinario, el desarrollo profesional y la búsqueda de la capacitación constante.

A Leandro de la Colina por ser mi brújula y debatir por horas este proyecto.

A mis amigos Valentina, Fernando y Juan Pablo quienes leyeron este trabajo y me brindaron sus opiniones más sinceras.

A la Lic. Prof. Myrian Errecalde por resolver con dedicación cada consulta relacionada con las citas y la bibliografía de este trabajo final.

Especialmente a mi Director y Co-director de Tesis, Dr. Julio César Augusto Spota y Mg. Rodrigo Cárdenas Holik, por desafiarme constantemente y acompañarme en la búsqueda de calidad académica respetando siempre mi opinión y valorando mi criterio en el marco de honestidad profesional. No podría haber elegido mejor.

Resumen

El presente trabajo final de maestría analiza el marco normativo argentino relacionado a las infraestructuras críticas y la ciberseguridad desde la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el mes de julio del año 2011, hasta la Resolución N° 1380 del mes de diciembre del año 2019. Asimismo, se investiga el estado jurídico-institucional de la temática en España, dada la similitud en la cultura, cantidad de habitantes, el idioma y la influencia en materia legislativa, además del lugar que ocupa en el ranking del Índice Nacional de Ciberseguridad. El análisis en su conjunto se efectúa, en pos de fomentar una mejora en la protección de las infraestructuras críticas argentinas. Mediante un análisis exploratorio de carácter descriptivo y ordenamiento cronológico, el trabajo presenta una serie de hallazgos donde los aciertos conviven con superposiciones y elementos redundantes. Esto condujo a la necesidad de establecer aspectos rescatables y, mediante una reflexión crítica sobre el estado general de la problemática, a la proposición de una posible solución con carácter institucional.

La propuesta consiste en la creación de una agencia estratégica, con características innovadoras y objetivos claros, destinada a reorganizar la situación bajo análisis dentro de la estructura de la Administración Pública Nacional. De ser llevada a la práctica, la iniciativa institucional contará con la capacidad de maximizar la protección y defensa de las infraestructuras críticas y, por extensión, favorecerá la implementación de un esquema de ciberseguridad desde un enfoque donde prevalecen los conceptos de resiliencia (compuesto por la prevención, la respuesta y la recuperación), cooperación internacional, y coordinación entre los sectores público y privado; en un contexto de armonía con los sistemas institucionales de seguridad interior, defensa nacional, gestión integral e inteligencia nacional. En efecto, la agencia y su estructura serán el aporte para la gestión de las infraestructuras críticas argentinas que permitiría perpetuar en el tiempo medidas, políticas y documentos que tienen un objetivo ulterior y superior a todos: garantizar el adecuado funcionamiento de los servicios esenciales de la sociedad argentina, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Palabras claves: agencia, resiliencia, infraestructuras críticas, ciberseguridad.

Índice

Índice de figuras y tablas

1. Introducción

Globalmente, la perturbación de las infraestructuras críticas de la información de una nación puede ocasionar la afectación de los derechos humanos, la destrucción de bienes, efectos económicos e, inclusive, pérdidas de vidas humanas. En efecto, el riesgo de dicha alteración se ve agravado por la proliferación de ciberamenazas, el incremento en el uso de las tecnologías y "[…] la dependencia de la nación sobre redes informáticas y de información para comunicaciones, gestión de datos y el funcionamiento de las infraestructuras críticas (en adelante "IC") lo torna cada vez más vulnerables a […] ataques cibernéticos contra nuestra infraestructura de información" (*Institute for Information Infrastructure Protection* - I3P, 2003), así como el complejo sistema de interdependencia que vincula a las diferentes infraestructuras, inclusive entre naciones. Ciertamente, la República Argentina no está exenta de dichas perturbaciones, riesgos y amenazas.

En particular, la capacidad para prevenir, responder y recuperarse frente a una afectación parcial o total de cualquier IC requiere de la preparación de las personas y la articulación de las instituciones, empresas y organismos que se relacionan directa (o indirectamente) con ellas. Sin duda, tanto la prevención como la reacción y la resiliencia[1] de estas infraestructuras dependen de una multiplicidad de actores del sector público y privado que demandan liderazgo, habilidades de negociación, compromiso, capacitación, desarrollo tecnológico y, especialmente, confianza[2].

Frente a la necesidad de avanzar y construir a favor de la protección y resiliencia de las IC, se realiza un análisis retrospectivo e introspectivo donde se explora la evolución cronológica del derecho argentino del año 2011 al año 2019 concerniente a la ciberseguridad y a dichas

[1] Para el presente trabajo final de maestría, se tendrá en cuenta la definición brindada por T.D. O'Rourke donde "la resiliencia de una comunidad es un atributo general que refleja el grado de preparación de la comunidad y la capacidad de responder y recuperarse del desastre" (O'Rourke, 2007, pág. 25).

[2] En el marco del presente trabajo final de maestría, la confianza expresa un capital intangible de importancia primordial en el establecimiento de iniciativas estratégicas toda vez que abona el acercamiento entre actores con agendas diferenciadas y/o atributos disimiles. Tanto es así, que "en el entorno actual, muchos autores coinciden en que la confianza es un elemento crítico en el desempeño de alianzas estratégicas" (Fadol & Sandhu, 2013, pág. 107). Inclusive, entre las recomendaciones a la Comisión Europea y otros organismos sobre la adopción de medidas de seguridad en infraestructuras críticas, se destaca que "en la cooperación público-privada, un enfoque basado en la confianza y el respeto debe implementarse activamente y no debe darse por sentado. Esto servirá para reducir la imprevisibilidad, evitar malentendidos y aumentar el intercambio de información" (Tessari & Muti, 2021, pág. 44).

infraestructuras, así como el modelo desarrollado por España en la materia para avanzar en los hallazgos encontrados y, finalmente, efectuar un análisis con vocación prospectiva que admite proponer una posible solución que permita contribuir a afianzarnos en la materia a nivel internacional.

En particular, el desarrollo del tema se basa en un análisis normativo argentino (mayoritariamente en el ámbito del derecho administrativo) en el rango temporal definido con anterioridad, dentro del cual fue posible vislumbrar la carencia de un sistema institucional nacional de protección de las infraestructuras críticas de la información y un único organismo que avanzara en el fortalecimiento de las mismas, articulando los diferentes ministerios y organismos de la Administración Pública Nacional (en adelante "APN") así como aquellas empresas u organismos del sector privado que se relacionan con la temática. Además, las superposiciones en los objetivos y funciones de las secretarías, subsecretarías, direcciones nacionales y direcciones creadas a lo largo del tiempo tornan imprescindible el desarrollo de una solución que permita la perduración y el cumplimiento de los objetivos establecidos en la Estrategia Nacional de Ciberseguridad. Más precisamente, el octavo objetivo de dicho instrumento que hace referencia a la Protección de las Infraestructuras Críticas Nacionales de Información.

La gestión para la protección de las infraestructuras críticas de la información y la ciberseguridad requiere de un enfoque interdisciplinario y multidisciplinario, cuyo liderazgo y cumplimiento demanda profesionales de diversas formaciones (tanto técnicas como no-técnicas o sociales) a favor del fortalecimiento de la protección y resiliencia de las infraestructuras que soportan servicios esenciales para la sociedad. En efecto, el descubrimiento del caos normativo en una temática tan específica como esta permite un análisis jurídico-institucional que sienta las bases para evitar repetir las falencias detectadas y crear una estructura, mediante la propuesta del trabajo final de maestría, que permite fortalecer las IC nacionales e incrementar la estabilidad, la confianza y la tranquilidad de la sociedad.

El tema propuesto como trabajo final de maestría fue escogido con base en el incremento en el uso de tecnologías, el aumento en las probabilidades de ocurrencia de un ciberataque y la afectación a las IC de Argentina que podría impactar en el plano económico, social y en la vida, entre otros. Además, se torna necesario comprender el estado de la temática jurídico-institucional en nuestro país y la relevancia de tener un organismo dentro de la APN que

perdure independientemente de los cambios políticos, con la capacidad de adaptarse a los avances tecnológicos y articular a los distintos sectores. En efecto, los servicios esenciales para la sociedad (aún no definidos), cuyos sectores fueron establecidos en la normativa argentina, requieren de una entidad que sea referente en el plano nacional e internacional para que la protección y resiliencia de dichas infraestructuras se fortalezca. Considerando los conocimientos obtenidos a lo largo de la carrera académica de la estudiante de la maestría y la experiencia laboral actual y en el Congreso de la Nación, fue posible analizar la temática con un enfoque jurídico-estratégico a favor del trabajo multifacético e interdisciplinario que requiere la temática para concluir en una propuesta integral que genera aportes a nivel nacional para el posicionamiento internacional de la Argentina y amparando los derechos de la sociedad en su conjunto a la vez que se salvaguardan los valores de la República.

2. Planteamiento del problema

2.1. Formulación del problema

Dada la dependencia socioeconómica de la sociedad para con la tecnología y su rápida evolución, la amplitud de los conceptos y definiciones, así como la multiplicidad de sectores afectados, dentro de un contexto político donde se sancionan y promulgan normativas que crean organismos, modifican su nomenclatura y dependencia funcional y organizacional, modifican objetivos y repiten funciones, es que se torna necesario afrontar la protección de dichas infraestructuras desde un punto de vista multidisciplinario, teniendo en cuenta al sector público y privado conjuntamente.

La problemática actual reside en que aún no se ha desarrollado un sistema de protección de las infraestructuras críticas de la información, de carácter intersectorial y multinivel, que permita ser el puntapié para el amparo de dichas infraestructuras y que, a la vez, esté compuesto por organismos y entes de la APN y del sector privado. El problema a resolver, que va de la mano con el octavo objetivo de la Estrategia Nacional de Ciberseguridad, requiere de un órgano cuya función se relacione con el impulso, coordinación y supervisión de aquellas actividades relacionadas con la instancia de identificación y protección de IC en el territorio nacional.

En consecuencia, dada la complejidad de la materia, su incidencia sobre la seguridad de la sociedad y la importancia que asume para el normal funcionamiento de las estructuras

básicas nacionales e internacionales, es que se vuelve imprescindible definir un sistema institucional para la protección de las infraestructuras críticas de la información. En el presente trabajo se propondrá la creación de una agencia dentro de la estructura organizativa estatal que encabece dicho sistema e incluya responsabilidades relacionadas con el correcto funcionamiento de los servicios esenciales para la sociedad. Para ello, dicha institución incluirá, dentro de sus funciones, la valoración de los principales activos de dichas infraestructuras, la determinación de la criticidad de las mismas, el contacto y capacitación de los operadores críticos de las infraestructuras, la articulación a favor de la investigación y desarrollo de tecnología de ciberseguridad y la coordinación tanto entre el sector público y privado, y la cooperación internacional con el fin de coordinar las actividades que se requieran en materia de infraestructuras críticas de la información y ciberseguridad a nivel nacional.

El presente trabajo pretende avanzar sobre un aspecto jurídico-institucional de la ciberseguridad y aspira a responder los siguientes interrogantes: ¿qué organismo tiene la función de identificar las infraestructuras críticas de la información en la Argentina?, ¿cómo y quién es responsable de los registros que contienen la información crítica de dichas infraestructuras? y ¿existe un sistema nacional institucionalizado que tenga como objetivo principal la protección de las IC?

Frente a esto, se efectuó un análisis exhaustivo de la normativa nacional y se investigó el estado del arte en la temática en España, arribando a una propuesta diseñada para el contexto latinoamericano y más precisamente argentino, con el fin de generar una solución constructiva hacia la resolución del problema.

2.2. Objetivos: general y específicos

Objetivo general:

Este trabajo tiene como principal objetivo abordar la problemática relacionada con la ciberseguridad y las infraestructuras críticas de la información en Argentina, desde el punto de vista de la normativa nacional, con el fin de proponer la creación de un organismo estatal descentralizado, federal, autónomo y autárquico, dependiente del Presidente de la Nación, que cumpla con el octavo objetivo de la Estrategia Nacional de Ciberseguridad.

Objetivos específicos:

- Exponer en el marco teórico el estado jurídico-institucional del derecho argentino en materia de infraestructuras críticas y ciberseguridad desde el año 2011 al año 2019, considerando lo reglamentado por el Poder Ejecutivo Nacional (en adelante "PEN"). Asimismo, plasmar la situación jurídico-institucional de España de manera sucinta, con el objetivo de identificar el estado general de la temática de la ciberseguridad y las infraestructuras críticas de la información. Todo ello, a fin de poner en perspectiva la madurez en la que se encuentra dicha disciplina en un país referente en la materia dentro del contexto internacional, además de estar vinculado a través de una estrecha asociación histórica y cultural con nuestro país.
- Analizar la normativa argentina expuesta en el marco teórico mediante la presentación de aquellos ejes y principios rectores a rescatar de la problemática bajo estudio. A la vez, organizar por subtemas lo presentado en el marco teórico y exponer los hallazgos encontrados del análisis. Los subtemas a considerar serán la identificación de las infraestructuras críticas de la información y ciberseguridad con base en los sectores considerados, su definición y relevancia para la Nación; la investigación, innovación y desarrollo; la coordinación entre los sectores público y privado; y la capacitación y concientización en ciberseguridad, así como la cooperación internacional.
- Señalar los hallazgos revelados a partir de lo expuesto sobre España y establecer aquello que podría considerarse a la hora de implementar un sistema institucional a favor de la protección de las infraestructuras críticas.
- Presentar la propuesta de solución a los hallazgos analizados con anterioridad mediante la exposición de una estructura organizativa a nivel federal, liderada por una agencia y compuesta por cinco direcciones generales con responsabilidades en el correcto funcionamiento de las infraestructuras que soportan los servicios esenciales de la sociedad. Además, plantear la necesidad de efectuar acuerdos y convenios con organismos y sistemas institucionales existentes para confluir los esfuerzos que se realizan en la actualidad hacia el cumplimiento de un objetivo común: la protección de las IC.

2.3. Hipótesis

Desde una perspectiva general, puede sostenerse que la normativa argentina consideró a la protección de las infraestructuras críticas de la información y a la ciberseguridad como temáticas importantes y relacionadas desde el año 2011 (Resolución N° 580/2011). Sin embargo y aun con los cambios políticos, no se tuvo en cuenta la identificación, relevamiento, catalogación y resguardo de la información y activos de dichas infraestructuras (paso clave para la protección), así como la articulación de los distintos actores interesados. Además, desde el PEN no se tomaron las acciones necesarias para hacer cumplir los objetivos de la Estrategia Nacional de Ciberseguridad y, en particular, el octavo objetivo que hace a la protección de dichas infraestructuras (Decreto N° 577/2017).

Frente a ello y dadas las falencias en la legislación argentina, es que se considera como necesaria la creación de un organismo que centralice, y ejecute actividades y funciones en torno al cumplimiento del octavo objetivo de la Estrategia Nacional de Ciberseguridad en miras a la protección de las infraestructuras críticas de la información argentinas.

3. Marco teórico

El presente apartado se dividirá en tres subtítulos. En primer lugar, se hará mención a algunos conceptos básicos de derecho que permitirán asentar la base para que el lector avance en el análisis jurídico-institucional con las nociones necesarias. En segundo lugar, se hará referencia a las normas (leyes, decretos, resoluciones y decisiones administrativas) en forma cronológica, desde el año 2011 hasta el mes de diciembre del año 2019[3], relacionadas con las infraestructuras críticas de la información y la ciberseguridad en la Argentina, con el objetivo de facilitar un panorama de la temática con base en el territorio caótico que es el andamiaje normativo nacional. Finalmente, se hará una breve mención al estado de la temática en España para tener otra perspectiva y referencia de la experiencia en dicho país.

[3] El período de tiempo de estudio se inaugura por motivo atinente a la problemática de la investigación dado que en el 2011 se pueden observar los primeros vestigios en lo que hace al avance normativo con base en las infraestructuras críticas y se acota al 2019 dada la dificultad que representa investigar algo que continúa en desarrollo en el ámbito jurídico-institucional.

3.1. Breve introducción a algunos conceptos básicos de derecho

Es innegable la aceleración temporal en la creación y uso diario de las tecnologías que ejercen una gran influencia en prácticamente todos los aspectos de una sociedad. Frente a esto, como externalidades directas de la globalización, resultan incuestionables los efectos positivos y negativos que conllevan. Sin embargo y a pesar de haberse generado un desarrollo significativo en el plano normativo, la velocidad con la que avanza la tecnología (COMPTIA, 2020) desborda su correlato legal al no poder verse reflejado en el derecho argentino las complejidades políticas, estratégicas, operativas, económicas y sociales inherentes al tema en cuestión.

Son diversos los autores, entre ellos Hans Kelsen, que consideran que "el derecho aparece como un orden social, como un sistema de normas que regulan la conducta recíproca del hombre" (Kelsen, 2010, pág. 31) lo cual no debe escapar al encauzamiento del comportamiento humano frente a la tecnología con el resguardo de Tratados Internacionales de Derechos Humanos[4], la Constitución Nacional y los tratados internacionales restantes. En efecto, el derecho debe acompañar la cada vez más impetuosa evolución de la tecnología y aquello que atañe a la información. Es frente a dichas afirmaciones y dada la naturaleza de la norma, que se torna imprescindible la regulación legislativa de las cuestiones que hacen al comportamiento del ser humano para con algo tan determinante para los intereses nacionales como las infraestructuras críticas de la información y su protección.

A través de la Constitución Nacional, la República Argentina adopta la forma representativa, republicana y federal con una división de poderes entre el Poder Judicial, Legislativo y Ejecutivo a favor del resguardo del estado de derecho, los derechos de los particulares y la seguridad jurídica (Durante & Bestard, 2010). Específicamente, el derecho argentino se encuentra integrado por normas ordenadas y jerarquizadas[5], donde es posible visualizar

[4] Con "[…] jerarquía constitucional, no derogan artículo alguno de la primera parte de la Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos" como dicta el artículo 75°, inciso 22, de la Constitución Nacional Argentina de 1994.

[5] En términos generales, las normas en Argentina entran en vigencia cuando son publicadas en el Boletín Oficial y la obligatoriedad de cumplimiento comienza desde esa fecha. Sin embargo, la publicación de dichos documentos de decisión no necesariamente materializan la ejecución de la norma ya que, para ello, se requiere los esfuerzos del Poder Ejecutivo quien será el responsable de poner en marcha el aparato estatal para avanzar en la práctica con lo que el derecho impone.

distintas relaciones de subordinación y coordinación con una estructura piramidal. Abelardo Torré (2003) afirma que en la pirámide:

> Las normas se distribuyen en las distintas gradas, que se escalonan desde el vértice hasta la base, disminuyendo en el mismo sentido su generalidad: es por ello que mientras en el plano más alto se encuentran las normas constitucionales - en sentido positivo - en la base de la pirámide se hallan las normas individuales. Entre ambos extremos, se encuentran los tratados internacionales, las leyes *stricto sensu*, los decretos del Poder Ejecutivo, etc. (Torré, 2003, pág. 255)

El Poder Legislativo Nacional (en adelante "PLN") tiene "[…] entre sus atribuciones legislar en materia de aduana y comercio, finanzas y seguridad tanto de las provincias entre sí como con los estados extranjeros" (Baretto, 2011, pág. 71) y es ejercido por el Congreso de la Nación compuesto por la Honorable Cámara de Diputados de la Nación y el Honorable Senado de la Nación. Para la efectiva sanción de las leyes, se requiere la aprobación bicameral de los proyectos lo cual permite que haya una perdurabilidad de las leyes y que se refuercen "[…] los mecanismos de corrección, se minimizan las posibilidades de incurrir en error y se enriquece el proyecto a partir de dos perspectivas, que no siempre son equivalentes" (Centro de Implementación de Políticas Púbicas para la Equidad y el Crecimiento, 2003, pág. 10).

Acorde al artículo 87 de la Constitución Nacional Argentina, el PEN es encabezado por el Presidente de la Nación y tiene entre sus atribuciones ser el responsable político de la administración general del país así como expedir las instrucciones y reglamentos para la ejecución de las leyes de la Nación[6]. La Argentina cuenta con un sistema presidencialista - algunos autores afirman que a partir de la reforma de la Constitución Nacional de 1994 es hiperpresidencialista[7]- el cual se caracteriza por que "el jefe del ejecutivo es electo popularmente, […] define la composición del gobierno y lo dirige, y posee alguna facultad legislativa otorgada constitucionalmente" (Carey, 2006, pág. 122). En efecto, la composición

[6] El artículo 99 de la Constitución Nacional Argentina enlista las atribuciones restantes del Presidente de la Nación.

[7] "El diseño institucional argentino ha favorecido la conformación de un sistema hiperpresidencialista que reúne en el Poder Ejecutivo amplios poderes de gobierno y legislación y que, si bien, le otorgan una primacía sobre los restantes poderes (fundamentalmente sobre el legislativo), en épocas de crisis enfatizan sus debilidades y lo vuelven propenso a su quiebre". (Parodi, 2016, pág. 75)

del gobierno y la estructura organizacional se efectúa a través de normas jurídicas generales las cuales no deberían ni podrían contradecir las normas que emanan del PLN.

Frente a esto, se torna necesario hacer una breve referencia a la noción del derecho administrativo - considerado como un derecho local o provincial dado que cada provincia debe legislar sus instituciones locales - y definida por el Dr. Marienhoff como:

> El conjunto de normas y de principios de derecho público interno, que tiene por objeto la organización y el funcionamiento de la administración pública, como así la regulación de las relaciones interorgánicas, interadministrativas y las de las entidades administrativas con los administrados. (Marienhoff, 1995, pág. 160)

Por otra parte, teniendo en cuenta las distintas fuentes del derecho administrativo - rama del derecho que compete al presente trabajo -, la Figura 1 permite ordenar las normas que emanan del PEN[8] piramidalmente de la siguiente manera:

Figura 1: Representación gráfica de la pirámide de derecho administrativo nacional argentino que muestra el orden de prelación de las normas. Fuente: elaboración propia.

[8] "En general, dentro de los regímenes políticos que consagran la separación de los poderes, se denomina decreto o reglamento, a las normas jurídicas emanadas del Poder Ejecutivo." (Torré, 2003, pág. 344)

En lo que hace a la APN, la misma "está integrada por los organismos de la Administración Central (AC), los organismos descentralizados (OD) y las instituciones de la seguridad social (ISS)" (Rubio, 2017). Los segundos, conocidos como agencias y organismos autónomos, deben por un lado encontrar el equilibrio entre la independencia y el control de las estructuras institucionales, y por el otro rendir cuentas por las políticas y acciones que realicen.

Estas instituciones se caracterizan por la "especialización en un ámbito de políticas públicas y un marco institucional que las hace o debe hacerlas (relativamente) autónomas de las autoridades políticas y de los ministerios de línea" (Bertranou, 2013, pág. 12). En lo que hace a la especialización, la creación de una agencia u organismo descentralizado permite:

> Hacer frente a los problemas de asimetría de información en áreas de gestión muy técnicas, e incrementar de esta manera la calidad y eficiencia en la provisión de servicios públicos y elaboración de políticas. Por otro lado, la mayor autonomía es vista como una herramienta que permite resolver los problemas originados por la baja credibilidad de las promesas y compromisos realizados por los funcionarios políticos y tomar distancia de sus políticas. (Rubio, 2017)

Asimismo, acorde a un estudio de los organismos descentralizados del PEN, estos se caracterizan por contar o han contado con una asignación legal de recursos, poseer patrimonio estatal, tienen capacidad para administrarse a sí mismos, son creados por el Estado y los autores admiten que hay consenso en que su creación debe ser por ley, están sometidos al control estatal y persiguen un fin público (Oszlak, Malvicino, & Ouviña, 2001) y "poseen personalidad jurídica propia, por lo cual están habilitados para actuar en juicios, celebrar contratos en su nombre, entre otras cosas" (Rubio, 2017). En Argentina, algunos ejemplos de organismo descentralizados pueden observarse en instituciones de investigación y desarrollo como el Instituto Nacional de Tecnología Agropecuaria (INTA), agencias de regulación y control como Ente Nacional Regulador de la Electricidad (ENRE), de archivo y preservación como el Banco de Datos Genéticos, u organismos a cargo del pago de subsidios, becas y formación de investigadores científicos de carrera como el Consejo Nacional de Investigaciones Científicas y Técnicas de Argentina (CONICET).

En lo que respecta al presente trabajo final, en el mismo se hará referencia a distintos documentos de decisión dictados en el ejercicio de la función administrativa[9], tales como resoluciones, disposiciones, decretos y decisiones administrativas que producen efectos jurídicos generales. Dichas normas son declarativas y permiten tanto reglamentar las leyes que emanan del PLN - sin alterar su espíritu[10] - como, en su defecto, dictar decretos que rigen únicamente dentro del ámbito del PEN y de la Administración Pública que provengan de la Jefatura de Gabinete de Ministros[11] o de los distintos Ministerios o Secretarías[12].

3.2. Evolución cronológica del derecho argentino aplicado a las IC y la ciberseguridad del año 2011 al 2019

En esta sección se describirán los contenidos normativos, objetivos y los aspectos de orden institucional de los distintos organismos, secretarías, subsecretarías, direcciones nacionales y direcciones creadas en el marco de las IC y la ciberseguridad, con el fin de orientar al lector en la disposición organizativa que tuvo el Estado a lo largo de los años definidos. Asimismo, se hará una breve referencia al Sistema de Gestión Integral Nacional (donde se incluye el Ministerio, luego Secretaría de Modernización y subsidiarias), al Sistema de Inteligencia Nacional, al Sistema de Defensa Nacional y una breve mención del Sistema de Seguridad Interior. Es posible anticipar que el país ha generado un amplio pero confuso marco regulatorio, como se verá más adelante, presumiblemente conocido a través de la

[9] "De acuerdo al concepto de función administrativa […], ésta es toda la actividad realizada por los órganos administrativos y la actividad realizada por los órganos legislativos y judiciales excluidos sus respectivas funciones específicas." (Capítulo VII: Fuentes Nacionales del Derecho Administrativo, Gordillo, 2013, pág. 19).

[10] "El Presidente de la Nación tiene las siguientes atribuciones: 2. Expide las instrucciones y reglamentos que sean necesarios para la ejecución de las leyes de la Nación, cuidando de no alterar su espíritu con excepciones reglamentarias." (Artículo 99°, inciso 2°, Constitución Nacional Argentina, 1994).

[11] "Al jefe de gabinete de ministros […] le corresponde: expedir los actos y reglamentos que sean necesarios para ejercer las facultades que le atribuye este artículo y aquellas que le delegue el presidente de la Nación, con el refrendo del ministro secretario del ramo al cual el acto o reglamento se refiera." (Artículo 11°, inciso 2°, Constitución Nacional Argentina, 1994).

[12] "Los ministros no pueden por sí solos, en ningún caso, tomar resoluciones, a excepción de lo concernientes al régimen económico y administrativo de sus respectivos departamentos." (Artículo 103°, Constitución Nacional Argentina, 1994).

publicación[13] en el Boletín Oficial - presunción *juris et de iure*[14]- relacionado con las IC y la ciberseguridad.

Año 2011

Los primeros indicios, en lo que respecta al interés jurídico en torno a las IC nacionales, pueden observarse en la Resolución N° 580/2011 aún vigente. Dicha norma considera que las comunicaciones virtuales dependientes de la infraestructura digital son consideradas como infraestructura crítica, ya que es imprescindible para el funcionamiento de los sistemas de información y comunicaciones tanto para el sector público como privado. Asimismo, la resolución se fundamenta en las constantes amenazas a las que se encuentra expuesta dicha infraestructura digital y que podrían ocasionar graves incidentes en los sistemas de información y comunicaciones. La importancia de dicha resolución radica en que la misma crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad que:

> Tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8° de la Ley N° 24.156[15] y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y

[13] "Es el acto por el que se pone en conocimiento de los habitantes del Estado, la promulgación del proyecto de ley" (Torré, 2003, pág. 338).

[14] "La presunción legal *juris et de jure*, reposa en una necesidad prácticamente ineludible que la justifica: es la necesidad de certeza y seguridad en las relaciones humanas, que desaparecería si pudiera alegarse como excusa el desconocimiento de la ley. Como dice el aforismo latino, *ignorantia juris non excusat*". (Torré, 2003, pág. 339).

[15] a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social. b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias. c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones. d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional. (Artículo 8°, Ley N° 24.156, 1992).

> estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías. (Artículo 2°, Resolución N° 580, 2011)

El Programa, originalmente a cargo de la Oficina Nacional de Tecnologías de la Información (en adelante "ONTI")[16], enumera dieciocho objetivos entre los que se destacan el inciso b) que hace referencia a la elaboración de políticas de resguardo de la seguridad digital con especial hincapié en las IC, el inciso d) que determina el establecimiento de prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad y la implementación de los últimos avances en tecnología para la protección de las IC, el inciso ñ) para monitorear los servicios del Sector Público Nacional y las infraestructuras identificadas como críticas para la prevención de posibles fallas de seguridad y el inciso o) a favor de promover la concientización en relación a los riesgos que acarrea el uso de medios digitales y del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica (Artículo 3°, Resolución N° 580, 2011) .

A partir de dicho Programa y con el fin de que el sector privado, los organismos interjurisdiccionales y las organizaciones civiles adhieran al mismo, la ONTI estableció el Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad y el Convenio de Confidencialidad (Disposición N° 3 del año 2011). Este último obliga a los adheridos a la reserva y secreto de los datos e información a la que acceda aún después del vencimiento del plazo, de la rescisión o resolución del contrato o cese o interrupción de la relación laboral (Disposición N° 3, 2011).

Año 2013

A través de la Disposición N° 2/2013, la ONTI estableció en agosto de ese año la creación de cuatro grupos de trabajo en la esfera de dicho organismo y en el marco del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Los grupos de trabajo son el ICIC-CERT (*Computer Emergency Response Team* por su sigla en inglés), el ICIC-GAP (Grupo de Acción Preventiva), ICIC-GICI (Grupo de Infraestructuras Críticas de

[16] Creada en agosto del año 2003 con la responsabilidad primaria de "asistir al Subsecretario de la Gestión Pública en la formulación de políticas e implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado, promoviendo la integración de nuevas tecnologías, su compatibilidad e interoperabilidad de acuerdo con los objetivos y estrategias definidas en el Plan Nacional de Modernización del Estado. Promover la estandarización tecnológica en materia informática, teleinformática o telemática, telecomunicaciones, ofimática o burótica" (Planilla anexa al artículo 2°, Decreto N° 624, 2003).

Información) e ICIC-INTERNET SANO[17], los cuales fueron creados con objetivos y tareas definidas con el fin de desarrollar y formular proyectos y propuestas que promuevan la protección de infraestructuras críticas de información y ciberseguridad, entre otras. Considerando el objetivo del presente trabajo, se hará referencia a los objetivos más relevantes de dichos grupos de trabajo. Teniendo en cuenta al ICIC-CERT:

> Administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encausar sus posibles soluciones de forma organizada y unificada (inciso a); asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos del Sector Público Nacional que hubieren adherido (inciso b); centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos (inciso c); actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa (inciso d) y difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional (inciso f). (Disposición N° 2/2013)

Mientras que los objetivos del ICIC-GICI se establecen en el artículo 6° de la Disposición, siendo los más relevante para el presente trabajo de maestría:

> Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado haciendo especial hincapié en las infraestructuras críticas (inciso b); establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas (inciso c); alertar a los organismos que se adhieran al presente Programa sobre casos de detección de intentos de vulneración de infraestructuras críticas, sean estos reales o no (inciso d); coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de

[17] En el marco temporal del presente trabajo, no es posible definir si efectivamente estos grupos se encuentran conformados y trabajando activamente en el cumplimiento de los objetivos establecidos. Tampoco es posible determinar si la disposición que crea a los grupos de trabajo fue derogada explícita o tácitamente.

> vulneración de las infraestructuras críticas del Sector Público Nacional (inciso e). (Disposición N° 2, 2013)

Por otra parte, entre los objetivos del ICIC-GAP es posible resaltar:

> Investigar nuevas tecnologías y herramientas en materia de seguridad informática (inciso a); Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional (inciso b); Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información (inciso c); Monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad (inciso d). (Disposición N° 2, 2013)

Mientras que el ICIC-INTERNET SANO creado en el marco del "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad", debiera:

> Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica (inciso a). (Disposición N° 2, 2013)

Por otra parte, el Ministerio de Defensa de la Nación creó, en el año 2013 mediante la Resolución N° 385, la Unidad de Coordinación de Ciberdefensa en el ámbito de la Jefatura de Gabinete de dicho Ministerio, con la función de:

> Coordinar las políticas y el desempeño de los actores vinculados a la ciberdefensa en la jurisdicción. El principal fundamento para la creación del área fue la existencia en las Fuerzas Armadas de un proceso de generación de capacidades y unidades especializadas para emergencias tele-informáticas. La constitución de la Unidad de Coordinación se enmarca en un concepto de ciberdefensa asociado a la protección del ciberespacio. [Donde] se establece que la ciberdefensa requiere de la participación de todos los miembros del sistema de la defensa e innovación tecnológica del país. (Cornaglia & Vercelli, 2017)

Año 2014

Por otra parte, en el mes de mayo del año 2014 se dispuso la creación del Comando Conjunto de Ciberdefensa a través de la Resolución N° 343 "dependiente orgánica, funcional y operacionalmente del Estado Mayor Conjunto de las Fuerzas Armadas" (Cornaglia & Vercelli, 2017) y "la principal capacidad que debe desarrollar este nuevo comando es la de conjurar y repeler ciberataques contra infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar" (Subsecretaría de Ciberdefensa - Ministerio de Defensa - Presidencia de la Nación). Entre sus funciones, resaltan la coordinación de las acciones ejecutadas por las reparticiones de ciberdefensa del Instrumento Militar de la Nación, así como la determinación de IC a ser protegidas. De igual manera, el Comando interviene en "[…] la supervisión de los centros de respuesta de cada Fuerza y capacitación de personal propio. Además, interviene en la elaboración, revisión y experimentación de la Doctrina de Ciberdefensa"[18] (Casarino & Ortiz, 2019, págs. 47-48).

En diciembre del mismo año y a través del Decreto N° 2645/2014, se definió a la ciberdefensa como "las acciones y capacidades desarrolladas por el instrumento militar en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo" (Capítulo III, Inciso A.II, punto 9, Decreto N° 2645, 2014).

Año 2015

En el mes de marzo del año 2015, se sancionó la Ley N° 27.126 la cual realizó algunas modificaciones a la Ley N° 25.520 del año 2001 (conocida como la Ley de Inteligencia Nacional) que hacía referencia a las bases jurídicas, orgánicas y funcionales del Sistema de Inteligencia de la Nación. Dicha norma estableció que:

> El marco jurídico en el que desarrollarán sus actividades los organismos de inteligencia, conforme la Constitución Nacional, los Tratados de Derechos Humanos suscriptos y los que se suscriban con posterioridad a la sanción de la presente ley y a toda otra norma que establezca derechos y garantías. (Artículo 1°, Ley N° 27.126, 2015)

En el artículo 24 de dicha ley, se disolvió la Secretaría de Inteligencia y se efectuó la transferencia del personal, bienes, presupuesto vigente, activos y patrimonio a la Agencia

[18] En el marco temporal del presente trabajo, no es posible determinar la existencia de la Doctrina de Ciberdefensa y sus implicancias para con las infraestructuras críticas y la ciberseguridad en Argentina.

Federal de Inteligencia (en adelante "AFI") y se mantuvo la función que hace referencia a "la producción de inteligencia criminal referida a los delitos federales complejos relativos a […] ciberdelitos, y atentatorios contra el orden económico y financiero, […] con medios propios de obtención y reunión de información" (Artículo 6°, inciso 2°, Ley N° 27.126, 2015). Asimismo, en el artículo 5° se establece que la AFI "[…] será el organismo superior del Sistema de Inteligencia Nacional y dirigirá el mismo, abarcando los organismos que lo integran" (Artículo 5°, inciso 2°, Ley N° 27.126, 2015).

Ese mismo mes, el Ministerio de Defensa de la Nación emitió una Decisión Administrativa en donde se incorporó la Dirección General de Ciberdefensa, dependiente directamente del ministro, cuya responsabilidad primaria es la de "intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas de ciberdefensa para la jurisdicción del Ministerio de Defensa y su instrumento militar dependiente" (Planilla Anexa al Artículo 1°, Decisión Administrativa N° 15, 2015). Entre las acciones a resaltar, se encuentra la de "entender en la coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de la infraestructura crítica" (Planilla Anexa al Artículo 1°, Decisión Administrativa N° 15, 2015, punto 2).

En el mes de junio del año 2015, a través del Decreto N° 1067/2015, se transfiere el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad a la órbita de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros. Dicha Subsecretaría tenía diversos objetivos como el de formular un marco regulatorio que propicie la identificación y protección de las IC del Sector Público Nacional, las organizaciones civiles, el sector privado y el ámbito académico fomentando la cooperación y colaboración de dichos sectores (Objetivo 1, Planilla Anexa al Artículo 2°, Decreto N° 1067, 2015) así como "entender en la elaboración de la Estrategia Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad, […] elaborar políticas de capacitación para el Sector Público Nacional y contribuir a la capacitación de los sectores nombrados anteriormente" (Objetivos 2 y 5, Planilla Anexa al Artículo 2°, Decreto N° 1067, 2015). En lo que hace a la responsabilidad primaria de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad, es preciso destacar

que debía “entender en todos los aspectos relativos a la ciberseguridad y protección de las IC, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional” (Anexo II, Decreto N° 1067, 2015). En cuanto a las acciones de dicha Dirección, es necesario nombrar:

> Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital […] fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas (punto 4), establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas (punto 5), investigar e incorporar nuevas tecnologías y herramientas en materia de seguridad informática para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional (punto 6), monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad (punto 7), alertar sobre casos de detección de intentos de vulneración de infraestructuras críticas así como de las vulnerabilidades encontradas (punto 8), promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional y al público en general, como también el rol compartido entre el Sector Púbico Nacional y privado para el resguardo de las infraestructuras críticas (punto 13). (Anexo II, Decreto N° 1067, 2015)

De forma complementaria a la Ley de Inteligencia Nacional, en el mes julio del año 2015 se aprobó la Nueva Doctrina de Inteligencia Nacional “[…] que configura un cuerpo doctrinario tendiente a sentar las bases de un profundo proceso de reforma y modernización del Sistema de Inteligencia Nacional” (Considerando, Decreto N° 1311, 2015) y mediante la cual se aprobó la estructura orgánica y funcional de la AFI, entre otras cosas. Dicha Doctrina explicita, en el primer anexo, que:

> La inteligencia nacional es una actividad que se inscribe dentro del marco del Estado constitucional social y democrático de derecho orientada fundamentalmente a producir conocimientos acerca de las problemáticas – riesgos, conflictos – inscritas en la defensa nacional y la seguridad interior, siempre en función de la protección y promoción de los intereses políticos, institucionales, sociales,

económicos y culturales del pueblo argentino. (Anexo 1, Folio 12, Decreto N° 1311, 2015)

En dicha Doctrina, se afirma que en el ámbito de la seguridad interior se debe tener en cuenta una serie de problemáticas relevantes[19] y, específicamente, aquellos fenómenos delictivos como el terrorismo, los atentados contra el orden constitucional y la vida democrática, la criminalidad organizada y "las acciones que atenten contra la ciberseguridad, delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos" (Anexo 1, Folio 14, punto 4, Decreto N° 1311, 2015).

Teniendo en cuenta la problemática de la ciberseguridad de forma específica, la AFI tiene en su estructura funcional la Dirección Operacional de Inteligencia sobre Ciberseguridad, la cual produce información orientada a "[…] las acciones que atenten contra la ciberseguridad en el marco de la defensa nacional o la seguridad interior, y de los grupos nacionales y extranjeros responsables de llevarlas a cabo" (Anexo I, artículo 49, Decreto N° 1311, 2015). Tal como se ilustra en la Figura 2, internamente, dicha Dirección esta compuesta por la Dirección de Inteligencia Informática la cual produce inteligencia relacionada con los "[…] riesgos y conflictos vinculados o derivados del uso de las tecnologías de información y la comunicación que afecten la defensa nacional o la seguridad interior" (Anexo I, artículo 49, inciso a, Decreto N° 1311, 2015) y la Dirección de Inteligencia sobre Delitos Informáticos la cual produce "[…] inteligencia orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades" (Anexo I, artículo 49, inciso b, Decreto N° 1311, 2015) a través de oficiales y analistas de inteligencia especializados en ciberseguridad. La siguiente ilustración mejorada[20] presenta la estructura mencionada:

[19] Las cuales "[…] pueden ser locales, nacionales, internacionales o transnacionales" (Anexo 1, Folio 42, Decreto N° 1311, 2015).

[20] La versión original del organigrama expuesto correspondiente al Decreto N° 1311/2015, Anexo III, Folio 80 puede encontrarse en el Anexo - Captura 1.

Figura 2: Sección del organigrama de la AFI vinculada a la estructura operacional de inteligencia. Fuente: elaboración propia.

En concordancia con esto, en Argentina se determinó que el Sistema de Inteligencia Nacional se encuentra conformado no solo por la AFI, sino también por la Dirección Nacional de Inteligencia Criminal (DINICRI) que depende del Ministerio de Seguridad de la Nación cuya función es "[…] la producción de inteligencia criminal, aunque aquella referida a delitos federales complejos o delitos contra los poderes públicos y el orden constitucional, está a cargo de la AFI" (Anexo I, artículo 18, Decreto N° 1311, 2015) y la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM) dependiente del Ministerio de Defensa que "tiene como función la producción de inteligencia estratégica militar" (Anexo I, artículo 19, Decreto N° 1311, 2015). Esta situación presenta para las Direcciones Nacionales nombradas anteriormente, que dependen del organismo superior del Sistema de Inteligencia Nacional, una dualidad en el reporte de productos. Es decir, dependen organizacionalmente de los ministerios, pero a su vez dependen funcionalmente de la AFI.

Los productos generados (que pueden ser de nivel estratégico o táctico) provienen del análisis de la información de inteligencia[21] obtenida de fuentes públicas o reservadas y son destinados al Presidente de la Nación, a los Ministerios de Defensa y Seguridad, así como a otros ministerios y dependencias gubernamentales pertinentes. Los conocimientos producidos por el Sistema de Inteligencia Nacional permiten la elaboración y formulación de las políticas de defensa nacional y seguridad interior proporcionando "[…] una labor de

[21] Considerada como tal "[…] aquella que comprende las observaciones y mediciones obtenidas o reunidas de fuentes públicas o reservadas, referidas a eventos o problemáticas relevantes del ámbito de la defensa nacional o de la seguridad interior, o que tienen incidencia en estas esferas, y cuya recolección, sistematización y análisis permite elaborar un cuadro de situación del conjunto de las problemáticas en el nivel estratégico o en el nivel táctico" (Anexo 1, artículo 9, Decreto N° 1311, 2015).

apoyo a la toma de decisiones del Estado encargados de la elaboración, formulación, implementación y evaluación de las políticas y estrategias de defensa nacional y de seguridad interior" (Anexo 1, artículo 15, Decreto N° 1311, 2015).

En el mes de agosto se incorporan, a través de la Resolución N° 1046/2015, los organismos que se detallan en la Figura 3[22]:

Figura 3: Sección del organigrama de la Jefatura de Gabinete de Ministros vinculada a la protección de infraestructuras críticas de información y ciberseguridad. Fuente: elaboración propia.

En lo que respecta al presente trabajo, se hará referencia a las tres Direcciones. Primeramente, entre las acciones de la Dirección de Elaboración e Interpretación Normativa, es posible destacar:

> Elaborar los proyectos de normativa […] en materia de protección de infraestructuras críticas de información y ciberseguridad (punto 1); brindar asesoramiento y soporte permanente a las jurisdicciones y entidades del Sector Público Nacional en materia de protección de infraestructuras críticas de información y ciberseguridad (punto 4); interpretar con alcance general y obligatorio para el Sector Público Nacional la normativa sobre la protección de infraestructuras críticas de información y ciberseguridad (punto 5), elaborar convenios marcos con el fin de establecer alianzas bilaterales y multinacionales en materia de protección de infraestructuras críticas de información y ciberseguridad (punto 9). (Anexo II, Resolución N° 1046, 2015)

[22] El organigrama ha sido rediseñado para una mejor visualización de su constitución, pudiendo acceder a la versión original en el Anexo - Captura 2.

Por otra parte, la Dirección Técnica de Infraestructuras Críticas de Información y Ciberseguridad tiene entre sus acciones "analizar los servicios que el Sector Público Nacional brinda a través de la red de internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad" (punto 1, Anexo II, Resolución N° 1046, 2015). Además, la Dirección de Capacitación, Concientización y Difusión debe "diseñar y proponer políticas de capacitación de recursos humanos en materia de ciberseguridad y de protección de infraestructuras críticas de información" (punto 1, Anexo II, Resolución N° 1046, 2015).

A razón de la asunción de la nueva gestión gubernamental nacional, en el mes de diciembre del año 2015, se efectuó un cambio en la organización ministerial de gobierno "con el propósito de racionalizar y tornar más eficiente la gestión pública, creándose nuevos organismos y disponiéndose transferencias de competencias" (Decreto N° 13, 2015). Frente a ello, se incorporó al Ministerio de Modernización en el marco de la necesidad de un Estado moderno y a favor del desarrollo de tecnologías aplicadas a la administración pública central y descentralizada.

Año 2016

En función de las competencias asignadas al Ministerio de Modernización por el decreto nombrado con anterioridad y a favor de la organización de las responsabilidades de cada área, la APN publicó en el mes de enero del año 2016 el Decreto N° 13. En dicho documento, se crea la Subsecretaría de Tecnología y Ciberseguridad y se enumeran doce objetivos entre los cuales es preciso destacar:

> Entender en la elaboración de la estrategia nacional de infraestructura tecnológica, la protección de infraestructuras críticas de información y ciberseguridad en el ámbito del Sector Público Nacional (punto 1); asistir al Ministro en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los sectores (punto 7); difundir las mejores prácticas y elaborar políticas de capacitación para el Sector Público Nacional y contribuir a la capacitación de las organizaciones civiles, del sector privado y del ámbito académico en temas de seguridad de la información y protección de

información crítica, que así lo requieran (punto 10). (Puntos 1, 7 y 10 de la Planilla Anexa al artículo 3°, Decreto N° 13, 2016)

En el mes de julio del mismo año y a través del Decreto N° 898, se mantienen dichos objetivos y se amplían a diecisiete, incorporando algunos relacionados a las telecomunicaciones y redes públicas sin efectuar modificaciones en aquellos relativos a la ciberseguridad e infraestructuras críticas de la información. Sin embargo, es preciso destacar el objetivo quince que establece "participar en grupos de trabajo multisectoriales, comisiones y organismos nacionales e internacionales interviniendo en acuerdos, convenios y tratados internacionales que incluyan aspectos relacionados con redes y telecomunicaciones en el Sector Público Nacional" (Decreto N° 898, 2016).

Por otra parte, el Ministerio de Defensa de la Nación también sufrió modificaciones a partir de la asunción del nuevo gobierno y se creó la Subsecretaría de Ciberdefensa dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa. Se reemplazó a la Dirección General de Ciberdefensa, se eliminó la responsabilidad primaria que tenía anteriormente y se mantuvo la acción relacionada con "entender en la coordinación con los organismos y autoridades de los distintos Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructuras críticas" (Planilla anexa al artículo 2°, Decreto N° 42, 2016).

En el mes de marzo, a través de la Decisión Administrativa N° 232/2016, se aprueba la estructura organizativa dentro del Ministerio de Modernización que se observa en la Figura 4[23]:

[23] El organigrama ha sido rediseñado para una mejor visualización de su constitución, pudiendo acceder a la versión original en el Anexo - Captura 3.

Figura 4: Sección del Organigrama del Ministerio de Modernización vinculada a la tecnología y ciberseguridad. Fuente: elaboración propia.

Específicamente, se hará referencia a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dado que la responsabilidad primaria y las acciones tienen relación directa con el objetivo del presente trabajo final de maestría. Frente a ello, es preciso destacar que su principal responsabilidad es la de "asistir en todos los aspectos relativos a la ciberseguridad y protección de las IC, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional" (Anexo II, Decisión Administrativa N° 232, 2016). Entre las acciones a realizar se destaca:

> Elaborar, en coordinación con el sector privado, políticas de resguardo de la seguridad digital con actualización constante, con foco específico en las infraestructuras críticas (punto 4); monitorear los servicios que el Sector Público Nacional brinda a través de la red de internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad (punto 7) y alertar en casos de intentos de vulneración de infraestructuras críticas así como de las vulnerabilidades encontradas (punto 8). (Anexo II, Decisión Administrativa N° 232, 2016)

En el mes de mayo del año 2016 se aprobó, a través de la Decisión Administrativa N° 546/2016, la estructura organizativa del Ministerio de Defensa. Allí se incorporó la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa y la Dirección Nacional de Diseño de Políticas de Ciberdefensa, ambas dependientes de la Subsecretaría de Ciberdefensa como se observa en la Figura 5[24]:

[24] Dada la multiplicidad de áreas y la longitud de la nomenclatura, el organigrama del Ministerio de Defensa ha sido rediseñado para una mejor percepción de los componentes. El esquema original se encuentra disponible en el Anexo - Captura 4.

Figura 5: Sección del organigrama del Ministerio de Defensa vinculada a la ciencia, tecnología y producción para la defensa. Fuente: elaboración propia.

Considerando el presente trabajo, se hará hincapié en la responsabilidad primaria de la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa quien debe "coordinar los trabajos y proyectos en investigación y desarrollo en el tema de la ciberdefensa entre el Ministerio, el Estado Mayor Conjunto de las Fuerzas Armadas, los Estados Mayores Generales de las Fuerzas Armadas y otros organismos públicos y privados" (Decisión Administrativa N° 546, 2016).

En el mes de noviembre de dicho año y a través de la Resolución N° 490-E/2016, el Ministerio de Modernización de la Nación determinó la estructura organizativa de segundo nivel de la Subsecretaría de Tecnología y Ciberseguridad, así como las coordinaciones que se desprenden de las mismas tal como puede observarse en la Figura 6[25]:

Figura 6: Sección del organigrama del Ministerio de Modernización vinculada a la tecnología y ciberseguridad. Fuente: elaboración propia.

[25] El esquema original se encuentra disponible en el Anexo - Captura 5.

Como puede observarse en la Figura 6, la Dirección de Operaciones Técnicas de Ciberseguridad depende de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad y en el Anexo II de la Resolución N° 490-E se establecen las acciones que debe cumplir. Por otra parte, algunas de las acciones que debía efectuar dicha Dirección Nacional, fueron delegadas a la Dirección de Operaciones Técnicas de Ciberseguridad. Frente a ello, es preciso destacar las siguientes:

> Proponer y coordinar el diseño de políticas, normas y procedimientos destinados a fortalecer la seguridad de la información, la seguridad informática y la protección de las infraestructuras críticas de información (punto 1); analizar los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad (punto 2) y alertar sobre casos de detección de intentos de vulneración de infraestructuras críticas así como de las vulnerabilidades encontradas (punto 3). (Anexo II, Resolución N° 490-E/2016, 2016)

Además, la Resolución N° 490-E/2016 incorpora, dentro de la estructura de la Dirección de Operaciones Técnicas de Ciberseguridad, dos Coordinaciones como se muestra en la Figura 7[26]:

[26] La figura fue creada e incluida en el trabajo con el objetivo de que pueda visualizarse la estructura organizativa ya que la norma carece de una esquematización.

Figura 7: Sección del organigrama que muestra la estructura de la Dirección de Operaciones Técnicas de Ciberseguridad. Fuente: elaboración propia.

Considerando el presente trabajo, es menester destacar la sexta acción de la Coordinación de Operaciones de Ciberseguridad que establecía "proponer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas en materia de su competencia" (Anexo IV, Resolución N° 490 - E/2016, 2016). Por otra parte, es posible recalcar que la Coordinación de Proyectos e Investigación de Ciberseguridad incluye acciones tales como el desarrollo e integración de las plataformas de análisis de vulnerabilidades, de gestión y de servicios de ciberseguridad y de infraestructuras críticas de información de la Subsecretaría de Tecnología y Ciberseguridad (punto 1), investigar sobre nuevas tecnologías y herramientas en materia de seguridad informática y las relativas a nuevas amenazas cibernéticas (punto 5), colaborar con el sector privado para elaborar conjuntamente políticas de resguardo de la seguridad digital con actualización constante haciendo especial hincapié en las IC (punto 7), entre otras.

Año 2017

En el mes de julio del año 2017 se crea el Comité de Ciberseguridad en la órbita del Ministerio de Modernización a través del Decreto N° 577/2017 (aún vigente). Dicha norma establece que el Comité estará integrado por los Ministerios de Modernización, de Defensa y de Seguridad y, posteriormente, se amplió la composición de dicho organismo y se integraron representantes de la Secretaría de Asuntos Estratégicos, del Ministerio de

Relaciones Exteriores y Culto y del Ministerio de Justicia y Derechos Humanos[27] mediante el Decreto N° 480/2019.

Los fundamentos para la creación del Comité se basan en la necesidad de obtener la "capacidad para responder a incidentes de seguridad de gran escala, legislación en la materia, la protección de infraestructuras críticas, capacidad para colaborar con otros países, así como la cultura de seguridad desarrollada por los ciudadanos" (Decreto N°577, 2017) y se plantea la necesidad de que se realice una adecuada protección en materia de ciberseguridad dado el incremento y la diversidad en las amenazas y ataques informáticos que podría generar un amplio impacto en las IC del país.

El Comité fue creado con el objetivo de elaborar la Estrategia Nacional de Ciberseguridad[28] en coordinación con las áreas competentes de la APN (artículo 2°, inciso a, Decreto N° 577, 2017) y, además, se le encomendó a dicho Comité diversas tareas enumeradas en el segundo artículo del Decreto entre las que se encuentran:

> Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad (inciso b), convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente (inciso c), impulsar el dictado de un marco normativo en materia de Ciberseguridad (inciso d), y fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales (inciso e). (Artículo 2°, Decreto N° 577/2017)

En el mes de octubre del mismo año, el Ministerio de Seguridad de la Nación resolvió, a razón de la iniciativa de la Unión Internacional de Telecomunicaciones denominada Agenda sobre Ciberseguridad Global, la Estrategia Nacional de Ciberseguridad, la fuerte dependencia de la Ciberseguridad en la prestación de servicios esenciales, la creación del

[27] Dicha incorporación se sustenta en el alcance global y abordaje internacional de las amenazas, la transversalidad a las diferentes áreas del gobierno y a la necesidad de una adecuación permanente del marco normativo.

[28] Conviene destacar que en el marco de dicho Decreto, se considera como necesario que la Estrategia contemple los propósitos y objetivos para desarrollar el marco normativo así como medidas técnicas, organizacionales, de políticas y procedimientos a favor de la protección del ciberespacio incluidas las infraestructuras críticas a la vez que desarrolla una cultura de ciberseguridad.

Comité de Ciberseguridad y la existencia de Equipos de Respuesta ante Incidentes de Seguridad Informática, la conformación del Comité de Respuesta de Incidentes de Seguridad Informática propio. La Resolución N° 1107 establece los objetivos del Comité de Respuesta entre los cuales se encuentra "colaborar en la protección de las infraestructuras críticas del MINISTERIO DE SEGURIDAD y sus órganos dependientes" (artículo 1°, inciso b, Resolución N° 1107-E/2017, 2017), y tendrá dentro de sus funciones la elaboración de "[…] informes de recomendación para la protección de las IC del Ministerio de Seguridad y sus órganos dependientes" (artículo 5°, inciso g, Resolución N° 1107-E/2017, 2017), entre otras.

Año 2018

En el mes de marzo del año 2018, a través del Decreto N° 174/2018 se efectuó un reordenamiento en el organigrama del PEN donde se reformaron diversos organismos y suprimieron aquellos cargos considerados como innecesarios. A partir de dicha norma, el Ministerio de Defensa sufrió cambios como que la Subsecretaría de Ciberdefensa pasó a depender de la Secretaría de Investigación, Política Industrial y Producción. Dicha Secretaría tenía entre sus objetivos el de "entender en la formulación, aprobación y supervisión del cumplimiento de las políticas y programas de los organismos de investigación y desarrollo del sector de Ciberdefensa" (Decreto N° 174, 2018, objetivo n° 9) así como incentivar el intercambio de información y coordinar los organismos científicos y tecnológicos relacionados con ciberdefensa.

En el caso de la Subsecretaria de Ciberdefensa, tiene el objetivo de ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas, así como otros nueve objetivos entre los que es posible destacar:

> Entender en la coordinación con los organismos y autoridades de los distintos Poderes del Estado para contribuir desde la jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica (Objetivo 2); y fomentar políticas de convocatoria, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado (Objetivo 7). (Decreto N° 174, 2018)

En lo que hace a la cooperación en la investigación y asistencia técnica, la Subsecretaría de Ciberdefensa tiene entre sus objetivos "promover el intercambio y la cooperación en materia

de ciberdefensa con los ámbitos académico, científico y empresarial" (Objetivo 8, Decreto N° 174, 2018) e "impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados" (Objetivo 9, Decreto N° 174, 2018).

Cabe destacar, similar al Sistema de Inteligencia Nacional, que a partir de dicha norma el Comando Conjunto de Ciberdefensa depende funcionalmente de la Subsecretaría de Ciberdefensa, pero depende organizacionalmente del Estado Mayor Conjunto de las Fuerzas Armadas.

Considerando al Ministerio de Modernización, se crea la Secretaría de Infraestructura Tecnológica y País Digital cuyos objetivos se encuentran en el Decreto N° 174/2018. Allí, se repiten varios de los objetivos pertenecientes a la Subsecretaría de Tecnología y Ciberseguridad (Decreto N° 898/2016). Los objetivos repetidos se relacionan con: la elaboración de la estrategia nacional de infraestructura tecnológica y la protección de infraestructuras críticas de información; la asistencia al ministro para la formulación de un marco regulatorio específico que propicie la identificación y protección de las IC del Sector Público Nacional; el entendimiento en materia de dictado de normas, políticas, estándares y procedimientos de Infraestructura Tecnológica y Ciberseguridad; y la difusión de buenas prácticas y elaboración de políticas de capacitación para el sector público, organismos civiles, el sector privado y el ámbito académico a favor de la seguridad de la información y la protección de información crítica y protección de información crítica.

Por otra parte, la Secretaría de Infraestructura Tecnológica y País Digital incorpora en el objetivo relacionado con la cooperación internacional, el concepto de ciberseguridad ya que debe:

> Participar en grupos de trabajo multisectoriales, comisiones y organismos nacionales e internacionales interviniendo en acuerdos, convenios y tratados internacionales que incluyan aspectos relacionados con infraestructura tecnológica, ciberseguridad, redes y telecomunicaciones en el Sector Público Nacional. (Objetivo 12, Decreto N° 174, 2018)

En el mes de marzo del año 2018, el Jefe de Gabinete de Ministros aprobó varias estructuras organizativas a través de la Decisión Administrativa N° 297/2018 y se determinaron aquellas áreas dependientes de las Secretarías creadas en el Decreto N° 174/2018. Considerando el

carácter del tema a analizar en el presente trabajo, se hará mención a la Secretaría de Infraestructura Tecnológica y País Digital, y se hará especial hincapié en la Dirección Nacional de Infraestructura Tecnológica y Ciberseguridad y su estructura compuesta por tres direcciones y tres coordinaciones, con sus respectivas jerarquías, como puede observarse en la Figura 8[29]:

Figura 8: Sección del organigrama del Ministerio de Modernización vinculada a la infraestructura tecnológica y ciberseguridad. Fuente: elaboración propia.

Considerando las acciones que se desprenden de las áreas dependientes de la Dirección Nacional de Infraestructura Tecnológica y Ciberseguridad, se hará referencia a la Dirección de Infraestructuras Críticas de Información y Ciberseguridad, a la Coordinación de Operaciones de Ciberseguridad, así como a la Coordinación de Comunicación y Proyectos de Ciberseguridad dada su vinculación con el presente trabajo. Entre las acciones de la Dirección nombrada, conviene destacar:

> Supervisar el cumplimiento de la normativa vigente en materia de ciberseguridad (acción n° 1); asistir en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, comprendiendo la generación de capacidades de detección, defensa y respuesta ante incidentes del Sector Público Nacional (acción n° 2); proponer y diseñar la política de seguridad de la información y ciberseguridad […] en coordinación con el sector privado, políticas de resguardo con actualización constante, con foco específico en las infraestructuras críticas (acción n° 5);

[29] Las versiones originales se encuentran en el Anexo - Capturas 6 y 7.

> investigar e incorporar nuevas tecnologías y herramientas que permitan detectar de forma automática las vulnerabilidades de ciberseguridad para minimizar los riesgos de la infraestructura digital del Sector Público Nacional (acción n° 6); monitorear los servicios que el Sector Público Nacional brinda a través de la red de internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad y alertar en casos de intentos de vulneración. (Decisión Administrativa N° 297, 2018, Anexo IV, pág. 31-32)

Por otra parte, entre las acciones definidas para la Coordinación de Operaciones de Ciberseguridad es posible recalcar aquella que hace referencia a la recepción de las alertas generadas por organismos de diversos niveles del Gobierno en el territorio nacional y entes del sector privado que posean información sobre IC (acción n° 4) y "desarrollar e integrar las plataformas de análisis de vulnerabilidades, de gestión, y de servicios de ciberseguridad y de infraestructuras críticas de información" (acción n° 6) (Decisión Administrativa N° 297, 2018, Anexo IV, págs. 27). En lo que respecta al marco normativo y a los proyectos relacionados con ciberseguridad, la Coordinación de Comunicación y Proyectos de Ciberseguridad tiene entre sus acciones:

> Promover la cultura de ciberseguridad incluyendo la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las organizaciones de gobierno, la ciudadanía y el sector privado (acción n°4); desarrollar e integrar las plataformas de análisis de vulnerabilidades, de gestión, y de servicios de ciberseguridad y de infraestructuras críticas de información (acción n° 6). (Decisión Administrativa N° 297, 2018, Anexo IV, págs. 28 y 29)

En julio de dicho año, el Ministerio de Defensa actualizó los lineamientos y las prioridades estratégicas mediante la aprobación de una nueva Directiva de Política de Defensa Nacional dentro de la cual se considera que "[…] la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independiemente del origen de la agresión" (Anexo I, Decreto N° 703, 2018, pág. 9). Asimismo, a favor de la prevención de ciberataques y ciberexplotación contra las IC, el Ministerio de Defensa deberá "[…] fortalecer las capacidades de vigilancia y control del ciberespacio" (Anexo I, Decreto N° 703, 2018, pág. 25). Sin embargo, se define que el Estado Mayor Conjunto de las Fuerzas Armadas deberá no solo fortalecer las capacidades

de anticipación, sino también de disuasión, vigilancia y control de aquellas infraestructuras consideradas como críticas que sean del Sistema de Defensa Nacional específicamente.

Posteriormente, y a través del Decreto N° 802/2018, se creó el cargo de Secretario de Gobierno de Modernización quien debiera continuar las acciones y responsabilidades del Ministro de Modernización de la Nación.

Año 2019

En el mes de febrero del año 2019 se realizó nuevamente una modificación en el organigrama de la APN a través de la Decisión Administrativa N° 103/2019, la cual altera el nombre de la Dirección Nacional de Ciberseguridad (antes Dirección Nacional de Infraestructura Tecnológica y Ciberseguridad), y pasa a depender directamente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros (antes dependía de la Secretaría de Infraestructura de Tecnología y País Digital dependiente del Ministerio de Modernización). De dicha Dirección Nacional se desprenden dos organismos de los seis que había previamente y, en general, las acciones que se detallaban se distribuyeron entre ambas. En la Figura 9[30] se observa la nueva organización:

Figura 9: Sección del organigrama de la Jefatura de Gabinete de Ministros vinculada a la ciberseguridad. Fuente: elaboración propia.

La responsabilidad primaria de la Dirección Nacional de Ciberseguridad era la de "entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas

[30] Este es otro ejemplo de organigrama donde los nombres de las áreas operacionales no pueden verse correctamente por el tamaño del recuadro que los contiene, hecho que propició la alteración de su morfología, manteniendo el original en un apartado que puede ser accedido en el Anexo - Captura 8 del presente trabajo.

de información, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional" (Decisión Administrativa N° 103, 2019, Anexo II, pág. 2) y se determinan las acciones que debe efectuar, entre las que es posible destacar:

> Elaborar, en coordinación con el sector privado, políticas de resguardo de la seguridad digital con actualización constante, con foco específico en las infraestructuras críticas (acción 3); establecer prioridades y planes estratégicos de abordaje de la ciberseguridad, fomentando el desarrollo de proyectos de cooperación otros Estados y Organismos internacionales y nacionales (acción 4). (Decisión Administrativa N° 103, 2019)

Considerando a la Dirección de Infraestructuras Críticas de Información, es menester destacar las siguientes acciones:

> Proponer y diseñar la política de seguridad de la información y ciberseguridad, incluyendo, en coordinación con el sector privado, políticas de resguardo con actualización constante, con foco específico en las infraestructuras críticas (acción n° 4); monitorear los servicios que el Sector Público Nacional brinda a través de la red de internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad y alertar en casos de intentos de vulneración de infraestructuras críticas, así como de las vulnerabilidades encontradas (acción n° 6). (Anexo V, págs. 6 y 7, Decisión Administrativa N° 103, 2019)

En el caso de la Coordinación de Comunicación y Proyectos de Ciberseguridad, es preciso resaltar las siguientes acciones:

> Promover la realización de proyectos de cooperación con otros Estados y Organismos internacionales y nacionales, incluyendo provincias, municipios y ámbitos de innovación y desarrollo […] (acción n° 1); proveer apoyo tecnológico a los organismos del Sector Público Nacional y organizaciones privada que por su infraestructura sean de interés nacional en análisis de vulnerabilidades, estructuras de protección de centros de datos, y riesgos de ciber-amenazas en general, con foco

especial en las infraestructuras críticas teniendo en cuenta los recursos disponibles (acción n° 8). (Anexo V, págs. 5 y 6, Decisión Administrativa N° 103, 2019)

En el mes de mayo de dicho año, en virtud de lo establecido en el decreto que creó el Comité de Ciberseguridad, se aprobó la Estrategia Nacional de Ciberseguridad (aún vigente) que define los principios esenciales y ocho objetivos centrales del país en lo que respecta a la protección del ciberespacio, dentro de los cuales se establecen acciones concretas. Dicha Estrategia, considerada como un documento fundacional y dinámico, se basa en que el ciberespacio es un elemento esencial en la vida de las personas y las organizaciones que involucra "[…] graves riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos terroristas y la confrontación entre los Estados" (Resolución N° 829, 2019).

La Estrategia Nacional de Ciberseguridad se sustenta en los siguientes principios rectores:

- el respeto por los derechos y libertades individuales;
- el liderazgo, construcción de capacidades y fortalecimiento federal;
- la integración internacional;
- la cultura de ciberseguridad y responsabilidad compartida entre organizaciones públicas y privadas, académicas, sociedad civil y la ciudadanía; y
- el fortalecimiento del desarrollo socioeconómico.

Por otra parte, la Estrategia propone ocho objetivos fundamentales a cumplir que permitirán fijar las previsiones nacionales en materia de protección del ciberespacio como ser: 1) concientización del uso seguro del Ciberespacio entendido como "[…] el proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ello la adopción de habitos basados en las mejores prácticas" (Anexo I, Resolución N° 829, 2019, pág. 5); 2) capacitación y educación en el uso seguro del ciberespacio "[…] entendido como el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio" (Anexo I, Resolución N° 829, 2019, pág. 5); 3) desarrollo del marco normativo con el fin de "adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos para hacer frente a los desafíos que plantean los riesgos del ciberespacio asegurando los derechos fundamentales" (Anexo I, Resolución N° 829, 2019, pág. 6); 4) fortalecimiento de capacidades de prevención, detección y respuesta "[…] frente

al uso del Ciberespacio con fines ilegales" (Anexo I, Resolución N° 829, 2019, pág. 6); 5) protección y recuperación de los sistemas de información del Sector Público; 6) fomento de la industria nacional de la ciberseguridad; 7) cooperación internacional a favor de "contribuir a la mejora de la ciberseguridad en el ámbito internacional" (Anexo I, Resolución N° 829, 2019, pág. 7); y 8) la protección de las infraestructuras críticas nacionales de la información para el "fortalecimiento de la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país" (Anexo I, Resolución N° 829, 2019, pág. 7). Las acciones a destacar del octavo objetivo incluyen: la promoción de la definición, identificación y protección de dichas infraestructuras; la articulación del sector público-privado "[…] para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques, a partir de los recursos y responsabilidades de cada organización" (Anexo I, Resolución N° 829, 2019, pág. 8); el fortalecimiento de "[…] la cooperación para el intercambio de información ante vulnerabilidades y amenazas" (Anexo I, Resolución N° 829, 2019, pág. 8.

En dicha Resolución, se consideró a la Secretaría de Gobierno de Modernización como el "[…] organismo apropiado para dar impulso a los actos administrativos y acciones necesarios a fin de cumplir con los objetivos de la citada Estrategia Nacional de Ciberseguridad" (Resolución N° 829, 2019) y se creó la Unidad Ejecutiva para que coordine el funcionaminto y brinde asistencia administrativa al Comité de Ciberseguridad (Anexo II, Resolución N° 829, 2019).

En el mes de septiembre de ese mismo año, se estableció la definición de infraestructuras críticas de la información, así como los criterios de identificación y los sectores a considerar con el fin de elaborar "[…] las normas, políticas y planes para la protección de las infraestructuras que respaldan servicios críticos, permitiendo la identificación de sistemas, equipamiento y actores involucrados" (Considerando, Resolución N° 1523, 2019). Además, se dispuso un glosario de términos relacionados con la ciberseguridad con el fin de establecer un lenguaje común entre los distintos actores que intervengan y cuya revisión y actualización pasa a ser responsabilidad del Director Nacional de Ciberseguridad.

Se define a las infraestructuras críticas de la información como "[…] las tecnologías de información, operación y comunicación, así como la información asociada que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas" (Resolución N° 1523, 2019, Anexo I) y a las IC como:

> Aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. (Resolución N° 1523, 2019, Anexo I)

Por otra parte, los criterios de identificación son el impacto en la vida humana, en lo económico, en el medio ambiente, en el ejercicio de los derechos humanos y de las libertades individuales, en lo público o social, en el ejercicio de las funciones del Estado, en la soberanía nacional y en el mantenimiento de la integridad territorial nacional. En adición a esto, se avanzó en la determinación de aquellos sectores que deben considerarse para la eventual identificación de las IC: el de energía, tecnologías de información y comunicaciones, transportes, hídrico, salud, alimentación, finanzas, nuclear, químico, espacial y Estado.

Por otra parte, en el mes de octubre del año 2019, se actualizó el Organigrama de Aplicación de la APN mediante el Decreto N° 684/2019 y, en lo que hace al Ministerio de Defensa y al presente trabajo, se hará referencia a la estructura organizativa que se observa en la Figura 10[31]:

[31] Se esquematiza la figura a partir de lo expuesto en la Planilla Anexa al artículo 2°, Anexo II del Decreto N° 684/2019

Figura 10: Sección del organigrama del Ministerio de Defensa que muestra la estructura de las Subsecretarías nombradas. Fuente: elaboración propia.

En particular, la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares, tiene entre sus objetivos el de ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas y, además:

> Asistir al Secretario en el planeamiento, diseño y elaboración de la política de ciberdefensa […] (Objetivo 1); impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados (Objetivo 13). (Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019)

En lo que hace a los objetivos de la Subsecretaría de Ciberdefensa que se relacionan con las IC, conviene destacar:

> Entender en la coordinación con los organismos y autoridades de los Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica (Objetivo 8); asistir al Secretario en el dictado de normas para el diseño, implantación y construcción de las redes soporte operacional de Infraestructuras Críticas de interés para la Defensa Nacional, reduciendo el riesgo de vulnerabilidades cibernéticas que limiten la disponibilidad de acceso y la operabilidad de los titulares de dichas Infraestructuras críticas (Objetivo 9); y entender en la coordinación con las agencias u organismos reguladores de la prestación de los servicios esenciales y de producción de bienes de interés para la Defensa Nacional, como contribución para la elaboración de normas específicas relativas a la protección de la tecnología operacional (OT) de

> esas infraestructuras críticas y de los procesos productivos de interés para la Defensa Nacional (Objetivo 11). (Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019)

Por otra parte, la Subsecretaría de Investigación Científica y Política Industrial para la Defensa, que depende de la Secretaría de Investigación, Política Industrial y Producción para la Defensa ,tiene diversos objetivos entre los cuales es posible distinguir:

> Asistir al Secretario en la formulación de políticas, planes, programas, medidas e instrumentos para el desarrollo y gestión de un Sistema Científico y Tecnológico para la Defensa, que articule con los organismos y recursos del sector […] (Objetivo 1); y asistir en la elaboración de un plan plurianual científico y tecnológico para la defensa y sus reformulaciones, como así también en la complementación y apoyo entre el Sistema Científico Tecnológico para la Defensa y el sector privado (Objetivo 5). (Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019)

El 25 de octubre del año 2019, el Ministerio de Defensa de la Nación publicó la Resolución N° 1380/2019 la cual efectúa una modificación de la definición de ciberdefensa entendiendo a la misma como:

> Las acciones y capacidades desarrolladas por el Ministerio de Defensa, el Estado Mayor Conjunto y las Fuerzas Armadas para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar […] a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia. (Artículo 1°, Resolución N° 1380, 2019)

Asimismo, la Resolución hace referencia a las IC de la Defensa Nacional[32] agrupando dentro de las mismas aquellas:

[32] Consideradas como "[…] las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto en la capacidad operacional del Instrumento Militar en el ciberespacio y/o en la prestación de los servicios esenciales así como la producción de bienes de interés para la Defensa". (Resolución N° 1380, 2019, Anexo I, pág. 7)

> Del instrumento militar, las propias del Ministerio de Defensa, así como las denominadas Infraestructuras Críticas de Interés para la Defensa Nacional, que agrupa a las soporte de Servicios Esenciales de interés para la defensa y las de los procesos productivos de bienes sensibles. (Considerando, Resolución N° 1380, 2019)

Además, dicha Resolución tiene en anexo la Política de Ciberdefensa la cual tiene en cuenta, entre otras aristas, la creación del Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa Nacional y el Centro Nacional de Ciberdefensa. Considerando el Plan, el mismo establece su objetivo[33] y los actores intervinientes en la protección de dichas IC tales como el Comité de Ciberseguridad, Secretaría de Gobierno de Modernización, Entes Reguladores, Operadores Críticos y el Ministerio de Defensa. Es de destacar que se le da a los Entes Reguladores la potestad de "elaborar el catálogo de infraestructuras críticas del sector estratégico que les corresponda" (Anexo 4, Resolución N° 1380, 2019, pág. 9). Además, el Plan enumera una serie de instrumentos de política: regulatorios, para la interacción en el ciberespacio, y educativos y de concientización. Asimismo, se determina que la Subsecretaría de Ciberdefensa es el órgano dentro del Ministerio de Defensa "responsable de la Protección de las infraestructuras críticas de la Defensa Nacional" (Anexo 4, Resolución N° 1380, 2019, pág. 10) y que "[…] desde el CSIRT[34] DEFENSA se realizará el monitoreo de las redes OT[35] de las IICC de los servicios esenciales de interés para la Defensa Nacional…" (Resolución N° 1380, 2019, Anexo 4, Pág. 10) procesando, además, "[…] la información recibida desde los sensores y demás hardware específico de las redes TO que se instalen en los puntos acordados con los Entes Reguladores de los servicios

[33] "Fortalecer la seguridad y la capacidad de recuperación de la infraestructura crítica de la Defensa, mediante la gestión de riesgos físicos y cibernéticos a través de los esfuerzos colaborativos e integrados de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras de soporte, conforme corresponda según se trate de IICC Propias o IICC de Interés para la Defensa Nacional". (Anexo 4, Resolución N° 1380, 2019, pág. 7)

[34] La Organización de Estados Americanos (OEA) establece que "un equipo de respuesta a incidentes en seguridad informática (CSIRT por sus siglas en inglés) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular. […] Los CSIRT a nivel nacional […] responden a incidentes en seguridad informática a nivel de un estado-país". (OEA, 2016, pág. 3)

[35] "La tecnología operativa [o TO, cuyo acrónimo en inglés es *OT* y proviene de *Operational Technology*] es hardware y software que detecta o causa un cambio, a través del monitoreo y/o control directo de equipos industriales, activos, procesos y eventos" (Gartner, 2020).

esenciales y objetivos estratégicos de las IICC de interés para la Defensa" (Anexo 4, Resolución N° 1380, 2019, pág. 6).

3.3. El modelo de España

Hasta el momento, en el presente trabajo se analizó el estado jurídico-institucional de las IC y la ciberseguridad en Argentina. Sin embargo, para tener otra perspectiva, es necesario tomar como referencia la experiencia y el estado del arte en otros países. Por ello, se analizará de forma breve las normas e instituciones de España para efectuar un análisis de derecho comparado[36], con el fin de obtener conclusiones teóricas y de orden práctico que nos permita realizar, más adelante, aportes para nuestro país. En efecto, se ha considerado a España dada la similitud en la cultura, cantidad de habitantes, el idioma y la influencia en materia legislativa, además del lugar que ocupa en el ranking del Índice Nacional de Ciberseguridad (*NCSI* por su sigla en inglés) como se verá a continuación.

3.3.1. Índice Nacional de Ciberseguridad

El Índice Nacional de Ciberseguridad (en adelante *"NCSI"*) es un índice global elaborado por la *e-Governance Academy* (en español Academia de Gobierno Electrónico[37]) que provee una visión general de la capacidad en ciberseguridad de cada país, señalando buenas prácticas y mostrando qué aspectos deben mejorarse. Inclusive, mide la preparación de los países para la prevención de las amenazas cibernéticas y la gestión de los incidentes cibernéticos. Se basa en una metodología transparente donde los datos que se observan de cada país son de acceso público y se actualizan constantemente a medida que se obtiene nueva información y luego de verificar la evidencia enviada (*National Cyber Security Index,* 2019). Para que la evidencia sea aceptada:

> Todos los materiales de prueba deben ser de información pública y de acceso público. Solo los datos oficiales pueden considerarse probatorios. Las evidencias

[36] "Disciplina consiste en el estudio comparativo de instituciones o sistemas jurídicos pertenecientes a diversos lugares o épocas, con el fin de determinar las notas comunes y las diferencias que entre ellos existen, y derivar de tal examen conclusiones sobre la evolución de tales instituciones o sistemas, y criterios para su perfeccionamiento y reforma". (Torré, 2003, pág. 98)

[37] Es una organización de consultoría compuesta por un grupo de expertos fundada para la creación y transferencia de conocimiento y mejores prácticas relacionadas con e-gobernanza, e-democracia, ciberseguridad y el desarrollo de sociedades de información abierta. (Rikk, 2018, pág. 34)

> aceptadas son: actos legales, documentos oficiales y sitios web oficiales. (National Cyber Security Index, 2021)

En particular, el índice incluye los aspectos más importantes relacionados con la seguridad de la red y la información, la identificación electrónica, la protección de datos personales y los servicios esenciales de un país, entre otros aspectos (Rikk, 2018). Para su evaluación, se enfoca en aspectos mensurables y tiene en cuenta la legislación vigente, las unidades establecidas (organizaciones, departamentos, etc.), los formatos de cooperación (por ejemplo: consejo, comité, etc.) y los resultados o productos obtenidos (por ejemplo: políticas, ejercicios etc.).

Para el presente trabajo y con el fin de considerar a España y Argentina en lo que respecta a su situación en ciberseguridad y servicios esenciales, se emplea dicho índice porque se caracteriza por utilizar evidencia pública conformada por actos legales y normas, documentos y sitios web oficiales. Contar con la posibilidad de tener y analizar un índice que permita valorar la capacidad en ciberseguridad de ambos países con base en indicadores valorables numéricamente obtenidos mediante una metodología transparente, es clave para asentar las diferencias básicas entre la Argentina y España en lo que hace a las IC y la ciberseguridad. Desde el principio y considerando el ranking mundial de países del Índice, es sencillo observar que el país europeo supera ampliamente a Argentina. Sin embargo, poder observar cuáles son los indicadores que diferencian a ambos, permite evaluar por dónde empezar y qué acciones debe tomar Argentina para estar mejor posicionada a nivel internacional.

En diciembre del año 2019, se realizó una consulta en la página del *NCSI* y en el ranking de los cinco primeros países se encontraba Grecia, República Checa, Estonia, España y Lituania como se muestra en la Figura 11:

Figura 11: Ordenamiento de los mejores cinco de países del *National Cyber Security Index*. Fuente: *National Cyber Security Index*, 2019.

Además, se muestra una captura de pantalla de la página web donde se puede observar el número de ranking, el país, el índice (*NCSI*), el nivel de desarrollo digital (DDL)[38] y la diferencia[39]. Allí se observa que España se encuentra en el cuarto puesto del índice nacional de ciberseguridad, en contraposición a nuestro país, que ocupa el puesto número 57° en el ranking:

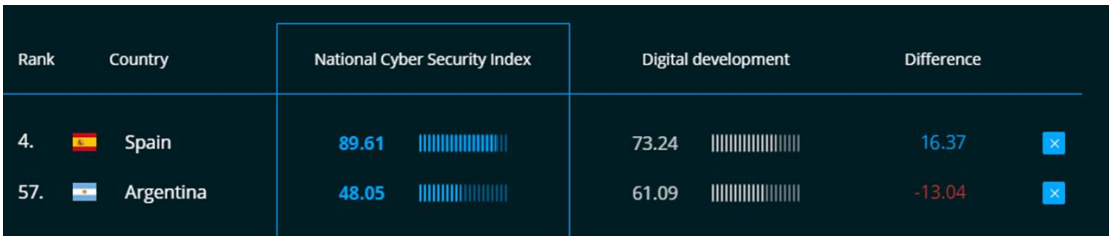


Figura 12: Comparativa de España y Argentina considerando el Índice Nacional de Ciberseguridad y el Desarrollo Digital entre ambos países. Fuente: *National Cyber Security Index*, 2019.

El *NCSI* se basa en tres indicadores, compuestos a su vez por cuatro criterios valorados numéricamente que permiten evaluar la situación del país al momento de efectuar la búsqueda en la página. Los indicadores son: generales de ciberseguridad, línea base de ciberseguridad y gestión de incidentes y crisis.

El primer indicador está compuesto por el desarrollo de políticas de ciberseguridad, la información y análisis sobre ciberamenazas, el desarrollo educativo y profesional, y la contribución global a la ciberseguridad. En materia de políticas, ambos países se encuentran

[38] Acorde a la página, el DDL muestra el porcentaje de cumplimiento promedio del índice de desarrollo de las TIC y el índice de preparación en red.

[39] Muestra la diferencia entre *NCSI* y *DDL*. En azul: ciberseguridad avanzada. En rojo: ciberseguridad detrás del desarrollo digital.

al mismo nivel habiendo desarrollado de igual forma la unidad de política de ciberseguridad, la coordinación en política de ciberseguridad y la estrategia de ciberseguridad. Sin embargo, ninguno de los dos países ha desarrollado el plan para la implementación de la estrategia de ciberseguridad como puede observarse en la Figura 13:

Figura 13: Comparativa de España y Argentina considerando el desarrollo de políticas de ciberseguridad. Fuente: *National Cyber Security Index*, 2019.

Considerando la contribución global para con la ciberseguridad, Argentina ha avanzado de igual manera que España en lo que hace a la Convención sobre la Ciberdelincuencia y en la representación en formatos de cooperación internacional.

A razón de los indicadores sobre protección de los servicios esenciales, se tiene en cuenta la identificación de los operadores de servicios esenciales mediante un acto legal, los requisitos de seguridad cibernética para operadores de servicios esenciales (quienes deberán gestionar los riesgos), la autoridad competente para la supervisión de los operadores de servicios esenciales en relación a los requisitos de ciberseguridad y el monitoreo regular de las medidas de seguridad que permita evidenciar la implementación efectiva de las políticas de seguridad informática. Lamentablemente, Argentina no cumple con ninguno de estos criterios mientras que España ha avanzado considerablemente en cada uno, como se puede observar en la Figura 14:

Figura 14: Comparativa de España y Argentina considerando la protección de servicios esenciales. Fuente: *National Cyber Security Index*, 2019.

Finalmente, considerando los indicadores de incidentes y gestión de crisis, y en el marco de la respuesta a ciberincidentes, Argentina cumple con la unidad de respuesta a incidentes cibernéticos de la misma manera que España. Sin embargo, el país latinoamericano en los criterios restantes (responsabilidad de informar y único punto de contacto para la coordinación internacional de seguridad cibernética) no se destaca. Por otra parte, considerando la gestión de crisis cibernética, tanto Argentina como España han efectuado un mínimo esfuerzo participando en ejercicios internacionales de crisis cibernética sin haber efectuado un plan de gestión de crisis cibernéticas, ni apoyo operativo de voluntarios en crisis cibernéticas. A diferencia de Argentina, España sí efectuó ejercicios de gestión de crisis a nivel nacional. Lo comentado hasta aquí se refleja en la Figura 15:

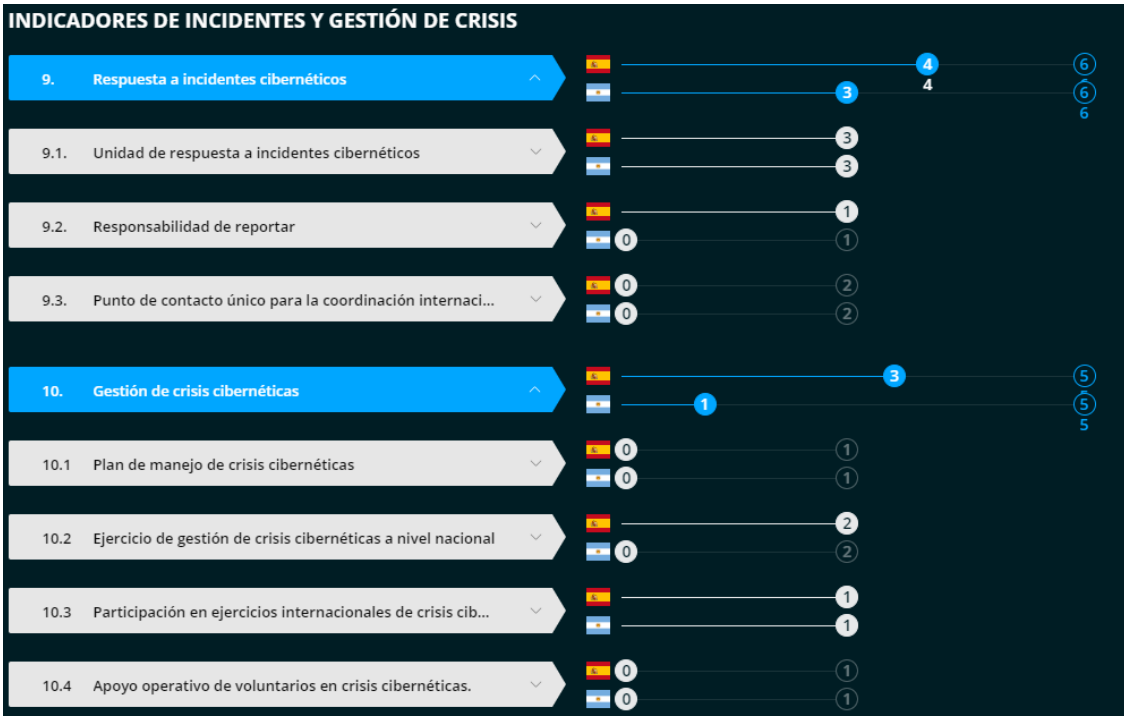


Figura 15: Comparativa de España y Argentina considerando los indicadores de incidentes y gestión de crisis. Fuente: *National Cyber Security Index*, 2019.

3.3.2. Los organismos y normas españolas que conforman el Sistema de Protección de las IC

La aprobación de la Estrategia de Seguridad Nacional 2017 y las transformaciones tecnológicas y digitales provocaron que en el año 2019 el Consejo de Seguridad Nacional español actualizara la Estrategia Nacional de Ciberseguridad (la primera fue aprobada en el año 2013) cuyos principios rectores son la unidad de acción, la anticipación, la eficiencia y la resiliencia.

La Estrategia Nacional de Ciberseguridad española cuenta con un objetivo general y cinco objetivos específicos, los cuales pueden observarse a continuación:

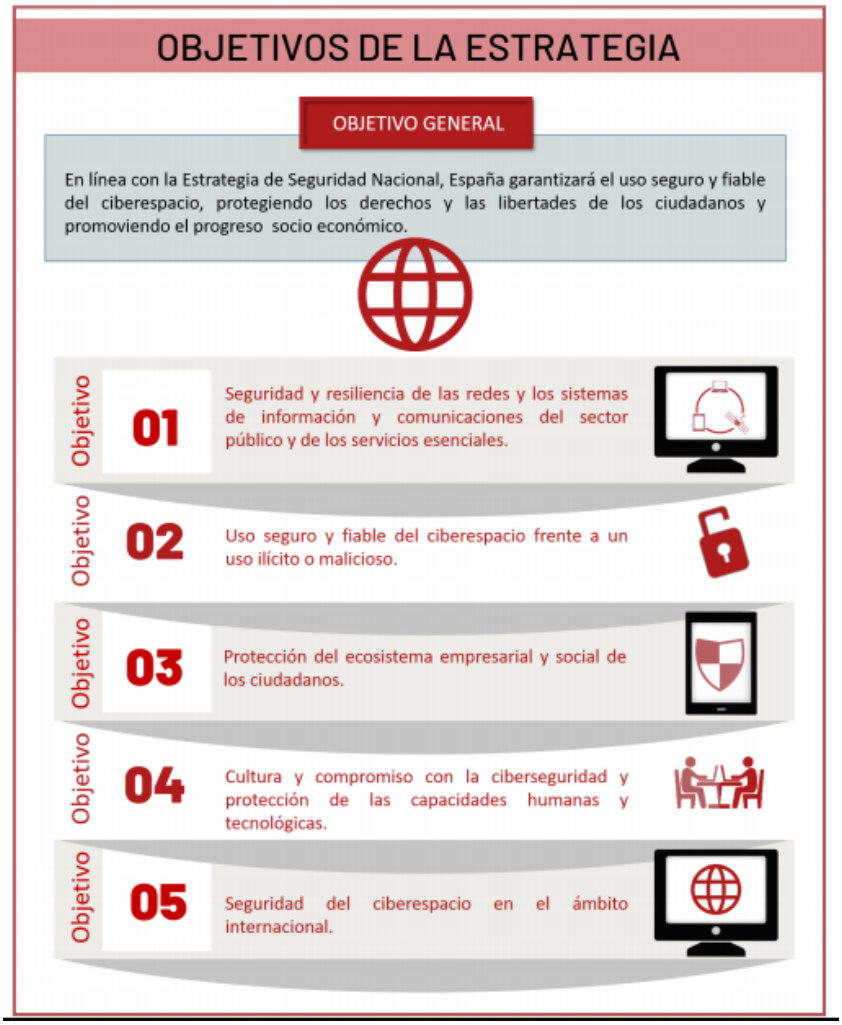


Figura 16: Ilustración que muestra el objetivo general y los objetivos específicos de la Estrategia Nacional de Ciberseguridad de España 2019. Fuente: Estrategia Nacional de Ciberseguridad - Gobierno de España - Presidencia del Gobierno, 2019, pág. 41.

Es de destacar el primer objetivo específico que contiene dos líneas de acción tales como "reforzar las capacidades ante las amenazas provenientes del ciberespacio" y "garantizar la seguridad y resiliencia de los activos estratégicos para España" (Presidencia del Gobierno - Departamento de Seguridad Nacional, 2019, págs. 44-46). Por su parte, el quinto objetivo tiene una única línea de acción a seguir para "contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales" (Presidencia del Gobierno - Departamento de Seguridad Nacional, 2019, pág. 54). Además de las líneas de acción, España ha determinado una serie de medidas que especifica aquello que debe efectuarse para avanzar y cumplir con la Estrategia de Seguridad Nacional (2017). Frente a ello, las medidas a resaltar para

incrementar la seguridad y la resiliencia de las redes y sistemas de comunicación del sector público y de los servicios esenciales (objetivo I) son:

> Mejorar la capacidad de detección y análisis de las ciberamenazas […] así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz; potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas; impulsar el desarrollo de plataformas de […] intercambio de información y coordinación para la mejora de la ciberseguridad sectorial; garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana; ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégicos; potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas. (Presidencia del Gobierno - Departamento de Seguridad Nacional, 2019, págs. 44-47)

Por otra parte, la estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional español se encuentra conformado por los siguientes organismos:

Figura 17: Ilustración que muestra la estructura de la ciberseguridad en el Sistema de Seguridad Nacional de España 2019. Fuente: Estrategia Nacional de Ciberseguridad - Gobierno de España - Presidencia del Gobierno, 2019, pág. 65.

Considerando la protección de las IC, España se ha organizado con base en la Directiva Europea 2008/114/CE del Consejo sobre la identificación y designación de Infraestructuras Críticas Europeas[40] y la necesidad de mejorar su protección. La Directiva es un documento legislativo vinculante para los países pertenecientes a la Unión Europea que establece el procedimiento de identificación y designación de IC europeas y la evaluación de la necesidad de proteger dichas infraestructuras para los Estados pertenecientes a dicha comunidad.

La importancia de esta Directiva radica no solo en el hecho que es la primera norma europea en establecer los estándares para la identificación y designación de las IC, sino porque define una serie de conceptos. Es posible destacar que allí una infraestructura crítica es considerada como:

> El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o

[40] Considerada como "la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros […]" (Artículo 2, inciso b, Directiva 2008/114/CE del Consejo de la Unión Europea, 2008)

> destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones. (Artículo 2°, inciso a, Directiva 2008/114/CE del Consejo de la Unión Europea, 2008)

Asimismo, se definen los criterios horizontales de identificación de dichas infraestructuras tales como el número de víctimas (potencial de muertes o heridos), el impacto económico (magnitud de las pérdidas económicas o deterioro de productos, incluyendo el impacto medioambiental) y el impacto público (incidencia en la confianza de la población, sufrimiento físico y la alteración de la vida cotidiana) y se establecen los sectores considerados como IC europeas (Anexo I, Directiva 2008/114/CE del Consejo de la Unión Europea, 2008).

A partir de la Directiva y en pos de obtener una cooperación pública-privada en lo que hace a la protección de las IC, España ha desarrollado un marco regulatorio con un "[…] enfoque regulado, mediante el cual se utiliza la legislación como un punto de apoyo o instrumento obligado para lograr la cooperación de todos los agentes" (Sánchez Gómez, Protección de Infraestructuras Críticas en España: Marco Regulatorio y Organizativo, 2014, pág. 30). Frente a lo cual, en el presente trabajo se hará referencia a la Ley 8/2011 y al Real Decreto 704/2011, consideradas como las normas más importantes para el presente trabajo, ya que enmarcan íntegramente la temática y fueron elaboradas con un alto nivel de consenso entre los distintos agentes afectados (Considerando, Real Decreto 704/2011, 2011).

Por un lado, la Ley 8/2011 (conocida como la Ley de Protección de las Infraestructuras Críticas y en adelante "LPIC") es de carácter general e integral[41] ya que establece medidas con el fin de adaptar al sistema político e institucional del país las obligaciones establecidas en la Directiva comentada anteriormente. De esta manera, se torna imprescindible destacar:

[41] "Anteriormente la protección de [las infraestructuras críticas] no se materializaba en una única Ley, sino que se encontraba dispersa en diversas leyes como la Ley 16/1987 de 30 de julio, de Ordenación de los Transportes Terrestres; la Ley 21/2003 de 7 de julio, de Seguridad Aérea o la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones, ya derogada por la Ley 9/2014 de 9 de mayo, General de Telecomunicaciones". (Galindo Sierra, 2016, pág. 10)

- la terminología a emplearse tal como la definición de las infraestructuras críticas como parte de las infraestructuras estratégicas[42], el concepto de servicio esencial, los criterios horizontales de criticidad, interdependencias, Catálogo Nacional de Infraestructuras Estratégicas, entre otros (artículo 2° y 4°);
- crea una estructura organizativa a nivel nacional como el Sistema de Protección de Infraestructuras Críticas (artículo 5° al artículo 13°) compuesta por "[…] una serie de instituciones, órganos y empresas, procedentes tanto del sector público como privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales…" (Artículo 5°, Ley 8/2011, 2011);
- se establecen los agentes y competencias que conforman el Sistema, tales como:
    a. la Secretaría de Estado de Seguridad del Ministerio del Interior: responsable de la política de seguridad de las IC nacionales (artículo 6°);
    b. el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante "CNPIC"): director y coordinador de las actividades relacionadas con la protección de las IC (artículo 7°);
    c. los Ministerios y organismos integrados en el Sistema (artículo 8°);
    d. la Comisión Nacional para la Protección de las Infraestructuras Críticas, el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas: la primera es un órgano político y el segundo es un órgano técnico que efectúa el seguimiento y la preparación de las materias de la Comisión (artículo 11° y 12°);
    e. y los operadores críticos del sector público y privado: las empresas u organismos que gestionan o poseen infraestructuras críticas quienes deberán cumplir con las obligaciones que se generen en base a los planes de seguridad y quienes deberán nombrar a los responsables de seguridad y enlace con la Administración Pública (artículo 13°);

[42] Considera a las infraestructuras críticas como "las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" (Ley 8/2011, 2011, pág. 4).

- Y constituye un esquema de planificación y documentación compuesto por cinco instrumentos con el fin de proteger efectivamente las infraestructuras mediante el establecimiento de responsabilidades: el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los Planes de Seguridad del Operador, los Planes de Protección Específicos y los Planes de Apoyo Operativo (artículo 14°).

Por otro lado, de forma complementaria a dicha ley, el 20 de mayo del año 2011 se aprobó el Real Decreto 704/2011 o Reglamento de Protección de las Infraestructuras Críticas el cual desarrolla, completa y amplía los aspectos contemplados en la LPIC cumpliendo, a su vez, con la Directiva 2008/114/CE del Consejo de la Unión Europea nombrado anteriormente.

Del Real Decreto es preciso resaltar el Catálogo Nacional de Infraestructuras Estratégicas definido como:

> El registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas así como aquellas clasificadas como críticas europeas que afectan a España. (Artículo 3°, Real Decreto N° 704, 2011)

Por otra parte, el CNPIC "[…] es el órgano responsable del Catálogo […] a la hora de gestionar su contenido, explotarlo, dar accesos y custodiar su seguridad" (Sánchez Gómez, Protección de Infraestructuras Críticas en España: marco regulatorio y organizativo, 2014, pág. 52) y quién deberá efectuar el proceso de identificación de una infraestructura como crítica[43] (Artículo 5°, inciso 3°, Real Decreto N° 704, 2011). Se establece que el Catálogo será secreto y contendrá la información relativa a la descripción de las IC, la ubicación, la titularidad y administración, los servicios que prestan, los medios de contacto y el nivel de seguridad que requiere sobre la base de los riesgos evaluados lo cual se obtendrá del Centro Nacional para la Protección de las Infraestructuras, los operadores críticos y los responsables del Sistema (Artículo 4°, Real Decreto N° 704, 2011).

[43] "La clasificación de una infraestructura como crítica europea supondrá la obligación adicional de comunicar su identidad [por parte del CNPIC] a otros Estados miembros que puedan verse afectados de forma significativa por aquella, de acuerdo con lo previsto por la Directiva 2008/114/CE" (Artículo 5°, inciso 4°, Real Decreto N° 704, 2011).

Por otra parte, el Decreto establece taxativamente las funciones de todos los agentes de la LPIC entre los cuales, cabe destacar los siguientes:

- Secretaría de Estado de Seguridad: "diseñar y dirigir la estrategia nacional de protección de IC" (Artículo 6°, inciso a, Real Decreto N° 704, 2011) y aprobar el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes de Seguridad de los Operadores y sus actualizaciones a propuesta del CNPIC, aprobar los diferentes Planes de Protección Específicos y los Planes de Apoyo Operativo (Artículo 6°, inciso b-e, Real Decreto N° 704, 2011).
- CNPIC cuyas funciones a destacar son: "asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones como órgano de contacto y coordinación con los agentes del Sistema" (Artículo 7°, inciso a, Real Decreto N° 704, 2011); "ejecutar y mantener actualizado el Plan Nacional de Protección de las infraestructuras críticas […] [y] determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo" (Artículo 7°, inciso b y c, Real Decreto N° 704, 2011); mantener operativo y actualizado el Catálogo considerando el alta, baja y modificación de las infraestructuras en base a los criterios horizontales y los efectos de interdependencias sectoriales (Artículo 7°, inciso d, Real Decreto N° 704, 2011); "participar en la realización de ejercicios y simulacros en el ámbito de la protección de las IC" (Artículo 7°, inciso i, Real Decreto N° 704, 2011) ; y ser "el Punto Nacional de Contacto con organismos internacionales y la Comisión Europea […]" (Artículo 7°, inciso k, Real Decreto N° 704, 2011).
- Los ministerios y organismos integrados en el Sistema de Protección de Infraestructuras, cuyas funciones se encuentran en el artículo 8° del Real Decreto. Es de destacar: participar, a través del Grupo de Trabajo Interdepartamental, en la elaboración, revisión y actualización de los Planes Estratégicos Sectoriales y verificar su cumplimiento (inciso a y b); colaborar en la designación de los operadores críticos (inciso c); y "proporcionar asesoramiento técnico […] en la catalogación de las infraestructuras y poner a disposición del CNPIC la información técnica para determinar la criticidad" (Artículo 8°, inciso d, Real Decreto N° 704, 2011).
- Comisión Nacional para la Protección de las Infraestructuras Críticas, cuyas funciones a destacar son: "aprobar los Planes Estratégicos Sectoriales [y] designar a

los operadores críticos [e] impulsar aquellas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas" (Artículo 11°, inciso c y d, Real Decreto N° 704, 2011).

- Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, cuyas funciones a destacar son: "elaborar, con la colaboración de los agentes del Sistema y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión [y] proponer a la Comisión la designación de los operadores críticos por sector estratégico (Artículo 12°, inciso a y b, Real Decreto N° 704, 2011).
- Operadores Críticos, definidos como "las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica" (Artículo 2°, inciso m, Ley 8/2011, 2011) y pueden ser tanto empresas como organismos (Artículo 14°, Real Decreto N° 704, 2011). Las funciones a destacar son (Artículo 13°, Real Decreto N° 704, 2011): brindar colaboración técnica para la valoración de sus propias infraestructuras y actualización de los datos para el Catálogo (inciso 2a); "colaborar […] en la realización de los análisis de riesgo sobre los sectores estratégicos" con el Grupo de Trabajo (Artículo 13°, inciso 2b, Real Decreto N° 704, 2011); y elaborar el Plan de Seguridad del Operador y actualizarlo, así como elaborar un Plan de Protección Específico por cada una de las infraestructuras con su respectiva actualización periódica (inciso 2c y 2d).

Finalmente, el Real Decreto complementa a la LPIC explicitando la finalidad, elaboración, contenido, aprobación, registro, clasificación, revisión y actualización de los diferentes instrumentos de planificación creados en el marco de la LPIC como ser el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los Planes de Apoyo Operativo, los Planes de Seguridad del Operador y los Planes de Protección Específicos tal como figuran en los Artículo 16° al 32° de Real Decreto N° 704/2011. En la Figura 18 se resume esquemáticamente los distintos instrumentos que enmarca al Sistema de Protección de las Infraestructuras Crítica españolas y los agentes que efectúan dichos documentos en el orden de prelación correspondiente:

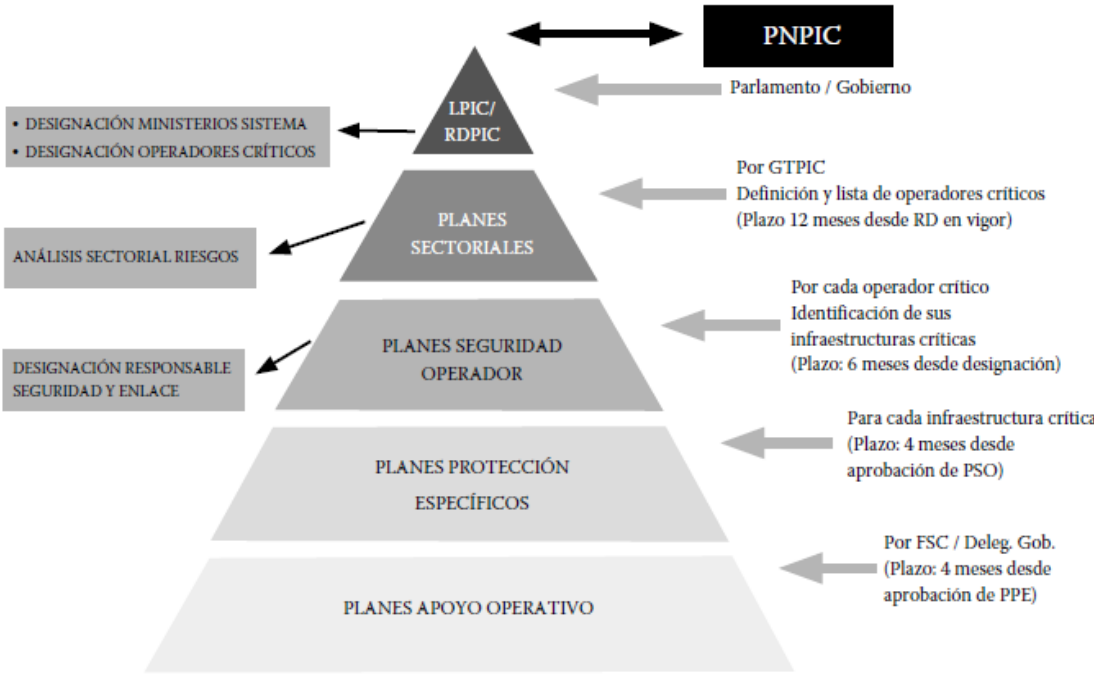


Figura 18: Instrumentos de planificación creados por la LPIC y ampliados en el Real Decreto 704/2011. Fuente: Sánchez Gómez, Protección de Infraestructuras Críticas en España: Marco Regulatorio y Organizativo, 2014.

4. Metodología

La metodología que se utilizó para el desarrollo del trabajo involucró el análisis y revisión de la normativa de la Argentina, así como lo expuesto de España, a fin de sugerir y aportar una posible resolución del problema aplicable al contexto latinoamericano y, más precisamente, a Argentina.

El tipo de investigación a realizar es exploratorio, dado que el objetivo es examinar un tema o problema poco estudiado y obtener la información necesaria para llevar a cabo una investigación más completa respecto del contexto actual. Además, el estudio a realizar es de alcance descriptivo, ya que hará referencia al estado normativo del tema de las infraestructuras críticas de la información y la ciberseguridad en la Argentina durante el período 2011-2019 para plantear una posible solución jurídico-institucional del problema. Asimismo, al efectuar una revisión de documentos, se utilizará un enfoque de investigación analítico cualitativo y un análisis holístico a partir de la aplicación de un razonamiento lógico deductivo.

5. Hallazgos

En el marco teórico se expuso de manera cronológica el universo de normas nacionales relacionadas con las IC y la ciberseguridad en la Argentina desde el año 2011 (la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad) hasta el mes de diciembre del año 2019 (con la Resolución N° 1380/2019 del Ministerio de Defensa de la Nación, la cual define el término ciberdefensa y hace referencia a las infraestructuras críticas de la Defensa Nacional así como la Política de Ciberdefensa), con el fin de presentar exhaustivamente el estado jurídico-institucional de la temática. La intención cifrada en la lógica de la presentación adoptada era que el orden cronológico le permita al lector acompañar la evolución jurídica que hace a las infraestructuras críticas de la información y la ciberseguridad. Sin embargo y a partir de la apreciación integral del conjunto normativo atinente a la problemática de investigación, es posible arribar a la conclusión de que dicho marco regulatorio es tan amplio como confuso.

En efecto, a medida que se avanzó en la investigación, se constató la superposición desorganizada de varias normas con distintas jerarquías normativas (resoluciones, decretos, decisiones administrativas) procedentes de diferentes organismos que establecían disposiciones ejecutivas (tales como acciones y responsabilidades) y/o estructurales (tales como funciones y dependencias)[44]. Dicha superposición podría darse a causa de los cambios de visión e intereses tanto durante el desarrollo de cada una de las gestiones político-estatales, como las reformas organizacionales efectuadas por obra de los cambios en la APN.

En el análisis efectuado fue posible identificar veintiún (21) organismos del Sistema Nacional de Gestión Integral cuya jerarquía, denominación, responsabilidades y acciones han variado, y en algunos casos han sido reciclados y reiterados. Con base en el Sistema Nacional de Gestión Integral, en el marco teórico se analizaron los organismos de la tabla 1:

[44] Esto se puede observar, por ejemplo, en enero del 2016 que mediante un Decreto se establece la estructura organizativa del Ministerio de Modernización. En julio del mismo año, a través de otro Decreto se presentan los objetivos de la Subsecretaria de Tecnología y Ciberseguridad, cuya estructura se declara en marzo 2016 a través de una decisión administrativa, siendo la dirección y las coordinaciones que le pertenecen a dicha dirección nacional, creadas mediante una Resolución en noviembre del 2016.

Tabla 1: *Organismos y dependencias analizadas en el marco teórico pertenecientes al Sistema de Gestión Integral y relacionadas con las infraestructuras críticas y la ciberseguridad desde el año 2013 al año 2019. Fuente: elaboración propia.*

Dependencia	Organismo	División interna de primer nivel	División interna de segundo nivel	División interna de tercer nivel	Norma	Vigencia
Oficina Nacional de Tecnologías de Información	**Grupo de Infraestructuras Críticas de Información**				Disposición N° 2/2013	Agosto 2013
	ICIC-CERT, ICIC-GAP, ICIC-GICI, ICIC-INTERNET SANO					
Subsecretaría de Protección de Infraestructuras críticas de Información y Ciberseguridad	**Dirección Nacional de Infraestructuras críticas de Información y Ciberseguridad**				Decreto N° 1067/2015	Junio 2015
		Dirección de Elaboración e Interpretación Normativa			Resolución 1046/2015	Agosto 2015
		Dirección Técnica de Infraestructuras críticas de Información y Ciberseguridad				
		Dirección de Capacitación, Concientización y Difusión				
Ministerio de Modernización	**Subsecretaría de Tecnología y Ciberseguridad**				Decreto N° 13/2016	Enero 2016
					Decreto N° 898/2016	Julio 2016

		Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad			Decisión Administrativa N° 232/2016	Marzo 2016
			Dirección de Operaciones y Técnicas de Ciberseguridad	Coordinación de Operaciones de Ciberseguridad	Resolución N° 490-E/2016	Noviembre 2016
				Coordinación de Proyectos de Investigación de Ciberseguridad		
Secretaría de Infraestructura Tecnológica y País Digital					Decreto N° 174/2018	Marzo 2018
	Dirección Nacional de Infraestructura Tecnológica y Ciberseguridad	Dirección de Infraestructuras Críticas de Información y Ciberseguridad			Decisión Administrativa N° 297/2018	
		Coordinación de Operaciones de Ciberseguridad				
		Coordinación de Comunicación y Proyectos de Ciberseguridad				
Secretaría de Gobierno de Modernización	**Dirección Nacional de Ciberseguridad**	Dirección de Infraestructuras Críticas de Información			Decisión Administrativa N° 103/2019	Febrero 2019
		Coordinación de Comunicación y Proyectos de Ciberseguridad				

Considerando la magnitud de lo señalado, es clara la dificultad para efectuar un análisis y detectar aquellos avances plasmados en acciones y/o documentos que podrían traer luz al tema de las infraestructuras críticas de la información y la ciberseguridad en la Argentina.

Sin embargo, es posible resaltar que la importancia que se le brindó al tema desde el Estado fue en declive o en el mejor de los casos, inconsistente. Esto es así dado que las responsabilidades fueron otorgadas a organismos con un orden jerárquico o de prelación inferior. Es decir, las funciones más importantes en principio se encontraban en manos de Secretarías y Subsecretarías para finalmente terminar en manos de Direcciones o Coordinaciones, cada vez más alejadas del Presidente de la Nación. La excepción a esto se puede observar en el año 2019 cuando la temática pasa a ser responsabilidad de un Director Nacional dependiente directamente del Secretario de Modernización que respondía al Jefe de Gabinete de Ministros que a su vez dependía directamente del Presidente de la Nación. Por ello, las medidas y acciones efectuadas por el Director Nacional podían ser rápidamente consideradas por el Jefe de Estado.

Considerando al Sistema de Defensa Nacional, el desarrollo de la temática con base en las IC nacionales y, en menor medida la ciberseguridad, fue pequeño, aunque no menos importante. En términos generales, dicho Sistema y los organismos que lo conforman no se inmiscuyen prácticamente en el tema de la ciberseguridad (aunque se propuso contribuir desde la jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica en el Decreto N° 42/2016). Reflexionamos que, quizás, la dificultad de relacionar el ámbito de la defensa (y la ciberdefensa) con el término ciberseguridad se corresponde con la diferenciación que hace la Argentina en la jurisdicción de la seguridad interior y la defensa nacional en el espacio terrestre, marítimo, espacial y aéreo que, en el caso del ciberespacio, debería ser contemplado de manera diferente a favor de trabajar conjuntamente ya que, en ese dominio, lo que hace a la prevención y la defensa no es tan sencillo separar jurisdicciones.

A partir del marco teórico, es posible enlistar once (11) organismos relacionados con la ciberdefensa, la ciberseguridad y las IC en el Sistema de Defensa Nacional y su evolución desde la dependencia (funcional y organizacional) y la nomenclatura como puede observarse en la tabla 2:

Tabla 2: *Organismos y dependencias analizadas en el marco teórico pertenecientes al Sistema de Defensa Nacional y relacionadas con las infraestructuras críticas y la ciberseguridad desde el año 2013 al año 2019. Fuente: elaboración propia.*

Dependencia	Organismo	División interna de primer nivel	Norma	Vigencia
Jefatura de Gabinete del Ministerio de Defensa	**Unidad de Coordinación de Ciberdefensa**		Resolución N° 385/2013	Octubre 2013
Estado Mayor Conjunto de las Fuerzas Armadas	**Comando Conjunto de Ciberdefensa**		Resolución N° 343/2014	Mayo 2014
Ministerio de Defensa			Decreto N° 2645/2014	Diciembre 2014
Ministerio de Defensa	**Dirección General de Ciberdefensa**		Decisión Administrativa N° 15/2015	Marzo 2015
Secretaría de Ciencia, Tecnología y Producción para la Defensa	**Subsecretaría de Ciberdefensa**		Decreto N° 42/2016	Enero 2016
Secretaría de Ciencia, Tecnología y Producción para la Defensa	**Subsecretaría de Ciberdefensa**		Decisión Administrativa N° 546/2016	Mayo 2016
		Dirección Nacional para el Desarrollo Científico de la Ciberdefensa		
		Dirección Nacional de Diseño de Políticas de Ciberdefensa		
Secretaría de Investigación, Política Industrial y Producción	**Subsecretaría de Ciberdefensa**	Comando Conjunto de Ciberdefensa de las Fuerzas Armadas	Decreto N° 174/2018	Marzo 2018
Secretaría de Estrategia y Asuntos Militares			Decreto N° 684/2019	Octubre 2019
Secretaría de Investigación, Política Industrial y Producción para la Defensa	**Subsecretaría de Investigación, Política Industrial para la Defensa**			

Visto esto, todo indica que la regulación de la temática, principalmente por parte del Ministerio de Defensa de la Nación, fue más organizada que lo efectuado por el Sistema de Gestión Integral. Además, es posible observar que en lo que hace al orden en la APN, el Sistema de Defensa Nacional evolucionó positivamente a favor de la especificación de la ciberdefensa ya que, lo que al principio era una Unidad, luego una Dirección General, luego una Subsecretaría perteneciente a una Secretaría relacionada con la ciencia, tecnología y producción a la investigación y finalmente se contempló la necesidad de que la ciberdefensa sea tratada conjuntamente dentro de las Fuerzas Armadas mediante el Comando Conjunto perteneciente al Estado Mayor Conjunto de las Fuerzas Armadas.

Lamentablemente, en lo que hace a la visualización y organización del ordenamiento jurídico argentino respecto a la temática de las infraestructuras críticas de la información y la ciberseguridad, se torna dificultoso efectuar un análisis íntegro e interrelacionado entre los distintos organismos nombrados a causa de la ya mentada desorganización normativa imperante en el área. A pesar de haber efectuado una revisión de más de treinta organismos pertenecientes al Sistema Nacional de Gestión Integral, Sistema de Seguridad Interior, Sistema de Inteligencia Nacional y al Sistema de Defensa Nacional del PEN, se torna inviable vislumbrar un avance o ejecución efectiva en lo que hace a la protección de las infraestructuras críticas de la información y la ciberseguridad.

El derecho argentino, en este caso a través del PEN, ha realizado un esfuerzo considerable para ordenar, mediante distintos tipos de reglamentos[45], el comportamiento frente a la tecnología en lo que hace a la ciberseguridad y a las infraestructuras críticas de la información. Sin embargo, los resultados de dicho esfuerzo redundan en la implantación de una multiplicidad de formalidades y obligaciones jurídicas causadas por la intervención de distintos funcionarios en diferentes gestiones políticas durante los nueve años analizados. El involucramiento simultáneo y permanente - pero sin orden ni concierto - de una plétora de actores dotados con capacidad e intención de generar normativas, dificultan la comprensión de la temática, la trazabilidad de la evolución y la estabilidad del derecho. Ciertamente, es posible vislumbrar que los diferentes organismos pertenecientes a los sistemas

[45] "[…] el reglamento es a la vez la más extendida y la más problemática de las fuentes del derecho administrativo. Su extensión deviene de una tendencia […] de la administración a fijar continuamente, sin demasiado estudio ni reflexión, normas generales propias para todo lo que hace". (Capítulo VII, Gordillo, 2013, pág. 21)

institucionales analizados (Seguridad Interior, Gestión Integral, Defensa Nacional e Inteligencia Nacional) trabajan la problemática de manera encapsulada, segmentada y compartimentada, sin cohesión ni coacción. Frente a lo cual, se puede visibilizar la repercusión negativa y directa en la capacidad de Argentina para amparar y defender las IC nacionales, así como para posicionarse internacionalmente en la temática conforme lo indicado por las iniciativas político-estratégicos nacionales trazadas por el PEN.

En este contexto, es necesario acompañar al jurista Agustín Gordillo, quien hace referencia a la excesiva normativización mediante el empleo de reglamentos[46] por parte del PEN y afirma que "no es en los actos individuales donde la administración despliega toda su arbitrariedad: Es en la redacción de largos reglamentos, seudo normas generales que luego alega limitarse a cumplir, cuando ella los ha preparado y emitido" (Capítulo VII, Gordillo, 2013, pág. 22).

Frente al desorden normativo, institucional y organizacional identificado a la luz del análisis efectuado previamente, surge que el estado de la ciberseguridad y las IC en Argentina requieren de una reorganización temática. A razón de ello, el presente capítulo estará dividido en tres partes donde primero se examinará en profundidad aquellas normas analizadas en el marco teórico y podrían ser rescatadas consiguiendo, a su vez, ser la base del Sistema de Protección de Infraestructuras Críticas y Ciberseguridad[47] en Argentina (el cual aún no fue creado). Luego, se señalizarán los hallazgos de aquello presentado en el marco teórica mediante una organización por subtemas que servirán de guía para la propuesta final a presentar. Finalmente, se puntualizarán aquellos hallazgos obtenidos con base en la normativa e instituciones analizadas de España que servirán de brújula para la propuesta final del presente trabajo.

[46] "En la inmediatez diaria de la vida administrativa, el reglamento es la norma de mayor importancia momentánea. Se ha podido decir que es la fuente cuantitativamente más importante del derecho administrativo, lo cual es ciertamente peligroso para la vigencia del derecho administrativo y el Estado de derecho". (Capítulo VII, Gordillo, 2013, pág. 22)

[47] Es de destacar que se emplea el término "infraestructuras críticas" en general dado que abarca la protección física y lógica de dichas infraestructuras. En efecto y manteniendo el criterio de la Resolución N° 1523/2019, el término infraestructura crítica de la información se encuentra dentro del concepto infraestructura crítica en general.

5.1. Las normas e instituciones a rescatar

En términos generales y con base en el marco teórico, es posible apreciar un notorio avance en la temática durante el año 2019. En dicho año, se establecieron definiciones, objetivos y criterios en torno a las infraestructuras críticas de la información y la ciberseguridad que deberían ser considerados como el cimiento sobre el que se podría construir, a nivel nacional, el sistema de protección de dichas infraestructuras.

Frente a esto, es de destacar la existencia de la definición de los términos IC e infraestructuras críticas de la información, ambos publicados en el Boletín Oficial, los criterios de identificación y los sectores determinados, así como el glosario de términos de ciberseguridad[48] (documento que debía realizarlo la Dirección de Elaboración e Interpretación creada por la Resolución N° 1046/2015) detallados en los anexos de la Resolución N° 1523/2019.

Por otra parte, es necesario expresar la importancia no solo de la existencia sino de la labor conjunta y multidisciplinaria que representa el Comité Nacional de Ciberseguridad creado a través del Decreto N° 577/2017 ya que reúne, en un único órgano, a los Ministerios de Modernización, Defensa, Seguridad, Relaciones Exteriores y Culto y al Ministerio de Justicia y Derechos Humanos, así como a la Secretaría de Asuntos Estratégicos (los últimos tres incorporados a través del Decreto N° 480/2019). La composición y ampliación de los integrantes del Comité demuestra el alcance global, el abordaje internacional de las amenazas, la importancia de la cooperación internacional así como la transversalidad de las diferentes áreas del gobierno. El Comité, en efecto, cumplió con el objetivo de elaborar la Estrategia Nacional de Ciberseguridad mediante el trabajo multidisciplinario de los organismos del PEN nombrados.

Considerando la Estrategia Nacional de Ciberseguridad, es imprescindible remarcar los principios rectores y los objetivos encuadrados allí, dado que trazan una línea de acción a futuro que deberían ejecutarse de forma efectiva por el PEN. Es menester relacionar los distintos organismos que son competentes por la temática - incluidos aquellos que componen el Comité Nacional de Ciberseguridad - y destacar la innovación tecnológica, el trabajo interdisciplinario, intradisciplinario y multidisciplinario de la temática, la confidencialidad

[48] El cual permite establecer un marco terminológico para todo el país y los diversos sectores estratégicos.

y reserva de la información obtenida, así como la constante capacitación y concientización de todos los actores relacionados.

Con base en el tema del presente trabajo final de maestría, es necesario rescatar el octavo objetivo de la Estrategia que hace referencia a la protección de las infraestructuras críticas nacionales de información. Allí se contempla la necesidad de promocionar la definición (actualmente establecida) e identificación (se han determinado los criterios y sectores, sin fijar la responsabilidad ni el procedimiento para ello) de estas últimas. Por otra parte, la Estrategia establece la necesidad de "articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas de ataques" (Anexo I, Resolución N° 829, 2019, pág. 8) contra dichas infraestructuras, y el fortalecimiento de la cooperación para el intercambio de información frente a vulnerabilidades y amenazas. *A contrario sensu*, en lo que hace al cumplimiento de los objetivos del Comité, es necesario remarcar que dicho organismo no elaboró el plan de acción necesario para la implementación de la Estrategia (artículo 2°, inciso b, Decreto N° 577, 2017) y falló en su propósito de impulsar el dictado de un marco normativo en materia de ciberseguridad (artículo 2°, inciso d, Decreto N° 577, 2017).

Por otra parte, la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (Resolución N° 580/2011), junto al Formulario de Adhesión y el Convenio de Confidencialidad (Disposición N° 3/2011), podrían ser considerados como un posible puntapié para iniciar al país en el plan de acción de identificar, entre los sectores a considerar[49], a aquellas infraestructuras que podrían ser críticas. La importancia de estos documentos radica en el hecho de que es una iniciativa que puede impulsar la determinación de aquellas infraestructuras, industrias y organismos que brinden servicios esenciales para la sociedad. Una forma de iniciar con el plan de identificación podría ser que las infraestructuras, las industrias y los organismos se adhieran al Programa mediante el formulario diseñado a tal fin (un registro voluntario que debería requerir una evaluación posterior) y firmen el convenio de confidencialidad con el objetivo de resguardar la información que se obtenga del análisis. Será, luego de dicha adhesión, donde algún organismo del Estado - hoy no se determina cuál - deberá evaluar si corresponde considerarlo

[49] "Sectores identificados: energía, tecnologías de información y comunicaciones, transportes, hídrico, salud, alimentación, finanzas, nuclear, químico, espacial y Estado" (Resolución N° 1523, 2019, Anexo I).

como infraestructura crítica de la información y su criticidad, para establecer formalmente su importancia y ejecutar los mecanismos de protección y defensa que correspondan considerando los criterios de identificación - aún no se establece el margen para evaluar la magnitud de los distintos impactos - establecidos[50] en el año 2019.

Desafortunadamente, es complejo detectar y determinar el organismo o institución responsable de la aplicación y ejecución del Programa en la actualidad, puesto que en sus inicios (año 2011) se encontraba bajo la órbita de la Oficina Nacional de Tecnologías de Información (ONTI) y en el año 2016 fue transferido a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros (Decreto N° 1067/2015). Finalmente, y considerando el organigrama de la APN, el Programa no vuelve a nombrarse dentro de las responsabilidades u objetivos de ninguna Secretaría, Subsecretaría, Dirección Nacional, Dirección o Coordinación creados posteriormente. Frente a ello, podría inferirse que se derogó el Programa o, en su defecto, se realizó su transferencia a otro organismo que no es posible identificar dada la falta de claridad en la normativización y, por ende, no es posible controlar dicho Programa y su aplicación. Consideramos necesario reivindicar la importancia y aplicabilidad de dicho Programa en el marco de una adhesión voluntaria por parte de las infraestructuras que podrían ser consideradas como críticas con el fin de, a partir de dicha acción, analizar la criticidad, determinar y declararla como infraestructura crítica con el objetivo último de tomar las medidas necesarias en el marco de la protección que se requiera.

5.2. Normas organizadas por subtemas

En términos generales, es posible observar que nuestro país se caracteriza por tener un marco normativo amplio en lo que hace a la protección de las IC y ciberseguridad y, a pesar de ser confuso, resultaría contraproducente eliminarlo por completo y pretender iniciar de cero la regulación de la temática siendo más eficiente dirigir los esfuerzos a mejorar lo realizado. Frente a ello, en el apartado 5.1 se intentó rescatar lo considerado como importante y

[50] Criterios de identificación: impacto en la vida humana; impacto económico; impacto en el medio ambiente; impacto en el ejercicio de los derechos humanos y de las libertades individuales; impacto público o social; impacto en el ejercicio de las funciones del Estado; impacto en la soberanía nacional; impacto en mantenimiento de la integridad territorial nacional. (Resolución N° 1523, 2019, Anexo I).

necesario de elaborar y desarrollar, en pos de fomentar una línea de reflexión orientada a producir legislación a la altura de las complejidades presentadas y lograr imprimirle un espíritu prospectivo al cuerpo normativo con el fin de contar con capacidades para el tratamiento de una problemática presente y que, a su vez, subsista con la evolución de la tecnología.

Teniendo en cuenta el caos apreciable en el marco teórico, a continuación se examinarán - considerando el ordenamiento jurídico - aquellas acciones y objetivos a rescatar de la extensa normativa argentina. Frente a ello, se tendrá en cuenta el marco regulatorio necesario para la identificación de las IC; el monitoreo, alerta, soporte y respuesta en el marco de la prevención, la protección y la defensa de dichas infraestructuras frente a vulnerabilidades, ataques y amenazas cibernéticas que pudieran afectar los servicios esenciales para la sociedad; la coordinación público-privado; la investigación, desarrollo e innovación; la capacitación y concientización; y la cooperación internacional.

5.2.1 Identificación, protección y defensa de las infraestructuras críticas de la información: marco regulatorio, monitoreo, alerta y soporte.

Desde el año 2011 se consideró como necesaria la elaboración de un marco regulatorio que propicie la identificación de las IC - objetivo que se repitió en el año 2015 para la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad (Decreto N° 1067, 2015) y en el año 2016 para la Subsecretaría de Tecnología y Ciberseguridad (Decreto N° 3/2016) - y que aún se encuentra pendiente. Contemporáneamente, el Comité Nacional de Ciberseguridad debía "fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales" (artículo 2°, inciso e, Decreto N° 577/2017) lo cual fue acogido en el considerando de la Resolución N° 1523/2019 (que incorpora la definición de IC y de infraestructuras críticas de la información y el glosario de términos de ciberseguridad). En ésta última norma, se admite que la presentación de dichos conceptos, junto con los criterios para identificar a las IC y los sectores a considerar, permitiría elaborar "[…] normas, políticas y planes para la protección de las Infraestructuras que respaldan servicios críticos, permitiendo la identificación de sistemas, equipamiento y actores involucrados, entre otros aspectos" (Considerando, Resolución N° 1523, 2019). Teniendo esto en cuenta, el Comité cumplió en parte con su tarea de fijar los criterios para la definición e identificación de las IC pero resta avanzar en la determinación de los lineamientos que hacen a dichas actividades

y la protección de las infraestructuras críticas nacionales. Igualmente, en ninguno de estos documentos (ni en la Estrategia) se especifica quién es el responsable de definir, identificar y proteger a las mismas.

Por otra parte, el concepto de elaboración de políticas de resguardo de la seguridad digital con especial hincapié en las IC fue reiterado en múltiples ocasiones a lo largo de los años. Primero, mediante el Programa Nacional de Infraestructuras Críticas y Ciberseguridad (2011), para luego incorporar la importancia de elaborar dichas políticas en conjunto con el sector privado mediante el ICIC-GICI (2013), como acción de la Subsecretaría de Tecnología y Ciberseguridad (2015), de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2015 y 2016), de la Coordinación de Operaciones de Ciberseguridad (2016) y hasta la Dirección Nacional de Ciberseguridad (2019). Sin embargo, no es posible encontrar las políticas publicadas, los convenios con el sector privado ni un documento, plan o norma que establezca la forma de cumplir con dicho objetivo.

Con respecto a otras formas y documentos elaborados para regular la temática, es posible encontrarnos con la idea de diseñar políticas, normas y procedimientos destinados a fortalecer la seguridad digital entre las acciones de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad (2015). Asimismo, se observa la misma acción pero reemplaza el concepto de seguridad digital por seguridad de la información (e incorpora la noción de seguridad informática) entre las acciones de la Dirección de Operaciones Técnicas de Ciberseguridad dependiente de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2016).

En este mismo orden de ideas, el concepto de regular documentalmente la temática incluye el establecimiento de prioridades y planes estratégicos para el abordaje de la ciberseguridad detectado en el Programa (2011), el ICIC-GICI (2013), la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2015) y la Coordinación de Operaciones de Ciberseguridad, dependiente de la Dirección de Operaciones Técnicas de Ciberseguridad (2016). Lamentablemente, tampoco se hallaron documentos redactados que permitan al menos inferir el cumplimiento de los mismos.

Por otra parte, es posible observar que se hace referencia a la elaboración de la Estrategia Nacional de Protección de Infraestructuras Críticas de Ciberseguridad como objetivo de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad

(2015) para luego pasar a la Subsecretaría de Tecnología y Ciberseguridad (2016). Sin embargo, no es posible detectar este objetivo nuevamente, lo cual nos permite inferir que quizás pasó a ser lo que se conoce como la Estrategia Nacional de Ciberseguridad - elaborada y publicada en el año 2017. Caso contrario, queda pendiente la confección de la Estrategia Nacional de Protección de Infraestructuras Críticas y Ciberseguridad y la determinación del organismo que deba realizarla.

Por otro lado, en algún punto en el tiempo el Sistema de Gestión Integral tuvo en cuenta la importancia que representa la interpretación de la normativa sobre la protección de las infraestructuras críticas de información y ciberseguridad, como puede observarse en la Dirección de Elaboración e Interpretación Normativa (Resolución N° 1046/2015). En otras palabras, se establece que un organismo perteneciente a la APN (administración que debe realizar reglamentaciones y regulaciones de leyes existentes) debía también interpretarlas. En atención a los principios representativos, republicanos y federales establecidos por la Constitución Nacional, la interpretación de las normas debe mantenerse entre las funciones del Poder Judicial y, el hecho de que el PEN contemple la necesidad de interpretar sus propias regulaciones, podría significar que las mismas no son correctamente redactadas.

Considerando al Sistema de Defensa Nacional, el Comando Conjunto de Ciberdefensa (2014) debía "establecer los criterios rectores a nivel del Instrumento Militar para la determinación de infraestructuras críticas a ser protegidas" (Casarino & Ortiz, 2019, pág. 49). No obstante, no fue posible corroborar si dicho Comando efectuó la tarea. Esto demuestra que, a pesar de constituirse como una meta clara, no fue un objetivo cumplido a lo largo de los años o las gestiones políticas.

Posteriormente, la Política de Ciberdefensa (anexa a la Resolución N° 1380/2019) define en el Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa, que los Entes Reguladores debían elaborar el catálogo de IC de los sectores estratégicos, lo cual nos permite inferir que dichos entes debían identificar a las mismas conforme corresponda. Asimismo, se le otorga a la Subsecretaría de Ciberdefensa la responsabilidad de la protección de las IC de la Defensa Nacional. Ambos hallazgos son particularmente destacables, ya que en los nueve años analizados en el presente trabajo, es la primera (y única) vez que se observa en la normativa argentina el concepto de "catálogo" relacionado con las IC y, también, la primera vez que el Sistema de Defensa Nacional declara qué organismo es responsable de la protección de las IC de su jurisdicción.

Asimismo, distintos organismos del Sistema de Defensa Nacional tienen entre sus objetivos el de contribuir a la política nacional de ciberseguridad y de protección de IC pero no la elaboración de la misma. De esta forma, la Dirección General de Ciberdefensa (2015) y la Subsecretaría de Ciberdefensa (2016, 2018 y 2019), tenían la responsabilidad de contribuir a algo inexistente en la realidad. Sin embargo, ¿cómo se contribuye si no se establece que debe crearse ni se define qué organismo debe realizarlo?

En lo que hace a las normas analizadas en el marco teórico, el PEN hace referencia al control, aviso y el apoyo de expertos como acciones que permitirían prevenir posibles fallas y vulnerabilidades en dichas infraestructuras. En lo que respecta al monitoreo, se percibe que en las normas analizadas se enfatiza en la necesidad de efectuar dicho control sobre los servicios que brinda el Sector Público Nacional considerados como IC en el Programa (2011), en las acciones de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2015 y 2016), de la Coordinación de Operaciones de Ciberseguridad (2016), en las acciones de la Dirección de Infraestructuras Críticas de Información y Ciberseguridad (2018) y en las acciones de la Dirección de Infraestructuras Críticas de Información y Ciberseguridad (2019). En el marco del Sistema de Defensa Nacional, el monitoreo de las redes de tecnología operacional de las IC de los servicios esenciales de interés para la Defensa Nacional sería uno de los objetivos del CSIRT DEFENSA (2019)[51].

Considerando el concepto de la prevención frente a interrupciones o afectaciones en las infraestructuras críticas de la información, es posible observar que dos organismos entre los años 2011 y 2019 tenían como objetivo analizar los servicios que el Sector Público Nacional brinda a través de internet y aquellos considerados como IC para prevenir fallas de seguridad. En particular, eran acciones de la Dirección Técnica de Infraestructuras Críticas de Información y Ciberseguridad (2015) y más adelante de la Dirección de Operaciones Técnicas de Ciberseguridad (2016). Es posible presumir que dicho análisis acompaña la capacidad de monitorear y acceder a la información de dichas infraestructuras siempre con el objetivo de prevenir y resguardar los servicios esenciales que brindan las IC a la sociedad. En referencia al monitoreo, el ICIC-GAP tiene entre sus objetivos el "monitorear los servicios [del] Sector Público Nacional […] y aquellos que se identifiquen como

[51] Boletín Oficial. Resolución 1380/2019. Anexo I. pág. 6. (2019, 25 de octubre). Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029.

Infraestructura Crítica para la prevención de posibles fallas de seguridad" (Disposición N° 2, 2013). Es interesante recalcar que la Coordinación de Proyectos de Investigación de Ciberseguridad (2016) tiene entre sus acciones el desarrollo e integración de las plataformas de análisis de vulnerabilidades, de gestión y de servicios de ciberseguridad y de infraestructuras críticas de información, lo cual se repite entre las acciones de la Coordinación de Operaciones de Ciberseguridad (2018) y en la Coordinación de Comunicación y Proyectos de Ciberseguridad (2018) de igual forma. Luego, se propone brindar apoyo tecnológico en el análisis de vulnerabilidades a los organismos del sector público y privado con foco en las IC mediante las acciones de la Coordinación de Comunicación y Proyectos de Ciberseguridad (2019). Finalmente, es de destacar que el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2011) tiene entre sus objetivos el monitoreo de los servicios del Sector Público y las IC para la prevención de posibles fallas de seguridad.

El ICIC-GICI (2013) tiene, entre sus objetivos, alertar a los organismos que forman parte de dicho Programa en caso de detectar intentos de vulneración de las IC. La acción de alertar se repite en las acciones de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2016) incorporando el concepto de alertar las vulnerabilidades encontradas, tarea delegada a la Dirección de Operaciones Técnicas de Ciberseguridad (2016) más allá del Programa. En este mismo orden de ideas, el alertar la detección tanto por intentos de vulneración como las vulnerabilidades de las IC puede encontrarse entre las acciones de la Dirección de Infraestructuras Críticas de Información y Ciberseguridad (2018), lo cual se repite entre las acciones de la Dirección de Infraestructuras Críticas de Información (2019). Esto mismo se amplía a través de las acciones definidas de la Coordinación de Operaciones de Ciberseguridad (2018), entre las que se destaca la recepción de las alertas generadas por organismos de diversos niveles del gobierno y del sector privado que posean información sobre IC.

Por otra parte, el concepto de asesoramiento y soporte para la protección de infraestructuras críticas de la información y ciberseguridad se puede encontrar entre los objetivos del ICIC-CERT (2011), quien debía asesorar técnicamente ante incidentes de seguridad y encausar posibles soluciones y del ICIC-GAP (2011) quien debía asesorar sobre "herramientas y técnicas de protección y defensa de [los] sistemas de información" (Disposición N° 2, 2013) a los organismos pertenecientes al Programa Nacional de Infraestructuras Críticas de

Información y Ciberseguridad. Asimismo, se ve que la Dirección de Elaboración e Interpretación Normativa (2015) tenía, entre sus responsabilidades, la acción de brindar asesoramiento y soporte permanente en materia de protección de IC y ciberseguridad mediante la elaboración de normas. Será, más adelante, una acción de la Coordinación de Comunicación y Proyectos de Ciberseguridad (2019) el proveer apoyo tecnológico a los organismos del Sector Público Nacional y organizaciones privadas de interés nacional en el análisis de vulnerabilidades, estructuras de protección de centros de datos y riesgos de ciberamenazas con foco especial en las IC. En el presente trabajo final de maestría consideramos que el soporte y apoyo, tanto técnico como no-técnico, al sector público y privado, por parte del Estado resulta de una importancia estratégica ya que permite acompañar a los operadores y responsables de las infraestructuras críticas de la información en caso de ciberamenazas y ciberataques que pudieran afectar a la sociedad en su conjunto.

En lo que hace a la respuesta, es preciso destacar el objetivo del ICIC-GICI (2013) que hace referencia a la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de las IC del Sector Público. Por otro lado, es importante resaltar que la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2015) y la Dirección Nacional de Ciberseguridad (2019) tiene como responsabilidad primaria entender en todos los aspectos relativos a la ciberseguridad y la protección de las IC (la Dirección del año 2019 hace referencia a las infraestructuras críticas de la información) además de generar capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional. En el año 2016 y a raíz de modificaciones en el organigrama de Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad, surge la responsabilidad primaria de "asistir en todos los aspectos relativos a la ciberseguridad y protección de las IC, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional" (Anexo II, Decisión Administrativa N° 232, 2016). Surge en el octavo objetivo de la Estrategia Nacional de Ciberseguridad, la necesidad de "articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques, a partir de los recursos y responsabilidades de cada organización" (Resolución N° 829, 2019).

Es importante recalcar que el Sistema de Defensa Nacional, en el marco de su jurisdicción, acompaña el concepto de anticipar y prevenir ciberataques y ciberexplotaciones a través de la definición de ciberdefensa (2019), en la medida en que pueda verse afectado el Ministerio

de Defensa, el Instrumento Militar o las infraestructuras operacionales soporte de los servicios esenciales de interés para la defensa como de procesos industriales de fabricación de bienes sensibles para la misma.

Por otra parte, en los nueve años analizados se puede observar que el Sistema de Seguridad Interior contribuye - exclusivamente - a la protección de las IC a través de la creación del Comité de Respuesta de Incidentes de Seguridad (2017) propio del Ministerio de Seguridad y sus órganos dependientes para colaborar y elaborar informes de recomendaciones a favor de la protección de dichas infraestructuras. Es nuestro entender que dicho Sistema y, en particular, las fuerzas de seguridad debieran participar en mayor medida de la protección de las IC nacionales.

Surge de lo analizado que la APN comenzó a considerar a la prevención mediante las acciones de monitoreo y alerta. Asimismo, se considera como potestad del Estado la de brindar soporte, apoyo y asesoramiento de la misma manera que pretende brindar respuesta y defensa ante amenazas, vulnerabilidades y ataques cibernéticos. Es lamentable no poder identificar un único organismo que tenga la experiencia y la capacidad técnica y específica que se requiere para el cumplimiento de estas acciones. Sin embargo, es invaluable poder observar que el Estado está dispuesto a hacerse cargo de ello y considera - de forma mínima - extender ese servicio al sector privado.

5.2.2 Coordinación público-privado

En lo que hace al universo normativo establecido en el marco teórico, tanto en el ámbito del Sistema de Gestión Integral como en el ámbito del Sistema de Defensa Nacional, resalta la idea de la colaboración y la importancia del rol compartido entre los sectores público y privado como se observa entre los objetivos del grupo de trabajo ICIC-INTERNET SANO quien debe "promover la concientización en relación [al…] rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica" (Disposición N° 2, 2013).

Desde el año 2011, el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2011) hace referencia a la identificación y protección de las IC del sector público y las organizaciones del sector privado. Asimismo, establece el rol compartido de ambos sectores para el resguardo de dichas infraestructuras. Esto mismo se repite entre los objetivos de la Subsecretaría de Protección de las Infraestructuras Críticas de la información y Ciberseguridad (2015) donde se incorpora al ámbito académico y los conceptos de

colaboración y cooperación entre los dichos sectores. De igual forma, esto se repite entre los objetivos de la Subsecretaría de Tecnología y Ciberseguridad (2016).

Asimismo, el ICIC-GICI (2013) hace referencia, entre sus objetivos, a la elaboración de una política de resguardo de seguridad digital conjuntamente, y al fortalecimiento de lazos entre los sectores públicos y privados. Por otra parte, el concepto de colaboración y fortalecimiento de lazos entre dichos sectores se repite en las acciones de la Dirección Nacional de Infraestructuras Críticas de información y Ciberseguridad (2015 y 2016). En el año 2016, nuevamente se repite el concepto de elaboración de las políticas de resguardo de la seguridad digital con foco en IC con el sector privado entre las acciones de la Coordinación de Proyectos e Investigación de Ciberseguridad (2016).

En el caso de la Dirección de Infraestructuras Críticas de Información y Ciberseguridad (nombrada como tal en la Decisión Administrativa N° 297/2018 y luego en la Decisión Administrativa N°103/2019 con un nombre similar) la acción establece proponer y diseñar la política de seguridad de la información y ciberseguridad con foco específico en las infraestructuras críticas y en coordinación con el sector privado.

Por otra parte, en el Sistema de Defensa Nacional, la Subsecretaría de Ciberdefensa (cuando dependía de la Secretaría de Investigación, Política Industrial y Producción - Decreto N° 174/2018 como su posterior dependencia de la Secretaría de Estrategia y Asuntos Militares - Decreto N° 684/2019) debía "impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados" (Objetivo 9°, Decreto N° 174/2018 y Objetivo 13°, Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019).

Es de recalcar que las normas argentinas del PEN acogen - mediante objetivos y acciones - la necesidad de coordinar al Sector Público Nacional con el sector privado a favor de la protección de las infraestructuras críticas de la información. Sin embargo, no es posible detectar la forma en la que se planea iniciar y consolidar la cooperación y coordinación entre ambos sectores. En particular, no es posible hallar un plan efectuado con el fin de avanzar en la colaboración y la construcción de la confianza en ambos sectores que podría haberse iniciado aun sin haber identificado las IC argentinas puesto que, efectivamente, esta asociación hubiera traído aparejada una serie de beneficios para ambos sectores a mediano y largo plazo en la aplicabilidad de la tecnología y recursos humanos. Convenios,

asociaciones y contratos son algunos de los instrumentos legales que podrían emplearse para iniciarse en la cooperación. De igual forma, no es posible determinar qué organismo debiera enfocarse en efectuar los planes y políticas que permitirían incrementar la confianza que se requiere para que esta asociación y trabajo mancomunado de ambos sectores sea posible. Esto afecta, no solo la posibilidad de responder ante incidentes de seguridad contra las IC, sino también la posibilidad de prevenir y anticipar las distintas amenazas, riesgos y comprender contramedidas para proteger a las IC. Asimismo, es imprescindible evaluar el interés que podría tener el sector privado de intercambiar información con el sector público, dado que "[…] la percepción de la industria sobre la capacidad del gobierno para gestionar situaciones críticas es sumamente importante para generar confianza y cooperación" (García Zaballos & Jeun, 2016, pág. 54).

En términos generales y a nivel mundial, las infraestructuras críticas de la información cuya afectación podría tener un impacto en la sociedad son propiedad, responsabilidad y operados por el sector público y el sector privado[52]. Por esto, la asociación entre ambos sectores es fundamental para identificar, proteger y defender dichas infraestructuras. Por otra parte, cuando los Estados se centran en lograr que las IC sean más seguras y resilientes mediante la gestión del riesgo y el incremento de la confianza entre los sectores público y privado, se obtiene una facilitación del crecimiento económico del país (*Public Safety Canada*, 2014, pág. 4).

La Estrategia Nacional de Ciberseguridad establece que será necesario el:

> Fortalecimiento de la cooperación para el intercambio de información ante vulnerabilidades y amenazas, así como la promoción de los esfuerzos coordinados dentro de las redes industriales a favor del fortalecimiento y resguardo de los servicios críticos y productivos (Anexo I, Objetivo 8°, Resolución N° 829, 2019)

en el marco de la protección de las infraestructuras críticas de la información nacionales. Consideramos que la implementación efectiva de cualquier plan relacionado con las IC nacionales depende, en gran medida, de la interrelación entre los agentes de ambos sectores,

[52] "Las IC, mismo perteneciendo a áreas estratégicas para los países, ya no son nacionalizadas como en el pasado, y su control está mayormente a cargo del sector privado. En la mayoría de las veces, corresponde a los Gobiernos nacionales el papel de regulador". (Villamizar, 2018)

el intercambio de información sistemática y multidireccional[53] y la continua cooperación en el marco de la confianza mutua. Dicho intercambio es la contribución más significativa y necesaria a la hora de anticipar las amenazas, riesgos, dependencias y compartir todo tipo de conocimientos y experiencias sobre posibles contramedidas para proteger y defender las IC. Para ello, es imprescindible que las organizaciones y empresas del sector privado perciban que el gobierno es igual o más capaz que el sector privado para gestionar situaciones críticas o, al menos, que se le ofrezcan los incentivos adecuados para acompañar las iniciativas público-privado auspiciadas desde el Estado. Además, el sector privado deberá comprender su alcance e importancia en la protección de dichas infraestructuras independientemente del interés por proveer un servicio a cambio de ingresos económicos, del mismo modo que el sector público tiene la obligación de custodiar los derechos, deberes y garantías de los ciudadanos argentinos. Es decir, ambos tienen distintos objetivos susceptibles de armonización estratégica y es el Estado quien debe velar por el todo.

5.2.3 Investigación, desarrollo e innovación

En términos generales y con base en lo analizado hasta aquí, es posible observar que tanto en el Sistema de Gestión Integral como en el Sistema de Defensa Nacional se hace referencia a la investigación, desarrollo e innovación (en adelante "I+D+i") con el fin de disminuir las vulnerabilidades relacionadas con la ciberseguridad, los riesgos en las IC, así como cooperar e intercambiar con los ámbitos académicos, científicos y empresariales en pos de un avance en la protección de dichas infraestructuras conjuntamente.

Considerando al Sistema de Gestión Integral, esto se observa entre los objetivos del ICIC-GAP quien debiera "investigar sobre nuevas tecnologías y herramientas en materia de seguridad informática" (Disposición N° 2, 2013) e "incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional" (Disposición N° 2, 2013). Además, es posible observar la acción de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad (2015) de "investigar e incorporar nuevas tecnologías y herramientas en materia de seguridad informática para minimizar todas las posibles vulnerabilidades de la

[53] Donde ambos sectores deberán participar y comprender la criticidad de cooperar mutuamente dado que las IC no pueden ser protegidas de forma aislada, sino que por el contrario, los esfuerzos en conjunto multiplicarían la resiliencia de las mismas.

infraestructura digital del Sector Público Nacional" (Anexo II, punto 6°, Decreto N° 1067, 2015). Asimismo, es preciso destacar la acción de la Coordinación de Proyectos e Investigación de Ciberseguridad en la Resolución N° 490-E/2016 ya que demostró avances significativos especificando qué desarrollar, considerando las vulnerabilidades, las amenazas y la tecnología y herramientas que podrían disminuir el riesgo de afectación de las IC. Lamentablemente, *a posteriori* no se encontró normativa que permita inferir que el Sistema de Gestión Integral conservó en detalle aquello que debía realizar para avanzar en la I+D+i en ciberseguridad y tecnología a favor de la protección de las infraestructuras críticas de la información que podría haber marcado el rumbo de la temática.

En el año 2018, con una nueva gestión política y luego de un gran reordenamiento de la estructura del PEN, se repitió esa misma acción incorporando la automatización en la detección de dichas "[…] vulnerabilidades de ciberseguridad para minimizar los riesgos de la infraestructura digital del Sector Público Nacional" (Decisión Administrativa N° 297, 2018) en el marco de la Dirección de Infraestructuras Críticas de Información y Ciberseguridad.

Por otra parte, no se conocen acuerdos de cooperación realizados entre los organismos pertenecientes al Sistema y organismos, institutos, académicos y empresas que podrían, definitivamente, haber maximizado el avance de la I+D+i en ciberseguridad, impactando positivamente en la sociedad en general, contribuyendo a la seguridad de los sistemas informáticos que emplea el ciudadano, la protección de datos y/o información personal así como al resguardo de las infraestructuras que brinda servicios esenciales.

En términos generales, para el presente trabajo final de maestría, se acompaña la noción de la Directiva de Política de Defensa Nacional, la cual afirma que la Defensa Nacional:

> Es una función esencial e indelegable del Estado Nacional y tiene por objetivo rector garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación y la protección de la vida y la libertad de sus habitantes. (Considerando, Decreto N° 703, 2018)

Considerando la I+D+i (y producción de tecnología) en Argentina por parte del Sistema de Defensa Nacional, parecería que el Ministerio de Defensa, el Instrumento Militar y todos los

actores que forman parte del Sistema, deben ser impulsores de dicha actividad, en conjunción con otros actores y el sector privado para resguardar la función de la Defensa Nacional. Inclusive, es imprescindible la participación del Sistema en la I+D+i, con el objetivo de incrementar la protección y defensa de las infraestructuras críticas de información de la Nación, en pos de alcanzar el máximo resguardo posible de los intereses nacionales frente a las amenazas que pudieran vulnerar las infraestructuras que soportan servicios esenciales para la sociedad.

En lo que hace al recorte temporal contemplado en el presente trabajo (2011-2019) y el marco teórico planteado, es posible observar que se creó la Unidad de Coordinación de Ciberdefensa en el ámbito de la Jefatura de Gabinete del Ministerio de Defensa mediante la Resolución N° 385/2013. Allí "[…] se establece que la ciberdefensa requiere de la participación de todos los miembros del sistema de la defensa e innovación tecnológica del país" (Cornaglia & Vercelli, 2017).

En mayo del año 2016 se creó la Subsecretaría de Ciberdefensa - dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa - que tenía a cargo dos direcciones nacionales. Considerando la I+D+i, es importante destacar a la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa, cuya responsabilidad primaria era la de "[…] coordinar trabajos y proyectos de investigación y desarrollo en el tema de ciberdefensa" (Decisión Administrativa N° 546, 2016) teniendo en cuenta diversos actores que forman parte del Sistema como el Ministerio, el Estado Mayor Conjunto de las Fuerzas Armadas, organismos públicos y privados, entre otros.

En el año 2018, la Subsecretaría de Ciberdefensa pasó a depender de la Secretaría de Investigación, Política Industrial y Producción cuyo objetivo era:

> Entender en la formulación, aprobación y supervisión del cumplimiento de las políticas y programas de los organismos de investigación y desarrollo del sector de Ciberdefensa, como así también en la promoción del intercambio de información técnica y en la coordinación y conducción superior de los organismos científicos y tecnológicos del área de ciberdefensa. (Decreto N° 174, 2018, objetivo n° 9)

Finalmente, en el mes de octubre del año 2019 se actualizó nuevamente el organigrama de la APN y la Subsecretaría de Ciberdefensa mantuvo sus responsabilidades y acciones pero

pasó a depender de la Secretaría de Estrategia y Asuntos Militares. Dicha Secretaría tenía entre sus acciones la de "entender […] en el cumplimiento de las políticas y programas de los organismos de investigación y desarrollo del sector Ciberdefensa y en la coordinación y conducción superior de los organismos científicos y tecnológicos del área de Ciberdefensa" (Objetivo 11, Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019).

Por otra parte, exógeno del ámbito de la ciberdefensa, la Secretaría de Investigación, Política Industrial y Producción para la Defensa tenía entre sus objetivos el de:

> Asistir en la elaboración de un plan plurianual científico y tecnológico para la defensa y sus reformulaciones, como así también en la complementación y apoyo entre el Sistema Científico Tecnológico para la Defensa y el sector privado. (Objetivo 5, Planilla anexa al artículo 2°, Anexo II, Decreto N° 684/2019)

Esto demuestra la articulación entre los diferentes sectores a favor del desarrollo científico y tecnológico para la defensa.

A partir del presente análisis, es de recalcar que en el Sistema de Defensa Nacional se ha hecho énfasis en la idea de que la I+D+i es necesaria y se ha incorporado la temática al ámbito de la ciberdefensa. Teniendo en cuenta los intereses máximos de la Defensa Nacional, es posible presuponer que esto es en pos de la soberanía nacional. Asimismo, se puede observar que el Sistema ha considerado particularmente la cooperación y coordinación con los sectores públicos, privados y al Sistema Científico Tecnológico para la Defensa en materia de I+D+i lo cual, llevado a la práctica, podría generar resultados excepcionales impactando positivamente en el país.

Es de lamentar que la norma carezca de las debidas especificaciones a la hora de considerar la importancia de crear y trabajar en la I+D+i haciendo énfasis en las infraestructuras críticas de la información y la ciberseguridad. Por otra parte, será importante evaluar la aplicabilidad de lo que podría desarrollarse en el marco del Sistema al ámbito civil, industrial y comercial, para poder ejecutarlo en los sectores y organismos identificados como IC.

Dado que las IC pueden ser objeto de ataques que generen un impacto negativo en la sociedad, y teniendo presente que la prevención ya no es la única forma de salvaguardar dichas infraestructuras dados los conocimientos de los ciberatacantes y las técnicas que

emplean, resulta indispensable una inversión continua y el diseño de un plan para la I+D+i[54] en ciberseguridad que haga especial hincapié en las IC en la Argentina. Creemos que a favor de la prevención y la resiliencia de dichas infraestructuras, es imprescindible continuar con la línea del Sistema de Defensa Nacional a favor de la "[…] obtención y creación propia [a modo de soberanía y autodeterminación tecnológica] de productos, metodologías, procesos y sistemas resilientes que sean lo suficientemente sofisticados, [eficaces y eficientes] para la detección temprana de posibles vulnerabilidades contra las infraestructuras críticas de la información en la Argentina" (Taverna, I+D+i en ciberseguridad = prevención y resiliencia de las infraestructuras críticas, 2020).

En referencia a la normativa analizada, es posible observar que la interrelación entre los distintos sistemas institucionales nacionales existentes dificulta la interacción de aquellos organismos e instituciones que forman parte del ámbito militar, civil, académico, público y privado; lo cual obstaculiza la maximización del beneficio que podría aportar el trabajo en conjunto y sistemático en un plan a corto y mediano plazo sobre I+D+i.

Considerando la temática, es imprescindible recalcar que en el segundo artículo del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (Resolución N° 580/2011) establece como objetivo promover la relación entre las organizaciones públicas y privadas y sus interdependencias para desarrollar estrategias y funciones en un foro común con el fin de llevar al entorno productivo las tecnologías disponibles.

Además, el sexto objetivo de la Estrategia Nacional de Ciberseguridad trae luz a la necesidad de desarrollar la industria de ciberseguridad nacional y potenciar las capacidades tecnológicas ya que contempla, entre sus objetivos, el de promover la industria nacional de la ciberseguridad con el fin de:

> Fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a

[54] Los autores Fuentes Pujol y Arguimbau Vivó afirman que la "investigación y desarrollo son dos actividades científicas y tecnológicas de gran valor porque implican la creación de nuevo conocimiento, elemento clave para el progreso general de la sociedad. Si a ellas se le añade la aplicación práctica de los progresos a través de la innovación tendremos el ciclo completo de un sistema de investigación". (Fuentes Pujol & Aguimbau Vivó, 2008)

> las diferentes amenazas, fomentando las actividades de investigación, desarrollo e innovación tanto a nivel público como privado. (Anexo I, pág. 7, Resolución N° 829, 2019)

5.2.4 Capacitación y concientización

Ciertamente, la maximización de los beneficios de las tecnologías requiere de usuarios y expertos capacitados para la adecuada operación y uso de las plataformas y herramientas de ciberseguridad. Tal como afirman los autores Disparte y Furlow:

> La tecnología es una pieza crítica del rompecabezas de la ciberseguridad, pero al igual que un automóvil que contiene la última tecnología en seguridad, la mejor defensa sigue siendo un conductor bien capacitado. (Disparte & Furlow, 2017)

Por ello, considerar el resguardo de las infraestructuras críticas de la información de cualquier país requiere del diseño de procedimientos, procesos y métodos técnicos, pero, principalmente, de una buena gestión del capital humano. Frente a ello, la fuerza laboral perteneciente a dichas infraestructuras debería desarrollar, implementar y efectuar estrategias cibernéticas, tanto defensivas como ofensivas, así como habilidades organizativas y de comunicación, lo cual incluye roles técnicos y no técnicos, así como trabajar en el marco de la multidisciplinariedad.

En efecto, es posible destacar dos objetivos de la Estrategia Nacional de Ciberseguridad los cuales hacen referencia a la concientización del uso seguro del ciberespacio como:

> El proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ella la adopción de hábitos basados en las mejores prácticas. (Anexo I, objetivo 1°, Resolución N° 829, 2019)

y a la capacitación en el uso seguro del ciberespacio "[…] entendido como el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio" (Anexo I, objetivo 2°, Resolución N° 829, 2019). Sin embargo, lamentablemente dichos objetivos no hacen énfasis en la capacitación y concientización, en torno a las infraestructuras críticas de la información, siendo que debería ser un foco por demás imprescindible para evaluar medidas y planes a corto, mediano y largo plazo.

En lo que respecta al Sistema de Gestión Integral, la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad tenía entre sus acciones:

> Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el SECTOR PÚBLICO NACIONAL y al público en general, como así también del rol compartido entre el SECTOR PÚBLICO NACIONAL y privado para el resguardo de la infraestructura crítica. (Anexo II, Decreto N° 1067, 2015)

Esta acción reapareció bajo la responsabilidad de la Coordinación de Comunicación y Proyectos de Ciberseguridad dependiente de la Dirección Nacional de Ciberseguridad (antes Dirección Nacional de Infraestructura Tecnológica y Ciberseguridad) dependiente, a su vez, de la Secretaría de Gobierno de Modernización - antes Ministerio de Modernización - de forma directa. Lamentablemente, no fue posible encontrar evidencia suficiente para determinar que se cumplió con algunas de las políticas en materia de capacitación y concientización propuestas.

Luego, la Dirección de Capacitación, Concientización y Difusión (2015) debía diseñar y proponer políticas de capacitación en ciberseguridad y protección de infraestructuras críticas de información. Más adelante mediante el Decreto N° 174/2018, el Ministerio de Modernización creó la Secretaría de Infraestructura Tecnológica y País Digital incorporando nuevos objetivos entre los cuales es posible destacar el número once que considera la capacitación y concientización al sector público, privado y académico mediante mejores prácticas y políticas de capacitación.

En términos generales, en el ámbito de la Defensa Nacional se suele hacer hincapié en la formación del recurso humano castrense[55] desde el liceo militar pasando por los diferentes institutos de las Fuerzas Armadas, facultades y universidades. En lo que hace a la

[55] La Defensa Nacional como sistema comprende al Instrumento Militar de la Nación bajo la dirección del Ministerio de Defensa. En consecuencia, el componente militar converge con el político-administrativo a fin de dar cuenta de un propósito complejo como el estipulado en el artículo 2º de la ley de Defensa Nacional 23.554: "garantizar de forma permanente la Soberanía, Independencia, Integridad Territorial, Capacidad de Autodeterminación y vida y libertad de los Habitantes" (Ley N° 23.544, 1988). En atención a la magnitud del propósito impuesto por la norma, las respectivas capacitaciones contempladas para los elementos político-administrativos y militares del sistema de Defensa son (deben ser) diferenciales, en virtud de que los desempeños esperados deberían ostentar un cariz complementario. Ergo, la segregación de funciones obedece al imperativo de especialización profesional propio de cualquier tramitación ordenada frente a un objetivo complejo.

ciberdefensa, es posible observar que uno de los objetivos de la Subsecretaría de Ciberdefensa, como entidad jerárquica directiva en el elemento político-administrativo era el de "fomentar políticas de convocatoria, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado" (Anexo I, Objetivo 7°, Decreto N° 174, 2018). Este mismo objetivo se repite en octubre del año 2019 cuando se actualiza el organigrama de la APN mediante el Decreto N° 684/2019 y la Subsecretaría de Ciberdefensa pasa a depender de la Secretaria de Estrategia y Asuntos Militares.

En particular, en materia de capacitación y concientización la normativa fue breve, austera y poco clara, dificultando la efectiva aplicación y planificación. Igualmente, es de destacar que en el ámbito público y a través de las normas del PEN, se haya considerado a ambos como una parte importante de la ciberseguridad y la ciberdefensa. Sin embargo, lo establecido ha sido breve y poco claro provocando dificultades a la hora de planificar y aplicar planes relacionados con la capacitación y concientización de los operadores y responsables de las infraestructuras que soportan servicios esenciales para la sociedad. Nos encontramos con la falta de un Esquema Nacional de Capacitación y Concientización en Ciberseguridad para las Infraestructuras Críticas que tenga en cuenta la colaboración público-privado y la academia, así como un organismo centralizado que pudiera efectuar una capacitación y concientización dirigida a los operadores críticos con el objetivo de maximizar la protección de las IC.

5.2.5 Cooperación internacional

En Argentina, la Estrategia Nacional de Ciberseguridad (Anexo I, Resolución N° 829, 2019) tiene entre sus principios rectores la integración internacional. Además, su séptimo objetivo se relaciona con la cooperación internacional a favor de contribuir a la mejora de la ciberseguridad en dicho ámbito. También, avanza con algunas medidas y acciones que se deberían realizar como promover el desarrollo de acuerdos regionales e internacionales a favor de un ciberespacio pacífico y seguro, el fortalecimiento de la presencia del país en materia de ciberseguridad y en todos los organismos internacionales, así como mantener una participación activa en todos los ámbitos académicos y técnicos internacionales. Además, en el octavo objetivo de la Estrategia - el cual se relaciona con la protección de las IC - una de las acciones a realizar es el fortalecimiento de la cooperación en el intercambio de información ante vulnerabilidades y amenazas. Esto puede relacionarse y extenderse al ámbito internacional, en la medida en que la cooperación con otras naciones en esta temática

en particular podría significar una efectiva prevención y preservación de las IC ante amenazas y ataques.

Por otra parte, considerando los organismos analizados en el marco teórico, es posible observar que la APN incursionó en la temática pretendiendo impulsar relaciones internacionales en el marco de la ciberseguridad y las IC desde el PEN a través del Sistema de Gestión Integral. Esto puede visualizarse en una de las acciones de la Dirección de Elaboración e Interpretación (2015) que hace referencia a la elaboración de convenios para establecer alianzas bilaterales y multinacionales en la temática. En el año 2016, el Decreto N° 898/2016 amplía los objetivos de la Subsecretaría de Tecnología y Ciberseguridad (creada por el Decreto N° 13/2016) e incorpora la participación en "grupos de trabajo multisectoriales, comisiones y organismos nacionales e internacionales interviniendo en acuerdos, convenios y tratados internacionales que incluyan aspectos relacionados con redes y telecomunicaciones en el Sector Público Nacional" (Objetivo 15, Decreto N° 898, 2016). Es menester destacar este objetivo, ya que a pesar de ser muy completo, quien redactó la norma perdió la oportunidad de incorporar la noción de ciberseguridad e IC a favor de la cooperación internacional. Sin embargo, estos conceptos son incluidos en el objetivo citado precedentemente de la Secretaría de Infraestructura Tecnológica y País Digital a través del Decreto N° 174/2018.

Asimismo, en el año 2019 se creó la Dirección Nacional de Ciberseguridad dependiente de la Secretaría de Gobierno de Modernización que tenía entre sus acciones establecer "prioridades y planes estratégicos de abordaje de la ciberseguridad, fomentando el desarrollo de proyectos de cooperación otros Estados y Organismos Internacionales y nacionales" (Planilla Anexo al Artículo 2°, Anexo II, Decisión Administrativa N° 103, 2019, pág. 3).

Es preciso señalar que Argentina cuenta, entre sus instrumentos legales de cooperación internacional, con el Convenio sobre la Ciberdelincuencia (Council of Europe, 2001) - mejor conocido como Convención de Budapest por haberse celebrado en esa ciudad el 23 de noviembre del año 2001 - el cual fue incorporado a la normativa nacional a través de la ley N° 27.411 en el año 2017. Dicho Convenio es el primer tratado internacional que tiene como objetivo generar una política penal común y la protección de la sociedad frente a la ciberdelincuencia "[…] mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional […] reforzada, rápida y eficaz" (Council of Europe, 2001, pág. 2). El Convenio hace referencia a los riesgos de que las redes informáticas y la información

electrónica sean utilizadas para cometer ciberdelitos y a la importancia en la prevención de los actos que podrían poner en peligro la confidencialidad, la integridad y la disponibilidad (los tres pilares de la ciberseguridad) de los sistemas redes y datos informáticos y el abuso sobre los mismos[56].

Para este trabajo final de maestría, se considera que la lógica de la cooperación y colaboración internacional radica en el por qué, cuándo y cómo colaborar que, en general, se relaciona con el cumplimiento de intereses nacionales y la gestión de hostilidades colectivas de los distintos países, así como resguardar las IC compartidas ya sean dependientes[57] o interdependientes[58]. Frente a ello, es de suma importancia que la APN haya avanzado – breve pero significativamente - en la reglamentación de la cooperación internacional en el ámbito del Sistema de Gestión Integral considerando al cibercrimen, la ciberseguridad y las IC ponderando la dificultad de disociar la jurisdicción nacional de la internacional en el ciberespacio. Sin embargo, se considera que para que la cooperación internacional sea efectiva y Argentina se posicione internacionalmente en la temática, es menester que el organismo que deba impulsar dicha cooperación se encuentre en un orden de prelación mayor que los organismos analizados aquí. Es decir, será necesario que quien impulse la cooperación internacional en materia de ciberseguridad en pos de la protección de las IC se encuentre estratégicamente ubicado dentro del organigrama más cerca del Presidente de la Nación.

Asimismo, en el marco de la ciberseguridad consideramos que debería haber mayor énfasis en la cooperación internacional dada la naturaleza sin fronteras del ciberespacio y el incremento en la sofisticación de las ciberamenazas que puede afectar global e

[56] Fuera del aspecto de la cooperación internacional como uno de los principios rectores de la Convención, es necesario comprender de la comisión de delitos vinculados con las tecnologías de la información y las comunicaciones son una afectación a la Seguridad Interior, por lo que es imprescindible incorporar a las fuerzas de seguridad y policiales que investigan dichas conductas típicas y antijurídicas, y al Poder Judicial, con el fin de maximizar la protección de dichas infraestructuras.

[57] La dependencia entre infraestructuras puede ser definida como "un enlace o conexión entre dos infraestructuras, a través del cual el estado de una infraestructura influye o se correlaciona con el estado de la otra" (Rinaldi, Peerenboom, & Kelly, 2001, pág. 14).

[58] La interdependencia entre infraestructuras puede ser considerada como "la relación bidireccional entre dos infraestructuras a través de las cuales el estado de cada una influye o se correlaciona con el estado de la otra" (Rinaldi, Peerenboom, & Kelly, 2001, pág. 14). La interdependencia de las infraestructuras puede ser física, cibernética, geográfica, lógica y/o ambiental.

indistintamente a cualquier país. Inclusive, el intercambio de información e inteligencia[59] así como la asistencia mutua entre Estados y organizaciones internacionales, pueden tornarse esenciales para responder ante una ciberamenaza, una cibercrisis y/o un ciberataque que pudiera poner en riesgo a las IC de cualquier país. Es claro que la efectividad de dicha cooperación depende de los objetivos estratégicamente alineados de las políticas y las relaciones bilaterales-multilaterales. Frente a ello, las políticas nacionales y los acuerdos internacionales que abordan la temática de la ciberseguridad deben ser considerados como instrumentos básicos para avanzar en la cooperación entre Estados[60].

5.3. Hallazgos del análisis del *NCSI* y España

Con base en el breve análisis efectuado en el marco teórico, percibir a España como un ejemplo superador en comparación a Argentina es una conclusión que se desprende de la simple descripción de los avances logrados en la materia por el país ibérico. Sin embargo, el *NCSI* provee una visión de la capacidad en ciberseguridad de ambos países y es posible determinar qué aspectos deben mejorarse. A continuación, se presentarán los principales hallazgos con base en Argentina y en el marco de la comparativa de ambos países.

Teniendo en cuenta el desarrollo de políticas de seguridad cibernética, resalta particularmente que Argentina no ha efectuado el plan de implementación de la estrategia de seguridad cibernética (lo que se conoce como la Estrategia Nacional de Ciberseguridad) para ejecutar las acciones a realizar y cumplir con los objetivos definidos allí. Por otra parte, el *NCSI* muestra que la Argentina no ha avanzado en los criterios de protección de servicios esenciales que se requieren: identificación de operadores críticos, los requisitos de

---

[59] "[…] señalan Klimburg y Mirti, las actividades de contrainteligencia (por ejemplo, las dirigidas a la detección de las ciberintrusiones más sofisticadas) dependerán muy a menudo de la recolección ofensiva de inteligencia, aunque también del intercambio de información entre socios internacionales" (Domínguez Bascoy, 2015, pág. 216).

[60] Argentina firmó dos Memorándums de Entendimiento considerados como "acuerdo entre entidades que se comprometen a producir una o más acciones de provecho común" (Postigo de Bedia & Díaz de Martínez, 2006, pág. 162) con Chile y con España, así como una asociación (*partnership* en inglés) con Estados Unidos sobre políticas cibernéticas. En el caso del acuerdo con Chile, el mismo tiene como principal objetivo "la cooperación recíproca en materia de ciberseguridad, ciberdefensa y ciberdelito en el ámbito del ciberespacio" (DPI Cuántico, 2018, pág. 2). Con España, el Ministerio de Modernización de la República Argentina firmó un memorando con el Ministerio de Energía, Turismo y Agenda Digital del Reino de España con el objetivo de "impulsar el establecimiento de estrategias comunes para la protección del ciberespacio, coordinando acciones que intensifiquen y optimicen las capacidades existentes, el desarrollo del talento, contribuyendo al impulso y consolidación de la industria de la ciberseguridad" (Cancillería Argentina, 2017).

ciberseguridad que ellos deben cumplir, la autoridad competente dispuesta por el gobierno para supervisar los requisitos que deben cumplir dichos operadores y el seguimiento periódico de las medidas de ciberseguridad que los operadores deben efectivamente implementar. Además, el criterio de respuesta a incidentes cibernéticos permite concluir que Argentina deberá centrar sus esfuerzos en que los proveedores de servicios y los operadores críticos informen los ciberincidentes que ocurrieron, en el marco de la cooperación y la mejora continua, con el fin último de disminuir la probabilidad de que vuelvan a suceder. Finalmente, para mejorar la gestión de crisis cibernética y considerando la valoración del *NCSI*, Argentina debiera establecer desde el gobierno un plan de gestión a gran escala y establecer procedimientos para el soporte operativo ante cibercrisis por parte de voluntarios.

Haciendo especial hincapié en la cooperación internacional y considerando que es uno de los pilares más importantes sobre los que se debe trabajar para incrementar la protección de las IC y ciberseguridad, Argentina carece de un único punto de contacto para la asistencia entre los diferentes países y organismos internacionales en el marco de la temática, lo cual dificulta la posibilidad de compartir información[61] que podría maximizar la prevención y resiliencia en las IC.

Por todo esto, es posible concluir que Argentina deberá trabajar en diferentes aspectos para posicionarse a nivel internacional y proteger sus servicios esenciales. El índice nos permite priorizar, a favor de dicha protección, la necesidad de que exista un acto legal que establezca quién y cómo identificar operadores de servicios esenciales para luego avanzar en las medidas subsiguientes.

Considerando la normativa española, es importante tener en cuenta que el país avanzó desordenadamente legislando normas que no se relacionaban entre ellas, en pos de proteger las IC nacionales (como puede observarse en la Ley 16/1987, la Ley 21/2003 o la Ley 32/2003, entre otras). Pese a ello, es sumamente destacable la idea de que, mediante una única ley y un decreto que la reglamenta, y basándose en su experiencia y la Directiva de la Unión Europea, España logró esquematizar y reordenar un conjunto de organismos, agentes y valores que, complementados con la Estrategia Nacional de Ciberseguridad (2019) ha resultado en el Sistema de Protección de las Infraestructuras Críticas de España. En

[61] Se podría compartir información y conocimiento en lo que respecta a incidentes cibernéticos, ciberamenazas, vulnerabilidades y experiencias.

resumidas cuentas, mediante dichas normas asigna responsabilidades y establece funciones a cada organismo y agente creado. Asimismo, determina la relación entre ellos, diferencia órganos políticos de los técnicos y genera un esquema de planificación y documentación compuesto por cinco instrumentos (con su respectivo orden de prelación). De igual forma, establece la necesidad de identificar y determinar dichas infraestructuras definiendo y caracterizando al Catálogo Nacional de infraestructuras estratégicas y a su responsable, así como el contenido y la reserva de divulgación que se requiere para ello.

En efecto, haber elegido a España en el marco del derecho comparado nos ha permitido conocer un Sistema institucional íntegro, eficiente, complejo pero consumado cuyo objetivo es la protección de los servicios esenciales de la sociedad ibérica. Frente a ello, se podría tomar el modelo español y ajustarlo de forma tal que sea propio y aplicable al contexto de nuestro país teniendo en miras la organización y los instrumentos que emanan del Sistema español. Ciertamente, será imprescindible que se avance con un reordenamiento nacional con base en los organismos y las responsabilidades para instaurar un Sistema de Protección de las Infraestructuras Críticas Nacional en Argentina que tenga como objetivo principal articular a todos los agentes, sistemas e interesados en la protección de las IC.

No obstante, es claro que nuestro país no podría replicar íntegramente el modelo español puesto que allí todos los agentes del Sistema dependen, en resumidas cuentas, del Ministerio del Interior. Es decir, dependen de un ministerio dentro del PEN español. Nuestra experiencia hasta aquí permite concluir que Argentina no debería basar la dirigencia y responsabilidad del Sistema de Protección de las Infraestructuras Críticas Nacionales en un Ministerio dada la práctica de modificar permanentemente las instituciones, responsabilidades, objetivos y acciones por los intereses y gestiones políticas. Sino que deberá encontrar, en la reorganización del tema, un esquema organizativo-institucional que permita resguardar la información (evitando cualquier divulgación, alteración y destrucción), identificar y determinar (sobre la base de criterios horizontales y objetivos) las IC y relacionar a todos los agentes interesados para crear y articular los documentos que hagan falta para proteger las infraestructuras que soportan servicios esenciales. Este será el desafío en nuestro país y en el presente trabajo pretendemos presentar y aportar una posible solución.

6. Propuesta final

En el marco de los hallazgos, es menester avanzar en una posible solución que contemple las normas nacionales rescatadas en los apartados 5.1 y 5.2 del presente trabajo final de maestría, como pilares fundacionales. Frente a ello y ante la necesidad de avanzar en la protección de las IC en Argentina, en este apartado se exhibirá una propuesta de solución a lo señalado en el capítulo anterior mediante la presentación de una estructura organizativa a nivel federal liderada por una agencia y compuesta por cinco direcciones generales. Además, se propone efectuar acuerdos y convenios con organismos y sistemas institucionales existentes para confluir los esfuerzos que se realizan en la actualidad hacia el cumplimiento de un objetivo común: la protección de las infraestructuras críticas argentinas.

En el presente apartado se presentará una estructura organizativa diseñada para ser incorporada en la APN a fin de contribuir a remediar gran parte de los problemas y caos observados hasta este punto y permite, a su vez, cumplir principalmente con el octavo objetivo de la Estrategia Nacional de Ciberseguridad titulado Protección de las Infraestructuras Críticas Nacionales de Información. Ciertamente, en el presente trabajo final de maestría se acompaña la idea de que:

> Cada país cuenta con una organización vertical en el tema de las [IC] dirigida desde el más alto nivel del gobierno, el que por medio de las políticas y acciones tendientes a asegurar sus recursos críticos, da el ejemplo al resto de la sociedad. (ZAGREB - Consultores Limitada, 2008, pág. 8)

Frente a ello, se propone la creación de la Agencia Federal de Protección de las Infraestructuras Críticas (sigla y en adelante "AFEPIC") que forme parte de la organización nacional en niveles estratégicos[62] y que provea liderazgo y supervisión actuando como elemento principal del Sistema de Protección de Infraestructuras Críticas de la República Argentina a crear[63].

---

[62] "Los niveles tácticos y estratégicos - en su mayoría iniciados por voluntad política - podrían, por ejemplo, estar activos en la elaboración de estrategias CIIP, establecer conexiones internacionales (a nivel estratégico, táctico, operativo/técnico) y comenzar a participar en diálogos internacionales con redes de actores públicos y privados". (Global Forum on Cyber Expertise - Meridian, 2016, pág. 21)

[63] Taverna, A., & Cárdenas Holik, R. (2020). Sistema de Protección de Infraestructuras Críticas de la República Argentina: Ciberinteligencia para la toma de decisiones. Triarius, Volumen 4 - n° 76, 18-27.

En efecto, la AFEPIC deberá emplear un enfoque regulado, es decir, deberá hacer uso de la legislación y normativa como un instrumento obligatorio para trabajar en asociación con los actores públicos y privados para la construcción de la confianza mutua, la negociación, políticas, planes y procesos específicos que permitan proteger a las infraestructuras que soportan servicios esenciales para la sociedad argentina.

A partir del caos normativo analizado con anterioridad, es posible afirmar que la creación de organismos a través de documentos que emanan del PEN no es un enfoque acertado. Por ese motivo, se propone que la Agencia sea creada por ley, es decir, que sea el PLN quien la cree como organismo descentralizado del PEN dependiente directamente del Presidente de la Nación. Considerando lo presentado en el apartado 3.1 del presente trabajo final de maestría, la creación por ley de dicho organismo permitiría que la misión, visión y funciones de la misma perduren en el tiempo y el hecho de que el PLN se componga de dos cámaras permite que haya pluralidad de visiones y perspectivas, y una menor probabilidad de incurrir en errores. Además, por ser un organismo descentralizado, la Agencia se especializaría en un ámbito de políticas públicas pudiendo actuar de forma relativamente autónomas de las autoridades políticas sin perder de vista el cumplimiento de su horizonte fundacional, con sus acciones y planes siempre trabajando en favor de la sociedad y la protección de sus servicios esenciales. Asimismo, tendría una asignación legal de recursos, patrimonio estatal, la capacidad para administrarse, personalidad jurídica propia y estaría sometida al control estatal pudiendo perdurar en el tiempo independientemente de los cambios en la APN.

Para el presente trabajo final de maestría, se presume que el titular de la Agencia debe tener conocimientos técnicos en la temática, habilidades de comunicación[64], relaciones con el mundo político, liderazgo y la capacidad para resolver situaciones de emergencia. Se sugiere que sea elegido por concurso público y mediante convocatoria pública abierta.

Además, es necesario incorporar la noción de que la protección de las IC debe ser una política de estado y un compromiso del nivel superior de gobierno - por ello se propone una Agencia multinivel con relación directa con el Presidente de la Nación - que comprometa la participación de los actores públicos y privados que se relacionen con la temática, que identifique responsables y establezca metas, plazos y documentos a implementar dada la

[64] Ya que deberá garantizar la coordinación, la cooperación y el intercambio de información entre los actores públicos y privados a favor de un trabajo mancomunado entre todos los integrantes del Sistema.

criticidad del tema a nivel nacional. Será imprescindible que las funciones de la agencia sean armónicas y complementarias a la misión de otros organismos tales como el Ministerio de Seguridad de la Nación, el Ministerio de Defensa de la Nación, la AFI y los pertenecientes al Sistema de Gestión Integral. A su vez, la Agencia propuesta será el preludio para avanzar hacia un Sistema de Protección de Infraestructuras Críticas de la Información.

Con base en lo considerado hasta aquí y teniendo en cuenta la creación de la AFEPIC, se propone a continuación su posible misión y visión como declaraciones fundamentales que establecen propósitos y metas a largo plazo:

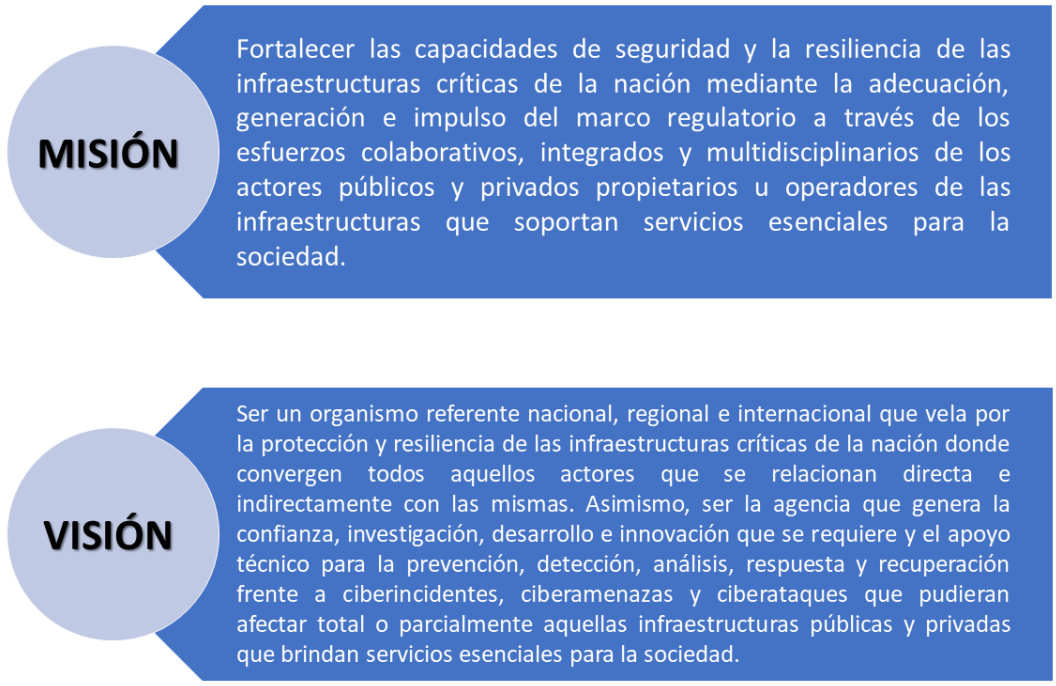


Figura 19: Posible misión y visión de la Agencia propuesta. Fuente: elaboración propia.

Funciones:

- Diseñar, aprobar y dirigir para su implementación la Estrategia Federal de Protección de las IC[65] y su respectivo plan con el compromiso de todos los actores involucrados.

[65] En el marco de la Resolución N°1380/2019, la Política de Ciberdefensa establece la necesidad de crear el Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa la cual debiera contribuir a la Estrategia Federal de Protección de las Infraestructuras Críticas y a los planes sectoriales. Es importante remarcar la relevancia de emplear la experiencia de los organismos de Defensa Nacional para dirigir los esfuerzos entorno a la seguridad de las infraestructuras críticas que soportan servicios a la sociedad.

- Diseñar políticas, normas y procedimientos destinados a fortalecer la ciberseguridad de las IC.
- Liderar y dirigir los esfuerzos necesarios para una efectiva identificación y catalogación de las IC nacionales.
- Declarar las IC nacionales y custodiar la información sensible que de ellas se obtenga, así como mantener actualizado el Inventario Federal de Infraestructuras Críticas.
- Impulsar la coordinación y cooperación entre los sectores público, privado y organismos internacionales competentes promoviendo el intercambio de información e inteligencia sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional fomentando la prevención y alerta temprana[66].
- Promover la cooperación con los actores relacionados con la protección de los servicios esenciales con el fin de mejorar conjuntamente las capacidades de prevención, detección, análisis, respuesta y recuperación para ciberincidentes, ciberamenazas, ciberataques contra IC, ya sean potenciales o en curso, fomentando la prevención, alerta temprana, investigación, desarrollo e innovación.
- Preservar y promover la existencia de una cultura de seguridad y ciberseguridad de las IC en el ámbito de la APN y los actores privados que participen en el Sistema.
- Aprobar el Plan Federal para la Identificación de las Infraestructuras Críticas Nacionales, el Plan Federal de Cooperación Multisectorial Público-Privado, el Plan Federal para la Investigación, Desarrollo e Innovación en Ciberseguridad para la Protección de las Infraestructuras Críticas, el Plan Federal de Capacitación y Concientización de los Operadores Críticos, el Plan de Seguridad de los Operadores y los Planes Estratégicos Sectoriales.
- Ratificar los Planes de Protección Específicos de cada sector y las políticas, programas y las eventuales propuestas de mejoras de estos que emanen de las direcciones generales.

[66] En la actualidad y a través del Decreto N° 1311/2015, se contempla la cooperación en materia de información entre los organismos de la APN y la AFI a favor de la detección de amenazas y conflictos que pudieran afectar a la defensa nacional y la seguridad interior. En particular, es menester tomar las acciones y medios que se emplean para el cumplimiento de dicha misión institucional e incluir la información que es imprescindible para la protección de las infraestructuras críticas nacionales además de incluir al sector privado para maximizar los resultados.

- Impulsar y coordinar las actividades relacionadas con la protección de las IC con organismos internacionales, nacionales y actores privados competentes.
- Promover la cooperación con los distintos sectores y actores competentes con el fin de ampliar, mejorar y fortalecer conjuntamente las capacidades y mecanismos de prevención, detección, análisis, respuesta y recuperación frente a los riesgos de seguridad que atenten contra las IC nacionales.
- Impulsar a la industria nacional en ciberseguridad para la protección de las IC haciendo especial hincapié en la investigación, desarrollo e innovación.

Además de las funciones de la AFEPIC, la misma tendrá dentro de su organigrama cinco Direcciones Generales, con alcance interno y externo, con funciones propias con el fin de cumplir con la misión de la Agencia. La estructura sugerida es la que se muestra en la Figura 20:

Figura 20: Posible organigrama y división interna de la Agencia Federal de Protección de las Infraestructuras Críticas. Fuente: elaboración propia.

En pos de la protección de las IC nacionales se torna imprescindible definir qué organismos y empresas públicas y privadas deben ser consideradas como tales, sobre la base de los sectores y criterios establecidos en la Resolución N° 1523/2019. Frente a ello, se crea la Dirección General de Identificación de las Infraestructuras Críticas que deberá identificar, designar y catalogar a las IC en el Inventario Federal de Infraestructuras Críticas - proceso permanente, constante y dinámico - cuya criticidad podría fundamentarse en los vínculos existentes entre los riesgos y el impacto que podría ocasionar una afectación parcial o total de las mismas. Como se dijo con anterioridad, en principio podría emplearse el Programa Nacional de Protección de las Infraestructuras Críticas para analizar aquellos inscriptos voluntariamente.

A partir del desarrollo de la Estrategia Federal de Protección de las Infraestructuras Críticas, las funciones de la Dirección General de Identificación de las Infraestructuras Críticas podrían variar e, inclusive, ampliarse. Sin embargo, para el presente trabajo final de maestría se considerarán las siguientes funciones:

- Colaborar en el diseño e implementación de la Estrategia Federal de Protección de las Infraestructuras Críticas, su respectivo plan y las actualizaciones que surjan.
- Elaborar y ejecutar el Plan Federal para la Identificación de las Infraestructuras Críticas Nacionales.
- Desarrollar un marco regulatorio que propicie la identificación y designación de las IC y sus interdependencias.
- Identificar, recopilar, analizar y valorar la información sobre posibles IC procedente de actores públicos y privados[67].
- Realizar y gestionar el contenido del Inventario Federal de Infraestructuras Críticas[68].
- Mantener operativo y actualizado el Inventario Federal de Infraestructuras Críticas[69].
- Establecer los criterios horizontales y determinar la criticidad de las infraestructuras incluidas en el Inventario.
- Identificar las interrelaciones, dependencias e interdependencias que afectan a las infraestructuras críticas del país.
- Asistir en el diseño del marco regulatorio destinado a fortalecer la ciberseguridad de las IC.

Por otra parte, dado que la asociación público-privado es considerada como imprescindible (sino fundamental) para mantener la seguridad y resiliencia de las IC, se crea la Dirección General de Coordinación Público-Privado que específicamente se relaciona con dicho concepto y que permite actuar a favor del cumplimiento del octavo objetivo de la Estrategia

[67] Podría iniciarse con aquellas inscriptas en el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad creado a través de la Resolución N° 580/2011 empleando el formulario de adhesión y el convenio de confidencialidad presente en la Disposición N° 3/2011.

[68] En principio, el inventario debiera contener datos generales de las infraestructuras críticas (como sector al que pertenece, localización física, responsable de enlace u operadores, descripción básica del servicio que brinda) y datos específicos (como impacto que podría ocasionar una interrupción parcial o total, ámbito geográfico y poblacional que cubre, interrelación con otras infraestructuras y la descripción detallada de sus funciones y sistemas, entre otros).

[69] Será responsable del alta, baja y modificación de la información sobre la base de la información brindada por los responsables de las infraestructuras críticas.

Nacional de Ciberseguridad a favor del "fortalecimiento de la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país" (Anexo I, Resolución N° 829, 2019, pág. 7).

A los efectos de su cumplimiento, el titular de dicha Dirección General deberá tener entre sus habilidades la capacidad de generar confianza entre los diversos actores, así como definir y articular de forma clara las metas, y mantener una comunicación eficaz y eficiente, así como promover la flexibilidad y adaptabilidad.

Básicamente, la implementación exitosa de cualquier plan, iniciativa y programa relacionado con la protección de las IC depende, principalmente, de la labor de esta Dirección en la medida en que la misma debe articular y coordinar la interrelación de los distintos actores públicos y privados que sean parte y se relacionen con las IC. En el presente trabajo final de maestría se sugiere emplear un enfoque basado en el sector público dada la historia de nuestro país y su forma de accionar siendo imprescindible encontrar el equilibrio entre las necesidades del privado y la incidencia de los servicios esenciales que prestan a la sociedad. Mediante este enfoque, la responsabilidad de desarrollar y coordinar la protección de las IC de la Nación estará en manos del sector gubernamental y será la autoridad principal para atraer las voluntades de los actores privados merced a una estrategia, basada en incentivos mutuamente beneficiosos, en vez de articular la iniciativa de forma coactiva. Es claro que el sector público y el sector privado, de forma independiente y desarticulada, no pueden asegurar los activos críticos de la Nación o, en su defecto, requerirían mayores esfuerzos financieros y humanos. Por el contrario, trabajar conjuntamente para elevar el resguardo de las IC sería más económico, eficiente y de rápida implementación.

A fin de delimitar las tareas de la Dirección General e independientemente de las mejoras y ampliación que pudiera ocasionar la creación de la Estrategia Federal de Protección de las Infraestructuras Críticas, para el presente trabajo de maestría se considerará como funciones de la Dirección General las siguientes:

- Elaborar, actualizar y ejecutar el Plan Federal de Cooperación Multisectorial Público-Privado para lograr la cooperación de todos los agentes relacionados con las infraestructuras que soportan servicios esenciales para la sociedad.

- Elaborar documentos legales[70] para instrumentar la cooperación entre los distintos actores.
- Actuar como punto de contacto especializado entre los distintos sectores y actores que se relacionen con las IC.
- Fomentar la cooperación y colaboración sobre la base de la confianza mutua con los actores públicos y privados relacionados con la protección de las IC.
- Promover la continua colaboración intersectorial, interinstitucional y multinivel en cuestiones de infraestructura crítica.
- Mantener las relaciones y comunicaciones fluidas entre los distintos actores para efectuar consultas continuas en el marco de la protección de las IC.
- Impulsar el intercambio de información[71] a favor de la comprensión común de amenazas, vulnerabilidades, dependencias, conocimientos y experiencias para desarrollar conjuntamente posibles contramedidas.
- Participar en la elaboración y actualización de los Planes Estratégicos Sectoriales.
- Colaborar en la designación de los responsables de los operadores de las IC.
- Proporcionar asistencia para la catalogación de las IC y la determinación de la criticidad en base a la interrelación con los distintos responsables de las IC.
- Colaborar en el diseño e implementación de la Estrategia Federal de Protección de las Infraestructuras Críticas, su respectivo plan y las actualizaciones que surjan.
- Asistir en el diseño del marco regulatorio destinado a fortalecer la ciberseguridad de las IC.

Considerando el constante avance y evolución de los riesgos tecnológicos, es indispensable una inversión continua en lo que hace a la investigación, desarrollo e innovación en ciberseguridad con especial hincapié en las IC de la Argentina. Inclusive, la construcción de una cultura de colaboración en I+D+i en ciberseguridad y ciberdefensa a nivel nacional permitiría desarrollar soluciones adaptables y plausibles de emplear en nuestro país. En efecto, es imprescindible la obtención y creación propia - a modo de incrementar los niveles de soberanía y autodeterminación tecnológica - de métodos, procedimientos y mecanismo

[70] Mediante convenios, asociaciones, acuerdos y contratos u otros instrumentos.
[71] Idealmente dicho intercambio de información debiera ser sistemático y multidireccional.

para la detección temprana de posibles vulnerabilidades, ciberamenazas y ciberataques contra las infraestructuras críticas de la información en la Argentina.

Frente a ello y dada la importancia de impulsar la industria nacional en materia de ciberseguridad a la par de resguardar las infraestructuras que brindan servicios esenciales a la sociedad, es que se crea la Dirección General de Investigación, Desarrollo e Innovación para la Protección de las Infraestructuras Críticas. La misma debiera orquestar y articular todos los organismos e investigadores independientes que efectúen y tengan los conocimientos en materia de I+D+i en ciberseguridad que realizan actividades de investigación. Es imprescindible establecer una visión y plan basados en objetivos claros a corto, mediano y largo plazo (evitando la replicación, duplicación o superposición de esfuerzos) en pos de proteger las IC nacionales y tornarlas más resilientes. Independientemente de las mejoras y ampliaciones que pudiera requerir la efectiva publicación e implementación de la Estrategia Federal para la Protección de las Infraestructuras Críticas, para el presente trabajo final de maestría se considera que la Dirección General bajo análisis debiera tener las siguientes funciones:

- Elaborar, actualizar y ejecutar el Plan Federal de Investigación, Desarrollo e Innovación en Ciberseguridad para la Protección de las Infraestructuras Críticas con objetivos a corto, mediano y largo plazo[72].
- Colaborar en el diseño e implementación de la Estrategia Federal de Protección de las Infraestructuras Críticas, su respectivo plan y las actualizaciones que surjan.
- Asistir en el diseño del marco regulatorio destinado a fortalecer la ciberseguridad de las IC.
- Promover la investigación, desarrollo e innovación en ciberseguridad para incrementar la protección y resiliencia de las IC a favor de alcanzar el máximo resguardo posible de los intereses nacionales frente a las diferentes amenazas que pudieran vulnerar aquellas infraestructuras que brindan servicios esenciales a la sociedad.

[72] Podría tener en cuenta el panorama de amenazas en evolución, métricas anuales e información relevante que permita identificar prioridades y actualizar los objetivos en base a la dinámica y evolución tecnológica. La actividad de I+D+i debería contemplar aspectos técnicos y no-técnicos.

- Impulsar el desarrollo y mejora de las prácticas de intercambio de información en la comunidad de IC con el fin de proteger la información sensible y efectuar cambios en políticas y procesos que se relacionen con las mismas.
- Alentar la investigación, desarrollo e innovación que permitan incorporar nuevas tecnologías y herramientas en materia de ciberseguridad con el fin de minimizar las posibles vulnerabilidades y amenazas de las IC.
- Promover la investigación, desarrollo e innovación para la integración de plataforma de análisis de vulnerabilidades, de gestión, de detección de amenazas cibernéticas, así como otras herramientas en materia de ciberseguridad que permitan incrementar la protección y resiliencia de las IC.
- Promover acuerdos de cooperación para trabajar mancomunadamente entre los organismos pertenecientes al Sistema Nacional de Ciencia y Tecnología, Sistema de Seguridad Interior y Sistema de Defensa Nacional[73] y a todos aquellos institutos, académicos e investigadores que trabajen temas relacionados con la ciberseguridad para la protección de las IC[74].
- Trabajar conjuntamente con el Comité Nacional de Ciberseguridad para coordinar a los diversos actores que puedan aportar a la investigación, desarrollo e innovación para la protección de las IC.
- Consolidar una estructura de investigación, desarrollo e innovación de tecnología y producción para la protección de las IC.
- Promocionar el intercambio de información técnica, investigaciones y conocimientos con aquellos organismos científicos y tecnológicos que trabajen temas relacionados a la protección de las IC[75].
- Facilitar e impulsar iniciativas y actividades para incentivar las inversiones en ciberseguridad para el diseño de medidas y herramientas que fortalezcan la seguridad y resiliencia de las IC.

---

[73] Como el Ministerio de Defensa Nacional, el Estado Mayor Conjunto de las Fuerzas Armadas, los Estados Mayores Generales de las Fuerzas Armadas, el área responsable de la ciberdefensa y otros organismos relacionados.

[74] Es importante que la Dirección General sea el principal orquestador de los distintos organismos, institutos y académicos independientes para que las investigaciones y desarrollos sean aplicables a la realidad y a las infraestructuras críticas nacionales.

[75] Se podrían desarrollar procesos simplificados y estandarizados para promover la integración y coordinación del intercambio de información a través de una doctrina desarrollada conjuntamente y procedimientos operativos estándar de apoyo resguardando cualquier información considerada sensible o confidencial.

- Impulsar el desarrollo y empleo de modelos de simulación para el análisis de las dependencias e interdependencias entre las diferentes IC y los riesgos acumulados.
- Delinear y ejecutar actividades que maximicen el intercambio de conocimiento entre los actores que efectúen I+D+i relacionados con la protección de las IC.

En el marco del presente trabajo final de maestría, acompañamos el concepto de que la formación y concientización en lo que hace a la ciberseguridad y a la protección de los servicios esenciales es sustancial, y es por ello que se considera como necesario administrar y reorganizar la capacitación de los recursos humanos que operan las IC con el fin de incrementar la cantidad de profesionales con conocimientos en seguridad cibernética para conservar los intereses de la Nación y la sociedad. Una posible prognosis de este escenario indicaría que en un lapso de tiempo reducido sería inevitable e imprescindible crear un Esquema Nacional de Capacitación y Concientización en Ciberseguridad para las Infraestructuras Críticas que contemple la colaboración público-privado con la participación del gobierno, la academia y el sector privado. Asimismo, será importante coordinar ejercicios de simulación y desarrollar planes de formación y concientización dirigidos, especialmente, a los operadores de las IC con el fin de facilitar el cambio y la innovación, promover el liderazgo y aumentar el número de profesionales calificados en ciberseguridad para hacer frente a las ciberamenazas, ciberataques y vulnerabilidades[76].

Frente a ello, se crea la Dirección General de Capacitación y Concientización a los Operadores de las Infraestructuras Críticas con el objetivo de que centralice sus esfuerzos en la formación constante - mediante convenios con organismos e instituciones de formación - de los operadores de las IC[77]. Independientemente de la publicación de la Estrategia Federal de Protección de las Infraestructuras Críticas y su efectiva implementación, para el presente

[76] En el corto y mediano plazo, consideremos la posibilidad de aplicar un sistema de reserva de personal calificado en ciberseguridad y ciberdefensa pertenecientes a los sectores público y privado quienes podrían ser contactados - mediante un comité de crisis - a partir de incidentes de seguridad informática que impacten en las infraestructuras críticas de la información en la Argentina (y la región). Esta medida permitiría hacer frente a las ciberamenazas existentes a la fecha, a la onerosidad que representa contar con fuerza laboral calificada en todos los niveles y sectores de las infraestructuras y, a la vez, proteger los intereses de la Nación prontamente.

[77] Se considerará operadores a aquellos actores y trabajadores responsables del funcionamiento diario de las infraestructuras que brindan servicios esenciales a la sociedad. Tendrán, a su vez, la obligación de valorar sus propias infraestructuras, actualizar los datos destinados al Inventario Federal y proveer la colaboración técnica que requiera la AFEPIC. Asimismo, cada infraestructura crítica deberá designar a un Responsable de Seguridad y Operadores para que la colaboración y comunicación sea ágil y dinámica.

trabajo final de maestría, se considerarán las siguientes funciones para dicha Dirección General:

- Elaborar, actualizar y ejecutar el Plan Federal de Capacitación y Concientización de los Operadores Críticos a favor de una permanente formación y actualización de conocimientos en lo que hace a la ciberseguridad, protección y resiliencia de las IC
- Colaborar en el diseño e implementación de la Estrategia Federal de Protección de las IC, su respectivo plan y las actualizaciones que surjan.
- Asistir en el diseño del marco regulatorio destinado a fortalecer la ciberseguridad de las IC.
- Promover el aprendizaje de los ejercicios de incidentes que se realicen para maximizar la resiliencia de las IC[78].
- Impulsar y diseñar planes de formación para el personal que guarde relación con la protección de los servicios esenciales en pos de comprender a la prevención y a la seguridad de manera integral.
- Organizar ejercicios y simulacros conjuntos intersectoriales para mejorar la preparación de la prevención y respuesta de los operadores de las IC frente a cualquier ciberamenaza, ciberincidente y/o ciberataque.
- Realizar planes y programas de capacitación que permitan que los operadores de las IC sean conscientes sobre el entorno de ciberseguridad y las diferentes medidas que permitan proteger aquello que soporta servicios esenciales.
- Impulsar el desarrollo, implementación y realización de estrategias para mejorar las habilidades comunicacionales, las capacidades de los roles técnicos y no técnicos para potenciar la capacidad de prevención y respuesta frente a cualquier afectación a las IC.
- Promover la concientización y capacitación de los operadores de las IC en relación a los riesgos que acarrea el uso de medios digitales e internet.
- Impulsar convenios con instituciones de formación existentes, ya sean privadas o públicas, para el diseño y dictado de capacitaciones dirigidas a los operadores de las IC.

[78] Es importante mejorar la capacidad de respuesta de los operadores de las infraestructuras críticas frente a cualquier amenaza e incidente de seguridad que pueda afectar parcial o totalmente a las mismas, así como diseñar y probar los planes de contingencia y continuidad de los mismos.

- Desarrollar planes y programas para mejorar conjuntamente las capacidades del capital humano en lo que hace a la prevención, detección, análisis, respuesta y recuperación para ciberincidentes, ciberamenazas, ciberataques contra IC ya sean potenciales o en curso fomentando la resiliencia, alerta temprana, investigación, desarrollo e innovación.
- Delinear y ejecutar actividades multisectoriales a favor de la capacitación y formación multidisciplinaria de los operadores para la protección de las IC.

Por otro lado, la falta de jurisdicción en el ciberespacio imposibilita que los riesgos que enfrenta cualquier nación y, en particular, las IC de un país no puedan contenerse o circunscribirse a las fronteras del mismo. Asimismo, raramente las IC funcionan de forma aislada, sino que por el contrario, suelen tener interdependencias que no necesariamente se encuentran en un mismo país y cuya afectación puede ocasionar consecuencias locales, regionales e internacionales.

Asimismo, la Estrategia Nacional de Ciberseguridad le da relevancia a la cooperación internacional pretendiendo impulsar acciones como desarrollar acuerdos a nivel regional e internacional que contribuyan a la generación de un ciberespacio pacífico y seguro; fortalecer la presencia de la República Argentina en todos los organismos internacionales, en materia de ciberseguridad; y mantener una participación activa en todos los ámbitos académicos y técnicos internacionales (Resolución N° 829, 2019, Anexo I, pág. 7), que en el ámbito de las IC, podría cumplirse con la Dirección General para la Cooperación Internacional en materia de Infraestructuras Críticas.

En particular y a nivel internacional, Argentina debiera trabajar prontamente en el establecimiento de un marco legislativo nacional y un plan de acción de cooperación para la seguridad internacional en el ciberespacio con el fin de relacionarse con otros Estados. Además, es menester que el país genere y comparta información e intercambie experiencias en varios niveles para promover activamente la cooperación con países dentro y fuera de la región. Será la confianza un valor imprescindible a la hora de trabajar con otros países. Inclusive, se podría tomar la experiencia española presentada en el marco teórico y, en particular, la Directiva Europea 2008/114/CE del Consejo de Europa sobre la identificación y designación de Infraestructuras Críticas Europeas, para realizar un marco normativo

aplicable a los países pertenecientes al Mercado Común del Sur (Mercosur)[79] a favor de la protección de aquellas IC que afectan a dos o más países pertenecientes al mismo. En igual sentido, se podría extender la cooperación entre estos países para el intercambio de información y el apoyo técnico en situaciones de emergencia o crisis que pudieran afectar a dichas infraestructuras.

Frente a esto, e independientemente de los objetivos de la Estrategia Federal de Protección de las Infraestructuras Críticas que podría ampliar o mejorar las funciones de la Dirección General, para el presente trabajo final de maestría se consideran imprescindible las siguientes funciones:

- Ser el punto nacional de contacto, a través de los procesos y canales existentes, con organismos internacionales en materia de IC.
- Impulsar las relaciones internacionales en el marco de la ciberseguridad y la protección de las IC nacionales[80].
- Promover acuerdos y convenios marcos con el fin de establecer alianzas bilaterales y multinacionales en materia de protección de las IC.
- Participar en grupos de trabajo multisectoriales, comisiones y organismos internacionales y nacionales.
- Intervenir en convenios y tratados internacionales que incluyan aspectos relacionados a las IC y ciberseguridad.
- Contribuir al diseño de políticas y estrategias coordinadas a nivel internacional en aquellos aspectos que refuercen la resiliencia y protección de las IC, así como fomentando el desarrollo, investigación e innovación mediante convenios con organismos internacionales.

[79] Creado en el año 1991 a través del Tratado de Asunción, "El Mercado Común del Sur es un proceso de integración regional instituido inicialmente por Argentina, Brasil, Paraguay y Uruguay al cual en fases posteriores se han incorporado Venezuela y Bolivia, ésta última en proceso de adhesión" (Mercosur, 2018).

[80] Sería importante que se impulse la asistencia mutua con el fin de compartir información e inteligencia en lo que respecta a incidentes cibernéticos, ciberamenazas, vulnerabilidades y experiencias para maximizar la prevención y resiliencia de las infraestructuras críticas tal como "[…] señalan Klimburg y Mirti, las actividades de contrainteligencia (por ejemplo, las dirigidas a la detección de las ciberintrusiones más sofisticadas) dependerán muy a menudo de la recolección ofensiva de inteligencia, aunque también del intercambio de información entre socios internacionales" (Domínguez Bascoy, 2015, pág. 216).

- Colaborar en el diseño e implementación de la Estrategia Federal de Protección de las Infraestructuras Críticas, su respectivo plan y actualizaciones con miras en las experiencias y contactos internacionales.
- Asistir en el diseño del marco regulatorio destinado a fortalecer la ciberseguridad de las IC.
- Delinear, organizar y ejecutar actividades relacionadas con la protección de las IC con organismos y grupos de trabajo internacionales.

Sobre la base de lo nombrado hasta aquí, en el presente trabajo final de maestría se considera que la AFEPIC debería relacionarse con otros agentes, organismos y sistemas institucionales dada la importancia de tomar decisiones y medidas tendientes a prevenir y anticipar emergencias mediante alertas tempranas. Asimismo, impulsar el monitoreo para generar información clave para el desarrollo de estrategias de prevención y acciones ante vulnerabilidades y ciberamenazas que pudieran afectar a las IC. A nivel estratégico, la producción de ciberinteligencia - proveniente de fuentes internas o externas[81] - generarían herramientas decisionales que también impulsaría la prevención de las acciones que pudieran afectar parcial o totalmente aquellas infraestructuras que brindan servicios esenciales a la sociedad.

En el marco de lo comentado con anterioridad, se considera que dada las habilidades de los recursos humanos, la experiencia, funciones y procesos internos de ciertos organismos existentes, es imprescindible que la AFEPIC realice acuerdos, convenios y/o contratos con ellos conforme las necesidades, propósitos y metas específicas de la Agencia y, en caso de ser necesario, en apoyo de las entidades que así lo requieran.

Como se pudo observar en los hallazgos, se toma en cuenta los cimientos normativos e institucionales aún vigentes, entre los cuales se encuentra el Comité Nacional de Ciberseguridad. En efecto y como ya se comentó, la labor conjunta y multidisciplinaria así como la importancia que se le brinda al alcance global de la ciberseguridad y la cooperación internacional hace que el Comité deba mantenerse en el tiempo con los objetivos que ya fueron delineados en el Decreto N° 480/2019 y enumerados en el marco teórico. Frente a

[81] El producto puede ser obtenido por los elementos pertenecientes al Sistema de Inteligencia Nacional, fuentes públicas o por organismos internacionales.

ello, se considera que la AFEPIC debería trabajar conjunta y colaborativamente[82] con el Comité a favor del cumplimiento de los siguientes objetivos:

- Colaborar en el plan de acción para la implementación de la Estrategia Nacional de Ciberseguridad con foco en las IC Nacionales.
- Participar en la implementación de medidas en el marco del plan de acción para la implementación de la Estrategia Nacional de Ciberseguridad.
- Colaborar y asesorar en el dictado de un marco normativo en materia de ciberseguridad con especial hincapié en las IC.
- Favorecer las relaciones entre el Comité y aquellos actores, públicos o privados, que operen o sean propietarios de IC.
- Impulsar mejoras e incrementos presupuestarios para áreas específicas que se relacionen con la ciberseguridad y las IC.
- Promover acciones de mejora para las distintas estrategias, planes, políticas y programas que desarrollen.
- Fomentar actividades de investigación, desarrollo e innovación en ciberseguridad para la protección de las IC.
- Fomentar los programas de capacitación y concientización en ciberseguridad para los operadores de las IC.

Por otra parte, en el marco teórico se hizo referencia a ciertos objetivos del ICIC-CERT y se puntualiza en la importancia del monitoreo, alerta y soporte para las infraestructuras críticas de la información en las diferentes normas. Asumiendo que el CERT Nacional (en la disposición que lo crea se lo llama "ICIC-CERT") es el actual orquestador y contacto de todos los Centros de Respuesta a Incidentes Informáticos (que se distinguen acorde a su jurisdicción temática o local[83]) e intercambian información de utilidad, en materia de protección de IC se podrían ampliar los objetivos del ICIC-CERT a favor de:

- Actuar como repositorio y administrar la información sobre reportes de incidentes de seguridad en las IC.

[82] Quedará pendiente analizar si debieran efectuarse acuerdos interadministrativos u otra forma de convenio.
[83] Como es el caso del BA-CSIRT con jurisdicción en la Ciudad Autónoma de Buenos Aires o el MINSEG-CSIRT con jurisdicción en el Ministerio de Seguridad de la Nación y sus órganos dependientes, entre otros.

- Asesorar técnicamente y brindar soporte para encauzar posibles soluciones de forma organizada y unificada a favor de la protección de las IC.
- Monitorear, controlar y analizar los sistemas y servicios que brindan las IC para prevenir fallas de seguridad y vulnerabilidades.
- Proporcionar apoyo tecnológico, mediante el análisis de vulnerabilidades y riesgos, para el resguardo de los servicios esenciales para la sociedad.
- Recibir alertas y dar aviso en caso de detectar intentos de vulneración o ciberataques en pequeña, mediana o gran escala contra las IC Nacionales.

En la misma línea de ideas, consideramos prudente y necesario que la AFEPIC realice un convenio marco u acuerdo interadministrativo con el ICIC-CERT con el fin de aprovechar las tecnologías, contactos, experiencias y conocimientos obtenidos desde su creación (2013) para maximizar la protección de las IC. Frente a lo cual, ambos podrían trabajar conjunta y colaborativamente con el fin de:

- Promover la coordinación para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad en las IC nacionales.
- Centralizar los reportes sobre incidentes de seguridad ocurridos en las IC nacionales y facilitar el intercambio de información para afrontarlos[84] [85].
- Difundir información útil que permita incrementar los niveles de seguridad y resiliencia de las IC.
- Intercambiar información sobre ciberamenazas, vulnerabilidades, mejores prácticas y herramientas para la prevención y resolución de incidentes y posterior recuperación de las IC.

[84] Inclusive, en la Resolución que crea el Comité de Repuesta de Incidentes de Seguridad Informática del Ministerio de Seguridad de la Nación se establece que dicho Comité deberá colaborar con la protección de las infraestructuras propias del Ministerio y los órganos dependientes (Resolución N° 1107-E/2017). Con esta idea en mente, es primordial que dicho Comité (entendido como un CSIRT jurisdiccional del Ministerio de Seguridad) debiera informar al ICIC-CERT (CERT Nacional) el cual deberá, a su vez, reportar los incidentes de seguridad de las infraestructuras críticas a la Agencia.

[85] Considerando a la Defensa Nacional, en el Anexo de la Resolución N° 1380/2019 se establece que el CSIRT DEFENSA realizará el monitoreo de las redes OT de las infraestructuras críticas de los servicios esenciales para la Defensa Nacional. Dicho monitoreo debiera generar informes que podrían ser compartidos con el ICIC-CERT (CERT Nacional) y, a la vez con la AFEPIC a favor del intercambio de información entre las distintas infraestructuras críticas que pudieran verse afectadas por vulnerabilidades y posibles incidentes de seguridad. Es preciso recalcar, nuevamente, la importancia de emplear la experiencia de los organismos del Sistema de Defensa Nacional en el marco de su evolución, mejoras y avances en la temática.

- Incluir al personal del ICIC-CERT en las distintas capacitaciones que se brinden a los operadores de las IC.

Igualmente, en el marco del presente trabajo consideramos que será necesario que AFEPIC ponga a disposición, a largo plazo, un equipo técnico propio que brinde asistencia a las IC para la resolución de incidentes con especial foco a la rápida recuperación de las mismas. A corto y mediano plazo, la AFEPIC podría tener una nómina actualizada de técnicos y expertos pertenecientes al Sistema de Inteligencia Nacional, al Sistema de Defensa Nacional y al Sistema de Seguridad Interior, así como especialistas del ámbito privado que formen parte directa o indirectamente de las IC y tengan conocimientos en la tecnología que allí funciona. Estos especialistas podrían ser convocados de forma voluntaria para la resolución de ciberincidentes y ciberataques que pudieran afectar a las infraestructuras que brindan servicios esenciales para la sociedad[86].

Además, será menester que la AFEPIC se relacione con los sistemas nacionales e institucionales como el Sistema de Inteligencia Nacional, el Sistema de Seguridad Interior, Sistema de Gestión Integral y el Sistema de Defensa Nacional. En efecto, dichos sistemas tienen funciones que se relacionan con la protección de las IC y son propias de los agentes y organismos pertenecientes a dichos sistemas. Asimismo, es claro que la innovación tecnológica, la confidencialidad y reserva de la información obtenida, la constante capacitación y concientización de todos los actores relacionados y la cooperación internacional requieren de una labor multidisciplinaria, así como un trabajo en conjunto que permita multiplicar los resultados y evitar la duplicación de esfuerzos para la protección de las IC. Frente a ello y con el fin último de potenciar la labor de la AFEPIC y redireccionar los esfuerzos de los sistemas institucionales existentes a favor de la protección de las IC, la coordinación entre la Agencia y los sistemas permitiría, mediante el intercambio de información:

- Producir conocimientos y efectuar informes acerca de las problemáticas, riesgos y conflictos inscritos en la defensa nacional y la seguridad interior en función de la protección de las infraestructuras que brindan servicios esenciales a la sociedad.

[86] Esta iniciativa funciona como analogía del concepto de reservista que se emplea en las Fuerzas Armadas.

- Producir información y realizar reportes orientados a las acciones que atenten contra las IC nacionales declaradas.
- Producir inteligencia sobre los riesgos y conflictos vinculados al uso de la tecnología de la información y comunicación que se empleen en las IC nacionales[87].
- Producir inteligencia sobre las amenazas que pudieran afectar a las IC nacionales.
- Fortalecer las capacidades de anticipación, disuasión, vigilancia y control en aquellas IC nacionales que sean operadas o de propiedad de los organismos y agentes del Sistema de Defensa Nacional y del Sistema de Seguridad Interior.

Asimismo, la AFEPIC debiera establecer relaciones, convenios y acuerdos con todos aquellos elementos que se vinculen con la ciberseguridad y ciberdefensa que puedan relacionarse directa o indirectamente con las IC independientemente de las jurisdicciones y sectores a los que pertenece. Esto teniendo siempre en mente a importancia de hacer valer la experiencia obtenida por parte de los organismos, elementos y empresas en materia de tecnología y ciberseguridad a favor de resguardar los servicios esenciales de la sociedad.

[87] En el marco del Decreto N° 1311/2015 analizado, el Sistema de Inteligencia Nacional podría cumplir con esto dado lo establecido en los objetivos de la Dirección de Inteligencia Informática la cual forma parte de la Dirección Operacional de Inteligencia sobre Ciberseguridad dentro del organigrama de la AFI.

7. Reflexiones finales

No man is an island, entire of itself;

every man is a piece of the continent, a part of the main[88]

J. Donne

La conclusión del trabajo final de maestría amerita el sopesado de los aspectos tratados en cada apartado mediante la aplicación de una mirada de signo integrador que permite recopilar, de manera secuencial, lo más relevante de cada momento del escrito a fin de ensamblarlo en una conclusión estilada con espíritu propositivo.

En principio y por medio del marco teórico, fue posible dar a conocer conceptos básicos del derecho, exponer cronológicamente las diferentes normas que se relacionan directamente con las IC y la ciberseguridad en la Argentina en el período comprendido por los años 2011 y 2019 y presentar brevemente el estado de la temática en España. Sin duda, la extensión del marco teórico responde a una sucesión de hitos presentes durante los nueve años analizados, que no hacen más que empañar la visión de un objetivo que ha quedado lejos de sucederse. En otras palabras, se halló una superpoblación de normas que se repitieron en el tiempo sin un avance visible en la protección de las IC argentinas.

La normativa analizada se caracteriza por la superposición, la duplicidad, la desorganización de términos y, claro, el caos. Frente a ello, en primer lugar, fue necesario extraer y rescatar aquello que se legisló desde el PEN y reordenar lo normativizado en cinco subtemas: 1) identificación, protección y defensa de las IC, 2) coordinación público-privado, 3) investigación, desarrollo e innovación, 4) capacitación y concientización y 5) cooperación internacional, y finalmente presentar una propuesta de solución que permita superar la problemática planteada en el presente trabajo.

Considerando las preguntas establecidas en el planteamiento del problema y luego de la investigación efectuada, se concluye que en la normativa argentina analizada desde el año 2011 al año 2019 y a pesar de haber una repetición de conceptos y una sobrerregulación de la temática, no se establece explícitamente qué organismo es responsable de identificar las

[88] Traducción del inglés “Ningún hombre es una isla, entero de sí mismo; cada hombre es un trozo de continente, una parte del principal” de John Donne (Poem Hunter, 2003).

infraestructuras críticas de la información en Argentina a pesar de señalar, en diferentes ocasiones, la importancia de dicha identificación. Asimismo, se concluye que en el Sistema de Gestión Integral no se hace referencia a ningún registro, inventario y/o catálogo que contenga la información crítica de las infraestructuras identificadas ni qué organismo debiera actualizar dicho registro. En contraposición, en el Sistema de Defensa Nacional y mediante la Política de Ciberdefensa (Resolución N° 1380/2019), se estableció que los Entes Reguladores debían elaborar el catálogo de infraestructuras críticas del sector estratégico pero no se observa el concepto de actualizarlo. Finalmente, a lo largo de los nueve años analizados no se encontró el objetivo ni la creación de un sistema nacional institucional cuyo principal objetivo sea la protección de las IC a pesar de que Argentina cuenta con variados sistemas que articulan diferentes organismos, órganos y elementos. Asimismo, no es posible encontrar en los nueve años analizados, acciones concretas que hayan materializado los objetivos y acciones de los distintos sistemas institucionales analizados y que se relacionan con dichas infraestructuras. Considerando esto y a pesar de tener una Estrategia Nacional de Ciberseguridad, no fue posible individualizar el plan (o planes) que permitan cumplir con el octavo objetivo relacionado con la protección de las IC.

En el marco de dichos hallazgos y a sabiendas de la necesidad de avanzar en la solución al problema, en el presente trabajo final de maestría se estableció la importancia de trabajar de forma mancomunada y desarrollar un Sistema de Protección de las Infraestructuras Críticas de la Información, de carácter interagencial, que permita ser el puntapié para el amparo de dichas infraestructuras y que, a la vez, esté compuesto por órganos y entidades de la APN y del sector privado. Dicho sistema debiera tener como principal meta el cumplimiento del octavo objetivo de la Estrategia Nacional de Ciberseguridad y estar encabezado por un organismo cuyas funciones se relacionen con el impulso, coordinación y supervisión de aquellas actividades relacionadas con la instancia previa a la protección de IC en el territorio nacional.

Esta agencia de creación propia, la Agencia Federal de Protección de las Infraestructuras Críticas, será quien encabece el Sistema y permita materializar aquellas acciones, objetivos y planes rescatables de los nueve años analizados y diversificados a lo ancho de la APN bajo una sola perspectiva y en un único organismo federal que cumpla con todas las necesidades, así como mejorar, con las lecciones aprendidas, aquello que se realizó y ejecutar lo que quedó pendiente. Sería el responsable de la identificación, registro y catálogo de los activos

de las IC, quien impulsará la coordinación y cooperación entre los sectores públicos, privados y organismos internacionales además de promover la cooperación con los distintos sectores y actores para ampliar, mejorar y fortalecer conjuntamente las capacidades y mecanismos de prevención, detección, análisis, respuesta y recuperación frente a los riesgos de seguridad que atenten contra las IC nacionales. Asimismo, como se sostiene en el epígrafe y a lo largo del trabajo final de maestría, el ser humano no debe hacer las cosas de forma aislada sino más bien, trabajar mancomunadamente para mejorar continuamente. Lo mismo ocurre en materia de ciberseguridad y la protección de las IC.

Además, a raíz de los hallazgos en el presente trabajo final de maestría, se establecen los objetivos a cumplir de las cinco direcciones generales que componen a la Agencia en cuestión y se puntualiza en las acciones que debieran cumplir para avanzar en la solución del problema planteado: la carencia de un único organismo que ampare las IC nacionales de Argentina y sea el responsable de la identificación, del registro y catálogo de los activos críticos. Inclusive, será dicha Agencia y las direcciones que la componen los responsables del desarrollo de políticas nacionales, políticas particulares, normas y procedimientos, planes estratégicos y de acción que gocen de coherencia interna al momento de regular la temática de la ciberseguridad, sean cohesivos entre sí, posean implicancias interagenciales y la capacidad de perpetuarse en el tiempo, transversales al sector público y privado, invitando al ámbito académico e investigativo a participar de dicha iniciativa.

Lo desarrollado intenta ser un aporte y guía inicial que recupera lo aprendido del año 2011 al año 2019 y plasma las falencias normativas encontradas para crear por ley nacional, una agencia federal que forme parte de la organización nacional en niveles estratégicos aplicable a los altos mandos, que encabece el Sistema de Protección de las Infraestructuras Críticas Nacionales en la Argentina (hoy inexistente), tomando lo propio y el modelo español como norte, para dirigir los esfuerzos hacia el resguardo de los valores de nuestro país y las IC. Además, el presente trabajo final de maestría propone herramientas con miras al futuro de una Nación que debe insertarse en el ámbito internacional, potenciándola geopolíticamente, en un mundo interdependiente e interconectado que exige la gestión de las IC.

De lo expuesto en el presente trabajo final de maestría se desprende, como líneas futuras de investigación y posibles acciones, la elaboración de la Estrategia Federal de Protección de las Infraestructuras Críticas y su respectivo plan lo cual deberá marcar el rumbo de la temática brindando objetivos y acciones concretas para la Agencia. Asimismo, se nombraron

una serie de documentos que deben ser considerados para iniciar en la confección de los mismos como el Plan Federal para la Identificación de las Infraestructuras Críticas Nacionales, el Plan Federal de Cooperación Multisectorial Público-Privado, el Plan Federal de Investigación, Desarrollo e Innovación en Ciberseguridad para la Protección de las Infraestructuras Críticas, el Plan Federal de Capacitación y Concientización de los Operadores Críticos, diseñar el Plan de Seguridad de los Operadores (organismos o empresas declaradas como IC) que contemple el seguimiento, control y actualización de los planes de seguridad y de contingencia de cada operador, acorde a la experiencia y conocimiento; y el diseño de los Planes Estratégicos Sectoriales que deberán formularse para cada sector y a partir de la identificación de las IC. Considerando la capacitación y concientización, queda pendiente el análisis de aquellas que se efectuaron en los diferentes Sistemas Institucionales y evaluar la posibilidad de extender estos mismos a otros sectores de la APN y a los operadores de las IC de la información que deban defender las mismas. De igual manera, resta resolver la articulación de la nómina de expertos y técnicos que trabajaría para la Agencia y la ubicación en el organigrama del área técnica y sus funciones dentro del organismo creado. Además, permanece en suspenso el desarrollo de métodos y mecanismos para que haya una real articulación entre los distintos organismos pertenecientes al Sistema de Seguridad Interior, el Sistema de Inteligencia Nacional, el Sistema de Defensa Nacional y el Sistema de Gestión Integral, y otros organismos que se relacionen con la protección de las infraestructuras críticas de la información y la ciberseguridad en Argentina. Sobre todo, queda pendiente profundizar en la labor que debieran realizar conjuntamente el Sistema de Seguridad Interior y el Sistema de Defensa Nacional - en particular el área de la ciberdefensa - en el marco de la protección de las IC y la creación de la Agencia, dadas las limitaciones legislativas a favor de prevenir y responder frente a un ciberataque y considerando, en especial, el origen, impacto y modo de afectación del mismo. Considerando el *NCSI*, sería interesante efectuar un estudio sobre los distintos índices e indicadores internacionales en materia de ciberseguridad que permita ahondar en el estado de la protección de las infraestructuras críticas nacionales y examinar las posibles medidas a tomar para mejorar la situación en Argentina. Por otra parte, con base en el análisis de España, queda pendiente el análisis de los distintos documentos e instrumentos creados en dicho país a través de la Ley 8/2011 y el Decreto Real 704/2011 (como la Estrategia Nacional de Protección de las Infraestructuras Críticas o el Plan Nacional de Protección de las Infraestructuras Críticas, entre otros) como puntapié para avanzar en los documentos que nuestro país debiera realizar

y ejecutar. Asimismo, queda pendiente el análisis de derecho comparado de otros países que pudieran servir de referencia para mejorar y situar a la Argentina en el plano internacional en pos de la protección de las IC.

En síntesis, Argentina se encuentra ante una oportunidad única. Si bien se cometieron errores en el pasado, existe la intención y la capacidad para remediarlos y construir a partir de una serie de recursos rescatados. Estos cimientos permitirán fortalecer las capacidades y relaciones entre las instituciones gubernamentales (sector público) y las organizaciones del sector privado, con el fin ulterior de prevenir y disminuir la probabilidad de que cualquier incidente de seguridad afecte la continuidad de servicios vitales que pertenecen a los sectores identificados como energía, tecnologías de información y comunicaciones, salud, entre otros. La resiliencia, la prevención y la reacción son los pilares fundacionales de este trabajo.

La proliferación de la tecnología, sus riesgos y las ciberamenazas requieren de una Nación que acompañe los avances, la evolución y el aprendizaje de los errores cometidos, pudiendo lograrse mediante la sanción de una ley que cree una estructura organizativa con una misión, visión y funciones que sean el norte de la protección de las infraestructuras críticas argentinas, bajo la conducción directa del presidente democráticamente electo, a favor de velar por los servicios que son esenciales para la sociedad.

8. Referencias bibliográficas

Arroyo Arzubi, C. (Noviembre de 2004). La Producción para la Defensa en la República Argentina. Buenos Aires, Argentina: I.E.E.R.I, Congreso de la Nación Argentina, Circulo de Legisladores. Obtenido de http://www.ieeri.com.ar/actividades/docs/act%20-%20vii%20encuentro%20-%20la%20producci%D3n%20para%20la%20defensa%20en%20la%20rep%DAblica%20argentina.pdf

Baretto, L. (2011). El Poder Legislativo como objeto de estudio de la Política Exterior argentina. *IV Jornadas de Investigación en Humanidades* (págs. 71-75). Bahía Blanca: Universidad Nacional del Sur.

Bertranou, J. (2013). Creació de agencias especializadas, capacidad estatal y coordinación interinstitucional. Análisis del caos de la Agencia Nacional de Seguridad Vial de Argentina. *Revista Perspectivas de Políticas Públicas*, 11-39.

Cancillería Argentina. (23 de Febrero de 2017). Memorando de Entendimiento sobre Cooperación en materia de Ciberseguridad entre el Ministerio de Modernización de la República Argentina y el Ministerio de Energía, Turismo y Agenda Digitall del Reino de España. Madrid, España. Obtenido de https://tratados.cancilleria.gob.ar/tratado_archivo.php?tratados_id=kqSpmpo=&tipo=kg==&id=kp6jnZU=&caso=pdf

Carey, J. (2006). Presidencialismo versus Parlamentarismo. *Posdata*, 121-161.

Casarino, P., & Ortiz, J. (2019). La Ciberdefensa y la Ciberinteligencia Militar. *Ciberespacio n° 21*, 43-52.

Centro de Implementación de Políticas Púbicas para la Equidad y el Crecimiento. (2003). *El Poder Legislativo Nacional.* Buenos Aires: CIPPEC.

COMPTIA. (2020). *Comptia*. Obtenido de https://www.comptia.org/content/research/it-industry-trends-analysis

Constitución Nacional Argentina. (15 de Diciembre de 1994). Ley N° 24.430. Buenos Aires, Argentina: Infoleg.

Cornaglia, S., & Vercelli, A. (2017). La Ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad N°20*, 46-62. doi:http://dx.doi.org/10.17141/urvio.20.2017.2601

Council of Europe. (23 de Noviembre de 2001). Convention on Cybercrime. Budapest. Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Decisión Administrativa N° 103. (20 de Febrero de 2019). Boletín Oficial 20/02/2019. Ciudad de Buenos Aires, Argentina: Secretaría de Gobierno de Modernización.

Decisión Administrativa N° 15. (4 de Marzo de 2015). Boletín Oficial 04/03/2015. Buenos Aires, Argentina: Ministerio de Defensa.

Decisión Administrativa N° 232. (29 de Marzo de 2016). *Boletín Oficial 29/03/2016*. Buenos Aires, Argentina: Ministerio de Modernización.

Decisión Administrativa N° 297. (09 de Marzo de 2018). Boletín Oficial 09/03/2018. Ciudad de Buenos Aires: Ministerio de Modernización.

Decisión Administrativa N° 546. (30 de Mayo de 2016). *Boletín Oficial 30/05/2016*. Buenos Aires, Argentina.

Decreto N° 1067. (10 de Junio de 2015). Boletín Oficial 10/06/2015. Buenos Aires, Argentina: Administración Pública Nacional.

Decreto N° 13. (10 de Diciembre de 2015). Boletín Oficial 10/12/2015. Buenos Aires, Argentina: Presidente de la Nación Argentina.

Decreto N° 1311. (06 de Julio de 2015). Boletín Oficial 06/07/2015. Buenos Aires, Argentina.

Decreto N° 174. (02 de Marzo de 2018). Boletín Oficial 02/03/2018. Ciudad de Buenos Aires, Argentina: Presidente de la Nación.

Decreto N° 2645. (30 de Diciembre de 2014). Boletín Oficial 30/12/2014. Buenos Aires, Argentina: Ministerio de Defensa.

Decreto N° 42. (07 de Enero de 2016). Boletín Oficial 07/01/2016. Buenos Aires, Argentina: Presidente de la Nación.

Decreto N° 480. (11 de Julio de 2019). Boletín Oficial 11/7/2019. Ciudad de Buenos Aires, Argentina.

Decreto N° 577. (28 de Julio de 2017). Boletín Oficial 28/07/20177. Ciudad de Buenos Aires, Argentina: Poder Ejecutivo Nacional.

Decreto N° 684. (03 de Octubre de 2019). Boletín Oficial 03/10/2019. Buenos Aires, Argentina: Administración Nacional.

Decreto N° 703 . (30 de Julio de 2018). Boletín Oficial 30/07/2018. Ciudad de Buenos Aires, Argentina.

Decreto N° 802. (5 de Septiembre de 2018). Boletín Oficial 05/9/2018. Ciudad de Buenos Aires, Argentina.

Decreto N° 898. (27 de Julio de 2016). Boletín Oficial 27/07/2016. Ciudad de Buenos Aires, Argentina: Administración Pública Nacional.

Directiva 2008/114/CE del Consejo de la Unión Europea. (08 de Diciembre de 2008). Diario Oficial de la Unión Europea 08/12/2008. Obtenido de https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Disparte, D., & Furlow, C. (16 de Mayo de 2017). La mejor inversión en ciberseguridad que puede realizar es una mejor formación. *Harvard Business Review*. Obtenido de

https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Disposición N° 2. (08 de Agosto de 2013). Boletín Oficial 08/08/2013. Buenos Aires, Argentina: Jefatura de Gabinete de MInistros - Secretaría de Gabinete y Coordinación Administrativa - Subsecretaría de Tecnologías de Gestión - Oficina Nacional de Tecnologías de Información.

Disposición N° 3. (16 de Septiembre de 2011). Boletín Oficial 16/09/2011. Buenos Aires, Argentina: Jefatura de Gabinete de ministros - Secretaría de Gabinete - Subsecretaría de Tecnologías de Gestión - Oficina Nacional de Tecnologías de Información.

Domínguez Bascoy, J. (2015). La ciberseguridad: aspectos jurídicos internacionales. *Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteizko*, 161-224.

DPI Cuántico. (26 de Abril de 2018). Memorandum de Entendimiento sobre cooperación en materia de ciberseguridad, ciberdelito y ciberdefensa entre la República Argentina y la República de Chile. Buenos Aires, Argentina. Obtenido de https://dpicuantico.com/sitio/wp-content/uploads/2018/09/Normativa-Suple-Derecho-Internacional.pdf

Durante, A., & Bestard, A. (2010). El principio de la División de Poderes en la Argentina Actual. *Derecho UBA*. Obtenido de http://www.derecho.uba.ar/investigacion/investigadores/publicaciones/bestard-el-principio-de-la-division-de-poderes-en-la-argentina-actual.pdf

Fadol, Y., & Sandhu, M. (2013). The role of trust on the performance of strategic alliances in a cross-cultural context: A study of the UAE. *Benchmarking An International Journal*, 106-128.

Fuentes Pujol, E., & Aguimbau Vivó, L. (2008). I+D+I: Una Perspectiva Documental. *Anales de Documentación n°11*, 43-56.

Galindo Sierra, F. (2016). *Protección de Infraestructuras Críticas: un análisis de derecho comparado.* Málaga: Facultad de Derecho - Universidad de Málaga.

García Zaballos, A., & Jeun, I. (2016). *Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Cribbean and Selected Countries.* Washington, DC: Inter-American Development Bank (IDB) and Korea Internet & Security Agency (KISA).

Gartner. (15 de Mayo de 2020). *www.gartner.com*. Obtenido de https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Gelli, M. A. (2011). *Constitución de la Nación Argentina: Comentada y Concordada* (4ta edición ampliada y actualizada ed.). Buenos Aires: La Ley.

Global Forum on Cyber Expertise - Meridian. (2016). *La Guía de Buenas Prácticas GFCE-MERIDIAN en Protección de Infraestructuras Críticas de Información para desarrolladores de políticas gubernamentales.*

Gordillo, A. (2013). Tomo 8: Teoría General de Derecho Administrativo, Capitulo VI: Entes Públicos. En A. A. Gordillo, *Tratado de Derecho Administrativo* (págs. 185-188). Obtenido de https://www.gordillo.com/pdf_tomo8/capitulo06.pdf

Gordillo, A. (2013). *Tratado de derecho administrativo, Tomo 1 - Parte General* (11a edición ed.). Buenos Aires: F.D.A. Obtenido de https://www.gordillo.com/tomo1.php

Institute for Information Infrastructure Protection - I3P. (2003). *Cyber Security Research and Development Agenda.*

Juan Carlos I, Jefatura del Estado. (Abril de 2011). Ley 8/2011. *Boletín Oficial Español*. Obtenido de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Kelsen, H. (2010). *Teoría Pura del Derecho.* Buenos Aires: Eudeba.

Ley N° 23.544. (13 de 04 de 1988). Boletín Oficial 13/04/1988. Argentina.

Ley N° 24.156. (26 de Octubre de 1992). Boletín Oficial 26/10/1992. Buenos Aires, Argentina.

Ley N° 27.126. (03 de Marzo de 2015). Boletín Oficial 03/03/2015. Ciudad Autónoma de Buenos Aires, Argentina.

Marienhoff, M. (1995). *Tratado de Derecho Administrativo: Tomo I.* Buenos Aires: Abeledo Perrot.

Mercosur. (8 de Junio de 2018). *Mercosur*. Obtenido de https://www.mercosur.int/quienes-somos/en-pocas-palabras/

Ministerio de Defensa - Presidencia de la Nación. (2019). *Modelo Argentino de Modernización del Sistema de Defensa.* Obtenido de https://www.infodefensa.com/wp-content/uploads/ModeloArgentinodeModernizaci%C3%B3ndelSistemadeDefensa.pdf

Naciones Unidas. (2019). *World Economic Situation and Prospects.* Obtenido de https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESP2019_BOOK-ANNEX-en.pdf

National Cyber Security Index. (10 de 09 de 2021). *NCSI - Data collection*. Obtenido de https://ncsi.ega.ee/data-collection/

OEA. (2016). *Buenas Prácticas para establecer un CSIRT nacional.* Washington: Secretaría General de la Organización de los Estados Americanos (OEA). Obtenido de https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

O'Rourke, T. (2007). *Critical Infrastructure, Interdependencies, and Resilience.* The Bridge.

Oszlak, O., Malvicino, G., & Ouviña, H. (2001). Estudio de los Organismos Descentralizados del Poder Ejecutivo Nacional: Informe Final. *UNPRE*.

Parodi, C. (2016). El sistema presidencial argentino: bases para la innovación institucional en el siglo XXI. *Perspectivas de las Ciencias Económicas y Jurídicas - Facultad de Ciencias Económicas y Jurídicas de la UNLPam*, 61-82.

Poem Hunter. (3 de Enero de 2003). *Poem Hunter*. Obtenido de https://www.poemhunter.com/poem/no-man-is-an-island/

Postigo de Bedia, A., & Díaz de Martínez, L. (2006). *Diccionario de Términos de la Administración Pública.* Buenos Aires: Dunken.

Presidencia del Gobierno - Departamento de Seguridad Nacional. (2019). *Estrategia Nacional de Ciberseguridad.* España: Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad - Gobierno de España. Recuperado el 2019

Public Safety Canada. (Marzo de 2014). Critical 5: Forging a Common Understanding for Critical Infrastructure. Obtenido de https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

Real Decreto N° 704. (21 de Mayo de 2011). Boletín Oficial del Estado 21/05/2011. España. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

Resolución N° 1046. (20 de Agosto de 2015). Boletín Oficial 20/08/2015. Buenos Aires, Argentina: Jefatura de Gabinete de Ministros.

Resolución N° 1107-E. (12 de Octubre de 2017). Boletín Oficial 12/10/2017. Ciudad de Buenos Aires, Argentina: Ministerio de Seguridad.

Resolución N° 1380. (25 de Octubre de 2019). Boletín Oficial 25/10/2019. Ciudad de Buenos Aires, Argentina: Ministerio de Defensa.

Resolución N° 1523. (12 de Septiembre de 2019). Boletín Oficial 12/09/2019. Ciudad de Buenos Aires, Argentina: Secretaría de Gobierno de Modernización - Jefatura de Gabinete de Ministros.

Resolución N° 319. (29 de Mayo de 2008). Boletín Oficial 29/05/2008. Buenos Aires, Argentina: Ministerio de Ciencia, Tecnología e Innovación Productiva. Obtenido de https://www.argentina.gob.ar/sites/default/files/resol_mincyt_319_08.pdf

Resolución N° 490 - E/2016. (16 de Noviembre de 2016). Boletín Oficial 16/11/2016. Buenos Aires, Argentina: Ministerio de Modernización.

Resolución N° 580. (28 de Julio de 2011). Boletín Oficial 28/7/2011. Buenos Aires, Argentina: Jefatura de Gabinete de Ministros.

Resolución N° 580. (04 de 09 de 2018). Boletín Oficial 04/09/2018. Ciudad de Buenos Aires, Argentina: Ministerio de Modernización.

Resolución N° 829. (24 de Mayo de 2019). Boletín Oficial 24/05/2019. Ciudad de Buenos Aires, Argentina: Jefatura de Gabinete de Ministros - Secretaría de Gobierno de Modernización.

Rikk, R. (2018). *National Cyber Security Index 2018.* Tallin, Estonia: Estonia Development Cooperation. Recuperado el 2019, de https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies.* USA: IEEE Control System Magazine.

Rubio, J. (2017). Organismos descentralizados en el Estado nacional: ¿administración centralizada por otros medios? *CIPPEC*.

Sánchez Gómez, F. (2014). Protección de Infraestructuras Críticas en España: Marco Regulatorio y Organizativo. *Seguridad y Ciudadanía - Revista del Ministerio del Interior*, 19-73.

Subsecretaría de Ciberdefensa - Ministerio de Defensa - Presidencia de la Nación. (s.f.). *Ciberseguridad en el Sector Público.* ITU.

Taverna, A. (2020). I+D+i en ciberseguridad = prevención y resiliencia de las infraestructuras críticas. *Proceedings of the 2020 IEEE Biennal Congress of Argentina - IEEE ARGENCON 2020, in press*.

Taverna, A., & Cárdenas Holik, R. (2020). Sistema de Protección de Infraestructuras Críticas de la República Argentina: Ciberinteligencia para la toma de decisiones. *Triarius, Volumen 4 - n° 76*, 18-27.

Tessari, P., & Muti, K. (2021). Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations. *DIRECTORATE-GENERAL FOR EXTERNAL POLICIES, POLICY DEPARTMENT*.

Torré, A. (2003). *Introducción al derecho* (14a edición ed.). Buenos Aires: Abeledo Perrot.

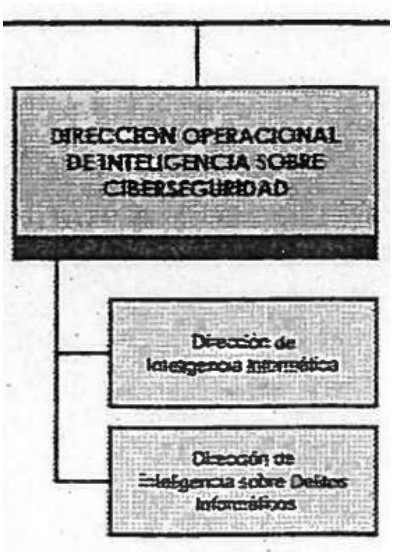
Villamizar, C. (2018). *Estudio sobre Protección de Infraestructuras Críticas en caso de desastre natural.* Junta Interamericana de Defensa - Secretaría de la JID. Obtenido de http://scm.oas.org/pdfs/2018/CP39205SINFORME.pdf

ZAGREB - Consultores Limitada. (Diciembre de 2008). *Informe Final: Estudio para la definición e identificación de infraestructuras críticas de la información en Chile.* Chile: ZAGREB.

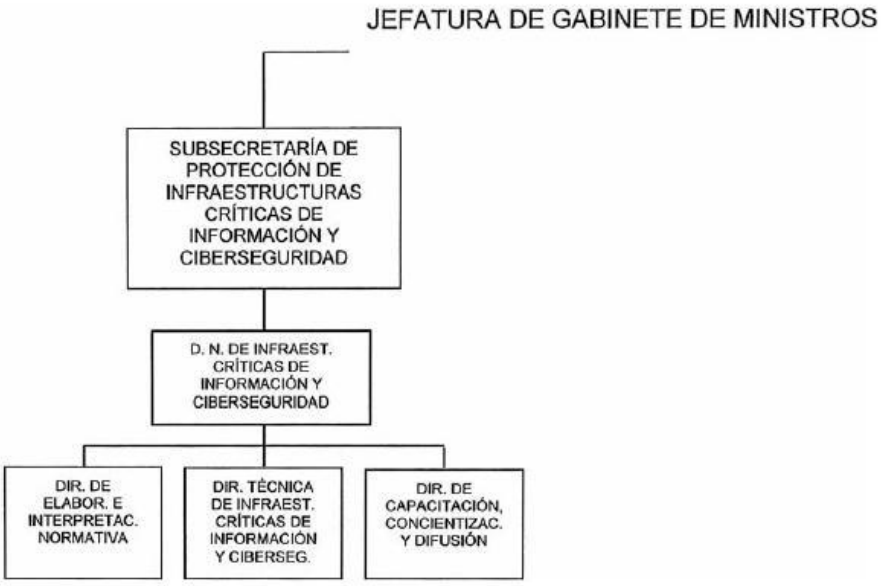
9. Anexos

Se muestran a continuación una serie de Capturas de los plexos normativos en los que en su contenido figuran organigramas que por su diseño tuvieron que ser adaptados para ser presentados de manera clara y prolija.

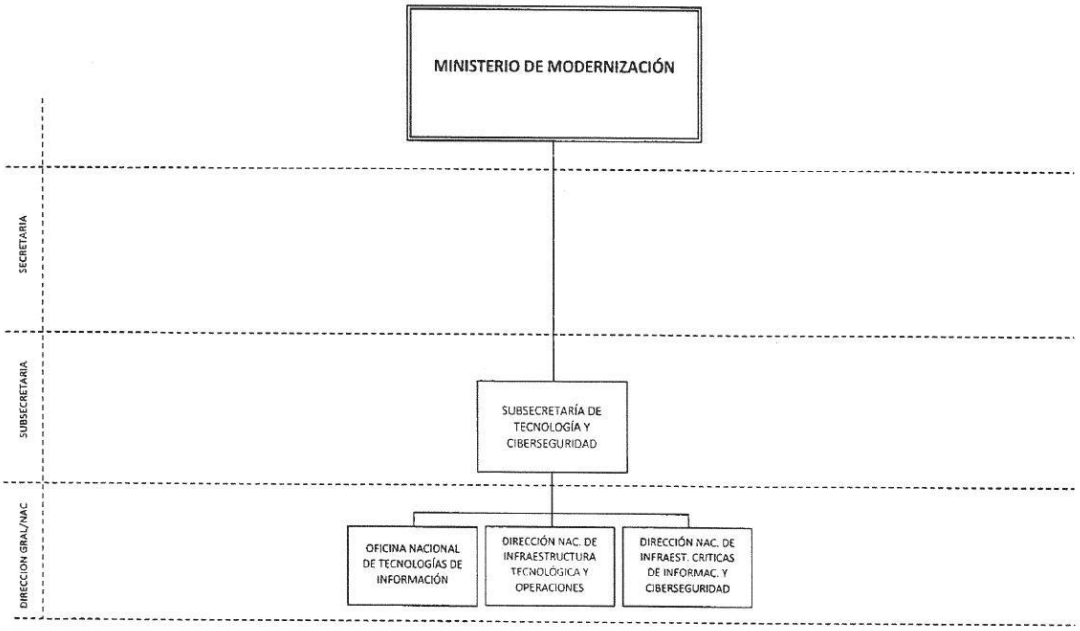
Captura 1



Captura 2

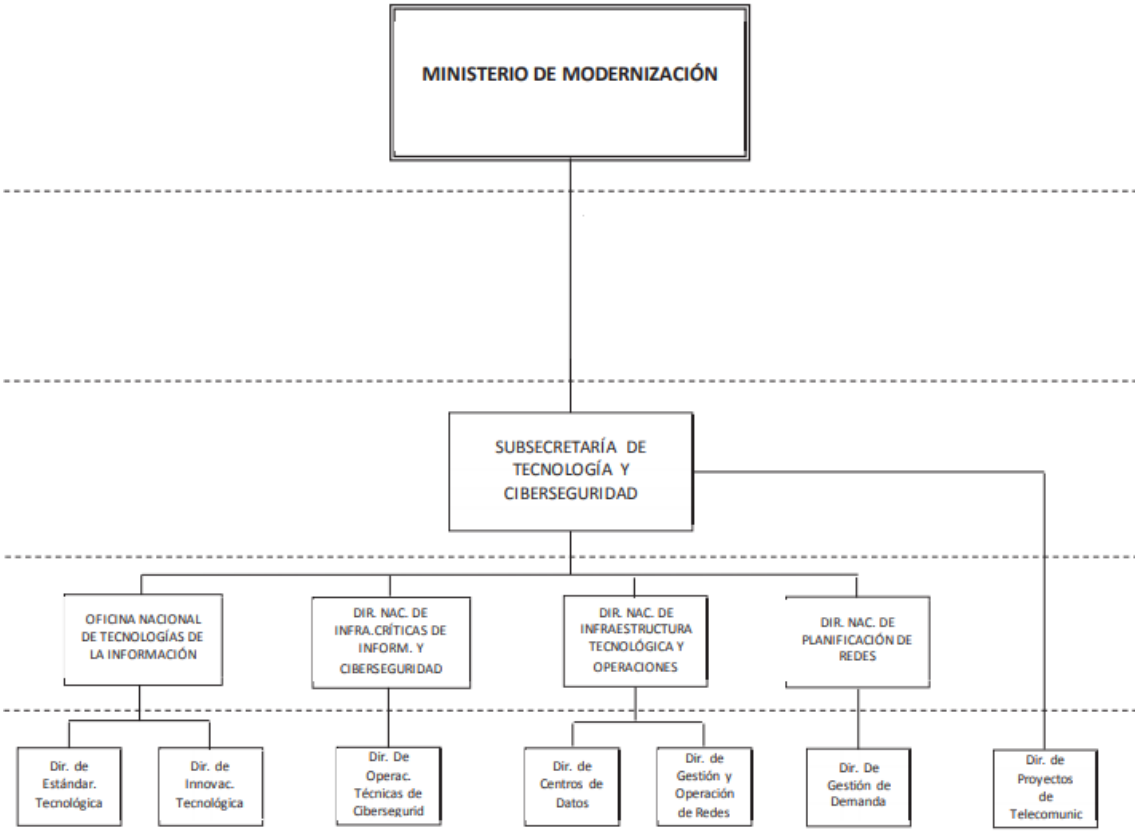


Captura 3

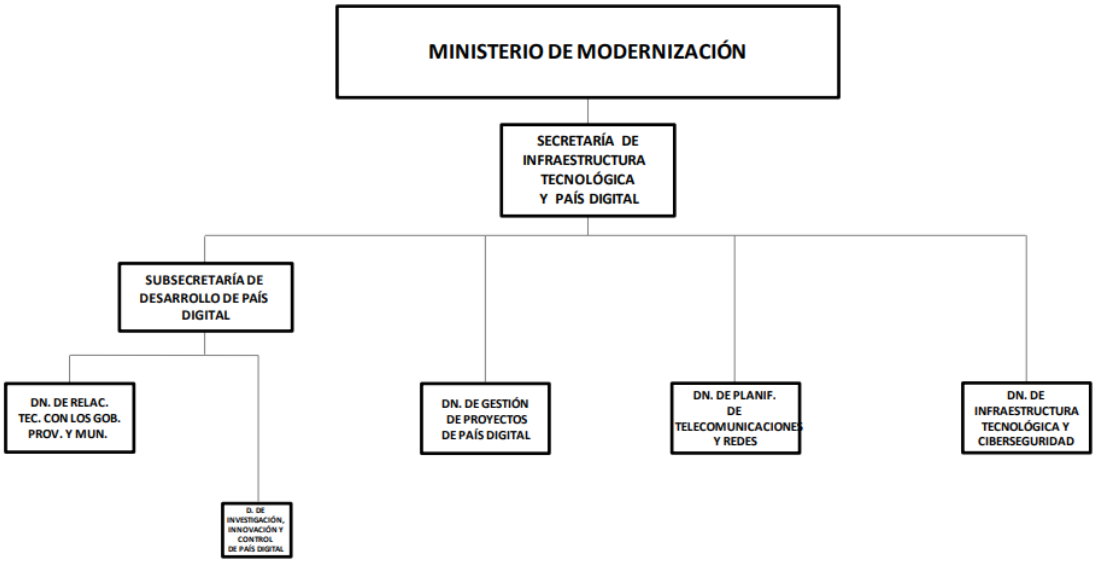


Captura 4

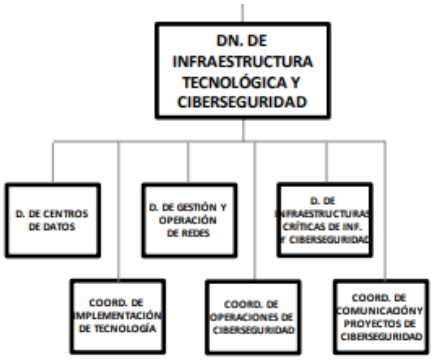
Captura 5



Captura 6



Captura 7



Captura 8