ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TITULO: La incumbencia de la ciberdefensa en la protección de las infraestructuras criticas en el nivel operacional.

AUTOR: MY (EA) Luis Andrés Fidalgo

TUTOR: CR (EA) Santiago Augusto PICÓN

AÑO: 2024

RESUMEN

En Argentina, la ciberdefensa como parte de la defensa es fundamental para la protección de las infraestructuras críticas y las comunicaciones estratégicas del país. La Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa, y el Comando Conjunto de Ciberdefensa perteneciente al Estado Mayor Conjunto de las Fuerzas Armadas, coordinan las actividades de protección de los sistemas y redes militares.

Se abordará el concepto de ataque como la materialización de amenazas contra infraestructura critica, explorando la problemática de la atribución, el marco legal aplicable y la capacidad de reacción adecuada, aspectos que resultan cruciales dentro de una estrategia defensiva establecida en la Directiva de Política de Defensa Nacional y la reglamentación conjunta vigente. En este contexto, se analizarán los alcances de la ciberdefensa en el marco de las políticas de defensa y su rol en el cumplimiento de las leyes para la protección de infraestructuras críticas a nivel operacional, enfatizando la importancia de una respuesta normativa y operativa coordinada frente a ciberamenazas.

En este sentido nos adentraremos en analizar la incumbencia de la ciberdefensa, en la protección de las infraestructuras críticas a nivel operacional, analizando la normativa vigente y los desafíos que enfrenta la ciberdefensa en Argentina.

Se estudiarán las definiciones aceptadas de sus partes constitutivas en la Defensa Nacional con su marco normativo investigando incumbencias, restricciones e interpretaciones del nivel estratégico nacional, el nivel operacional y el ciberespacio con las características que lo definen y sus implicancias.

Con los conceptos centrales ya definidos, el desarrollo se enfocará en analizar la determinación de las infraestructuras críticas y el rol que cumple la ciberdefensa en su identificación y protección. Además, se examinará el papel de las agencias de ciberdefensa en la identificación de vulnerabilidades. Este análisis se complementa con una evaluación de los riesgos y amenazas cibernéticas actuales, incluyendo un estudio de casos relevantes de ciberataques a infraestructuras críticas, para enriquecer la perspectiva y contextualizar las necesidades de protección en Argentina.

PALABRAS CLAVES

Ciberdefensa, infraestructura crítica, objetivo de valor estratégico.

Índice

INTRODUCCIÓN

En el contexto actual, la creciente digitalización global ha generado un entorno de alta vulnerabilidad para los Estados. El uso de las Tecnologías de la Información y la Comunicación (TIC) no solo ha permitido una mayor interconexión y modernización de infraestructuras críticas en sectores como la energía, el transporte, las telecomunicaciones y el sistema financiero, sino que también ha expuesto a las naciones a nuevos tipos de amenazas: los ataques cibernéticos. Estos ataques pueden variar desde la interrupción de servicios esenciales hasta la inteligencia, la filtración de información clasificada o el sabotaje de sistemas militares y/o gubernamentales. La ciberdefensa, por lo tanto, ha pasado a ocupar un lugar preeminente en las estrategias de Defensa Nacional (Intini, 2020).

En la República Argentina, la ciberdefensa todavía se encuentra en pleno desarrollo necesario para enfrentar eficazmente las ciberamenazas que pueden afectar tanto al sector público como al privado. A pesar de los avances recientes, como la creación del Comando Conjunto de Ciberdefensa, Instituto de Ciberdefensa de las Fuerzas Armadas y otras medidas de ciberseguridad adoptadas por el Estado, existen múltiples desafíos que limitan la efectividad de estas iniciativas. Entre ellos se destacan la carencia de una normativa colaborativa y cooperativa que integre y regule las acciones de ciberdefensa y ciberseguridad, el escaso marco doctrinal consolidado en el ámbito militar y la escasa coordinación interinstitucional entre los distintos organismos encargados de la defensa, seguridad nacional y desarrollo cibernético.

Con el auge de los ataques cibernéticos cada vez más sofisticados, la ciberdefensa se ha convertido en una necesidad global. Incidentes como el ataque a Estonia en 2007 y la operación Stuxnet en 2010 han demostraron la vulnerabilidad de las redes y la necesidad de una respuesta para proteger las infraestructuras críticas (Wall, 2011); (Ottis, 2007).

El término "ciberdefensa" comenzó a ganar prominencia a finales del siglo XX y principios del XXI, a medida que los ataques cibernéticos se hacían más sofisticados y generalizados. Incidentes notables, como el ataque cibernético a Estonia en 2007 y la operación Stuxnet en 2010, destacaron la importancia crítica de proteger infraestructuras críticas y redes de comunicación contra amenazas cibernéticas.

En respuesta a estos desafíos, países miembros de la OTAN empezaron a establecer estrategias nacionales de ciberseguridad y desarrollar capacidades específicas de ciberdefensa. Esto incluye la creación de unidades especializadas, centros de operaciones de seguridad cibernética y la promulgación de leyes y políticas para regular el uso seguro de las tecnologías

de la información y comunicación y proteger la infraestructura nacional contra ataques digitales (Ottis, 2007); (Wall, 2011).

Así, La ciberdefensa, entendida como el conjunto de medidas destinadas a proteger las infraestructuras críticas, las redes informáticas y las operaciones estratégicas de un Estado ante amenazas provenientes del ciberespacio, ha adquirido una relevancia indiscutible en el ámbito de la seguridad nacional (Resolución N° 829, 2019). En el caso de la República Argentina, la Defensa Nacional enfrenta nuevos desafíos que demandan la integración de estrategias de ciberdefensa de forma urgente y efectiva, dada la creciente interdependencia de las infraestructuras críticas del país con las Tecnologías de la Información y la Comunicación (TIC) (Resolución N° 1380/2019).

En tal sentido se han realizado estudios e investigaciones que son afines y abarcan el tema a tratar, que aborda la importancia de la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información, dado que el ciberespacio se ha convertido en un nuevo campo de batalla y la Argentina necesita ponerse al día en el desarrollo de infraestructuras y tecnologías (Agostina Taverna, 2021).

Asimismo, Di Cézare (Niss, 2023) explora la compleja relación entre la soberanía de los Estados y el ciberespacio, enfatizando la necesidad de un marco propio de análisis. Di Cézare argumenta que la realidad material del ciberespacio, incluyendo hardware, software y cables submarinos, afecta la soberanía nacional. El autor critica la dependencia de las naciones en tecnologías dominadas por empresas privadas que a menudo responden a intereses gubernamentales extranjeros. Di Cézare destaca la necesidad de que Argentina, a través de la Red federal de fibra óptica (REFEFO), Empresa Argentina de Soluciones Satelitales S.A (ARSAT) y el desarrollo de tecnologías propias como Yarará y Coral, se fortalezca en el ámbito cibernético para garantizar su soberanía.

Por otra parte, Cornaglia y Vercelli (Niss, 2023), analizan a la ciberdefensa en Argentina entre 2006 y 2015, se analizan las normas producidas por el Ministerio de Defensa y la Jefatura de Gabinete de ministros, las cuales buscaban sistematizar la legislación en materia de ciberdefensa y generar información para la creación de políticas públicas. Los autores concluyen que, a pesar del aumento de la normativa específica, la legislación argentina aún no tiene una codificación general sobre ciberdefensa, y que la cooperación interestatal es crucial para su desarrollo. La investigación destaca la importancia del concepto de "legítima defensa" y la necesidad de un marco jurídico que regule el sector público y privado en relación a la ciberdefensa.

El trabajo de Casale (Casale, 2022), analiza el rol de la ciberdefensa en el contexto del componente terrestre. El trabajo investiga el marco legal argentino y las amenazas que enfrenta la ciberdefensa, para luego establecer un proceso de trabajo y un elemento que pueda ejecutarlo dentro del teatro de operaciones terrestre, considerando la formación y equipamiento necesario. El estudio se basa en la doctrina nacional e internacional, y destaca la necesidad de un enfoque multidisciplinario y la actualización constante del marco legal para responder a la evolución tecnológica del ciberespacio.

El artículo, desarrollado por Fonseca, Perdomo, Gratacos y Ortiz, el grupo de expertos independientes, explica cómo se podrían aplicar las normas del Derecho Internacional Humanitario (DIH) al ciberespacio, representando uno de los primeros esfuerzos por adaptar las leyes de conflicto armado a las realidades de los conflictos cibernéticos. Basándose en las opiniones de expertos como Jeimy Cano y María José Bejarano, los autores del articulo destacan cómo el ciberespacio ha emergido como un nuevo campo de batalla, en el que los ataques a infraestructuras críticas representan una amenaza asimétrica para la soberanía de los Estados (Revista ESG, 2014).

Los mismos mencionan que el aumento de ciberataques significativos, como los ocurridos en Estonia y Georgia, ha llevado a la OTAN adoptar políticas de ciberdefensa, creando organismos especializados y un plan de acción concreto en respuesta a estos ciberataques mediante la creación de instituciones como el Centro Técnico de Respuestas a Incidentes Informáticos (NCIRC) (Revista ESG, 2014).

Aunque el Manual de Tallin no constituye un tratado oficial, ofrece una guía fundamental para la aplicación del Derecho Internacional Humanitario en conflictos cibernéticos, adaptando las normativas existentes al ámbito del ciberespacio (Revista ESG, 2014).

Estos antecedentes de la ciberdefensa reflejan una evolución continua desde la protección de sistemas militares hasta la defensa integral de infraestructuras críticas en un mundo cada vez más digitalizado y conectado.

Actualmente la ciberdefensa ha cobrado una importancia central en la Defensa Nacional de la República Argentina, tiene una preponderancia especial en la guerra futura, siendo el "software o código" uno de los principales vectores para destruir o inutilizar un sistema informático, a diferencia del "hardware" cuando se trata de los sistemas tradicionales, particularmente en un contexto donde la digitalización global ha aumentado tanto las oportunidades como las amenazas que enfrentan los Estados (Niss, 2023). La creciente dependencia de infraestructuras críticas que operan en el ciberespacio, como las redes de

energía, telecomunicaciones, finanzas y defensa, expone al país a ciberamenazas que pueden comprometer su soberanía (Resolución N°1523 , 2019). La Directiva de Política de Defensa Nacional 2021, establecida por el Decreto 457/2021, establece que: *la misión de conjurar y repeler las amenazas de naturaleza militar estatal corresponde al Sistema de Defensa Nacional, según lo dispuesto por el artículo 2° de la citada Ley N° 23.554, reglamentado por el artículo 1° del Decreto N° 727/06.*

En el ámbito legislativo, Argentina ha avanzado en la creación de un marco normativo robusto que incluye la promulgación de leyes específicas como la Ley de Delitos Informáticos y la Ley de Protección de Datos Personales, estableciendo las bases para la protección de la información crítica y la persecución de los delitos cibernéticos. Además, la creación del Comité de Ciberseguridad (Decreto N° 577, 2017), modificado por el Decreto 480/2019, ha impulsado la formulación de una Estrategia Nacional de Ciberseguridad que busca coordinar acciones entre los sectores públicos y privados para prevenir y mitigar las ciberamenazas.

En este marco, se ha consolidado el Comando Conjunto de Ciberdefensa en el Estado Mayor Conjunto de las Fuerzas Armadas, el cual tiene la tarea de proteger las infraestructuras críticas estratégicas del país (PC11-01, 2023). Este comando se ha constituido como una estructura clave para detectar, prevenir y responder a ciberataques que puedan comprometer los sistemas de defensa y seguridad del Estado.

A pesar de los avances normativos y organizativos, Argentina aún enfrenta desafíos significativos en su capacidad de ciberdefensa. Uno de los principales retos es la dificultad para identificar de manera precisa la naturaleza del agresor en el ciberespacio, dada la capacidad de los atacantes para ocultar su identidad y orquestar ataques desde jurisdicciones extranjeras. Esta falta de atribución inmediata complica la posibilidad de una respuesta ágil y efectiva, como lo plantea el Manual de Tallin (2013), que aborda el marco jurídico internacional aplicable a la ciberguerra.

Además, la adaptación tecnológica sigue siendo un desafío crucial. A pesar de la creación de organismos como el Instituto de Ciberdefensa de las Fuerzas Armadas, que busca formar a personal especializado, la infraestructura tecnológica de defensa aún requiere modernización. El Estado necesita integrar plenamente la ciberdefensa dentro de la doctrina militar para enfrentar de manera eficiente las amenazas contemporáneas, en especial aquellas transnacionales que no respetan fronteras y que operan en un entorno sin límites geográficos claros.

Además, la adaptación tecnológica sigue siendo un desafío crucial. A pesar de la creación de organismos como el Instituto de Ciberdefensa de las Fuerzas Armadas, que busca

formar a personal especializado, la infraestructura tecnológica de defensa aún requiere modernización. El Estado necesita integrar plenamente la ciberdefensa dentro de la doctrina militar para enfrentar de manera eficiente las amenazas contemporáneas, en especial aquellas transnacionales que no respetan fronteras y que operan en un entorno sin límites geográficos claros.

El Plan Federal de Prevención de delitos tecnológicos y ciberdelitos (Resolución N° 75/2022), junto con resoluciones como Resolución N° 580/2011, establecen una prioridad clara en la protección de infraestructuras críticas en Argentina, reconociendo la vulnerabilidad de sectores estratégicos ante ciberataques. Estas políticas promueven la cooperación interinstitucional y público-privada para fortalecer la resiliencia de los sistemas críticos del país. Sin embargo, el nivel de colaboración entre los sectores gubernamentales, como el Ministerio de Defensa, la Secretaría de Inteligencia de Estado (SIDE) y otras entidades, aún necesita ser fortalecido para garantizar una respuesta integral y coordinada ante las ciberamenazas.

La ciberdefensa militar argentina se organiza principalmente desde el Nivel Estratégico Nacional a través de la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa, la cual coordina las actividades relacionadas con la protección de sistemas y redes de comunicación militar. Este organismo trabaja en estrecha colaboración con otros sectores del gobierno, como la Secretaria de Inteligencia de Estado (SIDE) y la Secretaría de Gobierno de Modernización, para asegurar una respuesta integral ante incidentes cibernéticos y fortalecer la resiliencia de las infraestructuras críticas, para luego a través del Comando Conjunto de la Fuerzas Armadas en el nivel estratégico operacional traducir las directivas e intenciones de nivel superior y generar las directivas necearías para la ejecución de las políticas de ciberdefensa y acciones de las niveles inferiores.

En resumen, el estado actual de la ciberdefensa en Argentina refleja importantes avances normativos y organizativos, como lo son, la creación del Instituto de Ciberdefensa de las fuerzas Armadas y la Subsecretaria de Ciberdefensa del Ministerio de Defensa, para la supervisión y coordinación dentro del sistema de Defensa Nacional, el Comando Conjunto de Ciberdefensa, para la implementación, ejecución y coordinación de las operaciones de ciberdefensa desarrolladas por las Fuerzas Armadas, y la formulación de un marco legal robusto, no obstante, el país enfrenta desafíos significativos que limitan su efectividad frente a las ciberamenazas complejas (ciberataque: dos, ransomware, ingeniería social, entre otros), y de la modernización tecnológica de sus infraestructuras críticas.

A partir este trabajo, se busca analizar la normativa y las capacidades actuales y evaluar las vulnerabilidades y proponer estrategias viables para mejorar la integración de la ciberdefensa en la doctrina militar y su coordinación con otros sectores clave. Estas propuestas contribuirán a fortalecer la planificación estratégica y la protección de infraestructuras críticas, garantizando que Argentina pueda enfrentar los crecientes desafíos del ciberespacio, tanto en tiempos de paz como en escenarios de conflicto.

El problema estudiado se planteó de la siguiente forma: determinar la participación, alcance y efectos desde el punto de vista de la ciberdefensa en la protección de las infraestructuras críticas en el nivel operacional mediante el interrogante de: ¿Qué incumbencia tiene la ciberdefensa a nivel operacional en la determinación de las infraestructuras críticas y la planificación de su defensa?

La presente investigación se limitó al estudio de la incumbencia, atribuciones y acciones de la ciberdefensa en el nivel operacional, según las leyes nacionales, normas y doctrina conjunta argentina.

Para al análisis y desarrollo del presente trabajo se tomó bibliografía especializada en el tema, asimismo, se contemplaron trabajos de investigación y artículos sobre algún caso para dar un marco más específico de las acciones desarrolladas, alcances y consecuencias de las acciones desde el punto de la ciberdefensa.

El alcance de esta investigación abarcó el estudio exhaustivo de la incumbencia de la ciberdefensa en la República Argentina, desde el marco normativo hasta las capacidades operativas y doctrinales de las instituciones militares de defensa. Se propone un análisis integral de las siguientes áreas clave:

Marco Normativo y Doctrinal: abordó la normativa existente en Argentina sobre ciberdefensa y ciberseguridad, incluyendo leyes como la Ley de Defensa Nacional (Ley 23.554), los Decretos 577/2017 y 457/2021, y resoluciones que establecen políticas y estrategias de ciberdefensa. Se analizó cómo estos marcos normativos contribuyen o limitan la protección de las infraestructuras críticas.

Infraestructuras Críticas: El estudio identificó las infraestructuras críticas en Argentina, tales como los sectores de energía, telecomunicaciones, transporte y salud. Se analizó el grado de vulnerabilidad de estas infraestructuras frente a las ciberamenazas y cómo la ciberdefensa contribuye a su protección.

Ciberamenazas: Se identificaron las ciberamenazas (ataque dos, ransomware, ingeniería social, entre otros), a las que está expuesta la República Argentina, haciendo énfasis en los

desafíos normativos que limitan la respuesta ante ciberataques. Se analizarán casos recientes de ciberincidentes que involucren infraestructuras críticas.

A pesar del enfoque integral del trabajo, existieron varias limitaciones que debieron considerarse como son:

El marco normativo de ciberdefensa en Argentina enfrenta una limitación en función de los posibles cambios que pudieran surgir durante el periodo de investigación. A medida que el país avanza en la implementación de políticas y normativas sobre ciberdefensa, podrían sancionarse nuevas leyes o modificarse normativas vigentes, como el Decreto 577/2017 o la Directiva de Política de Defensa Nacional 2021 (Decreto N° 457/2021). Estos cambios normativos podrían redistribuir responsabilidades y competencias entre los organismos involucrados, así como introducir nuevas directrices en el abordaje de las ciberamenazas. Por esta razón, la investigación y el análisis de la normativa se limitaron a los documentos vigentes hasta el 01 de octubre de 2024.

Acceso a información clasificada: Gran parte de la información relevante sobre ciberdefensa y la Defensa Nacional es clasificada por su naturaleza sensible. Esto limita el acceso a datos sobre incidentes y políticas operativas específicas, lo cual condiciono la profundidad del análisis.

Datos cuantitativos limitados: Existe una escasez de datos cuantitativos públicos y verificados sobre ciberataques que afecten infraestructuras críticas en Argentina, lo que limito el alcance del análisis empírico de las amenazas y respuestas efectivas.

Colaboración interinstitucional: El grado de colaboración entre las instituciones nacionales y su disposición a compartir información y recursos podría condicionar el desarrollo de la investigación. La falta de acceso a ciertos organismos clave limito el análisis sobre la coordinación interinstitucional en el ámbito de la ciberdefensa.

En resumen, la investigación se centró en desarrollar un enfoque descriptivo sobre la ciberdefensa en el nivel operacional en Argentina, abarcando las normativas, las capacidades militares y las vulnerabilidades de las infraestructuras críticas, mientras se reconocen las limitaciones inherentes a la disponibilidad de información y la evolución constante de las tecnologías en el ciberespacio.

Este trabajo de investigación contribuye teóricamente al campo del nivel operacional al abordar de manera integrada la incumbencia de la ciberdefensa como una dimensión fundamental de la Defensa Nacional. Los principales aportes se estructuran en los siguientes:

Marco teórico de ciberdefensa

El estudio profundizara en la construcción teórica del concepto de ciberdefensa dentro del marco del nivel operacional, enfocándose en cómo este concepto se incorpora en la doctrina militar y las políticas de defensa del Estado argentino. A través del análisis de normativa como son el Decreto N° 457/2021, el Decreto N° 577/2017 y Reglamento de Ciberdefensa y Guerra Electrónica para la Acción Militar Conjunta, el trabajo explora el alcance y las limitaciones de la normativa actual para integrar el ciberespacio en la estrategia de defensa del nivel operacional, lo cual aporta una base teórica robusta para futuros estudios y políticas en este campo.

Evaluación y protección de infraestructuras críticas

Desde una perspectiva teórica aplicada, el trabajo se enfoca en la evaluación de las infraestructuras críticas en Argentina, como lo son los sectores de energía, transporte y telecomunicaciones, analizando su vulnerabilidad frente a las ciberamenazas. Este análisis tiene el potencial de ofrecer una guía sobre los riesgos actuales y las medidas de protección necesarias, lo cual resulta fundamental para la seguridad de estas infraestructuras esenciales y el fortalecimiento de la ciberdefensa nacional.

Capacidades en la ciberdefensa militar

Se propondrán estrategias para mejorar la capacidad de ciberdefensa en las Fuerzas Armadas argentinas, basadas en un estudio comparativo de doctrinas internacionales y análisis de los recursos y capacidades nacionales. Estas recomendaciones incluyen el diseño de programas de formación especializada y la actualización tecnológica, proporcionando herramientas prácticas para la modernización del sistema de defensa argentino y su preparación frente a ciberamenazas emergentes.

Contribuciones a la doctrina militar

Finalmente, el trabajo ofrecerá un aporte a la doctrina militar en Argentina al consolidar el concepto de ciberdefensa en el marco de la Defensa Nacional del nivel operacional. Este enfoque teórico buscara promover una integración de la ciberdefensa en la planificación operacional, estableciendo una base para la formulación de una doctrina de defensa más inclusiva que responda a las realidades del ciberespacio. Las recomendaciones teóricas en este trabajo fomentan una visión más amplia de la defensa nacional y abren el camino para futuras investigaciones en ciberseguridad y defensa.

El objetivo general de este trabajo es el de analizar la incumbencia de la ciberdefensa en el marco de las políticas de defensa y cumplimiento de las leyes vigentes para la protección

de la infraestructura critica en el nivel operacional. Para el estudio de este objetivo, se establecieron los siguientes objetivos específicos:

Establecer los puntos en conflicto entre lo establecido en la doctrina y las necesidades propias del ciberespacio para desarrollar una activa ciberdefensa.

Establecer el grado de participación del nivel operacional para protección de la infraestructura crítica y desde que momento se debería desarrollar la ciberdefensa.

Como hipótesis se planteó que, la ciberdefensa a nivel operacional al tener una participación activa en el asesoramiento para la determinación de los objetivos de valor estratégico como así también en la planificación de su defensa, mediante la identificación de las vulnerabilidades cibernéticas, la evaluación del impacto de los ataques, la propuesta de medidas de mitigación y la colaboración con otros actores para la implementación de estrategias de protección de aquellas infraestructuras críticas. La importancia de la ciberdefensa en la protección de las mismas, conlleva a que Argentina desarrolle capacidades y políticas específicas para esta tarea como las que realiza el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.

Por ello, si la ciberdefensa abarca la protección de infraestructuras críticas de la República Argentina, será necesario que la ciberdefensa a nivel operacional desempeñe un rol activo en la identificación de vulnerabilidades, evaluación de riesgos, planificación de la defensa y coordinación con otros actores.

Esta hipótesis sugiere que la ciberdefensa no se limite a la defensa militar, sino que tienda a una incumbencia mucho más amplia e impacte directamente en la defensa de objetivos de valor estratégico para el funcionamiento de la sociedad, lo que requerirá una participación activa de la ciberdefensa a nivel operacional previo a una situación de crisis o conflicto armado, involucrándose en procesos de análisis, planificación y coordinación desde la paz.

Para abordar el análisis de la incumbencia de la ciberdefensa en la defensa nacional en el nivel operacional, se utilizó un método hipotético deductivo enfoque cualitativo y exploratorio-descriptivo. Esta metodología permite investigar la normativa, las capacidades institucionales y los desafíos de la ciberdefensa en el nivel operacional, vinculados a la protección de infraestructuras críticas.

El método de investigación será cualitativo y se centrará en la recolección y análisis de datos secundarios obtenidos a partir de fuentes documentales, como normativas nacionales e internacionales, políticas públicas, informes de organismos de defensa, y estudios de caso sobre ciberdefensa en Argentina y otros países. Además, se complementará con un análisis descriptivo

que permitirá comprender las dinámicas de la ciberdefensa en el contexto militar y su interacción con los sistemas de seguridad nacionales e internacionales.

El diseño de la investigación es de carácter exploratorio-descriptivo, donde se explorará el estado actual de la ciberdefensa en Argentina y las normativas vigentes, se describirán las capacidades del Comando Conjunto de Ciberdefensa y las acciones coordinadas entre las Fuerzas Armadas y otras instituciones.

La unidad de análisis central será la ciberdefensa en Argentina en el contexto de la protección de infraestructuras críticas. Se investigarán las políticas de defensa nacional, los organismos encargados de la ciberseguridad (Subsecretaria de Ciberdefensa del ministerio de Defensa, Comando Conjunto de Ciberdefensa, Instituto de Ciberdefensa de las Fuerzas Armadas) y las infraestructuras críticas que se protegen mediante estas políticas (energía, telecomunicaciones, defensa, etc.).

Marco normativo: Revisión de leyes y decretos que regulan la ciberdefensa (Ley 23.554, Decreto 577/2017, Decreto 457/2021).

Capacidades operativas: Evaluación de los recursos y capacidades de las Fuerzas Armadas y otros organismos en materia de ciberdefensa.

Infraestructuras críticas: Identificación de los sectores clave y su vulnerabilidad ante ciberamenazas.

Coordinación interinstitucional: Análisis del nivel de cooperación entre el Estado y el sector privado.

Dado que se trata de un estudio cualitativo y documental, no se trabajará con una población definida en términos numéricos. Sin embargo, la muestra seleccionada estará compuesta por documentos oficiales, informes de organismos especializados en ciberdefensa (Ministerio de Defensa, Comando Conjunto de Ciberdefensa, entre otros).

La recolección de datos secundarios será la técnica principal, utilizando fuentes como: Normativa oficial (leyes, decretos, resoluciones), Informes de organismos nacionales e internacionales, Artículos académicos y publicaciones. El análisis se realizará mediante una combinación de análisis documental y análisis de contenido. Se revisarán las normativas

La metodología que se propuso un estudio analítico-descriptivo. Se trabajará con fuentes de datos basadas en leyes, leyes complementarias, decretos y resoluciones de la República Argentina, así como con doctrina militar conjunta, trabajos de investigación y bibliografía desarrollada por autores especializados en el tema.

Se realizará el análisis de la problemática relacionando gran parte de los conceptos expuestos en el desarrollo de la Especialización en estrategia operacional y planeamiento militar

conjunto, recorriendo los caminos conceptuales técnicos de las ciencias duras, el marco legal en el cual se desarrollan las competencias de la ciberdefensa y algunas de las habilidades necesarias para gestionar, asesorar, asistir y participar en la conducción de las acciones en el llamado “Quinto Dominio”.

Se considera de suma importancia analizar cómo el nivel operacional, encargado de ejecutar las políticas del estado relacionadas con la defensa nacional y el uso del ciberespacio, establece y enfrenta los límites entre la seguridad y la defensa, con un enfoque de actuar desde la paz al momento de definir las incumbencias, como ello podría mejorar el diseño de misiones, organización, funciones y tareas para los organismos y elementos de ciberdefensa dentro de las fuerzas.

Este trabajo busca realizar una descripción, a través de una definición categórica de las incumbencias de la ciberdefensa nacional, que facilite la dirección de los esfuerzos de ciberdefensa en la defensa de las infraestructuras críticas, de todos los actores involucrados en el nivel operacional.

CAPÍTULO 1
Marco normativo y conceptos fundamentales

Definición de ciberdefensa

La ciberdefensa es el conjunto de estrategias, operaciones y medidas implementadas por un Estado para proteger sus sistemas de información, redes digitales e infraestructuras críticas frente a amenazas provenientes del ciberespacio. Este concepto adquiere especial relevancia en un entorno global interconectado donde las Tecnologías de la Información y la Comunicación (TIC) son fundamentales para la seguridad nacional, económica y social (Vergara & Trama, 2017).

Desde el ámbito militar, la ciberdefensa implica capacidades defensivas y ofensivas destinadas a garantizar la soberanía y la estabilidad del Estado en el ciberespacio. No solo busca prevenir y mitigar incidentes, sino también realizar operaciones que permitan neutralizar amenazas y salvaguardar infraestructuras críticas esenciales para la continuidad operativa de un país. En el caso de Argentina, la Ley N° 23.554 de Defensa Nacional y el Decreto N° 457/2021 establecen que la ciberdefensa es una responsabilidad compartida entre las Fuerzas Armadas,

los organismos gubernamentales y el sector privado, destacando su importancia en la protección del ciberespacio como dominio estratégico (Resolución N° 580/2011).

El ciberespacio se ha reconocido como un dominio operacional junto con tierra, mar, aire y espacio. Su defensa no solo requiere de herramientas tecnológicas avanzadas, sino también de una cooperación interinstitucional para integrar recursos, capacidades y conocimientos, especialmente en sectores críticos como energía, transporte y telecomunicaciones. Este enfoque multidimensional subraya la necesidad de contar con estrategias nacionales y doctrinas específicas que reflejen la complejidad del ciberespacio y su importancia en la planificación estratégica de defensa (Resolución N° 829/2019).

Definición de ciberespacio y defensa en el ámbito militar y civil

El ciberespacio se define como un entorno multidimensional compuesto por infraestructuras físicas, sistemas lógicos y actores humanos. Este dominio incluye elementos tangibles como servidores, cables submarinos y centros de datos, así como componentes intangibles como protocolos, software y redes digitales interconectadas. Su naturaleza global y descentralizada lo convierte en un espacio esencial para la operación de infraestructuras críticas y la comunicación en todos los niveles de la sociedad (Resolución N° 580/2011).

En el ámbito militar, el ciberespacio ha sido formalmente reconocido como un dominio estratégico de operaciones. Según el PC 11-01 (2023), reglamento de ciberdefensa y guerra electrónica para la acción militar conjunta, en su capítulo III: Actividades cibernéticas y electromagnéticas (CEMA, del inglés Cyber and Electromagnetic Activities), las operaciones en este dominio buscan garantizar la libertad de acción, proteger los sistemas propios y neutralizar la capacidad del adversario para operar en el ciberespacio. Estas acciones incluyen desde la identificación de vulnerabilidades hasta la ejecución de operaciones ofensivas que degraden o deshabiliten los sistemas enemigos. Además, el espectro electromagnético se superpone con el ciberespacio, lo que exige una asignación eficiente de recursos para garantizar la seguridad de las redes militares y la coordinación en tiempo real (PC11-01, 2023).

En el ámbito civil, el ciberespacio sostiene infraestructuras críticas como telecomunicaciones, transporte, energía y servicios financieros. Los incidentes en este entorno pueden tener un impacto devastador en la economía, la defensa nacional y el bienestar social (Resolución N°1523/2019). La Resolución N° 829/2019, que establece la Estrategia Nacional de Ciberseguridad, enfatiza la importancia de la colaboración público-privada para proteger estos sectores y mitigar los riesgos emergentes.

La defensa del ciberespacio requiere de un enfoque integral que combine capacidades técnicas avanzadas, políticas regulatorias y cooperación internacional. Este enfoque permite no solo prevenir incidentes, sino también garantizar la resiliencia frente a ciberataques que puedan comprometer la seguridad del Estado y la estabilidad de su infraestructura estratégica (Dirección Nacional de Ciberseguridad, 2023).

Diferenciación entre ciberdefensa, ciberseguridad y ciberataques

Aunque están estrechamente relacionadas, la ciberdefensa y la ciberseguridad tienen objetivos y enfoques distintos. La ciberseguridad se centra en proteger los sistemas de información mediante medidas técnicas y organizativas que aseguren la confidencialidad, integridad y disponibilidad de los datos frente a amenazas internas y externas. Por otro lado, la ciberdefensa adopta un enfoque más amplio y estratégico, diseñado para salvaguardar la soberanía nacional y garantizar la continuidad operativa frente a ciberamenazas complejas (Vergara & Trama, 2017).

La ciberdefensa incluye capacidades ofensivas, defensivas y de exploración que permiten identificar, prevenir y mitigar amenazas avanzadas en el ciberespacio. Estas capacidades son esenciales para proteger infraestructuras críticas, garantizar la seguridad de las redes estratégicas y neutralizar a los adversarios (PC11-01, 2023). Según el PC 11-01 (2023), en su capítulo III, se establece que las operaciones de ciberdefensa abarcan desde la neutralización de ataques cibernéticos hasta la realización de operaciones ofensivas dirigidas a degradar las capacidades del adversario en el ciberespacio. Estas acciones son vitales para garantizar la soberanía y la estabilidad nacional.

La ciberseguridad, en cambio, tiene un alcance técnico y operativo, enfocado en prevenir incidentes mediante la implementación de medidas de protección en los sistemas de información. La Resolución N° 580/2011 destaca que la ciberseguridad es una primera línea de defensa frente a amenazas como malware, ataques de denegación de servicio (DDoS) y ransomware. Este enfoque es complementario a la ciberdefensa, ya que actúa como una capa protectora que mitiga riesgos y reduce la superficie de ataque.

Por otro lado, los ciberataques son acciones ofensivas diseñadas para interrumpir, manipular o destruir sistemas digitales e infraestructuras críticas. Estas amenazas pueden ser ejecutadas por actores estatales, cibercriminales, hacktivistas o grupos terroristas. los ciberataques representan una amenaza significativa para la seguridad nacional, especialmente en sectores estratégicos como energía y telecomunicaciones (PC11-01, 2023). Ejemplos como

los ciberataques que tuvieron lugar contra Estonia en el año 2007 evidencian cómo estas acciones pueden generar impactos operativos, económicos y sociales a gran escala (Ottis, 2007).

Infraestructuras críticas

Las infraestructuras críticas (IC) son los sistemas, activos y redes esenciales para el funcionamiento de la sociedad, cuyo daño o interrupción puede generar un impacto devastador en la defensa nacional, la economía, la salud pública y el bienestar de la población. En un mundo altamente interconectado y dependiente de las Tecnologías de la Información y la Comunicación (TIC), proteger estas infraestructuras se ha convertido en una prioridad estratégica para los Estados, incluyendo a la República Argentina (Resolución N°1523/2019), (PC11-01, 2023). Según el Informe Dirección Nacional de Ciberseguridad, CERT.ar (2023), los sectores de energía, transporte, telecomunicaciones, servicios financieros y salud son los más vulnerables frente a ciberamenazas, lo que subraya la necesidad de políticas integradas de protección.

En Argentina, la Ley N° 23.554 de Defensa Nacional y normativas como el Decreto N° 457/2021 establecen que la protección de las infraestructuras criticas forma parte esencial de la seguridad y defensa del país. Además, la Resolución N° 580/2011 crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, definiendo lineamientos para identificar, evaluar y mitigar los riesgos asociados a estos sistemas estratégicos (Resolución N° 580/2011).

Definición de infraestructuras críticas en el contexto de la Defensa Nacional

En el contexto de la Defensa Nacional, las infraestructuras criticas se definen como activos y sistemas cuyo funcionamiento es esencial para la defensa y la estabilidad de un país. Su interrupción o destrucción puede tener consecuencias catastróficas en la operatividad estatal y en la vida cotidiana de sus ciudadanos. La Resolución N° 580/2011 establece que las infraestructuras criticas incluyen sistemas físicos y virtuales que deben ser protegidos para garantizar la continuidad de servicios esenciales, mientras que el PC 11-01 (2023), clasifica los incidentes cibernéticos por su impacto en estas infraestructuras, destacando la importancia de un enfoque preventivo y coordinado.

Asimismo, PC 11-01 (2023), en su capítulo III señala que la identificación y protección de infraestructuras criticas requiere un planeamiento estratégico que combine capacidades cibernéticas y electromagnéticas. En el ámbito militar, las infraestructuras criticas no solo son objetivos de protección, sino también recursos indispensables para el despliegue y coordinación de operaciones conjuntas, lo que refuerza su relevancia dentro de la estrategia de defensa nacional.

Un ejemplo paradigmático de la relevancia estratégica de las infraestructuras críticas se observa en el sector energético, cuya vulnerabilidad quedó evidenciada en el ataque al programa nuclear de Irán. Este incidente, protagonizado por el gusano informático Stuxnet, logró infiltrarse en los sistemas de control industrial responsables de la operación de las centrifugadoras nucleares, causando un retraso significativo en el desarrollo del programa durante varios años. Este caso no solo expone las debilidades inherentes a dichas infraestructuras, sino que también ilustra cómo actores adversarios pueden emplearlas como herramientas de coerción geopolítica, subrayando la intersección entre la ciberdefensa y la dinámica de poder internacional, (Wall, 2011).

Tipologías de infraestructuras críticas: Energía, telecomunicaciones, transporte, servicios financieros, salud, entre otras

Las infraestructuras críticas abarcan una amplia gama de sectores que son interdependientes y esenciales para el funcionamiento del Estado y la sociedad. En el caso de Argentina, los sectores clave incluyen energía, telecomunicaciones, transporte, servicios financieros, salud e infraestructuras gubernamentales. A continuación, se describen estas tipologías y su relevancia estratégica:

El sector energético, que incluye la generación, transmisión y distribución de electricidad, así como las infraestructuras de petróleo y gas, es considerado crítico para la estabilidad económica y la defensa nacional. La Resolución N° 1380/2019 establece directrices para fortalecer la resiliencia de este sector frente a ciberataques, como el ransomware o el sabotaje a redes SCADA[1], sistemas industriales que controlan procesos energéticos esenciales (Resolución N° 1380/2019).

[1] Un sistema SCADA es una red de hardware y software para la monitorización, supervisión y control en tiempo real de máquinas e instalaciones industriales. SCADA son las siglas de Supervisory Control and Data Acquisition (control de supervisión y adquisición de datos) (eMaint por Fluke Corporation, 2023).

El PC 11-01 (2023), en su capítulo III, menciona la dependencia de sistemas digitales hace que este sector sea un objetivo prioritario para adversarios que buscan desestabilizar a un Estado. El documento señala la necesidad de coordinar esfuerzos entre el sector público y privado para proteger estas infraestructuras de amenazas avanzadas.

El sector de telecomunicaciones incluye redes de comunicación, sistemas satelitales como Empresa Argentina de Soluciones Satelitales S.A (ARSAT) y la Red Federal de Fibra Óptica (REFEFO). Este sector es fundamental tanto para la conectividad civil como para las operaciones militares. La Resolución N° 1523/2019 subraya la importancia de implementar medidas de protección frente a ataques de denegación de servicio (DDoS) y espionaje cibernético, que pueden comprometer la seguridad de las comunicaciones nacionales (Resolución N°1523/2019).

Se destaca que el ciberespacio y el espectro electromagnético están interrelacionados en este sector, lo que exige una gestión eficiente de frecuencias y una defensa coordinada de las redes críticas (PC11-01, 2023).

El transporte, que abarca sistemas ferroviarios, carreteras, puertos y aeropuertos, es esencial para la logística, el comercio y las operaciones militares, en tal sentido el Decreto N° 480/2019 reconoce este sector como prioritario para la defensa nacional, destacando la necesidad de integrar tecnologías avanzadas para protegerlo frente a ciberamenazas (Decreto N° 480/2019).

El Informe Dirección Nacional de Ciberseguridad, CERT.ar (2023), menciona como los ciberataques a sistemas de transporte han aumentado en los últimos años, afectando tanto a la movilidad de bienes y personas como a la operatividad militar en contextos de crisis.

El sector financiero, que incluye bancos y sistemas de pago, es uno de los más vulnerables a ataques cibernéticos. El PC 11-01 (2023), clasifica los incidentes en este sector como de alto impacto debido a su capacidad de desestabilizar economías enteras. La Resolución N° 1523/2019 enfatiza la necesidad de fortalecer las capacidades de respuesta frente a fraudes cibernéticos y campañas de ransomware dirigidas a bancos y plataformas de pago digital (Resolución N°1523/2019).

El sector salud incluye hospitales, sistemas de atención médica y laboratorios. Durante la pandemia de COVID-19, este sector enfrentó un aumento significativo de ciberataques, lo que evidenció su vulnerabilidad (Revista Summa, 2020), (González, 2021). La Resolución N° 580/2011 menciona que la protección de este sector es fundamental para garantizar la continuidad de los servicios de salud pública, especialmente en contextos de emergencia (Resolución N° 580/2011).

Las infraestructuras gubernamentales incluyen sistemas de mando y control, bases de datos críticas y redes de comunicación del Estado. Estos activos son objetivos prioritarios para actores hostiles que buscan desestabilizar a los gobiernos mediante ciberataques. El Decreto N° 577/2017 y la Resolución N° 829/2019 subrayan la importancia de proteger estos sistemas frente a amenazas externas mediante estrategias de ciberdefensa y ciberseguridad (Decreto N° 577/2017), (Resolución N° 829/2019).

Relación entre ciberdefensa y protección de infraestructuras críticas

La relación entre la ciberdefensa y la protección de las infraestructuras críticas (IC) se ha convertido en un tema de relevancia estratégica en el marco de la seguridad nacional. Las IC, que abarcan sectores esenciales como energía, telecomunicaciones, transporte, servicios financieros y salud representan el núcleo de la estabilidad política, económica y social de los Estados modernos. Sin embargo, su dependencia de las Tecnologías de la Información y la Comunicación (TIC) las ha vuelto altamente vulnerables frente a ciberamenazas. En este contexto, la ciberdefensa desempeña un papel fundamental como mecanismo de protección activa y reactiva frente a incidentes que podrían comprometer la operatividad del Estado y la seguridad de sus ciudadanos (Dirección Nacional de Ciberseguridad, 2023)

En Argentina, la relación entre la ciberdefensa y las IC está definida por un marco normativo robusto que incluye la Ley N° 23.554 de Defensa Nacional, el Decreto N° 457/2021 y la Resolución N° 580/2011, entre otros. Estos instrumentos establecen que la protección de las IC es una responsabilidad compartida entre las Fuerzas Armadas, las instituciones gubernamentales y el sector privado, y subrayan la necesidad de una respuesta coordinada para mitigar riesgos cibernéticos.

Impacto de las ciberamenazas en las infraestructuras críticas

Las ciberamenazas representan un riesgo significativo para las IC, ya que tienen la capacidad de interrumpir servicios esenciales, generar pérdidas económicas masivas y desestabilizar la seguridad nacional. Para Dirección Nacional de Ciberseguridad, CERT.ar (2023), los sectores más vulnerables en Argentina son el energético, el de telecomunicaciones, el de servicios financieros, transporte y salud, los cuales han experimentado un aumento constante en la frecuencia y sofisticación de los ataques cibernéticos.

Las principales ciberamenazas que afectan a las infraestructuras criticas incluyen:

Ransomware: Este tipo de ataque bloquea el acceso a los sistemas hasta que se paga un rescate. Durante 2022, varias instituciones financieras argentinas sufrieron ataques de ransomware que afectaron la operatividad de sus sistemas durante semanas (PC11-01, 2023), (Dirección Nacional de Ciberseguridad, 2023).

Ataques de denegación de servicio (DDoS): Los DDoS sobrecargan los sistemas de las IC, haciendo que no puedan responder a solicitudes legítimas. Este tipo de ataque es particularmente peligroso en el sector de telecomunicaciones, donde las interrupciones pueden afectar tanto a las comunicaciones civiles como a las operaciones militares (PC11-01, 2023).

Explotación de vulnerabilidades: Los sistemas SCADA, utilizados para controlar procesos industriales en sectores como energía y transporte, son altamente vulnerables a ciberataques (Dirección Nacional de Ciberseguridad, 2023).

Impacto nivel operacional

El impacto de las ciberamenazas en las IC trasciende lo técnico y afecta aspectos nivel operacional y nivel estratégicos. En el ámbito civil, un ataque a la infraestructura energética puede paralizar la economía, mientras que, en el ámbito militar, una interrupción en las telecomunicaciones podría comprometer la coordinación de operaciones conjuntas. Según el PC 11-01 (2023), en su capítulo III, las ciberamenazas no solo afectan la capacidad de respuesta inmediata, sino que también generan un impacto prolongado en la Defensa Nacional al debilitar las capacidades, la confianza pública en la resiliencia del Estado (PC11-01, 2023).

Además, los actores hostiles utilizan las IC como objetivos estratégicos para desestabilizar naciones. Los ataques dirigidos a sectores como el energético y el transporte no solo generan pérdidas económicas directas, sino que también tienen un efecto psicológico en la población y las instituciones, exacerbando la percepción de falta de defensa (Vergara & Trama, 2017).

La ciberdefensa como herramienta en la protección de las infraestructuras críticas

La ciberdefensa es un componente fundamental para garantizar la defensa de las IC frente a ciberamenazas. A diferencia de la ciberseguridad, que se centra en medidas técnicas para proteger sistemas y redes, la ciberdefensa adopta un enfoque más amplio y estratégico, combinando capacidades ofensivas, defensivas y de exploración para salvaguardar la soberanía nacional (PC11-01, 2023).

La ciberdefensa aporta una serie de capacidades clave para la protección de las IC, entre las que destacan:

Monitoreo y detección de amenazas: Los sistemas de monitoreo en tiempo real son esenciales para identificar patrones anómalos y detectar amenazas antes de que causen daño. La implementación de tecnologías avanzadas, como la inteligencia artificial, permite anticipar posibles ataques y reforzar las defensas (PC11-01, 2023).

Mitigación y respuesta a incidentes: La ciberdefensa incluye protocolos específicos para contener ataques en curso y restaurar la funcionalidad de las IC. La Resolución N° 580/2011 destaca la importancia de contar con planes de contingencia y recuperación adaptados a cada sector estratégico.

Capacidades ofensivas: En casos de agresión estatal o amenazas transnacionales, la ciberdefensa también permite desplegar operaciones ofensivas para neutralizar las capacidades del adversario. Estas operaciones incluyen la interdicción de redes hostiles y la generación de efectos cibernéticos diseñados para desactivar infraestructuras críticas enemigas (PC11-01, 2023).

Coordinación interinstitucional: La protección de las IC requiere una estrecha colaboración entre las Fuerzas Armadas, las agencias gubernamentales y el sector privado. La Resolución N° 829/2019 establece lineamientos para fomentar esta cooperación, destacando la necesidad de compartir información y recursos para fortalecer la resiliencia de las IC.

La ciberdefensa debe integrarse en todos los niveles de la conducción militar y gubernamental para garantizar una respuesta efectiva frente a ciberamenazas. Esto incluye la identificación de vulnerabilidades, la evaluación de riesgos y la implementación de estrategias de protección que abarquen tanto el ámbito físico como el digital (PC11-01, 2023).

En el contexto argentino, el Decreto N° 457/2021 regula la planificación estratégica de la ciberdefensa, asignando al Comando Conjunto de Ciberdefensa la responsabilidad de proteger las IC. Este organismo actúa como un puente entre las políticas de defensa y las necesidades operativas, asegurando que las capacidades cibernéticas estén alineadas con los objetivos nacionales (Decreto N° 457/2021).

Legislación y políticas relacionadas con la ciberdefensa y las infraestructuras críticas

La evolución de las ciberamenazas y su impacto en las infraestructuras críticas (IC) han impulsado a los Estados a desarrollar marcos normativos y políticas integrales que aborden la protección del ciberespacio desde un enfoque estratégico. La ciberdefensa, como componente central de estas estrategias, no solo se enfoca en mitigar riesgos cibernéticos, sino también en garantizar la soberanía y la estabilidad nacional frente a actores malintencionados. En este sentido, tanto las normativas nacionales como las políticas internacionales desempeñan un papel crucial en la regulación, coordinación y ejecución de medidas que protejan estos activos estratégicos.

En Argentina, el marco normativo nacional ha sentado las bases para la protección del ciberespacio, con un enfoque especial en las IC. A nivel internacional, la cooperación entre Estados, organismos multilaterales y el sector privado ha fomentado el intercambio de información y la implementación de mejores prácticas en ciberdefensa. Ambos enfoques son complementarios y esenciales en un mundo interconectado.

Marco normativo nacional

El marco normativo argentino para la ciberdefensa y la protección de IC se basa en leyes, decretos y resoluciones que establecen directrices específicas para abordar las amenazas cibernéticas y garantizar la resiliencia de los sistemas estratégicos.

La Ley N° 23.554 define los principios rectores de la Defensa Nacional, asignando al Sistema de Defensa Nacional la responsabilidad de proteger al país frente a amenazas externas, incluidas las provenientes del ciberespacio. Esta ley establece un enfoque integral que incluye la participación de las Fuerzas Armadas, las instituciones gubernamentales y el sector privado en la protección de activos estratégicos, incluyendo las IC (Ley 23554, 1988).

El Decreto N° 457/2021 regula la planificación estratégica de la defensa en Argentina, incorporando explícitamente la ciberdefensa como un componente esencial del Sistema de Defensa Nacional. Este decreto asigna al Comando Conjunto de Ciberdefensa la responsabilidad de coordinar operaciones en el ciberespacio y proteger las IC frente a ciberamenazas. Asimismo, refuerza la necesidad de integrar capacidades cibernéticas en la

doctrina militar, priorizando la cooperación interinstitucional y la modernización tecnológica (Decreto N° 457/2021).

El Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, establece como objetivo principal el identificar y proteger las IC frente a amenazas cibernéticas y físicas. Este programa promueve la evaluación de riesgos, la implementación de sistemas de monitoreo y la creación de protocolos de respuesta ante incidentes. La integración de este programa con los planes de defensa nacional ha permitido una respuesta más coordinada frente a incidentes que afectan sectores como energía, transporte y telecomunicaciones (Resolución N° 580/2011).

La Resolución que aprueba la Estrategia Nacional de Ciberseguridad, que establece lineamientos específicos para proteger las redes críticas y las IC en Argentina, enfatiza en la importancia de la colaboración público-privada, destacando que la protección del ciberespacio no puede recaer exclusivamente en las instituciones gubernamentales. La estrategia también aborda la necesidad de capacitación continua y el desarrollo de capacidades tecnológicas avanzadas para mitigar riesgos emergentes (Resolución N° 829/2019).

Puntos en conflicto entre la doctrina tradicional y las necesidades del ciberespacio

El ciberespacio, como nuevo dominio de operaciones, ha planteado desafíos únicos para la doctrina tradicional de defensa nacional. Este entorno se caracteriza por su rápida evolución, su naturaleza transnacional y su complejidad técnica, lo que contrasta con la rigidez y el enfoque sectorial de doctrinas existentes. En el contexto argentino, el Decreto N° 457/2021 y la Ley N° 23.554 de Defensa Nacional establecen un marco general para la defensa, pero no necesariamente se ajustan a las demandas específicas del ciberespacio, lo que genera tensiones que dificultan el desarrollo de una ciberdefensa activa y efectiva (Resolución N° 580/2011).

Uno de los principales puntos de conflicto es la estructura jerárquica y centralizada de las doctrinas tradicionales frente a la naturaleza descentralizada e interconectada del ciberespacio. Las doctrinas actuales tienden a priorizar modelos operativos que requieren largas cadenas de mando y decisiones centralizadas, lo cual puede resultar ineficaz para responder a amenazas cibernéticas que demandan respuestas rápidas y flexibles (PC11-01, 2023).

Además, la doctrina tradicional no siempre considera la colaboración público-privada como una prioridad. Sin embargo, en el ciberespacio, esta cooperación es esencial, ya que gran parte de las infraestructuras críticas están gestionadas por el sector privado, lo que conlleva a establecer y pensar una colaboración entre las Fuerzas Armadas, las agencias civiles y las

empresas privadas como clave para garantizar la protección de estas infraestructuras frente a ciberataques (Vergara & Trama, 2017).

Otro punto de conflicto radica en las limitaciones normativas para la actuación de las Fuerzas Armadas en el ciberespacio, la Ley N° 23.554 restringe su intervención a amenazas externas, lo que dificulta su rol en incidentes cibernéticos que pueden no estar claramente delimitados por fronteras físicas. Esto contrasta con la necesidad de adoptar un enfoque más proactivo que permita anticiparse a las amenazas y coordinar respuestas ante ciberataques transnacionales (Ley 23554, 1988), (PC11-01, 2023).

Además, la falta de un marco legal específico para la ciberdefensa genera incertidumbre operativa. La ausencia de definiciones claras sobre competencias y responsabilidades en el ámbito cibernético limita la capacidad del Estado para responder eficazmente a incidentes críticos (Dirección Nacional de Ciberseguridad, 2023).

Capítulo 2

Determinación de Infraestructuras Críticas: El Rol de la Ciberdefensa

La determinación de las infraestructuras críticas (IC) es un proceso estratégico esencial para garantizar la seguridad nacional y la estabilidad operativa de un Estado. Estas infraestructuras son definidas como sistemas, activos y servicios cuya interrupción o destrucción tendría consecuencias devastadoras en sectores clave como la economía, la salud pública, la defensa y el bienestar general de la población (Vergara & Trama, 2017). En el contexto actual, la creciente dependencia de las Tecnologías de la Información y la Comunicación (TIC) y el aumento de ciberamenazas han elevado la relevancia de la ciberdefensa como un componente clave en la protección de las IC.

En Argentina, el marco normativo establece un enfoque integral para identificar, evaluar y proteger las IC. La Ley N° 23.554 de Defensa Nacional, junto con el Decreto N° 457/2021, subraya la necesidad de garantizar la resiliencia de estos sistemas mediante un esfuerzo coordinado entre las instituciones gubernamentales, las Fuerzas Armadas y el sector privado. Además, la Resolución N° 580/2011 crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, estableciendo procesos específicos para su identificación y protección.

Identificación de las infraestructuras críticas nacionales

El proceso de identificación de las IC nacionales en Argentina se basa en la evaluación de riesgos, la dependencia de las TIC y la interconexión entre sectores estratégicos. Este enfoque integral permite priorizar recursos y diseñar políticas que minimicen las vulnerabilidades frente a incidentes de naturaleza física, lógica o híbrida, se destaca que este proceso requiere la participación activa de actores clave, incluyendo organismos estatales, fuerzas de seguridad y el sector privado (Resolución N° 580/2011).

La normativa argentina aún no establece un procedimiento detallado y unificado para determinar si una infraestructura es critica o no sin embargo las diversas leyes, decretos, resoluciones y disposiciones aportan elementos para determinar un posible proceso de determinación de las IC en Argentina en un esquema que incluye las siguientes etapas:

Evaluación de riesgos: Identificar las amenazas y vulnerabilidades que afectan a cada sector estratégico; los sectores energéticos y de telecomunicaciones son los más vulnerables debido a su dependencia de sistemas digitales y su exposición a ciberamenazas globales (PC11-01, 2023).

Identificación de interdependencias: Analizar cómo los sectores estratégicos están conectados entre sí y cómo un incidente en uno de ellos podría generar un efecto dominó en otros, enfatizando que estas interdependencias son críticas en sectores como el transporte, el energético y salud, que dependen de redes de telecomunicaciones robustas y seguras (Resolución N° 829/2019), (Resolución N°1523/2019).

Priorización de activos: Clasificar los sistemas y activos en función de su importancia estratégica y su impacto potencial en la defensa nacional. Este paso es clave para asignar recursos de manera eficiente y proteger aquellos activos que representan un mayor riesgo (Resolución N°1523/2019), (PC11-01, 2023).

Implementación de la protección: Diseñar e implementar medidas de defensa adaptadas a las características de cada infraestructura, estas medidas incluirían desde la instalación de sistemas de detección de intrusiones, la realización de simulacros de ciberincidentes en ambientes seguros o sanboxing[2] hasta ejercicios la protección de infraestructuras críticas de nivel táctico y operacional.

[2] El sandboxing es una práctica de ciberseguridad que consiste en ejecutar código en un entorno aislado, llamado "sandbox", para analizarlo sin afectar el sistema operativo o dispositivo host.

En este proceso, la ciberdefensa desempeña un rol esencial al proporcionar herramientas para identificar, prevenir y mitigar amenazas avanzadas; subrayando que las operaciones de ciberdefensa permiten así monitorear redes críticas en tiempo real, detectar anomalías y coordinar respuestas ante incidentes, garantizando la continuidad operativa de las IC.

Factores que definen una infraestructura como crítica

Definir una infraestructura como crítica implica evaluar su relevancia estratégica para la seguridad y estabilidad del país. Según la Resolución N° 580/2011, los factores principales que determinan si un activo o sistema es crítico incluyen su impacto en la economía, la defensa, la salud pública y el bienestar social. Además, deben considerarse las interdependencias con otros sectores estratégicos y su nivel de exposición a amenazas físicas y cibernéticas.

Una infraestructura se considera crítica si su interrupción o destrucción comprometería la soberanía y estabilidad del país. Por ejemplo, el sector energético es crucial para garantizar la continuidad de servicios esenciales y la operatividad de las fuerzas de defensa. La Resolución N° 1380/2019 establece que las redes eléctricas y los sistemas de petróleo y gas son objetivos prioritarios en las estrategias de ciberdefensa debido a su importancia estratégica.

La dependencia de las TIC aumenta la vulnerabilidad de las IC frente a ciberamenazas, sectores como telecomunicaciones y servicios salud están altamente expuestos a incidentes como ataques de denegación de servicio (DDoS) y ransomware. Esta dependencia requiere medidas específicas de protección, incluyendo la segmentación de redes y la implementación de sistemas de monitoreo avanzado.

Las IC suelen estar interconectadas, lo que amplifica el impacto de un incidente en un sector determinado. Por ejemplo, un ciberataque a las telecomunicaciones podría interrumpir servicios financieros y operaciones logísticas. La Resolución N° 829/2019 destaca la necesidad de analizar estas interdependencias para diseñar políticas de protección más efectivas, debido a que el daño a una infraestructura crítica puede tener consecuencias devastadoras en la economía y el bienestar social como así también una pérdida de confianza en las instituciones.

La exposición a amenazas físicas y cibernéticas es un factor clave para clasificar una infraestructura como crítica, las mismas deben ser monitoreadas de forma continua para identificar vulnerabilidades y prevenir incidentes que puedan comprometer su integridad (PC11-01, 2023).

La ciberdefensa como herramienta de protección

La ciberdefensa proporciona capacidades específicas para proteger las IC frente a amenazas emergentes. Estas incluyen:

Monitoreo y detección en tiempo real: Identificar anomalías en redes críticas y anticipar posibles ataques. El monitoreo continuo es esencial para prevenir incidentes que puedan generar un efecto cascada en sectores estratégicos, (PC11-01, 2023).

Coordinación interinstitucional: La protección de las IC requiere una colaboración efectiva entre las Fuerzas Armadas, las agencias gubernamentales y el sector privado. La Resolución N° 829/2019 fomenta esta cooperación mediante el intercambio de información y la realización de ejercicios conjuntos.

Respuesta a incidentes: Implementar protocolos para contener ataques en curso y restaurar la funcionalidad de las IC. Estas capacidades incluyen desde la neutralización de ciberataques hasta la ejecución de operaciones ofensivas dirigidas a deshabilitar redes adversarias, (PC11-01, 2023).

Desarrollo de capacidades técnicas: Fortalecer la resiliencia de las IC mediante la capacitación del personal y la adopción de tecnologías avanzadas. Esto es particularmente relevante en sectores como el transporte, donde los sistemas SCADA son vulnerables a ataques dirigidos.

Incumbencia de la ciberdefensa en la identificación de infraestructuras críticas

La ciberdefensa desempeña un rol crucial en la identificación, protección y gestión de las infraestructuras críticas (IC) frente a un panorama global de ciberamenazas en constante evolución. En un mundo interconectado y dependiente de las Tecnologías de la Información y la Comunicación (TIC), las IC son esenciales para garantizar la seguridad nacional, la estabilidad económica y el bienestar social. La detección temprana de vulnerabilidades y la implementación de medidas preventivas son fundamentales para reducir los riesgos y mitigar los efectos de posibles ataques cibernéticos.

En Argentina, el marco normativo y doctrinal establece un enfoque integral para abordar la seguridad de las IC, destacando el papel de las agencias de ciberdefensa y la coordinación interinstitucional. La Ley N° 23.554 de Defensa Nacional y el Decreto N° 457/2021 asignan al Comando Conjunto de Ciberdefensa la responsabilidad de identificar vulnerabilidades y desarrollar capacidades para proteger estos activos estratégicos. Además, normativas como la

Resolución N° 580/2011 y la Resolución N° 829/2019 refuerzan la necesidad de colaboración entre las Fuerzas Armadas y las agencias civiles para garantizar la resiliencia de las IC.

Rol de la ciberdefensa en la identificación de vulnerabilidades

La identificación de vulnerabilidades en las IC es una tarea crítica que recae en las agencias de ciberdefensa, las cuales deben actuar como la primera línea de protección frente a las ciberamenazas. Estas agencias tienen como principal objetivo analizar, evaluar y mitigar los riesgos asociados a la operación de sistemas críticos, utilizando tecnologías avanzadas y metodologías específicas para prevenir incidentes que puedan comprometer la defensa nacional.

La identificación de vulnerabilidades implica un enfoque sistemático que incluye:

Análisis de riesgos para evaluar las amenazas potenciales y las debilidades inherentes en los sistemas de las IC. Según el PC-11-01 (2023), sectores como energía y telecomunicaciones presentan mayores riesgos debido a su alta dependencia de las TIC y su exposición a ciberataques sofisticados, como ransomware y ataques de denegación de servicio (DDoS); Implementar sistemas de monitoreo en tiempo real para identificar anomalías en las redes críticas. El PC-11-01 (2023) subraya que el monitoreo continuo permite anticipar posibles ataques y minimizar los tiempos de respuesta; y realizar simulacros para probar la resiliencia de las IC ante ciberamenazas. La Resolución N° 580/2011 menciona que estos ejercicios son fundamentales para identificar puntos débiles y diseñar protocolos efectivos de respuesta.

El papel de las agencias de ciberdefensa no se limita a la identificación de vulnerabilidades; también incluye la elaboración de estrategias y protocolos para mitigar riesgos. Según la Resolución N° 829/2019, estas agencias son responsables de coordinar esfuerzos con otros organismos estatales y privados para garantizar la resiliencia de las IC frente a incidentes de alta complejidad. Además, se destaca que la capacidad de identificar vulnerabilidades en tiempo real es esencial para evitar interrupciones en los servicios estratégicos del Estado (PC11-01, 2023).

Coordinación entre las fuerzas armadas y agencias civiles para la protección de las Infraestructuras Críticas

La protección de las IC requiere una estrecha coordinación entre las Fuerzas Armadas y las agencias civiles, ya que estas infraestructuras son gestionadas en gran medida por el sector

privado, pero su interrupción tiene implicaciones directas en la seguridad nacional. La colaboración interinstitucional es fundamental para garantizar un enfoque integral que combine capacidades militares, técnicas y administrativas.

La Resolución N° 580/2011 enfatiza la necesidad de establecer canales seguros para el intercambio de información sobre amenazas y vulnerabilidades. Este enfoque permite a las agencias civiles y militares trabajar con datos precisos y en tiempo real para prevenir incidentes.

Asimismo, diseñar planes de acción que incluyan la participación de todos los actores relevantes. Las operaciones conjuntas permiten coordinar recursos y capacidades para garantizar una respuesta rápida y efectiva ante ciberincidentes, (PC11-01, 2023).

Realizar ejercicios que involucren a las Fuerzas Armadas, las agencias civiles y el sector privado, son esenciales para evaluar la eficacia de los protocolos de respuesta y mejorar la coordinación en situaciones de crisis, (Resolución N° 829/2019).

La coordinación entre las Fuerzas Armadas y las agencias civiles aporta importantes beneficios, como el fortalecimiento de la resiliencia de las infraestructuras críticas al abordar vulnerabilidades de forma conjunta, la optimización de recursos mediante la compartición de capacidades y conocimientos que evita duplicaciones, y la capacidad de responder rápidamente a incidentes, garantizando una gestión eficiente que minimiza los impactos en la seguridad nacional y el bienestar social.

Evaluación de riesgos y amenazas cibernéticas a las infraestructuras críticas

La evaluación de riesgos y amenazas cibernéticas se ha convertido en un pilar fundamental para garantizar la seguridad de las infraestructuras críticas (IC). Estas infraestructuras, esenciales para el funcionamiento de un Estado, son cada vez más vulnerables debido a su dependencia de las Tecnologías de la Información y la Comunicación (TIC). En un entorno global donde las ciberamenazas son más frecuentes y sofisticadas, el análisis proactivo de los riesgos permite mitigar los efectos de posibles ataques y fortalecer la resiliencia de los sistemas estratégicos.

En Argentina, la protección de las IC frente a ciberamenazas está regulada por normativas como la Ley N° 23.554 de Defensa Nacional, el Decreto N° 457/2021 y la Resolución N° 580/2011, que establece el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Estas leyes destacan la importancia de identificar las principales amenazas y aprender de los casos relevantes ocurridos en otros países para prevenir incidentes de alto impacto.

Las ciberamenazas dirigidas a las IC son diversas y abarcan desde ataques directos hasta la explotación de vulnerabilidades en las redes digitales interconectadas. Estas amenazas pueden ser ejecutadas por actores estatales, cibercriminales, terroristas o hacktivistas, con objetivos que van desde la desestabilización política hasta el lucro económico. En Argentina, sectores como energía, salud, telecomunicaciones y servicios financieros son los más expuestos, (Dirección Nacional de Ciberseguridad, 2023).

Principales ciberamenazas:

Ransomware: El ransomware es una de las amenazas más frecuentes contra las IC. Este tipo de ataque encripta los datos del sistema y exige un rescate para restaurar el acceso. El ransomware ha afectado a sectores estratégicos como el energético y el financiero en América Latina. En Argentina, varios ataques recientes a empresas privadas han demostrado la necesidad de implementar medidas de protección avanzadas (Dirección Nacional de Ciberseguridad, 2023).

Ataques de denegación de servicio (DDoS): Los ataques de DDoS tienen como objetivo sobrecargar los sistemas, impidiendo su operatividad. Este tipo de ataque es particularmente peligroso para el sector de telecomunicaciones, donde las interrupciones pueden tener un efecto dominó en otros sectores. Los DDoS representan una amenaza crítica debido a su capacidad para paralizar servicios esenciales, (PC11-01, 2023).

Explotación de vulnerabilidades: La explotación de vulnerabilidades en sistemas obsoletos o mal configurados es una táctica común utilizada por actores malintencionados. Los sistemas SCADA, utilizados para controlar procesos industriales, son particularmente vulnerables a este tipo de ataque, (PC11-01, 2023).

Phishing y spear phishing: Estas técnicas buscan engañar a los usuarios para que revelen información sensible o instalen malware en los sistemas. Según la Resolución N° 580/2011, este tipo de amenaza es frecuente en sectores como los servicios financieros, donde los ataques dirigidos a empleados pueden comprometer datos críticos.

Ciberespionaje: El ciberespionaje tiene como objetivo acceder de forma no autorizada a información clasificada o estratégica. Este tipo de amenaza es común en sectores gubernamentales y de defensa, el ciberespionaje representa un desafío significativo para la protección de redes críticas en Argentina, (PC11-01, 2023).

El impacto de estas amenazas varía desde interrupciones temporales en los servicios hasta daños permanentes en los sistemas estratégicos. La Resolución N° 829/2019 subraya la necesidad de un enfoque integral que combine medidas preventivas, monitoreo continuo y respuestas rápidas para minimizar las consecuencias de estos ataques. Además, se destaca que

los sectores más afectados en Argentina han sido las telecomunicaciones y el transporte, lo que evidencia la importancia de priorizar la protección de estas áreas, (Dirección Nacional de Ciberseguridad, 2023).

Participación del nivel operacional en la protección de infraestructuras críticas

El nivel operacional en la defensa nacional constituye un componente clave para la implementación de estrategias destinadas a la protección de infraestructuras críticas (IC). Su rol es esencial para traducir las decisiones estratégicas en acciones concretas y efectivas, garantizando la resiliencia de sectores fundamentales como la energía, las telecomunicaciones, el transporte y los servicios salud. En el ámbito del ciberespacio, este nivel lidera la planificación y ejecución de operaciones cibernéticas, integrando capacidades tanto militares como civiles para abordar los desafíos de un entorno dinámico y complejo, (Resolución N° 580/2011), (PC11-01, 2023)

El marco normativo en Argentina, encabezado por la Ley N° 23.554 de Defensa Nacional y el Decreto N° 457/2021, establece la necesidad de articular esfuerzos entre las Fuerzas Armadas y otros actores relevantes para garantizar la protección de las IC. Sin embargo, el desarrollo de la ciberdefensa en este nivel enfrenta desafíos que van desde la identificación de vulnerabilidades hasta la implementación de estrategias tanto defensivas como ofensivas frente a ciberataques sofisticados, (Resolución N° 829/2019).

La protección de las IC en el nivel operacional implica la integración de múltiples acciones y capacidades. Una de sus responsabilidades clave es la coordinación interinstitucional, que busca conectar a las Fuerzas Armadas, las agencias civiles y el sector privado para intercambiar información sobre amenazas y vulnerabilidades. Esta colaboración es esencial para abordar las interdependencias entre sectores críticos y garantizar una respuesta unificada ante incidentes, tal como señala la Resolución N° 580/2011.

Las operaciones a nivel operacional también incluyen la ejecución de estrategias de protección, como el establecimiento de sistemas de monitoreo continuo y la implementación de protocolos de seguridad adaptados a las características específicas de cada infraestructura. Sectores como el energético y el de telecomunicaciones, altamente dependientes de sistemas digitales, se benefician particularmente de estas medidas, que buscan prevenir interrupciones y mitigar riesgos, (PC11-01, 2023).

En caso de un ciberataque, el nivel operacional lidera la gestión de incidentes, incluyendo la contención del ataque, la restauración de los servicios afectados y la implementación de medidas para prevenir futuros incidentes. Estas capacidades defensivas están respaldadas por sistemas de monitoreo en tiempo real y protocolos de actuación diseñados para minimizar el impacto de los ataques. Asimismo, el nivel operacional organiza ejercicios simulados que evalúan la resiliencia de las IC frente a ciberamenazas, permitiendo identificar puntos débiles y mejorar la preparación de los equipos encargados de la defensa cibernética, (Dirección Nacional de Ciberseguridad, 2023).

En cuanto al desarrollo de operaciones cibernéticas, el nivel operacional lidera actividades preventivas, defensivas y ofensivas. Las operaciones preventivas incluyen la identificación de vulnerabilidades, el análisis de tráfico de red y la realización de pruebas de penetración para evaluar la seguridad de los sistemas. Estas medidas proactivas son fundamentales para anticiparse a las ciberamenazas y reducir los riesgos, (PC11-01, 2023). La implementación de tecnologías avanzadas, como sistemas de detección de intrusiones, es una prioridad establecida en la Resolución N° 580/2011.

En las operaciones defensivas, el nivel operacional protege las IC frente a ciberataques en tiempo real mediante la contención de incidentes y la restauración de los servicios afectados. Estas acciones se complementan con medidas adicionales, como la segmentación de redes y el uso de criptografía para proteger información crítica, (PC11-01, 2023)

Las operaciones ofensivas, por su parte, están diseñadas para neutralizar amenazas y desactivar las capacidades del adversario. Estas actividades incluyen la ejecución de ciber efectos destinados a interrumpir comunicaciones enemigas, deshabilitar sistemas de mando y control, y sabotear infraestructuras críticas. Este enfoque es esencial para garantizar la libertad de acción en el ciberespacio y para proteger los intereses estratégicos del Estado, (PC11-01, 2023).

El desarrollo de la ciberdefensa en el nivel operacional enfrenta una serie de desafíos. La interoperabilidad entre actores es un aspecto crítico, ya que la colaboración de múltiples sectores puede verse limitada por diferencias en los sistemas y procesos utilizados. Esto subraya la necesidad de establecer estándares comunes que faciliten la integración de capacidades y recursos (Resolución N° 829/2019). Además, las restricciones legales actuales limitan la participación de las Fuerzas Armadas en ciertos aspectos de la ciberdefensa en el ámbito civil, lo que resalta la importancia de actualizar el marco normativo para adaptarlo a las realidades del ciberespacio, (Decreto N° 457/2021).

La brecha tecnológica es otro desafío significativo. El nivel operacional requiere herramientas avanzadas y tecnologías de última generación para enfrentar las ciberamenazas, pero la falta de inversión en infraestructura tecnológica puede limitar la capacidad de las operaciones cibernéticas. Asimismo, la escasez de personal capacitado en ciberdefensa representa un obstáculo adicional, lo que hace indispensable invertir en la formación y retención de expertos en ciberseguridad, (Dirección Nacional de Ciberseguridad, 2023), (PC11-01, 2023).

El nivel operacional desempeña un papel fundamental en la protección de las IC y en el desarrollo de una ciberdefensa efectiva. Su participación en la coordinación interinstitucional, la ejecución de operaciones cibernéticas y la gestión de incidentes es esencial para garantizar la seguridad de los sistemas estratégicos del Estado. Sin embargo, superar los desafíos actuales requerirá actualizar las normativas, invertir en tecnología y fortalecer las capacidades humanas para enfrentar las ciberamenazas contemporáneas y proteger las infraestructuras críticas que sostienen el funcionamiento de la sociedad.

CONCLUSIONES

La presente investigación demuestra la creciente relevancia de la ciberdefensa en el ámbito de la defensa nacional, especialmente en un contexto global marcado por la digitalización acelerada y las amenazas emergentes del ciberespacio. Argentina, en su esfuerzo por proteger infraestructuras críticas, enfrenta desafíos significativos que comprometen tanto la estabilidad de su sistema de defensa como su soberanía en un entorno cada vez más interdependiente. Este análisis evidencia la necesidad urgente de fortalecer la integración estratégica de la ciberdefensa a través de un marco normativo robusto, la modernización tecnológica y una mayor coordinación interinstitucional.

El ciberespacio requiere doctrinas que integren herramientas tecnológicas avanzadas y capacidades de inteligencia artificial para detectar y neutralizar amenazas. Sin embargo, PC 11-01 (2023), en su capítulo III, las doctrinas tradicionales suelen centrarse en infraestructuras físicas y estrategias convencionales, lo que deja un vacío en la preparación para amenazas cibernéticas. señala que esta brecha tecnológica es especialmente crítica en sectores como energía y telecomunicaciones, donde los sistemas SCADA son vulnerables a ataques avanzados.

El análisis normativo resalta cómo los marcos regulatorios actuales, aunque avanzados en comparación con años anteriores, aún presentan vacíos críticos que dificultan una respuesta integral a las ciberamenazas. Instrumentos como el Decreto N.º 457/2021 y la Ley N.º 23.554 de Defensa Nacional proporcionan una base, pero deben complementarse con enfoques más dinámicos que respondan a la naturaleza cambiante del ciberespacio. La falta de cohesión entre las normativas y las capacidades operativas limita el desarrollo de políticas efectivas y sostenibles para proteger las infraestructuras estratégicas.

Para abordar los puntos en conflicto y alinear la doctrina de defensa nacional con las demandas del ciberespacio, es imperativo llevar a cabo una serie de reformas estratégicas. En primer lugar, se debe revisar y actualizar el marco normativo vigente, adaptando las leyes y resoluciones existentes para otorgar una mayor flexibilidad y proactividad en la ciberdefensa, lo que permitirá responder con eficacia ante las amenazas cibernéticas emergentes. Además, resulta crucial promover la colaboración interinstitucional, estableciendo mecanismos formales que faciliten la cooperación entre las Fuerzas Armadas, las agencias civiles y el sector privado, dado que la ciberseguridad es un esfuerzo colectivo que debe involucrar a múltiples actores. Complementariamente, es esencial invertir en el fortalecimiento de las capacidades

tecnológicas de la ciberdefensa, priorizando la adopción de tecnologías avanzadas como sistemas de inteligencia artificial y monitoreo en tiempo real, tal como se estipula en la Resolución N° 580/2011, lo que permitirá mejorar la detección y respuesta ante ciberataques. Por último, es necesario que se considere las particularidades de este dominio, priorizando la flexibilidad operativa y la capacidad de respuesta rápida para hacer frente a los desafíos que plantea un entorno digital en constante cambio.

En el nivel operacional, destaca el papel central del Comando Conjunto de Ciberdefensa en la identificación y mitigación de riesgos. Sin embargo, este organismo necesita mayores recursos, formación especializada y herramientas tecnológicas de última generación para abordar con eficacia las amenazas complejas y transnacionales que caracterizan el ciberespacio contemporáneo. El estudio subraya la importancia de integrar doctrinas militares adaptadas al contexto cibernético, fortaleciendo así la capacidad de las Fuerzas Armadas para anticipar, detectar y responder a ciberataques de manera coordinada con otros actores estatales y privados.

La determinación de las IC y su protección mediante la ciberdefensa son elementos esenciales para garantizar la seguridad nacional y la estabilidad de un país. En Argentina, el marco normativo y los procesos establecidos proporcionan una base sólida para identificar y priorizar los activos estratégicos. Sin embargo, el creciente número de ciberamenazas y la dependencia de las TIC subrayan la necesidad de reforzar las capacidades de ciberdefensa y fomentar la cooperación interinstitucional e internacional. Este enfoque integral no solo protege las IC, sino que también fortalece la resiliencia del Estado frente a los desafíos del ciberespacio.

La ciberdefensa juega un papel central en la identificación y protección de las infraestructuras críticas. Las agencias de ciberdefensa, con sus herramientas y metodologías avanzadas, lideran los esfuerzos para identificar vulnerabilidades y mitigar riesgos en un entorno de amenazas crecientes. Sin embargo, la protección de las IC no puede lograrse sin una estrecha coordinación entre las Fuerzas Armadas y las agencias civiles. Esta colaboración, respaldada por un marco normativo sólido y un enfoque interinstitucional, es esencial para garantizar la resiliencia y seguridad de los activos estratégicos que sostienen el funcionamiento del Estado y la sociedad.

Por otra parte, la protección de infraestructuras críticas como la energía, las telecomunicaciones, el transporte y salud requiere no solo de capacidades técnicas avanzadas, sino también de una colaboración efectiva entre agencias gubernamentales y el sector privado. Las interdependencias entre estos sectores amplifican los riesgos, haciendo indispensable un enfoque multisectorial que optimice los recursos y garantice la resiliencia de los sistemas nacionales.

A pesar de los avances logrados en la coordinación interinstitucional, persisten desafíos significativos que requieren atención para fortalecer la ciberdefensa nacional. Entre estos desafíos se encuentra la falta de interoperabilidad, ya que las diferencias en los sistemas y procesos utilizados por las agencias civiles y militares dificultan una colaboración efectiva; como señala el PC 11-01 (2023), es fundamental desarrollar estándares comunes que faciliten la integración de capacidades. Además, existen limitaciones legales que restringen la participación de las Fuerzas Armadas en operaciones de ciberdefensa en el ámbito civil, lo que resalta la necesidad urgente de actualizar el marco normativo para adaptarlo a las realidades dinámicas del ciberespacio, tal como lo indica la Resolución N° 1523/2019. Por último, la escasez de talento especializado en ciberseguridad y ciberdefensa representa un obstáculo crítico para la implementación efectiva de estrategias conjuntas, lo que subraya la importancia de invertir en la formación y retención de profesionales capacitados, tal como se destaca en el Informe CERT.ar de las Dirección Nacional de Ciberseguridad (2023), para garantizar la resiliencia y efectividad de las políticas de defensa en este ámbito.

La evaluación de riesgos y amenazas cibernéticas a las infraestructuras críticas es fundamental para garantizar la seguridad nacional y la resiliencia frente a incidentes. En Argentina, los sectores estratégicos enfrentan desafíos significativos debido a la creciente sofisticación de las ciberamenazas y la interdependencia de las redes digitales. Aprender de casos internacionales, como los ataques a la red eléctrica de Ucrania o al oleoducto Colonial Pipeline, permite identificar vulnerabilidades y diseñar estrategias de protección más efectivas. La colaboración entre agencias gubernamentales, las Fuerzas Armadas y el sector privado es esencial para enfrentar estos desafíos y fortalecer la capacidad del país para proteger sus IC frente a un entorno de amenazas en constante evolución.

En conclusión, el trabajo resalta la urgencia de redefinir la incumbencia de la ciberdefensa en la Argentina, reconociéndola como un pilar esencial de la defensa nacional en el nivel operacional. A través de una combinación de análisis normativo, evaluaciones operativas y estrategias cooperativas, se sientan las bases para un sistema de ciberdefensa más resiliente y eficaz. Este enfoque no solo fortalecerá la capacidad del país para enfrentar las amenazas actuales, sino que también contribuirá a garantizar la seguridad de las infraestructuras críticas y, en última instancia, la soberanía del Estado argentino en el ciberespacio.

BIBLIOGRAFÍA

Aguerre, G. B. (2021). *Políticas públicas sobre ciberseguridad en América Latina: el caso de Argentina.* Ciudad de Mexico: Centro Latam Digital. Obtenido de https://centrolatam.digital/wp-content/uploads/2022/05/Reporte_ciberseguridad-en-argentina.pdf

BARETTO, J. F. (2017). La Defensa Nacional y la Estrategia Militar de Seguridad Cibernetica. República Argentina: Escuela Superior de Guerra Conjunta.

Casale, C. G. (2022). *La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el Nivel Operacional(Trabajo Fianl Integrador).* CABA: Escuela superior de Guerra.

Corbacho, A. L. (2011). *EVOLUCIÓN DEL PENSAMIENTO ESTRATÉGICO EN LAS RELACIONES INTERNACIONALES.* Buenos Aires, Argentina: UNIVERSIDAD DEL CEMA.

CR (R) Dr Justino Bertotto, G. B. (Sep de 2018). EPISTEMOLOGÍA Y ARTE DE LA ESTRATEGIA. Ciudad Autonoma de Buenos Aires, Argentina: Escuela Superior de Guerra.

Decisión Administrativa N° 641/2021. (s.f.). *Requisitos mínimos de Seguridad Informática Organismos Públicos*. República Argentina.

Decreto N° 11.856/2023. (s.f.). *Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad.* República Federativa de Brasil.

Decreto N° 457. (6 de Julio de 2021). *Directiva Politica de Defensa Nacional*. República Argentina.

Decreto N° 457/2021. (s.f.). *Directiva Politica de Defensa Nacional*. República Argentina.

Decreto N° 480/2019. (s.f.). *Modificación del Decreto N° 577/17*. República Argentina.

Decreto N° 577/2017. (s.f.). *Comité de Ciberseguridad*. República Argentina.

Decreto N° 703/2018. (s.f.). *Directiva de Poitica de Defensa Nacional*. República Argentina.

Dirección Nacional de Ciberseguridad. (2023). *Incidentes Informáticos.* Ciudad Autónoma de Buenos Aires: Dirección Nacional de Ciberseguridad, CERT.ar.

Disposición N° 1 CERT.ar Centro Nacional de Respuesta a Incidentes Informáticos. (21 de junio de 2021). *Jefatura de Gabinetes de Ministros*. República Argentina.

Disposición N°6 Comité Asesor para el desarrollo e implementación de aplicaciones seguras. (8 de abril de 2021). *Direccion Nacioanl de Ciberseguridad*. República Argentina.

Durán, J. D. (2011). La ciberdefensa en el ámbito militar. *Cuadernos de Estrategia ISSN N° 149*, 215-256.

Fernando Morales. (8 de Julio de 2024). Infobae. *Qué es y cómo funciona el Comando de Ciberdefensa, el equipo militar que actúa ante los ataques al sistema informático*

nacional. Obtenido de https://www.infobae.com/politica/2022/03/26/que-es-y-como-funciona-el-comando-de-ciberdefensa-el-equipo-militar-que-actua-ante-los-ataques-al-sistema-informatico-nacional/#:~:text=Tiene%20la%20responsabilidad%20de%20implementar,que%20deban%20ser%20inmedia

Fonseca, C. E., Perdomo, I. L., Gratacos, M., & Ortiz, J. U. (2014). El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra. *Revista ESG, 588*, 127-145.

Forbes Centroamerica. (10 de Abril de 2024). *Ciberseguridad, ciberdefensa y ciberespacio, los retos de Latinoamérica*. Obtenido de https://forbescentroamerica.com/2024/04/10/ciberseguridad-ciberdefensa-y-ciberespacio-los-retos-de-latinoamerica-dice-ceo-de-indra

GD (R) Eduardo A. Lugani, T. (. (2023). *El rol estratégico del Ejército Argentino para el desarrollo de la estrategia militar de disuasión convencional.* Cuidad Autonoma de Buenos Aires: Escuela Superior de Guerra.

Guerra, E. S. (s.f.). Bases para el pensamiento estrategico. Ciudad de Buenos Aires, Argentina: Escuela Superior de Guerra.

https://www.celag.org/que-esperar-de-las-relaciones-de-ee-uu-con-america-latina-para-2024/. (2024).

Intini, A. L. (15 de Nov de 2020). La ciberdefensa: avanzando de cara al futuro. *Infobae*, págs. https://www.infobae.com/opinion/2020/11/15/la-ciberdefensa-avanzando-de-cara-al-futuro/.

Jefatura de Gabinete de Ministros. (2024). *Argentina.gob.ar*. Obtenido de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad

Ley 23554. (13 de Abril de 1988). *Ley de Defensa Nacional*. CABA, Republica Argentina.

Lucía Alejandra Destro, E. d. (2014). *Los escritos académocos de la formación militar. Guía didactica para su Elaboración y Redacción.* (L. A. Destro, Ed.) CABA: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Ministerio de Defensa. (30 de Enero de 2023). *Argentina.gob.ar*. Obtenido de https://www.argentina.gob.ar/noticias/actualizacion-de-la-politica-de-ciberdefensa-y-creacion-de-dos-areas-para-la-supervision-y

Ministerio de Defensa. (25 de Septiembre de 2023). Defensa realizó las jornadas de reflexión y pensamiento nacional sobre inteligencias artificiales y ciberdefensa. *Argentina.gob.ar*. Obtenido de https://www.argentina.gob.ar/noticias/defensa-realizo-las-jornadas-de-reflexion-y-pensamiento-nacional-sobre-inteligencias

Niss, C. d. (2023). *Ciberdefensa y el ciclo evolutivo del ciberespacio.* CABA, Argentina: UNDEF libros.

Ottis, R. (2007). Análisis de los ataques cibernéticos de 2007 contra Estonia. *Centro de Excelencia Cooperativo de Defensa Cibernética, Tallin, Estonia* .

PC00-01. (2012). Doctrina básica para la acción militar conjunta. Republica Argentina.

PC11-01. (2023). Reglamento de Ciberdefensa y Guerra Electrónica para la Acción Militar Conjunta. Republica Argentina.

PC20-01. (2017). PLANEAMIENTO PARA LA ACCIÓN MILITAR CONJUNTA NIVEL OPERACIONAL. Republica Argentina.

Resolución N° 781/2015. (s.f.). *Políticas de Seguridad de la Información*. Republica Argentina.

Resolución N° 1380. (25 de Octubre de 2019). *Resolución Ministerio de Defensa*. Republica Argentina.

Resolución N° 1380/2019. (s.f.). *Resolución Ministerio de Defensa*. Republica Argentina.

Resolución N° 141/2019. (s.f.). *Jefatura de Gabinete de Ministros*. República Argentina.

Resolución N° 580/2011. (s.f.). *Programa Nacional de IICC*. República Argentina.

Resolución N° 75/2022. (s.f.). *Plan Federal de prevención de delitos tecnologicos y ceberdelitos*. República Argentina.

Resolución N° 829/2019. (s.f.). *Estrategia Nacional de Ciberseguridad*. República Argentina.

Resolución N°1523/2019. (s.f.). *Infraestructuras Críticas e Infraestructuras Críticas de Información y Glosario Terminología Ciberseguridad*. República Argentina.

Revista ESG. (2014). El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra. (C. E. Fonseca, I. L. Perdomo, M. Gratacos, & J. U. Ortiz, Edits.) *Revista ESG, 588*, 127-145.

Rivas, S. (2 de Agosto de 2022). La ciberdefensa desde adentro. *Pucara.org*. Obtenido de https://www.pucara.org/post/la-ciberdefensa-desde-adentro-hablamos-con-el-gral-an%C3%ADbal-intini-cdte-conjunto-de-ciberdefensa

Taverna, A., & Rutz, G. (2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. *Revista Defensa Nacional*, 171-186. Obtenido de https://www.undef.edu.ar/libros/wp-content/uploads/2022/02/06_DIGITAL.pdf

Vega, J. M. (16 de Marzo de 2023). *Realinstitutoelcano.org*. Obtenido de https://www.realinstitutoelcano.org/analisis/el-sector-de-ciberseguridad-en-america-latina-apuntes-para-leer-un-mapa-del-estado-en-construccion/

Vercelli, S., & Cornaglia, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *Revista Latinoamericana de Estudios de Seguridad*, 1-18. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/2601/1606

Vergara, E. d., & Trama, G. A. (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional.* Ciudad Autónoma de Buenos Aires: Editorial Visión Conjunta, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Wall, A. E. (2011). Demystifying the Title 10-Title 50 Debate. *Presidents and Fellows of Harvard College*, 85-142.

Wallace, D. A., & Reeves, S. R. (Febrero de 2020). Protecting Critical Infrastructure in Cyber Warfare. *University of California, Davis*, 1607-1641.

World Economic Forum. (2 de Mayo de 2024). *Lecciones de ciberseguridad de la batalla de América Latina contra las amenazas de ransomware*. Obtenido de https://es.weforum.org/agenda/2024/05/lecciones-de-ciberseguridad-de-la-batalla-de-america-latina-contra-las-amenazas-de-ransomware/

Zona Militar. (14 de Octrubre de 2024). Obtenido de https://www.zona-militar.com/2024/10/15/con-foco-en-fortalecer-sus-capacidades-de-ciberseguridad-las-fuerzas-armadas-brasilenas-realizan-el-ejercicio-cyber-guardian-6-0/