INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS
DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

"CIBERSEGURIDAD Y SOBERANÍA DIGITAL EN ARGENTINA: EL ROL DEL ESTADO EN LA PROTECCIÓN DE LA INFRAESTRUCTURA DIGITAL"

GRUPO N° 10

BARBOZA MARTÍN
PUGLIARA GUILLERMO ARIEL
TERRIBILE GILES JUAN MARTIN
MAMANI ESTEBAN MAXIMILIANO

TÍTULO PROFESIONAL / GRADO

LICENCIADO EN CONDUCCIÓN Y GESTIÓN OPERATIVA
LICENCIADO EN SISTEMAS AÉREOS Y AEROESPACIALES
LICENCIADO EN RECURSOS NAVALES PARA LA DEFENSA
LICENCIADO EN GESTIÓN Y SEGURIDAD DE LAS TICS

Índice General

1. Resumen del Proyecto

El estudio destaca los desafíos que enfrenta Argentina en la protección de su ciberseguridad y soberanía digital, debido a la falta de una delimitación jurisdiccional clara en el ciberespacio. Además, propone la creación de un Ministerio del Ciberespacio en Argentina, un organismo centralizado dedicado a la protección de la ciberseguridad y la soberanía digital del país. La propuesta responde a la creciente dependencia de tecnologías digitales y la necesidad de una estructura institucional robusta que coordine los esfuerzos de ciberdefensa a nivel nacional. Argentina enfrenta desafíos en la protección de sus infraestructuras críticas y en la regulación de actividades digitales, especialmente ante amenazas transnacionales y la falta de un marco jurídico adecuado que garantice la seguridad y privacidad de sus datos.

A través de un análisis comparativo de prácticas internacionales, se observa cómo otros países, como Brasil, España e Israel, han estructurado sus políticas de ciberdefensa mediante enfoques centralizados y colaborativos. Estos modelos destacan la importancia de integrar la defensa de infraestructuras críticas y la cooperación público-privada bajo una entidad específica. En este contexto, el Ministerio del Ciberespacio en Argentina tendría la autoridad para gestionar y coordinar todas las actividades relacionadas con la ciberseguridad nacional, implementar un sistema de identidad digital seguro y establecer normativas de protección de datos y privacidad, alineándose con marcos internacionales como la Convención de Budapest.

El proyecto también enfatiza la importancia de formar capital humano especializado en ciberseguridad y de retener talento dentro del ámbito público para reducir la dependencia de servicios extranjeros. Además, el Ministerio actuaría como un ente facilitador de la cooperación internacional en ciberdefensa, promoviendo acuerdos de inteligencia con aliados estratégicos y mejorando la respuesta del país ante amenazas globales.

En conclusión, este proyecto plantea que la creación del Ministerio del Ciberespacio fortalecería la soberanía digital de Argentina, mejoraría la seguridad de sus infraestructuras críticas y consolidaría su posición en el ámbito de la ciberseguridad regional.

2. Justificación/Fundamentación/Aportes

La ciberseguridad y la soberanía digital se han convertido en prioridades fundamentales para los Estados en todo el mundo, incluida Argentina. La creciente interdependencia de las infraestructuras digitales, la expansión de la conectividad global y el uso cada vez mayor de tecnologías avanzadas como la inteligencia artificial y el Internet de las Cosas (IoT) han generado nuevos desafíos de seguridad que requieren respuestas adaptativas y eficientes. Estas respuestas deben incluir tanto medidas de protección de la infraestructura digital como la salvaguarda de los derechos y la soberanía de los ciudadanos y el Estado en el ciberespacio.

En el caso de Argentina, la falta de un marco institucional adecuado, junto con las dificultades en la regulación del ciberespacio y la delimitación de jurisdicciones, subrayan la necesidad urgente de adoptar un enfoque estructurado y coordinado para abordar los desafíos de la ciberseguridad y la soberanía digital. La protección de las infraestructuras críticas digitales del país y la defensa de su espacio cibernético frente a amenazas transnacionales se han convertido en temas de alta prioridad para la seguridad nacional.

La creación de un ministerio del ciberespacio se presenta como una respuesta innovadora y fundamental para consolidar la autoridad del Estado argentino en el entorno digital. Este organismo centralizará la supervisión y gestión de las redes cibernéticas del Estado, permitiendo una respuesta ágil y eficaz ante incidentes, al tiempo que impulsa la cooperación internacional y el desarrollo de un robusto marco normativo en materia de ciberseguridad, privacidad y protección de datos.

Además, el Ministerio del Ciberespacio tendría un papel crucial en la generación de capital humano altamente especializado y en la retención de talento dentro del sector público, aspectos clave para garantizar la resiliencia y efectividad de las capacidades de ciberdefensa del país. La apuesta por el desarrollo de conocimientos y habilidades en ciberseguridad, en conjunto con la implementación de un sistema de identidad digital seguro, permitiría a Argentina fortalecer significativamente la protección de su soberanía digital y reducir su vulnerabilidad ante ciberamenazas transnacionales.

La justificación de este proyecto radica en la necesidad imperiosa de contar con un enfoque estructural y coordinado para la ciberseguridad y defensa del ciberespacio argentino. Esto permitiría al Estado ejercer un control efectivo sobre sus infraestructuras críticas digitales y la actividad cibernética de sus ciudadanos, empresas y organismos públicos, salvaguardando así su soberanía en el entorno digital en un contexto de crecientes amenazas y vulnerabilidades.

3. Planteamiento del Problema

3.1 Título:

La Dificultad de Delimitar la Jurisdicción en el Ciberespacio y su Impacto en la Ciberseguridad y Soberanía Digital de Argentina

Planteamiento del Problema:

La naturaleza global del ciberespacio y la falta de fronteras claras para determinar jurisdicciones plantea múltiples desafíos para los Estados en la defensa de su ciberseguridad y soberanía digital. Argentina, al igual que otros países, enfrenta la compleja tarea de ejercer control y protección sobre su infraestructura digital en un entorno que no respeta las fronteras geográficas convencionales. Los principales problemas en torno a la falta de delimitación jurisdiccional pueden detallarse en los siguientes ámbitos:

a. Ámbito Internacional y los Tratados Multilaterales

- **Conflictos de Jurisdicción**: La mayoría de los ataques y operaciones cibernéticas provienen de ubicaciones fuera del territorio nacional, lo cual genera una indefinición en cuanto a la jurisdicción aplicable y dificulta la cooperación internacional. Pese a la adhesión a tratados como la Convención de Budapest sobre ciberdelincuencia, la ausencia de un consenso global sobre cómo delimitar la jurisdicción en el ciberespacio complica la persecución de los ciberdelitos transnacionales.
- **Limitaciones de los Tratados actuales**: Aunque existen acuerdos que buscan regular el cibercrimen y establecer mecanismos de cooperación, su efectividad es limitada debido a la falta de adhesión de ciertos países y a la interpretación variable de los mismos. Esto restringe la capacidad de Argentina para perseguir y mitigar ataques originados fuera de sus fronteras.
- **Dependencia de Organismos Internacionales**: La participación en organizaciones como la OEA y la ONU permite cierta colaboración en ciberdefensa, pero sin un marco definido de jurisdicción en el ciberespacio, estas alianzas se ven limitadas a un nivel de cooperación teórico, sin capacidad de ejecución real sobre eventos cibernéticos transfronterizos.

b. Ámbito Nacional y el Marco Legal Interno

- **Desafíos en la Aplicación de las Leyes Nacionales de Ciberseguridad**: En ausencia de fronteras digitales claras, las leyes nacionales de ciberseguridad y de protección de datos en Argentina, como la Ley de Protección de Datos Personales, enfrentan limitaciones al aplicarse en el contexto global del ciberespacio. La ambigüedad en cuanto a la jurisdicción genera problemas en la identificación de responsabilidades y en la aplicación efectiva de sanciones.
- **Lagunas en la Legislación Nacional**: El marco legal argentino aún no contempla plenamente las particularidades de la soberanía digital, lo que impide establecer medidas específicas de protección de infraestructuras críticas en un entorno globalizado. Sin un marco que abarque la jurisdicción en el ciberespacio, los operadores de infraestructuras críticas no tienen parámetros claros para actuar ante amenazas cibernéticas de origen externo.
- **Escasa Adaptación a Normas Internacionales**: A pesar de los esfuerzos de adaptación, las normativas nacionales están desfasadas en relación con los estándares internacionales en ciberseguridad, lo cual afecta la cooperación efectiva y dificulta el ejercicio de una jurisdicción nacional coherente en el ciberespacio.

c. Ámbito Operativo y las Capacidades Nacionales de Respuesta

- **Deficiencias en la Coordinación Nacional**: La falta de una delimitación jurisdiccional clara dificulta la coordinación entre las diversas instituciones nacionales encargadas de la ciberseguridad, tanto en el ámbito civil como en el militar. Esta carencia afecta la capacidad del país para desarrollar respuestas ágiles y efectivas frente a amenazas cibernéticas transnacionales.
- **Capacidades Técnicas Limitadas para la Identificación y Atribución de Ataques**: Sin una infraestructura operativa avanzada, la capacidad de Argentina para identificar y atribuir ataques cibernéticos de origen extranjero es limitada. La atribución precisa de estos incidentes es fundamental para una respuesta efectiva, pero en el contexto actual, el país carece de las herramientas y de la tecnología para superar la barrera jurisdiccional.
- **Dependencia de Infraestructura Tecnológica Extranjera**: Argentina depende en gran medida de servicios tecnológicos extranjeros para gestionar y proteger su infraestructura digital. Esto implica una pérdida de control sobre los datos y sistemas críticos, comprometiendo su soberanía digital y exponiendo su infraestructura a riesgos que escapan de su control jurídico.

d. Ámbito Colectivo de Respuesta y Soberanía Digital

- **Falta de un Mecanismo Colectivo de Respuesta ante Ciberataques en Latinoamérica**: Aunque existen esfuerzos regionales para mejorar la cooperación en ciberseguridad, la falta de un mecanismo efectivo y unificado en América Latina limita las capacidades colectivas para enfrentar amenazas transnacionales. Sin una delimitación jurisdiccional, los países de la región tienen dificultades para coordinar respuestas rápidas y eficientes frente a incidentes de ciberseguridad.
- **Desafíos en la Protección de Infraestructuras Críticas Compartidas**: Algunas infraestructuras digitales, como redes de comunicación y servicios en la nube, son compartidas con otros países de la región. La ausencia de jurisdicción clara en el ciberespacio complica la protección de estos sistemas y afecta la soberanía digital argentina, dado que la seguridad de estos recursos depende también de la respuesta de terceros.
- **Ambigüedad en los Mecanismos de Respuesta Colectiva**: A nivel global, la ambigüedad jurisdiccional también complica los mecanismos de respuesta colectiva ante amenazas estatales o de actores no estatales. Esto es especialmente crítico en el caso de ciberataques contra infraestructuras militares y de inteligencia, ya que las respuestas suelen depender de tratados internacionales y, sin un ámbito jurisdiccional claro, Argentina carece de garantías para una acción coordinada.

e. Ámbito de Capacitación y Especialización en Ciberseguridad

- **Deficiencia en la Formación Especializada en Ciberseguridad**: En Argentina, la formación en ciberseguridad enfrenta múltiples desafíos. Existen limitaciones en la oferta educativa y en los programas de capacitación técnica avanzada, lo cual reduce la disponibilidad de profesionales capacitados para enfrentar las complejas amenazas del ciberespacio. Esta carencia impacta directamente en la capacidad del país para desarrollar una estrategia de ciberdefensa sólida y coordinada.
- **Escasez de Políticas de Retención en el Sector Estatal**: A pesar de la necesidad creciente de profesionales especializados en ciberseguridad, el sector estatal carece de políticas efectivas para retener a estos expertos. La falta de incentivos y de un plan de carrera adecuado dentro de las instituciones públicas fomenta la migración de talentos hacia el sector privado o al exterior, donde las condiciones laborales y salariales son más competitivas. Esto debilita la capacidad estatal para proteger la infraestructura digital crítica y dificulta la consolidación de un equipo nacional de ciberseguridad.

- **Insuficiente Colaboración Académico-Gubernamental**: La conexión entre las instituciones académicas y las necesidades del sector gubernamental en ciberseguridad es limitada, lo cual resulta en una escasa alineación entre la formación académica y las competencias requeridas en la práctica para la defensa del ciberespacio argentino. La falta de programas y becas específicas orientadas a la ciberseguridad en el ámbito estatal profundiza este problema, limitando el desarrollo de expertos que puedan aportar a la ciberseguridad nacional.

3.1 Conclusión del Problema

En conclusión, la protección de la soberanía digital y la ciberseguridad de Argentina enfrenta una serie de desafíos complejos y multifacéticos. La falta de delimitación clara de jurisdicción en el ciberespacio limita la capacidad del Estado para aplicar sus normativas nacionales y participar de manera efectiva en los esfuerzos de cooperación internacional y regional. Sin un marco jurisdiccional definido, se dificulta la aplicación de leyes y tratados vigentes, y se reducen las posibilidades de respuesta ante incidentes transnacionales que afectan a infraestructuras críticas.

Además, las capacidades operativas de ciberdefensa se ven restringidas por la dependencia de infraestructura tecnológica extranjera y por una falta de inversión en tecnologías propias que aseguren un mayor control sobre la seguridad nacional. Esta limitación operativa se agrava con la escasez de profesionales capacitados en ciberseguridad dentro del ámbito estatal y la carencia de políticas efectivas de retención de talento, que debilitan la capacidad de respuesta y coordinación ante ciberataques.

La inexistencia de programas especializados y de incentivos adecuados para la formación y permanencia de estos profesionales en el sector público representa una amenaza para la estabilidad y seguridad de las infraestructuras digitales del país. Estos problemas demandan una revisión exhaustiva y estructural de los enfoques nacionales en materia de ciberseguridad, con la integración de políticas que permitan tanto una mejor definición de los límites jurisdiccionales en el ciberespacio como una estrategia integral de capacitación y retención del talento en el ámbito estatal.

En un contexto global donde la soberanía digital es cada vez más vulnerable, Argentina debe afrontar estos desafíos con una visión estratégica y adaptativa, promoviendo una defensa eficaz de su infraestructura crítica y su integridad en el ciberespacio.

4. Hipótesis o Solución Propuesta

Propuesta para la Creación del "Ministerio del Ciberespacio" en Argentina

4.1 Contextualización del Problema

En el contexto actual, la ciberseguridad y la soberanía digital se han convertido en prioridades críticas para los Estados en todo el mundo, incluyendo a Argentina. La creciente interdependencia de las infraestructuras digitales, la expansión de la conectividad global y el uso de tecnologías avanzadas como la inteligencia artificial y el Internet de las Cosas (IoT), junto con las crecientes amenazas cibernéticas, plantean nuevos desafíos. Estos desafíos, a su vez, requieren respuestas adaptativas y eficientes que incluyen tanto medidas de seguridad digital como de protección de los derechos y la soberanía de los ciudadanos y el Estado.

En este contexto, la falta de un marco institucional adecuado, junto con dificultades en la regulación del ciberespacio y la jurisdicción sobre actividades digitales, subraya la necesidad de crear un organismo centralizado que articule los esfuerzos de ciberseguridad en Argentina. Un Ministerio del Ciberespacio sería el paso fundamental para abordar estos desafíos desde una perspectiva de seguridad nacional.

4.2 Funciones y Autoridad Transversal del Ministerio del Ciberespacio

El Ministerio del Ciberespacio sería una nueva entidad con competencias transversales sobre todos los sectores gubernamentales, encargada de coordinar, regular y gestionar las actividades relacionadas con la ciberseguridad y la protección digital.

- Responsabilidad centralizada: Este ministerio tendría la autoridad exclusiva para supervisar y gestionar todas las redes cibernéticas del Estado. Esto incluiría tanto las infraestructuras críticas como los sistemas de información que soportan servicios esenciales para el funcionamiento del país, tales como el suministro de energía, comunicaciones, transporte y salud. Esta autoridad le permitiría a la entidad coordinar la resolución de incidentes cibernéticos en tiempo real, activando protocolos de respuesta rápida ante ciberataques y colaborando estrechamente con otros ministerios como Defensa y Seguridad.
- Desarrollo y gestión de políticas públicas: El ministerio sería responsable de crear y mantener un marco normativo robusto en materia de ciberseguridad, privacidad y protección de datos. Además, fomentaría el cumplimiento de estándares internacionales en ciberseguridad, garantizando que Argentina esté alineada con acuerdos internacionales como la Convención de Budapest sobre delitos cibernéticos y la Agenda de Ciberseguridad de la ONU, entre otros tratados relevantes.

- Coordinación con otros ministerios y organismos internacionales: Este ministerio actuaría como el nexo principal para la cooperación nacional e internacional en ciberseguridad. Promovería acuerdos bilaterales y multilaterales con países aliados para el intercambio de inteligencia sobre amenazas cibernéticas y el establecimiento de procedimientos comunes en la lucha contra la ciberdelincuencia transnacional.

4.3 Regulación de Identidades Cibernéticas y Seguridad Digital

Una de las propuestas más innovadoras y necesarias del Ministerio del Ciberespacio sería la regulación de las identidades cibernéticas de los ciudadanos, empresas y organismos públicos. En la actualidad, el anonimato en el ciberespacio contribuye a la proliferación de actividades ilegales como el cibercrimen, el fraude y los ataques a infraestructuras críticas.

- Sistema de identidad digital: El ministerio podría implementar un sistema de identidad digital único que registre a cada persona en el ciberespacio bajo un número identificatorio único. Este sistema podría estar vinculado al Documento Nacional de Identidad (DNI) y contener información básica sobre el ciudadano, garantizando que todos los usuarios sean identificados de forma fehaciente.
- Autenticación fuerte con biometría: Para garantizar la seguridad en las transacciones electrónicas y el acceso a sistemas sensibles, el sistema de identidad digital utilizará doble autenticación con datos biométricos (huella digital, reconocimiento facial, etc.). Esto mejoraría la protección de datos personales y la verificación de identidad, asegurando que solo las personas autorizadas puedan acceder a los recursos críticos.
- Nuevas leyes sobre la privacidad y datos personales: La implementación de este sistema requeriría la creación de nuevas leyes que modifiquen o completen la Ley de Protección de Datos Personales (Ley 25.326). Si bien esta modificación podría entrar en conflicto con la protección de la privacidad de los ciudadanos, sería esencial que se establecieran mecanismos de control y transparencia sobre el uso de los datos personales, garantizando su protección frente a accesos no autorizados.

4.4 Capacitación y Formación Profesional en Ciberseguridad

Uno de los problemas más importantes que enfrenta Argentina es la falta de capacitación en ciberseguridad y la escasez de personal altamente especializado en este campo. Esta carencia afecta tanto a los organismos públicos como a las empresas privadas, creando vulnerabilidades en las infraestructuras digitales.

- Generación de capital humano especializado: El Ministerio del Ciberespacio debería fomentar, en colaboración con el Ministerio de Educación, la creación de carreras de grado y posgrado en ciberseguridad, incluyendo programas académicos centrados

en protección de infraestructuras críticas, inteligencia cibernética, tecnologías emergentes como la inteligencia artificial aplicada a la ciberseguridad, y la gestión de incidentes. Además, el ministerio podría promover programas de capacitación continua para profesionales en el campo, asegurando que el personal gubernamental se mantenga actualizado frente a las amenazas emergentes.

- Incentivos para retención de talento: Para resolver el problema de la fuga de talento hacia el sector privado, el ministerio podría crear incentivos salariales y beneficios adicionales para aquellos profesionales que se comprometan a trabajar en el ámbito público. Esto contribuiría a fortalecer las capacidades locales de ciberdefensa y disminuir la dependencia de servicios extranjeros.

4.5 Impacto en la Soberanía Digital

La creación de un Ministerio del Ciberespacio y la implementación de un sistema robusto de identificación digital y ciberseguridad serían fundamentales para fortalecer la soberanía digital de Argentina. Este enfoque permitiría al país tener control absoluto sobre sus infraestructuras digitales, datos personales y actividades cibernéticas, evitando la influencia de actores externos que puedan vulnerar la soberanía de la nación.

Protección frente a amenazas extranjeras: A través de la cooperación internacional y la capacitación de recursos humanos, Argentina podría afrontar mejor las amenazas cibernéticas transnacionales, como ataques de actores estatales o no estatales, que buscan obtener acceso no autorizado a datos sensibles o alterar la infraestructura crítica del país.

Estudio comparativo de marcos y prácticas internacionales: Para fundamentar esta propuesta, se realizó un análisis comparativo de modelos internacionales en ciberdefensa, que incluye el modelo brasileño de ciberdefensa (CDCiber), la Estrategia de Ciberseguridad Nacional de España y las capacidades avanzadas de Israel. Estos países proporcionan ejemplos valiosos en términos de centralización, defensa en profundidad y colaboración público-privada. Brasil destaca por su enfoque de coordinación centralizada en la protección de infraestructuras críticas; España subraya la importancia de la colaboración público-privada para implementar políticas de seguridad efectivas; e Israel aporta una visión innovadora de defensa en capas y de integración entre el sector público y privado. Este análisis se presenta en el **Marco Teórico Preliminar** como **Tabla 1**, y permite observar cómo una estructura institucional robusta y centralizada podría beneficiar a Argentina, a través de un Ministerio del Ciberespacio que asegure su soberanía digital y la protección de sus activos críticos en el ciberespacio.

4.6 Conclusión de la Hipótesis de Solución:

La dificultad para delimitar la jurisdicción en el ciberespacio es, sin lugar a dudas, uno de los principales obstáculos para la protección de la soberanía digital y la ciberseguridad en Argentina. Como se ha analizado, la falta de un marco jurisdiccional claro impide que el Estado ejerza de manera efectiva su autoridad sobre las redes cibernéticas, dificultando la aplicación de normativas nacionales, la participación en cooperación internacional y la gestión de incidentes transnacionales que afectan a infraestructuras críticas.

En este contexto, la creación de un Ministerio del Ciberespacio se presenta como una respuesta estructural y efectiva. Este organismo permitiría al Estado argentino consolidar su autoridad cibernética transversal, promoviendo un marco jurisdiccional definido y actuando como un ente coordinador para la protección de la soberanía digital. A través de este ministerio, Argentina podría mejorar su cooperación internacional, estableciendo acuerdos específicos sobre la jurisdicción cibernética y la gestión de incidentes, de acuerdo con los tratados internacionales y la legislación vigente.

Además, el Ministerio del Ciberespacio podría abordar otro desafío crítico: la falta de capacitación especializada en ciberseguridad. Implementando políticas educativas y creando programas de formación en conjunto con el Ministerio de Educación, se podría fortalecer las capacidades locales en el sector de ciberseguridad y garantizar la retención de talento dentro del ámbito estatal, un punto clave para garantizar la resiliencia y eficacia de las respuestas nacionales ante ciberamenazas.

Asimismo, la implementación de identificación cibernética única mediante autenticación biométrica y números identificatorios contribuiría significativamente a mejorar la seguridad y control del ciberespacio argentino, alineándose con la necesidad de proteger las infraestructuras críticas. Aunque esta medida requiere ajustes en la Ley de Protección de Datos Personales, su adopción permitiría una identificación fehaciente de los usuarios, reduciendo el riesgo de fraudes y ciberataques.

En resumen, la creación de un Ministerio del Ciberespacio no solo facilita la delimitación de la jurisdicción en el ciberespacio, sino que también mejoraría la seguridad digital, optimizaría las capacidades nacionales de ciberdefensa y resolvería la escasez de profesionales capacitados, fortaleciendo, de esta manera, la soberanía digital de Argentina en el ámbito cibernético. Este paso hacia la construcción de una infraestructura nacional de ciberseguridad robusta es imprescindible para abordar los desafíos de un ciberespacio cada vez más complejo y vulnerable.

5. Objetivos

Objetivo General:

El objetivo general de este trabajo es proponer un marco de ciberdefensa que refuerce la soberanía digital de Argentina. Este enfoque busca abordar los desafíos que enfrenta el país en la protección de su infraestructura crítica digital y la defensa de su espacio cibernético frente a amenazas transnacionales.

Objetivos Específicos:

a. Analizar el impacto de los conflictos en el ciberespacio sobre la infraestructura crítica de Argentina, identificando vulnerabilidades y necesidades de protección.
b. Examinar los tratados y normas internacionales relevantes para el fortalecimiento de la ciberdefensa nacional, evaluando su aplicabilidad y señalando las oportunidades de adaptación al contexto regional.
c. Desarrollar propuestas para una mayor cooperación regional en ciberdefensa, aprovechando las sinergias con organizaciones como MERCOSUR y UNASUR, que permitan una respuesta coordinada ante ciberamenazas compartidas.
d. Estudiar marcos de análisis, como MITRE ATT&CK y D3fend, para mejorar las capacidades de identificación, análisis y respuesta a incidentes cibernéticos en Argentina.
e. Explorar la factibilidad y los beneficios de la creación de un ministerio del ciberespacio como ente coordinador de las políticas y acciones de ciberseguridad a nivel nacional, fortaleciendo la soberanía digital del país.

6. Marco Teórico Preliminar

6.1 Introducción a la Ciberseguridad y Soberanía Digital

La ciberseguridad y la soberanía digital se han convertido en temas centrales para los estados, debido a las amenazas que suponen los ciberataques en el entorno digital global. La soberanía digital implica la capacidad de proteger y controlar la infraestructura y los datos críticos dentro de su ciberespacio. La resolución 1523/ 2019 de la Secretaría de Gobierno de Modernización, en el marco de la Estrategia Nacional de Ciberseguridad, estableció nuevas definiciones y criterios para la protección de las infraestructuras que respaldan servicios críticos. Esta resolución aborda los conceptos de Soberanía e integridad territorial al hablar de aquellas acciones que al afectar un sistema informático generen efectos dentro del territorio nacional cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio nacional. La resolución también aprueba el Glosario de Términos de Ciberseguridad, que define conceptos como acceso, amenaza, ciberataque, cookies y fuga de datos, entre otros**.** La falta de una delimitación jurisdiccional en el ciberespacio y la dependencia de infraestructuras tecnológicas extranjeras presentan retos significativos para Argentina en la defensa de su soberanía digital (Comité de Ciberseguridad, 2019).

6.2 Fundamentos de Ciberdefensa

La diferenciación entre ciberseguridad y ciberdefensa en Argentina se empezó a dar gradualmente, especialmente desde la creación de la Estrategia Nacional de Ciberseguridad en 2019. La ciberdefensa abarca las acciones orientadas a proteger las infraestructuras críticas y la estabilidad de un país frente a ciberamenazas. En Argentina, la Directiva de Política de Defensa Nacional (Decreto 457/2021) establece la ciberdefensa como una prioridad del Estado, resaltando la importancia de involucrar tanto a las fuerzas armadas como a entidades civiles en la defensa de sus activos críticos (Decreto 457/2021).

6.2.1 Conflictos en el "Quinto Dominio" y Derecho Internacional Público

El ciberespacio, también llamado el “quinto dominio” de conflicto, presenta desafíos únicos debido a la ausencia de fronteras físicas y la dificultad para atribuir ataques.

The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. "El Quinto Dominio: El Ciberconflicto y la Seguridad Nacional" es un libro escrito por Richard A. Clarke y Robert K. Knake, publicado en 2010. Los autores argumentan que la seguridad nacional está en riesgo debido a la vulnerabilidad de los sistemas informáticos y la falta de preparación para enfrentar amenazas cibernéticas.

La Convención de Budapest, principal tratado internacional en ciberseguridad, se enfoca en el cibercrimen, pero no aborda los conflictos interestatales en el ciberespacio. La cooperación internacional y el desarrollo de nuevas normativas, como las recomendaciones del Comité Jurídico Interamericano, son esenciales para fortalecer la postura de ciberdefensa de los estados en el entorno digital (Comité Jurídico Interamericano, 2020).

6.3 Revisión de la Literatura y Estado del Arte

6.3.1 Normativas y Tratados Internacionales

La Convención de Budapest sobre delitos cibernéticos es uno de los pocos marcos internacionales en ciberseguridad, aunque limitado en su alcance y su adopción a nivel mundial. En el contexto latinoamericano, Argentina ha trabajado para integrarse en tratados de la OEA y la UNASUR, pero enfrenta desafíos para adaptarse a estándares internacionales que incluyan la protección de la soberanía digital (Comité Jurídico Interamericano, 2020). La inclusión de estas normativas permitiría una mayor coordinación y efectividad en la persecución de ciberdelitos transnacionales.

6.3.2 Estrategias de Defensa y Protección de Infraestructuras Críticas

La Resolución 141/2019 del Comité de Ciberseguridad en Argentina establece mecanismos para proteger las infraestructuras críticas, promoviendo la colaboración público-privada y el desarrollo de protocolos de seguridad específicos (Comité de Ciberseguridad, 2019). Este enfoque está alineado con el de países como Brasil, que ha establecido el Centro de Defensa Cibernética (CDCiber) para coordinar la protección de infraestructuras estratégicas y garantizar una respuesta rápida ante ciberamenazas (Gómez, 2021). La experiencia brasileña resalta la importancia de una estructura centralizada y robusta para mejorar la resiliencia y respuesta en ciberdefensa.

6.3.3 Cooperación Regional (UNASUR, MERCOSUR)

La cooperación en el ámbito de la ciberseguridad es esencial para abordar las amenazas transnacionales que superan las capacidades de un solo país. En América Latina, la cooperación entre MERCOSUR y UNASUR facilita la creación de políticas y el intercambio de información para responder a los desafíos de ciberseguridad en la región. La tabla comparativa a continuación muestra cómo los enfoques de Brasil, España e Israel en ciberseguridad ofrecen lecciones prácticas para Argentina, resaltando la importancia de la colaboración público-privada, la integración de capacidades ofensivas y defensivas, y las alianzas internacionales:

Tabla 1

Aspecto	Brasil	España	Israel	Aplicación en Argentina
Protección de Infraestructuras Críticas	Defensa en profundidad con enfoque en protección centralizada de infraestructuras estratégicas. (Manual de Guerra Cibernética)	Directrices específicas en el Plan Nacional de Ciberseguridad para proteger infraestructuras críticas mediante cooperación público-privada.	Defensa en capas (Defensa en Profundidad) y con capacidades avanzadas de respuesta.	Crear una entidad nacional para coordinar y proteger infraestructuras críticas de manera centralizada, aplicando defensa en profundidad.
Capacidades Ofensivas y Defensivas	Enfoque en el desarrollo de capacidades de ataque y defensa cibernética integradas en la estrategia de defensa nacional.	Enfocada en la defensa, con colaboración en el ámbito de la Unión Europea para el desarrollo de estrategias de defensa colectiva.	Avances en capacidades ofensivas y defensivas (ej. Unidad 8200), integración con el sector militar y tecnológico.	Integrar capacidades ofensivas y defensivas en la estrategia nacional para disuadir y responder a ciberataques regionales.
Colaboración Internacional	Cooperación en MERCOSUR y OEA para fortalecer la ciberseguridad en el ámbito regional.	Participación en la Unión Europea y foros internacionales para el desarrollo de políticas comunes y normas de ciberseguridad	Alianzas bilaterales y multilaterales con países avanzados en ciberseguridad (EE. UU., Grecia, Japón).	Establecer alianzas estratégicas con países y bloques avanzados en ciberseguridad para compartir mejores prácticas y herramientas.

Sensibilización y Capacitación	Capacitación enfocada en la defensa nacional, con unidades especializadas para desarrollar habilidades en ciberseguridad.	Programas de sensibilización pública y campañas de concienciación para fomentar la cultura de ciberseguridad a nivel nacional.	Cultura de ciberseguridad desde la educación temprana hasta el servicio militar, formando un ecosistema de ciberseguridad.	Crear programas de sensibilización y capacitación a nivel nacional y fomentar una cultura de ciberseguridad desde la educación básica.
Integración Público-Privada	Coordinación entre el ejército y sectores críticos, con centralización bajo el CDCiber.	Fuerte cooperación público-privada para implementar políticas nacionales de ciberseguridad en sectores privados y estatales.	Integración del sector militar con startups y el sector privado, impulsando la innovación y la seguridad a nivel nacional.	Promover la colaboración entre el gobierno y el sector privado, especialmente en áreas tecnológicas y de infraestructuras críticas.
Desarrollo de Talento	Capacitación en unidades especializadas en el ámbito de defensa, aunque limitado en el sector civil.	Fomentan la formación continua y la retención de talento especializado en ciberseguridad mediante programas nacionales.	Fuerte enfoque en retención y desarrollo de talento mediante la educación y colaboración en el sector tecnológico y militar.	Crear programas de formación en ciberseguridad en colaboración con universidades y centros de investigación para retener talento.

6.4 Metodologías de Ciberdefensa y Marcos de Análisis para la Respuesta a Incidentes

La ciberdefensa efectiva se fundamenta en metodologías estructuradas que permitan la **detección, análisis y respuesta** a las ciberamenazas en tiempo real. En el contexto de Argentina, la implementación de marcos avanzados como **MITRE ATT&CK** y **D3fend** aporta una guía detallada y comprobada para enfrentar el ciclo de vida de los ataques, asegurando la protección de infraestructuras críticas y mejorando la resiliencia nacional frente a ciberincidentes.

MITRE ATT&CK es un marco de análisis que organiza y clasifica las tácticas y técnicas empleadas por los atacantes a lo largo de sus operaciones. Este sistema permite a las organizaciones entender cada etapa de un ataque, desde el reconocimiento inicial hasta el impacto final, proporcionando un inventario de tácticas que pueden ser identificadas y contrarrestadas. En Argentina, ATT&CK ofrece una herramienta fundamental para mapear amenazas y anticipar posibles vectores de ataque, permitiendo una respuesta informada y estructurada ante incidentes. Con un enfoque basado en **detección proactiva**, el marco ATT&CK posibilita que los defensores clasifiquen ataques específicos y ajusten sus defensas de acuerdo a tácticas conocidas.

D3fend complementa a ATT&CK proporcionando un repertorio de contramedidas específicas para cada técnica de ataque. Este marco guía la implementación de defensas en profundidad, ayudando a las organizaciones a estructurar sus respuestas y maximizar la resiliencia de sus sistemas de seguridad. D3fend permite a Argentina diseñar estrategias de defensa adaptativas, en las cuales cada capa de protección aborda una fase específica del ciclo de ataque, garantizando que las infraestructuras críticas estén protegidas desde múltiples ángulos.

Al integrar ATT&CK y D3fend en la estrategia de ciberdefensa nacional, Argentina puede construir una metodología robusta para la **respuesta a incidentes**, basada en las mejores prácticas internacionales. La implementación de estos marcos permite a los analistas de ciberseguridad clasificar, detectar y contrarrestar tácticas de ataque en tiempo real, mejorando la capacidad del país para responder a ciberincidentes de manera coordinada y efectiva. Esta combinación de metodologías y marcos proporciona una **defensa en profundidad y adaptativa**, alineada con los estándares globales y capaz de afrontar los desafíos de un ciberespacio cada vez más vulnerable.

Integrar estas metodologías en el contexto argentino no solo fortalece la ciberseguridad nacional, sino que también asegura que las respuestas sean proactivas y adaptativas, respondiendo a la evolución de las tácticas empleadas por los atacantes. De esta manera, ATT&CK y D3fend no solo ofrecen un marco teórico para la ciberdefensa, sino que

representan herramientas prácticas y estratégicas para estructurar y mejorar la **respuesta a incidentes cibernéticos** en el país.

6.5 Propuestas de Modificación del Tallinn Manual

El **Tallinn Manual** es una referencia jurídica clave para abordar conflictos en el ciberespacio, especialmente en situaciones de conflicto armado y amenazas interestatales. Sin embargo, este marco normativo se desarrolló principalmente en un contexto europeo, lo cual limita su aplicabilidad en países latinoamericanos como Argentina, que enfrentan desafíos geopolíticos y culturales específicos.

La adaptación del Tallinn Manual al contexto latinoamericano proporcionaría a Argentina y a sus socios regionales un **marco legal de ciberdefensa** alineado con sus necesidades y vulnerabilidades particulares. En colaboración con organismos como MERCOSUR y UNASUR, Argentina podría proponer modificaciones que reflejen la perspectiva regional en temas como soberanía digital, jurisdicción en el ciberespacio y protección de infraestructuras críticas. Estas adaptaciones podrían incluir directrices específicas para la cooperación regional en ciberseguridad, desarrollando un marco normativo común que facilite una **respuesta coordinada ante ciberincidentes transnacionales** y fortalezca la postura defensiva del país.

Además, al incorporar elementos relevantes del contexto local, las modificaciones propuestas asegurarían que el marco legal sea más aplicable a la realidad argentina y que facilite la colaboración internacional. Estas iniciativas no solo beneficiarían a Argentina, sino que también promoverían una mayor seguridad cibernética en toda América Latina, creando un espacio digital más seguro y menos susceptible a la influencia de actores malintencionados.

7. Metodologías y Técnicas Utilizadas para Sustentar / Contrastación de la Hipótesis

La metodología de este trabajo investigativo se diseñó para analizar la viabilidad y necesidad de crear un **Ministerio del Ciberespacio** en Argentina, centralizando la ciberseguridad y la protección de la soberanía digital. La hipótesis propuesta sostiene que este organismo permitiría al Estado argentino ejercer un control efectivo sobre las redes digitales nacionales, facilitando la coordinación en incidentes cibernéticos y garantizando una defensa robusta de infraestructuras críticas. A continuación, se describe la metodología aplicada para sustentar esta hipótesis.

7.1 Enfoque y Tipo de Estudio

Este estudio adoptó un enfoque **cualitativo y cuantitativo**, orientado a proporcionar un análisis integral que abarca tanto la caracterización de la problemática de ciberseguridad en Argentina como la evaluación de políticas y estrategias internacionales comparables. El diseño del estudio es **descriptivo y explicativo**, lo cual permite explorar en profundidad las deficiencias actuales en la ciberseguridad argentina, explicar las razones por las cuales un Ministerio del Ciberespacio sería una solución estratégica y sustentar esta propuesta mediante un análisis comparativo. Además, el diseño es **no experimental** y **transversal**, recopilando y analizando datos en un momento específico a partir de fuentes secundarias como resoluciones nacionales, estrategias de ciberdefensa, y directrices internacionales.

Unidades de Análisis y Variables Principales

Las unidades de análisis de este estudio se enfocan en tres áreas fundamentales:

1. **Infraestructura crítica y sistemas de información del Estado**: Incluye el análisis de las actuales políticas de ciberseguridad implementadas.
2. **Modelos internacionales de ciberdefensa**: Examina ejemplos de países avanzados en ciberseguridad, como Brasil, España e Israel, cuyas prácticas de defensa cibernética presentan características adaptables al contexto argentino.
3. **Marco jurídico y regulatorio**: Considera las leyes y normativas nacionales en ciberseguridad, así como la aplicación de marcos internacionales, como la Convención de Budapest, y la necesidad de una jurisdicción clara en el ciberespacio argentino.

Las principales variables del estudio son:

- **Eficiencia de las políticas de ciberseguridad actuales en Argentina** para proteger infraestructuras críticas.
- **Capacidades de respuesta ante ciberataques** en comparación con modelos internacionales.
- **Nivel de centralización y autoridad transversal** en el manejo de incidentes cibernéticos.

Población/Muestra y Unidades de Respuesta

La muestra de este estudio se basa en documentos oficiales, informes estratégicos de ciberdefensa y normativas aplicadas en Argentina. También incluye estudios comparativos de modelos de ciberseguridad en países de referencia. Las unidades de respuesta se definen en términos de:

- **Revisión de políticas nacionales e internacionales** en ciberseguridad, centradas en la protección de la infraestructura crítica y la jurisdicción cibernética.
- **Análisis comparativo** de estructuras de ciberdefensa centralizadas y su efectividad en otros países, para evaluar su aplicabilidad en el contexto argentino.

Técnicas de Recolección de Datos

La recolección de datos se realizó mediante técnicas de análisis documental, incluyendo:

- **Análisis de resoluciones y estrategias nacionales de ciberseguridad**, como la Resolución 141/2019 y la Estrategia de Ciberseguridad Nacional. Estos documentos proporcionaron una visión detallada de las políticas y limitaciones actuales.
- **Estudio comparativo de marcos y prácticas internacionales**: Se utilizó como referencia el modelo de ciberdefensa de Brasil (CDCiber), la Estrategia de Ciberseguridad Nacional de España y las capacidades avanzadas de Israel, especialmente en términos de defensa en profundidad y colaboración entre entidades públicas y privadas.
- **Revisión de tratados y normativas internacionales**: Se evaluaron documentos como el Tallinn Manual y la Convención de Budapest para considerar cómo adaptar o integrar normativas internacionales al marco legal argentino.

7.2 Procedimientos de Análisis de Datos

El análisis de datos se llevó a cabo en dos etapas clave:

1. **Análisis descriptivo y comparativo**: A través de la comparación de políticas y estructuras de ciberseguridad en países seleccionados, se evaluaron las ventajas de centralizar los esfuerzos de ciberdefensa bajo un organismo como el Ministerio del Ciberespacio. Este análisis permitió destacar las debilidades en la coordinación y jurisdicción de la ciberseguridad argentina, especialmente en el control de las infraestructuras críticas y la respuesta ante incidentes transnacionales.
2. **Evaluación de la hipótesis mediante un marco estructural**: Para validar la hipótesis de que un Ministerio del Ciberespacio fortalecería la ciberseguridad argentina, se contrastaron los resultados de las políticas actuales con los beneficios potenciales de un organismo centralizado, incluyendo la regulación de identidades digitales y la colaboración internacional. Además, se consideraron los requisitos de recursos humanos y la importancia de incentivar la formación y retención de talento en el ámbito público.

8. Referencias Iniciales y Bibliografía Preliminar

- Comité de Ciberseguridad. (2019). Resolución 141/2019 del Comité de Ciberseguridad. Argentina.
- Comité Jurídico Interamericano. (2020). Derecho Internacional y Operaciones Cibernéticas del Estado.
- Decreto 457/2021. Directiva de Política de Defensa Nacional. Argentina.
- Estrategia de Ciberseguridad Nacional. (2020). Política Nacional de Ciberseguridad. Argentina.
- Guía de Ciberdefensa. (2020). Orientaciones para el Diseño, Planeamiento, Implantación y Desarrollo de una Ciberdefensa Militar. Junta Interamericana de Defensa.
- Junta Interamericana de Defensa. (2020). Guía de Ciberdefensa.
- MITRE. (2020). ATT&CK Framework. Recuperado de https://attack.mitre.org/
- Observatorio Latinoamericano de Seguridad Cibernética. (2023). Guerra Ciber: Estrategias del Ejército Brasileño en Ciberdefensa. Recuperado de [URL de origen]
- Vergara, G. (2019). Manual de Ciberdefensa. Ministerio de Defensa, Argentina.
- Yler, M. (2021). Cyber Capabilities and National Power: Israel. Instituto Internacional de Estudios Estratégicos.