Facultad del Ejército
Escuela Superior de Guerra
"TG Luis María Campos"

UNDEF
Universidad de la Defensa Nacional

TRABAJO FINAL INTEGRADOR

Título: "La capacitación del Oficial Subalterno para ocupar puestos en organizaciones militares relacionadas con la ciberdefensa"

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor Heber Javier LAMBERTI

Director del TFI: MY CR (R) César Daniel CICERCHIA.

Ciudad Autónoma de Buenos Aires, de marzo de 2020.

Resumen

El frenético avance que han sufrido las tecnologías de la información y las comunicaciones, ha creado un cambio de paradigma el cual presenta nuevos beneficios y como así también nuevas amenazas. Estas amenazas, como se han visto en diferentes hechos tanto en el mundo como en nuestro país, pueden ser perjudiciales para las Infraestructuras Críticas del Estado y para su población, es por ello que los integrantes de nuestro Ejército deben capacitarse para enfrentarlas y poder formar parte de las organizaciones militares de ciberdefensa que hoy día existen en las Fuerzas Armadas o las que puedan llegar a crearse en un futuro.

El presente trabajo de investigación hace foco en dos ejes, el primero sobre el marco normativo que regula el empleo del ciberespacio y las actividades de ciberdefensa en la República Argentina y las limitaciones que se encuentran en éste, teniendo en cuenta la Ley de Defensa, la Ley de Seguridad Interior, creadas para normar el empleo de las Fuerzas Armadas, antes que el ciberespacio fuera considerado como un nuevo factor del ambiente operacional y de riesgo para la defensa nacional, así mismo se analizarán decretos y resoluciones. El segundo eje buscará presentar la oferta educativa existente en el ámbito de las Fuerzas Armadas bajo la órbita de la Universidad de la Defensa Nacional y en universidades públicas y privadas, la cual brindará la capacitación necesaria para que el personal de oficiales subalternos pueda ocupar puestos en organizaciones relacionadas con la ciberdefensa. También se presentarán diferentes hechos históricos que servirán de marco inicial para entender porque es necesario capacitar al personal en materia de ciberdefensa y ciberseguridad, realizando un análisis de casos de relevancia a nivel mundial y nacional.

Palabras claves

Ciberespacio, Ciberdefensa, Ciberseguridad, Capacitación, Educación.

Tabla de contenido

Introducción

Problema

Tema del Trabajo: La capacitación del oficial subalterno para ocupar puestos en organizaciones militares relacionadas con la ciberdefensa.

Antecedentes y justificación del problema

La evolución que han sufrido las tecnologías de la información, las comunicaciones y la infraestructura digital, sumado al crecimiento de Internet y la conectividad digital, han creado un cambio de paradigma, el cual exige adquirir conocimientos que permitan dirigir una organización para adoptar una serie de procedimientos especializados a fin de neutralizar y controlar las amenazas cibernéticas que se presentan en el ciberespacio. Esta evolución, obliga a trabajar en la capacitación del personal subalterno ya que estos son nativos digitales, por formar parte de la llamada Generación Y (millennials[1]), lo que hace que posean un perfil con rasgos de confianza, tolerancia y abiertos a los cambios y la Generación Z (centennials[2]), que son leales, reflexivos, de mente abierta y determinados.

En base a ese cambio de paradigma y a diferentes hechos a nivel mundial, es que han surgido diferentes conceptos como el de ciberseguridad y ciberdefensa, particularmente el segundo ha adquirido gran relevancia luego de la realización de numerosos ataques cibernéticos a infraestructuras críticas que ponen en riesgo la seguridad de los Estados.

Uno de los casos más relevante ocurrido el 27 de abril de 2007 en Estonia, más específicamente en Tallin, su capital, centro político, económico y financiero de este país. Para 2007 Estonia era el país más digitalizado de Europa, pudiendo sus 1,3 millones de habitantes con tan solo una tarjeta o su computadora pedir una receta médica, pagar sus impuestos, todas sus compras y hasta votar. Ese día un grupo de piratas informáticos, se cree rusos, produjeron el colapso de todo el sistema informático del país al realizar un ataque a la infraestructura crítica cibernética, dejando sin servicios a bancos, cajeros automáticos, servicios de banco online, páginas web, correo electrónico y otros. Es por ello que solicitó apoyo a la OTAN

[1] Millennials: Jóvenes nacidos a partir de los años 80. Son una generación que ha utilizado tanto medios analógicos como digital, hiperconectada y con altos valores sociales y éticos.
[2] Centennials: Jóvenes nacidos aproximadamente a mediados de los años 90 y del año 2000. Son una generación 100% digitales, completamente hiperconectados, son autodidactas y resolutivos.

(Organización del Tratado del Atlántico Norte) ante el ataque recibido, pero para ese entonces esta organización no contaba con ningún tipo de plan de contingencia ante este tipo de episodios, por lo que rápidamente en 2008 creó el Centro de Excelencia para la Ciberdefensa Colaborativa en Tallin, el cual publicó un documento en abril de 2013 que examina la aplicabilidad de diferentes normas internacionales a la nueva ciberdefensa llamado Manual de Tallin (Tallin Manual on the International Law Applicable to Cyber Warfare), hoy actualizado al Manual de Tallin 2.0.

Otros casos resonantes fueron los ataques a las centrifugadoras nucleares iraníes en Natanz, las filtraciones realizadas por Wikileaks o el ataque realizado a través del ransomware3 WannaCry en 2017, que afectó más de 150 países.

El Libro Blanco de la Defensa (Ministerio de Defensa, 2015), expresa que con el paso de los años, el concepto de ciberespacio ha ido evolucionando y tomando mayor importancia en lo que respecta a la Defensa Nacional. En tal sentido expone que, el concepto de ciberespacio se asocia a un cambio de paradigma científico-tecnológico, en el cual las tecnologías de la información adquieren particular importancia para el desarrollo de operaciones militares en la defensa de la Nación.

La Directiva de Política de Defensa Nacional (Poder Ejecutivo Nacional, 2018), aprobada por el Presidente de la Nación, establece los lineamientos centrales de la política de Defensa Nacional. Determina entre otras cosas, el desarrollo de las capacidades operacionales, involucrando a otras dependencias, más allá del Ministerio de Defensa, como la Inteligencia y la Investigación y el Desarrollo Tecnológico. En el marco de los escenarios mundial y regional, establece amenazas y riegos, estos últimos constituyen situaciones que, de configurarse, podrían afectar los intereses nacionales en materia Defensa, uno de estos en particular, es el empleo del ciberespacio con fines militares, incorporándolo como un nuevo ámbito de interés, debido a los fenómenos que se suscitan en el mismo.

Recientemente en el mes de noviembre de 2018, el Presidente de la Nación firmó, con la aprobación de la Cámara de Diputados, la ratificación de la Convención de Budapest o Convenio sobre la Ciberseguridad, creado en 2001 por el Consejo Europeo. Este convenio, es un tratado internacional al que se han adherido más de cincuenta y dos países en la búsqueda de cooperación para la lucha contra los delitos informáticos.

[3] Ransomware: Código malicioso que se emplea para secuestrar datos o información y el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

La aparición del ciberespacio marcó la creación de un nuevo factor del ambiente operacional, el cual a diferencia de los tradicionales: terrestre, aéreo, naval y aeroespacial, no posee límites definidos y abarca a los otros factores, es transversal y se superpone sobre ellos, es virtual y no reconoce fronteras locales o interestatales.

A partir de este nuevo paradigma, se deben establecer los conocimientos que debe poseer el oficial subalterno que desee ocupar puestos en organizaciones militares relacionadas con la ciberdefensa. Algunos de estos puestos ya se encuentran creados y otros podrían crearse en virtud de la evolución de la fuerza en base a este nuevo concepto.

Se debe tener en cuenta que las acciones de ciberdefensa se desarrollan en el ciberespacio. Es por ello que se debe definir al mismo, a tal efecto se presentan diferentes definiciones:

> El diccionario de la Real Academia Española (RAE, 2011) lo define en pocas palabras como un "ámbito artificial creado por medios informáticos". (p. 7475).
>
> Para la Unión Internacional de Telecomunicaciones (UIT, 2006) "el ciberespacio es aquel integrado por cientos de miles de servidores, ordenadores, encaminadores, conmutadores interconectados y sistemas de transporte de la información (cables, satélites, medios radioeléctricos) que permiten un funcionamiento armonioso de las infraestructuras básicas". (p. 1 Introducción).
>
> El Departamento de Defensa de los Estados Unidos de Norteamérica (DOD Dictionary, 2020) lo define como "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, y procesadores embebidos y controladores". (p. 55).
>
> El Manual Tallin (Manual Tallin, 2013) como "el entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y el espectro electromagnético, para almacenar, modificar e intercambiar datos utilizando redes de computadoras". (p. 211 Glosario de Términos). Y en materia de normas, la Organización Internacional de Normalización (ISO) ha presentado un nuevo estándar para mejorar la seguridad online, norma

> ISO/IEC 27032 para la ciberseguridad, definiendo al ciberespacio como "un entorno complejo que consta de interacciones entre personas, software y servicios destinados a la distribución mundial de información y comunicación"

Sin dejar de lado las definiciones mencionadas, para este trabajo se empleará la estipulada en la Resolución 1523/19 – Anexo 2, de fecha 12 de septiembre de 2019 de la Secretaría de Gobierno de Modernización, publicada en el Boletín Oficial, esta define al ciberespacio como un ambiente complejo en el cual interactúan personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas de tecnologías de información y comunicaciones. Aunque esta se contrasta con la presentada en el Glosario de Términos de Empleo Militar para la Acción Militar Conjunta (EMCOFFAA, 2015) el cual en su definición no contempla a las personas, siendo estas las responsables de la utilización de los diferente medios ya sean físicos o virtuales que le sean otorgados. Además, la definición que presenta la Resolución anteriormente mencionada, se encuentra alineada con expresado en las normas ISO.

En lo que respecta a la ciberdefensa, al igual que con el ciberespacio, su concepto ha ido evolucionando, no solo en su importancia sino también en su concepto y definición en todo el mundo. Particularmente en nuestro país la DPDN (Poder Ejecutivo Nacional, 2018), orienta a la política de ciberdefensa a reducir gradualmente las vulnerabilidades de los activos estratégicos de interés de la Defensa Nacional. (Anexo I, p. 18). Recientemente el mes de octubre de 2019, el Ministerio de Defensa publicó la Resolución Nro 1380/19, la cual en su Artículo 1ro presentó una nueva definición de la misma la cual hace foco en las acciones de seguridad que debe desarrollar el Ministerio de Defensa y sus Unidades dependientes para anticipar y prevenir ciberataques que puedan afectar tanto al Ministerio de Defensa como al Instrumento Militar y a sus Infraestructuras Críticas de interés para la Defensa Nacional. (Ministerio de Defensa, 2019).

En las Fuerzas Armadas, existen diferentes definiciones de ciberdefensa, pero tanto el Glosario de términos de empleo militar para la Acción Militar Conjunta (EMCOFFAA, 2015) como el Reglamento Conducción de las Fuerzas Terrestres (Ejército Argentino, 2015), concuerdan en que son el conjunto de acciones que se

desarrollan en el ciberespacio para prevenir y/o contrarrestar amenazas o agresiones cibernéticas.

En el ámbito de la Acción Militar Conjunta, el Comando Conjunto de Ciberdefensa (CCCD), creado por medio de la Resolución del Ministerio de Defensa Nro 343/14 (Ministerio de Defensa, 2014), fue la primera Unidad de las Fuerzas Armadas creada para abordar la temática sobre la ciberdefensa, esta posee la misión de ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

En referencia a la documentación rectora sobre el empleo del ciberespacio y especialmente en lo referido a la Ciberdefensa en el Ejército Argentino, existe escasa documentación, solo la Resolución Nro 2016-256-E-APN-MD (Ministerio de Defensa, 2016), la cual ordena la conformación de la Dirección de Ciberdefensa del Ejército Argentino y la Orden Especial del Jefe del Estado Mayor General del Ejército (JEMGE) Nro 39/5P/18 que ordena la conformación de la Dirección de Ciberdefensa del Ejército Argentino, pero la misma tiene clasificación de seguridad SECRETO, por lo que no va a ser utilizada para este trabajo.

Para el presente trabajo se tendrá en cuenta el trabajo realizado en la Escuela Superior de Guerra que trata sobre dos temas que son el ciberespacio y la conducción de la Ciberdefensa y cómo estas influyen en el combate moderno principalmente en las Operaciones Tácticas (Anca, 2015). El trabajo final integrador presentado por el Mayor Ariel Grogovinas sobre Ciberoperaciones (Grogovinas, 2018) y del Mayor Ezequiel Rodríguez Cisneros sobre Operaciones Ciberespaciales (Rodriguez Cisneros, 2012) de la Escuela Superior de Guerra Conjunta. La tesis realizada en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas la cual desarrolla el tema desde un punto de vista Estratégico, tomando en cuenta esta nueva dimensión, el marco legal y la situación nacional en esta temática (Baretto, 2017). Y la publicación del General de División (R) Evergisto de Vergara y del Contraalmirante (R) Gustavo Adolfo Trama sobre Operaciones Militares Cibernéticas – Planeamiento y Ejecución en el Nivel Operacional (De Vergara - Trama, 2017) de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

En el Ejército Argentino, en materia de educación en la temática que se trata, se realizan conferencias, simposios, cursillos y seminarios orientados a la Fuerza en

su conjunto en todo el país. En la Facultad de Ingeniería del Ejército (FIE) se dicta la Especialización en Criptografía y Seguridad en Teleinformática y la Maestría en Ciberdefensa, de las cuales se hará un análisis más detallado posteriormente, el Curso de Introducción a la Ciberdefensa y la Ciberseguridad dictado en la Escuela Superior de Guerra Conjunta, el cual es abierto para funcionarios públicos y del ámbito privado con posiciones de liderazgo y ejecutivas, integrantes de equipos de planeamiento y personas con interés en los campos de relaciones internacionales, seguridad y defensa. Por otro lado el Instituto Universitario Aeronáutico en el Centro Regional Universitario Córdoba dos posgrado relacionados a la temática que son la Maestría en Ciberdefensa y la Especialización en Seguridad Informática.

En el marco regional, el primer país en adoptar una política en materia de ciberdefensa fue Colombia, creando en el año 2012 el Comando Conjunto Cibernético y dependiente de este Unidades Cibernéticas de las tres Fuerzas Armadas (Estado Mayor Conjunto Operacional, 2019). En el año 2010 la República Federativa del Brasil, creó por medio de su Ministerio de Defensa el Centro de Defensa Cibernético del Ejército el cual comenzó a trabajar operativamente a partir del mes de septiembre de 2012 y actualmente en el mes de febrero de 2019 fue creada la Escuela Nacional de Defensa Cibernética (Edefa, 2019). El Ejército del Perú posee el Centro de Ciberdefensa creado en el año 2013. Estas Unidades brindan educación y capacitación a sus cuadros tanto en el ámbito específico como en el conjunto.

Formulación del Problema

¿Qué nivel de conocimientos debe adquirir el oficial subalterno para poder ocupar puestos de ciberdefensa en organizaciones militares relacionadas con esa temática?

Objetivos

Objetivo general

Establecer el nivel de conocimientos a adquirir por el personal de oficiales subalternos para poder operar en el nivel táctico y que les permita ocupar puestos en organizaciones militares relacionadas con la ciberdefensa.

Objetivos particulares

Objetivo particular Nro 1: Presentar diferentes hechos históricos que enmarcan la necesidad de capacitación del personal.

Objetivo particular Nro 2: Determinar el marco legal y las limitaciones existentes en el empleo del ciberespacio en la República Argentina.

Objetivo particular Nro 3: Presentar la oferta educativa existente en el país que permita a los oficiales subalternos alcanza el nivel de capacitación necesario para poder integrar organizaciones militares relacionadas con la ciberdefensa.

Marco teórico

Luego de haberse realizado un análisis y una apreciación de situación de la Directiva de Políticas de Defensa Nacional, la Estrategia Nacional de Ciberseguridad y la Política de Ciberdefensa, empleando el Proceso de Planificación de Comando para un Problema Militar Operativo Futuro, se ha identificado que se presenta un nuevo factor del ambiente operacional a tener en cuenta para la Defensa Nacional, denominado ciberespacio o espacio cibernético.

Teniendo en cuenta el reciente proceso de digitalización y el avance de las nuevas tecnologías de las comunicaciones y la informática su empleo con fines militares es uno de los riesgos en los que su posible evolución podría afectar los intereses nacionales y en materia de defensa. Razón por la cual, es de vital importancia capacitar al personal del Ejército Argentino en esta materia, tanto en el ámbito específico como conjunto y especialmente a los oficiales subalternos, a fin de poder enfrentar las amenazas que en la actualidad se presentan a nivel mundial y regional, tanto en tiempo de guerra como de paz.

El marco teórico que orienta el presente trabajo de investigación encuentra su base doctrinaria en diferentes documentos y teorías que nos permitirán alcanzar el objetivo general de la misma y así, proponer un diseño de capacitación para los oficiales subalternos que les permita operar en forma segura en el ciberespacio y que estos estén en capacidad de desempeñar puestos en organizaciones militares de ciberdefensa.

Para comenzar con esta investigación cabe mencionar que el término ciberespacio se utilizó por primera vez en la novela Neuromante de William Gibson (Gibson, 1984), al referirse a todos los recursos de información y comunicación disponibles en las redes informáticas, popularizándose su uso. Su definición ha ido cambiando con el tiempo y acompañando la evolución de la tecnología. Hoy en día la

Unión Internacional de Telecomunicaciones lo define como un terreno físico y no físico compuesto por diferentes elementos, entre ellos: redes, programas (software), ordenadores (hardware), usuarios, sistemas informáticos y contenido y tráfico de datos, con diferencias sustanciales en la componente física, ya que de no existir esta, la no física no podría desarrollarse.

La Resolución 1523/19 – Glosario de Términos de Ciberseguridad de la Secretaría de Gobierno de Modernización en su Anexo 2 define al ciberespacio como el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas de tecnologías de información y comunicaciones. El empleo de las redes de comunicaciones se encuentra presente en todo el ámbito de las Fuerzas Armadas (FFAA), tanto en el específico como en el conjunto, nos permiten interconectarnos y poder interactuar entre personas, son de aplicación constante y ayuda a que el proceso de toma de decisiones sea ágil y que la información llegue lo más rápido posible al receptor de la misma. Es por ello que al hablar de ciberespacio, se debe tomar al mismo desde un enfoque sistémico abordándolo de forma integral, en el cual el conjunto de elementos que lo compone se encuentra en interacción constante, de ésta se producirán nuevas cualidades con características diferentes para finalizar con un concepto superior al de los componentes que lo forman (EcuRed, 2019).

En la actualidad existe un vacío legal internacional en lo referente al empleo del ciberespacio debido a diferentes razones, entre ellas podemos nombrar una de las más importantes que es la lentitud en la aprobación de las diferentes legislaciones tanto nacionales como internacionales en contraposición con la rapidez con que evolucionan las tecnologías, provocando esto que las leyes regulatorias sean aprobadas en forma tardía y que su aplicación sea obsoleta. Es por ello que se continuará con un análisis profundo de las normas, leyes y tratados vigentes para determinar el marco legal en el cual encuadrar la capacitación. Se tendrá en cuenta la Ley de Defensa Nacional Nro 23554, el Decreto PEN4 Nro 727/06, la Ley de Seguridad Interior y la Ley de Inteligencia Nacional Nro 25.520 y el Convenio de Budapest sobre Ciberdelincuencia, entre otros.

[4] PEN: Poder Ejecutivo Nacional.

Dentro de las teorías de aprendizaje que se han estudiado en la materia Educación Militar, podemos enmarcar a esta propuesta de capacitación dentro de la teoría de aprendizaje social de Lev Vygotsky (1896–1934), quien responde al constructivismo. Vygotsky concibe al ser humano como un individuo social desde el momento de su nacimiento y al conocimiento, en sí mismo, como un producto social. Destacando la importancia de las influencias sociales en el desarrollo. El constructivismo educativo propone un proceso de enseñanza dinámico, participativo e interactivo del sujeto, de modo que el conocimiento sea una auténtica construcción operada por la persona que aprende. La enseñanza del educando está orientada a la acción, para crear nuevos conocimientos sobre la base de experiencias previas y su relación con el medio que lo rodea. Es por ello que, partiendo de los conocimientos básicos adquiridos previamente por los educandos en las diferentes fuentes de reclutamiento, en la capacitación del oficial subalterno en materia de ciberespacio se impartirán los temas en forma progresiva, enlazando sus ideas, alentado la participación e interacción entre el educador y los educandos y entre ellos mismos. Logrando así un proceso dinámico y participativo, en el que el educador es un orientador y facilitador, como señala el constructivismo. Asimismo, en esta teoría, en el proceso de enseñanza-aprendizaje establece que el educando es al único responsable de su propio proceso de aprendizaje y el procesador activo de la información, construye el conocimiento por sí mismo y nadie puede sustituirle en esta tarea. Por lo que el diseño de la capacitación a plantear debe contemplar que el educando la participación del educando en las actividades propuestas en un plazo estipulado y su posterior defensa, así como la propuesta de soluciones a las situaciones planteadas por el educador.

Metodología a emplear

El método que se empleará para la realización de la investigación será el deductivo. Por medio del cual, partiremos de un objetivo o premisa general, de la cual se desprenderán diferentes objetivos particulares y de sus respectivas conclusiones se arribará a conclusiones de carácter general que buscarán darán respuesta al objetivo general buscado. Para la presente investigación se utilizará el diseño explicativo. Se emplearán diferentes técnicas de validación, a saber: análisis bibliográfico, documental y lógico. Ver Anexo A: Esquema gráfico metodológico.

Capítulo 1
Hechos históricos que enmarcan el presente trabajo

El presente capítulo tiene por finalidad realizar un breve repaso de los hechos históricos a nivel mundial, regional y nacional, que cimientan la necesidad de incrementar este tipo de conocimientos, a fin de poder enfrenar las amenazas que se configuren contra la Defensa Nacional. También se darán a conocer cuáles son en la actualidad las organizaciones creadas parar enfrentar este tipo de amenazar a Nivel Conjunto y en el ámbito del Ejército Argentino y en las que los oficiales subalternos podrían llegar a ser destinados luego de obtener una capacitación acorde a la temática.

¿Porque debemos capacitarnos en ciberdefensa?: Un poco de historia

La creación y desarrollo de la llamada ARPANET (Advanced Research Project Agency Net)[5], en la década de 1960 inició con lo que luego sería la Internet. Esta red había sido concebida en un primer momento para formar una red militar de ordenadores interconectados que le permitía acceder a datos referidos a la Defensa Nacional, específicamente miliares desde cualquier punto del país, logrando con ello un salto cuantitativo en el manejo de la información, ganando posiciones en una época de Guerra Fría que se estaba llevando a cabo contra su principal enemigo, Rusia. Un poco más adelante en 1980, esta red ya llegaba a varias universidades que la utilizaban para fines académicos, por lo que el proyecto se dejó de lado al haber perdido su estado militar, privado y principalmente de seguridad, pasando a crear una nueva red militar llamada MILNET (Military Network)[6].

En los años 90 se da a conocer a nivel mundial Internet, la cual fue una evolución de la vieja red ARPANET, en base a esto comenzaron a realizarse cambios significativos especialmente en los entornos gráficos aflorando los correos electrónicos y navegadores. Esta evolución generó la aparición de los primeros hackers[7], expertos en tecnologías de comunicación e información, quienes utilizaban los conocimientos que habían obtenido para superar problemas asociados a la seguridad de los sistemas. Estos se reunían en clubes y laboratorios del Instituto

[5] Advanced Research Project Agency Net: Red de la Agencia de Proyectos de Investigación Avanzada. RAE 2018.
[6] Military Network: Red Militar. RAE 2018.
[7] Hacker: Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. RAE 2018.

Tecnológico de Masachuset (MIT). En base a esto es que al ver las posibilidades de infiltración por medios de las redes y viendo afectada primordialmente la seguridad nacional, es que se comienza a tomar al ciberespacio como un nuevo dominio, en el cual existen debilidades que pueden convertirse en vulnerabilidades a ser explotadas no solo por personas comunes, sino por otros Estados para obtener beneficios. Es por ello que, ante este tipo de vulnerabilidades se comienza a trabajar en la seguridad tanto física como virtual de los depositarios de información, buscando protegerlos de las posibles amenazadas de diferentes actores, los que poseen diferentes motivaciones las cuales pueden generar riesgos a la seguridad de las infraestructuras críticas, tanto en el sector público como en el privado. Podemos identificar como infraestructuras críticas a aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente (Jefatura de Gabinete de Ministros, 2019).

Se pueden nombrar brevemente algunos hechos, considerados más importantes que afectaron a la seguridad por medio de ciberataques.

El caso Estonia. Esta fue la chispa que encendió la mecha que hizo explotar a nivel mundial los ciberataques. Este fue el ataque de mayor importancia contra instituciones estatales y privadas llevada a cabo por un grupo de atacantes, se presume rusos, quienes un 27 de abril de 2007 iniciaron ataques por medio de robots informáticos (Botnets) que enviaron innumerables mensajes basura en forma masiva a organismos gubernamentales, medios de prensa y bancos, produciendo con esto la saturación de los servidores de estas entidades. Esta saturación provoco que los estonios no pudieran operar por medio de plataformas digitales de ningún tipo.

En otro país, el no poder operar por medio de estas plataformas, capaz no significaría un problema de gran envergadura, pero Estonia, para esa fecha era el país más digitalizado de Europa y todas las operaciones que realizaban sus ciudadanos eran vía internet.

El caso Georgia. En el año 2008, específicamente en agosto de ese año, se produjo la guerra entre pro rusos de las provincias de Osetia del Sur, Abjasia y la misma Rusia contra la República Democrática de Georgia. Días antes del inicio de

esta corta guerra que duró solamente 9 días, los medios de comunicación y portales de internet de las instituciones georgianas, recibieron ataques cibernéticos los cuales inutilizaron estos servicios. También, en este caso en similitud con Estonia, se cree que detrás de estos ataques están involucrados los servicios secretos rusos junto con piratas informáticos pro rusos adeptos al régimen de Valadimir Puttin.

El caso STUXNET. Otro caso de relevancia que modificó el escenario mundial fue este caso, nombrado así por el gusano informático de mismo nombre que afecta equipos que poseen el sistema operativo Windows, siendo este el primer gusano conocido por espiar y reprogramas sistemas industriales. Se cree que Estados Unidos en conjunción con Israel sabotearon durante 3 años (2008 - 2010), los sistemas informáticos de las instalaciones nucleares de Irán, principalmente su planta nuclear de Natanz, con la finalidad de retrasar su programa nuclear.

Aunque hay muchos más, hemos nombrado solamente algunos de los casos de mayor resonancia a nivel mundial. Por otro lado la Argentina no se encuentra exenta de este tipo de ataques.

El caso Ejército Argentino. En el marco nacional, el 19 de junio de 2017, la página oficial del Ejército Argentino fue afectada por acciones de piratas informáticas con supuestas amenazas del Estado Islámico (ISIS). En ella aparecía una foto y una frase que decía: "Esto es una amenaza. ISIS está en Argentina y muy pronto van a saber de nosotros" (Infobae, 2017). Esta amenaza fue solucionada a la brevedad y no produjo acciones maliciosas.

En marzo de 2019, la empresa de servicios de seguridad informática Symantec, en su reporte anual sobre Amenazas de Seguridad que realiza sobre 157 países, reveló que Argentina se encuentra en el puesto número 4 a nivel regional en recibir ataques cibernéticos y amenazas en línea, estando el podio encabezado por Brasil, México y Venezuela. En lo particular y específico, Argentina ocupa el 2do puesto en pishing[8] y ataques por internet, 3ro en spam[9] y cryptojaking[10], 4to en

[8] Phishing: Método o técnica de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño y suplantando su identidad digital.
[9] Spam: Se denomina así a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor.

boots[11] y 5to en malware[12], ataques a la red y ransomware. Lo que hace pensar seriamente a los dirigentes nacionales sobre la seguridad de su Estado.

Otro caso importante que al día de hoy no se sabe que sucedió exactamente, fue el apagón masivo que se produjo el día 16 de junio de 2019 y afecto a 50 millones de personas en Argentina y Uruguay. En el diario Perfil del día siguiente realizaron una publicación titulada: ¿El apagón masivo en Argentina se produjo por un ataque cibernético? Esta pregunta nace luego que desde la Administración Nacional de Electricidad de Paraguay dijeran que el problema comenzó con un suceso inexplicable en la red eléctrica argentina. A lo que el Secretario de energía Gustavo Lopetegui contesto: "Un ciberataque no es la hipótesis principal, pero no se puede descartar" (Perfil, 2019). Esto provocó trastornos en un día que se celebraban elecciones en las provincias de Formosa, San Luis y Santa Fe y a millones de personas en la segunda mayor economía en América del Sur.

Todos estos casos anteriormente nombrados, son el ejemplo de lo que le puede suceder a un país que posee o no un buen sistema de defensa ante posibles ataques cibernéticos. Nadie puede negar que Estados Unidos, China o Corea del Sur son países que están a la vanguardia en lo que respecta a la seguridad de la información, así mismo son pasibles de este tipo de ataques como lo demuestra la historia reciente.

Siendo Argentina un país que recibe constantemente ataques de este tipo, es que se hace imprescindible la capacitación del personal del Ejército Argentino, en especial sus cuadros, para poder ocupar puestos de ciberdefensa en las diferentes organizaciones con que cuentan las Fuerzas Armadas o que pueden llegar a crearse en un futuro a mediano o largo plazo. En la actualidad solo se posee a nivel Estratégico Militar el Comando Conjunto de Ciberdefensa (CCCD) y en el nivel Táctico el Ejército Argentino posee la Dirección de Ciberdefensa. En estas Unidades se ejecutan operaciones de ciberdefensa, mediante el empleo del ciberespacio, para prevenir, detectar o anular cualquier agresión que afecte los sistemas críticos de las Fuerzas

---

[10] Criptojacking: Método por el cual una amenaza en línea se esconde en una computadora o dispositivo móvil y utiliza los recursos de este para extraer dinero por medio de transacciones digitales.
[11] Bot: Programa informático que efectúa automáticamente tareas repetitivas a través de internet, cuya realización por una persona sería imposible o muy tediosa.
[12] Malware: Código malicioso o dañino, es un *software* que compromete la operación de un sistema al realizar una función o proceso no autorizado (NICCS, 2018). Acorde a la ISO/IEC, fue diseñado específicamente para dañar o interrumpir un sistema sin conocimiento ni consentimiento del propietario.

Armadas y a la Defensa Nacional. Esto requiere de personal altamente capacitado para poder enfrentar este tipo de amenazas.

La ciberdefensa en las Fuerzas Armadas Argentinas

La aparición de un quinto dominio llamado ciberespacio, el cual es transversal y engloba a los tradicionales terrestre, naval, aéreo y espacial, sumado a la evolución de los conflictos en el contexto regional e internacional, los hechos históricos acaecidos en diferentes partes del mundo y teniendo en cuenta los desafíos y riegos que plantea la Directiva de Política de Defensa Nacional, es que se vio la necesidad de crear diferentes elementos que sirvan a la Defensa Nacional en lo referente a las acciones a desarrollar para mitigar las posibles acciones a realizar por medio de ciberataques que pusieran poner en riesgo la seguridad y la vida de los habitantes de esta Nación. En este sentido es que desde el año 2010 y hasta la actualidad es que se han publicado una serie de documentos que buscan complementar o adecuar las diferentes organizaciones de ciberdefensa.

En las Fuerzas Armadas el órgano de mayor entidad sobre temas relacionados a la ciberdefensa es el Comando Conjunto de Ciberdefensa (CCCD) el cual depende en forma orgánica del Estado Mayor Conjunto de las Fueras Armadas (EMCOFFAA), este fue creado en el mes de mayo de 2014 bajo la Resolución Nro 343/2014 del Ministro de Defensa y que posee la siguiente misión:

> Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar. (Comando Conjunto de Ciberdefensa, 2019)

Sus funciones incluyen la coordinación de sus acciones con los Centros de Ciberdefensa de las Fuerzas Armadas y el establecimiento de criterios rectores (a nivel del Instrumento Militar), para la determinación de infraestructuras críticas a ser protegidas. Otras funciones adicionales incluyen:

Entender:

- En el establecimiento de estándares y procedimientos de Ciberdefensa, criptografía e informática forense.

- En la supervisión de los centros de respuesta de cada Fuerza Armada.
- En el proceso de capacitación de personal propio.
- En la organización y desarrollo de actividades académicas (foros, seminarios, simposios, etc.).

Intervenir en la elaboración, revisión y experimentación de Doctrina de Ciberdefensa.

Participar:

- A requerimiento del Ministerio de Defensa, en apoyo a otros Organismos.
- En la concientización de las FF.AA. en materia de Ciberdefensa.
- En la determinación y supervisión de los estándares de seguridad y certificación de protocolos afines en las Fuerzas Armadas.

Por otra parte existen diferentes antecedentes previos a la creación del CCCD (Comando Conjunto de Ciberdefensa, 2019), a saber:

- Resolución Nro 08 del 2010 del Ministerio de Defensa. Creación de un Grupo de Tareas para abordar la temática de la Ciberdefensa desde el punto de vista de la Defensa Nacional.
- Resolución Nro 580 del 2011 de la Jefatura de Gabinete de Ministros. Creación del Programa Nacional de Infraestructuras Críticas de la información y de la Ciberseguridad.
- Resolución Nro 59 del 2012 del Jefe del Estado Mayor Conjunto de las Fuerzas Armadas. Creación de un Elemento de Tareas para tratar Proyectos, Doctrina, Organización y Competencias vinculados con la Ciberdefensa.
- Resolución Nro 385 del 2013 del Ministerio de Defensa. Creación de la Unidad de Coordinación de Ciberdefensa en el Ministerio de Defensa.
- Directiva Nro 02 del 2013 del Jefe del Estado Mayor Conjunto de las Fuerzas Armadas. Elaboración de un Plan Estratégico de Ciberdefensa para el Instrumento Militar.

En lo que respecta a lo específico, el 30 de septiembre del año 2016, la Resolución Nro 2016-256-E-APN-MD ordena la conformación de la Dirección de Ciberdefensa del Ejército Argentino, la cual depende en forma funcional del CCCD. Esta Dirección conduce las operaciones de ciberdefensa en el ámbito del Ejército

Argentino, dando respuesta a posibles ciberataques, buscando prevenir y preservar activos de información de la Fuerza y los que le sean asignados. Además, por estar dentro de la órbita del Estado Mayor Conjunto en forma funcional, como se dijo anteriormente, debe contribuir con la misión del CCCD.

A la fecha, 15 Oct 19, la organización de la ciberdefensa militar cuenta con el CCCD a nivel conjunto y a nivel de cada Fuerza Armada, Direcciones de Ciberdefensa de cada Fuerza. Ver figura 1.

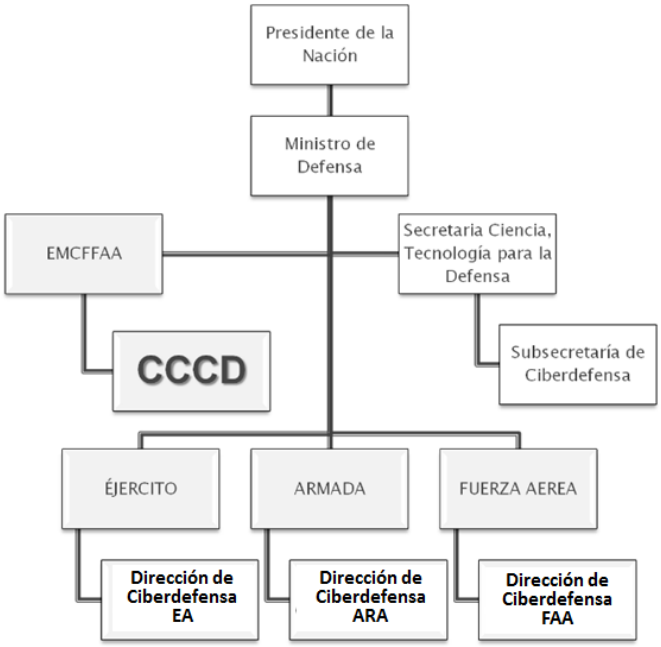


Figura 1: Organización de la Ciberdefensa Militar

Conclusiones parciales

- Los diferentes hechos históricos ocurridos en el mundo y en el país en torno a las diferentes acciones perpetradas por piratas informáticos, que operan en forma independiente para acrecentar su ego personal o por crackers que también actúan en forma independiente o para organizaciones, sean estas convencionales o no, buscando obtener beneficios en forma ilegal o provocar algún tipo de daño a la organización propietaria del sistema, fueron los que con sus acciones establecieron la necesidad de que el personal de las Fuerzas Armadas en todo el mundo deban capacitarse en ciberdefensa para poder enfrentar este tipo de amenazas.

- El caso Estonia fue el más significativo ya que gracias a este la OTAN produjo los Manuales Tallin 1.0 sobre la ley que debería regir la guerra cibernética y Tallin 2.0 el cual que añade un análisis jurídico sobre los incidentes cibernéticos que ocurren más comúnmente o a diario. Estos manuales son de aplicación internacional.
- La creación de organizaciones de ciberdefensa en el ámbito de las Fuerzas Armadas propició la necesidad de dotar a estas con personal capacitado e idóneo para poder operar en este tipo de ambientes, esto también hace imperioso que el personal se perfeccione en esta temática para poder enfrentar las amenazas u acciones que se realicen para desestabilizar la Defensa Nacional.

Capítulo 2
Marco legal y limitaciones existentes en el empleo del ciberespacio en la República Argentina

El presente capítulo buscará determinar las ventajas y limitaciones que presenta el marco legal existente a nivel nacional que regula el empleo del ciberespacio, a fin de poder desarrollar acciones de ciberdefensa y operar en forma segura en el mismo.

Plexo normativo de aplicación en la República Argentina

En lo referente al marco legal para el empleo del ciberespacio, el principal problema es la ausencia de un plexo normativo específico que regule el empleo del mismo, tanto a nivel nacional como internacional. Esto se da por variadas causas, una de las más importantes radica en que normalmente la evolución de las tecnologías y sus consecuencias generan normas luego de haber sucedido los hechos, lo que sumado a la lentitud en la aprobación de estas por parte de sus responsables hace difícil ganar la carrera para poseer una seguridad acorde a las necesidades existentes.

Para mitigar este tipo de falencias es que existe a nivel internacional una serie de acuerdos y convenios que buscan regular el empleo del mismo, como el Convenio de Budapest o Convenio del Consejo de Europa en Delito Cibernético, al cual el país se ha adherido recientemente como ya se ha nombrado anteriormente, la Carta de las Naciones Unidas (Art 41 y 51) o el Manual de Tallin 1.0 sobre el derecho internacional aplicable a la guerra cibernética.

Este manual fue creado en el año 2013 por un grupo de expertos de la OTAN, posteriormente a los ataques recibidos en Estonia por un grupo de hacker, se cree rusos, los cuales pusieron en jaque toda su infraestructura crítica cibernética. Tiene por objeto regular la ley internacional de seguridad cibernética y de los ciberconflictos armados, poseyendo algunas reglas respecto al jus ad bellum[13] y del jus in bello[14], ya que una operación cibernética puede causar lesiones o muerte a personas o daños a objetos. En el año 2017 salió a la luz el Manual de Tallin 2.0 el cual presenta al día de la fecha el análisis más completo existente en legislación sobre

[13] Jus ad bellum: Regulación del derecho internacional a la hora de declarar una guerra y ejecutarla.
[14] Jus in bello: Regulación de ciertos estándares en los conflictos armados cuando ya se están llevando a cabo.

operaciones en el ciberespacio y añade un análisis jurídico sobre los incidentes más comunes y por los cuales no es necesario el uso de la fuerza o de un conflicto armado.

En lo que respecta al marco legal nacional, las leyes fundamentales en que se basa la defensa nacional y que se deben tener en cuenta son la Ley Nro 23.554 – Defensa Nacional, la Ley Nro 24.059 – Seguridad Interior y la Ley 25.520 – Inteligencia Nacional, además de Decreto 703/2018 – DPDN y el Decreto 683/2018 – modificatorio del Decreto 727/2006.

Ley Nro 23.554 – Defensa Nacional

Esta ley fue sancionada el 13 de abril del año 1988 y promulgada posteriormente el 26 de abril de ese mismo año. En su Artículo 1º nombra la finalidad de la presente ley, la cual busca establecer las bases jurídicas, orgánicas y funcionales fundamentales para la preparación, ejecución y control de la defensa nacional. Así mismo el Artículo 2º de esta ley define a la defensa nacional como:

> La integración de la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y libertad de sus habitantes. (Honorable Congreso de la Nacion, 1988)

Como se puede leer, esta Ley limita las agresiones que pueden llegar a recibirse solo a aquellas que sean de origen externo. Posteriormente el Decreto reglamentario 727/2006 del 12 de junio del año 2006 de la presente Ley estipula principios básicos, competencias del Consejo de Defensa Nacional, atribuciones del Ministro de Defensa, del Estado Mayor Conjunto de las Fuerzas Armadas, Fuerzas Armadas y disposiciones complementarias. En este Decreto el Presidente de la Nación, definió en su Artículo 1º:

> Las Fuerzas Armadas, instrumento militar de la defensa nacional, serán empleadas ante agresiones de origen externo perpetradas por Fuerzas Armadas pertenecientes a otro/s Estado/s, sin perjuicio de lo dispuesto en la Ley Nº

> 24.059 de Seguridad Interior y en la Ley Nº 24.948 de Reestructuración de las Fuerzas Armadas en lo concerniente a los escenarios en los que se prevé el empleo del instrumento militar y a las disposiciones que definen el alcance de dicha intervención en operaciones de apoyo a la seguridad interior.
>
> Se entenderá como "agresión de origen externo" el uso de la Fuerza Armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas. (Honorable Congreso de la Nación, 2006)

Se puede ver que con este Decreto, se limita aún más el empleo de las Fuerzas Armadas sobre las acciones que pueden ser realizadas en pos de la Defensa Nacional acotando su accionar a Fuerzas Armadas de otro/s estado/s y entendiendo estas agresiones a las realizadas solo y tan solo por un Estado, excluyendo fuerzas no convencionales como grupos terroristas, crimen organizado o ejércitos de profesionales entre otros, ya que dentro de estos pueden existir fracciones destinadas a realizas operaciones de ciberdefensa o ciberseguridad tanto directa como indirecta. Luego de pasado 12 años y con el cambio de gobierno realizado en el año 2016, el cual posee un pensamiento diferente al gobierno anterior sobre el rol que ocupan las Fuerzas Armadas y la realidad actual que presenta la evolución de las tecnologías de la información y las comunicaciones y los conflictos actuales, es que en el año 2018, el Señor Presidente de la Nación y Comandante en Jefe de las Fuerzas Armadas, por medio del Decreto Nro 683/2018 modificó esta situación decretando se sustituya el Artículo 1º del Decreto Nro 727/2006 (reglamentario de la Ley de Defensa) por el siguiente:

> Las Fuerzas Armadas, instrumento militar de la defensa nacional, serán empleadas en forma disuasiva o efectiva ante agresiones de origen externo contra la soberanía, la integridad territorial o la independencia política de la REPÚBLICA ARGENTINA; la vida y la libertad de sus habitantes, o ante cualquier otra forma de agresión externa que sea incompatible con la Carta de las Naciones Unidas. (Honorable Congreso de la Nación, 2018)

En este nuevo decreto se puede ver que se elimina la restricción de hacer frente solamente a Fuerzas Armadas pertenecientes a uno o varios Estados, pasando estas a emplearse contra agresiones de origen externo, no realizando ningún tipo de diferencia entre fuerzas ya sean convencionales o no convencionales.

También, un cambio importante que ha producido este nuevo decreto hace referencia a lo que se debe entender cuando se habla de "agresión de origen externo", expresando:

> Que este tipo de agresiones no solo son de carácter estatal militar, sino que en ocasiones se manifiestan de otras formas que, sin dejar de tener su origen en el exterior, se desarrollan en nuestro territorio y/o tienen efectos en él, afectando intereses que la Defensa Nacional puede y debe contribuir a preservar. (Honorable Congreso de la Nación, 2018)

Como hemos nombrado anteriormente existe una diferencia entre la Ley de Defensa Nacional y la Ley de Seguridad Interior en cuanto al concepto de Seguridad Nacional, lo que se ve reflejado en su Artículo 4º. La Ley de Defensa Nacional (1988) afirma: "Para dilucidar las cuestiones atinentes a la defensa nacional, se deberá tener permanentemente en cuenta la diferencia fundamental que separa a la defensa nacional de la seguridad interior. La seguridad interior será regida por una ley especial" (p1 Art 4). Por lo que las Fuerzas Armadas no pueden intervenir dentro del propio territorio limitando las acciones que puede llevar a cabo la ciberdefensa. Por otro lado la Ley de Seguridad Interior plantea excepciones por las cuales estas pueden ser empleadas, estas excepciones son:

- Bridar apoyo a operaciones realizadas por Fuerzas de Seguridad – Fuerzas Policiales mediante la acción de sus elementos de intendencia, arsenales, sanidad, veterinaria, construcciones y transportes, así como de ingenieros y comunicaciones (Art 27 – Ley de Seguridad Interior).,
- Restablecimiento del orden dentro de la Jurisdicción Militar y preservación de las Fuerzas Armadas (Art 29 – Ley de Seguridad Interior).
- Como excepción: Las Fuerzas Armadas serán empleadas en el restablecimiento de la seguridad interior dentro del territorio nacional cuando el sistema de seguridad interior sea insuficiente a criterio del Presidente de la Nación. El empleo efectivo operacional de combate, podrá

> realizarse previa declaración del estado de sitio por parte del Congreso Nacional o por parte del Poder Ejecutivo nacional en la figura del Presidente de la Nación en caso de que el Congreso Nacional no se encontrase en funciones (Art 31 y 32 – Ley de Seguridad Interior).

En este último punto, si se podrán realizar acciones relacionadas a la ciberdefensa con la finalidad de preservar el bienestar y la integridad de los habitantes de la República.

Otra de las limitaciones que nos encontramos en esta Ley, se encuentra presente al momento de definir los espacios en lo que las Fuerzas Armadas pueden realizar la Defensa Nacional, los cuales se encuentran demarcados en el Artículo 5º, 28º y 30º.

> **Artículo 5º:** La defensa nacional abarca los espacios continentales, Islas Malvinas, Georgias del Sur y Sandwich del Sur y demás espacios insulares, marítimos y aéreos de la República Argentina, así como el sector antártico argentino, con los alcances asignados por las normas internacionales y los tratados suscriptos o a suscribir por la Nación esto sin perjuicio de lo dispuesto por el art. 28 de la presente ley en cuanto a las atribuciones de que dispone el Presidente de la Nación para establecer teatros de operaciones para casos de guerra o conflicto armado. Contempla también a los ciudadanos y bienes nacionales en terceros países, en aguas internacionales y espacio aéreo internacional. (Honorable Congreso de la Nacion, 1988)

> **Artículo 28º:** Para el caso de guerra o conflicto armado internacional el Presidente de la Nación podrá establecer teatros de operaciones, delimitando las correspondientes áreas geográficas. El comando de cada teatro de operaciones será ejercido por el oficial superior de las Fuerzas Armadas que designe al efecto el Presidente de la Nación, de quién dependerá en forma directa e inmediata. (Honorable Congreso de la Nacion, 1988)

> **Artículo 30º:** El Poder Ejecutivo nacional con aprobación previa del Congreso de la Nación, podrá declarar zona militar a los ámbitos que, por resultar de interés para la Defensa Nacional, deban ser sometidos a la custodia y protección militar.

> En caso de guerra o conflicto armado de carácter internacional o ante su inminencia, tal declaración estará sujeta a la posterior ratificación del Congreso de la Nación. (Honorable Congreso de la Nacion, 1988)

Luego de realizar una lectura analítica de estos últimos tres Artículos, se puede vislumbrar que al momento de definir los espacios de interés de la Nación, solo se definen espacios físicos, dejando afuera al ciberespacio. Esto ocurre por una razón de desarrollo y de evolución ya en el año 1988, momento en que se escribió esta Ley, este factor del ambiente operacional no formaba parte de la problemática de la Defensa como lo hace en la actualidad, encontrándose el empleo del ciberespacio con fines militares en la Directiva de Política de Defensa Nacional como uno de los principales riesgos, además esta interpreta al ciberespacio a la luz de las operaciones militares y la Defensa Nacional, lo que se verá más adelante al momento de analizar dicha Directiva.

Ley Nro 25.520 – Inteligencia Nacional

Respecto de esta ley, la misma tiene la finalidad de establecer las bases jurídicas, orgánicas y funcionales del Sistema de Inteligencia de la Nación. Se deberá tener especialmente en cuenta lo expresado en su el Artículo 5º ya que de no cumplir con este se estaría violando una Ley Nacional:

> Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario. (Honorable Congreso de la Nación , 2001)

Directiva de Política de Defensa Nacional (Decreto Nro 703/2018 – DPDN)

Este decreto es el documento que establece los lineamientos generales de la política de la Defensa Nacional determinado la visión y criterios que orientan la organización, el funcionamiento, la planificación, el desarrollo de capacidades operacionales, el empleo y la administración de los recursos humanos y materiales,

conforme a las apreciaciones estratégicas de los escenarios globales y regionales en materia de defensa y el impacto en la seguridad estratégica de la República Argentina. (Ministerio de Defensa, 2018)

Como se ha nombrado anteriormente la DPDN presenta riesgos para la Defensa Nacional, estos constituyen situaciones cuya probable evolución podría afectar los intereses en materia de defensa. Los riesgos que establece son: la competencia por los recursos estratégicos, ataques externos a objetivos estratégicos y la utilización del ciberespacio con fines militares. Este último riesgo nace de la evolución que han tenido las tecnologías de la información y las comunicaciones (TIC´s) en el escenario nacional, regional, mundial, sumado a los diferentes incidentes que se han sucedido en todo el mundo y que se han nombrado tanto en la introducción como en el capítulo 1 del presente trabajo de investigación. Este desarrollo tecnológico produjo el incremento de los riesgos asociados a la militarización del ciberespacio, consolidando al mismo como un ambiente más para la defensa, dadas las amenazas que podrían afectar intereses estratégicos para el país.

Al analizar este riesgo que se nos plantea, se puede ver que la desconfianza que existe a nivel mundial impacta en las políticas internacionales asociadas a los bienes globales como es el ciberespacio, es por ello que tanto las potencias regionales (Brasil - Chile) y las internacionales (EEUU – China - Rusia) han modernizado sus estrategias de defensa y sus fuerzas debido a la creciente conjunción de formas tradicionales y no tradicionales de agresión e influencia, integrando para esto instrumentos de diferentes índoles como son los económicos, políticos y ciberespaciales.

También este decreto hace foco en el empleo de la disuasión como protagonista relevante para hacer frente a estas amenazas y nueva forma de agresión e influencia; menciona el empleo de información falsa utilizando al ciberespacio como medio de explotación por parte de actores estatales y no estatales. Aunque particulariza que el empleo de amenazas cibernéticas sofisticadas proviene de organizaciones militares y agencias de inteligencia de los Estados, no de grupos o fracciones armadas sin un apoyo directo de estos.

Es por ello que luego de analizar el contexto en el que se aborda al ciberespacio, es que para el área de la Defensa Nacional se plantea una problemática de importancia en torno a la defensa de las Infraestructuras críticas del Sistema de Defensa Nacional y de todas aquellas que designe el poder político para su

preservación, entendiendo por infraestructura críticas de la defensa lo estipulado en la Resolución Nro 1380/2019 del Ministerio de Defensa:

> Son las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto en la capacidad operacional del Instrumento Militar en el ciberespacio y/o en la prestación de los servicios esenciales así como la producción de bienes de interés para la Defensa (Ministerio de Defensa, 2019)

En lo que respecta a lo estrictamente militar la directiva expresa que la consolidación del ciberespacio como un nuevo ambiente operacional configura una amenaza a los intereses estratégicos de la Defensa, esto influenciado por la evolución de las tecnologías y la extensión en forma global de la conectividad, convirtiendo al mismo en un ámbito en el que los Estados realizan acciones ofensivas y de influencia en la población, con el objetivo de ganar la mente, el corazón de estos y atraerlos a su causa generando focos de poder dentro de los países afectados. Es por ello que las organizaciones militares deben adecuarse a estas nuevas tendencias para minimizar el impacto de estos nuevos riesgos.

Las Fuerzas Armadas se encuentran en un proceso de adecuación para enfrentar este tipo de amenazas, el Comando Conjunto de Ciberdefensa es el órgano de mayor peso a nivel militar, dependiendo de este las Direcciones de Ciberdefensa de la Armada, Fuerza Aérea y Ejército y todas estas realizar operaciones interagenciales con otras áreas del gobierno para poder emplear todos los medios disponibles para la protección de las infraestructuras críticas del Estado.

Decisión Administrativa Nro 669/2004 – Políticas de Seguridad de la Información

Esta decisión establece que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del Artículo 8º de la Ley Nº 24.156 – Ley de Administración Financiera y sus modificatorias, deberán dictar o adecuar sus políticas de seguridad. El inciso a) nombra diferentes organismos del Estado los que son parte de la Administración Nacional, uno de ellos es la Administración Central dentro de la cual se encuentran las Fuerzas Armadas y por consiguiente el Ejército Argentino.

Esto basado en que la Administración Publica Nacional debe encontrarse actualizada en el empleo de nuevas tecnologías de gestión, información y comunicación las que poseen la finalidad de prestar servicios de la manera más eficientes y al mismo tiempo mejorar su gestión interna. Estos servicios deben ofrecer las máximas garantías de seguridad para evitar la comisión de delitos para preservar su confidencialidad, integridad y disponibilidad continua e ininterrumpida. Para lograr que esto pueda ser cumplido es que se deberán tener en cuenta las Política de Seguridad Modelo dictadas por Oficina Nacional de Tecnologías de la Información (ONTI) publicadas el 19 de febrero de 2015 bajo la Disposición Nro 01/2015, la cual dentro en su cláusula Políticas de Seguridad de la Información presenta como objetivos a cumplir:

- Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia. (Ofinica Nacional de Tecnologías de Información, 2015)

También esta Decisión Administrativa, ordena a las máximas autoridades de los organismos nombrado anteriormente la conformación de un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del organismo. Este comité tendrá las funciones de:

- Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
  Promover la difusión y apoyo, a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas. (Jefatura de Gabinete de Ministros, 2004)

En particular en las Fuerzas Armadas estos comités se encuentran representados a nivel conjunto por el Comando Conjunto de Ciberdefensa y a nivel específico las Direcciones de Ciberdefensa de la Armada, Fuerza Aérea y Ejército.

Resolución 69/2016 – Programa Nacional contra la Criminalidad Informática

Esta resolución fue sancionada posteriormente a la modificación del Código Penal en el año 2008, al cual se le incorporaron nuevos tipos de delitos vinculados con la criminalidad informática, teniendo en cuenta que la tecnología informática y las telecomunicaciones son un factor de preponderancia para el desarrollo social y económico y que el aumento de este tipo de delitos ha aumentado considerablemente en los últimos años configurando amenazas y riesgos para el Estado y sus ciudadanos los que se ven directamente afectados de manera grave por delitos diversos como la integridad sexual de los menores, los datos personales, la propiedad, la seguridad de las infraestructuras críticas del Estado, entre otras. Es por ello que ante este tipo de problemática se debe crear un Programa Nacional contra la Criminalidad Informática

bajo la órbita del Ministro de Justicia y Derechos Humanos y que tendrá como objetivos generales:

- Promover las acciones necesarias para mejorar las respuestas del sistema penal frente al desafío que plantean los delitos informáticos y los delitos cometidos valiéndose de herramientas de tecnología informática.
- Propiciar la eficiencia en la investigación de las causas penales mediante la utilización de medios modernos de obtención de pruebas basados en tecnología informática y de las telecomunicaciones, garantizando que su utilización se rija por normas respetuosas de los derechos fundamentales de los ciudadanos. (Ministerio de justicia y Derechos Humanos, 2016)

La presente resolución insta a los organismos de ciberdefensa de la fuerza a adecuarse a esta norma para poder accionar ante posibles incidentes en forma legal sobre las personas que realicen este tipo de actividad que principalmente busquen obtener datos de la Fuerza o accionar contra las infraestructuras críticas a defender.

Resolución Nro 829/2019 - Estrategia Nacional de Ciberseguridad

Esta estrategia nacional sienta los principios básicos y los objetivos que le permitan fijar las previsiones en la protección del ciberespacio con la finalidad de brindar un contexto seguro para su empleo por parte de las personas y organizaciones públicas y privadas, desarrollando acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas. (Jefatura de Gabinete de Ministros, 2019)

Esta resolución presenta ocho objetivos a cumplimentar, para este trabajo de investigación, más allá que todos son de importancia para el desarrollo de las acciones a llevarse a cabo en el ciberespacio, tomaremos en cuenta solo tres, estos son:

- **Objetivo Nro 1: Concientización del uso seguro del Ciberespacio**
  - En el marco del presente documento, es el proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ello la adopción de hábitos basados en las mejores prácticas.
  - Para ello será necesario:

        - Incrementar las actividades de concientización en el ámbito educativo.

- **Objetivo Nro 2: Capacitación y educación en el uso seguro del Ciberespacio**
    - En el marco del presente documento, es entendido como el proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio.
    - Para ello será necesario:
        - Promover la formación de profesionales, técnicos e investigadores.
        - Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes.
        - Incrementar las actividades transversales de formación en el sector académico.

- **Objetivo Nro 3: Desarrollo del marco normativo**
    - Adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.
    - Para ello será necesario:
        - Actualizar el marco jurídico tomando en cuenta la necesidad de principios comunes mínimos con la comunidad internacional.
        - Actualizar el marco normativo técnico en línea con las normas técnicas y las buenas prácticas reconocidas internacionalmente.

Particularmente estos objetivos generan acciones las cuales se encuentran en desarrollo, como la concientización en ciberseguridad y ciberdefensa y la creación de normativas, directivas y órdenes por parte del Comando Conjunto de Ciberdefensa y la Dirección de Ciberdefensa del Ejército (DCEA). Con respecto a la concientización, estas dos Unidades realizan charlas o seminarios de concientización en todo el país, las que buscan promover el uso responsable de los medios informáticos con que cuenta la Fuerza. En lo referente al marco legal, ambas se encuentran trabajando en la realización de directivas y órdenes especiales de carácter interno basadas en el plexo

legal nacional vigente para poder normar este tipo de acciones y que las mismas no generen inconvenientes innecesarios por el uso indebido de los medios.

En lo que respecta a la capacitación del personal, tema principal de esta investigación, además de lo realizado por las organizaciones nombradas anteriormente, existen carreras de posgrado dentro de la oferta educativa que presenta la Universidad de la Defensa Nacional en la figura de la Facultad de Ingeniería del Ejército y el Instituto Universitario Aeronáutico que permiten el perfeccionamiento del personal ante este nuevo tipo de amenazas. También en el ámbito civil se dictan carreras afines a la temática tanto en universidades nacionales como privadas en las que el personal puede capacitarse y perfeccionarse. Además, este tipo de capacitación permite a sus egresados ser considerados para formar parte de organizaciones de ciberdefensa y ser parte de los encargados de concientizar sobre esta temática.

Resolución Nro 1523/2019 - Glosario de términos sobre Ciberseguridad (Jefatura de Gabinete de Ministros, 2019)

La Jefatura de Gabinete de Ministros por medio de la Secretaría de Gobierno y Modernización aprobó esta resolución la cual presenta una serie de definiciones, las cuales poseen la finalidad de estandarizar el glosario de términos a utilizar en materia de ciberseguridad. Esta posee dos anexos, el 1ro, presenta la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación de estas y la determinación de los sectores identificados. Define Infraestructuras Críticas como:

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

Y define Infraestructuras Críticas de la Información como: las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas. (Jefatura de Gabinete de Ministros, 2019)

Además, dentro de este mismo anexo presenta ocho diferentes criterios para poder identificar estas Infraestructuras Críticas. De estos, solo nombraremos algunas de ellas para conocimiento general.

> Impacto en la vida humana. Existe impacto para la vida humana, en aquellos casos en los cuales debido a la afectación de un sistema informático, se genere riesgo de pérdida de vida o grave amenaza a la salud e integridad física de las personas. (Jefatura de Gabinete de Ministros, 2019)

> Impacto económico. Existe impacto económico para el país, en aquellos casos en los cuales debido a la afectación de un sistema informático se genere daño o amenaza de daño, grave, a la estructura productiva y/o financiera del país. (Jefatura de Gabinete de Ministros, 2019)

> Impacto en el ejercicio de las funciones del Estado. Existe impacto en el ejercicio de las funciones del Estado, cuando debido a la afectación de un sistema informático, se afecte de manera sustancial el normal desempeño de los órganos de los poderes Ejecutivo, Legislativo o Judicial. (Jefatura de Gabinete de Ministros, 2019)

En su anexo 2do presenta un glosario de términos de ciberseguridad, el cual posee la finalidad de estandarizar la terminología a utilizar en las diferentes áreas componentes del estado que deban emplear este tipo de terminología.

Una de las principales diferencias conceptuales que se presentan al momento de la lectura es la definición de ciberespacio, definiendo al mismo como un ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas TICs. (Jefatura de Gabinete de Ministros, 2019)

Teniendo en cuenta esta definición, se puede ver que toma al ciberespacio solo como un dominio virtual dejando fuera la parte física representada en los cuatro dominios físicos en los que se desarrollan las operaciones militares, lo que produce un conflicto con la definición que se utilizaba hasta ese momento por parte del CCCD y la DCEA la que expresaba:

> El ciberespacio es un ámbito, **tanto físico como virtual**, en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software y hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de información y comunicaciones (TICs).

Otra observancia que se puede realizar de las definiciones que presenta este anexo es la falta de una definición al término ciberdefensa, el cual fue posteriormente definido en la Resolución Nro 1380/19 – Ciberdefensa, la cual veremos a continuación.

Resolución Nro 1380/2019 - Ciberdefensa

En el mes de octubre de 2019, el Ministerio de Defensa publicó en el Boletín Oficial esta resolución la cual presenta 5 artículos en los cuales se presenta la definición de ciberdefensa y la presentación de una Política de Defensa. En su Artículo 1º define a la Ciberdefensa como:

> Las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciber-explotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia. (Ministerio de Defensa, 2019)

Sus otros 4 Artículos son de gran importancia para la ciberdefensa de los cuales se presentan a continuación:

Artículo 2º: Créase el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, donde funcionarán el CENTRO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS DEL MINISTERIO DE DEFENSA (CSIRT de DEFENSA), el CENTRO INTELIGENTE DE OPERACIONES DE SEGURIDAD (iSOC) del COMANDO CONJUNTO DE CIBERDEFENSA del ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS que centraliza la operación de los CENTROS DE OPERACIONES DE SEGURIDAD (iSOC) remotos de cada una de las Fuerzas Armadas y el LABORATORIO DE ANÁLISIS CIBERNÉTICO (CyberLab), entre otras plataformas y sistemas, cuyas actividades y mecanismos de implementación serán definidos por el SUBSECRETARIO DE CIBERDEFENSA a través de los actos pertinentes. (Ministerio de Defensa, 2019)

Artículo 3º: Apruébese la Política de Ciberdefensa consistente en CUATRO (4) Líneas de Acción principales que se desarrollarán conjugando TRES (3) ejes de políticas y cuya implementación se realiza a través de DOS (2) planes en orden de cumplimentar los objetivos aprobados por el artículo 2º del Decreto Nº 684 del 3 de octubre de 2019. (Ministerio de Defensa, 2019)

Artículo 4º: Créase en el ámbito de la SECRETARÍA DE ESTRATEGIA Y ASUNTOS MILITARES, **el Comité Consultivo de Ciberdefensa** que estará integrado por la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y POLÍTICA MILITAR, la SUBSECRETARÍA DE CIBERDEFENSA y el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS, cuyo cometido será la realización de estudios para la definición del Plan de adecuación de las Organizaciones Militares y la preparación de la propuesta de la DIRECTIVA PARA LA ELABORACIÓN DEL PLANEAMIENTO ESTRATÉGICO MILITAR (DEPEM) en materias de Tecnologías de la Información y Comunicaciones y ciberespacio en el término de treinta días desde el dictado de la presente. (Ministerio de Defensa, 2019)

Artículo 5º: Declárense Secreto Militar en los términos del Decreto N° 9390/1963, los Anexos I (IF-2019-96170351-APN-SSC#MD), II (IF-2019-

96170945-APN-SSC#MD), III (IF-2019-96171204-APN-SSC#MD), y V (IF-2019-96171563-APN-SSC#MD) que se acompañan a la presente Resolución. (Ministerio de Defensa, 2019)

Así mismo, esta Resolución cuenta con un Anexo IV, el cual presenta la Política de Ciberdefensa mencionada en el Artículo 3º. En este anexo se presentan Objetivos para cumplimentar la misión recibida por el Ministerio de Defensa, Líneas de Acción para cumplimentar esos Objetivos, Políticas para el desarrollo de estas Líneas de Acción y Planes trazados hacia el cumplimiento de los Objetivos. (Ministerio de Defensa, 2019)

- **Objetivos de la misión del Ministerio de Defensa en el Ciberespacio**
    - Anticipar y prevenir ataques en el ciberespacio.
    - Disminuir vulnerabilidades y aumentar la resiliencia de los sistemas y redes TICs de las FFAA; EMCO y Mindef.
    - Detectar amenazas y gestionar riesgos de ciberataques, y recuperación de los sistemas e infraestructura crítica de interés para la Defensa Nacional.
    - Adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la Defensa.
    - Contribuir a potenciar la base tecnológica e industrial nacional de ciberseguridad en trabajo conjunto con el Ministerio de Relaciones Exteriores y del Ministerio de Producción.
    - Impulsar programas de capacitación, para superar brecha entre los recursos humanos disponibles y los demandados.

- **Líneas de Acción para el cumplimiento de los Objetivos enumerados**
    - **LA1** - Creación del Centro Nacional de Ciberdefensa.
    - **LA2** - Proteger la disponibilidad del ciberespacio como espacio soberano.
    - **LA3** - Reingeniería de las redes de las Fuerzas Armadas, del Estado Mayor Conjunto y del Ministerio de Defensa.
    - **LA4** - Convergencia de las capacidades de las FFAA.

- **Políticas a gestionar para el desarrollo de las cuatro líneas de acción**
    - Política regulatorias (dictarlas, adaptarlas o interactuar).
    - Política de desarrollo de capacidades para la interacción en el ciberespacio.
    - Política de concientización y capacitación.

- **Planes trazados hacia el cumplimiento de los Objetivos**
    - Plan de Adecuación de las organizaciones militares.
    - Plan Nacional de Infraestructuras críticas de la Defensa Nacional

Luego de realizar un análisis de esta Resolución y de su Anexo IV, se pueden identificar las ventajas que esta presenta.

- La creación del Centro Nacional de Ciberdefensa.
- La reafirmación del Decreto 9390/1963 el cual califica al Secreto Militar a toda noticia, informe, material, proyecto, obra, hecho, asunto, que deba, en interés de la seguridad nacional y de los medios de defensa, ser conocido solamente por personas autorizadas y manteniendo fuera del conocimiento de cualquier otra. Ya que de ser conocida la Estrategia de Ciberdefensa por personal que no posea la autorización habilitante, la misma perdería su eficacia.
- La implementación de la Política de Ciberdefensa.
- Presenta al ciberespacio como el quinto dominio soberano de la Nación.
- La búsqueda de la disminución de vulnerabilidades a fin de resguardar las Infraestructuras Críticas y los Servicios Esenciales para la Defensa: plantas de generación eléctrica convención y nuclear, redes de transporte de la energía, comunicaciones, sistemas financieros y otros.

Para este trabajo es de fundamental importancia, el punto 3 de las Políticas a gestionar para el desarrollo de las cuatro líneas de acción, la cual trata sobre la Política de concientización y capacitación. Es por ello que al momento de describir el Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa Nacional, al referirse a los Instrumentos de Política, esta reconoce 3: los Instrumentos regulatorios, los Instrumentos para la interacción en el ciberespacio y los

Instrumentos educativos y de concientización, estos últimos de vital importancia para el presente trabajo. A estos últimos los divide en dos grupos: de concientización y de capacitación.

> **De concientización:** consiste en iniciativas de sensibilización en temas vinculados con la ciberseguridad. Mediante la realización de este tipo de eventos, se genera confianza dentro de la población objetivo y se crea conciencia del propósito y la función del equipo de respuesta a emergencias, lo que le permite operar con mayor eficacia. Uno de los aspectos más importantes de estas actividades es identificar las carencias y las necesidades de información de la comunidad objetivo. (Ministerio de Defensa, 2019)

> **De capacitación:** la capacitación de recursos humanos es otro tema fundamental a abordar y se instrumentará conjuntamente entre los distintos actores del Sistema de Ciberdefensa, convocados en el Consejo Asesor de Ciberdefensa, con la participación especial de la Universidad de la Defensa Nacional, entre otros organismos académicos de la especialidad. Contempla la oferta de Maestría y Especialización en Ciberdefensa dirigidos a profesionales con experiencia y conocimiento en diferentes aspectos específicos vinculados a la ciberdefensa y la ciberseguridad (TIC's, sistemas, derecho informático, políticas públicas, etc.), siguiendo modelos de currícula de los centros de formación de RRHH de renombre internacional.
>
> Asimismo, también se prevé el dictado de diferentes cursos de formación continua. Los cursos técnicos estarán destinados a formar a especialistas en seguridad informática y de redes; los cursos operacionales a entender al ciberespacio como un ámbito militar desde una perspectiva operativa, jurídica y técnica; y los cursos de nivel político – estratégico estarán destinados a desarrolladores de políticas de ciberdefensa y a adquirir conocimiento sobre el derecho internacional aplicable a las operaciones cibernéticas. (Ministerio de Defensa, 2019)

Conclusiones parciales

- La lentitud en la aprobación de las diferentes leyes, decretos, directivas y órdenes, tanto en el ámbito nacional como en el de las Fuerzas Armadas, provoca

arribar a la solución de los problemas en forma tardía, esto producto de la constante y rápida evolución de los métodos utilizados por los encargados de realizar operaciones cibernéticas que evolucionan más rápido que el marco legal.

- La falta de concientización del personal en materia de ciberdefensa y el desconocimiento del marco legal de aplicación a nivel nacional, puede provocar problemas a la seguridad en forma involuntaria que pueden afectar a los intereses de la Nación o de la organización a la que pertenecen. Para ello que se debe implementar lo antes posible el Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa Nacional presentado en la Resolución 1380/2019 en su Anexo IV, mediante la realización de diversos eventos (charlas, capacitaciones, publicidad, etc), con la finalidad de generar confianza dentro de la población y crear conciencia del propósito y la función del equipo de respuesta a emergencias.
- La adhesión a convenios internacionales en materia de ciberdefensa y ciberseguridad favorecen la inserción del país ante el mundo en la lucha contra la ciberdelincuencia, además permite poder hacer frente a agresiones de origen externo, no solo de Fuerzas Militares, sino también de otras formas.
- Las diferencias que existe entre la Ley de Defensa y la de Seguridad Interior con respecto al concepto de Seguridad Nacional, obstaculizan el apoyo que las Fuerzas Armadas se encuentran en capacidad de brindar con la finalidad de mitigar las acciones que afecten tanto las infraestructuras críticas del país como a su población.
- La actualización producida en el Decreto 683/2018 en lo referente al empleo de las FFAA tanto en forma disuasiva como efectiva ante agresiones de origen externo o ante cualquier otra forma de agresión externa y el Decreto PEN 703/2018 (DPDN), el cual al momento de hablar del incremento de los riesgos en base al desarrollo tecnológico asociado a la militarización del espacio, expresa que los actores capacitados para desarrollar medios cibernéticos capaces de explotar vulnerabilidades pueden ser estatales como no estatales, ósea, fuerzan convencionales como no convencionales, facilita la adopción de medidas de seguridad tendientes a proteger los diferentes Objetivos de Valor Estratégicos de la Nación.
- Se debería realizar una actualización de la Ley de Defensa Nacional ya que en la actualidad al momento de establecer un espacio definido para la Defensa, lo que

posteriormente será conocido como Teatro de Operaciones, se tiene en cuenta solo los espacios físicos dejando fuera de este al ciberespacio el cual conforma un nuevo factor del ambiente operacional como lo establece la Directiva de Política de Defensa Nacional.

- Tomando en cuenta lo expresado en la Estrategia Nacional de Ciberseguridad, particularmente lo expresado en sus objetivos 1ro y 2do, es necesario incluir en el proceso de formación de los oficiales y suboficiales, tanto en los Institutos de Formación como en los diferentes cursos regulares y complementarios, materias vinculadas con la ciberseguridad y la ciberdefensa, a fin de concientizar, capacitar y educar al personal en el uso y empleo del ciberespacio. Además, esto permitirá establecer criterios de educación comunes dentro de la fuerza.
- La existencia de diferentes tratados, convenios, estrategias y políticas tanto a nivel nacional como internacional sobre el uso del ciberespacio favorece el desarrollo y ejecución de acciones frente a la aparición de una amenaza cibernética.
- El Glosario de Términos presentado por la Jefatura de Gabinete, el cual busca estandarizar y definir conceptos relacionados con la ciberseguridad y la ciberdefensa, a fin de cerrar diferentes vacíos legales, aun presenta ciertas ambigüedades o diferencias conceptuales como lo es en el caso de la definición de ciberespacio. El mismo debería contrastarse con nuestra doctrina o con la doctrina comparada de otros países como son Estados Unidos de América, Rusia, China o Israel, para así lograr una mayor clarificación en sus términos.
- La aprobación de la Política de Ciberdefensa por medio de la Resolución 1380/2019 del Ministerio de Defensa no solo nos presenta al ciberespacio como un espacio soberano de la Nación sino que también le da la misión el Ministerio de Defensa de anticipar y prevenir ciberataques en el ámbito de la Defensa Nacional, para ello este deberá realizar la reingeniería de las Redes de las Fuerzas Armadas, del Estado Mayor Conjunto y del Ministerio de Defensa, además de la convergencia de las capacidades de las FFAA, lo que permitirá mejorar la seguridad y evitar vulnerabilidades en los sistemas de aquellos elementos que se abocan a la Defensa Nacional.
- La Política de Ciberdefensa insta al Ministerio de Defensa a impulsar programas de concientización para generar confianza y crear conciencia de seguridad, cuestión poco atendida por los usuarios de material perteneciente a las nuevas

TIC´s en la Fuerza. Otro punto importante es la capacitación del personal, lo cual es presentado en forma integral contemplando desde la oferta de Maestrías y Especializaciones dirigidas a profesionales, pasando por la realización de cursos regulares, complementarios y otros dirigidos a personal técnico para formar personal especialista y cursos a nivel político estratégico sobre derecho aplicable a las operaciones cibernéticas. Esto, sumado a la Estrategia Nacional de Ciberseguridad permite generar una línea de concientización y capacitación en dentro de las FFAA y principalmente dentro del Ejército Argentino a fin de que todo el personal comprenda la necesidad de operar en forma segura en el ciberespacio y así poder obtener los recursos humanos necesarios para ocupar puestos es organizaciones relacionadas con la ciberdefensa.

Capítulo 3
Oferta educativa existente a nivel nacional

El presente capítulo tiene por finalidad presentar la oferta educativa existente a nivel nacional, tanto en las Fuerzas Armadas bajo la órbita de la Universidad de la Defensa Nacional como en universidades públicas y privadas de la República Argentina que permita capacitar al personal de oficiales subalternos para poder integrar organizaciones relacionadas con la ciberdefensa.

La formación del oficial subalterno

El reglamento Lineamientos pedagógicos – didácticos de la educación en el Ejército, en su capítulo 1, sobre la educación expresa:

> La educación es un valor que se incorpora al hombre y que este adquiere en mayor o menor grado y que implica siempre, un cambio perfectivo de su comportamiento, de acuerdo con los valores de la cultura en la que está inserto. (Ejército Argentino, 2004, pág. 1)

A los Oficiales y Suboficiales del Ejército Argentino, se les debe dar prioridad en su educación, ya que estos son la columna vertebral de la Fuerza. Esta educación en los oficiales, en los que se centra esta investigación, abarca la formación profesional militar y superior, permitiendo un aprendizaje interdisciplinario con el fin de alcanzar competencias e integrar los conocimientos adquiridos para su desempeño profesional. El mejoramiento de estas competencias se logrará por medio de diferentes acciones educativas que se desarrollan dentro y fuera del Sistema Educativo del Ejército, estas pueden ser: carreras, cursos y el aprendizaje autónomo, entre otras.

Dentro del Sistema Educativo del Ejército (SEE), el subsistema de capacitación profesional busca formar y perfeccionar al personal de cuadros en forma individual con el fin de que estos puedan, a futuro, desempeñar los roles que se le asignen en base a sus conocimientos adquiridos. Las carreras y cursos serán las acciones educativas que se ejecutaran preferencialmente en este sistema, aunque también incluye al aprendizaje autónomo y la Educación Obligatoria. Así mismo, se debe aclarar que el SEE no trabaja en forma independiente, sino que dentro de la

órbita del Sistema Educativo Nacional, bajo el plexo normativo de la Ley de Educación Nacional Nro 26.206, la Ley de Educación Superior Nro 24.521 y la Ley de Educación Técnico Profesional Nro 26.058.

Las carreras son, para esta investigación, el principal elemento orientador que buscará brindar la capacitación necesaria para que el personal pueda ocupar puestos en organizaciones militares relacionados con la ciberdefensa. En el Ejército Argentino, su doctrina define a las carreras como:

> La acción educativa sistemática sujeta a la Ley de Educación Superior o Ley de Educación Técnico Profesional que otorga una titulación académica de grado o posgrado universitario, superior no universitario o técnica, habilitando para ejercer la profesión. Serán evaluadas y acreditadas, cuando corresponda, por la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU), según las normas establecidas por el Ministerio de Educación y Deportes, y evaluadas internamente por el propio Sistema Educativo del Ejército. (Ejercito Argentino, 2016, pág. 51)

La finalidad de esta acción educativa es la de proporcionar al personal la formación profesional, científica y técnica, que se requiere para el ejercicio profesional militar. En lo que respecta a los oficiales subalternos, este tipo de capacitación se desarrollará en su etapa de perfeccionamiento en el ámbito de la Educación Superior, en el Ejército Argentino en los institutos de formación superior con que cuenta o por medio del área de Extensión la que realiza diferentes convenios con universidades civiles, siempre que estas universidades posean carreras que respondan a las necesidades específicas de la Fuerza en pos del logro de los perfiles profesionales esperados y de la evolución profesional que se desea de su integrante.

Como hemos nombrado en la sección anterior, en la actualidad existen solo dos Unidades, una a nivel conjunto y una a nivel específico, que poseen la misión y la capacidad de realizar operaciones de ciberdefensa y en las cuales podrían ser destinados oficiales subalternos para ocupar puestos en ellas. Pero para poder ocupar estos puestos, estos oficiales deben estar capacitados en la materia.

Actualmente el CCCD, ha diseñado un Plan de Formación en Ciberdefensa para el personal de las Fuerzas Armadas, tanto para oficiales como suboficiales, este plan ha sido expuesto a las autoridades del Ministerio de Defensa y actualmente se

encuentra en análisis y estudio por esa cartera. El plan prevé la capacitación de los oficiales en diferentes etapas. En lo que respecta a los subalternos se divide en Formación Básica y Formación Especial. La primera está dividida en dos, se comienza con una Formación Inicial básica en ciberdefensa en los Institutos de Formación, para luego una vez egresados continuar con el perfeccionamiento del mismo por medio de clases dentro de una materia durante la realización de cursos regulares. La segunda busca la formación de los oficiales en los Institutos Superiores. Cada una de estas etapas propone objetivos a alcanzar, en la Etapa Básica de busca que el personal incorpore conceptos básicos de seguridad de la información en el ciberespacio, ciberseguridad y ciberdefensa para conocer las amenazas, riesgos, vulnerabilidades y metodologías básicas para proteger las organizaciones, además de comparar las diferentes doctrinas militares de ciberdefensa y los aspectos del Derecho Internacional Humanitario vinculados al ciberespacio. En la etapa de Formación Especial se busca completar los conceptos fundamentales de ciberseguridad y ciberdefensa para comprender los riesgos y vulnerabilidades de las TIC en las operaciones militares, proporcionar asesoramiento de Operaciones del Ciberespacio e integrar los planes particulares en el planeamiento y la conducción de las operaciones en los niveles Táctico y Operacional. Además, profundizar el conocimiento de la doctrina específica y conjunta de ciberdefensa, el marco legal nacional y los aspectos del DIH vinculados al ciberespacio durante las operaciones militares.

Teniendo en cuenta esta propuesta y centrándonos en los oficiales subalternos, es que se hace necesario capacitar a este personal en lo referente a la temática que se aborda a fin de que estos posean las capacidades necesarias para poder dirigir las operaciones a realizarse en este tipo de ambiente formando parte de las organizaciones existentes o las que a futuro se lleguen a implementar.

Para poder capacitar al personal se planteará un esquema dividido en dos etapas. Una etapa inicial a mediano plazo buscando aprovechar la oferta educativa existente en el ámbito de las Fueras Armadas y otra a largo plazo analizando universidades públicas y privadas.

Oferta educativa existente en el ámbito en las Fuerzas Armadas

La Universidad de la Defensa Nacional (UNDEF) es la organización educativa que regula la educación en las Fuerzas Armadas en forma específica y conjunta.

Esta se encuentra trabajando para implementar una política académica que adopta un modelo de formación basado en competencias, lo que permitirá afrontar no solo la obsolescencia del conocimiento científico y tecnológico, sino también integrar, por un lado, las dimensiones académicas con las trayectorias profesionales y, por otro, lo común de la formación militar con lo específico de cada Fuerza. De este modo, la política educativa que la orienta está en consonancia con las necesidades de la Fuerza en cumplimiento de su misión, con los cambios científicos, tecnológicos y las situaciones que emerjan en el contexto del país (UNDEF, 2019). Esta política académica se encuentra orientará a:

- Desarrollar la formación militar y civil en consonancia con los objetivos que la sociedad en su conjunto requiere para la Defensa Nacional.
- Mejorar la calidad y pertinencia de los programas académicos requeridos por el sistema universitario nacional y las políticas de Defensa Nacional.
- Promover la articulación de la Universidad, mediante la realización de proyectos académicos comunes, con otras instituciones del sistema universitario y del científico tecnológico nacional.
- Garantizar acciones tendientes a favorecer la inclusión y la calidad de la formación de los jóvenes, a través del desarrollo de dispositivos pedagógicos e institucionales apropiados en todas las etapas de las trayectorias educativas.
- Contribuir a la producción del conocimiento a través de políticas institucionales que vinculen las funciones de docencia de pregrado, grado y posgrado con las de investigación y extensión.

De la UNDEF dependen diferentes unidades educativas, de las cuales dos poseen dentro de su oferta educativa posgrados orientados a la ciberdefensa. Estas Unidades Académicas son: la Facultad de Ingeniería del Ejército (FIE) que se encuentra en el ámbito de la Ciudad Autónoma de Buenos Aires y que cuenta con la Especialización en Criptografía y Seguridad en Teleinformática y la Maestría en Ciberdefensa y el Centro Regional Universitario Córdoba - Instituto Universitario Aeronáutico, ubicado en la capital de la provincia, en la que se dicta la Maestría en Ciberdefensa y la Especialización en Seguridad Informática.

Oferta educativa de la Facultad de Ingeniería del Ejército

Especialización en criptografía y seguridad en teleinformática (Facultad de Ingeniería del Ejército, 2019)

El objetivo general de la misma es:

> Posibilitar a los graduados en informática, telecomunicaciones y electrónica el conocimiento y la profundización de los conceptos fundamentales que hacen a los sistemas de seguridad utilizados para resguardar la información. Incluye, además, las herramientas teóricas y prácticas que es necesario utilizar, tanto durante su procesamiento, como durante la fase de transmisión. (Facultad de Ingenieria del Ejército, 2019)

Los objetivos particulares son:

- Proporcionar conocimientos teóricos / prácticos sobre Criptografía y Seguridad Teleinformática, relacionados especialmente, a los Sistemas de Información y a las Redes de Computadoras, sobre las que estos sistemas utilizan para su vinculación.
- Dar a conocer las técnicas y los protocolos que se emplean habitualmente para asegurar un reparto seguro y confiable de la información, y un acceso controlado a la misma en instalaciones de uso compartido.
- Facilitar el dominio práctico de los algoritmos más importantes que se emplean para cifrar la información con la finalidad de asegurar una transmisión confiable, a costo mínimo.
- Dar a conocer los algoritmos y sistemas de autenticación, protección y privacidad más utilizados, así como con las tácticas más comunes de criptorruptura de cifrados.
- Posibilitar en los graduados la actualización de nuevos enfoques técnico-metodológicos y marcos teóricos relativos a las ciencias de la computación vinculada con la Seguridad Informática.

- Enseñar las problemáticas actuales emergentes de los paradigmas fundamentales de los Sistemas de Información y las Redes Teleinformáticas.
- Caracterizar la vinculación de los problemas que genera la necesidad de tener Sistemas Teleinformáticos con la operación eficaz de las Redes de Computadoras y los costos consecuentes.
- Articular teoría y práctica desde los conocimientos específicos para un aprovechamiento integrado de la práctica profesional.
- Facilitar el análisis, en sus múltiples dimensiones, de las características de los modelos criptográficos formales en sus diferentes lógicas y sus algoritmos de encriptamiento.
- Integrar marcos teóricos y estrategias de acción, con la finalidad de abordar satisfactoriamente modelos de estudio de costos y factibilidad de Sistemas Informáticos de Seguridad. (Facultad de Ingenieria del Ejército, 2019)

Esta se encuentra orientada a:

Proporcionar conocimientos teóricos prácticos sobre criptografía y seguridad de los Sistemas Informáticos, el dominio práctico de algoritmos empleados para el cifrado de datos y actualizar al personal frente a los nuevos enfoques que se presentan en la actualidad sobre de la seguridad informática. (Facultad de Ingenieria del Ejército, 2019)

Su modalidad de cursada es presencial, posee una duración de 1 año, dividido en 2 semestres con una carga horaria total de 389hs y con la obligatoriedad de entregar un trabajo final integrador para su aprobación. Anexo B: Plan de estudios de la Especialización en Criptografía y Seguridad en Teleinformática de la Facultad de Ingeniería del Ejército.

La misma se encuentra con Resolución Ministerial Nro 2277/2019 y acreditada por medio de la Resolución CONEAU Nro 844/2011 y categorizada por esta como “B” – Muy buena.

Maestría en ciberdefensa (Facultad de Ingeniería del Ejército, 2020)

Esta maestría se encuentra articulada con la Especialización en Criptografía y Seguridad Informática. Tiene por objetivo general:

> Formar profesionales con los conocimientos y las aptitudes necesarias para diseñar, desarrollar, implementar y gestionar las tecnologías necesarias que posibiliten la protección cibernética de los activos e infraestructuras críticas. (Facultad de Ingeniería del Ejército, 2020)

Se encuentra orientada a capacitar a los egresados para que estos puedan realizar el planeamiento de programas, procedimientos y normas relacionadas con la Ciberseguridad, así como para definir, analizar y evaluar los riesgos y amenazas inherentes a el uso de las TIC en su impacto en la información y en los activos informáticos de las organizaciones. (Facultad de Ingeniería del Ejército, 2020)

Al igual que la Especialización en Criptografía, su modalidad de cursada es presencial, posee una duración de 2 años, dividido en 2 semestres por año, con una carga horaria total de 748hs y con la obligatoriedad de entregar un trabajo final integrador para su aprobación. Anexo C: Plan de estudios de la Maestría en Ciberdefensa de la Facultad de Ingeniería del Ejército. (Faculta de Ingeniería del Ejército, 2020)

La misma posee reconocimiento oficial provisorio por medio de la Resolución Ministerial Nro RESOL-2019-2660-APN-MECCYT, de fecha 04 de septiembre de 2019, hasta tanto sea evaluada por la Comisión Nacional de Evaluación y Acreditación Universitaria.

Oferta educativa del Instituto Universitario Aeronáutico

Maestría en Ciberdefensa (Centro Regional Universitario Córdoba IUA, 2019)

El objetivo de esta maestría es el de: “formar profesionales para dar respuesta a los nuevos desafíos de seguridad para neutralizar y controlar las amenazas cibernéticas que se producen por la evolución de las tecnologías de la información y las comunicaciones” (Centro Regional Universitario Cordoba IUA, 2019)

En lo que respecta al plan de estudios, este tiene una duración de 2 años. Su modalidad de cursada es presencial. En el primer año se dictan materias obligatorias y electivas (se deben completar como mínimo 168hs), en el segundo año se dictan todas materias obligatorias y se debe presentar y aprobar una Tesis de Maestría. Posee una carga horaria total de 748hs. Anexo D: Plan de estudios de la Maestría en Ciberdefensa del Instituto Universitario Aeronáutico. (Centro Regional Universitario Cordoba IUA, 2019)

Esta maestría se encuentra reconocida oficialmente en forma provisoria, esto se otorga a todas la carreras nuevas hasta tanto se realice un dictado completo de la misma, este reconocimiento fue expedido por el Ministerio de Educación Cultura, Ciencia y Tecnología de la Nación, por medio de la Resolución Nro 1298/2019 de fecha 13 de mayo, luego de haber sido evaluada favorablemente por la CONEAU. (Centro Regional Universitario Cordoba IUA, 2019)

Especialización en Seguridad Informática (Centro Regional Universitario Córdoba - IUA, 2019)

El objetivo que busca alcanzar esta especialización es el de:

> Formar profesionales en las temáticas y problemáticas relacionadas con las aplicaciones y técnicas necesarias para la detección de vulnerabilidades en los sistemas informáticos, capaces de enfrentar problemas complejos de seguridad de la información con un conjunto de herramientas tecnológicas especializadas y modernas, a los efectos de poder proteger uno de los activos más importantes de las organizaciones, la información. (Centro Regional Universitario Córdoba IUA, 2019)

El perfil profesional al que apunta esta especialización busca que el egresado posea habilidades para:

- **Planeamiento:**
    - Elaborar los planes, programas, procedimientos y normas relacionados con la ciberdefensa para ejecutar y/o apoyar los objetivos de las organizaciones.

- Definir, analizar y evaluar los riesgos y amenazas inherentes al uso de la TIC y su impacto en las infraestructuras críticas de la defensa.
- Participar en el diseño de sistemas de información técnicamente factible y económicamente aceptable, considerando las buenas prácticas y los estándares de seguridad vigentes.
- Comprender y gestionar los aspectos tecnológicos, humanos, legales y éticos que inciden en la ciberdefensa.
- Planificar auditorías de ciberdefensa.

- **Ejecución:**
  - Aplicar las medidas de protección adecuadas respecto de las ciberamenazas identificadas sobre las infraestructuras críticas de la organización, la organización en si misma y sus individuos, con la finalidad de reducir o anular los riesgos inherentes a la ciberdefensa.
  - Ejecutar los procedimientos y normas relacionados con la ciberseguridad, recuperación de desastres y continuidad de las operaciones relacionadas con la ciberdefensa.
  - Evaluar las herramientas y los recursos tecnológicos requeridos para producir las respuestas necesarias ante cada tipo de incidente.
  - Ejecutar auditorías de ciberdefensa, realizar la explotación y proponer las acciones correctivas necesarias.

- **Asesoramiento:**
  - Ejercer el asesoramiento y la consultoría en materia de ciberdefensa, en organizaciones públicas o privadas.

Esta especialización posee una duración de cursada de un año en forma presencial, dividida en ocho módulos, desarrollándose cuatro módulos por cuatrimestre. Además, se debe presentar un Trabajo Final Integrador el cual luego de pasar por un tribunal evaluador que de aprobarlo, posteriormente

deberá ser expuesto. Para esto el alumno posee dos años para presentar y defender el trabajo final. Una vez expuesto y aprobado obtendrá el título de Especialista en Seguridad Informática, el cual posee reconocimiento oficial con validez nacional del mismo ya que es otorgado por el Ministerio de Educación, Ciencia y Tecnología. Anexo E: Plan de estudios de la Especialización en Seguridad Informática del Instituto Universitario Aeronáutico. (Centro Regional Universitario Cordoba IUA, 2019)

Por otro lado la Especialización en Seguridad Informática se encuentra acreditada por un período de seis años por medio de la Resolución Ministerial Nro 82 del 02 de febrero de 2012 y la Resolución Nro RESFC-2016-37-APN-CONEAU del 19 de octubre de 2016, como categoría B. (Centro Regional Universitario Córdoba IUA, 2019)

El contar con este tipo de oferta educativa permite al personal de oficiales del Ejército Argentino, tanto subalternos como jefes y superiores, la posibilidad de capacitarte para poder ocupar puestos en organizaciones de ciberdefensa. En lo referente a los oficiales subalternos, en el mediano plazo, incrementar la participación de estos en este tipo de carreras por medio de incentivos, como becas y flexibilización en su horario laboral para poder concurrir y cumplir con las horas cátedra requeridas para aprobar la misma, permitiría contar con personal para ocupar puestos en las organizaciones de ciberdefensa que existen en la actualidad y poseer una reserva tanto para reemplazar al personal anteriormente nombrado o para ocupar puestos en las nuevas organizaciones que puedan crearse a futuro.

Oferta educativa existente en el ámbito público y privado

En lo que respecta al largo plazo, se deberían implementar convenios con universidades tanto nacionales como privadas que dicten carreras afines. Un ejemplo de esto es la Universidad de Buenos Aires (UBA), en la que se dicta la Maestría en Ciberdefensa y Ciberseguridad, aprobada por la CONEAU en sesión Nro 501/2019, el objetivo de esta carrera es el de:

Complementar la formación de agentes gubernamentales y de ejecutivos empresariales mediante una sólida formación conceptual y una intensa

> capacitación instrumental en ciberdefensa y en ciberseguridad, de manera de posibilitar su actuación en casos de cibercrimen, especialmente en los casos de cibercrimen Organizado Transnacional, ciberespionaje, Activismo Hacker, ciberterrorismo y también en los casos de ciberagresiones entre estados naciones. (Universidad de Buenos Aires, 2019)

Esta maestría posee un régimen de estudio teórico práctico con una duración 2 años y se debe presentar un trabajo final de maestría para su aprobación. Esta otorga el título de Magister de la Universidad de Buenos Aires en Ciberdefensa y Ciberseguridad. Anexo F: Plan de estudios de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de Bueno Aires.

Conclusiones parciales

- La aprobación del Plan de Formación en Ciberdefensa propuesto por el CCCD, permitirá que todo el personal de las Fuerzas Armadas pueda capacitarse en esta materia, generando un standard en la adquisición de conocimientos durante gran parte de su carrera militar, permitiendo contar con gran cantidad de personal capacitado para cubrir puestos en organizaciones militares relacionadas con la ciberdefensa de acuerdo a sus capacidades y conocimientos adquiridos.
- Las carreras serán la mejor acción educativa a emplear para capacitar de manera técnico, profesional y científicamente al personal de oficiales subalternos que deseen formar parte de organizaciones militares de ciberdefensa.
- El contar con Unidades Académicas bajo la órbita de la UNDEF permite proporcionar a los oficiales subalternos las herramientas necesarias para capacitarse adecuadamente en ciberdefensa, bajo un modelo basado en competencias permitiéndoles obtener conocimientos científico y tecnológicos, además de integrar las dimensiones académicas profesionales y la formación militar, todo esto orientado a las necesidades de las Fuerza Armadas.
- La oferta educativa existente en la UNDEF permite a los oficiales subalternos capacitarse en ciberdefensa en dos puntos neurálgicos como son la Ciudad Autónoma de Buenos Aires (CABA) y la Ciudad de Córdoba, contando con 3 carreras de posgrado diferentes pero todas orientadas a la temática de estudio.
- Las cuatro carreras de posgrado que se encuentran en capacidad de cursar los oficiales subalternos tienen la fortaleza que se encuentran aprobadas y

acreditadas por la CONEAU, lo que les permite la utilización de este título a nivel nacional.

Conclusiones Finales

- Más allá que este trabajo final integrador busca obtener conclusiones a fin de establecer el nivel de capacitación que debe obtener los oficial subalterno para poder integrar organizaciones militares relacionadas con la ciberdefensa, se debe tener en cuenta que las amenazas cibernéticas no son exclusivas de las Fuerzas Armadas de un país, sino que estas producen acciones sobre todo organismo tanto públicos o privados buscando desestabilizarlos y obtener algún tipo de beneficio, lo que plantea la necesidad de capacitar al personal en esta temática en particular.
- Teniendo en cuenta que los oficiales subalternos egresan del Colegio Militar de la Nación con un título de grado (Licenciado en Conducción Gestión Operativa - Resolución Rectoral UNDEF N° 350/2017 - 07Dic2017) y luego de analizar la oferta educativa relacionada con la ciberdefensa existente en las Unidades Académicas dependientes de la Universidad de la Defensa Nacional y en la Universidad de Buenos Aires, los posgrados proporcionarán el nivel de conocimientos necesarios para que este personal pueda capacitarse a fin de ocupar puestos o desempeñar roles en las organizaciones relacionadas con la ciberdefensa existentes en el ámbito de las Fuerzas Armadas.
- Los perfiles y objetivos que poseen los tres carreras de posgrado que presenta la oferta educativa de la UNDEF permiten a los oficiales subalternos interesados en integrar organizaciones militares de ciberdefensa cumplir con los estándares necesarios para tal fin.
- La implementación de los principios rectores y los objetivos de la Estrategia Nacional de Ciberseguridad buscan principalmente concientizar al personal tanto de las Fuerzas Armadas como a la población en general en la importancia que tiene la seguridad de la información ante el avance de las tecnologías de la información y las comunicaciones y la vulnerabilidad que estas presentan.
- En base a los objetivo número 2 y 3 de la Estrategia Nacional de Ciberseguridad, se debe trabajar en la capacitación del personal de la fuerza, en lo que respecta a este trabajo de investigación, ampliar la oferta educativa en las universidades que dependen de la UNDEF en materia de ciberdefensa y crear convenios con universidades públicas y privadas que posibiliten a los oficiales subalternos interesados en integrar organizaciones de ciberdefensa poder perfeccionarse en estas.

- Sería muy beneficioso para todo el personal de las Fuerzas Armadas la aprobación del Plan de Formación en Ciberdefensa propuesto por el CCCD, ya que este permitiría capacitar al personal desde el momento que se encuentran en los institutos de formación y hasta avanzada su carrera militar, generando un número importante de personas capacitadas en la temática con las que hoy en día no se cuenta.
- La capacitación del personal de los oficiales subalternos para la conducción de operaciones de ciberdefensa requiere de conocimientos técnicos que deberían implementarse con cursos regulares, complementarios y capacitaciones Ad hoc en la figura de seminarios, conferencias, juegos de simulación y otros. Esta modalidad permitiría completar los conocimientos y habilidades que se requieren para comprender las tácticas, técnicas y procedimientos, tanto en Ciberoperaciones ofensivas como defensivas, así como mantenerse actualizados con la dinámica necesaria.
- La desactualización que presentan las leyes de Defensa Nacional y de Seguridad Interior, provoca un conflicto de intereses que dificulta el apoyo que las Fuerzas Armadas pueden brindar para mitigar las acciones que afecten a la seguridad Nacional. Así mismo, se debe actualizar el concepto de espacios físicos, teniendo en cuenta al ciberespacio como un nuevo elemento del ambiente operacional, ya que en la actualidad este concepto limita el empleo de los medios cibernéticos.
- La existencia de una Estrategia Nacional de Ciberseguridad, con la cual no se contaba hasta el año 2019, permite desarrollar una estrategia militar de aplicación sobre la Defensa Nacional, por medio de principios básicos y objetivos a alcanzar al mediano y largo plazo a fin de brindar un contexto seguro por medio del desarrollo de acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas.

Aporte profesional del autor

- Empleando a la UNDEF como núcleo de formación, crear a mediano plazo un sistema de capacitación para oficiales subalternos destinados en Unidades de la Ciudad Autónoma de Buenos Aires / Gran Buenos Aires y en la provincia de Córdoba, específicamente en su capital, que prevea un cupo limitado de ingreso a

las carreras de posgrado que ofrecen estas dos instituciones (FIE - IUA), apoyado en un sistema de becas que permita que el personal interesado, previa entrevista de ingreso y acreditación de título de grado habilitante, puedan perfeccionarse técnico profesionalmente y científicamente para en un futuro ocupar puestos en organizaciones miliares relacionadas con la ciberdefensa, ya sean las existentes en las Fuerzas Armadas o las que puedan llegar a crearse en un futuro producto de la evolución de las mismas. A largo plazo crear convenios con universidades públicas y privadas que permitan al personal que se encuentra destinado en otras provincias acceder a este tipo de capacitación.

Bibliografía

Documentos oficiales

Honorable Congreso de la Nación . (03 de Diciembre de 2001). Ley Nro 25.520 - Inteligencia Nacional. CABA, Argentina.

Honorable Congreso de la Nacion. (26 de Abril de 1988). Ley 23.554 - Defensa Nacional. CABA, Argentina.

Honorable Congreso de la Nación. (12 de Junio de 2006). Decreto 727/06 - Reglamentacion de la Ley 23.554. CABA, Argentina.

Honorable Congreso de la Nación. (23 de Julio de 2018). Decreto 683/06 - Reglamentacion de la Ley 23.554. caba, Argentina.

Infobae. (19 de 06 de 2017). *Hackearon la página del Ejército Argentino con supuestas amenazas de ISIS*, pág. 1.

Jefatura de Gabinete de Ministros. (20 de Diciembre de 2004). Decisión Administrativa 669/2004 - Políticas de Seguridad de la Información. CABA, Argentina.

Jefatura de Gabinete de Ministros. (12 de Septiembre de 2019). Resolución 1523/2019 - Glosario de términos de ciberseguridad. CABA, Argentina.

Jefatura de Gabinete de Ministros. (12 de Septiembre de 2019). Resolución 1523/2019 - Glosario de términos de ciberseguridad - Anexo I. CABA, Argentina.

Jefatura de Gabinete de Ministros. (12 de Septiembre de 2019). Resolución 1523/2019 - Glosario de términos de ciberseguridad - Anexo II. CABA, Argentina.

Jefatura de Gabinete de Ministros. (24 de Mayo de 2019). Secretaría de Gobierno de Modernización. *Resolución Nro 829/2019 - Estrategia Nacional de Ciberseguridad*. CABA, Argentina.

Ministerio de Defensa. (14 de Mayo de 2014). Resolución MD N° 343/14. *Comando Conjunto de Ciberdefensa*. CABA, Argentina.

Ministerio de Defensa. (2015). *Libro Blanco de la Defensa.* CABA: Latingráfica.

Ministerio de Defensa. (30 de Septiembre de 2016). Resolución Nro 2016-256-E-APN-MD. CABA, Argentina.

Ministerio de Defensa. (30 de Julio de 2018). Directiva de Política de Defensa Nacional. CABA, Argentina.

Ministerio de Defensa. (25 de Octubre de 2019). Resolución 1380/19 - Ciberdefensa - Anexo IV. CABA, Argentina.

Ministerio de Defensa. (25 de Octubre de 2019). Resolución 1380/2019 - Ciberdefensa. CABA, Argentina.

Ministerio de Defensa. (12 de Septiembre de 2019). Resolución 1523/2019 - Glosario de términos sobre ciberseguridad. CABA, Argentina.

Ministerio de justicia y Derechos Humanos. (11 de Marzo de 2016). Resolución 69/2016 - Programa Nacional contra la Criminalidad Informática. CABA, Argentina.

Ofinica Nacional de Tecnologías de Información. (19 de Febrero de 2015). Disposición Nro 01/2015 - Política de Seguridad Modelo . CABA, Argentina.

Poder Ejecutivo Nacional. (30 de Julio de 2018). Directiva de Políticas de Defensa Nacional. *Decreto 703/2018*. CABA, Argentina.

Libros

Gibson, W. (1984). *Neuromante.*
Rodriguez Cisneros, E. (2012). *Desafíos Operaionales en el Ciberespacio como nuevo campo de lucha.* CABA.
RAE. (2011). *Diccionario de la Real Academia de la Lengua Española - Version Digital v15.0.* Madrid.

Reglamentos

DOD Dictionary. (2020). *Joint Publication 1-02 - Department of Defese Dictionary Of Military Associated Terms.*
Ejército Argentino. (2004). *MFD-51-02 - Lineamientos pedagójicos - didácticos de la educación en el Ejército.* CABA.
Ejército Argentino. (2015). *ROB-00-01 - Conducción de las Fuerzas Terrestres.* CABA.
Ejercito Argentino. (2016). *RFD-51-01 - Educación en el Ejército.* CABA.
Ejército Argentino. (2016). *ROD-05-01- Coceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica.* CABA.
EMCOFFAA. (2015). *PC-00-02 - Diccionario de términos de empleo militar para la Acción Militar Conjunta.* CABA.

Publicaciones y artículos

Anca, L. J. (2015). *La conducción de las operaciones de Ciberdefensa: Principios básicos en el campo de combate moderno.* CABA.
Baretto, J. F. (2017). *La defensa nacional y la estrategia militar de seguridad cibernética.* CABA.
De Vergara - Trama. (2017). *Operaciones Militares Cibernéticas – Planeamiento y Ejecución en el Nivel Operacional.* CABA: Visión Conjunta.
Grogovinas, A. (2018). *La visualización de un marco referencial para el Nivel Operacional.* CABA.
Manual Tallin. (2013). *Manual Tallin sobre el derecho internacional aplicable a la guerra cibernética.* Cambridge: Cambridge University Press.
UIT. (2006). *Informe sobre las infraestructuras nacionales de seguridad del ciberespacio.* Informe sobre la Cuestión 9-1/2, Unión Internacional de Telecomunicaciones, Ginebra.

Sitios Web

Centro Regional Universitario Córdoba - IUA. (2019). *Centro Regional Universitario Córdoba IUA.* Recuperado el 26 de Sep de 2019, de https://www.iua.edu.ar/?page_id=571
Centro Regional Universitario Cordoba IUA. (2019). *Centro Regional Universitario Cordoba IUA.* Recuperado el 26 de Sep de 2019, de https://www.iua.edu.ar/?p=4191
Centro Regional Universitario Cordoba IUA. (2019). *Centro Regional Universitario Cordoba IUA.* Obtenido de https://www.iua.edu.ar/?page_id=3543
Centro Regional Universitario Cordoba IUA. (2019). *Centro Regional Universitario Cordoba IUA.* Obtenido de https://www.iua.edu.ar/?page_id=571#contenidos
Centro Regional Universitario Córdoba IUA. (2019). *Centro Regional Universitario Córdoba IUA.* Obtenido de https://www.iua.edu.ar/?page_id=3543

Centro Regional Universitario Córdoba IUA. (2019). *Centro Regional Universitario Córdoba IUA*. Obtenido de https://www.iua.edu.ar/?page_id=571#objetivos

Centro Regional Universitario Córdoba IUA. (2019). *Centro Regional Universitario Córdoba IUA*. Obtenido de https://www.iua.edu.ar/?page_id=571#coordinador

Comando Conjunto de Ciberdefensa. (2019). *Comando Conjunto de Ciberdefensa*. Obtenido de http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx

Comando Conjunto de Ciberdefensa. (2019). *Comando Conjunto de Ciberdefensa*. Obtenido de http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/ResenaHistorica.aspx

EcuRed. (4 de Junio de 2019). *EcuRed*. Recuperado el 17 de Junio de 2019, de https://www.ecured.cu/Harold_Lasswell

EcuRed. (4 de Junio de 2019). *EcuRed*. Recuperado el 17 de Junio de 2019, de https://www.ecured.cu/Enfoque_sist%C3%A9mico

Edefa, G. (2019). *Defensa.com*. Recuperado el 14 de Junio de 2019, de https://www.defensa.com/cyberseguridad/ejercito-brasileno-inaugura-escuela-defensa-cibernetica-ano

Ejército de Brasil. (2015). *CCOMGEX*. Recuperado el 13 de Junio de 2019, de Comando de Comunicaciones e Informática del Ejército: http://www.ccomgex.eb.mil.br/index.php/historico-ccomgex

Ejercito de Brasil. (12 de Enero de 2019). *ESCOM*. Recuperado el 13 de Junio de 2019, de www.escom.br

Estado Mayor Conjunto Operacional. (14 de Junio de 2019). *Comado Conjunto Cibernético*. Recuperado el 14 de Junio de 2019, de https://www.ccoc.mil.co/

Faculta de Ingeniería del Ejército. (2020). *Faculta de Ingeniería del Ejército - Universidad de la Defensa Nacional*. Obtenido de http://www.fie.undef.edu.ar/?attachment_id=7545

Facultad de Ingenieria del Ejército. (2019). *Facultad de Ingenieria del Ejército - Universidad de la Defensa Nacional*. Obtenido de http://wp.iese.edu.ar/?page_id=900

Facultad de Ingeniería del Ejército. (2019). *Facultad de Ingeniería del Ejército - Universidad de la Defensa Nacional*. Recuperado el 18 de 09 de 2019, de http://www.fie.undef.edu.ar/?page_id=133

Facultad de Ingeniería del Ejército. (2020). *Facultad de Ingeniería del Ejército - Universidad de la Defensa Nacional*. Obtenido de http://www.fie.undef.edu.ar/?page_id=7510

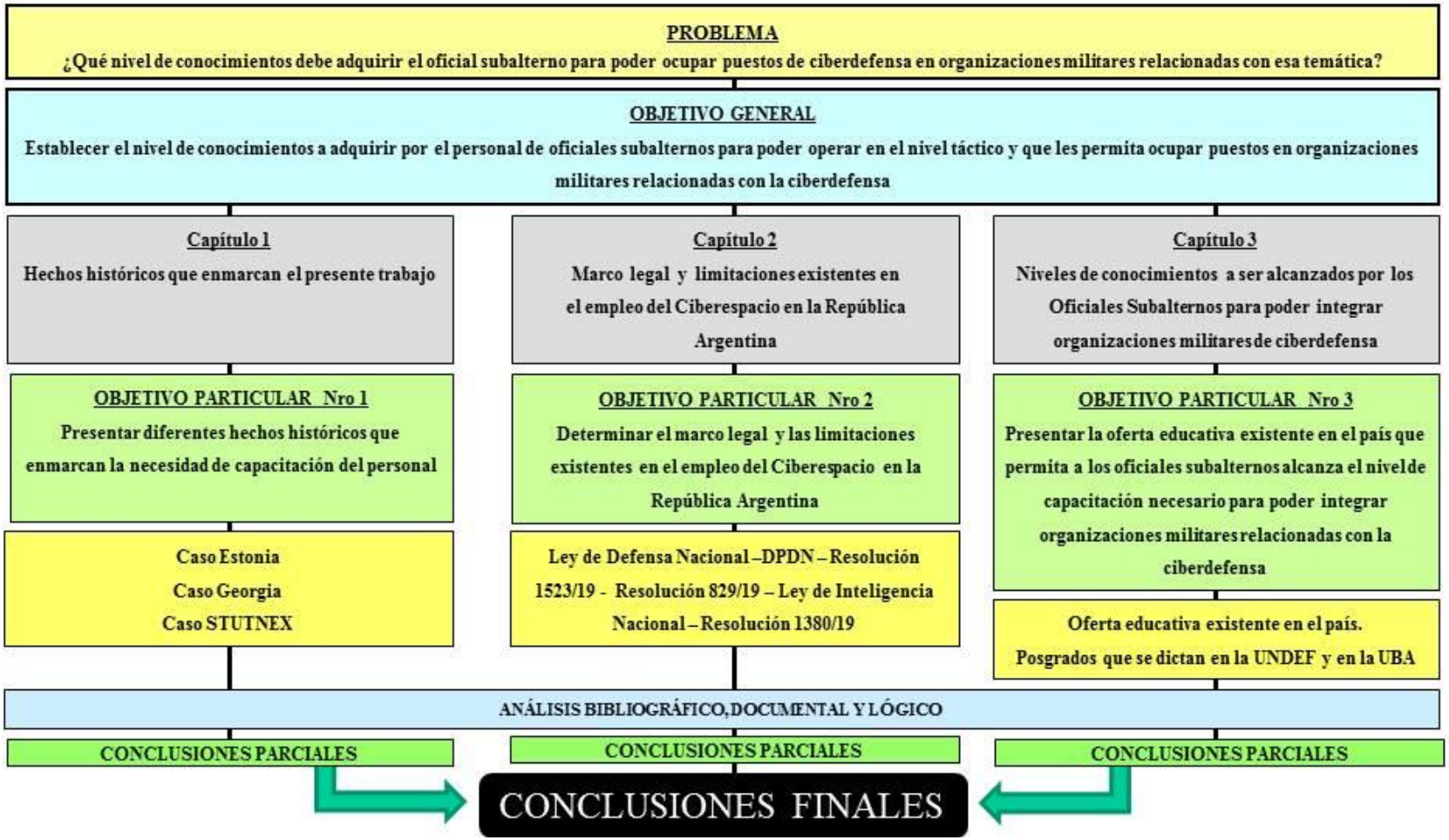
Perfil. (17 de 06 de 2019). *Perfil.com*. Obtenido de https://www.perfil.com/noticias/bloomberg/bc-argentina-no-descarta-ataque-cibernetico-en-apagon.phtml

UNDEF. (2019). *Universidad de la Defensa Nacional* . Recuperado el 15 de Sep de 2019, de https://www.undef.edu.ar/academica/politica-academica/

Universidad de Buenos Aires. (2019). *Universidad de Buenos Aires - Facultar de Ciencias Económicas*. Recuperado el 05 de Oct de 2019, de http://www.economicas.uba.ar/posgrado/posgrados/ciberdefensa-y-ciberseguridad/

Zona Militar. (05 de Noviembre de 2019). *Zona-militar*. Obtenido de https://www.zona-militar.com/2019/11/05/nueva-politica-de-ciberdefensa-ciberespacio-como-quinto-dominio-soberano-de-la-nacion/

Anexo A: Esquema gráfico – metodológico



Anexo B
Plan de estudios de la Especialización en Criptografía y Seguridad en Teleinformática de la Facultad de Ingeniería del Ejército

PLAN DE ESTUDIOS (Plan 2010)

CÓDIGO	ASIGNATURAS	CARGA HORARIA SEMANAL	CARGA HORARIA TOTAL	CORRELATIVIDAD
PRIMER SEMESTRE				
S 105	Criptografía	4 horas	40 horas	No tiene
S 101	Matemática aplicada a la Criptografía	4 horas	40 horas	No tiene
S 103	Teleinformática y Redes de Computadoras	4 horas	40 horas	No tiene
S 104	Gestión, Auditoria y Normas de Seguridad	4 horas	45 horas	No tiene
S 106	Régimen Legal del Manejo de los Datos	4 horas	32 horas	No tiene
SEGUNDO SEMESTRE				
S 206	Criptografía Avanzada	4 horas	48 horas	S 105
S 207	Forensia Informática Aplicada	4 horas	48 horas	S 106
S 202	Seguridad en Redes de Computadoras	4 horas	56 horas	S 103
S 205	Criptográfica Aplicada	6 horas	40 horas	No tiene

Anexo C
Plan de estudios de la Maestría en Ciberdefensa de la Facultad de Ingeniería del Ejército

I AÑO

CODIGO	ASIGNATURAS	REGIMEN	CARGA HORARIA TOTAL	CORRELATIVAS	MODALIDAD DICTADO	OBS

PRIMER SEMESTRE

01 CB	Introducción a la Seguridad Informática	Cuatrimestral I	45 Horas	No tiene	Presencial	
02 CB	Criptografía	Cuatrimestral I	50 Horas	No tiene	Presencial	
03 CB	Gestión, Auditoría y Normas de Seguridad	Cuatrimestral I	50 Horas	No tiene	Presencial	
08 CB	Régimen Legal de Manejo de Datos	Cuatrimestral I	32 Horas	No tiene	Presencial	

SEGUNDO SEMESTRE

05 CB	Forensia Informática Aplicada	Cuatrimestral I	48 Horas	No tiene	Presencial	
S 206	Criptografía Avanzada	Cuatrimestral I	48 Horas	CB 02	Presencial	
07 CB	Criptografía Aplicada	Cuatrimestral I	40 Horas	CB 02	Presencial	
04 CB	Seguridad en Redes	Cuatrimestral I	50 Horas	No tiene	Presencial	

Total de horas cursadas en primer año para la Maestría: 363hs

II ANO

CODIGO	ASIGNATURAS	REGIMEN	CARGA HORARIA TOTAL	CORRELATIVAS	MODALIDAD DICTADO	OBS

PRIMER SEMESTRE

13 CB	Introducción a la Ciberdefensa	Cuatrimestral I	35 Horas	No tiene	Presencial	
14 CB	Metodología de Tesis	Cuatrimestral I	20 Horas	No tiene	Presencial	
15 CB	Infraestructuras Críticas	Cuatrimestral I	40 Horas	No tiene	Presencial	
16 CB	Mecanismos de Ciberdefensa	Cuatrimestral I	30 Horas	No tiene	Presencial	
17 CB	Identificación de Riesgos y Amenazas	Cuatrimestral I	30 Horas	No tiene	Presencial	

SEGUNDO SEMESTRE

18 CB	Defensa de Sistemas Distribuidos	Cuatrimestral I	30 Horas	No tiene	Presencial	
19 CB	Comando y Control de la Ciberdefensa	Cuatrimestral I	40 Horas	No tiene	Presencial	
20 CB	Ciberdefensa Aplicada	Cuatrimestral I	40 Horas	No tiene	Presencial	
	Trabajo Final - Tesis	Cuatrimestral I	120 Horas	No tiene	Presencial	

Total de horas cursadas en segundo año para la Maestría: 385hs

Total de horas de la Maestría: 748hs

Anexo D
Plan de estudios de la Maestría en Ciberdefensa del Instituto Universitario Aeronáutico

ASIGNATURA	TIPO	CARGA HORARIA TOTAL	CORRELATIVIDADES	SEMESTRE
PRIMER AÑO				
Introducción a la Seguridad Informática	Obligatoria	45		1
Criptografía	Obligatoria	50		1
Gestión Auditoría y Normas de Seguridad	Obligatoria	50		1
Seguridad en Redes de datos	Obligatoria	50		1
Forensia Informática Aplicada	Electiva	48		1
Criptografía Avanzada	Electiva	48	Criptografía	2
Criptografía Aplicada	Electiva	40	Criptografía	2
Régimen Legal del Manejo de Datos	Electiva	32		2
Implementaciones de Seguridad en Distintos Sistemas Operativos	Electiva	45		2
Software Aplicativos	Electiva	45		2
Seguridad en Redes Inalámbricas	Electiva	45		2
Seguridad en la Información en las Redes de Defensa	Electiva	35		2
SEGUNDO AÑO				
Introducción a la Ciberdefensa	Obligatoria	35		3
Metodologías de Trabajo Final	Obligatoria	20		3
Infraestructuras críticas	Obligatoria	40		3
Mecanismos de Ciberdefensa	Obligatoria	30		3
Identificación de Riesgos y Amenazas	Obligatoria	30		4
Defensa en Sistemas Distribuidos	Obligatoria	30		4
Comando y control de la Ciberdefensa	Obligatoria	40		4
Ciberdefensa aplicada	Obligatoria	40		4
Trabajo Final	Obligatoria	120		4

Anexo E
Plan de estudios de la Especialización en Seguridad Informática del Instituto Universitario Aeronáutico

CONTENIDOS DEL PROGRAMA DE ESTUDIOS
MÓDULOS TEMÁTICOS
Introducción a la seguridad informática
Criptografía
Seguridad en Redes Inalámbricas
Seguridad en Redes de Datos
Auditoría y Control de la Seguridad Informática
Implementación de Seguridad en Sistemas Operativos
Gestión de la Seguridad Informática
Software Aplicativo
Seguridad de la Información en las Redes de Defensa

Anexo F
Plan de estudios de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires

CURSOS DE FORMACIÓN GENERAL
Tecnología de la información, ética y normativa jurídica
Introducción al gerenciamiento innovador (entrepreneurship)
Introducción a los paradigmas de programación
Tecnología de la información
CURSOS FUNDAMENTALES DE CIBERDEFENSA / CIBERSEGURIDAD
Introducción a la criptología
Evolución de la tecnología militar hasta el enfoque “Network-Centric Warfare”
Tecnología de redes I
Malware I
FUNDAMENTOS Y GERENCIAMEINTO DE LA CIBERDEFENSA Y DE LA CIBERSEGURIDAD
Ciberataques masivos a sistemas de información
Cursos específicos aspectos operativos de Ciberdefensa y Ciberseguridad
Principios y enfoques de diseño de software seguro
Proyecto sobre principios y enfoques de diseño de software seguro
Teoría organizacional y psicología organizacional
Diseño y desarrollo de la “Data Exchange Layer” en ambientes de gobierno
Data Mining – Data warehousing - Big Data
Tecnología de redes II
Seguridad en redes de computadoras
Malware II
Talleres de Investigación Supervisada y/o Tutoriales en Aspectos Operativos de Ciberdefensa y Ciberseguridad