VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN ESTRATEGIA MILITAR MARÍTIMA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN ESTRATEGIA MILITAR MARÍTIMA

TEMA: INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR

AUTOR: TAPIA CHICHANDE, ALEX PAÚL

DIRECTOR: ING. UQUILLAS SOTO, RICARDO PÍO

SANGOLQUÍ

2019

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**INCIDENCIA DE LAS OPERACIONES DE CIBER-DEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR**" fue realizado por el señor ***Tapia Chichande Alex Paúl*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 3 de diciembre del 2019

Firma:

Ing. Uquillas Soto Ricardo Pío

C.C.: 1708857329

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Tapia Chichande Alex Paúl***, con cédula de ciudadanía N° 1709426850, declaro que el contenido, ideas y criterios del trabajo de titulación***: Incidencia de las operaciones de ciberdefensa en las operaciones navales. Propuesta de un organismo para la Armada del Ecuador,*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 3 de diciembre del 2019

Firma

.....

Tapia Chichande Alex Paúl

C.C.: 1709426850

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***Tapia Chichande Alex Paúl*** *autorizó a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:* ***Incidencia de las operaciones de ciberdefensa en las operaciones navales. Propuesta de un organismo para la Armada del Ecuador*** *en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad*

Sangolquí, 3 de diciembre del 2019

Firma

.....

Tapia Chichande Alex Paúl

C.C.: 1709426850

DEDICATORIA

A Irene Alexandra mi esposa, mi compañera y amiga, quien ha sido mi fuente de inspiración porque con su amor y comprensión me ha dado fortaleza para terminar este trabajo.

A mis hijos Doménica y Alex, mis tesoros preciados por su comprensión en los momentos de ausencia.

A mis familiares y amigos por haber depositado su confianza en mí.

AGRADECIMIENTO

A Dios:

Por permitirme cumplir esta aspiración y ser parte fundamental en mi tranquilidad espiritual.

A Docentes y Asesores:

Por su guía y aporte académico mismo que me ha llevado al feliz término de este trabajo

A la Armada del Ecuador:

Por el haberme permitido aumentar el conocimiento en este curso de perfeccionamiento.

A las personas que han colaborado en este trabajo:

A mis amigos y compañeros por su apoyo en este trabajo

ÍNDICE DE CONTENIDOS

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El incremento en el uso de las tecnologías de la información y comunicaciones (TIC´s) en las operaciones navales, ha ocasionado que esta se vuelvan dependientes de las mismas, a tal forma que el correcto uso o no de las mismas pueden incidir en la correcta ejecución de las operaciones; a esta dependencia se suma los peligros existentes en el ciberespacio donde los sistemas y redes están propensos a ataques cibernéticos de diferente fuente, por lo cual se requiere una correcta defensa de los mismos a fin de evitar que los sistemas sean neutralizados por agentes externos. Por esta razón en este trabajo, se presenta la problemática existente por la falta de la capacidad de ciberdefensa en la Armada del Ecuador (ARE) por lo que se propone una organización para la Institución que permita explotar las capacidades de ciberdefensa, mediante operaciones cibernéticas en apoyo a las operaciones navales, además de establecer la situación actual de las operaciones de ciberdefensa, establecer los componentes que permitan mejorar las capacidades de ciberdefensa y plantear la propuesta de organización. Para esto se realizaron encuestas, entrevistas y una revisión documental que nos permite establecer la situación actual de la ciberdefensa en la ARE, posteriormente se establecieron los componentes necesarios para incrementar las capacidades de ciberdefensa como apoyo a las operaciones navales. Con el presente trabajo se pretende establecer una organización base para el Comando de Operaciones Navales (COOPNA), con la cual ejecute operaciones cibernéticas en apoyo de las operaciones.

PALABRAS CLAVES:

- **OPERACIONES NAVALES**
- **OPERACIONES CIBERNÉTICAS**
- **OPERACIONES DE CIBERDEFENSA**

ABSTRACT

The use in the use of information and communication technologies (ICT) in naval operations, has caused that the dependents of the same ones turn around, a form such that the correct use or not of the same ones can affect in the correct execution of operations; this dependence is compounded by the dangerous ones in cyberspace where systems and networks are prone to cyber attacks from different sources, which is why a correct defense of them is required in order to prevent systems from being neutralized by agents external. For this reason, in this paper, the existing problem is presented due to the lack of the capacity of cyber defense in the Ecuadorian Navy (ARE) for which an organization is proposed for the institution that allows to exploit the cyber defense capabilities, through cybernetic operations in support for naval operations, in addition to establishing the current situation of cyber defense operations, establishing the components that improve cyber defense capabilities and proposing the organization's proposal. For this, the surveys, interviews and a documentary review that allows us the current situation of the network in the area are shown, and then the components for the information capabilities are established as support for the naval operations. With the present work we intend to establish a base organization for the Naval Operations Command (COOPNA), with which to execute cybernetic operations in support of operations.

KEYWORDS:

- **NAVAL OPERATIONS**
- **CYBER OPERATIONS**
- **CYBER DEFENSE OPERATIONS**

CAPÍTULO I

EL PROBLEMA

1.1. Planteamiento del Problema.

La Unión Internacional de Telecomunicaciones (ITU), establece que las tecnologías de información y comunicaciones (TIC´s), serán en los próximos 15 años las catalizadoras fundamentales para alcanzar los Objetivos de Desarrollo sostenible, esta afirmación va de la mano con la importancia que han dado los países desarrollados al quinto dominio, el ciberespacio. Los ministros de defensa de los países de la Organización del Tratado del Atlántico Norte (OTAN), han acordado en reunión de febrero del 2018 prestar más atención a la ciberdefensa con la creación de un nuevo centro de operaciones. Expertos internacionales en Ciberdefensa aseguran que diariamente existen más de ocho millones de ataques informáticos a nivel mundial y cada día en aumento.

Dadas las capacidades que podrían tener las operaciones de ciberdefensa y el alto impacto de estas en la conducción militar, es necesario conocer cuál es la incidencia de efectuar o no operaciones de ciberdefensa antes y durante las operaciones militares y cuáles son las posibles repercusiones.

En la celebración del Foro Económico Mundial en enero del 2017, Jens Stoltenberg, secretario general de la OTAN, afirmo “los ciberataques pueden ser tan peligrosos y tan serios como un ataque armado, pueden dañar infraestructura critica, causar daño a las vidas humanas y minar las capacidades de defensa” (Community Latam, 2018). Dado esta importancia que se da en otros organismos de defensa mundial, es necesario reconocer la importancia al ciberespacio y los

problemas que podrían ocasionarse en caso de no tomarse en cuenta, dentro de la planificación de las operaciones militares.

En las Fuerzas Armadas (FFAA), las actividades de asesoramiento y planeamiento, las realiza el Estado Mayor de la fuerza operativa y como parte del proceso se encuentra la recopilación de la información necesaria que permita la toma de decisiones, escoger el mejor curso de acción, asesorar al Comandante y redactar los planes, como también supervisar el cumplimiento de lo planificado.

Ahora bien, el problema se da también cuando en las FFAA, se desconoce o no se investiga sobre la tecnología que usa el oponente o contra quien se debería planificar las operaciones de ciberdefensa. Cuando se logra investigar cuál es la tecnología que dispone su oponente, o contra la cual se deberá planificar las operaciones, deja de ser un tema netamente teórico y se transforma en un asunto de importancia, pues se logra comprender que existen oponentes que usan la tecnología para sacar ventaja en el teatro o área de operación.

En la actualidad la Armada del Ecuador no posee una infraestructura y/o organización donde se pueda realizar operaciones cibernéticas y dado que este nuevo ámbito ha tomado gran importancia a nivel mundial, se plantea las siguientes interrogantes ¿Cuál es la situación actual de las operaciones de ciberdefensa en la Armada del Ecuador? ¿Cuáles son los componentes que mejorarían la ciberdefensa para apoyo de las operaciones navales? ¿Cuál es la organización que necesita la ARE?

1.1.1. Identificación de las causas del problema

La información expuesta anteriormente nos ayuda evidenciar que la falta de conocimiento acerca de las operaciones de ciberdefensa y de un organismo que realicé el seguimiento y

continuidad a estas operaciones ha incidido en que estas no se ejecuten y que no permitan ser un apoyo a las operaciones navales. Con la ayudad de un diagrama causa efecto, se tratará de identificar las causas del problema a fin de definir en base a ellas el estudio que permita encontrar la solución más viable para resolver el problema planteado. En la figura 1, se puede apreciar el diagrama indicado.

En el diagrama de causa y efecto presentado, se puede observar que la falta de un organismo que se encargue de planificar, conducir y supervisar las operaciones de ciberdefensa, ha incidido en que no se ejecuten las operaciones de ciberdefensa y al no existir estas por su parte no han sido un apoyo a las operaciones navales. Se debe recordar que en la Armada existe la Dirección de Tecnologías de Información y Comunicaciones (DIRTIC) quien se encarga de la gestión de las TIC´s y el Comando de Operaciones Navales (COOPNA) que se encarga de conducir las operaciones navales.

Entre estos dos repartos no ha existido un consenso en quien debe ser el responsable de conducir las operaciones de ciberdefensa, por lo tanto, se debe realizar una investigación que permita conocer la situación actual de la ciberdefensa en la Armada del Ecuador, a fin de poder determinar los componentes que deben ser implementados en la ARE, para mejorar los niveles de ciberdefensa y luego proponer un organismo que se encargue de las operaciones de ciberdefensa.

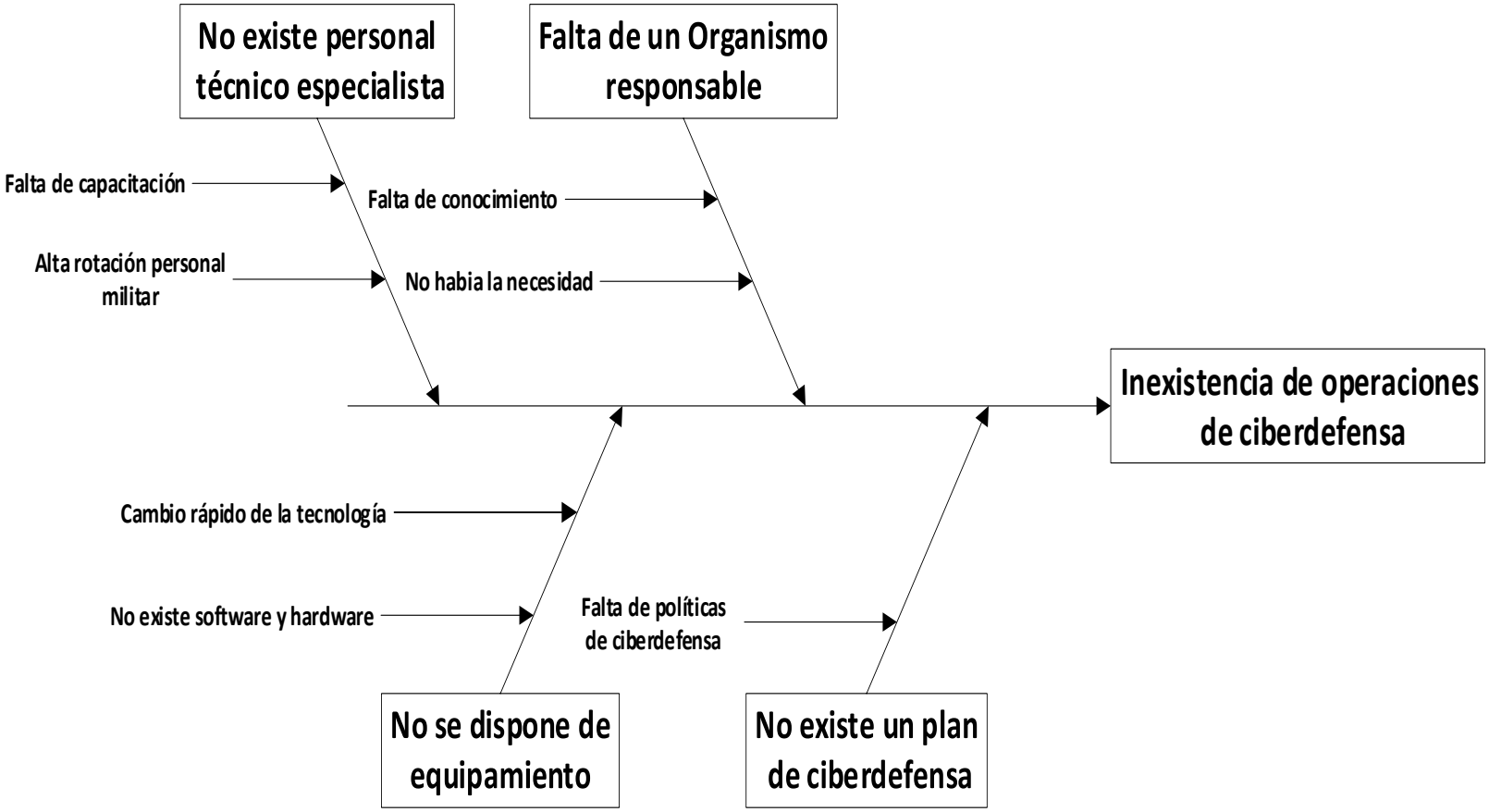

Figura 1. Diagrama Causa - Efecto

1.2. Formulación del Problema.

En virtud que existen varias interrogantes en cuanto al uso y explotación del ciberespacio por parte los organismos encargados del uso de la tecnología y de las operaciones navales en la Armada del Ecuador, es necesario conocer ¿Cuál es la incidencia de las operaciones de ciberdefensa en las operaciones navales? Y determinar ¿Qué tipo de organización requiere la ARE para poder conducir las operaciones de ciberdefensa? En este contexto es necesario conocer cómo se puede enfrentar los desafíos actuales y del futuro en el campo de la ciberdefensa. Es por ello que se requiere de una investigación tipo exploratoria mediante la cual se buscará obtener la mayor cantidad de información que permita conocer cuál es la línea base de la ciberdefensa en la Armada del Ecuador y justificar la necesidad de realizar operaciones de ciberdefensa a fin de proteger el ciberespacio mediante el planteamiento de una organización que permita a la Institución mejorar las capacidades en el ciberespacio y mejorar la protección del mismo, ante los ataques cibernéticos que puedan ocasionar fuerzas antagónicas, oponentes o enemigos ya su vez que permitan la denegación del uso del mismo del enemigo y sobre todo que estas operaciones contribuyan al desarrollo de las operaciones navales.

1.3. Justificación.

El desarrollo de las capacidades de Ciberdefensa permite dar protección a la infraestructura critica digital de Fuerzas Armadas y/o desarrollar una respuesta ante un ataque cibernético.

En la actualidad se ha evidenciado la importancia que han mostrado los Estados y los organismos de defensa a nivel mundial sobre el ciberespacio y la necesidad de su cuidado y su defensa ante ataques cibernéticos. Es por ello que este estudio trata de investigar la situación de

ciberdefensa en la Armada del Ecuador, también presenta como se encuentra la ciberdefensa a nivel mundial y que componentes debería tener la ARE para enfrentar los nuevos desafíos que presenta este dominio en la época actual.

Es por la importancia que se demostrado a nivel mundial, es que esta investigación tarta de proponer una organización de ciberdefensa para la Armada del Ecuador, que permita el desarrollo de doctrina y ejecución de operaciones de ciberdefensa que ayuden a la consecución de los objetivos militares estratégicos e incrementar las capacidades de ciberdefensa de Fuerzas Armadas y ser un apoyo a la conducción de las operaciones navales.

1.4. Objetivos de la Investigación.

1.4.1. Objetivo General.

Determinar la incidencia de las operaciones de ciberdefensa en las operaciones navales, mediante el análisis de la situación actual, a fin de establecer los componentes que permitan mejorar el nivel de ciberdefensa para apoyo de las operaciones navales y proponer un organismo para la Armada del Ecuador.

1.4.2. Objetivos Específicos.

- Determinar el nivel actual de las operaciones de ciberdefensa en la Armada del Ecuador.
- Establecer los componentes que permitan mejorar el nivel de Ciberdefensa para apoyo de las operaciones navales.
- Proponer un organismo de ciberdefensa para la Armada del Ecuador.

1.5. Matriz de consistencia

A fin de verificar la consistencia del planteamiento de esta investigación a continuación se presenta la matriz de consistencia del problema.

Tabla 1
Matriz de consistencia

MATRIZ DE CONSISTENCIA

TÍTULO: Incidencia de las operaciones de ciberdefensa en las operaciones navales. Propuesta de un organismo para la Armada del Ecuador.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
En la actualidad la Armada del Ecuador no posee una infraestructura y/o organización donde se pueda realizar operaciones de Ciberdefensa y dado que este nuevo ámbito ha toma-do gran importancia a nivel mundial, se plantea las siguientes interrogantes ¿Cuál es la situa-ción actual de las operaciones de Ciberdefensa en la Armada del Ecuador? ¿Cuáles son los componentes que mejorarían la ciberdefensa para apoyo de las operaciones navales? ¿Cuál es la organización que necesita la ARE?	**GENERAL** Determinar la incidencia de las operaciones de ciberdefensa en las operaciones navales, mediante el análisis de la situación actual, a fin de establecer los componentes que permitan mejorar el nivel de ciber-defensa y proponer un organismo para la Armada del Ecuador. **ESPECÍFICOS** 1. Determinar el nivel actual de las operaciones de Ciberde-fensa en la Armada del Ecua-dor. 2. Establecer los componentes que permitan mejorar el nivel de Ciberdefensa para apoyo de las operaciones navales. 3. Determinar la incidencia de las operaciones de ciberdefensa en las operaciones navales. 4. Proponer un organismo de Ci-berdefensa para la Armada del Ecuador.	¿La incidencia de las opera-ciones de Ciberdefensa en las operaciones navales, hace necesaria una organiza-ción de Ciberdefensa en la Armada del Ecuador?	**Variable Dependiente:** operaciones navales **Definición. –** Es el conjunto de acciones que se desarrollan me-diante el empleo de fuerzas de superficie, submarinas, infante-ría de marina o aeronavales en un teatro marítimo, en el que se espera encontrar fuerzas adver-sarias que se opongan al cum-plimiento de la misión**.** Es la ca-pacidad que tienen las unidades navales para poder navegar, combatir y detectar a las amena-zas. **Variable Independiente:** operaciones de ciberdefensa **Definición.** - Las operaciones en el ciberespacio son aquellas en las cuales se emplea las ciber capacidades para lograr los ob-jetivos militares o efectos a tra-vés del ciberespacio.	**ENFOQUE** Cualitativo **TIPO DE INVESTIGA-CIÓN** Exploratoria y correlacional. **DISEÑO DE INVESTIGA-CIÓN** No experimental **POBLACIÓN** Armada del Ecuador **MUESTRA** Personal técnico (DIRTIC) y Operativo (COOPNA) **TÉCNICAS** Observación y revisión docu-mental. **INSTRUMENTOS** Encuestas, entrevistas.

CAPÍTULO II

MARCO DE REFERENCIA

2.1. Antecedentes

El incremento de los ataques informáticos durante los últimos años ha ocasionado que los países desarrollados continúen reclutando hackers y especialistas en materia de seguridad informática para la defensa de su ciberespacio.

Los incidentes informáticos cada día son más frecuentes, esto ha originado que los países industrializados se encuentren en un proceso de mejoramiento de sus leyes y doctrinas que les permita definir o delimitar el campo de la ciberseguridad y la ciberdefensa.

Las Fuerzas Armadas modernas y los países desarrollados en sus últimos conflictos han desarrollado capacidades de operaciones en el ciberespacio, las cuales han sido utilizadas en contra de las fuerzas enemigas junto con las operaciones militares normales y por otro lado se han desarrollado operaciones cibernéticas encubiertas entre países que han sido utilizados para actos de espionaje, robo de información calificada o el uso de ciber armas que han mermado ciertas capacidades de los blancos de interés.

Los ataques a la infraestructura crítica del Estado pueden ser desde un ingreso no autorizado, ingreso de datos erróneos a los sistemas de información del adversario, inutilización de sistemas de vigilancia y detección satelital, denegación de servicios a los servicios informáticos

especialmente los relacionados con los sistemas de mando y control, manipulación de sistema de control de armamento o inutilización de sistemas de

La forma de vida de los ciudadanos del mundo ha cambiado vertiginosamente, todo depende del Internet tales como las comunicaciones, el comercio, la banca, entre otros, esto hace que se tomen diferentes medidas de protección para asegurar las redes, los computadores, los sistemas y equipos que están interconectados. Esta interconexión se da por medios alámbrico o inalámbricos y los cuales son susceptibles a cualquier ataque. En la siguiente figura se observa las interconexiones submarinas a nivel mundial, las cuales representan aproximadamente el 90% del tráfico mundial de datos, lo que hace un objetivo rentable para cualquier organización por la importancia que tienen las comunicaciones y la información que viaja por estos medios.

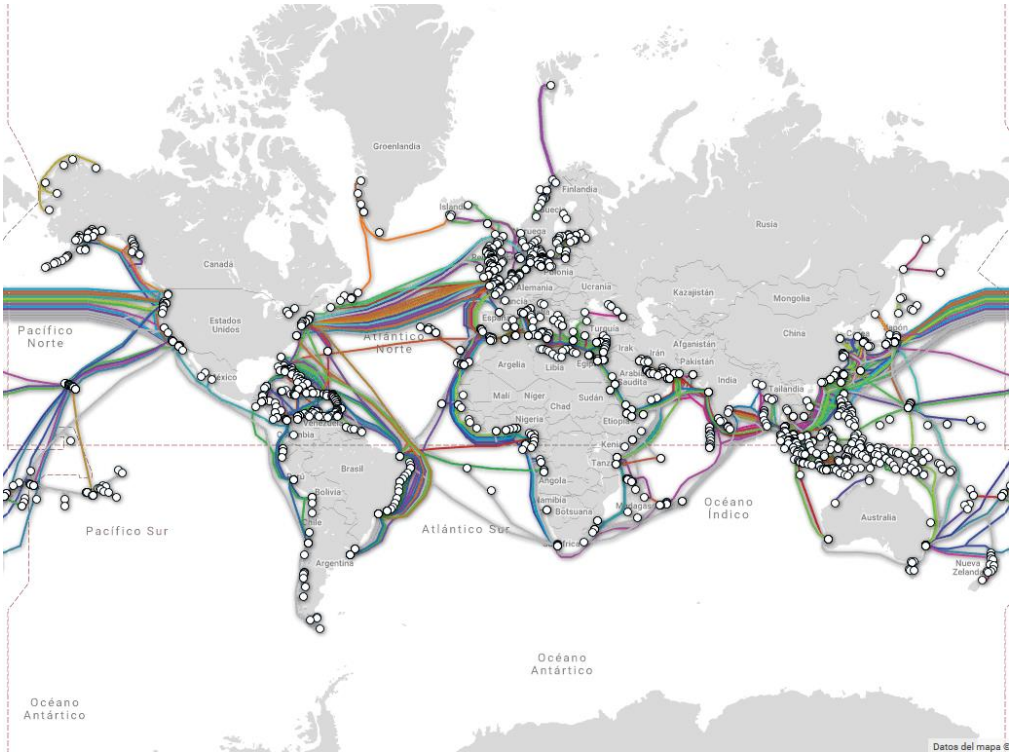

Figura 2. Mapa mundial de conexiones submarinas
Fuente: (TeleGeography, 2018)

Los organismos internacionales han establecido su preocupación sobre los riesgos que existen en la red, por lo cual han promulgado acciones combinadas entre los estados, a fin de minimizar los impactos en la red. Tenemos ejemplos de cooperación como es el caso de los países miembros de la OTAN y la Comunidad Europea quienes firmaron una declaración para mejorar la cooperación en tema de ciberseguridad y ciberdefensa. (Union Europea, 2018).

En la cumbre de la OTAN efectuada en Varsovia en julio del 2016, se desarrollaron algunos acuerdos entre otros (Instituto Espanol de Estudios Estrategicos, 2016):

- Al ciberespacio se lo reconoció como un nuevo dominio de las operaciones, junto a los dominios de la tierra, mar y aire.
- Mejoramiento de políticas y capacidades nacionales de ciberdefensa de los países integrantes, a fin de mantener las capacidades de acuerdo a la vertiginosa evolución de las tecnologías.
- Profundización de la cooperación entre los países de la Unión Europea en lo concerniente a ciberdefensa.

Así también tenemos otros organismos regionales y mundiales que han mostrado su interés en mejorar la cooperación en temas relacionados con el ciberespacio como es la ONU, en la cual el secretario General, Antonio Guterres sostuvo estar convencido que la próxima guerra comenzara con un ciberataque masivo para destruir la capacidad militar y tendrá afectaciones a la infraestructura básica de las naciones, por lo cual pidió reglas globales para minimizar el impacto de los ciberataques masivos. (Agencia Telam, 2018).

Según el Reporte anual del Foro Económico Mundial del año 2018, existe un crecimiento acelerado de dispositivos conectados a internet, los cuales se espera en el año 2020 alcancen la cantidad de 20.4 billones de dispositivos. Así también los ataques de denegación de servicios distribuidos, DDOS se han tornado comunes, dado que estos se han vuelto más persistentes en relación con años anteriores. Los costos financieros por perdidas debido a los diferentes ataques a las empresas, se estima que sea de aproximadamente de USD 8 trillones de dólares, en los próximos cinco años. Siendo industrias de diferente índole las que han sufrido ataques en os últimos cinco años, tales como la aviación, plantas de energía nuclear, telecomunicaciones, el gobierno, la banca, infraestructura critica, entre otras. Según este estudio la las probabilidades de sufrir un ataque cibernético son cada día más reales y con una afectación bastante grande, como se puede ver en la Figura No. 3 (Worls Economic Forum, 2018).

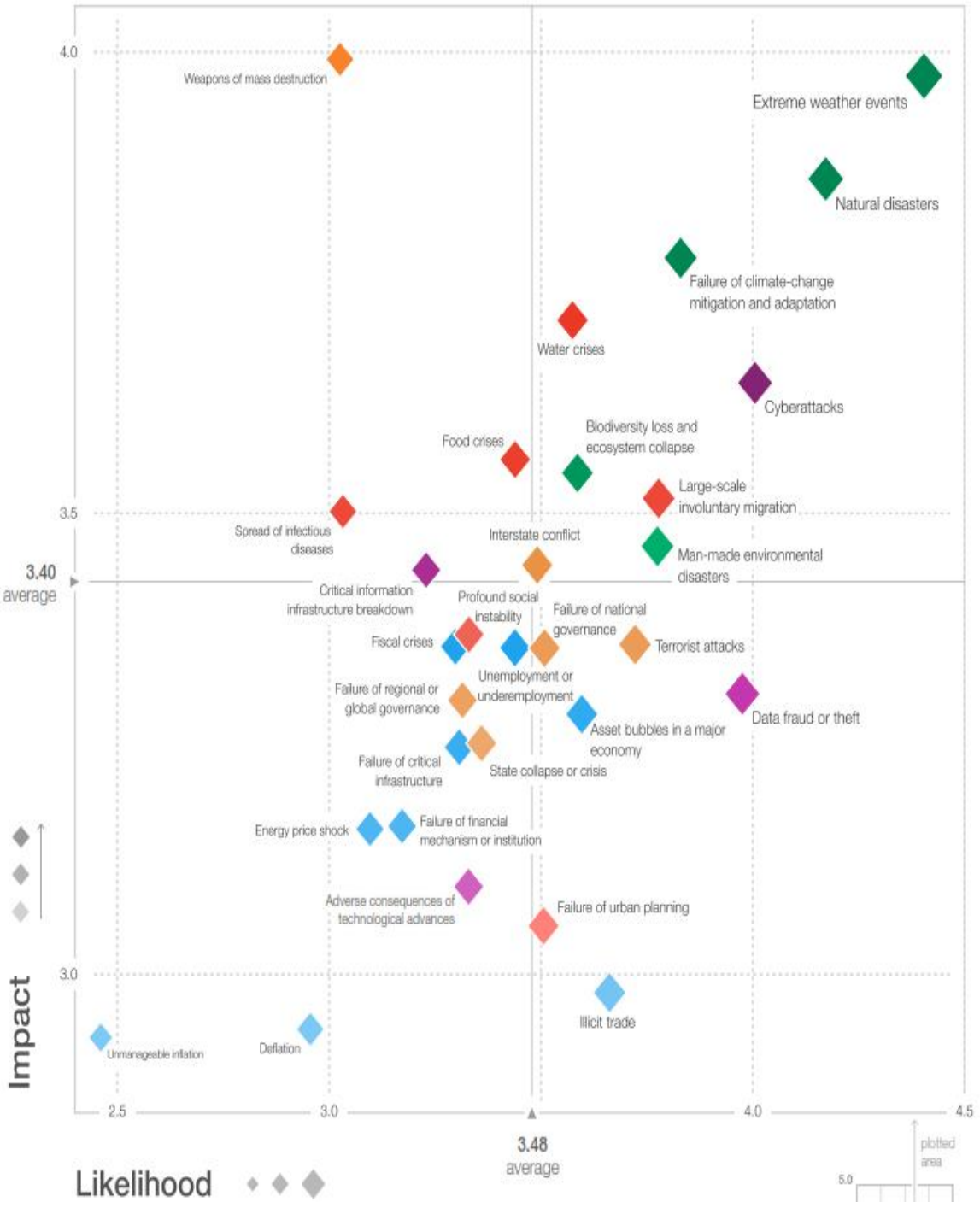

Figura 3. Panorama Mundial de Riesgo Global 2018
Fuente: (Worls Economic Forum, 2018)

2.2. Estado del Arte

2.2.1. Estado del arte a nivel mundial

La ciberdefensa es un elemento que ha tomado gran preponderancia a nivel mundial, es así que se lo ha denominado como el quinto dominio. Esta importancia permanece vigente en la actualidad, así lo demuestra los acuerdos mostrados en la cumbre de la OTAN en el año 2016, la misma que lo define como el quinto dominio.

Por otro parte, Estados Unidos como país de referencia mundial en al ámbito de la defensa también ha evolucionado en sus políticas de ciberdefensa, así como su forma de operar en el ciberespacio. (Departement of Defense, 2018). A esto se han sumado varios países y organizaciones a nivel mundial que han dado prioridad de la defensa del ciberespacio.

Por otro lado, se ha incrementado las técnicas de los ciberataques, estos cada día son más sofisticados al punto de considerarse unas ciberarmas, a nivel mundial ya existen países que utilizan estas ciberarmas para obtener los objetivos deseados. Existen un sinnúmero de ataques realizados a organizaciones privadas o públicas que han ocasionado grandes pérdidas económicas a nivel mundial.

2.2.2. Estado del arte a nivel regional

Un ejemplo de la importancia que ha tomado el quinto dominio a nivel regional, son los acuerdos de cooperación alcanzados entre Chile y Brasil en los ámbitos de capacitación, investigación y ayudas en caso de recibir ataques informáticos. (Grupo EDEFA, 2018). Por otro lado, Chile

y EEUU también firmaron acuerdo de cooperación a través de intercambios, ejercicios y capacitación en el ámbito de la ciberdefensa. (Grupo EDEFA, 2018).

También se puede indicar que, en materia de políticas de ciberdefensa, los países de la región han avanzado con respecto a este tema, lo que permite a las Fuerzas Armadas desarrollar la capacidad de ciberdefensa con el apoyo político. Entre los principales países que han desarrollado las estrategias de ciberseguridad y/o ciberdefensa, tenemos a Brasil, Colombia, Chile, Perú, entre otros.

2.2.3. Estado del arte a nivel local

En el Ecuador el tema de ciberdefensa se lo viene tratando desde el año 2014, cuando mediante acuerdo Ministerial se creó el sistema de ciberdefensa y posteriormente las Fuerzas Armadas trataron de ejecutar el proyecto "Implementación de a capacidad de ciberdefensa", sin embargo, este por falta de apoyo presupuestario no ha sido ejecutado hasta la actualidad.

En el Comando Conjunto de las Fuerzas Armadas se creó el Comando de Ciberdefensa, el cual tiene como misión:

> Defender, explotar el dominio cibernético y responder ante incidentes o amenazas que atenten la infraestructura crítica estratégica digital de FFAA: y del Estado; a través de la conducción de operaciones de ciberdefensa, a fin de contribuir a la misión del comando conjunto. (Miisterio de Defensa Nacional, 2014).

A pesar de existir un acuerdo sobre la creación del Sistema de Ciberdefensa, hasta la actualidad no se ha desarrollado las estrategias nacionales de ciberseguridad y ciberdefensa en el

Ecuador, por lo cual es una limitante a la hora de plantear una solución militar en el ámbito de ciberdefensa.

2.3. Fundamentos teóricos.

Las operaciones de ciberdefensa ejecutadas en algunos conflictos bélicos a nivel mundial, ha puesto en evidencia la capacidad que tienen ciertas naciones para operar en el ciberespacio, sin embargo, en la actualidad no es posible establecer los alcances reales que puedan tener estas operaciones. En resumen, se podría anticipar que los ataques cibernéticos cumplirían con los siguientes objetivos:

- Quebrantar la infraestructura logística del enemigo y la cadena de suministro.
- Distraer, confundir e inhabilitar el sistema C5IVR.
- Negar las capacidades similares del enemigo.
- Desarrollar oportunidades de atacar la infraestructura crítica del enemigo.

Estas capacidades que tienen los ataques cibernéticos pueden ser utilizados en favor de las operaciones militares propias, del enemigo o de las amenazas.

En la actualidad se puede observar que las operaciones militares dependen de la tecnología y en especial las operaciones navales, ya que el uso de los sistemas de mando y control hace que exista una posible vulnerabilidad ante los adversarios que posean la capacidad de realizar ataques cibernéticos.

Las capacidades del ciberespacio brindan oportunidades a las fuerzas militares y sus aliados para obtener y mantener las ventajas del uso continuo del ciberespacio, proporcionando seguridad económica y física a la nación. (Joint Chiefs of Staff, 2018)

Para las Armadas del mundo la ciberdefensa es una preocupación que ha ido en aumento, tratando que los sistemas e infraestructura asociados a los sistemas de mando y control estén mejor protegidos y tengan los controles necesarios, con el fin de prevenir, detectar y eliminar los ataques que impidan el cumplimiento de las operaciones.

En el ciberespacio el tiempo entre la ejecución y el efecto es cuestión de milisegundos, así también se puede establecer que las operaciones en el ciberespacio pueden crear efectos simultáneos en los niveles estratégicos, operativo y táctico en los múltiples dominios, por lo que su planificación a todo nivel es imperativa.

La capacidad de Ciberdefensa nivel Fuerzas Armadas en el Ecuador, se lo ha implementado limitadamente en el Comando Conjunto de las Fuerzas Armadas mediante el Comando de Ciberdefensa. En la Armada del Ecuador no se explota estas capacidades ya que no existe una organización que se encargue de la planificación y ejecución de las operaciones de ciberdefensa.

En este sentido se busca sincronización de las capacidades cibernéticas de los diferentes actores en el contexto de las Fuerzas Armadas, fin sumar esfuerzos en la protección del ciberespacio, para el desarrollo de las operaciones militares, en el caso de la Armada del Ecuador para la conducción de las operaciones navales.

2.4. Marco Conceptual.

2.4.1. Generalidades de la Ciberdefensa

Existen una gran cantidad de términos muy semejantes que deben ser establecidos, a fin de conocer los campos de acción en cada una de las áreas en las que actúa la ciberdefensa y tener la base teórica para el presente trabajo.

Al ciberespacio se lo conceptualiza como “el dominio global dentro del entorno de la información, compuesto por una red interdependiente de infraestructuras de tecnologías de la información, incluido el Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores” (Departament of Defense, 2012). Su gran importancia para los países tecnológicamente avanzados ha hecho que lo determinen como el quinto dominio siendo los otros: el aéreo, terrestre, marítimo y espacial. Este quinto dominio posee tres capas como se lo puede observar en la siguiente figura: la capa física con sus componentes geográficos y redes físicas; la capa lógica con su componente de redes lógicas y finalmente la capa social con sus componentes las personas y las ciber personas (Ejercito de los Estados Unidos, 2010).

Existen otras definiciones acerca del ciberespacio, como es el caso del Brasil el cual lo establece:

> Es una de las cinco áreas operacionales que penetra sobre las demás las cuales son: la tierra, el mar, el aire y espacio, que son interdependientes. Las actividades en el ciberespacio pueden crear libertad de acción para las actividades en otras áreas, así como actividades en otros dominios y también crea efectos dentro y a través del ciberespacio. (Operaciones militares ciberneticas, 2017).

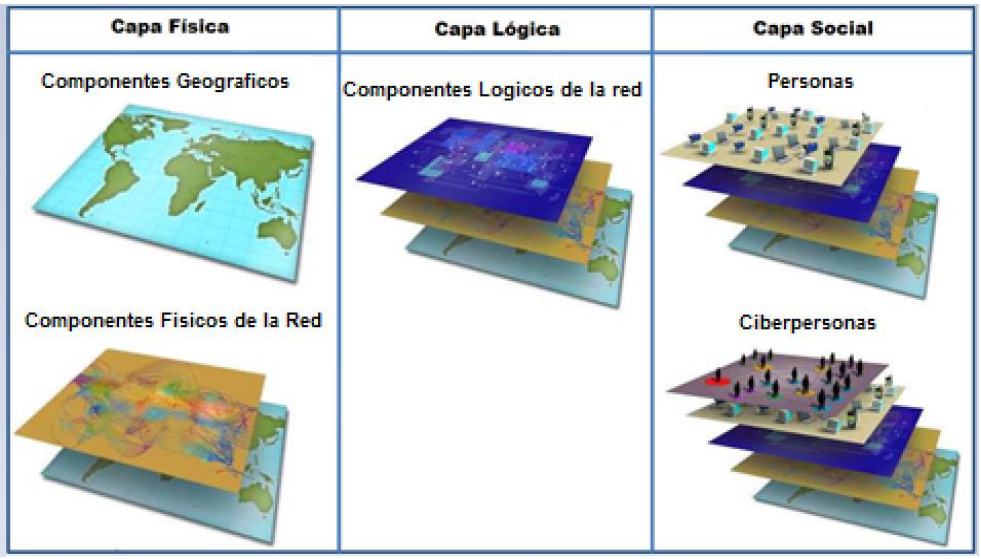

Figura 4. Capas en el ciberespacio
Fuente: (Ejercito de los Estados Unidos, 2010)

El ciberespacio es un dominio global, disponible para casi cualquier persona con acceso a una computadora con conexión a Internet, un teléfono inteligente o cualquier otro tipo de dispositivo multimedia de enlace. En este dominio existen muchos actores diferentes en paralelo, con varias necesidades, objetivos e intenciones. Algunos actúan solos, otros en redes poco conectadas o estructuras más formales. Los roles también pueden variar según la situación y pueden superponerse. Los actores pueden moverse entre categorías a lo largo del tiempo y dependiendo de sus objetivos y metas actuales. Además de todas las cosas positivas que ha generado el ciberespacio, ha sido simultáneamente un medio utilizado en conflicto desde hace más de dos décadas. En el ciberespacio las bandas de hackers rivales se enfrentan activamente entre sí, los grupos de protesta expresan sus opiniones a través del vandalismo virtual, las organizaciones criminales difunden el malware en busca de ganancias fáciles, entre otros. (Vankka, 2013).

Durante la primera década del siglo XXI, el propio ciberespacio se convirtió progresivamente en una fuente de conflicto importante. Las áreas de disputa estaban estrechamente ligadas a la

naturaleza del ciberespacio y al uso, mal uso y control de la información dentro de su dominio. Los conflictos implicaron desacuerdos sobre temas como el derecho de propiedad intelectual y el intercambio de archivos, los límites de la libertad de expresión, el equilibrio entre la privacidad y la seguridad en línea, y la gobernanza de Internet y la neutralidad de la red. (Deibert, Palfrey, Rahozinski, & Zittrain, 2011).

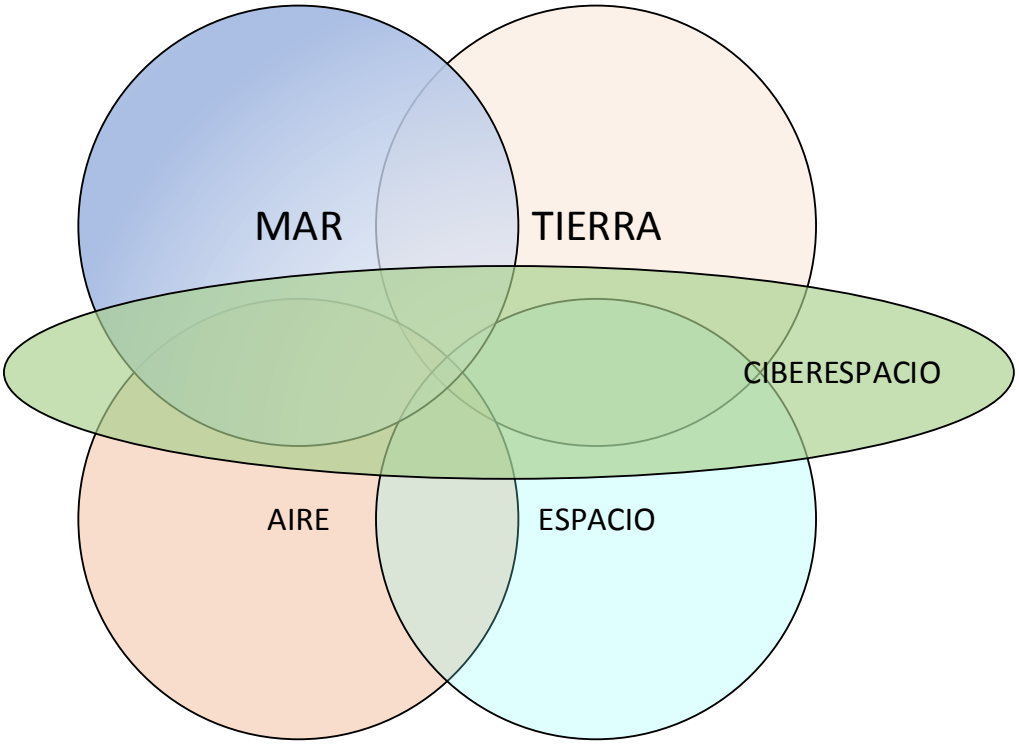

Figura 5. El ciberespacio como quinto dominio

El ciberespacio puede facilitar y acelerar todo tipo de enfrentamientos derivados del mundo físico, protestas callejeras coordinadas a través de los medios sociales hasta guerras a gran escala en las que se aprovecha el ciberespacio para difundir información al guerrero y al público en general en el fomento de la causa. Como objetivo del conflicto, tanto la infraestructura del ciberespacio

como los recursos de sus usuarios están expuestos a las consecuencias de estos conflictos. (Lewis, 2009).

Algunos de los actores no estatales más comunes en los ciberconflictos están definidos en la tabla No 2, agrupados por categorías, la motivación que tienen para realizar los ataques, los objetivos que persiguen, los métodos empleados comúnmente y los vectores de ataque explotados.

El Centro Superior de Estudios de la Defensa Nacional, CEDESEN, define a la Ciberdefensa como "la aplicación de las medidas de seguridad para proteger el ciberespacio de un ciberataque, para lo cual posee tres capacidades: defensa, explotación y respuesta" (Defensa, 2012).

Tabla 2

Principales actores no estatales en los ciberconflictos

Actores	Motivación	Objetivo	Método
Ciudadanos	Ninguna	Cualquiera	Indirecto
Script kiddies	Curiosidad, ego	Individuos, compañías y gobierno	Herramientas y scripts escritos previamente
Hacktivistas	Político, cambio social	Tomadores de decisión, víctimas inocentes	Protestas vía alteración de sitios web o ataques DDoS
Black-hat hackers	Ego, ganancia económica	Cualquiera	Malware, virus, explotación de vulnerabilidades
White-hat hackers	Idealismo, creatividad, respeto a las leyes	Cualquiera	Test de penetración, parches
Grey-hat hackers	Ambiguo	Cualquiera	Varios
Patriot hackers	Patriotismo	Adversarios de la nación	Ataques DDoS, alteración de sitos webs

CONTINUA

Ciberinformantes	Ganancia Financiera, agravio	Empleados	Ingeniería social, backdoors, manipulación
Ciberterroristas	Político y cambio social	Víctimas inocentes	Computadora basada en violencia y destrucción
Creadores de Malware	Ego, ganancia económica	Ninguno	Explotación de vulnerabilidades
Cyber scammers	Ganancia Financiera, agravio	Individuos, compañías pequeñas	Ingeniería social
Cibercriminales	Ganancia Financiera	Individuos y compañías	Malware para fraude, phishing, ataque DDoS o correo engañoso
Corporaciones	Ganancia Financiera	Infraestructuras y sistemas basados en TIC (privados o públicos).	Rango de técnicas de ataque o influencia de las operaciones
Agentes ciberespionaje	Ganancia financiera y política	Individuos, compañías y gobierno	Rango de técnicas de obtención de información
Cibersoldados	Patriotismo, desarrollo profesional	Adversarios de la nación	Basado en las capacidades del grupo

Fuente: (Vankka, 2013)

Otro de los conceptos que es muy importante definir es el concepto de ciberguerra o guerra cibernética, en este sentido Richard Clarke, experto en seguridad del gobierno de los Estados Unidos, la define como “el conjunto de acciones llevadas por el estado para perpetrar en los ordenadores o en las redes de otro país, con la finalidad de causar un prejuicio o alteración”. (Campus Internacional para la Seguridad y la Defensa, 2016).

Las operaciones en el ciberespacio son aquellas en las cuales se emplea las ciber capacidades para lograr los objetivos militares o efectos a través del ciberespacio. Se debe comprender que la

guerra moderna establece que todos los dominios: tierra mar, aire, espacio están interconectados por las operaciones del ciberespacio. (Air force, 2011). Es de comprender que las operaciones en el ciberespacio se planean igual que las operaciones en los demás dominios.

Existen tres tipos de operaciones definidas dentro de las operaciones cibernéticas, tales son las operaciones de exploración, operaciones de defensa y operaciones de respuesta. (Mando Conjunto de Ciberdefensa, 2018).

Las operaciones de exploración son aquellas que se realizan para recolección, búsqueda de información de redes propias o del enemigo, entre las principales actividades que se cumplen son:

- Inteligencia de ciberamenazas
- Alerta temprana ante posibles ataques
- Apoyo al planeamiento de las operaciones
- Obtención de información de sistemas adversarios por medio de fuentes abiertas (OSINT).

Las operaciones de defensa son aquellas que tienen que ver con la seguridad de los sistemas de información, redes de datos y comunicaciones propias y su capacidad para evitar ser atacados y detección de una posible infiltración en estos sistemas. Estas operaciones son preventivas, proactivas y reactivas.

Entre las actividades de defensa preventivas tenemos:

- Seguridad física
- Control de accesos
- Actualizaciones de hardware, software, sistemas operativos, entre otros.

- Escoriación de sistemas
- Análisis de vulnerabilidades
- Concienciación.

Entre las actividades de defensa proactivas tenemos:

- Inspecciones y auditorias
- Monitorización
- Test de penetración.

Entre las actividades de defensa reactivas tenemos:

- Gestión de incidentes
- Restauración de incidentes
- Análisis forense
- Acciones legales

Las operaciones de respuesta son aquellas acciones que se ejecutan con la finalidad de atacar los sistemas del adversario e impedir el control del ciberespacio.

2.4.2. Ataques cibernéticos

El crecimiento que ha tenido el uso del internet y de los sistemas de información, ha hecho que exista un incremento de las amenazas existentes en el ciberespacio, es allí que es necesario conocer sobre los diferentes tipos de ataques que pueden realizarse y como pueden utilizar los países para su uso y/o su protección del ciberespacio. Ver Figura No.5 Clasificación de las amenazas informáticas.

Según la OTAN los ataques cibernéticos son las acciones realizadas para interrumpir, denegar, degradar o destruir la información que reside en una computadora y/o red de computadoras (Cooperative Cyber Defence Centre of Excellence, 2018). Estos ataques pueden ocasionados por diferentes usuarios y con diferentes fines.

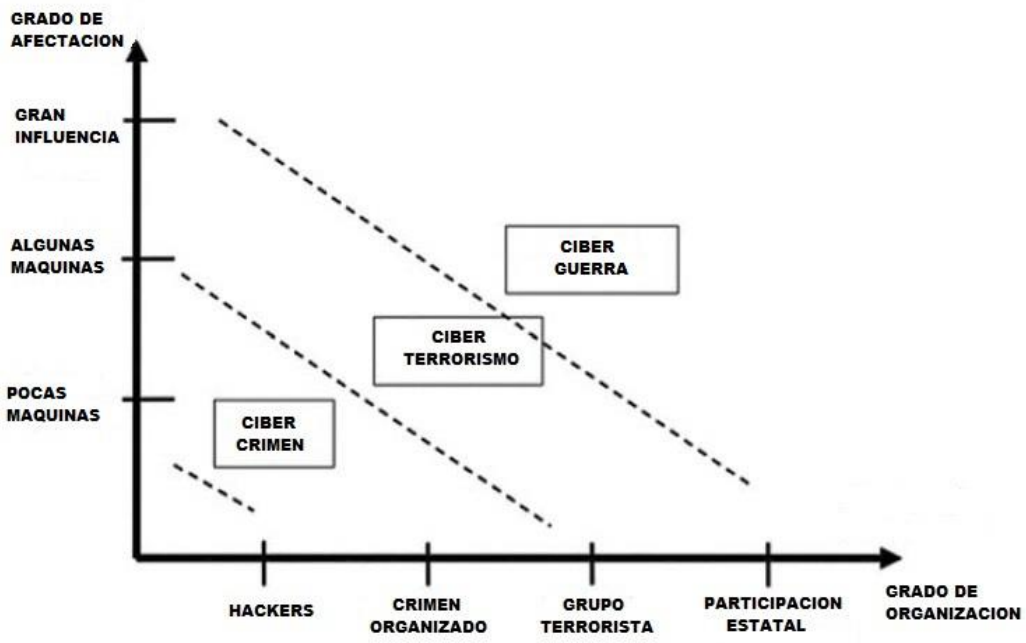

Figura 6. Clasificación de las amenazas cibernéticas
Fuente: *(Diaz del Rio Duran, 2011)*

Como se pudo observar en la figura anterior, cuando existe una participación estatal en los ataques cibernéticos, estos pueden tener una gran afectación, especialmente en la infraestructura critica del Estado. En el caso de la las operaciones navales que realiza la ARE, se puede decir que estas pueden ser afectadas en sus sistemas de mando y control, comunicaciones, computación, ciberdefensa, inteligencia, vigilancia y reconocimiento (C5ISR).

Todos los ataques en el ciberespacio son monitoreados a nivel mundial por diferentes organizaciones dedicadas a la seguridad informática, en la cual se puede observar el incremento

acelerado de los ataques cibernéticos a nivel mundial. (Ver Figura 7 Mapa de ataques cibernéticos en tiempo real)

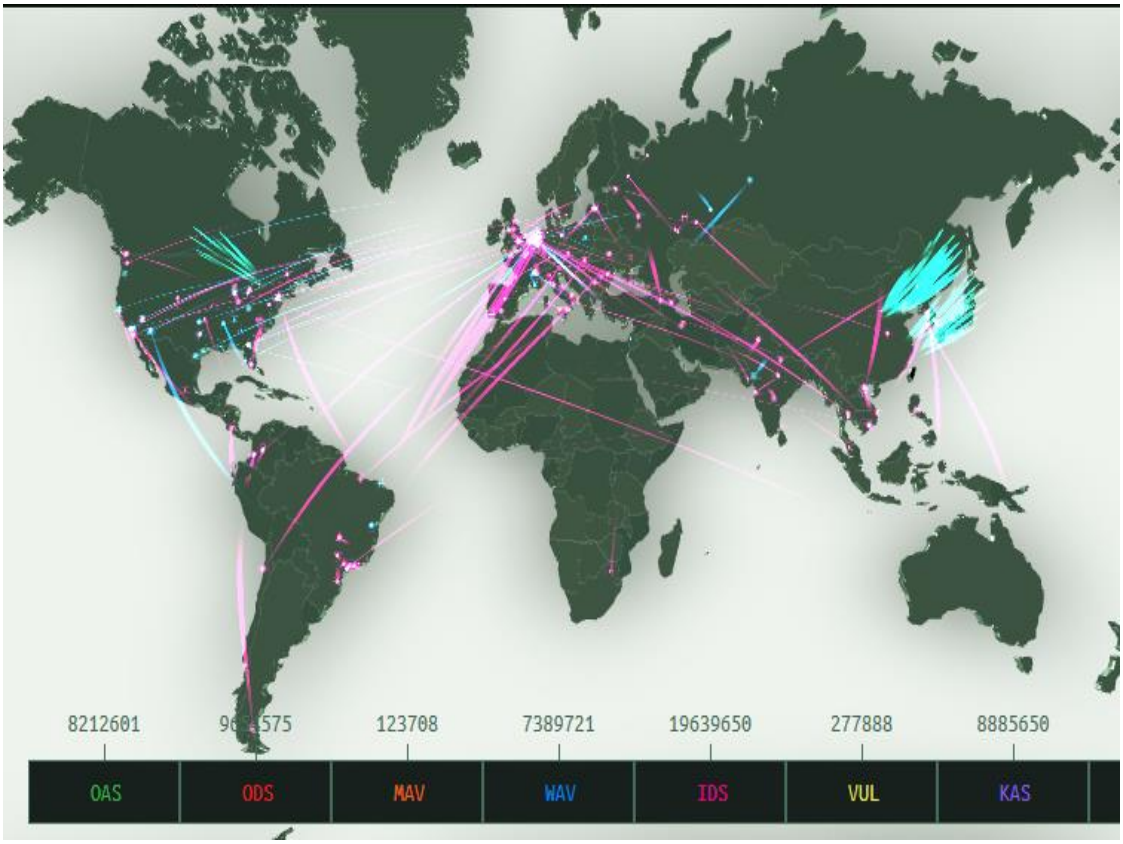

Figura 7. Mapa de ciberataques a nivel mundial en tiempo real
Fuente: (Kapersky, 2018)

Los ataques tienen un ciclo de vida, caracterizado por varias fases que se ejecutan en diferentes tiempos e instancias. Las etapas son las siguientes:

- Preparación del ataque
- Obtención del acceso
- Creación de la persistencia
- Ejecución de acciones
- Eliminación de rastros.

Como se puede observar en la siguiente figura, todas estas fases tienen ciertas actividades que deben cumplirse para la ejecución de un ataque, por lo tanto, no es factible conocer o tener un estimado de tiempo de los ciberataques, ya que esto dependerá del grado de conocimiento del atacante, de tipo de ciberarma que utilice y del grado de protección que tenga la organización objetivo.

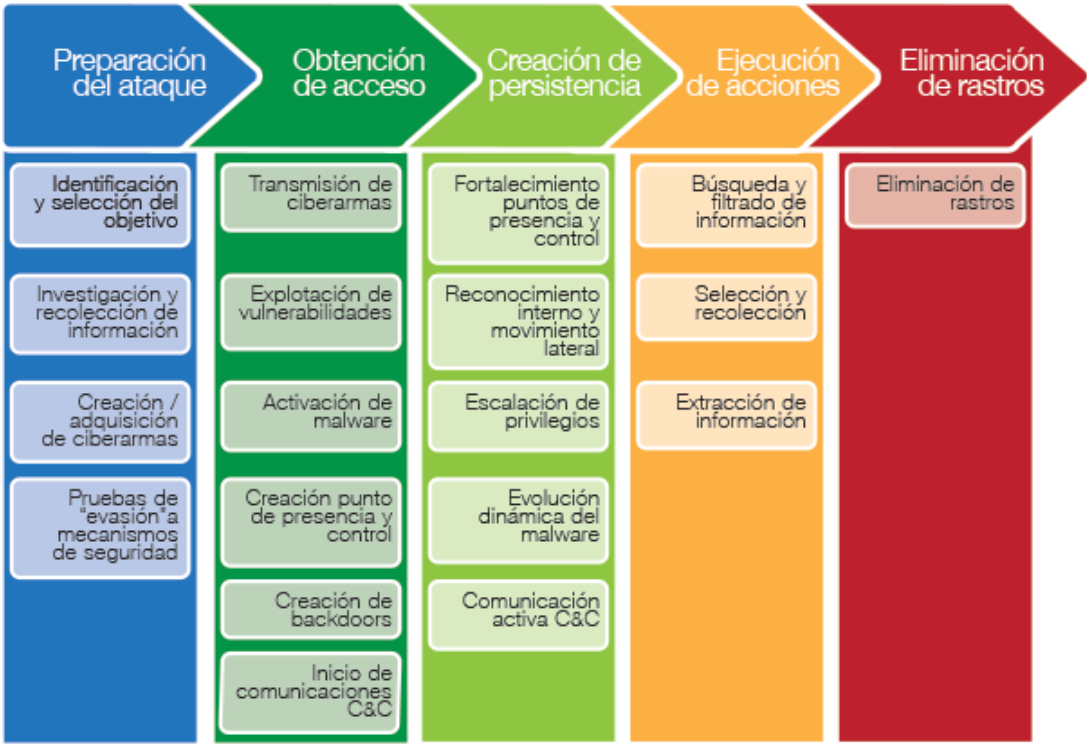

Figura 8. Ciclo de vida de un ciberataque
Fuente: (Polanco Marcos, 2015)

La evolución de las tecnologías ha ido de la mano del incremento de las amenazas, que han buscado explotar vulnerabilidades o aprovechar las limitadas capacidades de los sistemas, es por ello que a continuación presentamos las principales amenazas a las que se podría ver afectado los sistemas C5ISR.

Los principales ataques conocidos son los efectuados por malware[1], los cuales tienen algunas variantes y han evolucionado con el pasar del tiempo, entre los principales tenemos:

- Virus son programas maliciosos que infectan a otros archivos del sistema con la finalidad de modificarlo o dañarlo
- Troyanos es un programa que se hace pasar como software legítimo y cuando se ejecuta permite el robo de datos y acceso al sistema por una puerta trasera. (Kapersky, 2018)
- Gusanos son programas que realizan copias de sí mismo y multiplicándose a través de la red, ocasionando gran consumo de memoria del sistema o ancho de banda de la red. (Avast, 2018)
- Spyware son programas que recopilan información de una computadora y después son trasmitidos a una entidad externa sin el conocimiento o el consentimiento del propietario de los equipos. (Centro de Innovacion y soluciones empresariales y tecnologicas, 2018)
- Ransomware es un software malicioso que infecta los computadores y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. (Kapersky, 2018)

[1] Es la abreviatura de Maliciuos software, este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. (Rivero Marcelo, 2016).

También se debe mencionar las técnicas utilizadas para obtener información o para perpetrar un ataque entre las principales tenemos:

- Ingeniería social es el conjunto de acciones o engaños que realizan los ciberatacantes para obtener información a través de la manipulación de los usuarios. (GSM, 2018)
- Phishing conocido como suplantación de identidad, es un método que usan los ciberdelincuentes para obtener información confidencial, mediante el envió de correo electrónico de fuentes aparentemente confiables. (Seguridad de la Información, 2011)
- Denegación de servicios (DDoS) es un tipo de ataque a los servicios web de una organización, que consiste en la saturación de los servidores hasta el punto del colapso mediante la sobrecarga de mensajes, para este cometido utilizan los recursos de computadoras que se encuentran infectadas (bootnets). (TechTarget, 2012). De este último tipo de ataques tenemos una gran variedad de métodos, como son el ICMP Flood Attack[2], SYN flood[3], HTTP GET flood[4], entre otros.

Para el caso de las aplicaciones web existen técnicas que pueden explotar las vulnerabilidades, a continuación, citamos las más comunes (Ruben, 2018):

---

[2] Ataque que ocurre con la sobrecarga de paquetes ICMP, que hacen que el sistema falle.

[3] Ataque cuando una persona logra hacerse pasar por otra, falsificando datos e inunda con paquetes SYN la tabla de conexión de los servidores, hasta hacerlos caer.

[4] Ataque orientado a conexiones, que inundan la red en los puertos de servicios HTTP, mientras de hacen pasar por usuarios legítimos

- Inyección SQL esta técnica permite ejecutar un código SQL, debido a la presencia de una vulnerabilidad en la base de datos de la aplicación.
- Defacement es la desfiguración del sitio web cuya intención es arruinar la reputación de la organización
- Cross-Site request es un exploit malicioso mediante el cual se envían comando no autorizados de un usuario que el sitio web confía.

A pesar del esfuerzo que hacen los organismos e instituciones públicas y privadas por contrarrestar las diferentes técnicas de ataques, con el pasar del tiempo se ha podido observar el crecimiento de herramientas que facilita el trabajo a los atacantes, los cuales pueden realizar ataques sofisticados y sin mucho conocimiento de las técnicas empleadas. Esta forma de operar de por parte de diferentes actores hace que la seguridad de los sistemas de mando y control, los sistemas informáticos de las infraestructuras criticas sean vulnerables a cualquier persona que con el uso de estas herramientas desee realizar alguna acción negativa. En la siguiente figura se puede observar cómo han ido evolucionando las técnicas de ataques.

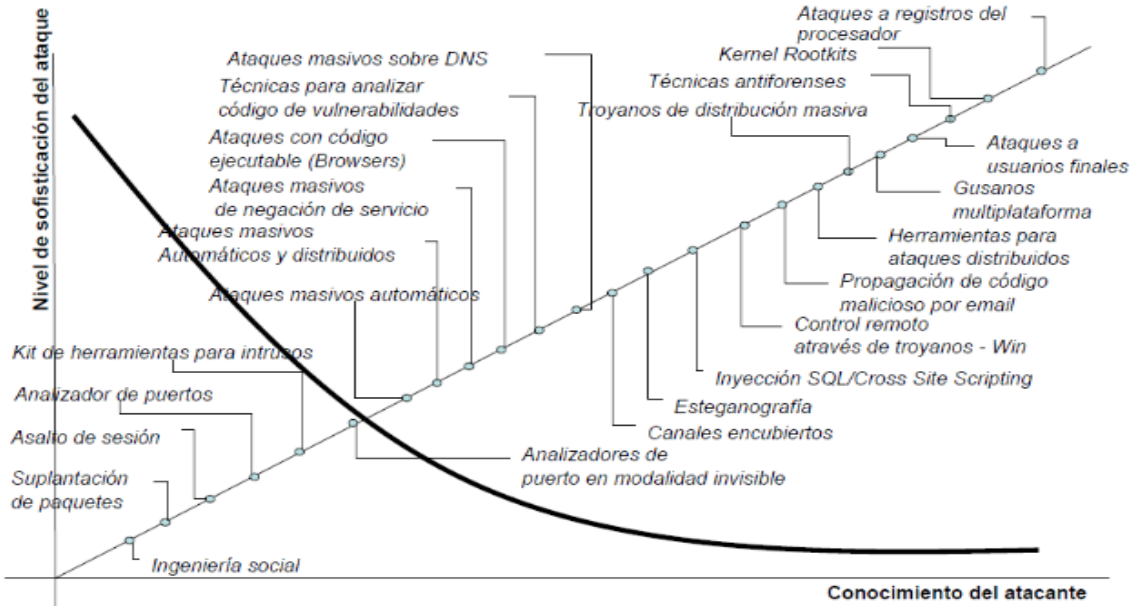

Figura 9. Evolución de los Ataques cibernéticos.
Fuente: (Medina & Martinez, 2011)

Según el informe presentado por la empresa Kaspersky se estima para el futuro que las amenazas informáticas se incrementen y especialmente en los casos citados a continuación: (Kapersky, 2017):

- Que exista un incremento en los ataques dirigidos, ATP contra los sistemas industriales e infraestructura critica.
- Uso de redes sociales para la elaboración de ataques
- Malware dirigido a las plataformas móviles.
- Ataques a los equipos del intenet de las cosas (IOT).
- Incremento del uso o proliferación del rasomware.
- Uso de técnicas de machine learning

A continuación, se muestra los principales casos de guerra cibernética ocurridos a nivel mundial en la cuatro últimas décadas, los cuales han causado grandes perjuicios a los países afectados y en las cuales se han utilizado varias de las técnicas descritas anteriormente y que con el pasar del tiempo han ido evolucionando.

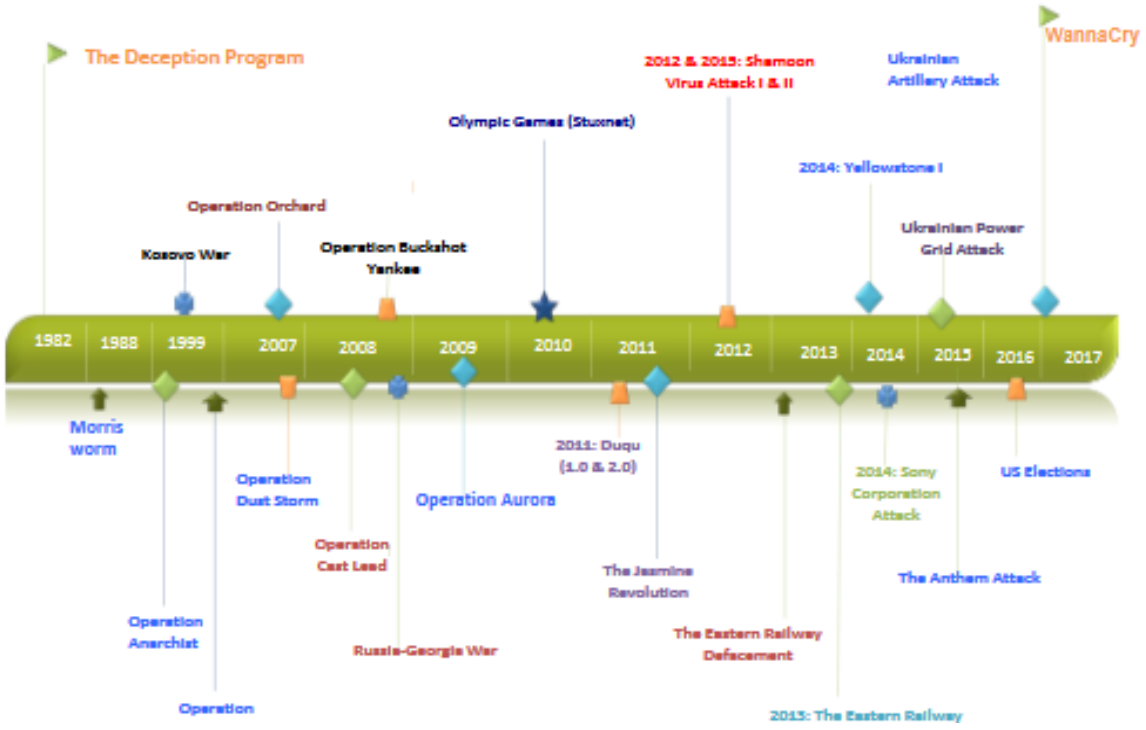

Figura 10. Principales casos de Ciberguerra a nivel mundial en las cuatro últimas décadas
Fuente: (Gazula, 2017)

2.4.3. Organizaciones de ciberdefensa

Las operaciones de ciberdefensa son desarrolladas por unidades o centros especializados que han sido creado por los diferentes países a fin de mantener la seguridad del ciberespacio. Estos centros Es por ello que en la tabla No. 3 se presenta los países que cuentan con estos centros.

Tabla 3

Organizaciones de Ciberdefensa a nivel internacional

No	PAIS	SIGLA	NOMBRE
1	EE. UU	USCYBERCOM	UNITED STATES CYBER COMMAND
		FCC-C10F	US FLEET CYBER COMMAND
		ARCYBER	ARMY CYBER COMMAND
		AFCYBER	AIR FORCES CYBER/24TH AIR FORCE
2	COLOMBIA	CCOC	COMANDO CONJUNTO CIBERNÉTICO
		UCEJC	UNIDAD CIBERNÉTICA EJÉRCITO
		UCARC	UNIDAD CIBERNÉTICA ARMADA
		UCFAC	UNIDAD CIBERNÉTICA FUERZA AÉREA
3	ARGENTINA	EMCFFAA	COMANDO CONJUNTO CIBERDEFENSA
4	VENEZUELA	DICOCIBER	DIRECCIÓN CONJUNTA DE CIBERDEFENSA
5	ECUADOR	COCIBER	COMANDO DE CIBERDEFENSA
6	PERÚ	CODEC	COMANDO OPERACIONAL DEL CIBERESPACIO
7	URUGUAY	CERT-Militar	CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA MILITAR. (En Proceso de Activación)
8	BRAZIL	CDCIBER	CENTRO DE DEFENSA CIBERNETICA (EJÉRCITO)
9	MÉXICO	CCCC	CENTRO DE CONTROL DE CIBERDEFENSA Y CIBERSEGURIDAD (ARMADA - En Proceso de Activación)
10	CHILE	CIC	COMITÉ INTER MINISTERIAL DE CIBERSEGURIDAD
11	CANADA	CCIRC	CENTRO DE RESPUESTAS A INCIDENTES CIBERNETICOS
12	BOLIVIA	N/A	NO CUENTA CON CIBERCOMANDOS
13	PARAGUAY	N/A	NO CUENTA CON CIBERCOMANDOS

FUENTE: (Realpe, 2017)

Como se puede observar en algunos de los países mencionados, la necesidad de mejor la seguridad en el ciberespacio, ha ocasionado que desarrollen organizaciones de ciberdefensa en respuesta a la necesidad, en alguno de los casos en función de sus necesidades poseen varias organizaciones para cumplir con el propósito.

Otros países han ido mucho más lejos con la creación de ejércitos dedicados a la defensa y protección del ciberespacio, dada la importancia que le han dado a la soberanía del ciberespacio.

A fin de constatar las estructuras que tienen cada uno de las organizaciones de ciberdefensa, se pondrá como ejemplo la estructura organizativa de los Estados Unidos como un referente mundial, también de Colombia como un referente regional de ciberdefensa y la estructura del Comando de Ciberdefensa de las Fuerzas Armadas de Ecuador.

En la siguiente figura se puede establecer la relación de mando que tiene el componente naval de ciberdefensa (FLTCYBERCOM/C10F), con el Comando de Ciberdefensa de los Estados Unidos (USCYBERCOM), con el Comando de operaciones navales (CNO) y con la Agencia de Seguridad Nacional (NSA).

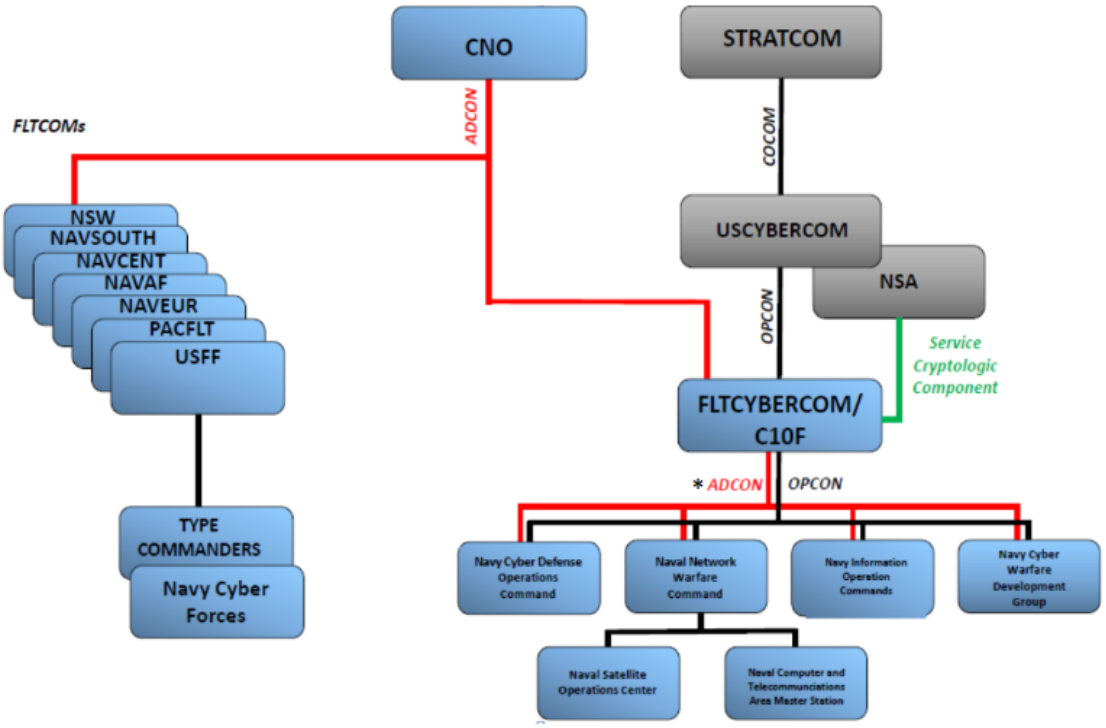

Figura 11. Estructura del Componente Naval de Ciberdefensa de los EEUU
Fuente: (Commander Navy Cyber Forces, 2014)

Así también se puede observar cuatro comandos subordinados al componente naval: el Comando de operaciones de Defensa (Navy Cyber Defense Command), el Comando de operaciones de Información (Navy Information Operation Command), el Comando de guerra en la red (Naval Network Warfare Command), y el grupo de desarrollo de guerra cibernética (Navy Cyber Warfare Development group).

- Comando de Operaciones de Ciberdefensa: Es aquel que coordina, monitorea y supervisar la defensa de las redes y sistemas informáticos de la Armada. (Marina de los Estados Unidos, 2018).
- Comando de operaciones de Información: Es el centro de operaciones de Información, el cual proporciona capacitación centrada en operaciones y soporte de planificación,

desarrollo de doctrina y procedimientos, para apoyo a la guerra futura basada en el efecto y gestión de los datos para las operaciones de Información. (Marina de los Estados Unidos, 2018).

- Comando de operaciones de Guerra de Red: Es aquel que tiene el mando y control de las redes de la Armada y realiza la coordinación para ataques conjuntos. (Marina de los Estados Unidos, 2018).
- Grupo de Desarrollo de Guerra Cibernética: Es el centro de innovación de la guerra cibernética y encargado de la investigación y desarrollo de capacidades avanzadas de guerra cibernética, criptología y electrónica de la Marina. (Marina de los Estados Unidos, 2018).

En la figura siguiente, se puede observar que para el funcionamiento del Componente naval existen 5 componentes operacionales: operaciones de Defensa en la red (Network Operation & Defense), operaciones de Información (Information Operation), Investigación y Desarrollo (R&D), operaciones del servicio de criptología (Service Cryptologic Component Operations) y operaciones de Inteligencia de señales (Fleet and Theater SIGINT Operations). (Commander Navy Cyber Forces, 2014)

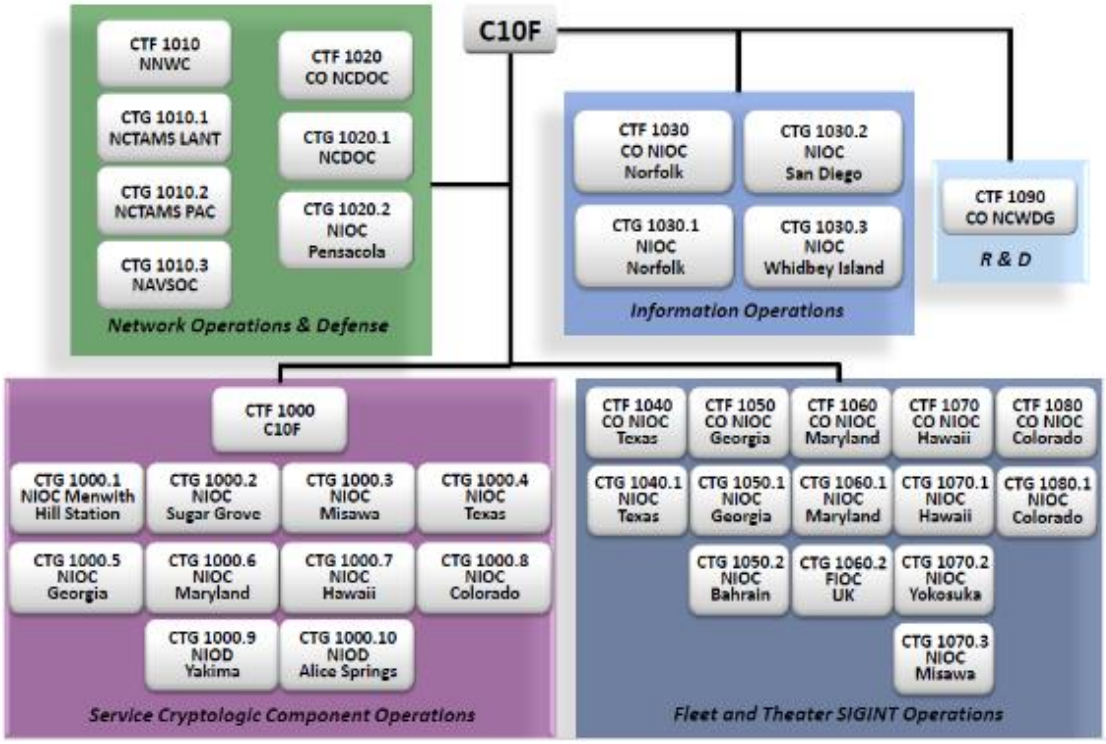

Figura 12. Componentes Operacionales del componente de ciberdefensa de la Armada
Fuente: (Commander Navy Cyber Forces, 2014)

Por su parte Colombia también tiene una organización muy parecida a la de los Estados Unidos, donde existe un Comando de Ciberdefensa Conjunto y los componentes en las diferentes fuerzas, como se puede observar en la siguiente gráfica.

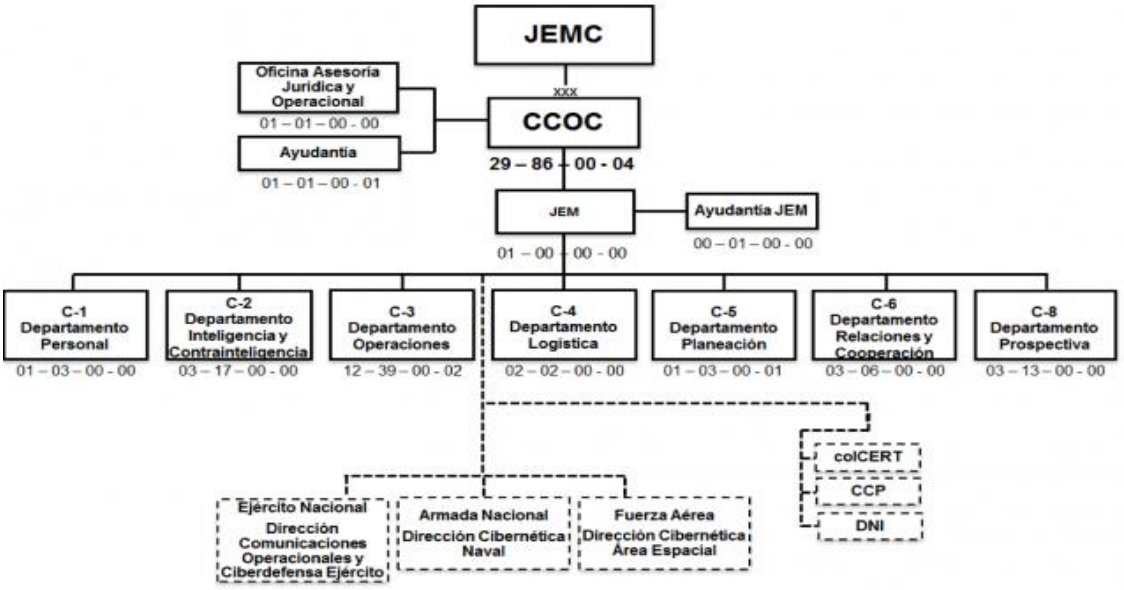

Figura 13. Organigrama del Comando de ciberdefensa de Colombia**.**
Fuente: (Comando Conjunto Cibernetico, 2018)

Para el caso de Ecuador, la estructura organizacional del Comando de Ciberdefensa que se muestra en la siguiente figura, donde se establece tres áreas principales: exploración, defensa y respuesta.

Figura 14. Estructura del Comando de Ciberdefensa de las Fuerzas Armadas
Fuente: (Comando Conjunto de las Fuerzas Armadas, 2017)

Todos estos centros de ciberdefensa han pasado por un proceso de madurez, donde existen etapas que deben ser cumplidas para poder llegar a la respectiva implementación, como se puede observar en la figura No. 15, existen etapas y/o áreas de trabajo que deben ir cumpliéndose para la correcta operación del centro de ciberdefensa, esto empieza con lo más básico como es el monitoreo de la red hasta obtener sistemas automatizados como el machine learning[5] que permiten tener un sistema autónomo de control.

Existen algunas funciones que deben implementarse y que son la base previa para tener un centro de ciberdefensa como son: un Centro de operaciones de red (Network Operations Centre,

[5] Es el campo de la inteligencia artificial que usa métodos estadísticos para dar a los sistemas informáticos la habilitad de autoaprendizaje.

NOC), centro de operaciones de seguridad (Security Operations Centre, SOC), Equipo de respuesta a incidentes cibernéticos (Cyber incident response team, CIRT) y el centro de ciberdefensa (Cyber defensa center, CDC).

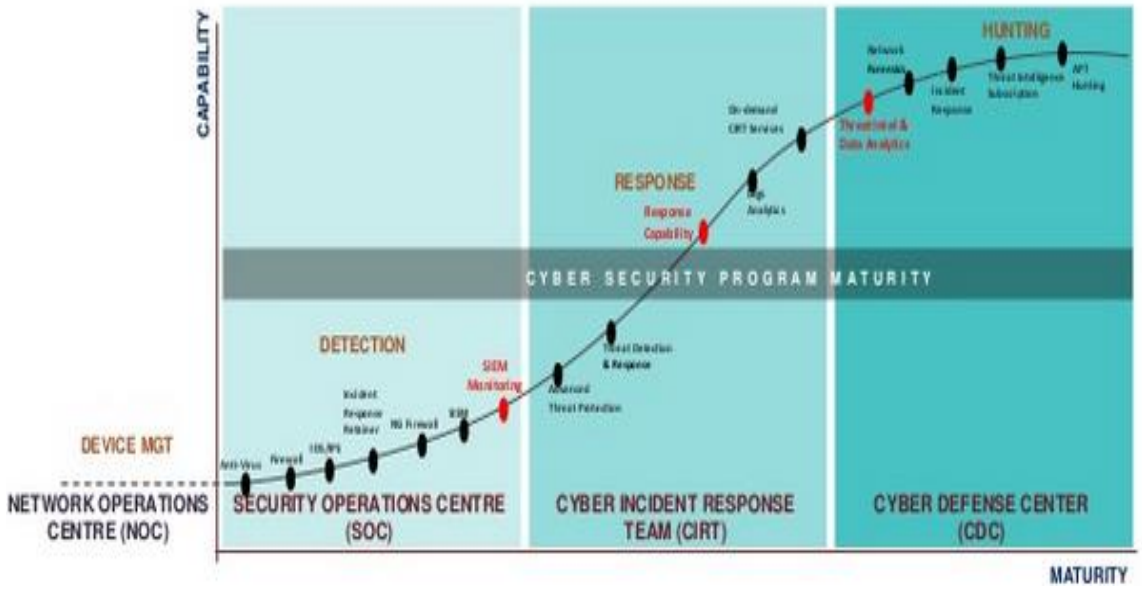

Figura 15. Nivel de madurez de un centro de ciberdefensa
Fuente: (Fireeye, 2018)

Network Operations Centre (NOC), llamada también como centro de control de la red, es una unidad central desde donde se controla y monitorea una o más redes. La función general es mantener las operaciones de red en óptimas condiciones, supervisando las telecomunicaciones em busca de alarmas o ciertas anomalías que puedan requerir atención para evitar la degradación de la red. (Techopedia, 2018)

Security Operations Center (SOC), es una unidad que posee un equipo de seguridad de la información responsable de supervisar y analizar la seguridad de una organización de forma continua. El objetivo del equipo SOC es detectar, analizar y responder a incidentes de ciberseguridad utilizando una combinación de soluciones tecnológicas y un conjunto sólido de procesos. Los

centros de operaciones de seguridad suelen tener personal de seguridad altamente capacitados encargados de la supervisión. El personal de SOC trabaja de cerca con los equipos de respuesta a incidentes organizacionales para garantizar que los problemas de seguridad se solucionen rápidamente después de su descubrimiento.

Los centros de operaciones de seguridad monitorean y analizan la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad. El SOC es responsable de garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente. (DigitalGuardian, 2018)

Cyber Incident Response Team (CIRT), conocido como "equipo de respuesta a incidentes informáticos", este grupo es responsable de responder a las brechas de seguridad, virus y otros incidentes potencialmente catastróficos en empresas que enfrentan riesgos de seguridad significativos. Además de los especialistas técnicos capaces de lidiar con amenazas específicas, debe incluir expertos que puedan guiar a los ejecutivos de las empresas en la comunicación adecuada después de tales incidentes. El CIRT normalmente opera en conjunto con otros grupos empresariales, como los equipos de seguridad del sitio, relaciones públicas y recuperación de desastres. (Gartner, 2018).

2.4.4. Generalidades de las operaciones navales

Las operaciones militares consisten en la aplicación de los principios políticos, de planificación, organización y administración en el uso de los recursos y de la fuerza militar, en la formación diaria y actividades de las unidades para conseguir metas u objetivos específicos.

Así también podemos definir a las operaciones navales como:

> […] el conjunto de acciones que se desarrollan mediante el empleo de fuerzas de superficie, submarinas, infantería de marina o aeronavales en un teatro marítimo, en el que se espera encontrar fuerzas adversarias que se opongan al cumplimiento de la misión […]. (Armada del Ecuador, 2014).

Entre los principales tipos de operaciones navales tenemos:

1. Operaciones de Defensa:
    a. Conquista: Son aquellas operaciones realizadas por la fuerza organizada del más fuerte, con el fin de buscar la situación que le permite la más pronta obtención del Control del Mar, mediante la batalla decisiva y el bloqueo naval.
    b. Disputa: Son aquellas operaciones realizadas por la fuerza organizada del más débil o por fuerzas equilibradas en un mar no controlado. El más débil busca el desgaste que le permita ir al encuentro decisivo. En caso de fuerzas equivalentes, no podría eludirse la decisión ya aceptarse la batalla, con operaciones de Contrataques menores, contraataques mayores y Flota en potencia.
    c. Ejercicio: Son aquellas actividades que permiten a la Fuerza Naval el mayor uso del mar y que este uso sea negado al adversario. Para esto se pueden realizar las siguientes operaciones.
        i. Defensa de Líneas de Comunicación Marítimas propias, mediante cobertura, protección indirecta y protección directa.
        ii. Ataque a las Líneas de Comunicación Marítimas del adversario.
        iii. Protección y apoyo a las fuerzas propias de invasión

iv. Defensa contra fuerzas enemigas de invasión

2. Operaciones permanentes:

   a. Operaciones de Mantenimiento de la Paz: Se desarrollan a requerimiento de la Organización de Naciones Unidas, en acuerdo con la Carta suscrita por los países miembros y al interés nacional. Estas operaciones son requeridas por la ONU a aquellos países miembros que aceptan participar y se acuerdan a través de un convenio entre las partes.

   b. Operaciones de Imposición de la Paz: Son aquellas operaciones militares llevadas a cabo con el consentimiento de la mayoría de las partes en disputa. Sirven para intermediar, controlar y facilitar los acuerdos alcanzados, tales como cese del fuego, tregua, etc. y apoyar los esfuerzos diplomáticos tendientes a asegurar la paz en el país o zona de conflicto.

   c. Operaciones de Ayuda Humanitaria: Están destinadas a aliviar el sufrimiento humano ante los efectos producidos por grandes desastres naturales como terremotos, tempestades, tsunamis, inundaciones, erupciones volcánicas, aislamientos, hambruna, etc.; de accidentes o desastres causados por el hombre como la contaminación, éxodos masivos de personas, campos de refugiados, etc.

   d. Operaciones de Interdicción Marítima (MIO): Acción de negar el acceso a puertos específicos a naves mercantes para la importación/exportación de mercancías a un país determinado o a varios países.

   e. Operaciones de Control de Tráfico Ilícito (OCTI): operaciones que realiza eventualmente la Fuerza de Superficie, en apoyo a la autoridad marítima y

permanentemente el Comando de Guardacostas para el control de las actividades marítimas y contribuir a combatir el contrabando en sus diversas formas, tráfico de armas, tráfico de estupefacientes, pesca ilegal, tráfico de ilegales y otras actividades ilícitas en el mar.

f. Operaciones Combinadas: operaciones y Ejercicios que se realizan con fuerzas navales de otros países que contribuyen a potenciar las capacidades combinadas para desarrollar operaciones de respuesta colectiva ante eventuales accidentes o incidentes.

g. Operaciones de Búsqueda y Rescate: Abarca todas las actividades referentes a la búsqueda de personas o naves en peligro, prestarles asistencia y trasladarlas a un lugar seguro.

h. Operaciones para Mitigar Desastres: Estas operaciones están relacionadas con las de Ayuda Humanitaria, ya que normalmente surgen de las consecuencias de los mismos fenómenos; su propósito es la de restablecer a corto plazo, los servicios básicos necesarios para sostener la vida de las personas en las áreas afectadas.

i. Operaciones de Apoyo al Desarrollo: Es un conjunto de actividades que el poder militar realiza para ayudar con los distintos frentes a cumplir los objetivos nacionales.

j. Operaciones Especiales: Son aquellas en las cuales la naturaleza de la operación, las características del área de operaciones, la característica y forma de actuar del enemigo, las condiciones particulares de la conducción, o la combinación de estos factores, obligan al empleo de tropas especialmente

entrenadas y equipadas y a la aplicación de procedimientos tácticos y técnicos particulares.

i. Operaciones ribereñas: Son operaciones de control, asalto u hostigamiento en las cuales se utiliza la rapidez, la sorpresa y el fuego nutrido sobre objetivos que se encuentren en los ríos o en sus riberas.
ii. Operaciones contra el terrorismo: El empleo de la fuerza militar será prioritario cuando se trate de actos terroristas que atenten contra cualquiera de los frentes de acción del Estado y sus objetivos nacionales.
iii. Operaciones en las áreas fronterizas: Las operaciones militares en la franja fronteriza, sea en un área rural o urbana, evitan o tratan de impedir la infiltración del personal insurrecto y de sus abastecimientos, a través de dichos sectores.
iv. Seguridad de la infraestructura nacional: Se clasifican bajo este nombre, algunas áreas y sitios especiales, en donde operan subestaciones de bombeo de combustibles, de energía hidroeléctrica, termoeléctrico, repetidor de microondas, radares, minas, puentes, oleoductos y líneas de conducción eléctrica; que conforman la base de la infraestructura económica y energética del país.

Una vez definidos los diferentes tipos de operaciones navales que se realizan en la ARE, es necesario establecer cuál de las capacidades de ciberdefensa apoyan a las diferentes operaciones navales, las cuales están descritas en la tabla No. 4.

Tabla 4

Operaciones de ciberdefensa en apoyo de las operaciones navales

TIPO DE OPERACIÓN NAVAL	OPERACIONES DE CIBERDEFENSA		
	EXPLORA-CIÓN	**DEFENSIVA**	**RES-PUESTA**
Operaciones de defensa			
Conquista	X	X	X
Disputa	X	X	X
Ejercicio	X	X	X
Operaciones permanentes			
Mantenimiento de la paz		X	
Imposición de la Paz		X	
Ayuda Humanitaria		X	
Interdicción marítima	X	X	
Control de Tráfico Ilícito	X	X	
Operaciones combinadas	X	X	
Operaciones de Búsqueda y rescate	X		
Operaciones para mitigar desastres	X		
Operaciones de apoyo al desarrollo	X		
Operaciones Especiales	X	X	

Las operaciones navales siguen ciertos principios los cuales han sido considerados como reglas que establecen los militares para dar la solución a un problema militar. En el devenir de los años el personal militar ha culturizado los principios de la guerra en su doctrina y en la toma de

decisiones, llegando a definirlos como conjunto de normas profesionales comunes, valores y patrones arraigados en la cultura naval.

En base a la aplicabilidad de estos principios como medidas a ser consideradas para la solución favorable de un conflicto, la Armada del Ecuador ha aceptado los siguientes:

- El objetivo representa la idea directriz de ser mantenido como guía indispensable para acciones posteriores. Es obtener un objetivo militar establecido que debe ser decisivo, alcanzable y claramente definido.
- Ofensiva es una actitud basada en una serie de acciones que constituyen la manera más eficaz y decisiva para alcanzar un objetivo común.
- Flexibilidad es la capacidad de adaptarse rápidamente y reaccionar frente a escenarios simultáneos y dinámicos cambiantes que superen lo inesperado, manteniendo la libertad de acción.
- Seguridad es cuidarse contra la acción del enemigo, evitando ser sorprendidos, estableciendo y manteniendo medidas de protección. Es esencial para mantener la libertad de acción y la potencia de combate, aplicando medidas de seguridad activas / pasivas con el fin de negar información crítica al adversario.
- Sorpresa consiste en elegir el momento, lugar y método para atacar al enemigo, de manera que este no se encuentre preparado para defenderse, ubicándolo en una situación inesperada que le imposibilite reaccionar con oportunidad.
- Concentración es confluir la potencia de combate en tiempo y espacio, en el momento y lugar decisivos, alcanzándose una potencia de combate superior para dar un golpe decisivo en el punto débil del enemigo, a fin de destruirlo o neutralizarlo.

- Unidad de mando significa que todas las fuerzas están bajo un mando responsable. Se requiere un solo comandante con la autoridad necesaria para dirigir todas las fuerzas en la búsqueda de un propósito unificado.
- La economía de las fuerzas es asignar el máximo de fuerzas al objetivo principal y el mínimo necesario a los objetivos secundarios.
- Movilidad es la capacidad de trasladar y mantener fuerzas hacia donde se necesiten, permite lograr y mantener la libertad de acción. Determina movimiento, flexibilidad y rapidez; facilita la sorpresa y provee de mayores opciones a la maniobra.
- Simplicidad es elaborar planes y órdenes claros, precisos y concisos, utilizando un lenguaje simple, sencillo, fácil de transmitir y de entender, reduciendo las malas interpretaciones y las situaciones confusas.
- Unidad de esfuerzo es la capacidad de operar en forma conjunta con el máximo esfuerzo, para lograr objetivos comunes.
- Mantenimiento de la moral basada en el liderazgo en todos los niveles, en el sentido de pertenencia de lo nacional, en la autoestima y fe institucional e inspirada en un objetivo común.

Algunos de estos principios pueden ser vinculados con acciones de ciberdefensa a fin de conseguir una aplicación de los mismos en las operaciones en el ciberespacio. Estos preceptos se construyen sobre los principios de la conducción exitosa de la operación y su apego es esencial para la consecución de la victoria. La aplicación de uno o más de los preceptos dependerá del tipo de operación a realizarse.

Tabla 5
Aplicabilidad de los principios de las operaciones en el área cibernética

PRINCIPIO	APLICACIÓN
Objetivo	Tener claro los objetivos a ser atacados
Ofensiva	Realizar ataques a las redes del oponente.
Flexibilidad	Tener la capacidad de hacer ataques simultáneos en el ciberespacio
Seguridad	Realizar acciones que protejan el ciberespacio propio
Sorpresa	Ataques cibernéticos no anunciados
Concentración	Realización de ataques preventivos hacia objetivos determinados
Unidad de mando	Utilización de un centro de control de red de la información
Economía de fuerzas	Poder realizar un ataque masivo al objetivo principal
Movilidad	Contar con recursos para hacer ataques a otros objetivos
Simplicidad	Todas las actividades deben ser comprendidas, para una mejor actuación de las operaciones
Unidad de esfuerzo	Las operaciones deben ser realizadas en forma conjunta por los actores
Mantenimiento de la moral	Todos los actores deben estar presentes de la defensa de lo nacional.

Dado que las operaciones en el ciberespacio son transversales a los diferentes tipos de operaciones, ya sean terrestres, aéreas o navales, es necesario recalcar que estas juegan un papel fundamental como apoyo a la ejecución de las operaciones militares, en este caso muy especial a las operaciones navales.

2.5. Marco Legal

La pirámide Kelseniana es un importante recurso que nos permite ver la jerarquía de las normas jurídicas, vamos a utilizar esta herramienta para mostrar y dar a conocer las regulaciones

establecidas relacionadas con las tecnologías. Es de entender que para este análisis se trataran las normas nacionales e internacionales que permiten a esta investigación tener un concepto ampliado de la jurisdicción en el área tratada. La jerarquía mencionada la podemos observar en la siguiente figura.

Figura 16. Jerarquía de Leyes - Pirámide de Kelsen

En la esfera internacional, se debe mencionar que varios países de la región han creado legislación para el correcto uso de las TIC´s y para sancionar los diferentes tipos de delitos como son el caso de Colombia, Brasil, Chile, Uruguay, entre otros. A nivel mundial podemos decir que existen países que ya contemplan en su legislaciones, la tipificación de los delitos informáticos, es así que organismos internacionales como la Organización de las Naciones Unida, ONU, la Comunidad Europea, la Organización de Estados Americanos, OEA, entre otros, conminan a sus países

miembros al establecimiento de leyes y aplicación de sanciones a los delincuentes que utilicen los medios tecnológicos para el cometimiento de actos ilícitos con los sistemas de información.

La legislación ecuatoriana posee algunos elementos que ayudan en la protección del ciberespacio, sin embargo, no es hasta el año 2014, con la aprobación del Código Orgánico Integral Penal, donde se tipifican los delitos informáticos.

La Constitución de la República del Ecuador en sus articulados consagra el derecho a la protección de datos de carácter personal, a la protección de la intimidad personal, al derecho a la inviolabilidad y al secreto de la correspondencia física y virtual.

La Ley de Seguridad Pública y del Estado: Publicada formulada en el 2010, establece la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar.

La Ley Orgánica y Acceso a la Información Pública, LOTAIP, divulgada en el 2004, tiene por objeto garantizar el libre acceso a la información pública, por parte de los ciudadanos, tal como los estipula la carta magna en el Art. 81, que señala "la información es un derecho de las personas que garantiza el Estado".

La Ley de Comercio electrónico, firmas electrónicas y mensajes de datos publicada en el año 2002, tiene como fin, dar un valor jurídico a los mensajes de datos, tal y como si fueran documentos escritos. Esta ley establece a la firma electrónica como un requisito de validez para dar legalidad a un documento.

La Ley de propiedad Intelectual publicada en el año de 1998, tiene como objetico brindar una adecuada protección a los derechos intelectuales y asumir la defensa de los mismos, a fin de brindar confianza al desarrollo tecnológico y económico del país. Es de mencionar que esta ley en

su codificación da el soporte legal para la protección de las bases de datos y programas de computador.

La Ley especial de telecomunicaciones publicada en el año 1992, tiene por objeto normar la instalación, operación y utilización de toda trasmisión, emisión, señales, imágenes, sonidos e información de cualquier naturaleza por medio de sistemas radioeléctricos, medios ópticos y otros sistemas electromagnéticos.

Código Orgánico Integral Penal penaliza los siguientes delitos: pornografía infantil, violación del derecho a la intimidad, revelación ilegal de información de bases de datos, interceptación de comunicaciones, pharming[6] y phishing[7,] fraude informático, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicaciones. A continuación, se muestra la tipificación de los delitos informáticos asociados con la seguridad

Tabla 6
Delitos Informáticos

DELITOS INFORMÁTICOS	SANCIÓN
ART 178 Violación a la intimidad	1-3 años
ART 190 Apropiación fraudulenta por medios electrónicos	1-3 años
ART 191 Reprogramación o modificación de información	1-3 años

CONTINÚA

[6] Técnica de explotación de una vulnerabilidad en los servidores de Dominio (DNS), redirige el nombre del dominio a otra máquina distinta.

[7] Técnica de ingeniería social que consiste en el envío de correos electrónicos, haciéndose pasar por un tercero (suplantación de identidad), con la finalidad de obtener datos confidenciales del usuario.

ART 192 Intercambio, comercialización o compra de información	1-3 años
ART 195 Infraestructura ilícita	1-3 años
ART 229 Revelación ilegal de base de datos	1-3 años
ART 230 Interceptación ilegal de datos	3-5 años
ART 232 Ataque a la integridad de sistemas informáticos	3-5 años
ART 233 Delitos contra la información pública reservada	5-7 años
ART 234 Acceso no consentido a un sistema informático	3-5 años

En lo concerniente a ciberdefensa, en el ámbito internacional, se debe mencionar la existencia del Manual de Tallin, el cual identifica el derecho internacional que puede aplicarse a la ciberguerra estableciendo 95 normas que deberían regir a este tipo de conflictos, incluyendo temas como soberanía, derecho internacional humanitario, el "just ad bellum[8]", el "just in bello[9]", entre otros. Sin embargo, se debe mencionar que las operaciones cibernéticas plantean ciertas consideraciones para el derecho internacional, como son los conceptos de soberanía/jurisdicción y atribución y responsabilidad.

Cuando se trata de establecer los límites al ciberespacio o considerar un lugar geográfico o físico al mismo, se genera una serie de dudas, dado que conceptualmente este definido por redes de computadoras y sistemas conectados, siendo esta conexión un entorno global, en donde no es factible aplicar un concepto de soberanía pues no existen límites que permita realizar esta separación.

[8] Es el derecho en la guerra con el fin de limitar el sufrimiento causado por la guerra.
[9] Es el derecho sobre el empleo de la fuerza con el fin imitar el uso de la fuerza entre Estados.

La aplicación de diferentes técnicas y capacidades en el ciberespacio, hace que las operaciones en el ciberespacio tengan una gran dificultad para localización del origen del mismo, lo que hace difícil atribuir una responsabilidad directa del ataque. Al no poder identificar efectivamente al atacante no es posible ejercer una adecuada respuesta y no hacer ejercicio de una legítima defensa.

Es así que a nivel mundial no se ha logrado un consenso en la aplicabilidad de normas de enfrentamiento en el ciberespacio, donde quedan varias inquietudes sobre el uso y manejo de las ciber operaciones, sin embargo, los países más desarrollados han declarado públicamente la creación de ejércitos de ciberdefensa para proteger la infraestructura critica del Estado ante un ataque cibernético o en su defecto realizar operaciones en el ciberespacio en forma no declarada.

En el Ecuador, en el campo de la ciberdefensa, se ha podido identificar las siguientes normativas:

- El Plan Nacional de Seguridad Integral 2019-2030, contiene 33 objetivos, 99 estrategias y 148 acciones, de los cuales expresaremos los objetivos y estrategias relacionados con la ciberdefensa (Gabinete Sectorial de Seguridad, 2019):
  - Objetivo 1: Defender la soberanía e integridad territorial (terrestre, marítimo, aéreo, espacio y promoviendo la seguridad y libertad de las personas en el ciberespacio); mediante la aplicación de estrategias militares multidimensionales sustentadas en capacidades estratégicas conjuntas.
    - Estrategia 1: Ejecutar acciones estratégicas orientadas a la disuasión y defensa de todo el territorio nacional.
    - Estrategia 2: Blindar la infraestructura critica del Estado.

- En el Plan Específico de la Defensa 2019-2030, se establece los siguientes lineamientos en cuanto a ciberdefensa (Ministerio de Defensa Nacional, 2019):
  - Objetivo 1: Fortalecer la defensa y la seguridad, indica que el Estado participara en el control efectivo del territorio nacional, fomentando las políticas y estrategias de ciberseguridad y ciberdefensa.
  - Objetivo 2: Fortalecer las capacidades estratégicas conjuntas de Fuerzas armadas, se establece que en el ámbito de ciencia y tecnología se fomentará la cooperación en investigación, desarrollo e innovación (I+D+i), orientados a fortalecer las capacidades de FFAA en el área de ciberseguridad.
- El Acuerdo Ministerial 281 del Ministerio de Defensa Nacional (MIDENA), del 24 de septiembre del 2014, crea el Sistema de ciberdefensa del MIDENA como el mecanismo que articula las instancias permanentes y de conformación que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional. Además, estructura el Comité de ciberdefensa y conforma el Comando de Ciberdefensa (COCIBER), en el Comando Conjunto de las Fuerzas Armadas (COMACO). Entre las atribuciones principales que se le atribuye al COCIBER es la de elaborar el Plan de Ciberdefensa y desarrollar la capacidad de ciberdefensa.

En el ámbito de la Armada del Ecuador, entre los elementos de gestión de la Institución se posee el Plan de Gestión Bicentenario, el cual tiene por objeto establecer los más amplios lineamientos para el direccionamiento de la organización. Entre las directrices a cumplir por los diferentes repartos se establece la necesidad de contar un centro de ciberdefensa, que permita dar apoyo y seguridad a las operaciones navales en el ámbito del ciberespacio. Esta necesidad que el

Mando naval ha presentado en el documento antes mencionado, es sin lugar a duda una necesidad Institucional, dada la importancia que ha tomado el ciberespacio en todas las actividades tanto operativas como administrativas.

2.6. Variables.

Dependiente: operaciones navales

Definición. - Las operaciones navales consisten en la aplicación de los principios políticos, de planificación, organización y administración en el uso de los recursos y de la fuerza naval, en la formación diaria y actividades de las unidades para conseguir metas u objetivos específicos. Es la capacidad que tienen las unidades navales para poder navegar, combatir y detectar a las amenazas.

Independiente: Operaciones de ciberdefensa

Definición. - Las operaciones en el ciberespacio son aquellas en las cuales se emplea las ciber capacidades para lograr los objetivos militares o efectos a través del ciberespacio.

A continuación, se presenta el cuadro de operacionalización de las variables.

Tabla 7

Operacionalización de las variables

VARIABLE	DIMENSION	INDICADORES	VALORES
Operaciones de ciberdefensa	Operaciones de defensa	Presencia de operaciones	Si - No
	Operaciones ofensivas	Presencia de operaciones	Si - No
	Operaciones de exploración	Presencia de operaciones	Si - No
Operaciones navales	Operaciones de defensa	Grado de incidencia	Alto – Medio - Bajo
	Operaciones Permanentes	Grado de incidencia	Alto – Medio - Bajo

2.7. Hipótesis.

¿La incidencia de las operaciones de ciberdefensa en las operaciones navales, hace necesaria una organización de ciberdefensa en la Armada del Ecuador?

CAPÍTULO III

METODOLOGÍA

3.1 Tipo de Investigación.

La investigación correspondiente a la incidencia de las operaciones de Ciberdefensa en las operaciones navales es de tipo exploratoria en donde se busca determinar aspectos relacionados a la influencia, importancia, características, entre otros, de las operaciones de ciberdefensa en apoyo a la conducción de las operaciones navales y dado que el alcance de esta investigación está dado por la propuesta de una organización de ciberdefensa para la Armada del Ecuador.

El enfoque metodológico que tiene este documento es: Cualitativo Inductivo, dado que se hará una recolección de datos para generar nuevas interrogante e ira desde un análisis general hasta llegar a una solución especifica

De igual forma es necesario efectuar una revisión documental de los diferentes procesos que tienen el centro de ciberdefensa a fin de determinar los componentes que pueden ser utilizados en la ARE, para realizar las operaciones.

El trabajo está orientado a dar una solución organizacional que permita mejorar la seguridad en el ciberespacio a fin de mejorar la disponibilidad, integridad y confidencialidad de la información que se maneja en las operaciones navales.

3.2 Población y muestra.

Para el presente trabajo de requiere identificar el mercado Objetivo, necesario para lograr una solución que permita a la Armada del Ecuador mejorar las capacidades de ciberdefensa en apoyo a las operaciones navales.

El mercado en el cual se va a observar las competencias de los sistemas informáticos y ciberdefensa, se centra en la Armada del Ecuador y en ciertas actividades relacionadas a la gestión y uso de sistemas informáticos y redes:

- Protección de redes
- Protección de Centros Informáticos y bases de datos (físicas y de datos)
- Protección de sistemas de mando y control
- Protección de la información en las operaciones navales.

Por tanto, el interés de la implementación de centro de ciberdefensa se centra en las operaciones de ciberdefensa en el ciberespacio que el Estado ecuatoriano en general y de la Armada del Ecuador en particular, pueda aplicarlas en los siguientes casos:

1) Operaciones navales de orden militar.
2) Operaciones navales como autoridad marítima
3) Operaciones de exploración en el ciberespacio.
4) Operaciones de respuesta ante ataques enemigos
5) Operaciones de defensa de los centros mando y control
6) Operaciones de defensa de la Red Naval de Datos, RDN

7) Operaciones de defensa de los centros de datos
8) Operaciones de defensa de la infraestructura critica, entre otros.

Para lograr todo este esfuerzo, es importante poseer una línea base de cómo está estructurada la gestión informática relacionada a la Armada del Ecuador, el cual define aspectos importantes, como el relacionado con el Software, el hardware y como esto es apoyado por la ciberdefensa.

La población está dada por los Oficiales que son especialistas en el área de seguridad de la información o informática y los Oficiales que tengan una experiencia en ciberdefensa, para el presente caso se tomaran los oficiales del curso de Estado Mayor y personal vinculado con el tema.

Dado que este es un conocimiento nuevo y se requiere de personas específicas que participen en la muestra se realizará un tipo de muestreo no probabilístico.

El cálculo de la muestra, será efectuada en base a la población detallada en la Tabla No.7, y de acuerdo a los siguientes parámetros:

Margen de error: 5%

Nivel de Confianza: 90%

La fórmula que se aplicará para el tamaño de la muestra, será la correspondiente a la ecuación estadística para proporciones poblacionales, la misma que se detalla a continuación:

$$n = \frac{z^2(p * q)}{e^2 + \frac{(z2 * (p * q))}{N}}$$

Donde:

n= Tamaño de la muestra

z= Nivel de confianza deseado

p= Proporción de la población con la característica deseada

q= Proporción de la población no deseado

e= Nivel de error a cometer

N= Tamaño de la Población

Tabla 8

Población considerada para la encuesta

NIVEL DE CONOCIMIENTO	OFICIALES
Título de Cuarto nivel en especialidades afines	6
Título de tercer nivel en áreas afines de conocimiento	18
Personal afín a la ciberdefensa	15
TOTAL	**39**

Nota: Elaborador por el autor, en base a información proporcionada por la Dirección General de Personal

Luego de aplicar la formula indicada se obtiene como resultado, que al menos se requiere 36 encuestados, para satisfacer los parámetros de confianza.

3.3 Métodos y tipos de muestreo.

El tipo de muestreo como se mencionó anteriormente será el tipo no probabilístico, por cuanto el personal al cual se ha dirigido la encuesta no ha sido aleatorio sino ha sido direccionado a personal con experiencia en el área o han tenido alguna vez un conocimiento sobre la materia a tratarse. La encuesta fue preparada y desarrollado en la herramienta informática Google Forms y cuyo detalle se adjunta en el Anexo

"B". Esta encuesta fue realizada de manera online, utilizando el correo de la Armada y la herramienta WhatsApp.

3.4 Técnicas e Instrumentos de recolección de información.

Los métodos y técnicas utilizados para la recopilación de datos, dado el enfoque cuantitativo se establecen como instrumentos de investigación:

- Encuesta realizada a una muestra no probabilística de la población naval para verificación de estado del conocimiento en ciberdefensa
- Entrevista cualitativas a personas expertas y que tengan relación con la ciberdefensa.
- Revisión documental de estado de madurez d

En base a estos métodos y técnicas se buscará dar una solución a la necesidad de que la Armada cuente con un organismo que le permita ser un apoyo en las operaciones navales en el ciberespacio.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Presentación de los resultados

4.1.1 Diagnostico situacional

4.1.1.1 Instrumento No. 1: Exploración Documental.

El Instrumento analizado en primer lugar fue una encuesta nivel mundial sobre las principales amenazas y vulnerabilidades que preocupan a las grandes empresa as a nivel mundial, la cual mencionaremos a continuación.

La encuesta Global de seguridad de la información del año 2017-2018[10], estableció los siguientes puntos: (Ernst & Young, S.L, 2017).

- Las ciberamenazas están catalogadas en tres categorías: ataques comunes, ataques avanzados (realizado por hackers sofisticados como grupos organizados, equipos de espionaje industrial, ciberterroristas y hasta naciones) y ataques emergentes (realizado por hackers sofisticados, pero orientados a tecnologías emergentes, como el aprovechamiento de vulnerabilidades en smartphones).

[10] Estudio global realizado por la empresa EY con la participación de más de 1200 empresas a nivel mundial.

- Entre las vulnerabilidades de ciberseguridad que más preocupa, es la que tiene que ver con los empleados desprevenidos o descuidados y las que utilizan mecanismos de control obsoletos.
- Los ataques de malware y phishing son las dos principales amenazas identificadas.

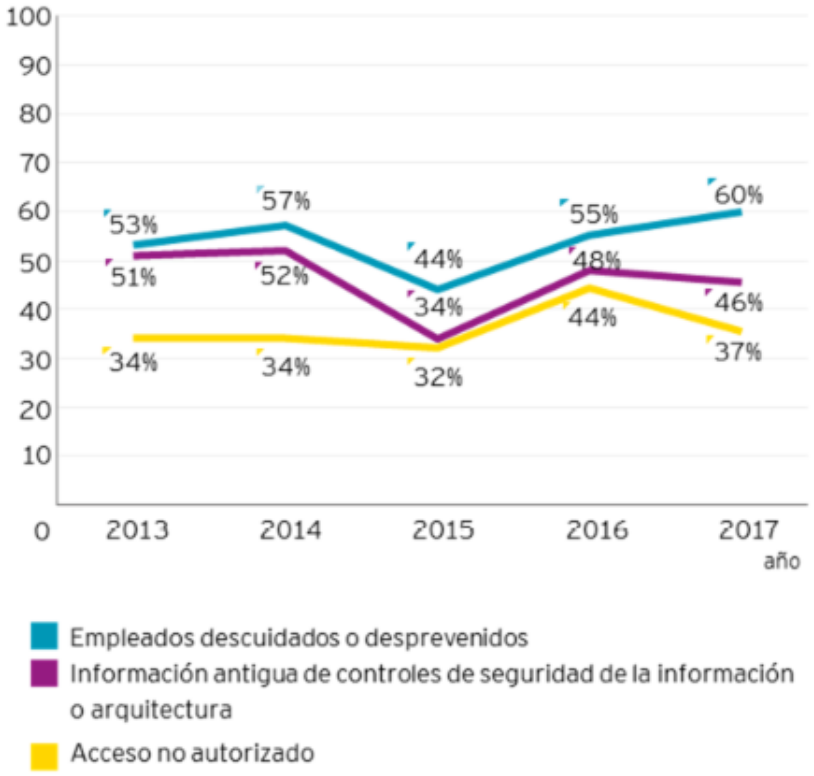

Figura 17. Vulnerabilidades con mayor preocupación en las empresas
Fuente: (Ernst & Young, S.L, 2017)

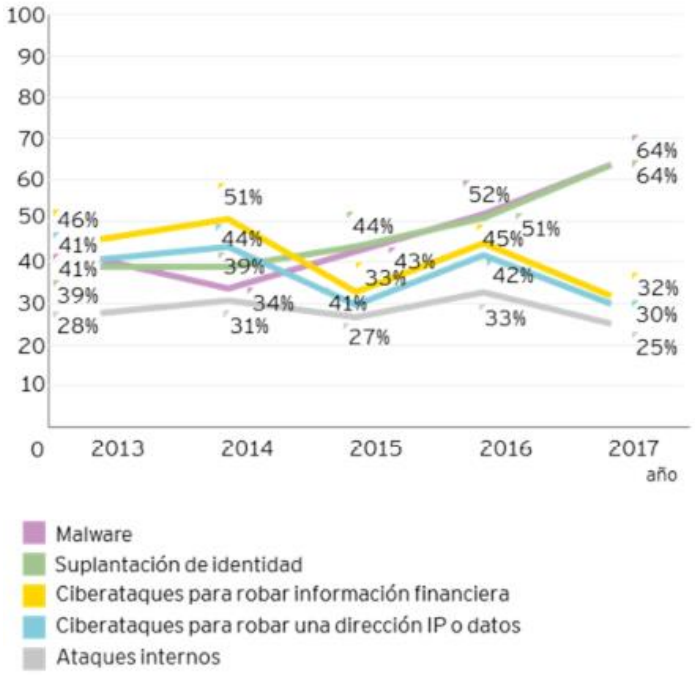

Figura 18. Amenazas de mayor preocupación
Fuente: (Ernst & Young, S.L, 2017)

Así también se considera el informe de ciberseguridad del año 2016 del Banco Interamericano de Desarrollo, BID, en el cual se establece la capacidad de seguridad cibernética y el nivel de madurez que tiene los países de América Latina y el Caribe.

Este informe para establecer los diferentes modelos de madurez de la seguridad cibernética en cada uno de los diferentes países realizó el análisis desde cinco dimensiones:

- Política y Estrategia: Con dos componentes principales: Estrategia de Ciberseguridad y Ciberdefensa.
- Cultura y sociedad: Con cuatro componentes: Mentalidad de seguridad cibernética, conciencia de seguridad cibernética, confianza en el uso del internet y privacidad en línea.

- Educación: Con cuatro componentes: Disponibilidad nacional de la educación y formación cibernéticas, desarrollo nacional de la educación de ciberseguridad, formación e iniciativas educativas públicas y privadas y gobernanza corporativa, conocimiento y normas.
- Marcos Legales: Con tres componentes: Marcos jurídicos de cibertinteligencia, investigación jurídica y divulgación responsable de la información.
- Tecnologías: Con siete componentes: Adhesión a normas, organizaciones de coordinación de ciberseguridad, respuesta a incidentes, resiliencia de la infraestructura nacional, protección de la infraestructura critica nacional, gestión de crisis, redundancia digital.

En este estudio se definen cinco niveles de madurez para cada una de las dimensiones:

- Inicial: En este nivel no existe nada o existe algo muy pequeño. También existe la posibilidad de un pensamiento, pero sin acción.
- Formativo: Algunas características han iniciado, han sido formuladas, pero se encuentran desorganizadas, mal definidas o son nuevas.
- Establecido: Las características están establecidas y funcionando. Pero no existe la suficiente asignación de recursos y poca toma de decisiones. Aunque se encuentra definido y funcional.
- Estratégico es cuando existe ya una selección de las características que se han implementad y que se encuentran dentro de los objetivos nacionales.

- Dinámico: La organización ha desarrollado métodos para cambiar las estrategias, según las necesidades. La ágil toma de decisiones, la reasignación de recursos y la dinámica de cambios se observan en este nivel.

De acuerdo con el informe presentado, Ecuador en las diferentes dimensiones tiene un promedio de madurez entre inicial y formativo, esto quiere decir que en ciertas áreas no existe nada y en algunas recién ha empezado a crecer. Ver Anexo "A"'- Capacidad cibernética del Ecuador.

4.1.1.2 Instrumento No. 2: Entrevista.

El Instrumento diseñado y aplicado se encuentra en el Anexo "B". La entrevista fue realizada por el investigador para lo cual se utilizaron herramientas como Excel para el procesamiento de datos. Posteriormente esta información fue transcrita y colocada en un resumen de acuerdo a las contestaciones realizadas por el personal entrevistado.

La entrevista fue aplicada a 5 personas:

- Comandante de operaciones navales
- Director de Tecnologías y Comunicaciones
- Asesor operaciones navales de la Academia de Guerra
- Experto asesor operacional
- Experto en seguridad informática.

De las respuestas a las interrogantes, este grupo de conocedores del tema contesto de la siguiente forma a las interrogantes.

¿Qué opina de la ciberdefensa en Ecuador en las FFAA y en la ARE?

- La ciberdefensa no se encuentra estructurada.
- La capacidad de ciberdefensa se encuentra en “pañales”
- No existe esta capacidad.
- Se encuentra en sus primeros pasos

¿Como debería organizarse la ciberdefensa?

- Debería ser organizado entre el nivel técnico y el nivel operativo.
- Se requiere de avanzado conocimiento técnico
- Se debe primero fortalecer la organización
- Debe ser parte del área operativa.

¿Cómo incide las operaciones de ciberdefensa en las operaciones navales?

- Son de gran importancia en las operaciones navales.
- Es necesario proteger los sistemas de mando y control
- La protección de los centros de control es de vital importancia
- La capacidad de económica de las organizaciones delictivas en muy fuerte lo que podría ocasionar in

¿Cuál considera la línea base de la Ciberdefensa en la Armada del Ecuador?

- Se encuentra en un nivel defensivo
- Está en estudio
- Se encuentra en preparación
- Todavía no se evidencia un crecimiento

- Esta en una fase inicial

¿Quién debería ser el reparto encargado de la Ciberdefensa?

- Debería ser un trabajo conjunto entre lo técnico y Operativo.
- Por responsabilidad debería tener la indicativa el sector Operativo.
- Debería ser el ente técnico en su etapa inicial.
- Es un trabajo conjunto.

¿Existe personal capacitado en el tema?

- No existe personal
- Es limitado el personal que conoce del tema
- Se debe capacitar al personal
- Se debe tener un plan de capacitación.

De las respuestas obtenidas por el grupo de conocedores del tema se puede concluir lo siguiente:

- Existe una gran incidencia de las operaciones de ciberdefensa en las operaciones navales, pues existe la necesidad de proteger los sistemas y asegurar la disponibilidad, confiabilidad e integridad de los mismos.
- Sobre la línea base o situación actual de las operaciones de ciberdefensa, el personal consultado ha manifestado que no existe ciberdefensa en la Armada del Ecuador y que este es un proceso que recién se está desarrollando, pero que todavía no hay nada en concreto.

- En referencia a la capacitación del personal se estableció por los entrevistados, que no existe la cantidad suficiente de personal capacitado para realizar este trabajo y que debe considerarse como primordial esta actividad, ya que el éxito de las operaciones depende del grado de conocimiento que tenga el personal.
- En cuanto a la organización se estableció que esta capacidad debe ser tratada desde el punto de vista operativo, pero que debe tener el respaldo del ente operativo, ya que son operaciones militares, con un grado de conocimiento altamente tecnificado.

4.1.1.3 Instrumento No. 3: Encuesta.

El Instrumento diseñado y aplicado se encuentra en el Anexo "C". La encuesta fue elaborada en la herramienta informática Google Forms, las preguntas fueron elaboradas en formato escala tipo Likert: Totalmente en desacuerdo, Neutral, Totalmente de acuerdo; preguntas de selección múltiple, y preguntas de marcar opciones. Este instrumento fue enviado por medio de correo electrónico y por medio de mensajes de WhatsApp a un grupo de conocedores en el área de Ciberdefensa, Seguridad de la información, operaciones navales, Vigilancia Marítima, entre otros.

Para la presentación de los resultados se usaron los recursos de la estadística descriptiva, se organizaron los datos obtenidos en distribuciones por frecuencias absolutas y luego cambiados a porcentajes, se representaron mediante diagrama de barras cada una de las preguntas del instrumento de recolección de datos.

A fin de cumplir con la metodología de la investigación se procedió a realizar la encuesta al personal que fueron parte de la población, los cuales contestaron la encuesta de acuerdo a lo observado en la siguiente gráfica.

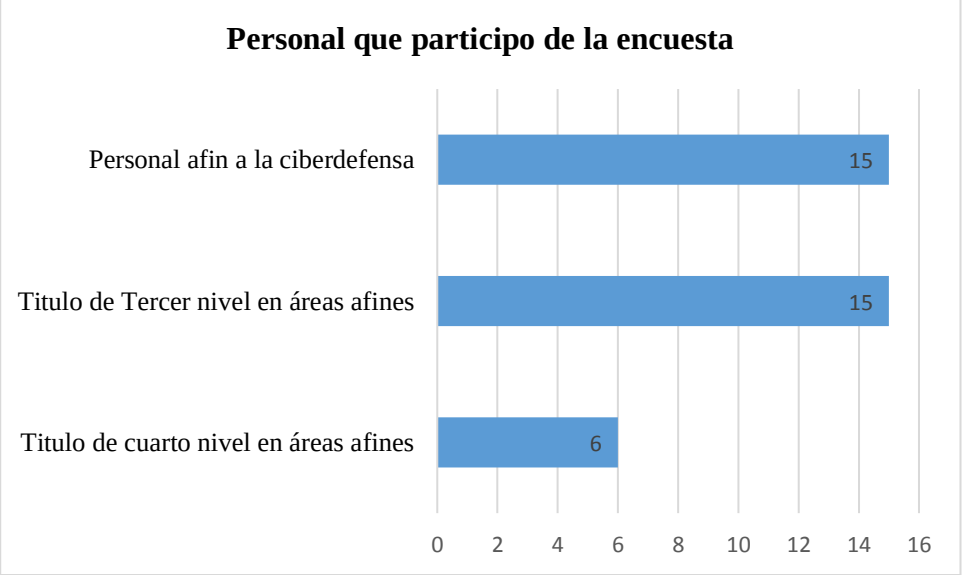

Figura 19. Personal que participó de la encuesta

En la primera sección de la encuesta se busca conocer el grado de percepción de la seguridad cibernética que existe en la Armada del Ecuador y donde se obtuvieron los siguientes resultados.

Tabla 9

Resultados de las respuestas a las preguntas sobre seguridad cibernética

SEGURIDAD CIBERNETICA	TD	%	N	%	TA	%
Pregunta 1	9	25,0%	24	66,7%	3	8,3%
Pregunta 2	18	50,0%	12	33,3%	6	16,7%
Pregunta 3	21	58,3%			15	41,7%
Pregunta 4	15	41,7%	21	58,3%	0	0,0%
Pregunta 5	30	83,3%	3	8,3%	3	8,3%
Pregunta 6	30	83,3%	6	16,7%	0	0,0%

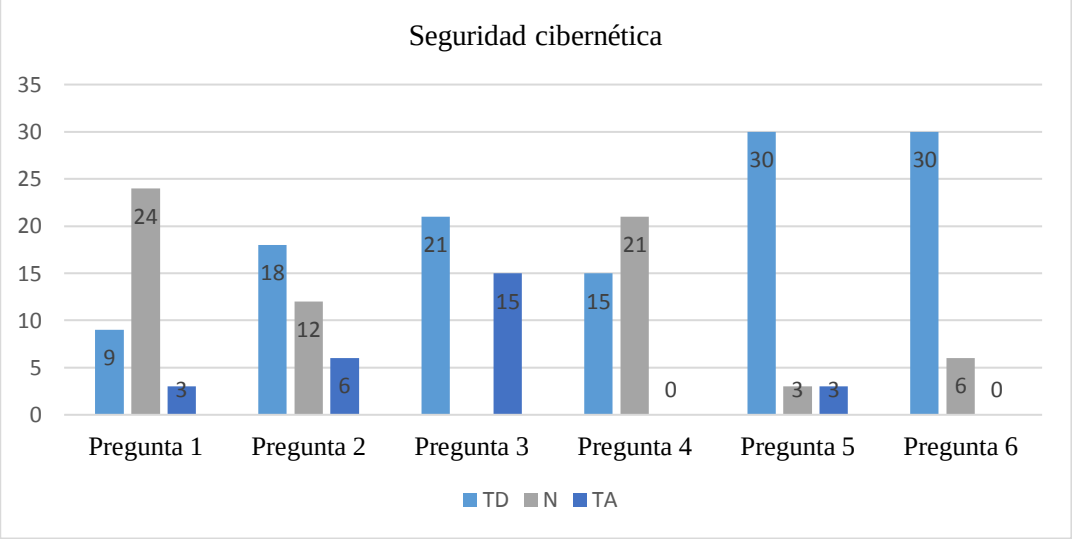

Figura 20. Resultados de las respuestas a las preguntas sobre seguridad cibernética

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en la tabla No. 9 y figura No.20, en la pregunta 1) ¿Considera que se implementan controles de detección, prevención y recuperación de la

información, para la protección contra código malicioso o virus? el **66,7%** considera que existe una posición **neutral** en esta pregunta.

En la pregunta 2) ¿Considera que se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad cibernética?, el **50,00%** está **totalmente de acuerdo** con la pregunta.

En la pregunta 3) ¿Ha sido víctima de un ataque informático?, 58,3% de los encuestados informó que **No** ha sufrido un ataque informático.

En la pregunta 4) ¿Qué nivel de seguridad tienen los sistemas informáticos en la Armada?, el **58,3%** opinó que el nivel de **medio** de seguridad en los sistemas de la Armada.

En la pregunta 5) ¿En su opinión considera suficiente la inversión en seguridad informática?, el **83,3%** contestó que **NO**.

En la pregunta 6) ¿Existe una cultura de ciberseguridad?, el **83,3%** opinó que está **totalmente desacuerdo**.

En conclusión, se puede observar que existe una concientización del sobre la importancia de la seguridad cibernética dentro de la Institución, también de debe considerar que no existe una suficiente inversión en seguridad para llevar a cabo el proceso de seguridad ya que no se han destinado los recursos para tal efecto, además que, en su mayor parte de los encuestados no han sufrido un ataque informático y finalmente se estableció que se debe mejorar la seguridad de los sistemas de la Armada, con la finalidad de no tener problemas en un futuro.

En la segunda sección donde se buscó conocer sobre el grado de conocimiento acerca de las capacidades de ciberdefensa, y a estas interrogantes se obtuvieron los siguientes resultados:

Tabla 10

Resultados de las respuestas a las preguntas sobre Ciberdefensa

CIBERDEFENSA	TD	%	N	%	TA	%
Pregunta 7	9	25,0%	0	0,0%	27	75,0%
Pregunta 8	0	0,0%	0	0,0%	36	100,0%
Pregunta 9	-	-	-	-	-	-
Pregunta 10	27	75,0%	0	0,0%	9	25,0%
Pregunta 11	3	8,3%	0	0,0%	33	91,7%

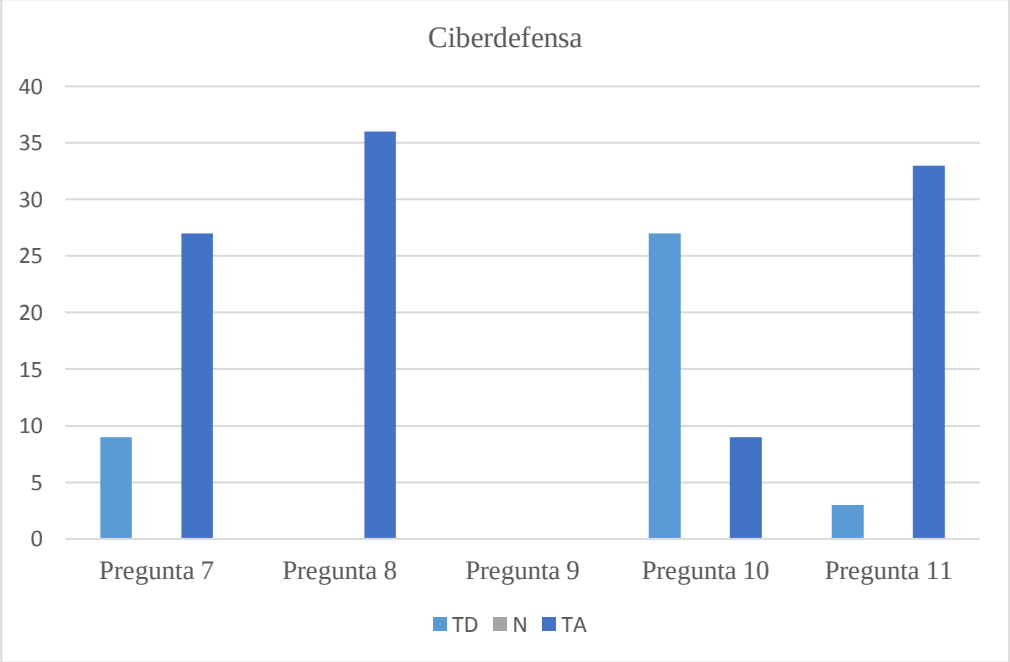

Figura 21. Resultados de las respuestas a las preguntas sobre Ciberdefensa

En la pregunta 7) ¿Ha escuchado hablar sobre las capacidades de Ciberdefensa?, el **75.0%** de los encuestados contestó que SI, lo que evidencia que los encuestados en algún momento ha escuchado sobre las capacidades de ciberdefensa.

En la pregunta 8) ¿Considera que estas capacidades podrían apoyar a la ejecución de las operaciones navales?, el **100%** de los encuestados contestó que **SI**, esto evidencia que los encuestados tienen la percepción que las capacidades de ciberdefensa apoyarían las operaciones navales.

En la pregunta 9) ¿En qué situaciones podría existir apoyo de la ciberdefensa?, el **100%** de los encuestados contestó la Ciberdefensa apoyaría a la **neutralización de los ataques cibernéticos**, en un **91,7%** estableció que apoyaría en la **protección de los centros de mando y control** y finalmente el **58,3%** indicó que ayudaría en la **búsqueda de Información**.

En la pregunta 10) ¿Considera que existe personal capacitado en ciberdefensa?, el **75,0%** de los encuestados contestó que **NO**, lo que demuestra que existe una percepción que no existe personal calificado y que se necesita gente capacitada para enfrentar esta nueva forma de trabajar.

En la pregunta 11) ¿Considera necesario que la Armada posea un centro de Ciber-defensa?, el **91,7%** de los encuestados contestó que **SI**, esto evidencia que existe una concientización de mejorar las capacidades de ciberdefensa y que la forma de hacerlo es con una organización que se encargue de este trabajo en contribución de las operaciones navales.

En conclusión, se puede determinar de las respuestas realizadas por los encuestados lo siguiente: que existe un conocimiento sobre las capacidades de la ciberdefensa y como estas

pueden ayudar a las operaciones navales, además consideran que no existe personal capacitado para llevar a cabo este proceso, y finalmente se estableció que la implementación de un centro de ciberdefensa puede ayudar a mejorar la ciberdefensa en las operaciones navales.

4.2 Análisis y discusión de los resultados

En base a los instrumentos de medición utilizados se va a proceder a determinar el nivel actual de las operaciones de Ciberdefensa en la Armada del Ecuador.

4.2.1 Matriz FODA

Para lograr cumplir con lo descrito anteriormente se utilizará la matriz FODA, donde se analizará los factores internos para identificar las fortaleza y debilidades como son: capacitación, infraestructura, organización, reglamentos y presupuesto. Por otro lado, se analizará el factor externo para identificar las amenazas y oportunidades desde el punto de vista político, tecnológico y social, como se observa en la Figura No. 22.

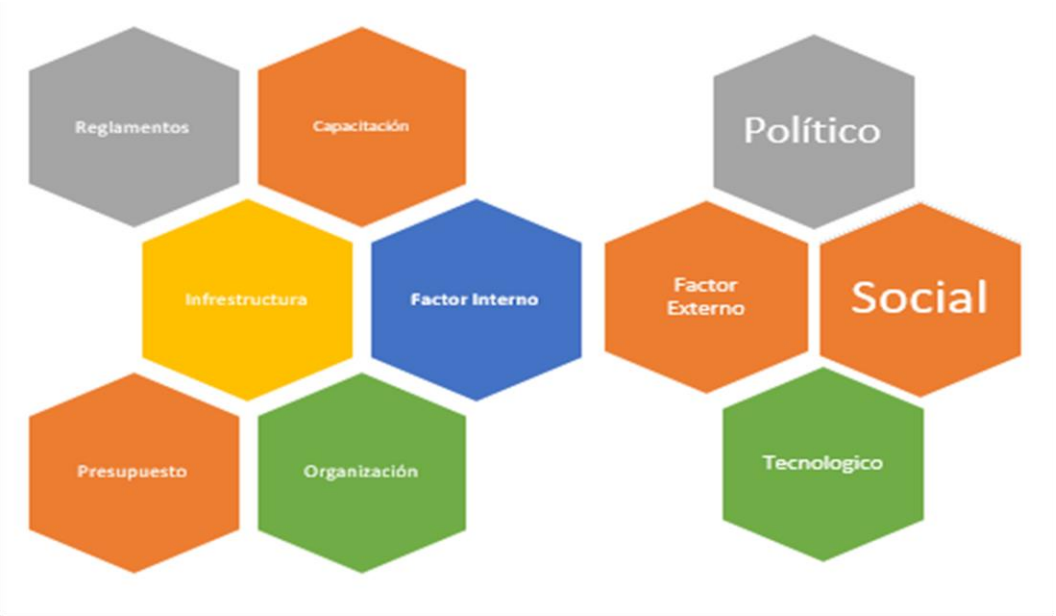

Figura 22. Factores a Evaluarse en la matriz FODA

Fortalezas

- Estructura jerárquica
- Personal con titulación y conocimientos de informática.
- Alto grado de compromiso con la Institución.

Debilidades

- Escasa actividad de operaciones de ciberdefensa.
- No existe una organización encargada de esta actividad.
- No existe suficiente personal capacitado
- No existe doctrina.
- Alta rotación del personal

- No existe equipamiento

Oportunidades

- Es un área de gran interés para la Armada del Ecuador.
- Se requiere de poco presupuesto para su operación.
- Convenios bilaterales o multilaterales con otras Armadas.

Amenazas

- Incremento de ataques cibernéticos.
- Políticas de Estado en el campo de la Ciberdefensa.
- Falta de leyes que regulen el uso del internet y redes sociales

4.2.2 Nivel de madurez

Considerando las cinco dimensiones del nivel de madurez, establecido por el BID, se realizará una analogía para establecer cómo se encuentra las operaciones de ciberdefensa en la Armada del Ecuador:

- Política y Estrategia: En cuanto a este componente se puede establecer que existe un interés por parte del mando naval en la creación de un centro de Ciberdefensa, sin embargo, no se ha generado doctrina que permita una ejecución eficaz de las operaciones de ciberdefensa, por lo tanto, se puede indicar que el nivel de madurez en este componente es un nivel inicial.
- Cultura y sociedad: En este componente se establece que existe una conciencia formativa de los peligros que existen en el personal de la Armada, existe una confianza

en el uso del internet y las personas están conscientes de los peligros existentes y del cuidado que deben tener cuando se encuentran en el ciberespacio. Por lo tanto, se puede establecer que este componente tiene un nivel de madurez formativo.

- Educación: En este componente se evalúa la formación y educación cibernética y conocimiento de las normas, en cuanto a este ámbito se establece que existe un nivel de madurez de inicial, pues todavía no se han formulado educación y formación en ciberdefensa en los diferentes cursos como son los de formación capacitación, y perfeccionamiento, que permita conocer de mejor forma los peligros que existen en el ciberespacio, las medidas de protección y las normas de sanción en caso de realizar algún ataque a los sistemas de la Armada.
- Marcos Legales: En este componente a nivel de Armada del Ecuador, se puede conocer que existe una Directiva sobre seguridad de la información, así como el acuerdo ministerial 166 sobre la implementación del Esquema General de Seguridad de la Información, EGSI. A estas normas a ser implementadas, se deben buscar los mecanismos que permita su cumplimiento. Dado estos antecedentes se puede inferir que el nivel de madurez es formativo.
- Tecnologías: En referencia a este componente se puede observar que la capacidad respuesta a incidentes es limitado, la protección de la estructura critica de la institución no ha podido ser desarrollado, no se ha implementado procesos de gestión de crisis que permita atenuar algún incidente y no se cuenta con sistemas de redundancia. Es por ello que se puede establecer que el nivel de madurez en este componente es inicial.

A continuación, presentamos la situación actual de las operaciones de ciberdefensa, basado en los cinco componentes del BID, como se muestra en la Tabla No. 11.

Tabla 11
Nivel de Madurez de la Ciberdefensa en la Armada del Ecuador

Componentes	Inicial	Formativo	Establecido	Estratégico	Dinámico
Política y Estrategia	X				
Cultura y sociedad	X	X			
Educación	X				
Marco legal	X	X			
Tecnologías	X				

Luego de haber establecido que la ciberdefensa se encuentra en niveles inicial y formativo en la Armada del Ecuador, es importante conocer cuáles son los niveles de madurez de las operaciones de ciberdefensa en las diferentes operaciones navales que son ejecutadas en la ARE.

En la Tabla No. 12 se puede observar el nivel de madurez de las operaciones de ciberdefensa en las operaciones navales, estableciéndose un nivel inicial o formativo en los diferentes tipos de operaciones navales.

Tabla 12

Nivel de madurez de las operaciones de ciberdefensa en las operaciones navales

OPERACIONES NAVALES	OPERACIONES DE CIBERDEFENSA														
	EXPLORACIÓN					DEFENSIVA					RESPUESTA				
	Inicial	Formativo	Establecido	Estratégico	Dinámico	Inicial	Formativo	Establecido	Estratégico	Dinámico	Inicial	Formativo	Establecido	Estratégico	Dinámico
Operaciones de defensa															
Conquista	X					X	X				X				
Disputa	X					X	X				X				
Ejercicio	X					X	X				X				
Operaciones permanentes															
Mantenimiento de la paz						X	X								
Imposición de la Paz						X	X								
Ayuda Humanitaria						X	X								
Interdicción marítima	X					X	X								
Control de Tráfico Ilícito	X					X	X								
Operaciones combinadas	X					X	X								
Operaciones de Búsqueda y rescate	X														
Operaciones para mitigar desastres	X														
Operaciones de apoyo al desarrollo	X														
Operaciones Especiales	X					X	X								

Una vez que se ha podido establecer la importancia de las operaciones de ciberdefensa y de cómo estas pueden incidir en las operaciones navales. Posteriormente establecer la situación actual de la ciberdefensa en la Armada del Ecuador, además de establecer los componentes que pueden ayudar a mejorar las operaciones de ciberdefensa y debido que no existe una organización que se encargue sobre este tema tan importante y de actualidad, la presente investigación establece como solución la creación de un centro de ciberdefensa que se encargue de incrementar las capacidades de ciberdefensa en la Armada del Ecuador a fin de contribuir con la seguridad del ciberespacio.

CAPÍTULO V

PROPUESTA

5.1 Propuesta

En virtud que la propuesta de este proyecto es presentar una organización para la Armada del Ecuador, que permita mejorar las capacidades de ciberdefensa en apoyo a las operaciones navales, se debe considerar que en la actualidad no existe una organización destinada para tal efecto, en virtud de esto se debe considerar que la nueva organización responda a los siguientes principios:

- Líneas de autoridad bien definidas
- Estructura jerárquica claramente definida
- Funciones definidas para cada nivel de la estructura

Para la creación de un organismo de ciberdefensa que mejore las capacidades de las operaciones de ciberdefensa en apoyo a las operaciones navales, se va a seguir el siguiente proceso.

- Se realizará el levantamiento de los procesos gobernantes.
- Se realizará la estructura orgánica.
- Se diseñará el manual de organización.

5.2 Procesos

A fin de determinar los procesos que debe cumplir este organismo de ciberdefensa, citaremos el mapa de procesos del Comando de Ciberdefensa, en los cuales se observan los procesos gobernantes, los procesos adjetivos y los procesos sustantivos.

Los procesos agregadores de valor identificados para una organización de ciberdefensa, son: exploración, defensa y respuesta.

El proceso de exploración es aquel el cual busca la recolección de la información sobre las ciber capacidades en los sistemas de información y comunicaciones del posible adversario.

Figura 23. Mapa de procesos del Comando de Ciberdefensa
Fuente: (Comando de Ciberdefensa, 2018)

El proceso de defensa es cíclico y está compuesto por tres etapas principales (National Cyber Security Authority, 2017):

- Planificación y evaluación. - Consiste en el inventario de los principales sistemas a defender en la organización, evaluación del riego, inspección de los controles existentes y diseño de la planificación. evaluación, inspeccionando los medios de defensa existentes (controles), y diseño de trabajo para cerrar las brechas de defensa.

- Ejecución. - Esta etapa es la realización del plan de trabajo mediante el desarrollo de los procesos organizativos, integración de herramientas y de la organización de ciber-defensa.
- Mantenimiento. - Se debe mantener las defensas actualizadas a la luz del cambio dinámico en el ciberespacio de la organización, como por ejemplo instalación de nuevos equipos, software, creación de nuevos servicios. Así también las amenazas y métodos de ataque cambian por lo cual también se debe evolucionar constantemente.

El proceso de respuesta es aquel en el cual se ejecutan y mantienen medidas y acciones ofensivas de acuerdo a las necesidades operativas para neutralizar, interrumpir, alterar o destruir amenazas o ataques.

A continuación, se describirán las diferentes actividades que se cumplen en cada uno de los procesos. Entre las principales actividades que se cumplen en los diferentes procesos:

- Actividades de Exploración
  - Elaborar hoja de ruta para cumplir la Orden de operaciones.
  - Elaborar el Plan de búsqueda de cibertinteligencia.
  - Realizar la Recolección de información mediante identificación de Señuelos y/ Teste de Penetración.
  - Realizar el análisis y producción de cibertinteligencia.
  - Elaborar informes para la toma de decisiones.
  - Analizar impactos y toma de decisiones
- Actividades de Defensa
  - Planificar la monitorización de los sitios WEB a ser controlados.

- Configurar herramientas para el monitoreo.
- Realizar el Monitoreo de disponibilidad confidencialidad e integridad de servicios de intranet y repartos navales.
- Informes de Monitoreo.
- Registrar los incidentes.
- Realizar la clasificación y priorización del incidente.
- Analizar la base de conocimientos para tratar el incidente.
- Coordinar la resolución del incidente.
- Elaborar informes de incidentes.
- Remitir Informes de resolución del incidente.
- Realizar el registro y recepción del pedido.
- Realizar la configuración de herramientas a utilizar.
- Ejecutar el Trabajo forense informático.
- Elaborar Informe de Investigación Forense Informático.
- Elaborar informes ejecutivos de Resolución de Incidentes / Investigación forense informático.
- Remitir Informes para interesados

- Actividades de Respuesta
  - Analizar los posibles Cursos de Acción.
  - Coordinar incremento de apreciaciones de cibertinteligencia para objetivo establecido.
  - Analizar la el curso de acción más probable.
  - Definir el curso de Acción a seguir.

- Ejecutar acciones de Degradación, Destrucción, Explotación y Limpieza.
- Investigación y Desarrollo de Ciberarmas.
- Elaborar informes de Respuesta.
- Evaluar informes del Curso de Acción Ejecutado.
- Ejecutar la actualización del Curso de Acción.
- Ejecutar la alimentación de doctrina de respuesta en repositorio

El mapa de procesos para el centro de ciberdefensa estaría dado de la siguiente manera:

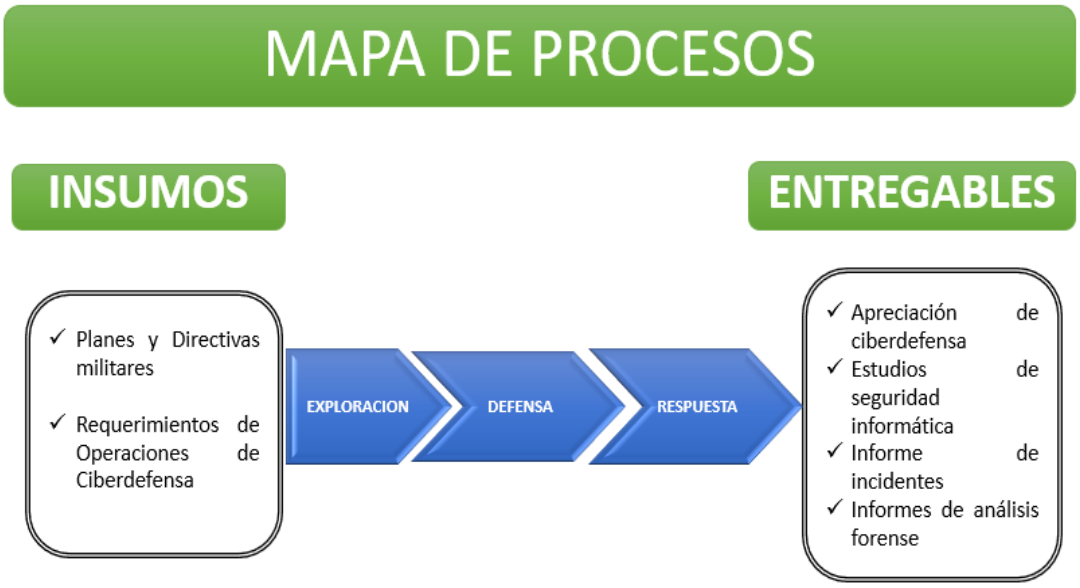

Figura 24. Mapa de Procesos del centro de ciberdefensa

5.3 Organización

De acuerdo a lo observado en los diferentes tipos de estructuras organizacionales internacionales y nacionales, se establece que estas organizaciones realizan operaciones militares, por lo cual

deben estar bajo el mando de una Órgano Operativo, en el caso de la Armada del Ecuador este debe estar bajo el mando del Comando de operaciones navales.

Considerando el análisis de la situación actual, así como el nivel de madurez que existe de las operaciones de Ciberdefensa y a fin de mejorar estos niveles se plantea la siguiente propuesta orgánica, donde se establecen las principales áreas que se requieren para poder llevar adelante las operaciones de ciberdefensa.

5.3.1 Órganos de Dirección

- Comando

Es el quien dirigirá la conducción de las operaciones de ciberdefensa.

5.3.2 Órganos de Asesoría

- Planificación

Es el área encargada de definir la planificación y crecimiento de la unidad para responder a las necesidades futuras.

5.3.3 Órganos de línea

- Operaciones de Exploración

Esta es el área donde se realizarán las operaciones de exploración, entre las principales actividades que desarrollará esta área son:

  - Elaborar el plan de búsqueda de cibertinteligencia/
  - Recolección de información mediante identificación de señuelos y pruebas de penetración.

- Elaboración de informes de cibertinteligencia.

- Operaciones de Defensa

  En esta sección se realizarán las operaciones de defensa, entre las principales actividades que desarrollará esta área son:

  - Realizar el monitoreo y control de los servicios.
  - Realizar el seguimiento de los incidentes.
  - Realizar análisis forenses
  - Realizar el hardering de la infraestructura.
  - Elaboración de informes de monitoreo
  - Elaboración de informes de análisis forenses

- Operaciones de Respuesta

En esta área se realizarán las operaciones de defensa, entre las principales actividades que desarrollará esta área son:

- Ejecutar acciones de degradación, destrucción, explotación y limpieza
- Investigación y Desarrollo de Ciberarmas.

En base a las necesidades presentadas, se puede establecer un organigrama propuesto como el determinado en la siguiente figura:

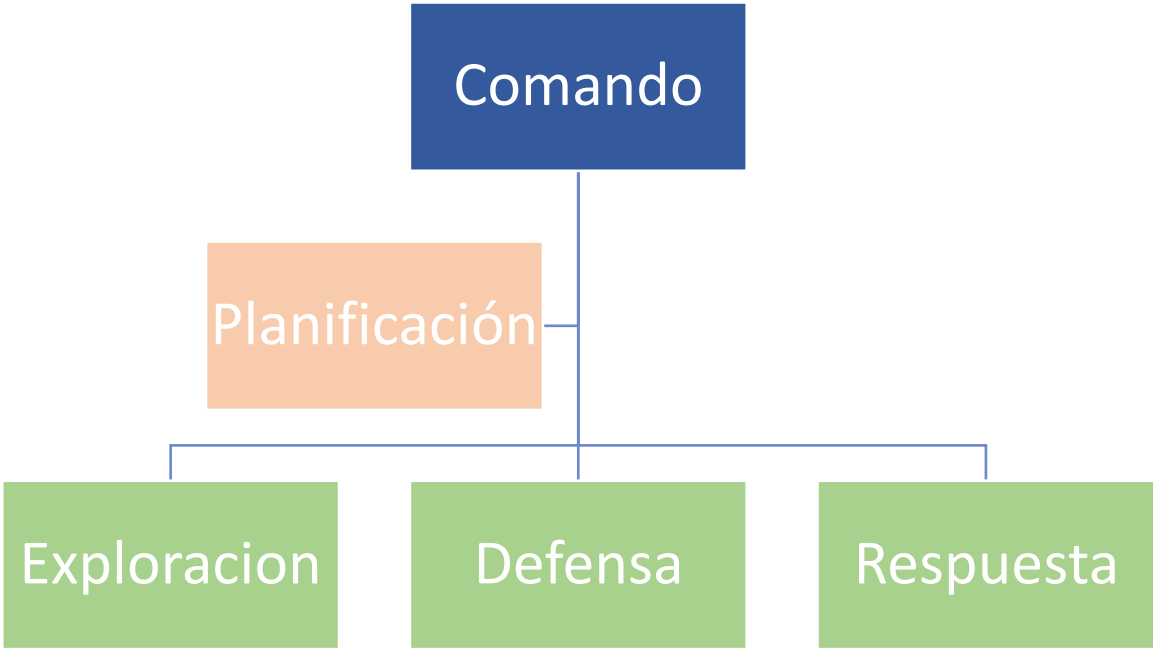

Figura 25. Organigrama Propuesto

Se debe entender que en el área de operaciones de ciberdefensa se debe considerar todos los pasos para tener una evolución hasta llegar a un centro de ciberdefensa, es decir cumplir con todas las funciones como son: Centro de administración de redes, un centro de seguridad de las operaciones y un equipo de respuesta a incidentes cibernéticos.

Dado que esta organización realiza operaciones militares, esta debe estar subordinada al Comando de Operaciones Navales por lo cual el Organigrama vigente de COOPNA debería ser modificado, tal y como se lo sugiere en la siguiente figura.

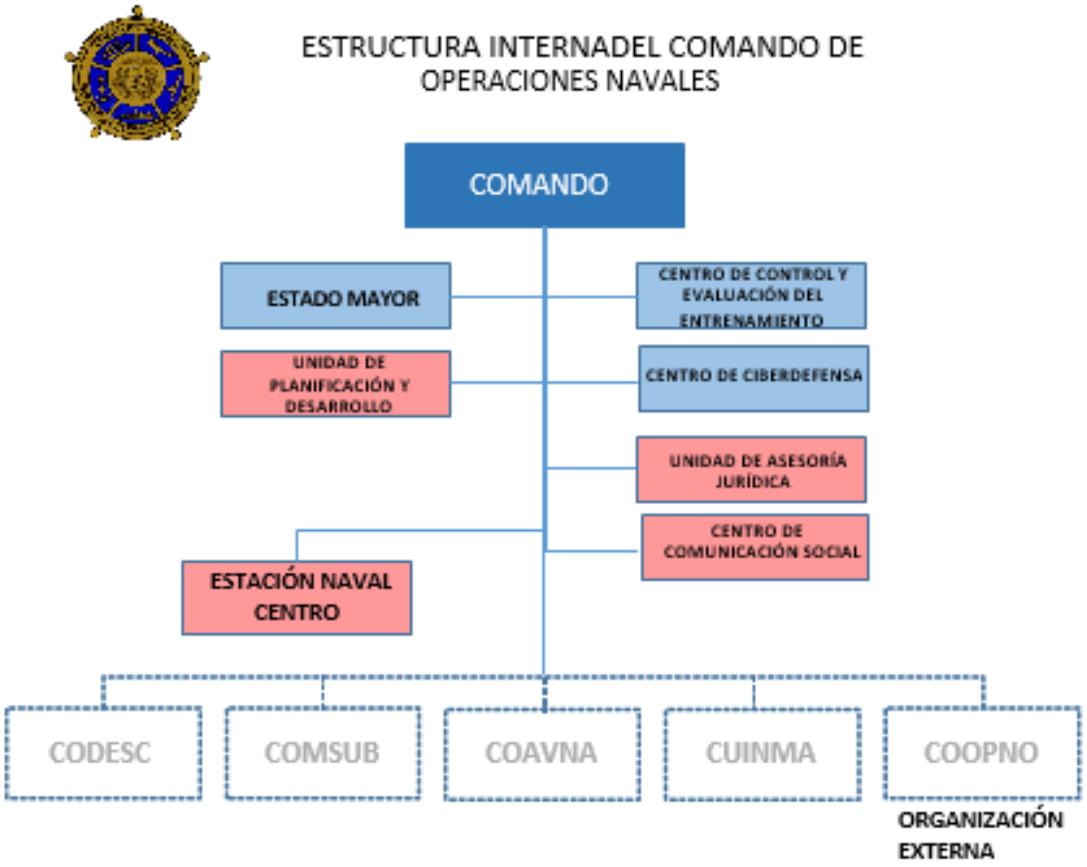

Figura 26. Organización modificada de COOPNA
Fuente: Autor basado en Manual de Organización COOPNA (Comando de Operaciones Navales, 2017)

5.3.4 Centro de Ciberdefensa

5.3.4.1 Función básica

Planificar, organizar, coordinar y conducir las operaciones de exploración, defensa y respuesta que garanticen la libertad de acción en el ciberespacio y nieguen el control del mismo a los adversarios a fin de contribuir a la conducción de las operaciones navales.

5.3.4.2 Responsabilidades

a. Dirigir las operaciones de ciberdefensa.

b. Asesorar al Comandante de operaciones navales en lo relacionado a las operaciones de ciberdefensa

c. Planificar, organizar, coordinar y conducir las operaciones de ciberdefensa que apoyen a las operaciones navales.

d. Coordinar con el Comando de Ciberdefensa la ejecución de los diferentes planes de ciberdefensa.

e. Planificar la búsqueda de información de cibertinteligencia

f. Planificar los de análisis de vulnerabilidades.

g. Supervisar la correcta ejecución del monitoreo de los sistemas.

h. Supervisar en coordinación con DIGEDO, la capacitación especializada del personal.

i. Planificar la sensibilización y concientización

j. Supervisar el cumplimiento de las novedades encontradas en las diferentes evaluaciones.

5.3.4.3 Cadena de Mando

Depende del Comandante de operaciones navales, informa al Jefe del Estado Mayor y coordina técnicamente con el Comando de Ciberdefensa.

5.3.5 Departamento de Exploración

5.3.5.1 Función básica

Recolectar información sobre las cibercapacidades de los sistemas de información y comunicaciones propias y del posible adversario a fin de contribuir a la conducción de las operaciones navales.

5.3.5.2 Responsabilidades

a. Ejecutar el plan de búsqueda de cibertinteligencia

b. Realizar el análisis y producción de cibertinteligencia.

c. Elaboración de informes de cibertinteligencia.

d. Recolección de información mediante identificación de señuelos y pruebas de penetración.

e. Realizar la Recolección de información mediante identificación de Señuelos y/ Test de Penetración.

f. Realizar análisis de vulnerabilidades

g. Elaborar informes para la toma de decisiones.

5.3.5.3 Cadena de Mando

Depende del Jefe del Centro de Ciberdefensa.

5.3.6 Departamento de Defensa

5.3.6.1 Función básica

Efectuar operaciones de Defensa en forma permanente en la infraestructura crítica digital de la Armada del Ecuador a fin de contribuir en la conducción de las operaciones navales.

5.3.6.2 Responsabilidades

a. Realizar concienciación y sensibilización

b. Realizar análisis de riesgos.

c. Realizar el monitoreo y control de los servicios.

d. Analizar los de incidentes.

e. Apoyar a la respuesta a incidentes.

f. Coordinar la respuesta a incidentes.

g. Realizar la remediación a incidentes in situ

h. Informar la respuesta a las vulnerabilidades.

i. Coordinar la respuesta a vulnerabilidades

j. Analizar los dispositivos o artefactos dentro de las redes.

k. Realizar la respuesta a dispositivos o artefactos.

l. Coordinar la respuesta a dispositivos o artefactos.

m. Detección de intrusiones o accesos no autorizados

n. Realizar análisis forenses

o. Realizar el hardering de la infraestructura.

p. Elaborar informes de monitoreo

q. Elaborar informes de análisis forenses

5.3.6.3 Cadena de Mando

Depende del Jefe del Centro de Ciberdefensa.

5.3.7 Departamento de Respuesta

5.3.7.1 Función básica

Ejecutar y mantener, medidas y acciones ofensivas de acuerdo a la necesidad operativa para neutralizar, interrumpir, alterar o destruir amenazas o ataques de potenciales adversarios a fin de contribuir a la conducción de las operaciones navales.

5.3.7.2 Responsabilidades

a. Ejecutar acciones de degradación, destrucción, explotación y limpieza

b. Realizar Investigación y Desarrollo de Ciberarmas.

c. Coordinar incremento de apreciaciones de Cibertinteligencia para objetivo establecido.

d. Analizar la el curso de acción más probable.

e. Definir el curso de Acción a seguir.

f. Elaborar informes de Respuesta.

g. Evaluar informes del Curso de Acción Ejecutado.

h. Ejecutar la actualización del Curso de Acción.

i. Desarrollar la doctrina de las operaciones de respuesta

5.3.7.3 Cadena de Mando

Depende del jefe del Centro de Ciberdefensa.

5.4 Orgánico

Una vez establecido los procesos que debe cumplir el Centro de Ciberdefensa y realizada la estructura orgánica, se va a proceder a levantar un orgánico provisional de esta nueva dependencia, considerando todas las actividades que debe cumplir la organización. El personal necesario esta descrito en la tabla No 13.

Se ha considerado que en los cuatro departamentos exista los Jefe departamentales quienes serán los responsables por que se cumplan las actividades de cada una de sus áreas. Así también se ha considerado personal de acuerdo a las actividades que den cumplir a las actividades de cada uno de los departamentos.

5.5 Formación

Dado que este es una especialidad nueva en el ámbito militar ecuatoriano, se debe tener un ciclo de formación que permita mantener en el tiempo este tipo de operaciones, para lo cual también se propone un ciclo de formación dividido en dos fases: básica y avanzada. Una capacitación especializada dependiendo del puesto que ocupe y una formación de acuerdo al rol que este ejerciendo, es decir para puestos técnicos, para funciones generalizadas y para funciones especializadas. En la siguiente figura se puede observar el proceso de formación que debería seguir el personal que preste sus servicios en esta área.

La operativización de esta propuesta está dada para que todo el personal que llegue a esta área y de acuerdo a su puesto reciba la formación generalizada, es decir: los cursos de básico de ciberdefensa, seguridad de las TIC y asesor en Ciberdefensa.

En caso del personal técnico ellos deberán los cursos de avanzado de ciberdefensa y administrador de seguridad. Este personal dependiendo de su puesto podrá seguir los siguientes cursos: Experto en malware, auditoria de seguridad, gestión de incidentes, monitorización de redes y análisis forense.

Tabla 13
Orgánico propuesto

	CENTRO DE CIBERDEFENSA		
	JEFATURA		
1			COMANDANTE DEL CENTRO DE CIBERDEFENSA
2			AMANUENSE
	UNIDAD DE PLANIFICACION		
3			JEFE DE UNIDAD DE PLANIFICACION
4			ANALISTA DE CIBERDEFENSA
	DEPARTAMENTO DE OPERACIONES DE EXPLORACION		
5			JEFE DEL DEPARTAMENTO
6			SUPERVISOR DE INFORMACION
7	E	14	ANALISTA DE INFORMACION
8			ANALISTA DE INFORMACION
9			ANALISTA DE CIBERDEFENSA
10			ANALISTA DE CIBERDEFENSA
11	E	15	ANALISTA DE CIBERDEFENSA
	DEPARTAMENTO DE OPERACIONES DE DEFENSA		
12			JEFE DEL DEPARTAMENTO
	DIVISION PROTECCION		
13			SUPERVISOR DE SEGURIDAD
14			ANALISTA DE CIBERDEFENSA
15			ANALISTA DE CIBERDEFENSA
16			ANALISTA DE CIBERDEFENSA
17			ANALISTA DE CIBERDEFENSA
18			ANALISTA DE CIBERDEFENSA
19			ANALISTA DE CIBERDEFENSA
20			TECNICO DE CIBERDEFENSA
21			TECNICO DE CIBERDEFENSA
22			TECNICO DE CIBERDEFENSA
23			TECNICO DE CIBERDEFENSA
24			TECNICO DE CIBERDEFENSA
	DIVISION FORENSE		
25			ANALISTA DE CIBERDEFENSA
26			TECNICO DE CIBERDEFENSA
	DEPARTAMENTO DE OPERACIONES DE RESPUESTA		
27			JEFE DEL DEPARTAMENTO
28			ANALISTA DE CIBERDEFENSA
29			ANALISTA DE CIBERDEFENSA
30	E	15	ANALISTA DE CIBERDEFENSA

Finalmente existen dos cursos para personal especialista que deben ser desarrollados de acuerdo a su perfil y ocupación dentro del centro: curso de cibertinteligencia y asesor legal en ciberdefensa.

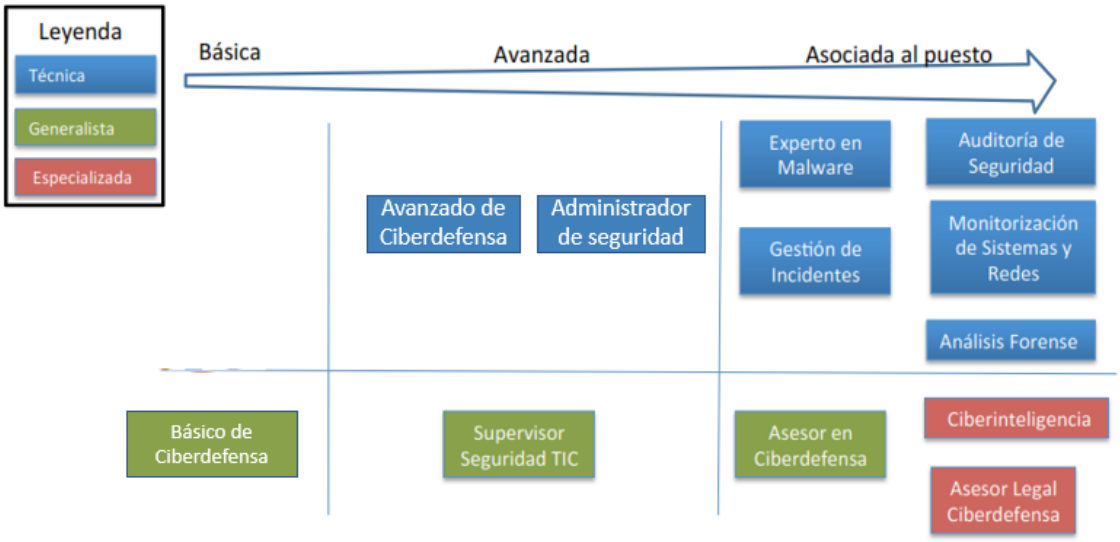

Figura 27. Proceso de formación del personal que integre el centro
Fuente: (Ministerio de Defensa España, 2015)

Dado que este personal debe estar en constante entrenamiento y capacitación dada cambio periódico de la tecnología producto del rápido avance tecnológico, se pone en consideración los cursos o certificaciones a los cuales personal de este centro debería realizarlo. En la siguiente figura se muestra el cuadro de capacitaciones según el nivel de conocimiento.

PLAN DE CAPACITACIÓN

CAPACITACIÓN BASICA

1	Curso básico de Ciberdefensa.
1	LPIC-1 (Linux Beginners)
2	Seguridad de la Información, Normas ISO 27000.
2	Curso básico de Hacking Ético
3	Curso básico de Inteligencia orientado a la Ciberdefensa.

CURSOS A CORTO PLAZO
CURSOS A MEDIANO PLAZO
CURSOS A LARGO LAZO

CAPACITACIÓN ESPECIALIZADA

DEFENSA	1	Transit 1
	1	Curso de Oficial de seguridad de la Información OSI.
	2	Fundamentos de Criptografía
	2	CISSP
	3	Curso de DDoS, Detección y Correlación.
	3	Seguridad en Sistemas de Control y Scada
	3	Computer Hacking Forensic Investigator CHFI
EXPLORACIÓN	1	CEH
	1	Curso de Ciber-Inteligencia.
	1	Curso de Social Media Business.
	1	Curso de obtención de inteligencia de fuentes abiertas (OSINT)
	2	Penetration Testing with Kali Linux (PWK)
	2	Curso de Ingeniería Inversa
	2	Wireless Security Expert (OWSE)
	2	CERTIFIED Trust Analyst (CTA)
	3	Profesional Security Tester (OPST)
	3	Profesional Security Analyst (OPSA)
	3	Proffesional Security Expert (OPSE)
RESPUESTA	1	CEH
	1	Hacking en Smartphones y otros dispositivos
	1	Penetration Testing with Kali Linux (PWK)
	2	APTs Ataques dirigidos
	2	Offensive Security Wireless Attacks (WIFO)
	2	Cracking the perimeter (CTP)
	2	Offensive Security Certified Professional (OSCP)
	3	Exploitation Expert (OSWE)
	3	Proffesional Security Expert (OPSE)

CAPACITACIÓN GERENCIAL

1	Programa de Nivelación o estandarización de conocimientos.
1	Ciberdefensa (procesos y servicios)
1	Infraestructuras Críticas Digitales.
1	Ingles B1
2	Planificación de las capacidades de Ciberdefensa
2	Gestión de servicios de TI (ISO/IEC 20000)
2	Gestión de Riesgos
2	BCP Continuidad del Negocio ISO 22301.
3	Legislación en Ciberseguridad y Ciberdefensa
3	Planificación y ejecución de operaciones de Ciberdefensa

Figura 28. Plan de capacitación

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones.

a. El desarrollo y uso de la tecnología ha generado una dependencia en las actividades operativas y su falta de protección facilita para que un agente externo pueda interferir en la conducción de las operaciones navales.

b. Las operaciones de ciberdefensa en la Armada del Ecuador se encuentran en un nivel de madurez inicial lo que ha limitado su aporte a la conducción de las operaciones navales.

c. El desarrollo de las operaciones de exploración, defensa y respuesta en la Armada del Ecuador, facilitará el acceso y control del ciberespacio, así como la negación del mismo al adversario.

d. La implementación de un centro de ciberdefensa en la Armada del Ecuador facilitará el desarrollo de las operaciones de ciberdefensa y una continuidad en las mismas, de tal forma que sean un apoyo a la conducción de las operaciones navales.

e. Existe todavía un vacío técnico y legal dentro de la Institución y del país en general que limita la ejecución de las operaciones de ciberdefensa con las respectivas garantías jurídicas.

6.2 Recomendaciones.

a. Poner en consideración del Comando de Operaciones Navales la revisión de la propuesta de un Centro de Ciberdefensa con su respectiva estructura orgánica, a fin de que sea analizado junto con sus asesores para su respectiva implementación.

b. Efectuar operaciones de ciberdefensa en conjunto con las operaciones navales, a fin de asegurar la disponibilidad, confiabilidad e integridad de los sistemas de Mando y Control durante las operaciones.

c. Se debe realizar un plan de capacitación para el personal que integre el centro con el objetivo de que se puedan desempeñar de una manera apropiada en las diferentes actividades.

d. Luego de un determinado tiempo se debe realizar un análisis de la situación actual, fin determinar cómo ha contribuido el centro de ciberdefensa en las operaciones navales.

BIBLIOGRAFÍA

Agencia Telam. (20 de febrero de 2018). *La Nacion*. Obtenido de https://www.lanacion.com.ar/2110654-la-onu-pide-reglas-globales-para-minimizar-el-impacto-de-las-ciberguerras

Air force. (2011). *Cyberspace Operations.*

Armada del Ecuador. (2014). *Concepto Estrategico - Directrices - Doctrina.* Quito.

Avast. (11 de octubre de 2018). *Gusano Informatico*. Obtenido de https://www.avast.com/es-es/c-computer-worm

Banco Interamericano de desarrollo. (2016). *Informe de Ciberseguridad 2016.*

Campus Internacional para la Seguridad y la Defensa. (08 de agosto de 2016). *La amenaza cibernética: ciberguerra y ciberdefensa*. Obtenido de https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

Cano, J. (2013). Ciberseguridad y Ciberdefensa: dos tendencias emergentes en un contexto global. Obtenido de 52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

Centro de Innovacion y soluciones empresariales y tecnologicas. (4 de octubre de 2018). *Spyware - Programa Espia*. Obtenido de https://www.ciset.es/glosario/488-spyware

Comando Conjunto Cibernetico. (03 de noviembre de 2018). *Comando Conjunto Cibernetico*. Obtenido de https://www.ccoc.mil.co/quienes_somos/organigrama

Comando Conjunto de las Fuerzas Armadas. (2017). *Implementación d ela Capacidad de Ciberdefensa.* Quito.

Comando de Ciberdefensa. (11 de noviembre de 2018). *Situación actual de la Ciberdefensa en el Ecuador.* Obtenido de http://media.arpel2011.clk.com.uy/ciber/20.pdf

Comando de Operaciones Navales. (2017). Manual de Organización. Guayaquil, Guayas, Ecuador.

Commander Navy Cyber Forces. (2014). *Commander's Cybersecurity Handbook.*

Community Latam. (11 de noviembre de 2018). *Problematica actual de la ciberdefensa*. Obtenido de https://www.cxo-community.com/2018/07/problematica-actual-de-la-ciberdefensa.html

Cooperative Cyber Defence Centre of Excellence. (10 de octubre de 2018). *Cyber Definition*. Obtenido de https://ccdcoe.org/cyber-definitions.html

Defensa, C. S. (2012). *El ciberespacio nuevo escenario de confrontación.* España.

Deibert, R. J., Palfrey, J. G., Rahozinski, R., & Zittrain, J. (20 de septiembre de 2011). *Access Contested: Security, Identity and resistence in Asian Cyberspace.* MIT. Obtenido de http://www.crysys.hu/skywiper/skywi

Departament of Defense. (2012). *Dictionary of Military and Associated Terms.*

Departement of Defense. (2018). *Cyber Strategy.* Washington.

Diaz del Rio Duran, J. J. (2011). *La ciberseguridad en el ámbito militar.* Madrid.

DigitalGuardian. (11 de noviembre de 2018). *www.digitalguardian.com*. Obtenido de https://digitalguardian.com/blog/what-security-operations-center-soc

Ejercito de los Estados Unidos. (2010). *Cybersapce Operations Concept Capability Plan 2016-2018.* USA.

Ernst & Young, S.L. (2017). *Global Information Security Survey 2017-2018.* Atlanta: BMC Agency.

Fireeye. (11 de noviembre de 2018). *SlideChare.* Obtenido de https://www.slideshare.net/primeinfoserv/fireeye-solutions

Gabinete Sectorial de Seguridad. (2019). *Plan Nacional de Seguridad Integral 2019-2030.* Quito.

Gartner. (11 de noviembre de 2018). *IT Closary*. Obtenido de https://www.gartner.com/it-glossary/cirt-cyber-incident-response-team

Gazula, M. B. (2017). *Cyber Warfare conflict Anaysis and Case Studies.* Cambridge: Masachusetts Institute of Technology.

Grupo EDEFA. (12 de noviembre de 2018). *Defensa*. Obtenido de https://www.defensa.com/chile/chile-brasil-firman-acuerdo-sobre-ciberdefensa

Grupo EDEFA. (13 de noviembre de 2018). *Defensa*. Obtenido de https://www.defensa.com/chile/chile-ee-uu-firman-acuerdo-cooperacion-ciberdefensa

GSM. (05 de octubre de 2018). *Que es ingenieria social?* Obtenido de https://gmsseguridad.com/ing-social-info.html

Instituto Espanol de Estudios Estrategicos. (02 de agosto de 2016). La cumbre de la OTAN en Varsovia. España. Obtenido de http://www.ieee.es/en/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf

Joint Chiefs of Staff. (08 de junio de 2018). Cyberspace Operations. Estados Unidos.

Kapersky. (2017). *Kapersky Lab Theat predictions for 2018.* Recuperado el 02 de septiembre de 2018, de https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf

Kapersky. (18 de noviembre de 2018). *Ciberamenza mapa en tiempo real*. Obtenido de https://cybermap.kaspersky.com/es

Kapersky. (11 de octubre de 2018). *Kapersky*. Obtenido de https://www.kaspersky.es/resource-center/threats/trojans

Kapersky. (05 de octubre de 2018). *Ransomware*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

Lewis, J. A. (2009). *The Korean Cyber Attacks and their Inplications for Cyber Conflict.* Washington: Center for Strategic and Internatinal Studies.

Mando Conjunto de Ciberdefensa. (12 de noviembre de 2018). Operaciones Militares en el Ciberespacio.

Marina de los Estados Unidos. (02 de noviembre de 2018). *Naval Network Warfare Command*. Obtenido de https://www.public.navy.mil/fltfor/nnwc/Pages/default.aspx

Marina de los Estados Unidos. (02 de noviembre de 2018). *Navy Cyber Defense Command*. Obtenido de https://www.public.navy.mil/fltfor/ncdoc/Pages/default.aspx

Marina de los Estados Unidos. (02 de noviembre de 2018). *Navy Cyber Warfare Development Group*. Obtenido de https://www.public.navy.mil/fltfor/NCWDG/Pages/default.aspx

Marina de los Estados Unidos. (02 de noviembre de 2018). *Navy Information Operations Command*. Obtenido de https://www.public.navy.mil/FLTFOR/iwtgnorfolk/Pages/NIOCNorfolkHistory.aspx

Medina, M., & Martinez, M. (Junio de 2011). Computación forense. Nicaragua.

Miisterio de Defensa Nacional. (12 de septiembre de 2014). Acuerso Ministerial 281. Quito, Ecuador.

Ministerio de Defensa España. (2015). *Plan de formación en Ciberdefensa.* Madrid.

Ministerio de Defensa Nacional. (2019). *Plan Especifico de la Defensa.* Quito: Ministerio de Defensa Nacional.

National Cyber Security Authority. (2017). *Cyber Defense Methodology.*

Operaciones militares ciberneticas. (2017). Buenos aires: Vision Conjunta.

Polanco Marcos. (05 de julio de 2015). *Magazcitum*. Obtenido de http://www.magazcitum.com.mx/?p=3034

Realpe, M. (29 de Noviembre de 2017). La Ciberdefensa en Colombia. Bogota.

Rivero Marcelo. (01 de octubre de 2016). *Infospyware*. Obtenido de https://www.infospyware.com/articulos/que-son-los-malwares/

Ruben, R. (20 de enero de 2018). *25 Tipos de ataques informáticos y como prevenirlos*. Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Seguridad de la Información. (2011). *Phishing*. Obtenido de https://www.segu-info.com.ar/malware/phishing.htm

Techopedia. (11 de noviembre de 2018). *Techopedia*. Obtenido de https://www.techopedia.com/definition/5377/network-operations-center-noc

TechTarget. (noviembre de 2012). *Ataque de denegación de servicios*. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

TeleGeography. (05 de noviembre de 2018). *Submarine Cable map*. Obtenido de https://www.submarinecablemap.com/

Union Europea. (20 de junio de 2018). *Union Europea*. Obtenido de https://eeas.europa.eu/headquarters/headquarters-Homepage/40881/cooperaci%C3%B3n-ue-otan-factsheet_es

Vankka, J. (2013). *Cyber Warfare.* Helsinki: National Defense University.

Worls Economic Forum. (2018). *The Global Risks Report 2018.* Geneva.