“El manejo de la ciberdefensa en la conducción de operaciones terrestres frente a una crisis”

Bonilla Guerrero, Jaime Iván y Guerrero Padilla, Oswaldo Alexander

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Defensa y Seguridad

¨Trabajo de titulación previo a la obtención del título de Magister en Defensa y Seguridad mención Estrategia Militar¨

Ing. Álvarez Vergara, Jorge Hugo

15 de diciembre de 2020

URKUND

Document Information

Analyzed document	TESIS Bonilla-Guerrero.docx (D87634147)
Submitted	12/3/2020 12:58:00 AM
Submitted by	
Submitter email	alexsolo93@hotmail.com
Similarity	8%
Analysis address	waaltamirano.espe@analysis.urkund.com

Sources included in the report

SA	**Universidad de las Fuerzas Armadas ESPE / Tesis Mayor Jerez Carlos CIBERDEFENSA 22 ABRIL 16H00.docx** Document Tesis Mayor Jerez Carlos CIBERDEFENSA 22 ABRIL 16H00.docx (D51063130) Submitted by: navaca4@espe.edu.ec Receiver: navaca4.espe@analysis.urkund.com	5
SA	**Universidad de las Fuerzas Armadas ESPE / Operaciones Ciberdefensa v1.4.docx** Document Operaciones Ciberdefensa v1.4.docx (D58456656) Submitted by: alexpaultapia@gmail.com Receiver: aamacias1.espe@analysis.urkund.com	10
W	URL: https://es.globalvoices.org/2015/05/09/venezuela-crea-la-direccion-conjunta-de-cib ... Fetched: 12/3/2020 12:59:00 AM	1
SA	**Universidad de las Fuerzas Armadas ESPE / TESIS FINAL AMPUDIA - TAPIA.docx** Document TESIS FINAL AMPUDIA - TAPIA.docx (D50470311) Submitted by: llrecalde@espe.edu.ec Receiver: llrecalde.espe@analysis.urkund.com	4
SA	**Universidad de las Fuerzas Armadas ESPE / Edwin Castro BL.docx** Document Edwin Castro BL.docx (D13416567) Submitted by: meescobar@espe.edu.ec Receiver: meescobar.espe@analysis.urkund.com	1

TCRN. (SP) JORGE HUGO ÁLVAREZ VERGARA

DIRECTOR

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**El manejo de la ciberdefensa en la conducción de operaciones terrestres frente a una crisis**", fue realizado por los señores **Tcrn. de E.M Bonilla Guerrero Jaime Iván y Tcrn. de E.M Guerrero Padilla Oswaldo Alexander** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustenten públicamente.

Sangolquí, 14 de diciembre de 2020

TCRN. (SP) ÁLVAREZ VERGARA JORGE HUGO

C.C.: 1708968878

DIRECTOR DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Nosotros **Tcrn. de E.M Bonilla Guerrero Jaime Iván, Tcrn. de E.M Guerrero Padilla Oswaldo Alexander** con cédulas de ciudadanía N° 0201400801 y N° 1710330885, declaramos que el contenido, ideas y criterios de trabajo de titulación: **"El manejo de la ciberdefensa en la conducción de operaciones terrestres frente a una crisis"**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 14 de diciembre de 2020

Tcrn. de E.M Bonilla G. Jaime I.

C.C.: 0201400801

Tcrn. de E.M Guerrero P. Oswaldo A.

C.C.: 1710330885

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros **Tcrn. de E.M Bonilla Guerrero Jaime Iván, Tcrn. de E.M Guerrero Padilla Oswaldo Alexander** con cédulas de ciudadanía No 0201400801 y No 1710330885, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"El manejo de la ciberdefensa en la conducción de operaciones terrestres frente a una crisis"**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 14 de diciembre de 2020

Tcrn. de E.M Bonilla Guerrero Jaime I.
C.C.: 0201400801

Tcrn. de E.M Guerrero Padilla Oswaldo A.
C.C.: 1710330885

Dedicatoria

TCRN. DE E.M IVÁN BONILLA

Este trabajo va dedicado, a mi esposa Alejandra y mis hijas Doménica e Ivonne, quienes llenan de luz mi existencia y son la motivación y razón para seguir adelante tanto en el plano familiar como profesional, un agradecimiento a mi madre Albita y a mí tía Rocío, quienes siempre han sido un ejemplo de profesionalismo y abnegación y quienes me han inculcado valores y principios de vida, finalmente mi agradecimiento a Dios, por ser el pilar que soporta y guía mi vida.

TCRN. DE E.M ALEX GUERRERO

Este trabajo está dedicado a Dios que siempre ha estado presente en mi vida con cada una de sus demostraciones, a mis hermosas hijas Daniela, Cristina y Melany Sofía que constituyen la pureza y alegría del día a día en esta maravillosa vida, a mis amados padres fortaleza, amor y cimiento familiar, a mis hermanas, amigos y familiares que me han apoyado con su compañía, cariño y sinceridad.

Agradecimiento

TCRN. DE E.M IVÁN BONILLA

Mi agradecimiento, primero a Dios, creador y dador de vida, a mi esposa Alejandra y mis hijas Doménica e Ivonne, quienes llenan de felicidad de vida y me impulsan a seguir adelante tanto en el plano familiar como profesional, finalmente agradezco a mi madre y a mí tía, con su ejemplo y esfuerzo me han dado las herramientas, para triunfar en esta vida.

TCRN. DE E.M ALEX GUERRERO

Mi agradecimiento al glorioso Ejército, institución del cual soy orgullosamente parte, misma que ha permitido capacitarnos durante nuestra carrera profesional y a la vez ha sido cobijo de nuestro desarrollo personal y familiar, a nuestros instructores, profesores y director del presente trabajo, que con su guía y conocimiento han sabido dirigir y hacernos culminar con este proyecto.

Índice

Índice de tablas

Índice de figuras

Resumen

El crecimiento acelerado de la tecnología, la proliferación de la informática en todas las instituciones del Estado, empresas, banca, industrias, ámbito militar, grupos sociales, población en general; han dado origen al surgimiento de un nuevo dominio (escenario) a nivel mundial denominado el ciberespacio; y con este han surgido múltiples amenazas que han conllevado a la violación de medidas de seguridad informática con el fin de obtener información de inteligencia gubernamental, militar, industrial, económica, científica, ataques a infraestructuras críticas, páginas web, uso de redes sociales como WhatsApp, Telegram para influir en la población y causar caos interno.

Conscientes de la complejidad de este dominio especial y transversal al resto de dominios conocidos, el alto volumen de ciberamenazas y factores de riesgo que deben ser enfrentados, eliminados o reducidos, tanto en el ámbito interno como externo en el ciberespacio y que atentan contra la Soberanía e Integridad Territorial y Seguridad Interna, hacen necesario que el Ejército integre dentro de su organización las políticas y estrategias para la defensa y protección de este nuevo dominio, en concordancia con las adoptadas por el Ministerio de Defensa y el Comando Conjunto de las Fuerzas Armadas.

Palabras clave:

- **CIBERESPACIO**
- **CIBERDEFENSA**
- **OPERACIONES DE DEFENSA, EXPLORACIÓN Y RESPUESTA**

Abstract

The accelerated growth of technology, the proliferation of information technology in all State institutions, companies, banks, industries, the military, social groups, the general population; They have given rise to the emergence of a new domain (scenario) at the world level called cyberspace; And with this, multiple threats have emerged that have led to the violation of computer security measures in order to obtain government, military, industrial, economic, scientific intelligence information, attacks on critical infrastructures, web pages, use of social networks such as WhatsApp , Telegram to influence the population and cause internal chaos.

Aware of the complexity of this special domain and transversal to the rest of known domains, the high volume of cyber threats and risk factors that must be faced, eliminated or reduced, both internally and externally in cyberspace and that threaten Sovereignty and Territorial Integrity and Internal Security, make it necessary for the Army to integrate within its organization the policies and strategies for the defense and protection of this new domain, in accordance with those adopted by the Ministry of Defense and the Joint Command of the Armed Forces.

Keywords:

- **CYBERSPACE**
- **CYBER DEFENSE**
- **DEFENSE OPERATIONS, EXPLORATION AND RESPONSE**

Capítulo I

El problema

Planteamiento del problema

La conducción de las Operaciones Terrestres de Respuesta a Crisis, se ve afectada debido a varios factores, entre otros:

- La inexistencia de políticas sobre este tema en la Fuerza Terrestre (F.T).
- La falta de un organismo de Ciberdefensa que apoye las operaciones de Respuesta a Crisis en la Fuerza Terrestre.
- Que amenazas cibernéticas afectan la conducción de operaciones de Respuesta a Crisis por parte de la Fuerza Terrestre en apoyo a la Policía Nacional.

Por lo que es necesario analizar estos factores para determinar cuáles serían las soluciones a ser adoptadas para mejorar la conducción de este tipo de operaciones, cuando se ejecuten.

En la actualidad la Fuerza Terrestre no dispone de ningún componente de Ciberdefensa que proporcione el apoyo requerido para lograr una mejor conducción de las operaciones terrestres de respuesta a crisis.

El Ministerio de Defensa Nacional (MIDENA) mediante Acuerdo Ministerial No 281 crea el Sistema de Ciberdefensa del Ministerio de Defensa Nacional para articular las instancias permanentes que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional, organismo que hasta la presenta fecha no ha sido conformado, paralelamente se crea el Comando de Ciberdefensa del Comando Conjunto (año 2014), y se diseña el Proyecto de ¨Implementación de la Capacidad de Ciberdefensa en FF.AA¨, que hasta la presente fecha se ha implementado apenas en un 2 %. (Comando de Ciberdefensa, 2019)

Las operaciones de Ciberdefensa han adquirido una gran importancia dentro de la conducción militar, por lo que es necesario contar con esta capacidad para aplicarla en apoyo a las operaciones militares de respuesta a crisis, desde el punto de vista legal, técnico y organizacional.

Formulación del problema

La ausencia de un órgano asesor en Ciberdefensa para la Fuerza Terrestre, incide negativamente en la conducción de las operaciones de respuesta a crisis en apoyo a la Policía Nacional (P.N) ante grave conmoción interna.

Preguntas de investigación

¿Qué marco legal establece la protección del ciberespacio y permite la ejecución de operaciones militares de Ciberdefensa?

¿Qué amenazas cibernéticas, afectarían la conducción de las Operaciones de Respuesta a Crisis en apoyo a la Policía Nacional ante grave conmoción interna?

¿Es necesaria la creación de un organismo asesor en Ciberdefensa para apoyar la planificación y conducción de las operaciones de Respuesta a Crisis en apoyo a la P.N?

Objeto de estudio

Creación de un órgano de asesoramiento de Ciberdefensa en la Fuerza Terrestre, para apoyar la conducción de las operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna.

Campo de acción

El presente estudio se realizará en la Fuerza Terrestre, considerando a la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), Dirección de Inteligencia y Dirección de Comunicación Social de la .Fuerza Terrestre en la parte técnica; al Comando del C.O 4 “CENTRAL”, C.E.M.A 71 y C.E.M.S 38 en la parte operativa, y como ente de asesoramiento al Comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas (COMACO).

Delimitación de la investigación

La presente investigación abarca el ámbito de la Ciberdefensa y las operaciones terrestres de respuesta a crisis en Apoyo a la Policía Nacional ante grave conmoción interna, la misma que se realizará en la Provincia de Pichincha, Distrito Metropolitano de Quito y cantón Sangolquí, jurisdicción donde se encuentran acantonadas las unidades que se consideraron en el campo de acción, considerando el período de enero a diciembre de 2019.

Justificación e importancia

La complejidad y alto volumen de ciberamenazas y factores de riesgo que deben ser enfrentados, eliminados o reducidos, tanto en el ámbito interno como externo en el ciberespacio y que atentan contra la Soberanía e Integridad Territorial y Seguridad Interna, hacen necesario que el Ejército integre dentro de su organización las políticas y estrategias para la defensa y protección de este nuevo dominio adoptadas por el MIDENA y COMACO.

(VARGAS, 2014), refiere que el impacto de las ciberamenazas, no solo causaría afectaciones que pondrían a prueba a los mandos militares si no que se verían involucradas las instituciones del estado, instituciones privadas como

la banca, empresas proveedoras de servicios públicos tales como energía eléctrica, agua telefonía, terminales aéreos, terrestres, marítimos, registro civil, hidrocarburos, entre otros, por lo que la demanda involucra a gran parte de la población y sus instituciones, razón por lo cual la seguridad y defensa del ciberespacio tiene implicaciones civiles, militares, económicas, políticas; de aquí la relevancia e importancia del tema en estudio, el cual abarcará la situación actual de la Ciberdefensa en la Fuerza Terrestre, presentando un panorama de la Ciberdefensa a nivel regional y mundial y que componentes técnicos u organización debería tener la Fuerza Terrestre para enfrentar estos nuevos desafíos, proponiendo estrategias de Ciberdefensa que apoyen a la conducción de operaciones de respuesta a crisis, que permitan generar doctrina y constituyan un apoyo para la conducción de operaciones terrestres, lo que permitirá al mando tomar decisiones oportunas y adecuadas durante la conducción de este tipo de operaciones; además, se cuenta con datos estadísticos que engloban ciberamenazas y ciberataques a nivel mundial, regional y nacional, lo que permitirá profundizar en nuestro problema de investigación.

Objetivos de la investigación

Objetivo General

Proponer la creación de un órgano asesor de Ciberdefensa en la Fuerza Terrestre, como estrategia, para apoyar la conducción de operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna.

Objetivos Específicos

Describir el marco legal que establece la protección del ciberespacio y su aplicabilidad en el ámbito de las operaciones militares de Ciberdefensa.

Determinar que amenazas cibernéticas, afectarían la conducción de las Operaciones de Respuesta a Crisis en apoyo a la P.N ante grave conmoción interna.

Demostrar la necesidad de crear un Órgano Asesor de Ciberdefensa en la Fuerza Terrestre, para apoyar la planificación y conducción de las operaciones en los niveles operativo y táctico.

Capítulo II

Marco teórico

Antecedentes de la investigación

Los ataques informáticos han crecido exponencialmente y cada día van en aumento, es así que según expertos internacionales a nivel mundial se realizan cerca de ocho millones de ataques informáticos por día; en la mayoría de los casos (casi el 80%) estuvo relacionada con la apropiación indebida de datos mediante técnicas como el skimming (clonación de tarjetas), el phishing y la explotación de sistemas de pago en línea. La Policía Nacional informa que, en la segunda mitad del 2015, el país experimentó un aumento importante en la cantidad de incidentes de fraude electrónico, en los que el público general fue el grupo más afectado con el 58,94% de todos los incidentes denunciados. Los ciudadanos también fueron víctimas de otro rango de actividades y delitos que involucran el uso de las TICS, como homicidios, esquemas piramidales, extorsiones, interceptaciones de comunicaciones y accesos no autorizados a sistemas de información. Las entidades del sector bancario son otro de los grupos más importantes en donde se detectaron incidentes, según los datos de la Policía Nacional, con un 38,48%, el 2,58% de las denuncias recibidas fueron por delitos que tenían que ver con ataques a niños y menores, como la pornografía, grooming (captación de menores con fines sexuales), acoso sexual y ciber-bullying. (SYMANTEC, 2019)

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 crítica, causar daño a las vidas humanas y minar las capacidades de defensa". Mato (2018)

El MIDENA mediante Acuerdo Ministerial No 281 Acuerda en su Artículo 1.- Crear el Sistema de Ciberdefensa del Ministerio de Defensa Nacional como el mecanismo que articula las instancias permanentes y de conformación que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional, a fin de coordinar e implementar políticas y estrategias de Ciberdefensa, organismo que hasta la presenta fecha no ha sido conformado y por consiguiente no se cuenta con una Estrategia Nacional de Ciberdefensa, que resguarde las diferentes operaciones para la defensa del ciberespacio. (Jerez, 2019)

Paralelamente en el 2014, se crea el Comando de Ciberdefensa del Comando Conjunto y se diseña el Proyecto de ¨Implementación de la Capacidad de Ciberdefensa en FF. AA¨, el mismo que cuenta con dictamen de prioridad desde el año 2015, emitido por la Secretaría Nacional de Planificación y Desarrollo (SENPLADES), hasta la presente fecha su ejecución ha sido del 2 %. (Comando de Ciberdefensa, 2019)

El COMACO, específicamente el Comando de Ciberdefensa dispone de información estadística de relevancia que corresponde a diferentes ciberataques que se han producido a nivel mundial, regional, nacional y que han afectado a infraestructuras críticas, bases de datos, información confidencial, sistemas de mando y control, páginas web institucionales; que son insumos importantes para el presente tema de estudio y constituyen información reservada.

El pasado mes octubre de 2019 en nuestro país, se produjo un hecho que genero una grave conmoción interna y mediante decreto ejecutivo N° 884 de fecha 03 de octubre de 2019, las FF.AA y específicamente la Fuerza Terrestre realizó operaciones de Respuesta a Crisis en apoyo a la P.N, sin embargo se enfrentó una amenaza que generó un escenario VICA (volátil, incierto, complejo y ambiguo) donde la gran cantidad de información falsa que se difundió a través del ciberespacio, alentó a la población en general a realizar acciones violentas que no fueron contempladas en la planificación de las unidades militares; dejando al descubierto la necesidad de contar con un órgano de Ciberdefensa que pueda asesorar y apoyar a los diferentes niveles, en la toma de decisiones y conducción de las operaciones para neutralizar y/o minimizar los efectos de esta malintencionada información.

Es así que la Ciberdefensa debe cumplir con un rol preponderante e involucrar al ciberespacio como un nuevo teatro acorde a la misión fundamental de la ¨Defensa de la Soberanía e Integridad Territorial¨ (Asamblea Nacional del Ecuador, 2008), así como en las operaciones de apoyo a otras instituciones contempladas en la Agenda Política de la Defensa, específicamente en las operaciones de respuesta a crisis (estado de excepción) en apoyo a la Policía Nacional.

Fundamentación teórica

Fundamentación general

Los ciber conflictos son una realidad latente es así que se han producido algunas acciones bélicas en el ciberespacio y alrededor de todo el planeta; derivados de un sinnúmero de amenazas y riesgos existentes; para enfrentarlas aparece 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". (TAPIA, 2018, pág. 24); la Ciberdefensa, engloba infinidad de terminología que debe ser abordada en la investigación como el ciberespacio, la ciberseguridad, ciberdefensa, infraestructuras críticas, ciberamenazas, ciberespionaje, ciberguerra, entre otros.

El ciberespacio es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan. (JEREZ, 2019, pág. 13)

Clarke & Knake, proponen: "el ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet". Es importante dejar en claro una diferencia: "Internet es una red de redes abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador conectado con cualquiera otra de las redes de internet". (Ampudia & Tapia, 2017, pág. 41)

Vicente Llongueras, realiza un análisis sobre lo que el ciberespacio representa para la seguridad nacional de un Estado: el ciberespacio es un elemento de poder dentro la seguridad nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI (LLongueras Vicente, 2013, pág. 42) , en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias forjándose y desarrollándose el concepto de las operaciones militares centradas en redes. (LLongueras Vicente, 2013, pág. 42)

Los países desarrollados y que lideran los avances tecnológicos, lo han considerado el quinto dominio y como tal posee tres capas: la capa física con sus componentes geoFiguras 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. (TAPIA, 2018, pág. 21)

Para el Centro Superior de Estudios de la Defensa Nacional de España CEDESEN, la Ciberdefensa es “la aplicación de medidas de seguridad para proteger el ciberespacio de un ciberataque, para lo cual posee tres capacidades: defensa, explotación y respuesta”. (TAPIA, 2018)

(LLongueras Vicente, La Ciberguerra; la guerra inexistente, 2013, pág. 26), refiere que: La Ciberseguridad no es exclusivamente un problema militar, aunque los conceptos y el lenguaje utilizado en este ámbito son igualmente una derivación de los conceptos utilizados tradicionalmente en el ejército: amenaza, agresión, ataque, defensa, son los términos más utilizados. Pero la ciberseguridad es un desafío para la sociedad como un todo y necesita una respuesta que surja de la cooperación entre los diversos actores. (LLongueras Vicente, La Ciberguerra; la guerra inexistente, 2013)

(GLOBALVOICES, 2015), hace referencia a que “La Ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos e impedir que fuerzas enemigas los utilicen para cumplir los suyos”. (GLOBALVOICES, 2015)

El Consejo Nacional de Política Económica y Social de Colombia, define a la Ciberdefensa como la Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la Soberanía Nacional. (Castro, 2015)

La OTAN ha definido a la Ciberdefensa como “la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques”. (Almeida, 2019, pág. 37)

La determinación de infraestructura crítica y su posterior protección, preocupa al poder político de los diferentes países y se convierte en una responsabilidad estatal, evitar posibles ataques cibernéticos hacia dicha infraestructura. Las Infraestructuras críticas, se definen como el conjunto de recursos, servicios, tecnologías de la información y redes, que, en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Estado. (Instituto Español de Estudios Estratégicos-Instituto Universitario "General Gutiérrez Mellado", 2010)

Lo que refiere a infraestructura crítica digital es aquella que incluye todo un sistema interconectado de redes y servicios tanto físicos como lógicos, activos de información cuya paralización, daño, inoperatividad, puede causar graves efectos a la población y al Estado en diferentes aspectos como la salud, transporte, seguridad de la población, economía o manejo eficiente del Estado. (Pástor, Pérez, Arnáiz, & Taboso, Seguridad nacional y Ciberdefensa, 2009)

Las ciberamenazas constituyen la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede afectar la confidencialidad, integridad, disponibilidad y autenticidad de la información.

Ciberespionaje y ciberguerra son dos conceptos que están íntimamente interconectados. El objetivo del primero es la obtención de información, información de tipo principalmente estratégico, que hoy en día se encuentra almacenada electrónicamente, si bien bajo grandes medidas de seguridad, en los servidores de las instituciones de defensa y estratégicas, de la inmensa mayoría de los países del mundo. Hoy en día, los ataques de ciberespionaje más sofisticados, son los desarrollados y ejecutados por las agencias de inteligencia militar. El objetivo es, como para Sun Tzu, el conocimiento del enemigo, con el fin de adquirir no solo ventajas militares, sino también de carácter político, comercial y económico. (Díaz, 2016, págs. 12-13)

En Ecuador, tras la aprobación en 2014 del Código Orgánico Integral Penal (Tapia, 2018), se tipifican como delitos informáticos: pornografía infantil, violación del derecho a la intimidad, revelación ilegal de información de bases de datos, interceptación de comunicaciones, pharming, phishing, 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. (Asamblea Nacional, 2014, pág. 55)

Fundamentación específica

Constitución Política de la República del Ecuador

- **Art. 66**.- hace referencia que los ciudadanos tenemos el derecho de tener la respectiva privacidad con nuestra información personal, que se manifiesta en la forma de utilizar dicha información así como de la respectiva seguridad,

siendo necesario para su difusión la autorización propia o alguna legislación legal que se encuentre en vigencia. Conforme a la ley. (Asamblea Nacional del Ecuador, 2008)

- **Art. 158**.- hace referencia a la misión de Fuerzas Armadas de la defensa de la soberanía en un amplio y ambiguo concepto y de la vigilia de los diferentes derechos, garantías que cada ciudadano debe tener con sus respectivas libertades, en concordancia con la Policía Nacional. (Asamblea Nacional del Ecuador, 2008)

Ley Orgánica de Seguridad Pública y del Estado

- **Art. 1.-** Del objeto de la ley.- La presente ley tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado. (Subía & Espinoza, 2020, pág. 107)

Código Orgánico Integral Penal

- El Código Orgánico Integral Penal, refiere a delitos que se presentan en las diferentes redes sociales como whatsaap, tinder, facebook que abarcan temas de pornografía en niños, entrega de información personal, ingreso a comunicaciones sin la debida autorización, infinidad de delitos informáticos como robos bancarios, extracción de contraseñas, delitos en contra de las diferentes actores. (Tapia, 2018)

Plan Nacional de Seguridad Integral

- El auge de los medios tecnológicos y digitales, genera un sinnúmero de requerimientos en materia de seguridad; su uso permite acceder a la información de manera más rápida, proporciona mayor fluidez en las comunicaciones e interconexión de los sistemas de información, sin embargo, estos medios presentan grandes vulnerabilidades ante ataques cibernéticos. (Ministerio de Defensa Nacional, 2018).

Política de la Defensa Nacional

- Las Fuerzas Armadas ejecutan operaciones militares en cumplimiento de su misión fundamental establecida en la Constitución: “defensa de la soberanía e integridad territorial” (Asamblea Nacional del Ecuador, 2008) en el espacio continental, insular, aéreo, marítimo, ulterior y ciberespacio, acciones que se llevan a cabo con los medios y capacidades existentes; complementariamente, contribuyen a la seguridad integral y al desarrollo nacional. (Ministerio de Defensa Nacional, 2018)
- En lo relacionado al espacio aéreo, el espacio ulterior y ciberespacio, se ha identificado el surgimiento de amenazas con capacidad de afectar seriamente el funcionamiento de las áreas y sectores estratégicos del Estado. (Ministerio de Defensa Nacional, 2018)
- Las Fuerzas Armadas ejecutan operaciones militares en cumplimiento de su misión constitucional fundamental, es decir: “la defensa de la soberanía e integridad territorial” (Asamblea Nacional del Ecuador, 2008) en el espacio continental, insular, aéreo, marítimo, ulterior y ciberespacio, acciones que se llevan a cabo con los medios y capacidades existentes;

complementariamente, contribuyen a la seguridad integral y al desarrollo nacional. (Ministerio de Defensa Nacional, 2018)

Acuerdo Ministerial 281 MIDENA

- Se crea el Sistema de Ciberdefensa del MIDENA para “articular las instancias que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional, mismo que aún no ha sido conformado” (TAPIA, 2018); paralelamente en el 2014 “se crea el Comando de Ciberdefensa (COCIBER), y se diseña el Proyecto de ¨Implementación de la Capacidad de Ciberdefensa en FF.AA”, implementado a la fecha apenas en un 2%. (Comando de Ciberdefensa, 2019)

Amenaza

- “Situación en la que se tiene la certeza de que un tercero pueda causar daño”. (Ministerio de Defensa Nacional, 2018)
- Una amenaza es causada por un actor frente a su manifestación. (Ministerio de Defensa Nacional, 2018)
- Dentro de las Políticas y Estrategias de la defensa la Política 4 trata sobre la seguridad que se debe mantener con respecto a la información prioritaria del estado considerada como estratégica en lo que refiere a la defensa. (Ministerio de Defensa Nacional, 2018):

1. Protección de todo lo que envuelve el uso de redes informáticas, sistemas de comunicaciones destinados para fines de defensa. (Ministerio de Defensa Nacional, 2018)
2. “Desarrollar la capacidad de Ciberdefensa”. (Ministerio de Defensa Nacional, 2018)

3. Hace referencia a integrar los diferentes sistemas de defensa electrónica tanto de instituciones públicas como privadas que permitan afrontar los diferentes riesgos y ciberamenazas que puedan causar afectación al Estado. (Ministerio de Defensa Nacional, 2018)

- Podemos definir algunas ciberamenazas en forma general, que serán consideradas en la investigación.
  - Phishing, técnica para estafar y obtener información confidencial de forma fraudulenta.
  - Malware, amenazas informáticas o software hostil (virus, spyware, gusanos, etc.).
  - Ataques Cibernéticos (para robar IP), robar, alterar o destruir datos o sistemas de información.
  - Ataques Internos, aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, esto con fin de obtener un beneficio.
  - Ciberespionaje, sustracción de información de los ordenadores y de la red mediante diferentes técnicas de craqueo.
  - Spoofing, suplantación de identidad, a través de la falsificación de los datos en una comunicación.
  - MitM, ataque informático en el que el atacante tiene conexiones independientes con las víctimas y trasmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí.
  - Ingeniería Social, obtener información, acceso o permisos en sistemas de información que les permitan realizar algún acto que perjudique a una persona u organización.

Riesgos

Un riesgo constituye o abarcan circunstancias, anomalías ya sean de carácter natural o provocados por el hombre que estarían en condiciones de generar Situaciones y fenómenos latentes, de origen natural o antrópico, que podrían generar graves efectos a la seguridad del Estado. (Ministerio de Defensa Nacional, 2018, pág. 52). Su carácter de permanencia e inevitabilidad constituyen un referente para la elaboración de planes que permitan gestionar sus probables consecuencias. (Ministerio de Defensa Nacional, 2018)

Órgano Asesor en Ciberdefensa

El MIDENA mediante acuerdo 281, artículo 1, crea el Sistema de Ciberdefensa del Ministerio de Defensa Nacional como mecanismo que articula las instancias permanentes y de conformación que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional, a fin de coordinar e implementar políticas y estrategias de Ciberdefensa. El Sistema se estructura y funciona de la siguiente forma (Ruiz & Ochoa, 2019):

Organización:

- Ministra/o de Defensa o su delegado/a, quien lo presidirá;
- Subsecretario/a de Gabinete Ministerial o su delegado/a;
- Subsecretario/a de Apoyo al Desarrollo o su delegado/a;
- Subsecretario de Defensa o su delegado/a;
- Coordinador/a General Jurídico o su delegado/a;
- Director/a de Ciberdefensa, actuará como secretario/a;
- Jefe del Comando Conjunto, o su delegado/a;
- Comandante del Comando de Ciberdefensa;

- Podrá contar con la participación de los/las funcionarios u otros especialistas cuando se lo requiera.

Funciones:

- Articular con los diferentes organismos internos, el desarrollo de capacidades para prevenir, detectar y defender las posibles amenazas que provienen del ciberespacio y del espectro radioeléctrico que afecten significativamente al país. (Proaño & Guerrero, 2020)
- Diseñar la concepción político-estratégica de Ciberdefensa en concordancia con la Agenda Política de la Defensa. (Proaño & Guerrero, 2020)
- Monitorear y evaluar la implementación de las políticas de Ciberdefensa, así como del adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos al ciberespacio. (Proaño & Guerrero, 2020)
- Promover la concepción política estratégica de Ciberdefensa a nivel nacional. (Proaño & Guerrero, 2020)
- Coordinar con las instancias correspondientes, el diseño de políticas públicas a nivel nacional en el ámbito de su competencia. (Proaño & Guerrero, 2020)
- Coordinar con las instancias competentes, el diseño de políticas a nivel regional que permitan la interacción de los órganos directivos y operativos de los Estados en el ámbito de Ciberdefensa. (Proaño & Guerrero, 2020)
- Promover iniciativas de capacitación y formación en el ámbito de Ciberdefensa. (Proaño & Guerrero, 2020)

- Las demás que, dentro de su ámbito de acción, le corresponde a la máxima autoridad del Ministerio de Defensa Nacional. (Proaño & Guerrero, 2020)

Competencias:

- Apoyar con el diseño e implementar la concepción político-estratégica de Ciberdefensa que se someterá a la aprobación de la máxima autoridad del Ministerio de Defensa.
- Coordinar con el Comando de Ciberdefensa Conjunto las estrategias necesarias para la ejecución del Plan de Ciberdefensa.
- Articular el adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos a la Ciberdefensa, y evaluarlo periódicamente.
- Proponer disposiciones y directrices para el desarrollo e implementación de la capacidad de Ciberdefensa, a ser concertadas en el Comité de Ciberdefensa.
- Promover la política de Ciberdefensa a nivel nacional y regional.
- Las demás que le asigne en su ámbito de acción, la máxima autoridad del Ministerio de Defensa.

Misión:

Operar las capacidades de defensa, exploración y respuesta en el espacio cibernético para proteger y defender la infraestructura crítica e información estratégica del Estado. (Proaño & Guerrero, 2020)

Funciones:

- Proteger la infraestructura crítica del Estado en el corto, mediano y largo plazo. (Ministerio de Defensa Nacional, 2014)

- Desarrollar la capacidad de Ciberdefensa en: exploración, prevención, defensa y respuesta. (Ministerio de Defensa Nacional, 2014)
- Generar una estructura del Comando de acuerdo al modelo de gestión por procesos de la Defensa. (Ministerio de Defensa Nacional, 2014)
- Elaborar el Plan de Ciberdefensa con calificación correspondiente, para conocimiento y análisis del Comité de Ciberdefensa y aprobación de la máxima autoridad del Ministerio de Defensa. (Ministerio de Defensa Nacional, 2014)
- Coordinar con la Dirección de Ciberdefensa los temas de su competencia. (Ministerio de Defensa Nacional, 2014)

Base legal

- Constitución Política de la República del Ecuador. (Asamblea Nacional del Ecuador, 2008)
- Declaración Universal de los Derechos Humanos. (Asamblea General de la ONU, 1948)
- Convención Americana sobre Derechos Humanos (Pacto de San José). (Conferencia Especializada Interamericana sobre Derechos Humanos San José, 1969)
- Código Orgánico Integral Penal.
- Plan Nacional de Desarrollo 2017-2021. (Secretaría Nacional de Planificación y Desarrollo, Senplades., 2017)
- Agenda Política de la Defensa Nacional. (Ministerio de Defensa Nacional, 2018)
- Acuerdo Ministerial No 281 del 12 de septiembre de 2014. (Ruiz & Ochoa, 2019)

Hipótesis

¿Se optimizará la planificación y conducción de las operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna con la creación de una estructura de Ciberdefensa en la Fuerza Terrestre?

Sistema de variables

Variable independiente

Órgano asesor en Ciberdefensa para la Fuerza Terrestre.

Variable dependiente

Conducción de operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna.

Conceptualización y Operacionalización de las variables

Conceptualización de las variables

- ***Dependiente*:** Conducción de operaciones de respuesta a crisis en apoyo a la Policía Nacional (P.N) ante grave conmoción interna.

  ***Definición*:** Empleo de Fuerzas Armadas en base a las misiones contempladas en la Agenda Política de la Defensa, participación en apoyo a otras instituciones, respuesta a crisis (con estado de excepción), operaciones de apoyo a la P.N ante grave conmoción interna (LSPE, Art. 11 innumerado, Art. 35), ejecutando operaciones: Antidelincuenciales, Conflictividad Interna (control del orden público) y Control de la población y sus recursos. (Academia de Guerra del Ejército, 2018)

- ***Independiente*:** Órgano asesor en Ciberdefensa para la Fuerza Terrestre.

  ***Definiciones*:**

- ***Órgano*. -** Parte de una organización con un fin determinado. (Real Academia de la Lengua Española, 2019)
- ***Asesor*.** - Que da consejos o información. (Real Academia de la Lengua Española, 2019)
- ***Ciberdefensa***. - "Aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques". (Almeida, 2019)

Operacionalización de las variables

- Anexo "A" (Operacionalización de Variables).
- Anexo "B" (Síntesis Gráfica de la Investigación Cuantitativa o Cualitativa).

Capítulo III

Marco metodológico

Enfoque de la investigación

Esta investigación se realizará con un enfoque Mixto, considerando un análisis cualitativo de la información que se recopiló de las entrevistas realizadas a los comandantes o representantes de las unidades seleccionadas al establecer la población para el presente estudio y análisis cuantitativo de la información obtenida en base a los registros de observación y encuestas realizadas al personal que participó en las Operaciones Realizadas en octubre de 2019.

Todo ello en base a la recopilación directa de varias fuentes que permitieron realizar un análisis crítico, verás y sustentado, elaborando modelos teóricos y contrastando la información obtenida con la proporcionada por el Comando de Ciberdefensa, ente encargado de la seguridad y protección del ciberespacio, estableciendo la situación actual que atraviesa la Fuerza Terrestre en esta campo, obteniendo resultados que con un análisis cualitativo y cuantitativo, permitieron establecer soluciones a la problemática y formular lineamientos y estrategias, para la ejecución de operaciones de Ciberdefensa en apoyo a las operaciones terrestres de respuesta a crisis.

- Enfoque Cuantitativo. - Para poder probar la hipótesis nos valemos del uso de los diferentes datos que se van generando, teniendo como base la aplicación numérica con el respectivo enfoque estadístico que permita dar a conocer diferentes patrones y por ende mostrar y calificar las diferentes teorías. (Sampieri Hernández, Collado Fernández, & Lucio Baptista, 2003)

- Enfoque Cualitativo. - Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación. (Hernandez, Fernandez, & Baptista, 2006)

Tipo de investigación

Existe una extensa clasificación de los tipos de Investigación Científica, sin embargo para el análisis y desarrollo de la investigación correspondiente a la Ciberdefensa en la conducción de Operaciones Terrestres de Respuesta a Crisis, se utilizaron dos tipos de investigación la Investigación Explicativa o Causal e Investigación Documental (Daen, 2011), mediante la conceptualización y contextualización de la información recolectada de las diversas fuentes consideradas.

Mediante una combinación de los métodos analítico y sintético, en conjugación con el inductivo y deductivo para la explicativa y biblioFigura y hemeroFigura para la documental (Daen, 2011), en razón de que se obtuvo información de fuentes primarias mediante el criterio y experiencia sobre el tema de expertos y responsables de las operaciones en el ciberespacio y terrestres; y fuentes secundarias tomando como base publicaciones de Ciberseguridad y Ciberdefensa adoptadas por varios países relacionadas al área de interés del presente estudio. Posteriormente se realizó una investigación de campo, que permitió complementar con entrevistas y encuestas la posible solución, además de ponerla a prueba en forma práctica.

Población

El universo seleccionado para esta investigación será el personal de oficiales y voluntarios de las siguientes unidades: Dirección de Inteligencia, Dirección de Tecnologías de Información y Comunicaciones (D.T.I.C's) y

Dirección de Comunicación Social de la Fuerza Terrestre (D.C.S.F.T) en la parte técnica, al Comando del C.O 4 “CENTRAL”, C.E.M.A 71 y C.E.M.S 38 en la parte operativa y al personal del Comando de Ciberdefensa del COMACO, de acuerdo al siguiente orgánico:

Muestra para el Desarrollo de la Investigación

Tabla 1

Muestra para el desarrollo de la Investigación

UNIDAD	OFICIALES	VOLUNTARIOS	TOTAL
Dirección de Inteligencia de la F.T	5	19	24
DTICS	8	32	40
D.C.S.F.T	7	15	22
Comando C.O 4	20	46	66
Comando Ciberdefensa COMACO	6	12	18
Curso de Estado Mayor de Arma 71	51	0	51
Curso de Estado mayor de Servicios 38	19	0	19
TOTAL	**116**	**124**	**240**

Nota: Escalafón de la Fuerza Terrestre año 2020

Muestra

Emplearemos un muestreo no probabilístico, considerando al personal responsable de las diferentes áreas que involucran la seguridad y defensa del ciberespacio y áreas afines a la problemática, el cálculo de la muestra será efectuado en base al personal especialista con un margen de error del 5 % y un nivel de confianza del 95 %.

Para calcular la muestra consideraré la fórmula para cálculo con población finita:

$$\text{Población Finita (n)} = \frac{z^2 * p * q * N}{e^2(N-1) + z^2 * p * q}$$

N= Tamaño del Universo.

e= error de estimación máximo aceptado.

Z= Nivel de Confianza.

p= Porcentaje de la población que tiene el atributo deseado

q= Porcentaje de la población que no tiene el atributo deseado

n= Tamaño de la muestra

Datos:

N= 240

e= 0,06

Z= 1,96

p= 0,7

q= 0,3

$$n = \frac{(1,96*1,96)*\ 0,7*0,3*240}{(0,06*0,06)*(240-1) + (1,96*1,96)*0,7*0,3} = \frac{193,61664}{0,8604 + 0,8067} = \frac{193,61664}{1,667136}$$

n = 116,13

n = 116.

Métodos de investigación

Para desarrollar el presente trabajo y considerando los tipos de investigación empleados, se aplicaron los siguientes métodos de investigación:

Método analítico.- “Consiste en la desmembración de un todo, descomponiéndolo en partes o elementos para observar las causas, naturaleza y efectos, busca contestar, por qué suceden determinados fenómenos, su causa o factor de riesgo asociado al fenómeno o cuáles son los efectos de esa causa”. (Ruiz R. , 2006). En general, estos diseños buscan la asociación o correlación entre variables. Esto quiere decir, relación de causalidad. En este tipo de estudio es fundamental la formulación de hipótesis. (Lira i Morel, 2016)

Método sintético. - Proceso de razonamiento que tiende a reconstruir un todo, a partir de los elementos distinguidos por el análisis; se trata en consecuencia de hacer una explosión metódica y breve, en resumen. En otras palabras, debemos decir que la síntesis es un procedimiento mental que tiene como meta la comprensión cabal de la esencia de lo que ya conocemos en todas sus partes y particularidades. (Ruiz R. , 2006)

Método inductivo. - Observa, estudia y conoce las características genéricas o comunes que se reflejan en un conjunto de realidades para elaborar una propuesta o ley científica de índole general. Plantea un razonamiento ascendente que fluye de lo particular o individual hasta lo general. Se razona que la premisa inductiva es una reflexión enfocada en el fin. Puede observarse que la inducción es un resultado lógico y metodológico de la aplicación del método comparativo. (Abreu, 2014)

Método deductivo. - Permite determinar las características de una realidad particular que se estudia por derivación o resultado de los atributos o enunciados contenidos en proposiciones o leyes científicas de carácter general formuladas con anterioridad. Mediante la deducción se derivan las

consecuencias particulares o individuales de las inferencias o conclusiones generales aceptadas. En resumen, el método inductivo permite generalizar a partir de casos particulares y ayuda a progresar en el conocimiento de las realidades estudiadas. (Abreu, 2014)

Método biblioFigura. - Se basa en la investigación y revisión de libros. (Daen, 2011)

Método hemeroFigura. - Se basa en artículos o ensayos de revistas y periódicos. (Daen, 2011)

Los mismos que se emplearon para construir la base teórica, a fin de buscar una solución y/o comprobar la hipótesis sobre el tema de investigación propuesto.

Técnicas de recolección de datos

Las técnicas para recolección de datos empleadas en la presente investigación, fueron las siguientes:

Entrevista. - Es la práctica que permite al investigador obtener información de primera mano. La entrevista se puede llevar a cabo en forma directa, por vía telefónica, enviando cuestionarios por correo o en sesiones grupales. (Ruiz R. , 2006)

Encuesta. - Es un proceso interrogativo que finca su valor científico en las reglas de su procedimiento, se lo utiliza para conocer lo que opina la gente sobre una situación o problema que lo involucra, y puesto que la única manera de saberlo, es preguntándoselo, luego entonces se procede a encuestar a quienes involucra, pero cuando se trata de una población muy numerosa, sólo se aplica ese a un subconjunto, y aquí lo importante está en saber elegir a las personas que serán encuestadas para que toda la población

esté representada en la muestra; otro punto a considerar y tratar cuidadosamente, son las preguntas que se les darán. (Ruiz R. , 2006)

Documental. - Basada en la investigación y revisión de libros (bibliográfica), artículos o ensayos de revistas y periódicos (hemerográfica); puede realizarse a través de fichas bibliográficas y hemerográficas.

Instrumentos de recolección de datos

Los instrumentos de recolección de datos a ser utilizados serán:

- Anexo “C” (Cuestionarios de Entrevistas).
- Anexo “D” (Cuestionarios de Encuestas).

Técnicas para el análisis e interpretación de datos

El análisis e interpretación de datos se lo realizará a través de:

- Recopilación de información obtenida mediante la aplicación de los instrumentos de recolección de datos.
- Procesamiento de la información para poder mostrar los datos en tablas y Figuras estadísticos.
- Finalmente, con el análisis e interpretación de la información.

Presentación de los resultados

Diagnóstico situacional

Instrumento No 1: Exploración documental

El instrumento analizado fue el Informe de Amenazas y Tendencias Edición 2019 del Centro Criptológico Nacional CCN-CERT del Ministerio de Defensa del Gobierno de España, donde se hace referencia y realizan análisis

de las ciberamenazas, su evolución y tendencias, cuyo ámbito es de carácter mundial.

El informe indica que el número de usuarios de internet en todo el mundo sobrepasa los cuatro mil millones de personas de un total aproximado de siete mil millones de habitantes, es decir que el 55 % de la población del mundo se encuentran conectadas al internet.

Tabla 2

Desglose de los usuarios mundiales de internet de acuerdo a ubicación geográfica

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2018 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

Nota: Informe de amenazas y tendencias CCN-CERT 2019

World Economic Forum WEF, The Global Risks Report 2019, 14Th edition 2019, señala que la tecnología sigue ocupando un papel importante en la configuración del panorama de riesgos globales para los individuos, los gobiernos y las empresas. En el informe citado, el "fraude y robo masivo de datos" fue clasificado como el cuarto riesgo más importante a nivel mundial, en un horizonte de 10 años, situando los "ciberataques" en quinta posición, pese a

todo, la mayoría de los encuestados auguran un crecimiento de los riesgos de ciberataques en 2019, especialmente en lo relativo a la sustracción de dinero y/o datos (82%) y la interrupción de las operaciones (80%), además se espera que los riesgos asociados a las noticias falsas y el robo de identidad aumenten en el 2019.

Los ciberataques unidos a una escasa adopción de medidas de seguridad, propiciaron nuevamente a la aparición de brechas masivas relacionadas con información personal; en otros lugares del mundo, las violaciones de datos personales afectaron a 150 millones de usuarios de la aplicación MyFitnessPal y a alrededor de 50 millones de usuarios de Facebook.

El pasado año también fue testigo de ciberataques dirigidos a las infraestructuras críticas. Las potenciales vulnerabilidades tecnológicas se han convertido en un problema de seguridad nacional. La segunda fuente de riesgos más citada en el Informe del WEF ha sido, precisamente, el emparejamiento de los ciberataques con las caídas de las infraestructuras de información críticas.

En una investigación realizada por Brookings, el 32% de los encuestados señaló que considera la IA como una amenaza para la humanidad, frente al 24%, que opinaba en sentido contrario. (Blanco, 2019)

Durante 2018, diversos equipos de investigación estudiaron el despliegue de 126.000 tweets y descubrieron que aquellos que contenían noticias falsas superaban a aquellos otros que contenían información verdadera, alcanzando la superficie de ataque (las personas) seis veces más rápido. Parece claro que la interacción entre las emociones y la tecnología se convertirá, probablemente, en una fuerza cada vez más disruptiva.

En lo que tiene que ver con código dañino, éste ha vencido en aumento desde el año 2018, es así que hay más de 800 millones de programas conocidos de este tipo y alrededor de 390 mil nuevas variantes se suman diariamente a esa cifra, en el entorno móvil, ya se contabilizan más de 27 millones de programas de malware, solo para Android.

Las tendencias de acuerdo al informe, mencionan que en 2019 y en los años posteriores los agentes estatales continuarán realizando campañas de intrusión como parte de sus estrategias nacionales. Las entidades de los sectores de gobierno, la defensa, las ONG continuarán siendo los objetivos prioritarios de sus operaciones. Estas intrusiones, probablemente, serán respaldadas (deliberada o accidentalmente) por proveedores de los sectores de telecomunicaciones y tecnología.

Los sistemas de información conectados a internet son vitales para la mayoría de las economías nacionales, por lo que constituyen un objetivo obvio en caso de conflicto o controversia; con la tecnología digital omnipresente y la explotación del internet de las cosas, las posibilidades de ataques son ilimitadas. Los ataques patrocinados por Estados pueden presentarse en todas las intensidades, y muchos de ellos, probablemente, se activarán como advertencia.

Los seres humanos siguen siendo el eslabón más débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas, es de esperar muchos más correos electrónicos de suplantación de identidad (phishing) y sitios web falsos diseñados para engañar al usuario y facilitar el acceso a datos confidenciales, tales como contraseñas o números de tarjetas de crédito.

Los dispositivos conectados a internet vía Wifi (profesionales, comerciales o domésticos) ofrecen nuevas formas para que los agentes de las amenazas penetren en las redes internas, atacando a los dispositivos conectados, incluyendo los ordenadores y generalmente al objeto de sustraer datos o información personal.

Instrumento No 2: Entrevista

El instrumento que se elaboró y administró se detalla en el Anexo ¨D¨. Para la realización de la entrevista nos valimos de una aplicación libre de Google llamada Drive, la cual nos permite el procesamiento de los datos obtenidos, mismos que fueron resumidos de acuerdo a las diferentes respuestas proporcionadas por el personal de entrevistados.

La entrevista fue aplicada a cinco oficiales superiores de las áreas técnicas, operativas y que tienen relación con el área de ciberdefensa, de acuerdo al siguiente detalle:

- Subdirector de Tecnologías de la Información de la Fuerza Terrestre
- Director de Comunicación Social de la Fuerza Terrestre
- Comandante del Comando Operacional No 4
- Comandante de los grupos operativos del Comando de Ciberdefensa

Las respuestas presentadas por los oficiales conocedores de la temática, una vez realizada la entrevista, se detallan a continuación:

Actualmente se habla sobre un nuevo dominio a nivel mundial denominado el ciberespacio. ¿Qué opinión tiene al respecto?

- Ciberespacio es un nuevo escenario donde se desarrollan eventos que atentan a la seguridad del Estado

- Ciberespacio involucra el uso de redes de información y datos
- Las nuevas amenazas asimétricas están involucradas al uso del ciberespacio
- Dependencia de la humanidad a los sistemas y dispositivos tecnológicos del Ciberespacio, se pueden generar conflictos como ciberguerras

¿Cuál es su opinión con respecto a la situación actual de la capacidad de ciberdefensa en la Fuerza Terrestre?

- Esta capacidad no está desarrollada
- No dispone
- No existe unidad de ciberdefensa en la Fuerza Terrestre
- Ejército debería formar parte de un comité de crisis para analizar amenazas en el ciberespacio, buscar mecanismos de cooperación

¿Cuál es su visión general, sobre cómo debería ser organizada la ciberdefensa en la Fuerza Terrestre?

- Una unidad por cada división, grupo de exploración y grupo de respuesta a incidentes
- Unidades de protección de datos, sistemas tecnológicos importantes, mando y control
- Debe tener capacidades técnicas y operativas
- Se debe organizar una capacidad de ciberseguridad, para proteger sus activos de información y asegurar las operaciones terrestres

¿Cuál sería a su criterio, la importancia de las operaciones de ciberdefensa en apoyo a las operaciones militares terrestres?

- Mando y control debe estar protegido, impidiendo el ingreso a los sistemas que generen pérdida de información o daños a la infraestructura crítica.
- Aportaría en la búsqueda de información, protección de sistemas
- Actuaría de manera transversal para mantener la sorpresa de las operaciones, combatir a la desinformación
- Vital importancia monitorear el ciberespacio para el cumplimiento de las operaciones

En su opinión: ¿Qué reparto debería ser el encargado de la ciberdefensa o es necesario la creación de un órgano de ciberdefensa para la Fuerza Terrestre?

- El Agrupamiento de Comunicaciones y Guerra Electrónica
- Es necesario la organización de una unidad de ciberdefensa
- Por ser una capacidad nueva se requiere de una estructura para esta área
- No ya que la ciberdefensa tiene sus propios objetivos y misiones

¿Considera Ud. que existe personal capacitado en el área de ciberseguridad y ciberdefensa en la Fuerza Terrestre?

- No existe personal capacitado para estas operaciones
- Es mínimo y más en áreas afines como sistemas, informática
- No existe
- Muy limitado número de personal capacitado

Del análisis de las respuestas presentadas por el personal de oficiales entrevistados, podemos llegar a las siguientes conclusiones:

- Existe dependencia de la humanidad con el ciberespacio, lo que genera un escenario donde se pueden ejecutar actos que atenten a la seguridad del estado y en niveles avanzados pueden crear conflictos como ciberguerras
- En la Fuerza Terrestre la capacidad de ciberdefensa no se encuentra desarrollada, es de vital importancia generar capacidades en esta área, de igual manera no existe personal capacitado para trabajar en esta área, lo que requiere un tratamiento especial.
- Las operaciones de ciberdefensa inciden de manera fundamental en las operaciones militares terrestres, por cuanto es necesario proteger los sistemas de mando y control, infraestructura crítica digital, la información de carácter reservado de la fuerza.
- La organización de la ciberdefensa debe ser materializada desde el punto de vista de las operaciones terrestres, con grupos operativos con misiones de exploración para la obtención de información en el ciberespacio y equipo de respuestas de incidentes de seguridad informática.

Instrumento No 3: Encuesta

El instrumento que se elaboró y administró se detalla en el Anexo ¨C¨. Para la realización de la encuesta nos valimos de una aplicación libre de Google denominada Drive con la herramienta de Formularios de Google, la cual nos permite generar datos estadísticos con Figuras que facilitan el entendimiento y comprensión de los resultados generados. La encuesta contaba con preguntas elaboradas en formato tipo Likert con opciones: en su totalidad, medianamente, poco, nada, totalmente de acuerdo, de acuerdo, indeciso, en desacuerdo, muy en desacuerdo, preguntas con diferentes opciones de selección, lo que nos

permitió conocer sobre el grado de conformidad de los encuestados hacia las diferentes interrogantes.

La encuesta fue remitida empleando medios tecnológicos a las diferentes áreas de interés, conocedoras de la temática planteada como son tecnologías de la información, inteligencia, comunicación social, comandos operacionales, ciberdefensa, mediante el uso de correos electrónicos personales, institucionales, mensajes de WhatsApp, donde se incluye el link correspondiente que le direccionaba de manera automática a la encuesta y por ende la tabulación de datos.

El personal que participó en la encuesta se detalla en la siguiente figura:

Figura 1

Personal que participó en la encuesta

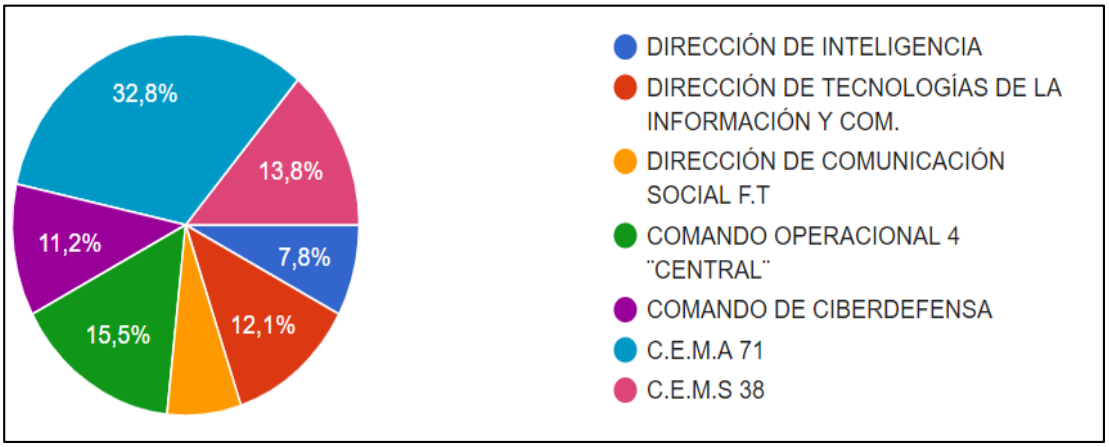


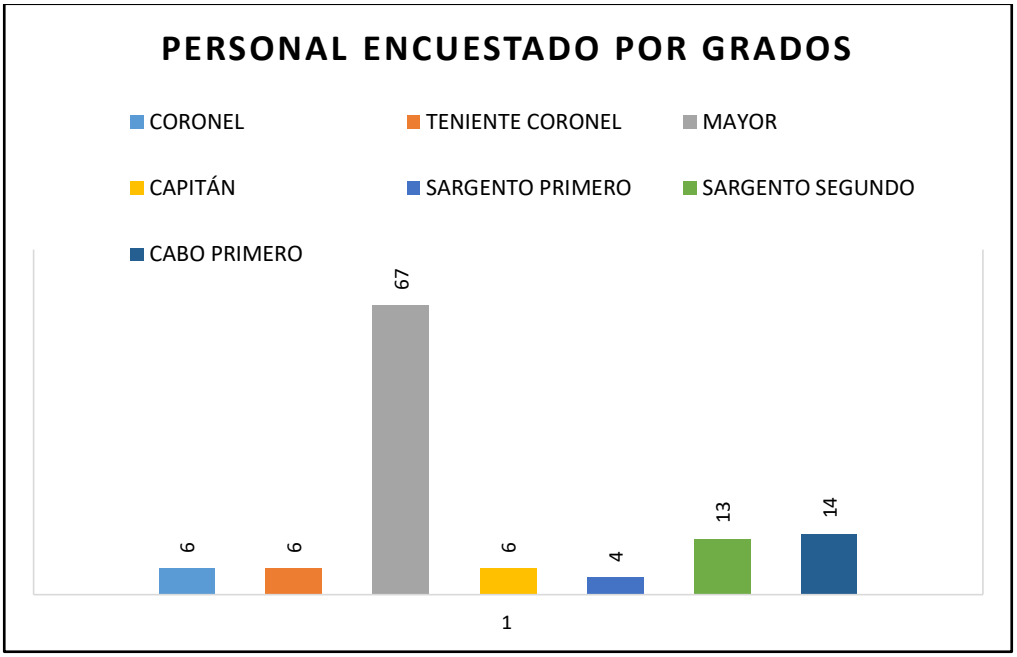
Figura 2

Numérico de personal que participó en la encuesta

La encuesta fue realizada a personal de oficiales y voluntarios de la Fuerza Terrestre, en los grados de Coronel, Teniente Coronel, Mayor, Capitán, Sargento Primero, Sargento Segundo, Cabo Primero, como se visualiza en la siguiente figura:

Figura 3

Numérico de personal encuestado por grados



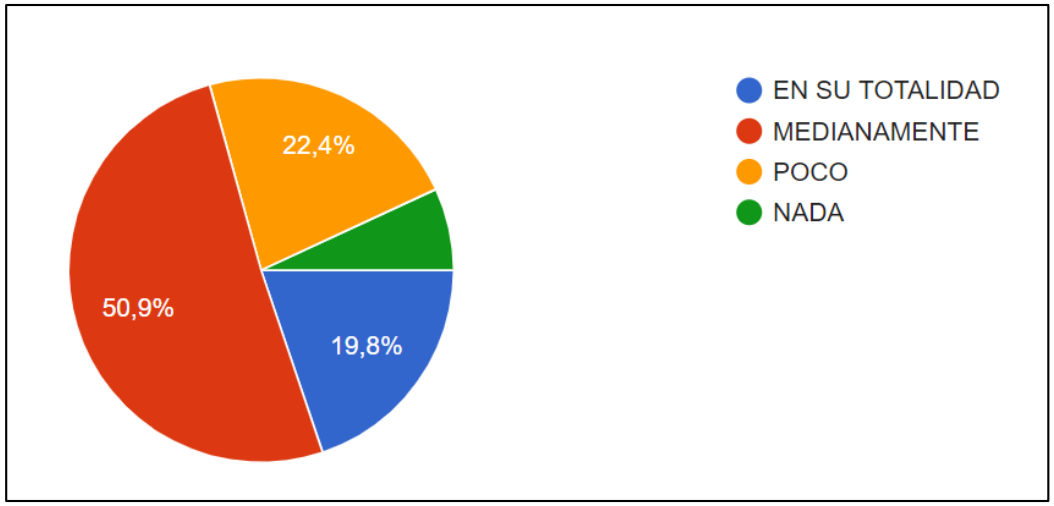
De manera individual, las respuestas generadas por el personal de encuestados de acuerdo a cada pregunta, fueron las siguientes:

Pregunta 1.- ¿Ha escuchado o tiene conocimiento acerca del quinto dominio conocido como el ciberespacio?

El 19,8 % de los encuestados indican que, en su totalidad, el 50,9 % medianamente, el 22,4 % poco y el 6,9 % nada de conocimiento, como se puede visualizar en la Figura 04; lo que refleja que la gran mayoría del personal de oficiales y voluntarios tienen poco conocimiento de este nuevo pero fundamental escenario.

Figura 4

Porcentaje de conocimiento del ciberespacio

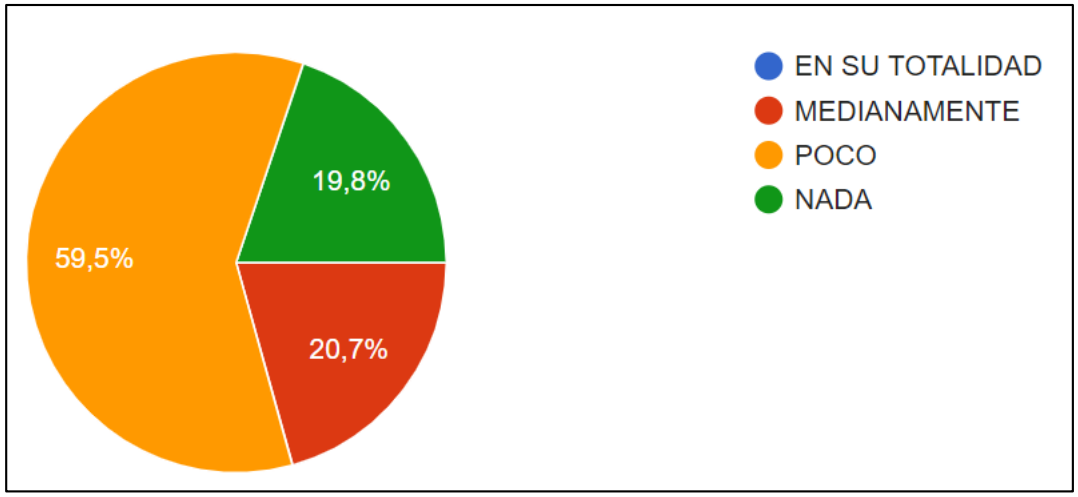


Pregunta 2.- A su criterio ¿Cree Ud. que existe una cultura de ciberseguridad en la Fuerza Terrestre?

Nadie afirma que exista una cultura total en ciberseguridad en la Fuerza Terrestre, el 20,7 % indica que medianamente, el 59,5 % poco y el 19,8 % nada, como se puede visualizar en la Figura 05; por lo que se puede apreciar que la mayoría de personal no maneja protocolos básicos de seguridad informática, que ponen en riesgo la información, los sistemas digitales.

Figura 5

Cultura de Ciberseguridad en la Fuerza Terrestre

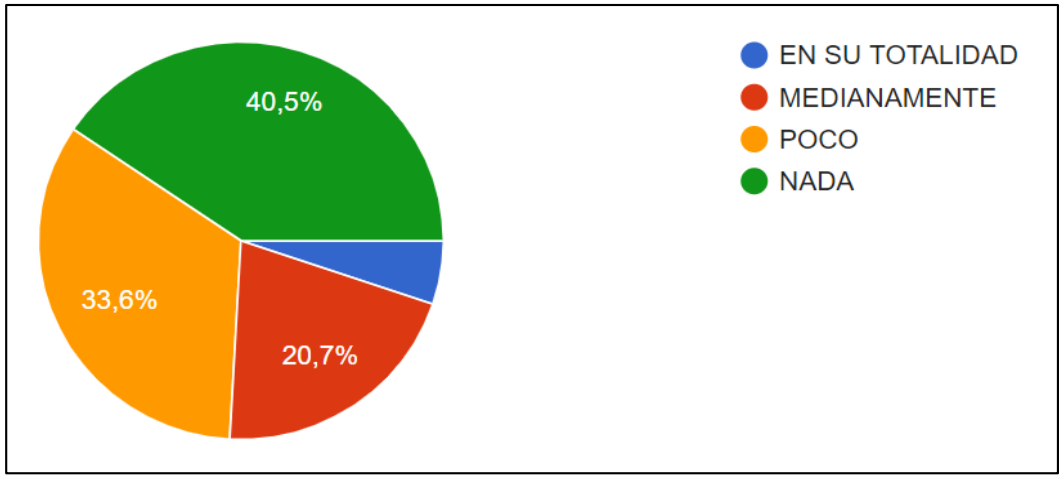


Pregunta 3.- Conoce Ud. Si su unidad ¿está en la capacidad de detectar y gestionar incidentes de seguridad cibernética?

El 5,2 % de los encuestados indican que, en su totalidad, el 20,7 % medianamente, el 33,6 % poco y el 40,5 % nada, como se puede visualizar en la Figura 06; es necesario que la Fuerza Terrestre dentro de su estructura cuente con un equipo de respuestas a incidentes de seguridad informática para suplir esta vulnerabilidad.

Figura 6

Porcentaje de detección y gestión de incidentes informáticos

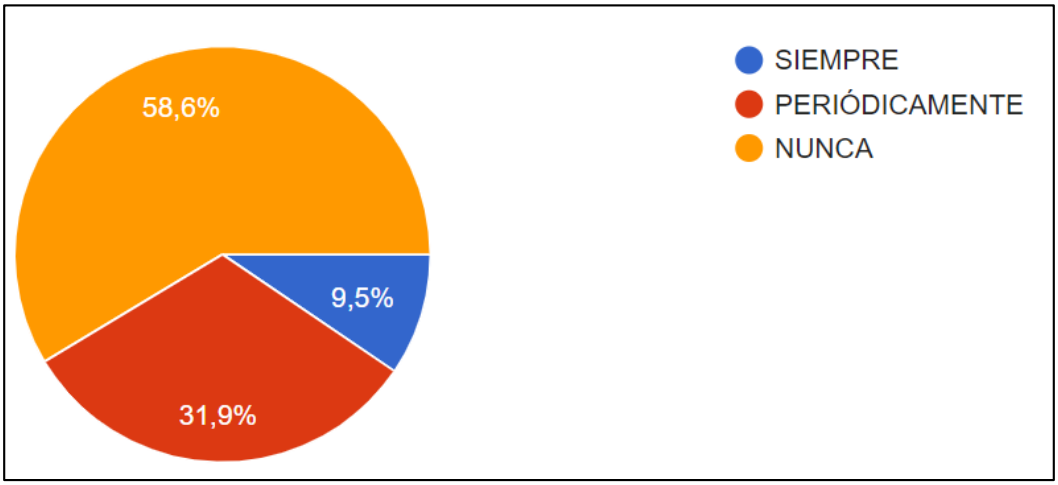


Pregunta 4.- ¿Ha instalado periódicamente parches o programas de seguridad del sistema operativo y de los principales programas de su ordenador institucional?

El 9,5 % de los encuestados indican que siempre, el 31,9 % periódicamente y el 58,6 % nunca, como se puede visualizar en la Figura 07; lo que nos da una visión general de que los equipos personales, correos institucionales, aplicaciones libres, páginas institucionales, entre otros, son vulnerables ante amenazas cibernéticas.

Figura 7

Protección del sistema operativo y programas de ordenadores

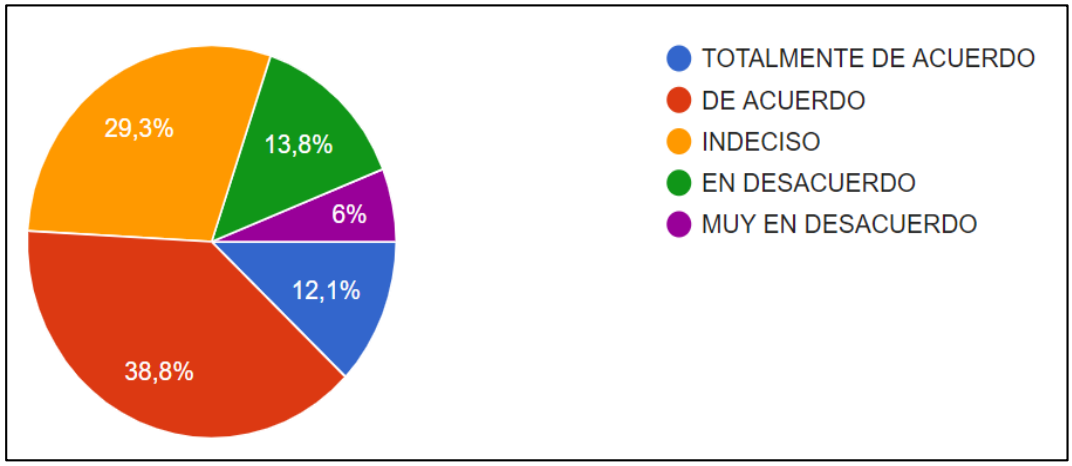


Pregunta 5.- En su vida laboral ¿Cree Ud. que ha sido objeto de algún ataque cibernético, es decir ingresos no autorizados a su correo institucional, robo de información, envío de información falsa, entre otros?

El 12,1% de los encuestados indican que están totalmente de acuerdo, el 38,8 % de acuerdo, el 29,3 % indeciso, el 13,8 % en desacuerdo y el 6 % muy en desacuerdo, como se puede visualizar en la Figura 08; lo que demuestra que en algún momento el personal ha sido víctima de ciberataques e ingresos no autorizados a los sistemas informáticos.

Figura 8

Porcentaje de haber sido objeto de algún ataque cibernético

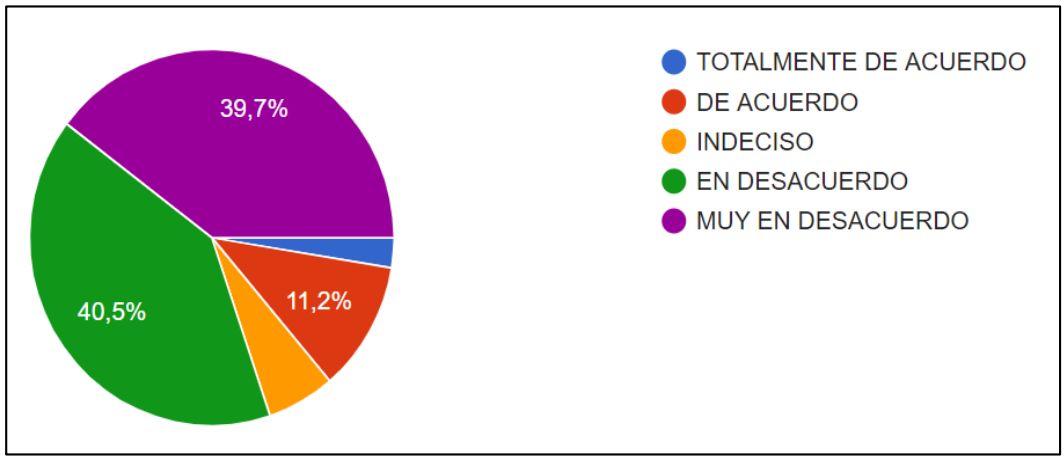


Pregunta 6.- A su criterio ¿En su unidad, la asignación presupuestaria es suficiente para la seguridad informática?

El 2,61% de los encuestados indican que están totalmente de acuerdo, el 11,2 % de acuerdo, el 7,6 % indeciso, el 40,5 % en desacuerdo y el 39,7 % muy en desacuerdo, como se puede visualizar en la Figura 09; por lo que es necesario que en las diferentes programaciones del gasto se reflejen valores presupuestarios acordes para satisfacer esta área crítica y vulnerable.

Figura 9

Asignación presupuestaria suficiente para seguridad informática

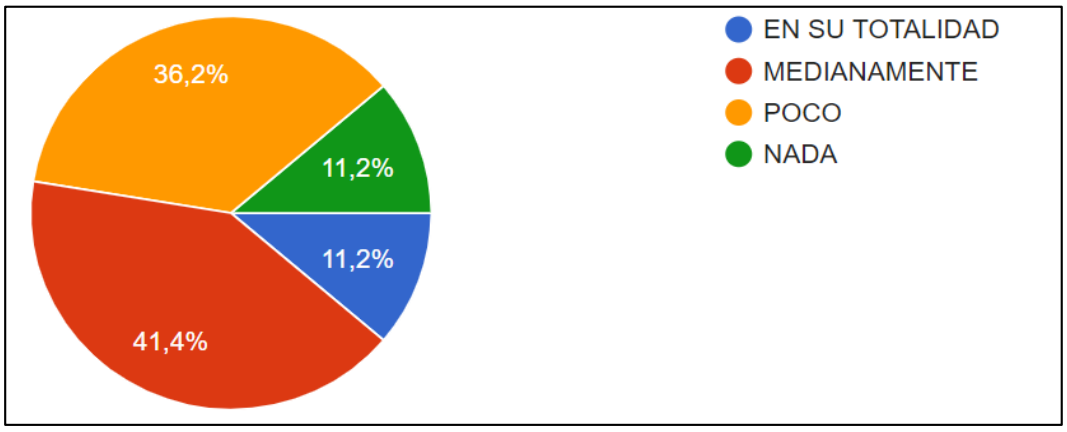


Pregunta 7.- ¿Tiene conocimiento de qué tipos de amenazas cibernéticas pueden afectar la conducción de operaciones militares de respuesta a crisis?

El 11,2 % de los encuestados indican que, en su totalidad, el 41,4 % medianamente, el 36,2 % poco y el 11,2 % nada, como se puede visualizar en la Figura 10; lo que muestra que se tiene desconocimiento de las diferentes amenazas cibernéticas existentes, lo que hace vulnerable a la institución a sufrir ciberataques.

Figura 10

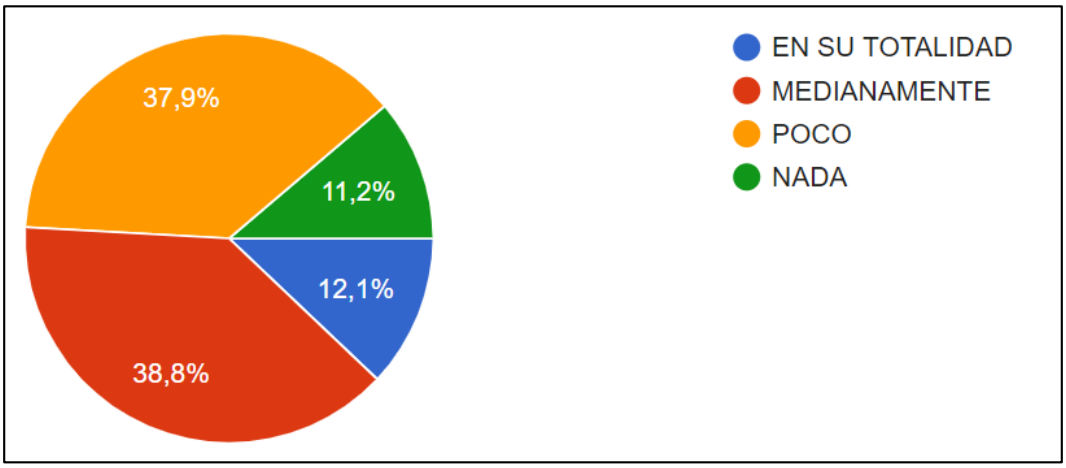
Conocimiento de ciberamenazas que pueden afectar a la conducción de operaciones



Pregunta 8.- ¿Conoce acerca de las capacidades que tiene la Ciberdefensa?

Figura 11

Conocimiento de las capacidades de ciberdefensa



El 12,1 % de los encuestados indican que, en su totalidad, el 38,8 % medianamente, el 37,92 % poco y el 11,2 % nada, como se puede visualizar en la Figura 11; lo que demuestra que gran parte del personal desconoce las

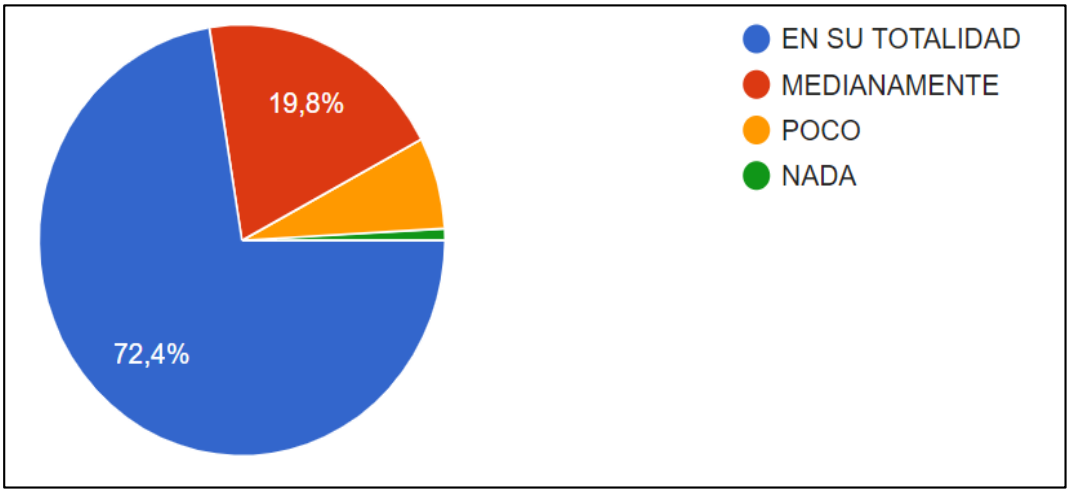
capacidades que tiene la ciberdefensa, su forma de operar y proteger los sistemas informáticos e infraestructura crítica digital.

Pregunta 9.- Considera Ud. que ¿Las operaciones de respuesta a crisis (estado de excepción) ante grave conmoción interna requieren el apoyo de las capacidades de Ciberdefensa?

El 72,4 % de los encuestados indican que, en su totalidad, el 19,8 % medianamente, el 6,9 % poco y el 0,9 % nada, como se puede visualizar en la Figura 12, lo que confirma que es necesaria la ejecución de operaciones de ciberdefensa en apoyo a las operaciones militares.

Figura 12

Apoyo de la ciberdefensa en las operaciones de respuesta a crisis



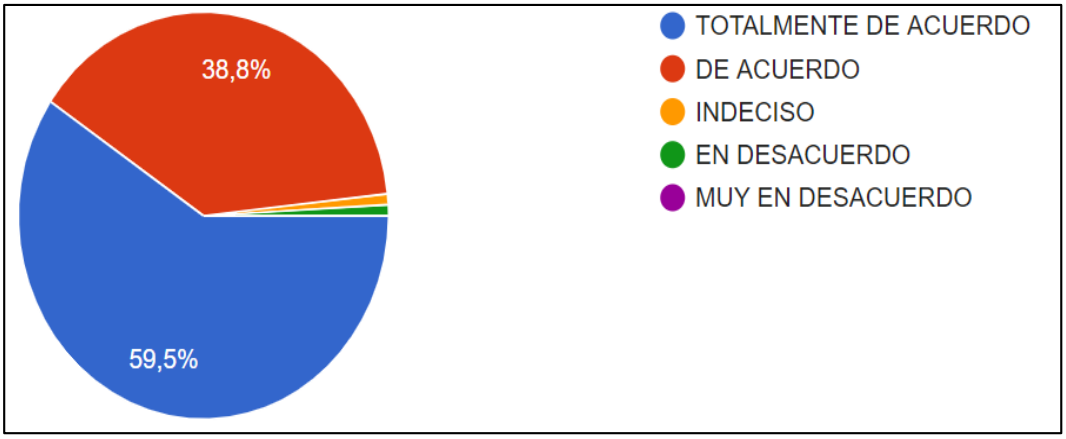
Pregunta 10.- Considera Ud. que ¿La ciberdefensa debería actuar de manera transversal en todo tipo de operaciones ejecutadas por la Fuerza Terrestre?

El 59,5 % de los encuestados indican que están totalmente de acuerdo, el 38,8 2 % de acuerdo, el 0,9 % indeciso, el 0,9 % en desacuerdo y

el 0 % muy en desacuerdo, como se puede visualizar en la Figura 13; lo que refleja que es necesario que las operaciones de ciberdefensa se ejecuten de manera transversal en todas las operaciones militares ya sea en el ámbito interno como externo.

Figura 13

Accionar de ciberdefensa de manera transversal en las operaciones de la Fuerza Terrestre

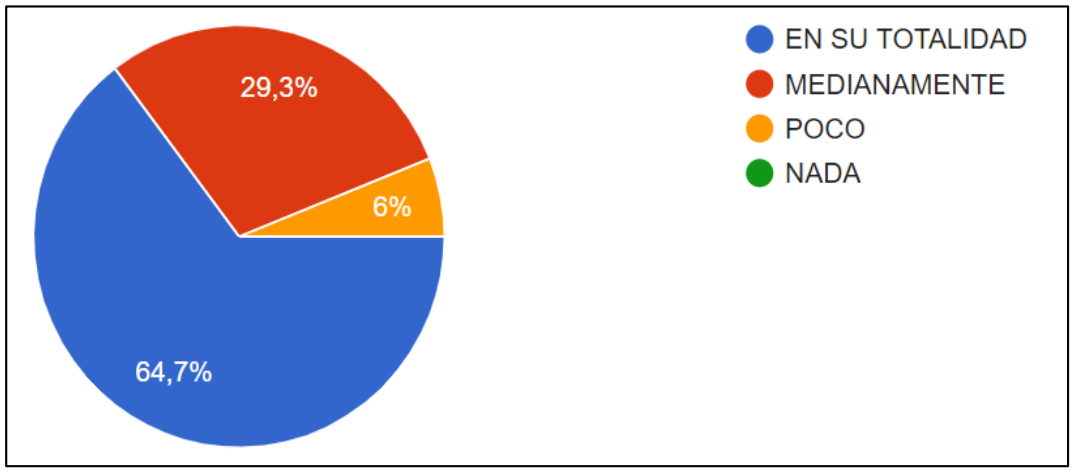


Pregunta 11.- A su criterio, considera Ud. que la ciberdefensa ¿Tiene la capacidad de buscar información que apoye a la planificación de las diferentes operaciones militares?

El 64,7 % de los encuestados indican que, en su totalidad, el 29,3 % medianamente, el 6 % poco y el 0 % nada, como se puede visualizar en la Figura 14; lo que evidencia que la ciberdefensa es fundamental para obtener información que permita y apoye en la planificación de las operaciones militares.

Figura 14

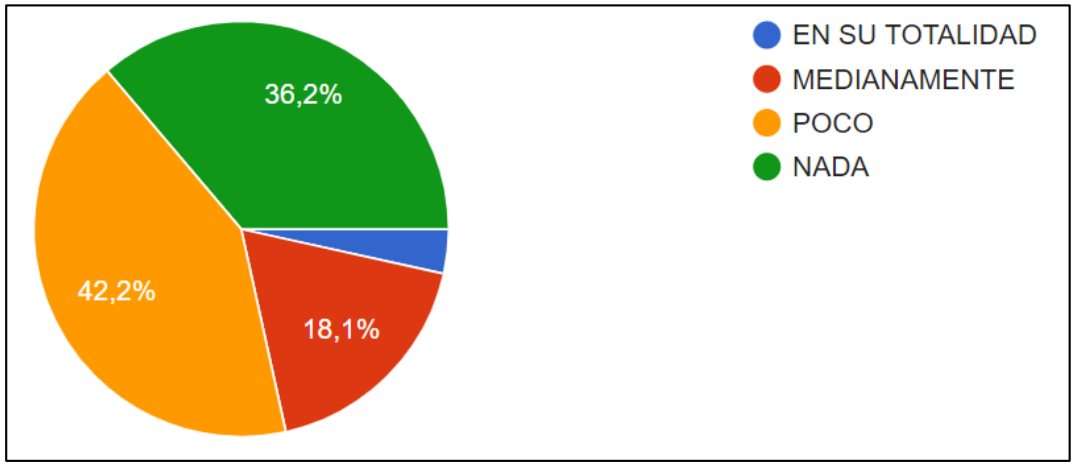
Capacidad de ciberdefensa de búsqueda de información



Pregunta 12.- A su criterio, dentro de su unidad ¿Existe personal capacitado en el área de la ciberseguridad y ciberdefensa?

Figura 15

Personal capacitado en ciberdefensa en las unidades militares



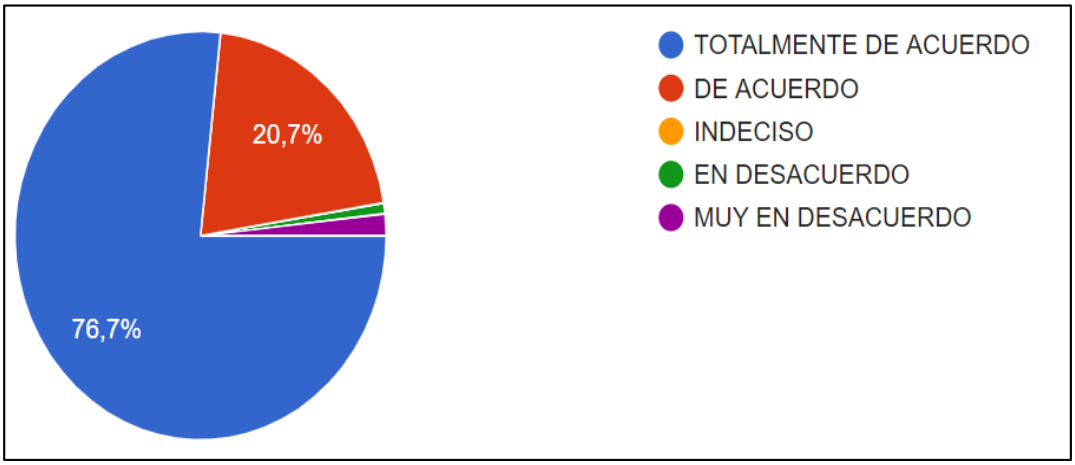
El 3,4 % de los encuestados indican que, en su totalidad, el 18,1 % medianamente, el 42,2 % poco y el 36,2 % nada, como se puede visualizar en la Figura 15; lo que evidencia que no existe o es mínimo el personal

especialista en ciberdefensa y que es urgente capacitar al personal militar en esta área técnica de fundamental importancia.

Pregunta 13.- Considera Ud. que ¿Es de suma importancia para la Fuerza Terrestre contar con un órgano de ciberdefensa?

Figura 16

Importancia de contar con un órgano de ciberdefensa en la Fuerza Terrestre



El 76,7 % de los encuestados indican que están totalmente de acuerdo, el 20,72 % de acuerdo, el 0 % indeciso, el 0,9 % en desacuerdo y el 1,7 % muy en desacuerdo, como se puede visualizar en la Figura 16; lo que hace pertinente que la Fuerza Terrestre cuente en su estructura con un órgano de ciberdefensa.

De las respuestas de los encuestados de manera general podemos indicar que existe un bajo nivel de conocimiento en el área de ciberseguridad y ciberdefensa, el personal capacitado en esta área es mínimo, además que las operaciones de ciberdefensa deben ejecutarse de manera transversal en todas las operaciones militares tanto en el ámbito interno como externo, por lo que es

necesario que se implemente un órgano de ciberdefensa en la Fuerza Terrestre con capacidades que permita asegurar los activos informáticos y la infraestructura crítica digital.

Capítulo IV

Desarrollo de la investigación

Describir el marco legal que establece la protección del ciberespacio y su aplicabilidad en el ámbito de las operaciones militares de ciberdefensa.

Podemos indicar que el marco legal vigente en el país, no es muy específico en lo referente al ciberespacio, que internacionalmente es considerado ya como el quinto dominio (tierra, aire, mar, órbita geoestacionaria y ciberespacio); sin embargo la constitución hace referencia a la protección de la información y privacidad de las personas, desde este concepto tanto en la Ley de Seguridad Pública y del Estado como la Política de la Defensa Nacional se consideran disposiciones y acciones orientadas a la vigilancia y protección del ciberespacio, las mismas que han sido operacionalizadas en el nivel militar a través del Comando Conjunto de las Fuerzas Armadas.

Paralelamente en el Código Orgánico Integral Penal, se han tipificado como delitos algunas ciberamenazas, con el objetivo de garantizar el derecho de los ciudadanos, organizaciones e instituciones (tanto públicas como privadas) a la privacidad de sus datos e información calificada, convirtiéndose en responsabilidad del estado a través de las instituciones correspondientes la vigilancia y protección del ciberespacio.

Para conocer el hecho debemos referirnos a la Constitución Política de la República del Ecuador, que en su Art. 66.- Reconoce y garantizará a las personas…19. Todos los datos personales deben ser protegidos lo que incluye su acceso y lo que se debe decidir con respecto a los mismos. (Asamblea Nacional del Ecuador, 2008).

Art. 158.- Da a conocer las misiones de Fuerzas armadas como es la fundamental basada en la garantía de la defensa soberana y del territorio de manera integral, así como proteger los derechos, garantías y libertades de sus ciudadanos. (Asamblea Nacional del Ecuador, 2008)

La Ley Orgánica de Seguridad Pública y del Estado (Subía & Espinoza, 2020), en su Art. 1.- “Del objeto de la ley.- La presente ley tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador”, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado. (Subía & Espinoza, 2020)

El Código Orgánico Integral Penal (Tapia, 2018), tipifica algunos delitos informáticos: pornografía infantil, violación del derecho a la intimidad, revelación ilegal de información de bases de datos, interceptación de comunicaciones, pharming, phishing, 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. (Tapia, 2018)

El auge de los medios tecnológicos y digitales, genera un sinnúmero de requerimientos en materia de seguridad; su uso permite acceder a la información de manera más rápida, proporciona mayor fluidez en las comunicaciones e interconexión de los sistemas de información, sin embargo, estos medios

presentan grandes vulnerabilidades ante ataques cibernéticos (Ministerio de Defensa Nacional, 2018).

La Política de la Defensa Nacional, contempla a las Fuerzas Armadas cumpliendo su misión fundamental establecida en la Constitución: “defensa de la soberanía e integridad territorial” (Asamblea Nacional del Ecuador, 2008) en el espacio continental, insular, aéreo, marítimo, ulterior y ciberespacio, acciones que se llevan a cabo con los medios y capacidades existentes; complementariamente, contribuyen a la seguridad integral y al desarrollo nacional. (Ministerio de Defensa Nacional, 2018)

En lo relacionado al espacio aéreo, el espacio ulterior y ciberespacio, se ha identificado el surgimiento de amenazas con capacidad de afectar seriamente el funcionamiento de las áreas y sectores estratégicos del Estado. (Ministerio de Defensa Nacional, 2018)

Las Fuerzas Armadas ejecutan operaciones militares en cumplimiento de su misión constitucional fundamental, es decir: “la defensa de la soberanía e integridad territorial” (Asamblea Nacional del Ecuador, 2008) en el espacio continental, insular, aéreo, marítimo, ulterior y ciberespacio, acciones que se llevan a cabo con los medios y capacidades existentes; complementariamente, contribuyen a la seguridad integral y al desarrollo nacional. (Ministerio de Defensa Nacional, 2018)

En el Acuerdo Ministerial 281 del MIDENA, Se crea el Sistema de Ciberdefensa del MIDENA para “articular las instancias que aborden el tema desde el nivel político-estratégico, estratégico militar y operacional, mismo que aún no ha sido conformado” (TAPIA, 2018); paralelamente en el 2014 “se crea el

Comando de Ciberdefensa (COCIBER), y se diseña el Proyecto de ¨Implementación de la Capacidad de Ciberdefensa en FF.AA", implementado a la fecha apenas en un 2%. (Comando de Ciberdefensa, 2019).

En la política de defensa nacional se define una amenaza, como "situación en la que se tiene la certeza de que un tercero pueda causar daño" (Ministerio de Defensa Nacional, 2018). Una amenaza es causada por un actor frente a su manifestación. (Ministerio de Defensa Nacional, 2018)

Como parte de las Políticas y Estrategias de la defensa en lo que hace referencia a la Política 4 menciona que es necesario y prioritario la protección de toda la información de carácter estratégica perteneciente al Estado en la arista de la defensa (Ministerio de Defensa Nacional, 2018) :

1. Protección de todo lo que envuelve el uso de redes informáticas, sistemas de comunicaciones destinados para fines de defensa. (Ministerio de Defensa Nacional, 2018)
2. "Desarrollar la capacidad de Ciberdefensa". (Ministerio de Defensa Nacional, 2018)
3. Hace referencia a integrar los diferentes sistemas de defensa electrónica tanto de instituciones públicas como privadas que permitan afrontar los diferentes riesgos y ciberamenazas que puedan causar afectación al Estado. (Ministerio de Defensa Nacional, 2018)

Al analizar este marco legal existente en el Ecuador y que hace referencia al ciberespacio, tenemos que la Constitución Política de la República del Ecuador, garantiza entre otros aspectos: "el derecho a la protección de datos personales de los ciudadanos, su intimidad y la inviolabilidad de su

correspondencia (pudiendo ser física y/o virtual)" (Asamblea Nacional del Ecuador, 2008); pero en forma muy general pues no considera la real dimensión de este derecho, ya que implica vigilar y proteger el ciberespacio, para evitar que las ciberamenazas actúen no solo en contra de los ciudadanos sino también contra instituciones públicas y privadas, como cuando se retiró el asilo diplomático al fundador de WikiLeaks, Julian Assange, donde se registraron más de 40 millones de ciberataques a portales web de instituciones públicas. (El Comercio, 2019)

Por otro lado la misma constitución en el artículo 158 da la responsabilidad a las Fuerzas de garantizar la soberanía ecuatoriana en el ciberespacio, sin embargo al no existir en la constitución objetivos nacionales permanentes, está misión no está contemplada dentro de los objetivos nacionales actuales, trayendo como consecuencia una total ausencia de presupuesto que limita el entrenamiento y equipamiento de las mismas para cumplir esta nueva y muy importante tarea.

Haciendo referencia a los miembros del Sistema de Seguridad Pública y del Estado se les impone prevenir los riesgos y amenazas de todo orden; este marco permite la acción de las FF.AA, en el ámbito de la ciberdefensa la cual se traduce en acciones del Ministerio de Defensa a través de la Política de Defensa Nacional, sin embargo una vez más la falta de presupuesto para invertir en este campo es una condicionante que impide operacionalizar en forma efectiva estas acciones.

En el Código Orgánico Integral Penal, se tipifican algunos delitos informáticos, constituyendo un respaldo que permite judicializar a los

responsables del cometimiento de este tipo de delitos y a la vez un elemento disuasivo para limitar su cometimiento dentro del territorio nacional.

En el Plan Nacional de Seguridad Integral, se consideran los nuevos desafíos que han surgido en materia de seguridad, gracias a la rápida evolución de las TICs, dejando al descubierto vulnerabilidades tanto para las instituciones del Estado como para toda la población, que se encuentran expuestos ante ataques que se puedan producir por el mal uso del ciberespacio. (Ministerio de Defensa Nacional., 2019).

El Ministerio de Defensa nacional mediante el Acuerdo Ministerial 281 en el año 2014 crea el Sistema de Ciberdefensa del MIDENA y el Comando de Ciberdefensa (COCIBER), órganos asesores que hasta el momento están materializados, pero no en su totalidad principalmente por falta de medios tecnológicos.

En la Política de la Defensa Nacional, se consideran diversas amenazas existentes entre ellas los ciberataques, los mismos que emplean diferentes formas de proceder empleando redes y sistemas de transmisión de datos que han generado diversas aristas de amenazas que se producen en el ciberespacio (Ministerio de Defensa Nacional., 2019); que tienen la capacidad de afectar seriamente el funcionamiento de las áreas y sectores estratégicos del Estado, siendo responsabilidad de las FF.AA implementar políticas, estrategias y fomentar capacidades para la ciberseguridad/ciberdefensa. (Ministerio de Defensa Nacional, 2018).

Las Fuerzas Armadas a través del COCIBER ejecutan operaciones de apoyo a la defensa de la soberanía e integridad territorial en el ciberespacio, con

los medios y capacidades existentes, siendo una difícil tarea que requiere mayor esfuerzo profesional debido a la limitación en medios tecnológicos.

El Sistema Nacional de Inteligencia tiene la responsabilidad de identificar las amenazas que atentan contra la integridad del estado, sin embargo, aún no se han definido cuales serían las ciberamenazas que pueden actuar dentro del territorio nacional, las mismas que serían el punto de partida para optimizar y mejorar la planificación y conducción de las operaciones militares de ciberdefensa.

Del estudio realizado podemos darnos cuenta que si bien el marco legal no es específico existen disposiciones en las leyes y políticas, tendientes a la protección y vigilancia del ciberespacio, que son operacionalizadas en los diferentes niveles, pero la cultura de ciberseguridad y ciberdefensa debe ser una responsabilidad desde el más alto nivel, por lo que se vuelve sumamente necesario que se trabaje y promulgue una ley en la que se cree un Sistema de Ciberseguridad y se emitan las responsabilidades correspondientes a todas las instituciones públicas y privadas para implementar la ciberseguridad y ciberdefensa según corresponda y se garantice la asignación de los recursos necesarios para este cometido..

Conclusiones Parciales.

- El marco legal vigente en el país, no es muy específico en lo referente al ciberespacio, sin embargo, garantiza la protección de la información y privacidad de las personas, además de la vigilancia y protección del ciberespacio, lo que ha permitido que el MIDENA y las Fuerzas Armadas, estructuren un Sistema de Ciberdefensa para cumplir este cometido.

- Dada la poca especificidad que tiene el marco legal en lo referente a ciberdefensa, esta no ha sido considerada como un objetivo nacional actual y por ende no existen los recursos necesarios para la implementación y eficiente funcionamiento del Sistema de Ciberdefensa Militar, lo que ha demorado su implementación principalmente debido a la falta de tecnología.
- El Sistema nacional de inteligencia aún no define las ciberamenazas que tienen mayor probabilidad de cometer ciberdelitos en el país, siendo este el primer paso para optimizar y mejorar la planificación y conducción de las operaciones militares de ciberdefensa.
- La cultura de ciberseguridad y ciberdefensa debe ser una responsabilidad del Estado, siendo necesario que se trabaje y promulgue una ley en la que se cree un Sistema de Ciberseguridad y se enlisten las responsabilidades correspondientes a todas las instituciones públicas y privadas para implementar la ciberseguridad y ciberdefensa según corresponda y se garantice la asignación de los recursos necesarios para este cometido.

Determinar que amenazas cibernéticas, afectarían la conducción de las operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna.

Las ciberamenazas se definen como posibilidades de cualquier tipo de que un evento o acción ocurra afectando la confidencialidad, integridad, disponibilidad y autenticidad de la información, ante los eventos suscitados durante el mes de octubre del 2019, el manejo de la información, su correcta difusión y el mal uso o tergiversación de la misma por parte de grupos de troles (cibernautas sin ética, que difundieron información falsa, con el objetivo de enardecer a la población e incitarla a atacar a las Fuerzas Militares y Policiales

que proporcionaban seguridad en instalaciones de importancia para mantener la continuidad del Gobierno y proveer de los servicio esenciales que requiere la población, e incluso un caso inédito como intentos de ingresar a la fuerza a las unidades militares, esto dio como resultado heridos de ambos bandos y destrucción de gran cantidad de material y medios militares.

Con este antecedente surge la necesidad de determinar cuáles son las Ciberamenazas, que ponen en peligro la conducción de las operaciones militares al proporcionar apoyo a la P.N en Operaciones de Respuesta a Crisis, para a considerar los controles y procedimientos necesarios en futuros procesos de planificación y conducción de este tipo de operaciones.

Para conocer el hecho, debemos partir de que no solo el ciberespacio trata de internet si no que en el mismo se encuentran inmiscuidos gran cantidad de redes de información a nivel mundial y además se suman todas las que se conectan a estas y desde donde se controlan. (Ampudia & Tapia, 2017)

Una amenaza es aquella situación en la que se tiene la certeza de que un tercero pueda causar daño y es causada por un actor frente a su manifestación. (Ministerio de Defensa Nacional, 2018) El Sistema Nacional de Inteligencia requiere que su esfuerzo sea orientado a identificar estas múltiples amenazas que atentan a la seguridad de las instituciones y por ende del Estado mismo. (Ministerio de Defensa Nacional, 2018)

Dentro de las Políticas y Estrategias de la defensa la Política 4 se refiere a “Proteger la información estratégica del estado, en materia de defensa” (Ministerio de Defensa Nacional, 2018):

1. Protección de todo lo que envuelve el uso de redes informáticas, sistemas de comunicaciones destinados para fines de defensa. (Ministerio de Defensa Nacional, 2018)
2. Desarrollar la capacidad de Ciberdefensa. (Ministerio de Defensa Nacional, 2018)
3. Hace referencia a integrar los diferentes sistemas de defensa electrónica tanto de instituciones públicas como privadas que permitan afrontar los diferentes riesgos y ciberamenazas que puedan causar afectación al Estado. (Ministerio de Defensa Nacional, 2018)

En los años 50, la palabra ciber se utilizaba para referirse a elementos cibernéticos, o la ciencia que entiende el control y movimiento de animales y máquinas. Poco después, este término se convirtió en un sinónimo de 'computarizado'. (Poggi, 2018)

En los años noventa llegó un nuevo término relacionado: el ciberespacio. Define así un espacio físico inventado que algunas personas creían que existía detrás de la electrónica de un computador. (Poggi, 2018)

Como riesgos en la Política de la Defensa Nacional, se definen a las: situaciones y fenómenos latentes, de origen natural o antrópico, que pueden afectar a las instituciones y a los ciudadanos causando graves daños de consecuencias inmedibles. (Ministerio de Defensa Nacional, 2018). Su carácter de permanencia e inevitabilidad constituyen un referente para la elaboración de planes que permitan gestionar sus probables consecuencias (Ministerio de Defensa Nacional, 2018). Los riesgos causados por el ser humano pueden configurar amenazas una vez que se ha identificado su motivación, la intención y

la capacidad para afectar a la seguridad pública y del Estado. (Ministerio de Defensa Nacional, 2018)

Las Ciberamenazas, las podríamos definir como todo acto que se pueda realizar en el dominio del ciberespacio, que pretenda disponer de aquella información que se transmite en el mismo para estar en condiciones de cometer actos fuera de la ley como delitos informáticos, ciberataques, entre otros.

El Código Orgánico Integral Penal (Tapia, 2018), dentro de sus enumeraciones ya tipifica varios delitos informáticos que se desenvuelven en el dominio del ciberespacio como el abuso de menores mediante la pornografía infantil, la violación del derecho a la intimidad que cada persona debe gozar, la revelación ilegal de información de bases de datos que genera grandes ingresos para los delincuentes informáticos, la interceptación de comunicaciones que en nuestro caso vulnera la seguridad de las operaciones, diferentes técnicas de ingeniería social como el pharming, phishing, fraude informático con grandes pérdidas para las instituciones bancarias, ataque a la integridad de sistemas informáticos como centros de datos, ingresos no consentidos a diferentes sistemas digitales. (Tapia, 2018)

En Ecuador no existe una clasificación definida de cuáles son las ciberamenazas que actúan en contra del Estado ecuatoriano, por lo que como resultado de la investigación bibliográfica realizada pondremos a consideración la información obtenida a fin de determinar que ciberamenazas podrían actuar en el cometimiento de ciberdelitos en nuestro país:

Según los resultados de la Encuesta Global de Seguridad de la Información período 2018-2019, los problemas cibernéticos más críticos

consideran al phishing (fraude electrónico) y malware como puntos de partida. Los ataques que se enfocan en el rango de disrupción se colocan en el tercer lugar de la lista, seguidos por ataques con un enfoque en robar dinero. A pesar de que se ha discutido mucho sobre las amenazas internas y las patrocinadas por entidades del gobierno, el miedo por los ataques internos se encuentra octavo en la lista mientras que el espionaje se encuentra al final. (EYGM Limited, 2019, pág. 22)

Tabla 3

Las 10 mayores amenazas cibernéticas para las organizaciones

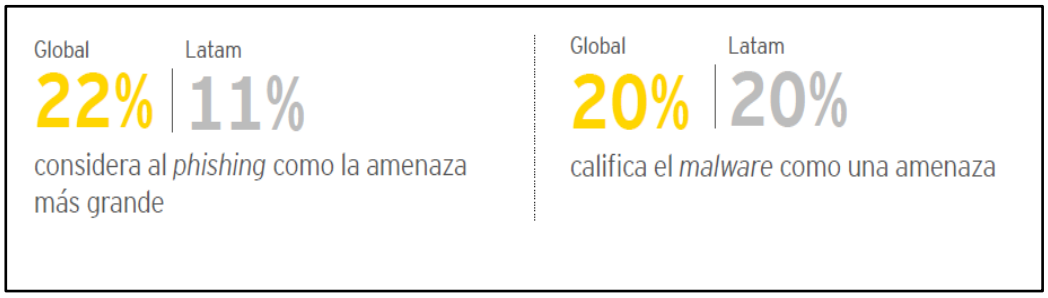
Los 10 tipos de información más valiosos para los crímenes cibernéticos	Las 10 mayores amenazas cibernéticas para las organizaciones
1. Información del cliente (17%)	1. *Phishing* (22%)
2. Información financiera (12%)	2. *Malware* (20%)
3. Planes estratégicos (12%)	3. Ataques cibernéticos (para interrumpir operaciones) (13%)
4. Información del Directorio (11%)	4. Ataques cibernéticos (para robar dinero) (12%)
5. Contraseñas del cliente (11%)	5. Fraude (10%)
6. Información de I&D (9%)	6. Ataques cibernéticos (para robar IP) (8%)
7. Información de fusiones y adquisiciones (8%)	7. *Spam* (6%)
8. Propiedad intelectual (6%)	8. Ataques internos (5%)
9. IP no patentada (5%)	9. Desastres naturales (2%)
10. Información de proveedores (5%)	10. Espionaje (2%)

Nota: Encuesta Global de Seguridad de la Información período 2018-2019

Según la misma encuesta el 20 % de la población Latinoamericana califica al malware como una amenaza y el 11 % considera al phishing como la amenaza más grande.

Figura 17

Las 2 principales amenazas cibernéticas en Latinoamérica

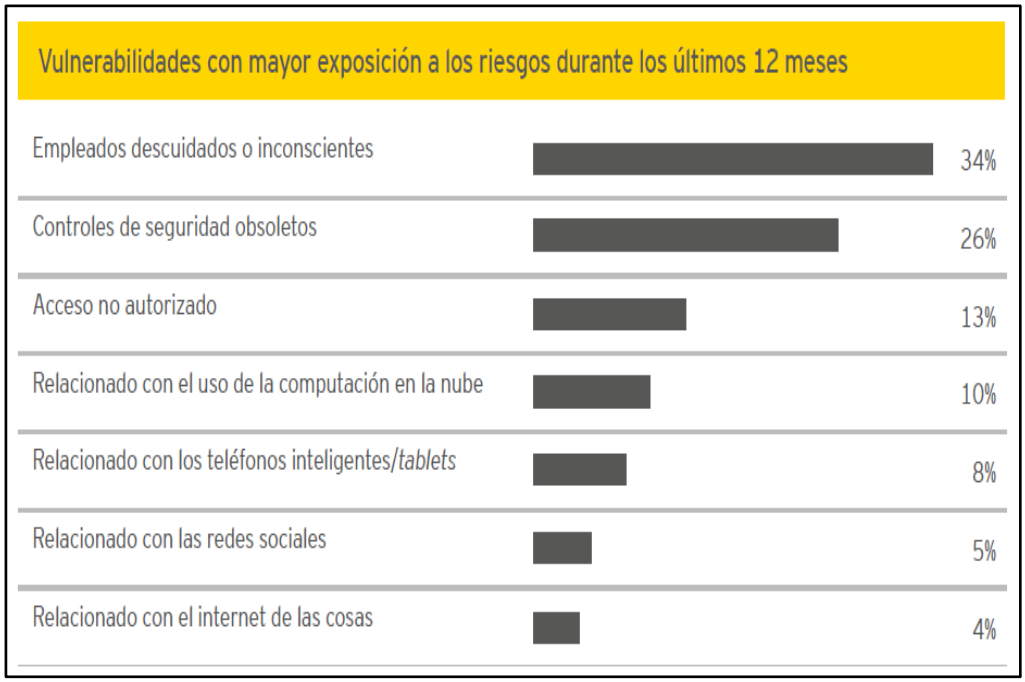


Nota: Encuesta Global de Seguridad de la Información período 2018-2019

Otro punto que se considera importante en esta encuesta son las Vulnerabilidades con mayor exposición a los riesgos durante los últimos 12 meses:

Tabla 4

Las 10 mayores vulnerabilidades cibernéticas para las organizaciones



Nota: Encuesta Global de Seguridad de la Información período 2018-2019

El Comando de Ciberdefensa incluye: el spoofing, phishing, pharming, hijacking, tampering, cracking, mitm e Ingeniería Social y también considera su uso como parte de las operaciones de Ciberdefensa. (Comando de Ciberdefensa, 2019)

Finalmente, del análisis de los acontecimientos suscitados en octubre del 2019 y sus posteriores consecuencias, se desprende que el uso malintencionado o manipulación de la opinión pública sobre las plataformas de medios sociales se ha convertido en una amenaza crítica, que debe ser considerada como un factor esencial dentro de la planificación de las operaciones de respuesta a crisis en apoyo a la Policía Nacional ante grave conmoción interna.

Considerando el análisis de los datos obtenidos en la investigación bibliográfica realizada nos permitimos plantear las siguientes amenazas cibernéticas que deben ser consideradas para la planificación y conducción de las operaciones militares y que justifican la necesidad de la creación de un Órgano de Ciberdefensa en la Fuerza Terrestre:

Tabla 5

Amenazas cibernéticas en Ecuador

AMENAZAS CIBERNÉTICAS EN ECUADOR		
AMENAZA	**DEFINICIÓN**	**EMPLEO DE LA CIBERDEFENSA**
Phishing	Mediante esta amenaza se tiene la capacidad de obtener información personal como usuarios, contraseñas, información personal de tarjetas de crédito, bancarias para cometer delitos. **Fuente especificada no válida.**	Operaciones de Defensa

Malware	Amenazas informáticas o software hostil, cómo: virus, gusanos, troyanos, keyloggers, botnets, spyware, adware, ransomware y sacareware.	Operaciones de Defensa
Ataques Cibernéticos (para robar IP)	Es cualquier tipo de acción ofensiva que se dirige a los sistemas informáticos de información, infraestructuras, redes informáticas o dispositivos informáticos personales, utilizando diversos métodos para robar, alterar o destruir datos o sistemas de información.	Operaciones de Defensa
Ataques Internos	Aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, esto con fin de obtener un beneficio, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.	Operaciones de Defensa, Exploración
Ciberespionaje	Acto que se realiza a través de los ordenadores y de la red mediante diferentes técnicas de craqueo y tras ciertas prácticas destinadas a la sustracción de información.	Operaciones de Defensa, Exploración
Ciberterrorismo	Emplea diferentes fuentes abiertas y cerradas para obtener información que le permita causar caos, daño, miedo a las víctimas. **Fuente especificada no válida.**	Operaciones de Defensa, Exploración
Spoofing	Amenaza que tiene que ver con la suplantación de identidad por medio del uso de redes para causar perjuicios a las personas que han sido víctimas.	Operaciones de Defensa

Hijacking	Secuestro, en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo por parte de un atacante.	Operaciones de Defensa
Tampering	Manipulación, manoseo, intromisión, en aplicaciones web para modificar los parámetros que se envían al servidor web como puntos de entrada de la aplicación, ya sea los que viajan en los formularios o en la propia URL.	Operaciones de Defensa
Cracking	Modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad y adware.	Operaciones de Defensa, Exploración
MitM	Man-in-the-middle (hombre-en-el medio) es un tipo de ataque informático en el que el atacante tiene conexiones independientes con las víctimas y trasmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante.	Operaciones de Defensa, Exploración
Ingeniería Social	Técnica usada para obtener información, acceso o permisos en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos.	Operaciones de Defensa

Manipulación de la opinión pública sobre las plataformas de medios sociales	Explotar las plataformas de medios sociales para difundir noticias basura y desinformación, ejercer censura y control, y socavar la confianza en los medios, las instituciones públicas y la ciencia.	Operaciones de Defensa, Exploración, Respuesta

Nota: COCIBER 2019

Conclusiones Parciales.

- En una época marcada por la Globalización y el auge de las TICs, se generan escenarios VICA (volátiles, inciertos, complejos y ambiguos), donde actúan amenazas híbridas que mutan o evolucionan aceleradamente, generando una demanda de seguridad por parte de las sociedades, que obliga a la tecnificación de todos los elementos del estado a fin de mantener la capacidad de garantizar el desarrollo en un ambiente de seguridad y confianza.
- En al ámbito de la Ciberdefensa, las ciberamenazas representan un grave problema, para la seguridad de las personas, grupos, instituciones y del mismo estado, ya que pueden actuar desde el otro lado del planeta o desde un sótano, cometiendo ciber delitos, cuyas consecuencias afectan la integridad de la información, de las personas y la seguridad de las empresas e instituciones del estado.
- Existe una demanda creciente de seguridad contra los delitos que se cometen en el ciberespacio, recayendo esta responsabilidad en el estado, que debe proporcionar los recursos necesarios para que sus Fuerzas Armadas adquieran la capacidad (conocimiento, entrenamiento y tecnología)

de realizar Operaciones de Ciberdefensa, que protejan el quinto dominio y apoyen la planificación y conducción de las operaciones militares.

- El Comando de Ciberdefensa del COMACO, es un órgano planificador ejecutor del nivel estratégico militar; lo que conlleva a la necesidad de crear un Órgano de Ciberdefensa para la Fuerza Terrestre para que en base a las ciber amenazas determinadas, asesore a los niveles operativo y táctico, para el empleo de la Ciberdefensa en la planificación y conducción de las operaciones militares.
- La manipulación de la opinión pública sobre las plataformas de medios sociales, debe ser considerada como la principal amenaza para la planificación y conducción de las operaciones militares, debiendo determinarse las tácticas, técnicas y procedimientos que emplean los troles, a fin de neutralizar sus acciones, sobre todo cuando existen situaciones de conflictividad social o grave alteración del orden público.
- Se deben contar con procedimientos y medidas de seguridad para aumentar la seguridad en el manejo de la información clasificada de todas las unidades del Ejército para evitar ataques internos y acciones de ciberespionaje, que pueden poner en peligro la conducción de las operaciones o encubrir robo de armamento y material.

Demostrar la necesidad de crear un Órgano Asesor de Ciberdefensa en la Fuerza Terrestre, para apoyar la planificación y conducción de las operaciones en los niveles operativo y táctico.

Vamos a partir mencionando que un órgano de ciberdefensa constituye una estructura técnica especializada, que tiene la capacidad de ejecutar

operaciones en el ciberespacio con la finalidad de proteger sus activos de información digital, sistemas de mando y control, infraestructura crítica, aplicaciones, y demás relacionados, de amenazas cibernéticas; de manera similar el aumento del uso de las redes sociales ha hecho de este medio un sistema muy apetecido para generar desestabilización y crear caos por el mal uso de la información, transmisión de información falsa, incitación a la violencia; acontecimientos que ha generado incertidumbre en la población, destrucción de bienes públicos y cuantiosas pérdidas económicas para el Estado, sin poder identificar a la persona, organización, que se encuentra detrás de todas estas actividades, las mismas que operan desde el anonimato.

Estas nuevas amenazas de carácter líquido, híbrido han generado que varios países a nivel mundial creen la necesidad de mejorar la seguridad en el ciberespacio, implementando capacidades de ciberdefensa como respuesta a estas amenazas difusas, mutantes y el Ecuador, específicamente la Fuerza Terrestre no debe ser la excepción ya que es un requerimiento prioritario para el apoyo a las diferentes operaciones terrestres que se ejecutan dentro de la misión fundamental de la Defensa del Territorio y la Integridad Territorial.

Para conocer el hecho, nos referiremos a la celebración del Foro Económico Mundial en enero del 2017, (Stoltenberg, 2017), donde el secretario general de la OTAN, afirmó que: “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” (TAPIA, 2018)

Ante esta problemática, la gran mayoría de países a nivel mundial, han implementado dentro de sus organizaciones y principalmente en los entes responsables de la defensa nacional, estructuras con capacidades técnicas y

personal especializado, que permitan mantener un control del gran espectro que representa el mal uso del ciberespacio, a nivel mundial podemos citar entre otros a Estados Unidos con el Comando Cibernético y sus comandos cibernéticos en cada una de sus fuerzas terrestre, naval y aérea, Canadá con el Centro de Respuestas a Incidentes Informáticos, Brasil con el Centro de Defensa Cibernética, Argentina con el Comando Conjunto de Ciberdefensa, Perú con el Comando Operacional del Ciberespacio, potencias como China, Rusia, etc.

Con todo este ambiente, nos podemos dar cuenta que este escenario líquido, requiere ser considerado dentro de un ambiente estratégico, operativo y táctico en razón que las operaciones de ciberdefensa deben ejecutarse de manera permanente en apoyo a las diferentes operaciones, manteniendo medidas permanentes de prevención, mitigación, control y protección que nos permitan hacer frente a las diferentes ciber amenazas, ciber ataques con capacidad de afectar a nuestros centros de mando y control, infraestructura crítica digital, así como también reaccionar ante el mal uso de las redes sociales por cualquier tipo de aplicación, generando respuesta inmediata con el fin de evitar que por influencia de las mismas se eleven los actos violentos ante crisis que se puedan generar en el país provocando caos, pérdidas humanas, económicas y que atenten a la seguridad nacional; claro ejemplo el que se evidenció en el mes de octubre de 2019, donde se requirió el empleo de la Fuerza Terrestre ejecutando operaciones de Respuesta a Crisis en apoyo a la P.N, donde se pudo constatar la gran cantidad de información falsa que se difundió a través del ciberespacio en las diferentes redes sociales como Whatsapp, Instagram, Facebook, que alentaba a la población en general a realizar acciones violentas que no fueron contempladas en la planificación de las

unidades militares; dejando al descubierto la necesidad de contar con un órgano de Ciberdefensa que pueda asesorar y apoyar a los diferentes niveles, en la toma de decisiones y conducción de las operaciones para neutralizar y/o minimizar los efectos de esta malintencionada información, al final de las manifestaciones el saldo involucra muertos, heridos, cuantiosas pérdidas económicas, destrucción de gran cantidad del centro histórico de Quito, incendio de instalaciones, entre otros.

Las operaciones de Ciberdefensa pueden servir como apoyo en la conducción diferentes operaciones terrestres, siendo necesario tener una visión general de las estructuras de diferentes organismos de ciberdefensa, que nos permitirán enfocar nuestra solución de acuerdo a la realidad del país.

Hoy por hoy la Fuerza Terrestre está ingresando a un proceso de transformación institucional que involucra necesariamente el alcanzar nuevas capacidades, disponer de una normativa legal que permita la ejecución de operaciones en el ámbito pertinente con seguridad y además la capacitación permanente de su personal en las diferentes áreas operativas, por lo que resulta prioritario que la fuerza disponga de un organismo de ciberdefensa que tenga la capacidad de prevenir y ejecutar operaciones en el ciberespacio de acuerdo a las diferentes amenazas cibernéticas que intenten causar daños en la infraestructura crítica digital como centros de mando y control, sistemas de radares, sistemas de comunicaciones, páginas y aplicaciones web institucionales, robo de información, entre otros; con personal técnico y especialista en ciberseguridad y ciberdefensa y áreas a fines a la seguridad de la información, con un alto compromiso por la institución, evitando la rotación del personal, con procesos que permitan dar un adecuado y oportuno tratamiento a

los incidentes de seguridad informática, manteniendo una relación estrecha con la academia y diferentes comunidades y centros especializados a nivel nacional e internacional, que permitan el intercambio de información y conocimiento para poder asegurar las diferentes áreas, generando doctrina y procesos de capacitación continua que permita estar a la par de los avances tecnológicos y no exista discontinuidad en el uso de herramientas, con gran capacidad de ejecutar operaciones de inteligencia y búsqueda de información por fuentes abiertas; todo esto permitirá que las operaciones de ciberdefensa puedan apoyar de manera transversal a la planificación y ejecución de las operaciones terrestres ya sea en el ámbito interno o externo, cumpliendo así de manera permanente con la misión de Fuerzas Armadas.

Conclusiones Parciales

- Actualmente la Fuerza Terrestre se encuentra en una indefensión, en razón de que puede ser víctima de ciberataques, ciberespionaje y un sin número de amenazas cibernéticas, por lo que es fundamental contar con un organismo que permita el control y defensa del ciberespacio.
- La creación de un organismo de ciberdefensa permitirá adquirir una nueva capacidad, que contribuirá de manera directa al proceso de transformación de la Fuerza Terrestre.

Conclusiones Generales

- El marco legal vigente en el país, no es muy específico en lo referente al ciberespacio, sin embargo, garantiza la protección de la información y privacidad de las personas, además de la vigilancia y protección del ciberespacio, lo que ha permitido que el MIDENA y las Fuerzas Armadas, estructuren un Sistema de Ciberdefensa para cumplir este cometido.

- Dada la poca especificidad que tiene el marco legal en lo referente a ciberdefensa, esta no ha sido considerada como un objetivo nacional actual y por ende no existen los recursos necesarios para la implementación y eficiente funcionamiento del Sistema de Ciberdefensa Militar, lo que ha demorado su implementación principalmente debido a la falta de tecnología.
- El Sistema nacional de inteligencia aún no define las ciberamenazas que tienen mayor probabilidad de cometer ciberdelitos en el país, siendo este el primer paso para optimizar y mejorar la planificación y conducción de las operaciones militares de ciberdefensa.
- La cultura de ciberseguridad y ciberdefensa debe ser una responsabilidad del estado, siendo necesario que se trabaje y promulgue una ley en la que se cree un Sistema de Ciberseguridad y se enlístenlas responsabilidades correspondientes a todas las instituciones públicas y privadas para implementar la ciberseguridad y ciberdefensa según corresponda y se garantice la asignación de los recursos necesarios para este cometido.
- En una época marcada por la Globalización y el auge de las TICs, se generan escenarios VICA (volátiles, inciertos, complejos y ambiguos), donde actúan amenazas híbridas que mutan o evolucionan aceleradamente, generando una demanda de seguridad por parte de las sociedades, que obliga a la tecnificación de todos los elementos del estado a fin de mantener la capacidad de garantizar el desarrollo en un ambiente de seguridad y confianza.
- En al ámbito de la Ciberdefensa, las ciberamenazas representan un grave problema, para la seguridad de las personas, grupos, instituciones y del mismo estado, ya que pueden actuar desde el otro lado del planeta o desde

un sótano, cometiendo ciber delitos, cuyas consecuencias afectan la integridad de las personas y la seguridad de las empresas e instituciones del Estado.

- Existe una demanda creciente de seguridad contra los delitos que se cometen en el ciberespacio, recayendo esta responsabilidad en el estado, que debe proporcionar los recursos necesarios para que sus Fuerzas Armadas adquieran la capacidad (conocimiento, entrenamiento y tecnología) de realizar Operaciones de Ciberdefensa, que protejan el quinto dominio y apoyen la planificación y conducción de las operaciones militares.
- El Comando de Ciberdefensa del COMACO, es un órgano planificador ejecutor del nivel estratégico militar; lo que conlleva a la necesidad de crear un Órgano de Ciberdefensa para la Fuerza Terrestre para que en base a las ciber amenazas determinadas, asesore a los niveles operativo y táctico, para el empleo de la Ciberdefensa en la planificación y conducción de las operaciones militares.
- La manipulación de la opinión pública sobre las plataformas de medios sociales, debe ser considerada como la principal amenaza para la planificación y conducción de las operaciones militares, debiendo determinarse las tácticas, técnicas y procedimientos que emplean los troles, a fin de neutralizar sus acciones, sobre todo cuando existen situaciones de conflictividad social o grave alteración del orden público.
- Se deben contar con procedimientos y medidas de seguridad para aumentar la seguridad en el manejo de la información clasificada de todas las unidades del Ejército para evitar ataques internos y acciones de

ciberespionaje, que pueden poner en peligro la conducción de las operaciones o encubrir robo de armamento y material.

- Las operaciones de Ciberdefensa pueden servir como apoyo en la conducción de diferentes operaciones terrestres, siendo necesario tener una visión general de las estructuras de diferentes organismos de ciberdefensa, que nos permitirán enfocar nuestra solución de acuerdo a la realidad del país.
- La Fuerza Terrestre está ingresando a un proceso de transformación institucional que involucra necesariamente el alcanzar nuevas capacidades, disponer de una normativa legal que permita la ejecución de operaciones en el ámbito pertinente con seguridad y además la capacitación permanente de su personal en las diferentes áreas operativas, por lo que resulta prioritario que la fuerza disponga de un organismo de ciberdefensa que tenga la capacidad de prevenir y ejecutar operaciones en el ciberespacio.

Capítulo V

Propuesta

La presente propuesta se fundamenta en la creación de un organismo asesor de ciberdefensa para la Fuerza Terrestre, que permita mejorar las capacidades de ciberdefensa en apoyo a la planificación y conducción de las operaciones terrestres, en el cual se definirán los procesos gobernantes, organización y la estructura orgánica básica, para una posterior implementación en la Fuerza Terrestre.

Desarrollo de la propuesta

Las estructuras generales de ciberseguridad y ciberdefensa de los países de la región, evidencian claramente la necesidad de contar con órganos, unidades de ciberdefensa dentro de las diferentes fuerzas terrestre, naval y aérea que apoyen a la planificación y conducción de las diferentes operaciones en el ámbito que corresponda y que sirvan de nexo y coordinación con la unidad rectora en este campo, refiriéndonos en nuestro caso al Comando de Ciberdefensa del Comando Conjunto.

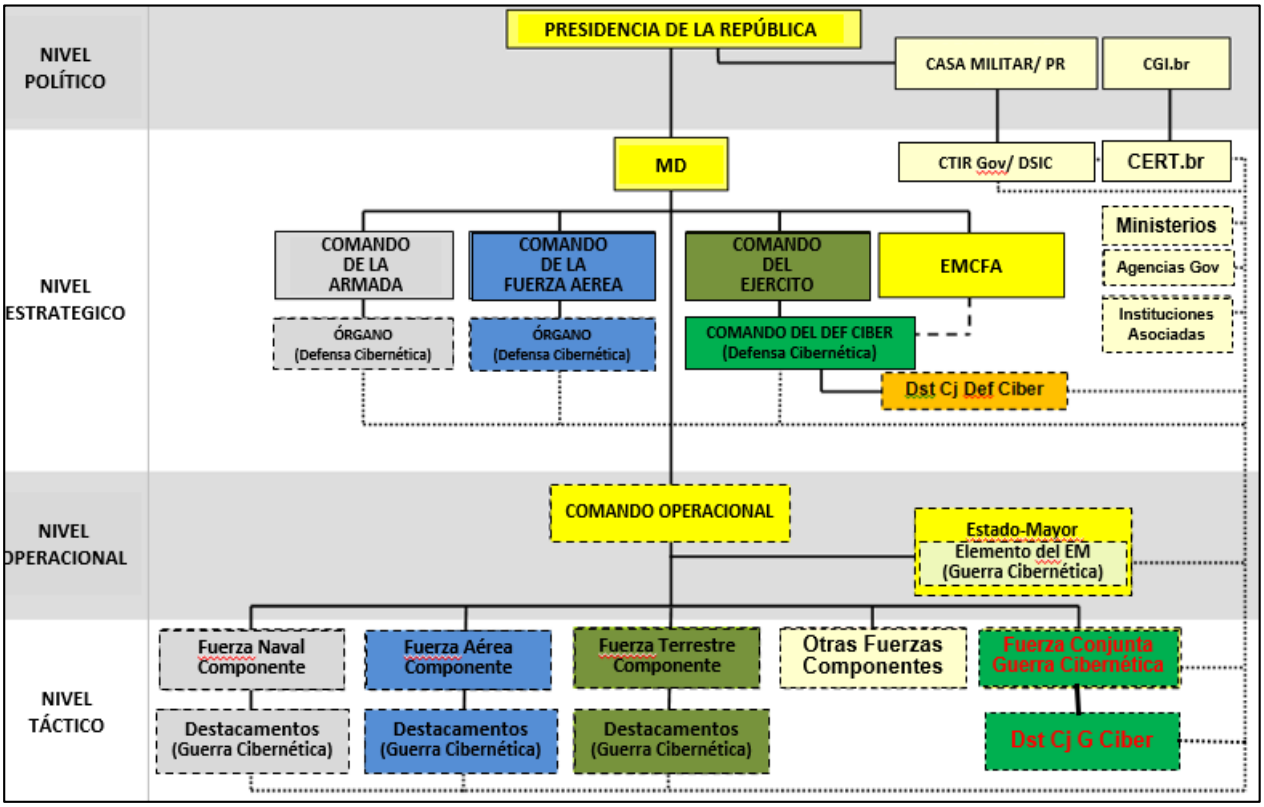
En Brasil, país referente en América por su capacidad y desarrollo en ciberseguridad y ciberdefensa, desde el nivel estratégico cada comando de fuerza cuenta con órganos de defensa cibernética y en el nivel operacional cada componente de fuerza dispone de destacamentos especializados en guerra cibernética con su respectiva Fuerza Conjunta de Guerra Cibernética.

A continuación, podemos observar la estructura y los diferentes órganos de ciberdefensa descritos, donde se puede evidenciar que es necesario contar

con un componente de ciberdefensa dentro de cada fuerza desde el nivel estratégico hasta el nivel táctico.

Figura 18

Estructuras y órganos del Sistema Militar de Defensa Cibernética

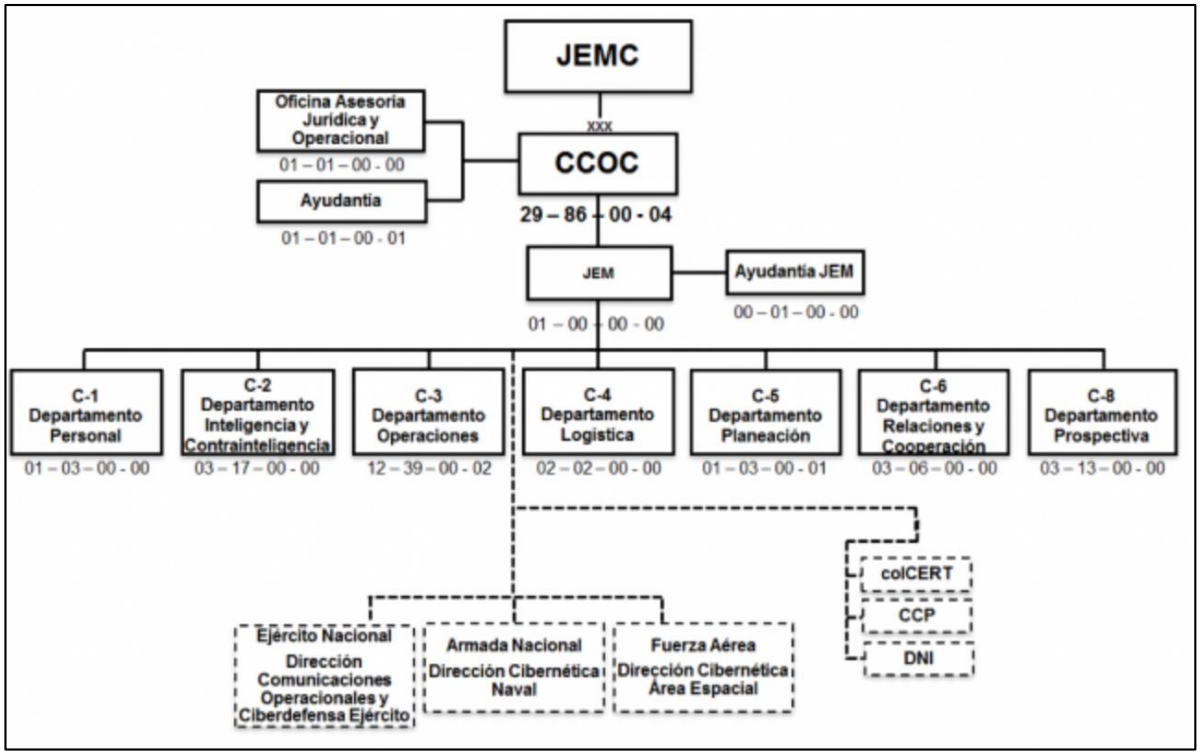


Nota: Ministerio de Defensa del Brasil, Inteligencia en Defensa Cibernética

Colombia dentro de su organización como ente rector cuenta con el Comando Conjunto Cibernético CCOC, entidad que gestionó la creación de las Unidades Cibernéticas del Ejercito Nacional, Armada Nacional y Fuerza Aérea Colombiana, con quienes ha consolidado su organización a fin de desarrollar las capacidades que permitan afrontar los nuevos desafíos impuestos.

Figura 19

Estructura orgánica del Comando Conjunto Cibernético



Nota: www.ccoc.mil.co/quines_somos/historia

La tendencia en la región es clara, lo que fundamenta la necesidad de la creación de un órgano de ciberdefensa en la Fuerza Terrestre que permita apoyar a la planificación y ejecución de operaciones bajo responsabilidad de la Fuerza Terrestre, por lo que es pertinente delinear aspectos relevantes de la organización que permitan tener una visión clara de las responsabilidades y atribuciones propias requeridas para un eficiente funcionamiento de esta entidad.

Procesos

Es necesario considerar las diferentes estructuras de ciberdefensa con los procesos que llevan a cabo para cumplir con las diferentes actividades

administrativas y operativas, en tal virtud tomamos como referencia a la organización del Comando de Ciberdefensa del Comando Conjunto con su mapa de procesos, que nos permite determinar los procesos que ejecutan las unidades de ciberdefensa.

Figura 20

Mapa de Macroprocesos del Comando de Ciberdefensa

Nota: Comando de Ciberdefensa, 2019

De acuerdo al mapa de macroprocesos se identifican los procesos gobernantes, sustantivos y adjetivos de esta unidad operativa, como se puede analizar los procesos que agregan valor a las unidades de ciberdefensa son la defensa, la exploración y la respuesta; operaciones que permiten mantener segura a las diferentes infraestructuras críticas digitales y poder ser alertados a tiempo ante posibles ciberataques que se puedan producir a nivel mundial por estados o grupos que operan al margen de la ley.

El proceso de defensa es aquel en el que se ejecutan medidas de prevención que garanticen la seguridad de las diferentes infraestructuras críticas

digitales, plataformas y equipos informáticos; detección de ciberataques, intrusiones, interrupciones, acciones hostiles deliberadas que atentan o comprometan los sistemas de información de la organización.

Las principales actividades que se realizan en el proceso de defensa son las siguientes:

- Concienciación en ciberseguridad.
- Planificar sitios WEB a ser monitoreados por su importancia.
- Configuración de herramientas y monitoreo de sitios WEB de la Fuerza Terrestre y sus unidades.
- Gestión de incidentes de seguridad informática mediante el registro, clasificación, priorización del incidente.
- Análisis Forense a través del registro, configuración de la herramienta a ser empleada e informe.
- Alerta temprana ante posibles ciberataques.
- Entrenamiento.

El proceso de exploración busca obtener información sobre capacidades cibernéticas de posibles adversarios, agentes hostiles y de nuestras propias redes.

El proceso de exploración cumple con las actividades que se detallan a continuación:

- Estudios de seguridad informática mediante análisis de vulnerabilidades, test de penetración, hackeo ético e informe.
- Realizar el Plan de búsqueda de cibertinteligencia.
- Ejecutar el ciclo de análisis y producción de ciberinteligencia.

- Obtener información de amenazas en el ciberespacio.
- Simulación de eventos que puedan afectar la infraestructura crítica digital.
- Entrenamiento.

El proceso de respuesta ejecuta acciones de carácter ofensivo de acuerdo al ciberataque o amenaza que ya ha sido perpetrada para contrarrestar, neutralizar, interrumpir o destruir los agentes hostiles.

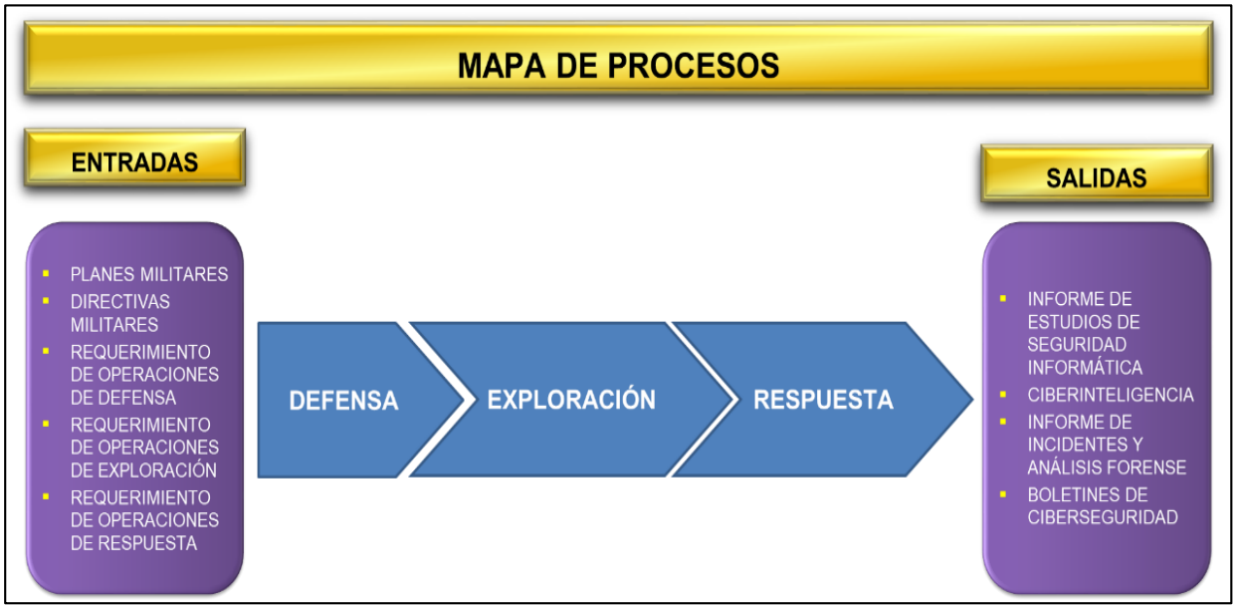
El proceso de respuesta ejecuta las siguientes actividades:

- Emitir directrices y lineamientos para la orden de operaciones.
- Reconocimiento y selección del objetivo.
- Analizar las herramientas ofensivas.
- Transmitir, comandar y controlar código malware.
- Explotar vulnerabilidades.
- Ejecutar operaciones ofensivas
- Desarrollo de ciberherramientas mediante el levantamiento de requerimientos, elaboración del diseño, desarrollo del prototipo, pruebas, validación y producción.
- Entrenamiento.

El organismo de ciberdefensa de la Fuerza Terrestre, presentaría el siguiente mapa de procesos:

Figura 21

Mapa de procesos del organismo de ciberdefensa para la F.T



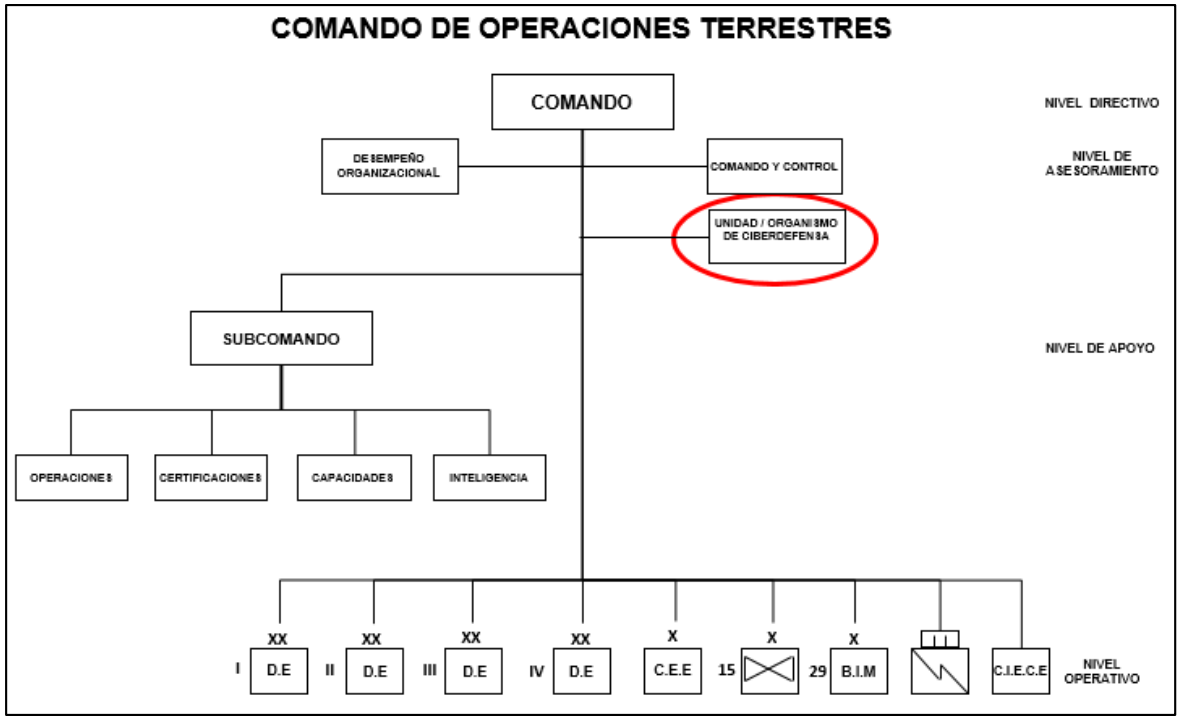
Estructura

Las unidades de ciberdefensa son entidades responsables de ejecutar operaciones militares, como se ha podido evidenciar en las estructuras de otros países, razón por la cual es pertinente que la unidad de ciberdefensa debe encuadrarse bajo un mando operativo, ya que estas operaciones servirán de apoyo a las diferentes operaciones terrestres que se vayan a planificar y ejecutar por las diferentes unidades, por tal razón deberá estar bajo el mando del Comando de Operaciones Terrestres.

Por consiguiente, es necesario realizar una modificación a la estructura actual del Comando de Operaciones Terrestres, como se puede observar en la propuesta a continuación:

Figura 22

Propuesta de estructura del Comando de Operaciones Terrestres



Considerando que la Fuerza Terrestre actualmente no dispone de unidad de ciberdefensa y existe un mínimo nivel de conocimiento y madurez en esta área, es necesario plantear una estructura orgánica que permita sanear y mejorar estos niveles, estableciendo las principales áreas con las que se debe contar para un normal desempeño de las diferentes funciones y por ende para la planificación y ejecución de las distintas operaciones de ciberdefensa.

Nivel Directivo

- Comando

Entidad responsable de la conducción de las operaciones de ciberdefensa.

Nivel de planificación y asesoramiento

- Planificación

  Entidad responsable de delinear la planificación de la unidad y desarrollo de acuerdo a las necesidades actuales y futuras.

  Nivel de operaciones

Nivel operativo

- Operaciones de defensa

  Entidad destinada a la planificación y ejecución de las diferentes operaciones de ciberdefensa; dentro de las actividades principales que se cumplirán en esta área tenemos: configuración de herramientas y monitoreo, gestión de incidentes de seguridad informática, análisis forense de dispositivos, alerta temprana ante posibles ciberataques a la infraestructura digital, elaboración de informes afines al área.

- Operaciones de exploración

  Entidad destinada a la planificación y ejecución de las diferentes operaciones de ciberexploración; dentro de las actividades principales que se cumplirán en esta área tenemos: obtener información de amenazas en el ciberespacio, ejecutar el ciclo de análisis y producción de ciberinteligencia, estudios de seguridad informática, simulación de eventos, elaboración de informes afines al área.

- Operaciones de respuesta

  Entidad destinada a la planificación y ejecución de las diferentes operaciones de ciberrespuesta; dentro de las actividades principales que se cumplirán en esta área tenemos: diseño y desarrollo de ciberarmas, explotación de vulnerabilidades.

De acuerdo a lo acotado, el organigrama para la estructura propuesta de la unidad / organismo de ciberdefensa para la Fuerza Terrestre, se muestra a continuación:

Figura 23

Propuesta de estructura de la unidad de ciberdefensa

Unidad de ciberdefensa

Responsabilidad principal

Ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio, responder ante incidentes o amenazas que atenten a la infraestructura digital de la Fuerza Terrestre y apoyar a la planificación de las operaciones terrestres.

Responsabilidades

- Planificar, ejecutar y conducir operaciones en el ciberespacio.
- Planificar, ejecutar y conducir operaciones de ciberdefensa en apoyo a las operaciones terrestres.

- Brindar asesoramiento al comandante del Comando de Operaciones Terrestres en temas de ciberdefensa.
- Mantener estrecha relación y coordinación con el Comando de Ciberdefensa del Comando Conjunto para la ejecución de los diferentes planes y directivas.
- Generar ciberinteligencia que permita la toma oportuna de decisiones.
- Mantener el control de los sistemas de información e infraestructura digital mediante el monitoreo permanente.

Departamento de defensa

Responsabilidad principal

Efectuar operaciones de defensa en forma permanente de la infraestructura crítica digital de la Fuerza Terrestre, mediante medidas de prevención, detección frente a acciones hostiles deliberadas.

Responsabilidades

- Preservar la integridad, confidencialidad y disponibilidad de la información.
- Proteger los datos, redes de comunicaciones, sistemas de mando y control, infraestructura crítica digital, radares, entre otros.
- Ejecutar campañas de concienciación en ciberseguridad.
- Protección de accesos indebidos a las redes informáticas.
- Detección de la presencia de elementos no autorizados en las redes institucionales.
- Planificar de acuerdo a la importancia sitios WEB a ser monitoreados de manera permanente de la Fuerza Terrestre.
- Ejecutar Análisis Forense de dispositivos.

- Gestión de incidentes de seguridad informática mediante el registro, clasificación, priorización del incidente.
- Remediar incidentes informáticos en el sitio.
- Realizar el robustecimiento de las infraestructuras críticas digitales.
- Detección de intrusos o accesos no autorizados.
- Alerta temprana ante posibles ciberataques.
- Elaborar los informes correspondientes afines al área
- Capacitación y entrenamiento del personal.

Departamento de exploración

Responsabilidad principal

Efectuar operaciones de ciberinteligencia en forma permanente a fin obtener información de capacidades cibernéticas que pueden ser empleadas por agentes hostiles.

Responsabilidades

- Ejecutar el ciclo de análisis y producción de ciberinteligencia.
- Ejecutar estudios de seguridad informática.
- Obtener información de amenazas en el ciberespacio.
- Obtener información de objetivos en fuentes abiertas y cerradas de información.
- Ejecutar análisis de vulnerabilidades a las diferentes redes y sistemas de la Fuerza Terrestre.
- Ejecutar pruebas de penetración en los sistemas informáticos.

- Simular eventos que puedan afectar la infraestructura crítica digital de la Fuerza Terrestre.
- Elaborar los informes correspondientes afines al área
- Capacitación y entrenamiento del personal.

Departamento de respuesta

Responsabilidad principal

Ejecutar acciones de respuesta de carácter ofensivo de acuerdo a la situación; neutralizando, destruyendo amenazas, ciberataques generados por elementos hostiles.

Responsabilidades

- Reconocimiento y selección de objetivos.
- Identificar la fuente u origen de la amenaza.
- Ejecutar acciones de degradación, interrupción, daños a la integridad de la información.
- Analizar herramientas ofensivas.
- Explotar vulnerabilidades.
- Desarrollar ciberarmas mediante investigación y desarrollo.
- Elaborar los informes correspondientes afines al área
- Capacitación y entrenamiento del personal.

Orgánico estructural y numérico

Establecida la propuesta para la creación de un organismo/unidad de ciberdefensa, con su estructura, procesos que se deben desarrollar, responsabilidades, actividades; resulta pertinente hacer el levantamiento del

orgánico provisional de esta entidad, que permitan un desarrollo eficiente y cumplimiento de las misiones asignadas, obteniendo los resultados que permitan al mando tomar las mejores decisiones; a continuación, se presenta la propuesta del orgánico de la Unidad de Ciberdefensa:

Tabla 6

Propuesta del Organismo de Ciberdefensa para el Ejército

UNIDAD DE CIBERDEFENSA DE LA FUERZA TERRESTRE	
ORD.	**ORGÁNICO**
	COMANDO
1	COMANDANTE DE LA UNIDAD DE CIBERDEFENSA
2	AMANUENSE
	DEPARTAMENTO DE PLANIFICACIÓN Y ASESORAMIENTO
3	JEFE DE DEPARTAMENTO
4	TÉCNICO DE CIBERDEFENSA
5	TÉCNICO DE CIBERDEFENSA
	SUBCOMANDO
6	SUBCOMANDANTE DE LA UNIDAD DE CIBERDEFENSA
7	OFICIAL DE PERSONAL
8	OFICIAL DE INTELIGENCIA
9	OFICIAL DE OPERACIONES
10	OFICIAL DE LOGISTICA
	DEPARTAMENTO DE DEFENSA
11	JEFE DE DEPARTAMENTO
12	ANALISTA GESTIÓN DE INCIDENTES
13	ANALISTA GESTIÓN DE INCIDENTES
14	ANALISTA GESTIÓN DE INCIDENTES
15	TÉCNICO EN ANÁLISIS FORENSE
16	TÉCNICO EN ANÁLISIS FORENSE
17	TÉCNICO DE CIBERDEFENSA
18	TÉCNICO DE CIBERDEFENSA
	DEPARTAMENTO DE EXPLORACIÓN
19	JEFE DE DEPARTAMENTO
20	ANALISTA DE CIBERINTELIGENCIA
21	ANALISTA DE CIBERINTELIGENCIA
22	TÉCNICO EN BÚSQUEDA DE INFORMACIÓN EN FUENTES ABIERTAS Y CERRADAS
23	TÉCNICO EN BÚSQUEDA DE INFORMACIÓN EN FUENTES ABIERTAS Y CERRADAS
24	TÉCNICO DE CIBERDEFENSA

25	TÉCNICO DE CIBERDEFENSA
	DEPARTAMENTO DE RESPUESTA
26	JEFE DE DEPARTAMENTO
27	TÉCNICO DE CIBERDEFENSA
28	TÉCNICO DE CIBERDEFENSA
29	TÉCNICO EN DESARROLLO DE SOFTWARE
30	TÉCNICO EN DESARROLLO DE SOFTWARE

Capacitación y formación

Dada la importancia de mantener la seguridad en el ciberespacio, es absolutamente prioritario disponer de personal calificado en todos los niveles de la organización desde el nivel directivo, operativo hasta el nivel técnico, capacitación que debe ser desarrollada de una manera permanente en el corto, mediano y largo plazo, lo que permitirá afrontar los riesgos y amenazas actuales en el ámbito de la seguridad cibernética.

La formación y capacitación estará dividida en nivel directivo, operativo y técnico que permita cumplir con las diferentes operaciones de defensa, exploración y respuesta.

La capacitación en el nivel directivo debe alcanzar las siguientes competencias:

- Concebir la estrategia de ciberseguridad y ciberdefensa
- Gestionar el sistema de ciberdefensa
- Asesorar en las políticas y acciones de ciberseguridad

Cursos de especialización requeridos:

- Curso de Políticas y Estrategias de Ciberseguridad
- Curso de riesgos y seguridad de la información.
- Gobierno y gerencia de ciberdefensa.

- Gestión de la seguridad de la información.
- Legislación en Seguridad de la Información.
- Infraestructuras críticas digitales

La capacitación en el nivel operativo correspondiente a jefes de departamento, debe alcanzar las siguientes competencias:

- Gestionar incidentes.
- Generar información de vulnerabilidades y amenazas.
- Analizar vulnerabilidades (on-line-in situ).
- Gestionar las acciones de informática forense.
- Gestionar la recopilación y monitorización de información de fuentes abiertas y cerradas
- Gestionar el Sistema de Detección de Instrucción, antivirus, cortafuegos, entre otros.

Cursos de especialización requeridos:

- Curso de ciberdefensa, comando y control del campo de batalla.
- Curso de Ataque cibernético.
- Curso de seguridad en redes de información.
- Curso de certificación como Auditor de Sistemas Informáticos (CISA).
- Curso de Análisis y seguridad de aplicaciones.
- Curso de Auditoría de sistemas y bases de datos.
- Curso de Certificación como investigador de informática forense.

La capacitación en el nivel técnico correspondiente a analistas y técnicos, debe alcanzar las siguientes competencias:

- Solventar incidentes.
- Generar información de vulnerabilidades y amenazas.
- Ejecutar las acciones de informática forense.
- Recopilar y monitorear información de fuentes abiertas y cerradas.
- Detectar instrucciones, antivirus, cortafuegos, entre otros.
- Actuar ante incidentes y pruebas de seguridad.
- Ejecutar acciones de informática forense.
- Configurar y administrar sistemas de seguridad en redes informáticas.
- Monitorear sistemas de seguridad de redes de informáticas.
- Auditar, sistemas informáticos

Cursos de especialización requeridos:

- Curso de ciberinteligencia.
- Curso de seguridad en entornos Unix/Linux.
- Curso de preparación a la certificación CIEH.
- Curso de introducción a la informática forense en infraestructuras industriales y sistemas de control (ICS, SCADA).
- Curso sobre redes de DDOS y Botnets.
- Curso de pentesting.
- Curso de pentesting y hacking.
- Curso de securización de dispositivos móviles.
- Curso de desarrollo avanzado de exploits.
- Certificación como investigador de informática forense.
- Certificación CISCO, CCNA.
- Curso de Ingeniería Inversa.

Validación de la propuesta

La propuesta presentada de acuerdo al análisis e investigación realizada es VÁLIDA y se adapta a las necesidades institucionales y operativas del Ejército Ecuatoriano, pudiendo convertirse en una guía para la implementación de un Órgano de Ciberdefensa en el Ejército Ecuatoriano.

Capítulo VI

Conclusiones y recomendaciones

Conclusiones

1. El marco legal vigente en el país, no es muy específico en lo referente al ciberespacio por lo que la ciberdefensa no ha sido considerada como un objetivo nacional actual u objetivo nacional permanente; sin embargo, garantiza la protección de la información y privacidad de las personas, además de la vigilancia y protección del ciberespacio, lo que ha permitido que el MIDENA y las Fuerzas Armadas, estructuren un Sistema de Ciberdefensa, con la infraestructura mínima para cumplir este cometido debido a una latente falta de recursos.
2. El Sistema nacional de inteligencia aún no define las ciberamenazas que tienen mayor probabilidad de cometer ciberdelitos en el país; además la cultura de ciberseguridad y ciberdefensa debe ser una responsabilidad del estado, siendo necesario que se trabaje y promulgue una ley en la que se cree un Sistema de Ciberseguridad y se enlisten las responsabilidades correspondientes a todas las instituciones públicas y privadas para implementar la ciberseguridad y ciberdefensa según corresponda y se garantice la asignación de los recursos necesarios para este cometido.
3. La Globalización y el auge de las TICs, generan escenarios VICA (volátiles, inciertos, complejos y ambiguos), donde actúan amenazas híbridas que mutan o evolucionan aceleradamente, generando una demanda de seguridad por parte de la sociedad ecuatoriana, lo que obliga a nuestras Fuerzas Armadas y en especial al Ejército Ecuatoriano

a tecnificar y adaptar su estructura de manera que pueda mantener o adquirir la capacidad de garantizar el desarrollo en un ambiente de seguridad y confianza, puesto que las ciberamenazas representan un grave problema, para la seguridad de las personas, grupos, instituciones y del mismo estado, pues su capacidad de actuar desde el otro lado del planeta o desde un sótano, cometiendo ciberdelitos, cuyas consecuencias afectan la integridad de las personas y la seguridad de las empresas e instituciones del estado.

4. El Comando de Ciberdefensa del COMACO, es un órgano planificador ejecutor del nivel estratégico militar; lo que conlleva a la necesidad de crear un órgano de ciberdefensa para la Fuerza Terrestre para que en base a las ciberamenazas determinadas, asesore a los niveles operativo y táctico, para el empleo de la ciberdefensa en la planificación y conducción de las operaciones militares; además se debe considerar que la manipulación de la opinión pública sobre las plataformas de medios sociales, es una grave amenaza para la planificación y conducción de las operaciones militares, debiendo determinarse las tácticas, técnicas y procedimientos que emplean los troles, a fin de neutralizar sus acciones, sobre todo cuando existen situaciones de conflictividad social o grave alteración del orden público; también se deben establecer procedimientos y medidas de seguridad para el manejo de la información clasificada de todas las unidades del Ejército a fin de evitar ataques internos y acciones de ciberespionaje, que pueden poner en peligro la conducción de las operaciones o encubrir robo de armamento y material.
5. Existe una demanda creciente de seguridad contra los delitos que se cometen en el ciberespacio, recayendo esta responsabilidad en el

estado, que debe proporcionar los recursos necesarios para que sus Fuerzas Armadas adquieran la capacidad (conocimiento, entrenamiento y tecnología) de realizar operaciones de ciberdefensa, que protejan el quinto dominio y apoyen la planificación y conducción de las operaciones militares.

6. La manipulación de la opinión pública sobre las plataformas de medios sociales, debe ser considerada como la principal amenaza para la planificación y conducción de las operaciones militares, debiendo determinarse las tácticas, técnicas y procedimientos que emplean los troles, a fin de neutralizar sus acciones, sobre todo cuando existen situaciones de conflictividad social o grave alteración del orden público.
7. Las operaciones de Ciberdefensa pueden servir como apoyo en la conducción diferentes operaciones terrestres, siendo necesario tener una visión general de las estructuras de diferentes organismos de ciberdefensa, que nos permitirán enfocar nuestra solución de acuerdo a la realidad del país.
8. La Fuerza Terrestre está ingresando a un proceso de transformación institucional que involucra necesariamente el alcanzar nuevas capacidades, disponer de una normativa legal que permita la ejecución de operaciones en el ámbito pertinente con seguridad y además la capacitación permanente de su personal en las diferentes áreas operativas, por lo que resulta prioritario que la fuerza disponga de un organismo de ciberdefensa que tenga la capacidad de prevenir y ejecutar operaciones en el ciberespacio que permitan la planificación y conducción de las operaciones de Respuesta a Crisis, no solo en apoyo a la Policía Nacional sino a las demás instituciones del estado, a las

cuales las Fuerzas Armadas Apoyan conduciendo este tipo de operaciones.

9. La Fuerza Terrestre está ingresando a un proceso de transformación institucional que involucra necesariamente el alcanzar nuevas capacidades, disponer de una normativa legal que permita la ejecución de operaciones en el ámbito pertinente con seguridad y además la capacitación permanente de su personal en las diferentes áreas operativas, por lo que resulta prioritario que la fuerza disponga de un organismo de ciberdefensa que tenga la capacidad de prevenir y ejecutar operaciones en el ciberespacio que permitan la planificación y conducción de las operaciones de Respuesta a Crisis, no solo en apoyo a la Policía Nacional sino a las demás instituciones del estado, a las cuales las Fuerzas Armadas Apoyan conduciendo este tipo de operaciones.

Recomendaciones.

1. Se ponga a consideración de la Dirección de Transformación del Ejército, la presente propuesta, como punto de partida en lo correspondiente a ciberdefensa, dentro del proceso de transformación institucional a fin de que nuestro Ejército alcance las capacidades de ciberdefensa y ciberseguridad.
2. Se considere a la ciberdefensa como un eje transversal en la planificación y conducción de las operaciones militares, no solo en apoyo a la Policía Nacional sino a las demás instituciones del estado, a las cuales las Fuerzas Armadas Apoyan conduciendo este tipo de operaciones.

3. Elaborar un programa de instrucción, que permita preparar oficiales y tropa para la planificación, conducción y ejecución de operaciones de ciberdefensa en apoyo a las operaciones militares.
4. Capacitar al personal militar en aspectos cotidianos de seguridad informática, mediante concienciación, factor primordial para evitar ser víctimas de delitos informáticos, robo de información, base de datos, entre otros.
5. De implementarse esta propuesta u otra estructura de ciberdefensa, realizar periódicamente una evaluación que permita evaluar, reajustar y continuar con el proceso de implementación del órgano de Ciberdefensa del Ejército.

Anexos

Anexo “A” (Operacionalización de Variables).

Anexo “B” (Síntesis Gráfica de la Investigación Cuantitativa o Cualitativa).

Anexo “C” (Cuestionarios de Entrevistas).

Anexo “D” (Cuestionarios de Encuestas).

Bibliografía

Abreu, J. L. (2014). El Método de la Investigación. *International Journal of Good Conscience*, 195-204.

Academia de Guerra del Ejército. (2018). PROPUESTA DE ACTUALIZACIÓN DEL MANUAL DE EMPLEO EN LAS OPERACIONES EN EL ÁMBITO INTERNO MCG-10-04. *PROPUESTA DE ACTUALIZACIÓN DEL MANUAL DE EMPLEO EN LAS OPERACIONES EN EL ÁMBITO INTERNO MCG-10-04*. Sangolquí, Ecuador.

Air Force. (2011). Cyberspace Operations. *Cyberspace Operations*. U.S.A.

Almeida, D. (2019). DESARROLLO DE CAPACIDADES DE CIBERDEFENSA EN LA ARMADA DEL ECUADOR. *DESARROLLO DE CAPACIDADES DE CIBERDEFENSA EN LA ARMADA DEL ECUADOR*. Quito, Ecuador.

Ampudia, C., & Tapia, R. (2017). LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN LAS FUERZAS ARMADAS DEL ECUADOR. PROPUESTA DE MANUAL DE TICs EN FUERZAS ARMADAS. *LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN LAS FUERZAS ARMADAS DEL ECUADOR. PROPUESTA DE MANUAL DE TICs EN FUERZAS ARMADAS.* QUITO, ECUADOR.

Asamblea General de la ONU. (1948). *www.ohchr.org*. Obtenido de Declaración universal de los derechos humanos: https://www.ohchr.org/en/udhr/documents/udhr_translations/spn.pdf

Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial.

Asamblea Nacional del Ecuador. (2008). *Constitución Política de la República del Ecuador.* Montecristi. Obtenido de https://educacion.gob.ec/wp-content/uploads/downloads/2012/08/Constitucion.pdf

Asamblea Nacional del Ecuador. (2009). *Ley de Seguridad Pública y del Estadao.* Quito.

Blanco, N. B. (2019). Infraestructuras Críticas y Ciberseguridad en las Fuerzas Armadas Dominicanas. *Seguridad, Ciencia y Defensa*, 13-21.

CARI. (2013). Ciberdefensa-Ciberseguridad Riesgos y Amenazas.

Castro, E. (2015). ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR. *ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR*. QUITO, ECUADOR.

Clarke, R. A., & Knake, R. K. (2010). Guerra en la red Los nuevos campos de batalla. *Guerra en la red Los nuevos campos de batalla*. Barcelona, España: Ariel.

COCIBER. (04 de Octubre de 2018). Ciberdefensa Aseguramiento de Infraestructuras Críticas. *Ciberdefensa Aseguramiento de Infraestructuras Críticas*. Quito.

COCIBER. (2019). *Informe de Redes Sociales-COCIBER-EXP-211.* Quito.

Comando de Ciberdefensa. (2019). *Informe Anual de Actividades.* Quito.

Comando de Ciberdefensa. (Noviembre de 2019). Informe de Implementación del Proyecto de Ciberdefensa . *Informe de Implementación del Proyecto de Ciberdefensa* . Quito, Pichincha.

Community Latam. (24 de Marzo de 2020). *Comunity Latam.* Obtenido de Problematica actual de la ciberdefensa: https://www.cxo-community.com/2018/07/problematica-actual-de-la-ciberdefensa.html

Conferencia Especializada Interamericana sobre Derechos Humanos San José. (22 de Noviembre de 1969). *http://www.tce.gob.ec*. Obtenido de http://www.tce.gob.ec/jml/bajar/CONVENCION%20AMERICANA%20SOBRE%20DERECHOS%20HUMANOS.pdf: http://www.tce.gob.ec/jml/bajar/CONVENCION%20AMERICANA%20SOBRE%20DERECHOS%20HUMANOS.pdf

Consejo Argentino para las Relaciones Internacionales. (Noviembre de 2013). Ciberdefensa-Ciberseguridad. *Ciberdefensa-Ciberseguridad*. Argentina.

Consejo Nacional de Política Económica y Social República de Colombia. (14 de Julio de 2011). LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA*. Bogotá.

Constitución Política de la República del Ecuador. (2008). *Constitución Política de la República del Ecuador.* Montecristi.

Daen, S. T. (2011). Tipos de Investigación Científica. *Revista de Actualización Clínica Volumen 9*, 621-624.

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

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

Díaz, J. R. (2016). Ciberamenazas: ¿el terrorismo del futuro? *Instituro Español de EStudios Estratégicos*, 1-21.

El Comercio. (15 de Abril de 2019). *El Comercio*. Obtenido de elcomercio.com: https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html.

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

EYGM Limited. (2019). *Encuesta Global de Seguridad de la Información.* EYGM.

GLOBALVOICES. (mayo de 2015). *Global Voices.* Obtenido de Global Voices: https://es.globalvoices.org/2015/05/09/venezuela-crea-la-direccion-conjunta-de-ciberdefensa/

GLOBALVOICES. (Mayo de 2015). *GLOBALVOICES*. Obtenido de https://es.globalvoices.org/2015/05/09/venezuela-crea-la-direccion-conjunta-de-ciberdefensa/: https://es.globalvoices.org/2015/05/09/venezuela-crea-la-direccion-conjunta-de-ciberdefensa/

Hernandez, R., Fernandez, C., & Baptista, P. (2006). *Metodología de la Investigación.* México: McGraw-Hill Interamericana.

Ibarra, V., & Nieves, M. (23,24,25 de Noviembre de 2016). La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. *VIII Congreso de Relaciones Internacionale* (págs. 1-16). Instituto de Relaciones Internacionales-UNLP.

Instituto Español de Estudios Estratégicos-Instituto Universitario "General Gutiérrez Mellado". (2010). *Ciberseguridad. Retos y Amenzas a la Seguridad Nacional en el Ciberespacio.* Obtenido de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Jerez, C. (Abril de 2019). ANÁLISIS DE LA ESTRUCTURA ORGANIZACIONAL CON LA INCORPORACIÓN DE LA CIBERDEFENSA COMO PARTE DE LA DIRTIC DE LA FUERZA AÉREA ECUATORIANA. *ANÁLISIS DE LA ESTRUCTURA ORGANIZACIONAL CON LA INCORPORACIÓN DE LA CIBERDEFENSA COMO PARTE DE LA DIRTIC DE LA FUERZA AÉREA ECUATORIANA*. Quito.

JEREZ, C. (ABRIL de 2019). ANÁLISIS DE LA ESTRUCTURA ORGANIZACIONAL CON LA INCORPORACIÓN DE LA CIBERDEFENSA COMO PARTE DE LA DIRTIC DE LA FUERZA AÉREA ECUATORIANA. *ANÁLISIS DE LA ESTRUCTURA ORGANIZACIONAL CON LA INCORPORACIÓN DE LA CIBERDEFENSA COMO PARTE DE LA DIRTIC DE LA FUERZA AÉREA ECUATORIANA*. QUITO, ECUADOR.

Lira i Morel, R. (2016). *Diseño y seguimiento del proceso de investigación : realidad, método y concepto .* Managua: PAVSA.

LLongueras Vicente, A. (2013). La Ciberguerra; la guerra inexistente.

LLongueras Vicente, A. (2013). La Ciberguerra; la guerra inexistente. *La Ciberguerra; la guerra inexistente*.

López, O. (2011). MEDICIÓN, TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN. *MEDICIÓN, TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN*, 1-11.

MC0571 - NATO Cyber Defence Concept. (s.f.). Cyber Defence Concept. *Cyber Defence Concept.*

metodoss.com. (06 de Abril de 2020). Obtenido de metodoss.com: https://metodoss.com/inductivo/

Ministerio Coordinador de Seguridad. (2014). *Seguridad Integral Plan y Agendas 2014-2017.* Quito D.M: EL TELÉGRAFO.

Ministerio de Defensa Nacional. (24 de Septiembre de 2014). Acuerdo Ministerial 281. *Acuerdo Ministerial 281*. Quito, Pichincha: MIDENA.

Ministerio de Defensa Nacional. (24 de septiembre de 2014). Acuerdo Ministerial 281. *Acuerdo Ministerial 281*. Quito: MIDENA.

Ministerio de Defensa Nacional. (2018). *Política de Defensa Nacional.* Quito, Pichincha: I.G.M.

Ministerio de Defensa Nacional. (2018). *Política de Defensa Nacional.* Quito, Pichincha: I.G.M. Recuperado el 2019, de https://www.defensa.gob.ec/

Ministerio de Defensa Nacional. (2019). *Plan Nacional de Seguridad Integral 2019-2030.* Quito D.M. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-matriz-web.pdf

Ministerio de tecnologías de la Información y las Comunicaciones de Colombia. (2020). *Ministerio de tecnologías de la Información y las Comunicaciones de Colombia*. Obtenido de Ministerio de tecnologías de la Información y las Comunicaciones de Colombia: https://www.mintic.gov.co/portal/inicio/

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2020). Página Web del Ministerio de tecnologías de la Información y las Comunicaciones. *Página Web del Ministerio de tecnologías de la Información y las Comunicaciones*. Colombia.

Organización de Estados Americanos. (2014). *SIMANTEC.* OEA.

Pástor, O., Pérez, J., Arnáiz, D., & Taboso, P. (Octubre de 2009). Seguridad nacional y Ciberdefensa. *Seguridad nacional y Ciberdefensa*. Madrid, España: Icono Imagen Gráfica, S.A.

Pástor, O., Pérez, J., Arnáiz, D., & Taboso, P. (Octubre de 2009). *Seguridad nacional y Ciberdefensa.* Obtenido de Seguridad nacional y Ciberdefensa: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

Poggi, N. (10 de Diciembre de 2018). *Prey*. Obtenido de https://preyproject.com: https://preyproject.com/blog/es/ciberamenazas-que-son-como-te-afectan-y-que-puedes-hacer-al-respecto/

Proaño, C., & Guerrero, R. (2020). EL MANEJO DE LA CIBERSEGURIDAD EN LAS FUERZAS ARMADAS. *EL MANEJO DE LA CIBERSEGURIDAD EN LAS FUERZAS ARMADAS*. Quito.

Real Academia de la Lengua Española. (2019). *Diccionario de la Real Academia de la Lengua Española.*

Red de Bibliotecas Universitarias. (14 de Mayo de 2014). *Manual de buenas prácticas en redes.* Obtenido de REBIUN: https://www.rebiun.org/

Ruiz, M., & Ochoa, M. (2019). INCIDENCIA DE LA CIBERDEFENSA EN LA PLANIFICACIÓN DE LAS OPERACIONES MILITARES CONJUNTAS.

INCIDENCIA DE LA CIBERDEFENSA EN LA PLANIFICACIÓN DE LAS OPERACIONES MILITARES CONJUNTAS. Quito, Ecuador. Obtenido de https://www.defensa.gob.ec/biblioteca/

Ruiz, R. (2006). *Historia y Evolución del pensamiento Científico.* México.

Sampieri Hernández, R., Collado Fernández, C., & Lucio Baptista, P. (2003). *Metodología de la Investigación.*

Secretaría Nacional de Planificación y Desarrollo, Senplades. (2017). *Plan Nacional de Desarrollo 2017-2021 "TODA UNA VIDA".*

Sosa, G. E. (2018). EL EMPLEO DE LAS REDES SOCIALES PARA EL MANEJO DE LOS ASUNTOS CIVILES EN UN TEATRO DE OPERACIONES. *EDES SOCIALES PARA EL MANEJO DE LOS ASUNTOS CIVILES EN UN TEATRO DE OPERACIONES.*

Stoltenberg, J. (2017).

Stoltenberg, J. (2018). *Community Latam 2018.*

Subía, T., & Espinoza, C. (Agosto de 2020). La Política de la Defensa Nacional 2018 y sus factores de incidencia en las tareas del Ejército Ecuatoriano. *La Política de la Defensa Nacional 2018 y sus factores de incidencia en las tareas del Ejército Ecuatoriano*. Quito. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2015/04/ene15_LEY-DE-SEGURIDAD-PUBLICA-Y-DEL-ESTADO.pdf

SYMANTEC. (Febrero de 2019). *ISTR Informe sobre las Amenazas para la Seguridad en Internet.* SIMANTEC.

Tapia, A. (2018). INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR. *INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR*. Quito, Ecuador. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

TAPIA, A. (2018). INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR. *INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR*. QUITO, ECUADOR.

TAPIA, A. (2018). INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR. *INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR*. QUITO, ECUADOR.

TAPIA, A. (2018). INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR. *INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR*. QUITO, ECUADOR. Obtenido de INCIDENCIA DE LAS OPERACIONES DE CIBERDEFENSA EN LAS OPERACIONES NAVALES. PROPUESTA DE UN ORGANISMO PARA LA ARMADA DEL ECUADOR.

Universidad de Cien Fuegos. (Octubre de 2019). Normas APA 7.a Edición Guía de citación y referenciación. *Normas APA 7.a Edición Guía de citación y referenciación*. Universo SUR.

USA Army's. (2010). Cybersapce Operations Concept Capability Plan 2016-2018. USA. *Cybersapce Operations Concept Capability Plan 2016-2018. USA*. U.S.A.

Vargas, C. (2014). Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. *Revista de tecnologias USCG*, 1.

VARGAS, E. M. (2014). CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL? *CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL?* Bogotá.