Análisis de la Situación Actual de Ciberdefensa en la Fuerza Terrestre 2020

Abad Páez, Walberto Antonio y Sandoval Loaiza, Patricio Cornelio

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 Magíster en Defensa y Seguridad, Mención Estrategia Militar

Mgtr. Sánchez Sánchez, Luis Vidal

10 de diciembre del 2020

Document Information

Analyzed document	Tesis MDS Ciberdefensa Abad-Sandoval.docx (D87142855)
Submitted	11/30/2020 1:35:00 AM
Submitted by	
Submitter email	wabad72@gmail.com
Similarity	6%
Analysis address	waaltamirano.espe@analysis.urkund.com

Sources included in the report

SA	**Universidad de las Fuerzas Armadas ESPE / Tesis completa - Carlos Espinoza_Tomás Subía Urk 15-AGO.docx** Document Tesis completa - Carlos Espinoza_Tomás Subía Urk 15-AGO.docx (D77861290) Submitted by: eegalarza@espe.edu.ec Receiver: eegalarza.espe@analysis.urkund.com	3
SA	**Universidad de las Fuerzas Armadas ESPE / TESIS para revision urcum.doc** Document TESIS para revision urcum.doc (D87053888) Submitted by: fernandoaguirre2008@hotmail.com Receiver: waaltamirano.espe@analysis.urkund.com	2
SA	**Universidad de las Fuerzas Armadas ESPE / TESIS PROANO GUERRERO 04 AGOSTO 020 corrección.docx** Document TESIS PROAÑO GUERRERO 04 AGOSTO 020 corrección.docx (D77521555) Submitted by: eegalarza@espe.edu.ec Receiver: eegalarza.espe@analysis.urkund.com	5
W	URL: https://www.inap.mx/portal/images/pdf/rap148.pdf Fetched: 8/28/2020 1:50:21 PM	2
W	URL: https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_ ... Fetched: 12/4/2019 10:21:13 AM	2
W	URL: https://core.ac.uk/download/pdf/187433111.pdf Fetched: 12/3/2019 7:09:57 PM	1

Sanchez Sanchez, Luis Vidal

Teniente Coronel EM

Director

C.C.: 1705912168

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Análisis de la Situación Actual de Ciberdefensa en la Fuerza Terrestre 2020**" fue realizado por los señores **Abad Páez, Walberto Antonio** y **Sandoval Loaiza, Patricio Cornelio** 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 sustente públicamente.

Sangolquí, 10 de diciembre de 2020

Sanchez Sanchez, Luis Vidal

Teniente Coronel EM

Director

C.C.: 1705912168

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Nosotros **Abad Páez, Walberto Antonio** y **Sandoval Loaiza, Patricio Cornelio**, con cédulas de ciudadanía n° 0602230609 y 1101924759, declaramos que el contenido, ideas y criterios del trabajo de titulación: **Análisis de la Situación Actual de Ciberdefensa en la Fuerza Terrestre 2020** 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, 10 de diciembre de 2020

.....
Abad Páez, Walberto Antonio
C.C.: 0602230609

.....
Sandoval Loaiza, Patricio Cornelio
C.C.: 1101924759

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

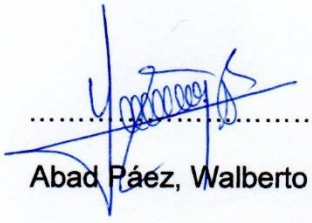
TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

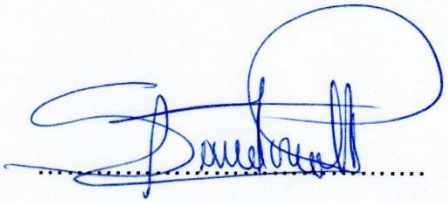
Nosotros **Abad Páez, Walberto Antonio** y **Sandoval Loaiza, Patricio Cornelio** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Análisis de la Situación Actual de Ciberdefensa en la Fuerza Terrestre 2020** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 10 de diciembre de 2020



Abad Páez, Walberto Antonio

C.C.: 0602230609



Sandoval Loaiza, Patricio Cornelio

C.C.: 1101924759

Dedicatoria

Dedico el presente trabajo de investigación a mi esposa Yesenia e hijos Antonio y Alejandro, quienes constituyen parte fundamental de mi vida, siendo el soporte e inspiración para el logro de mis objetivos académicos y profesionales. Ustedes con su llegada a mi vida han complementado esa fuerza e impulso que necesitaba, con su amor, esfuerzo, confianza, y comprensión, para poder cumplir todas las metas que me imponga.

Walberto Antonio Abad Páez

Dedico con todo mi amor el presente trabajo de investigación a mis queridos hijos Juan y José, quienes desde su llegada le dieron felicidad a mi vida y constituyen la base inspiradora que permite cumplir con mis objetivos personales, académicos y profesionales.

A mi estimado amigo y compañero Antonio Abad que con su confianza y apoyo a permitido culminar con éxito esta etapa y reafirma el compromiso de seguir luchando por metas futuras.

Patricio Cornelio Sandoval Loaiza

Agradecimiento

A nuestro Seños Dios por darnos la oportunidad de vivir a plenitud con alegrías y tristezas, junto a todas las personas que han participado directa o indirectamente en nuestro desarrollo profesional.

A la Academia de Guerra del Ejército y Universidad de Fuerzas Armadas ESPE, por ser partícipes de nuestro perfeccionamiento militar y aportar al desarrollo del conocimiento en el área de las ciencias de seguridad y defensa.

A nuestro director de Trabajo de titulación, por constituir la guia y soporte constante en el proceso de formulación y desarrollo de la presente investigación.

A todo el personal docente, quienes fueron participes de los nuevos conocimientos adquiridos y desarrollados.

Índice de Contenido

Índice de Tablas

Índice de Figuras

Resumen

El presente trabajo de investigación, tiene el propósito de analizar la situación actual de la ciberdefensa en la Fuerza Terrestre. Se inicia con el planteamiento el problema y objetivos de investigación. Se desarrolla una revisión bibliográfica respecto al ciberespacio y la ciberdefensa en el contexto militar a nivel mundial, regional y nacional, mediante la utilización de fuentes primarias y datos estadísticos. La revisión exploratoria documental se desarrolla en unidades o dependencias de la Fuerza Terrestre. Se aplica el método científico con un enfoque cualitativo, planteando la hipótesis de investigación conjuntamente con las variables, posteriormente se aplica el método, técnicas e instrumentos de recolección de datos para su análisis e interpretación. Con los resultados y hallazgos se plantea una propuesta para mejorar la ciberdefensa en la Fuerza Terrestre, mediante un sistema de gestión de ciberdefensa. Este sistema aporta con conceptualizaciones doctrinarias, estructura organizacional, arquitectura de la red y formula una proceso de ciberdefensa. La investigación concluye identificando las deficiencias que imposibilitan el mantenimiento de la ciberdefensa, las causas de los limitados recursos presupuestarios y de infraestructura que impactan en la defensa y seguridad de datos e infraestructura de tecnologías de la información y de las comunicaciones, se plantea nuevas líneas de investigación en esta nueva área de conocimiento militar.

Palabras clave:

- **CIBERDEFENSA**
- **CIBERSEGURIDAD**
- **CIBERESPACIO**
- **CIBERATAQUES**
- **FUERZA TERRESTRE**

Abstract

This research work is intended to analyze the current situation of cyberdefensa in Army. The approach starts with the problem and research objectives. A bibliographic review of cyberspace and cyberdefensa takes place in the military context at the global, regional and national levels, using primary sources and statistical data. The documentary exploratory review takes place in Army units or agencies. The documentary exploratory review takes place in units or units of the Army. The scientific method is applied with a qualitative approach, raising the research hypothesis in conjunction with the variables, the method, techniques and data collection tools are subsequently applied for analysis and interpretation. With the results and findings, a proposal is put forward to improve cyberdefensa in the Army, through a cyberdefensa management system. This system contributes with doctrinal conceptualizations, organizational structure, network architecture and formulates a process of cyberdefensa. The research concludes by identifying the deficiencies that make it impossible to maintain cyberdefense, the causes of the limited budgetary and infrastructure resources impacting the defense and security of data and infrastructure of information and communications technologies, new lines of research are proposed in this new area of military knowledge.

Key words:

- **CYBERDEFENSE**
- **CYBERSECURITY**
- **CYBERSPACE**
- **CYBERATTACKS**
- **ARMY**

El Problema

Planteamiento del Problema de Investigación

La creciente y vertiginosa expansión de las tecnologías de la información y de las comunicaciones (TIC), ha influenciado directamente en la exponencial difusión de datos e información a través de las redes, medios de transmisión y diferentes tecnologías de comunicación, en especial por la utilización del internet y el protocolo abierto de internet (IP[1]). El trafico global respecto al protocolo IP para el 2022 se proyecta alcanzará los 4.8 Zettabyte (ZB[2]) a nivel global (Cisco Systems, 2019), este uso acelerado incrementa el riesgo y afectación de activos críticos de las organizaciones o Estados, como son sus datos e infraestructura tecnológica en general.

La afectación se enfoca en la integridad, confidencialidad y disponibilidad de los datos, información e infraestructura tecnológica, por medio de ataques de TIC, originados por intrusiones no autorizadas, los cuales se presentan en forma continua y se incrementa a la par del mismo desarrollo tecnológico, impactando a sectores que administran aplicaciones de TIC, como servicios financieros, entidades gubernamentales, proveedores de servicios de salud, entre otros de no menor importancia.

La información se compone de un conjunto organizado de datos, los cuales constituyen actualmente uno de los principales activos de las organizaciones en general y su seguridad se convierte en crítica (Dixon, 2014).

Entre los objetivos principales de los ataques a nivel mundial se identifican perfiles de blancos de organizaciones y agencias militares, destacándose los de inteligencia (Emm y Chebyshev, 2018), por lo cual se define como una principal

[1] IP, Internet Protocol, Protocolo de Internet cuya función es mover los datagramas en diferentes redes.
[2] Zettabyte = 1024 Exabytes, Exabytes=1024 Petabytes .

amenaza global a los ciberataques, ciberdelincuencia o ciberterrorismo. A nivel internacional los Estados y organizaciones, han desarrollado estructuras de ciberdefensa para la seguridad y defensa de la información e infraestructura de TIC, pero a pesar de estos esfuerzos, más del 50 % de los ataques que se desarrollan causan daños y su recuperación puede tardar meses o incluso años (Cisco Systems, 2018).

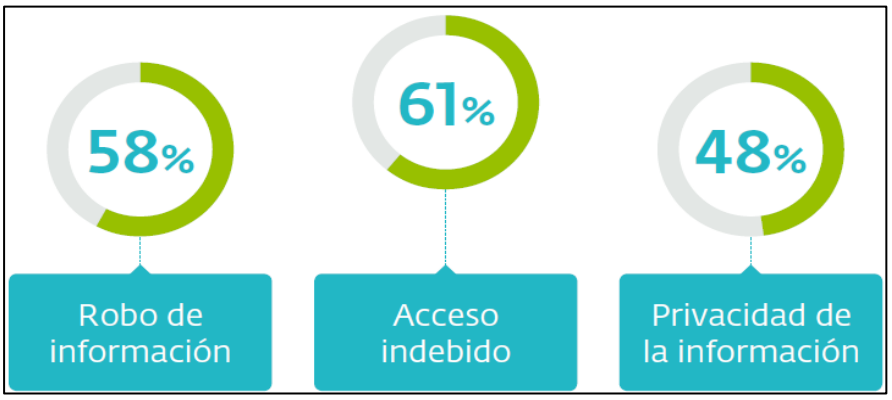
En Latinoamérica las diferentes organizaciones y entidades gubernamentales, en función de su desarrollo tecnológico y desarrollo de su transformación digital, han sufrido incidentes informáticos que han impactado en sus operaciones. En el 2017 se dispararon los incidentes de Ransomware[3] y para el 2018-2019 los incidentes de infecciones de código malicioso y minería de criptomonedas[4] (ESET, 2019).

La percepción de seguridad de TIC en Latinoamérica ante los incidentes y amenazas, determina la mayor preocupación respecto al acceso indebido, robo de información y la privacidad de la información, como se ilustra en la figura 1. Respecto a medidas para la seguridad y defensa de ciberataques, en la región se encuentra atrasada y más del 50 % de las organizaciones no cuentan con controles o políticas de seguridad implementadas, evidenciándose al sector de gobierno como el menos desarrollado y actualmente el más vulnerable en la región (ESET, 2019). En la figura 2 se observa los controles de seguridad (cifrado, 2FA[5] y EDR[6]) implementados por sector en Latinoamérica.

[3] Ransomware, ransom=rescate y ware=software, "secuestro de datos o sistemas"
[4] Criptomonedas, medio digital de intercambio transaccional económico
[5] 2FA, Two Factor Authentication, Autenticación de dos factores
[6] EDR, Endpoint Protection Platforms, protección de plataformas de puntos finales.

Figura 1

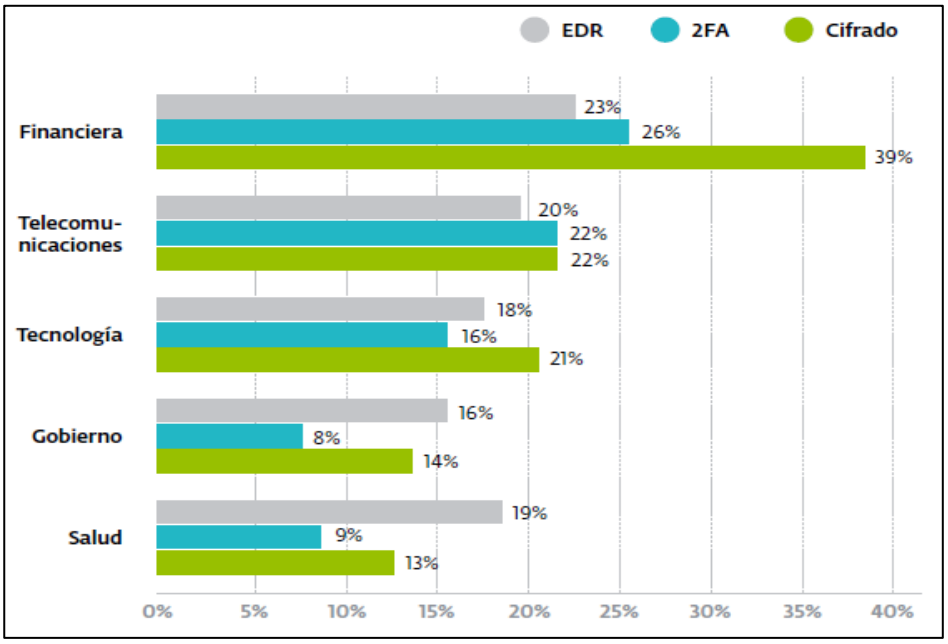
Preocupaciones de seguridad en Latinoamérica



Nota. Tomado de *ESET SECURITY REPORT Latinoamérica 2019* (p. 14), por ESET, 2019.

Figura 2

Implementación de controles de seguridad en Latinoamérica

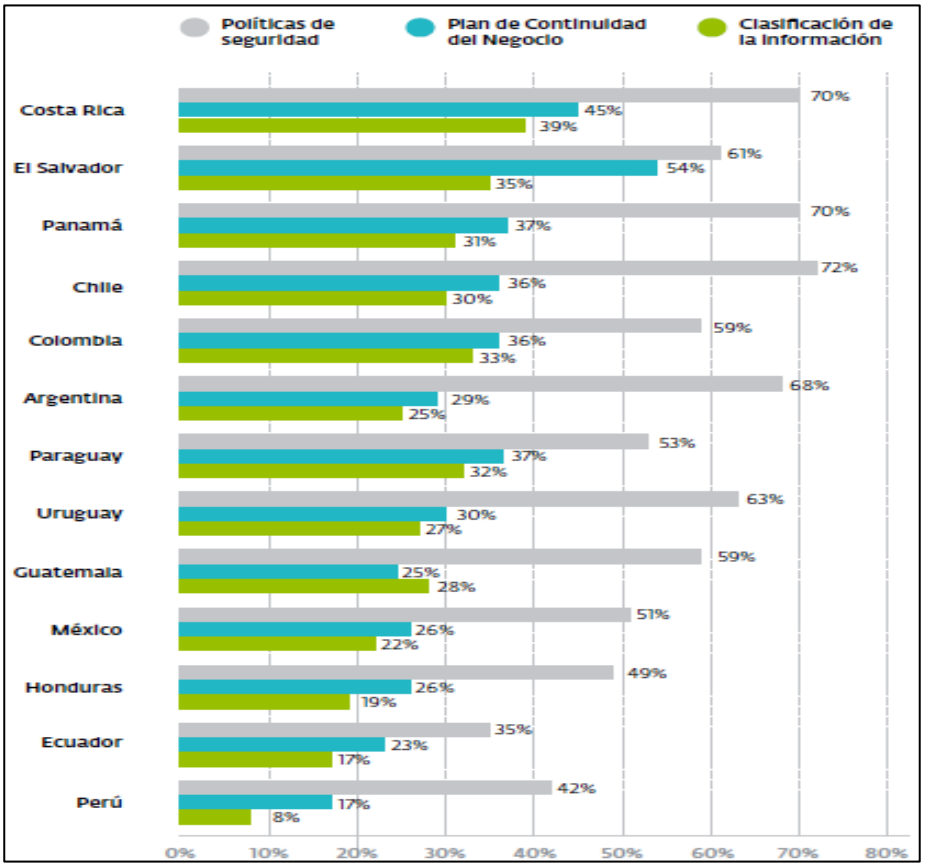


Nota. Tomado de *ESET SECURITY REPORT Latinoamérica 2019* (p. 19), por ESET, 2019.

A nivel nacional en el Ecuador hace pocos años se ha iniciado un desarrollo lento de la adopción de tecnologías de seguridad y defensa respecto a los datos, información e infraestructura de TIC del Estado, evidenciándose que se encuentra relegada respecto al desarrollo e implementación principalmente de políticas de seguridad, planes de continuidad y clasificación de la información, aspectos fundamentales de la ciberdefensa, en la figura 3 se ilustra los niveles de implementación de prácticas de gestión para la seguridad por país en Latinoamérica.

Figura 3

Prácticas de gestión para la seguridad por país



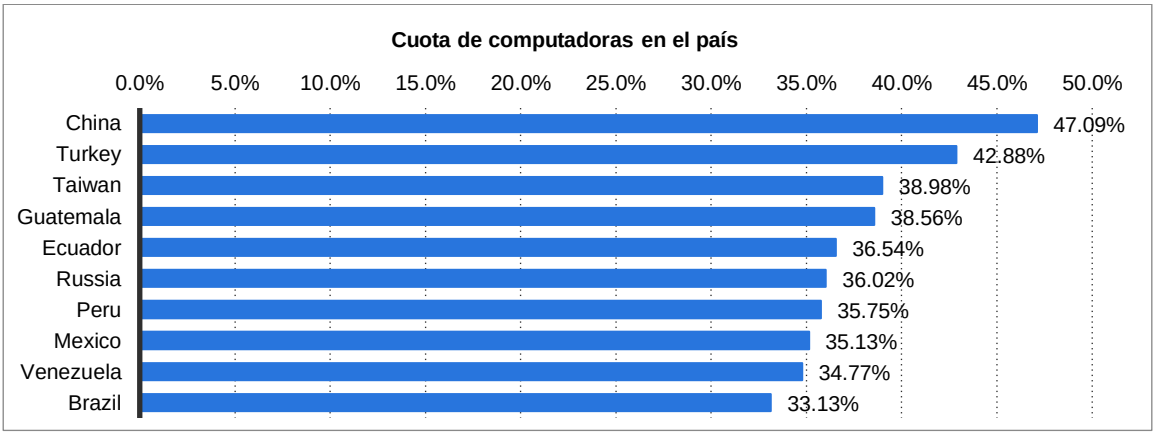
Nota. Tomado de *ESET SECURITY REPORT Latinoamérica 2019* (p. 20), por ESET, 2019.

Para una adecuada ciberdefensa a más de los recursos tecnológicos es fundamental complementarlos con una apropiada gestión, en el Ecuador los niveles de adopción de políticas de seguridad de TIC, planes de continuidad y clasificación de la información son inadecuados actualmente.

La adopción de una adecuada ciberdefensa para el Ecuador es de vital importancia, en función que los ataques o ciberataques a plataformas de TIC se han incrementado en los últimos años. En la figura 4 se observa los países con la tasa más alta de computadoras infectadas con malware en el año 2016 (Statista, 2019a). El Ecuador se ha convertido en uno de los principales países de origen del tráfico de ciberataques a nivel internacional, en la figura 5 se ilustra el tráfico de origen de ataques de Denegación de Servicio Distribuido (DDoS[7]) a nivel mundial (Statista, 2019b).

Figura 4

Países con la mayor tasa de infección de malware 2016

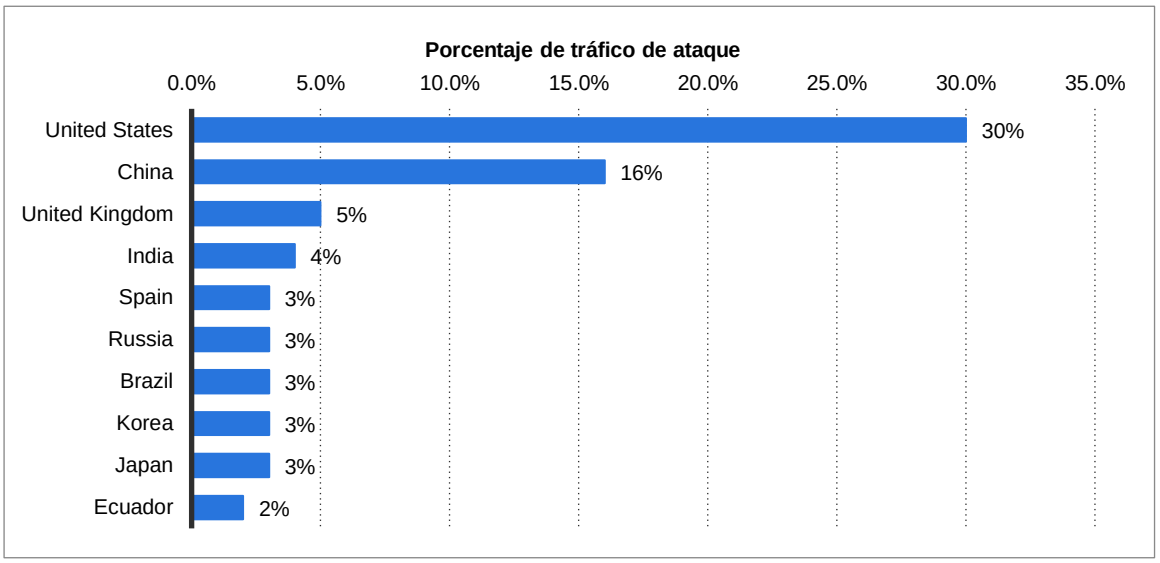


Nota. Tomado de *Countries with the highest rate of malware infected computers as of 4th quarter 2016* (p. 23), por Statista - Anti-Phishing Working Group (APWG), 2019, *Security software*.

[7] DDoS, Distributed Denial of Service, ataque de Denegación de Servicio Distribuido.

Figura 5

Principales países de origen del tráfico de ataques DDoS



Nota. Tomado de *Share of global denial of service (DDoS) attack traffic from November 2017 to April 2018, by originating country* (p. 40), por Statista - Akamai Technologies, 2019, IT security.

En este contexto la ciberdefensa de activos de datos, información e infraestructura de TIC, a nivel mundial se desarrolla no muy aceleradamente en comparación con el desarrollo tecnológico actual, en Latinoamérica este se encuentra retrasado y en Ecuador es inadecuada.

Formulación del Problema

En Ecuador ya se identifica en el ámbito global como una amenaza a los ataques cibernéticos o ciberataques, así como el involucramiento del ciberespacio para el cumplimiento de la misión fundamental de Fuerzas Armadas del Ecuador (FFAA) que se describe como "…defensa de la soberanía e integridad territorial 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" (Política de la Defensa Nacional del Ecuador "Libro Blanco", 2018, p. 41).

Los ciberataques, ciberterrorismo, ciberespionaje entre otros, presentan la capacidad de afectar el funcionamiento de áreas y sectores estratégicos a nivel nacional, así como a la datos, información e infraestructura tecnológica críticas de las organizaciones del Estado, lo cual comprometerá a la seguridad nacional en general, requiriendo incrementar capacidades para la ciberdefensa pero sin dependencia tecnológica (Política de la Defensa Nacional del Ecuador "Libro Blanco", 2018)

La necesidad de incrementar la seguridad y defensa de la datos, información e infraestructura de las TIC para las operaciones críticas y estructura de la Fuerza Terrestre (FT), se ha evidenciado en los últimos años. Como por ejemplo el caso de la " … presunta manipulación del sistema de inventarios logísticos de las Fuerzas Armadas … un funcionario público del Ejército, con rango de Analista 2, les ayudaba a borrar los registros del sistema informático" (El Telégrafo, 2018).

La FT del Ecuador está expuesta a posibles ataques informáticos o ciberataques por elementos internos o externos que desean obtener o modificar la información vulnerando las medidas de seguridad que se disponen o no actualmente. Conjuntamente con la ausencia de una legislación adecuada, falta de desarrollo de capacidades de la función judicial e insuficientes recursos disponibles para la ciberseguridad y ciberdefensa.

En función de los descrito se formula el problema ¿Cuáles son los inconvenientes que impiden una adecuada ciberdefensa y su impacto en la protección de datos, información e infraestructura de TIC de la FT de Ecuador?

Deficiente o débil Ciberdefensa en la FT.

Preguntas de Investigación

¿Cuáles son las dificultades que imposibilitan el mantenimiento de la confidencialidad, integridad y disponibilidad de la información y/o datos en la FT de Ecuador?

¿Cuáles son las causas por las cuales se presentan carencias de recursos disponibles para ciberdefensa en la FT de Ecuador?

¿Cuáles son las tecnologías, técnicas y/o modelos de gestión para mejorar la ciberdefensa en la FT de Ecuador?

Objeto de Estudio

Fuerza Terrestre del Ecuador

Campo de Acción

Ciberdefensa

Delimitación de la Investigación

Delimitación Temática

Respecto a la delimitación temática, la investigación se desarrollará en base a un marco general de seguridad y defensa, enfocado a la defensa de activos críticos de TIC de la FT del Ecuador, específicamente a la seguridad y defensa de la datos, información e infraestructura de TIC crítica de la FT en el contexto de la ciberdefensa.

Delimitación Espacial

El presente trabajo de investigación se desarrollará en la ciudad de Quito de la provincia de Pichincha, en el Comando General de la FT, específicamente en la Direcciones de Comunicaciones e Informática y Agrupamiento de Comunicaciones y Guerra Electrónica, complementándose con el uso de fuentes de información, base de datos e información general empleando la red informática mundial a través del uso del internet.

Delimitación Temporal

La investigación abarcará para su desarrollo y estudio la información o datos enmarcados en el período comprendido entre 2017 a 2020, considerando el entorno de la ciberdefensa en la FT del Ecuador.

Justificación de la Investigación

Relevancia

La presente investigación se enfoca a la ciberdefensa en la FT, como se describió en la delimitación y formulación del problema, los ataques cibernéticos internos y externos de diferente naturaleza, constituyen una amenaza real para la FT, FFAA y Estado Ecuatoriano, en función de lo cual su relevancia radica en la búsqueda de la mejora de la ciberdefensa, para hacer frente a las amenazas descritas, reducción de la brecha tecnológica actual, así como el incremento de la seguridad y defensa de la datos, información e infraestructura de TIC, lo cual contribuirá al cumplimiento de la misión de la FT y desarrollo nacional.

Originalidad

En función de la revisión bibliográfica el tema propone un aporte original para identificar las causas que impactan para el mejoramiento de la ciberdefensa y tener fundamentos para proponer el uso de nuevos conocimientos judiciales, doctrinarios, de procesos y/o modelos de ciberdefensa para la FT del Ecuador.

Factibilidad

La factibilidad del presente trabajo de investigación, está en función de la disponibilidad de recursos técnicos, económicos y humanos, así como el acceso a base de datos y a las dependencias de la FT ya delimitadas, se complementa con la experiencia, especialización y competencia de los investigadores.

Objetivos de la Investigación

Objetivo General

Determinar la situación actual de la ciberdefensa en la FT y su incidencia o impacto en la seguridad y defensa de datos e infraestructura de TIC.

Objetivos Específicos

Determinar las dificultades que imposibilitan el mantenimiento de la ciberdefensa en la FT.

Identificar las causas de los limitados recursos para la ciberdefensa en la FT.

Diseñar una propuesta que contribuyan a la mejora de la ciberdefensa en la FT.

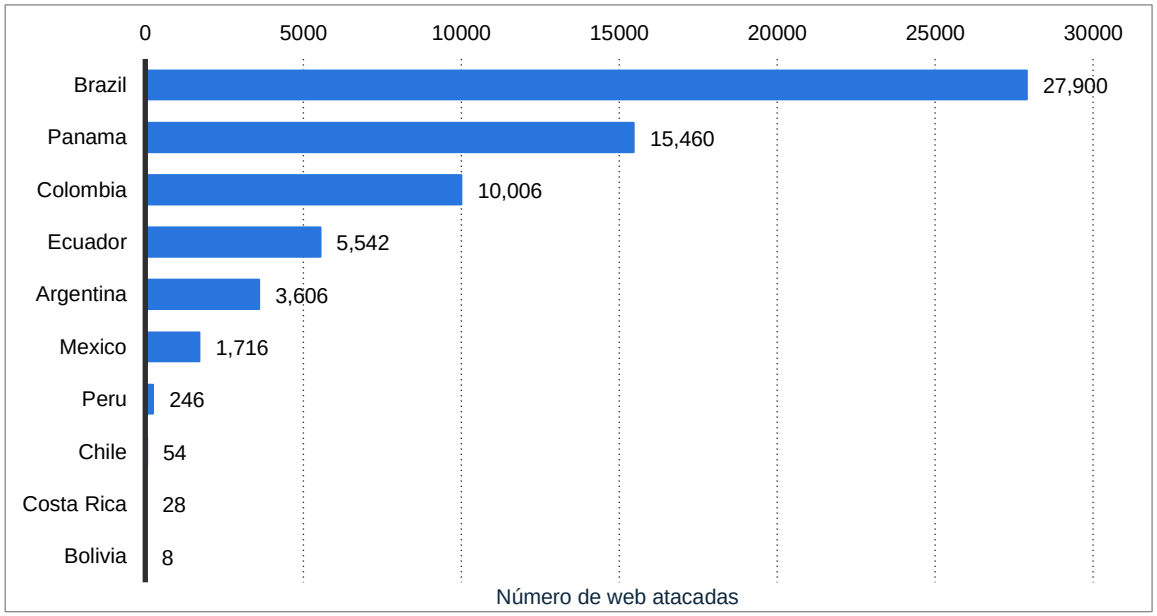
Marco Teórico

Antecedentes de la Investigación

En referencia a la identificación y formulación del problema de investigación descritos, se evidencia la crítica situación respecto a ciberataques en contra del Ecuador, lo cual compromete su seguridad y defensa, en la figura 6 se ilustra el número de ciberataques a aplicaciones web gubernamentales por países de Latinoamérica, en un período de siete días del 18 al 25 de junio de 2019, identificando al Ecuador con 5542 ataques desarrollados.

Figura 6

Ciberataques a web gubernamentales por países de Latinoamérica

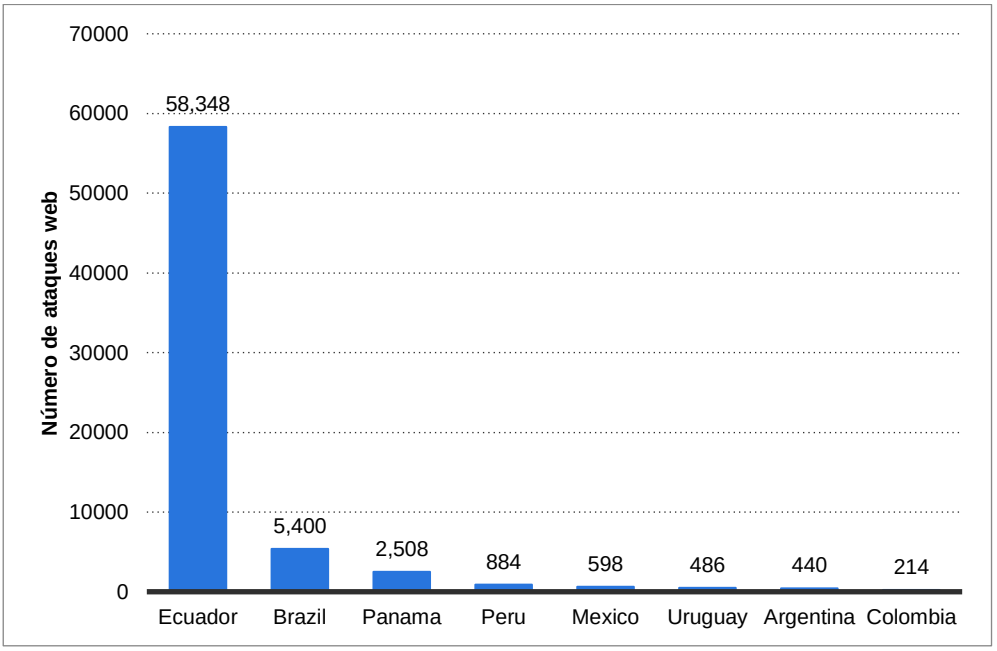


Nota. Tomando de *Latin American countries with the largest number of web application attacks observed in the public sector in June 2019*, por Statista – Akamai Technologies, 2019, Cyber Crime.

En el mismo período se ilustra en la figura 7, el Ecuador es el principal país que ha recibido ciberataques en la industria del juego en línea, en la figura 8 se describe que el Ecuador ha recibido 237.000 ciberataques a aplicaciones web de alta en el sector de alta tecnología, lo cual corrobora el estado crítico de su seguridad y defensa en el ciberespacio.

Figura 7

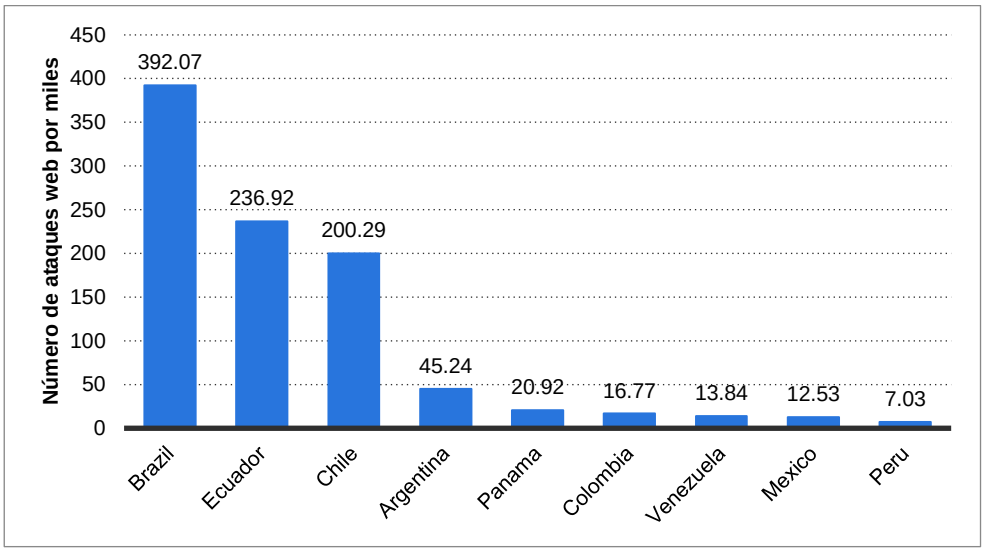
Ciberataques a cuentas de juego por países de Latinoamérica



Nota. Tomado de *Latin American countries with the largest number of web application attacks observed in gaming in June 2019*, por Statista - Akamai Technologies, 2019, Cyber Crime.

Figura 8

Ciberataques a web de alta tecnología por países de Latinoamérica



Nota. Tomado de *Latin American countries with the largest number of web application attacks observed in the high technology sector in June 2019 (in 1,000s)*, por Statista - Akamai Technologies, 2019, Cyber Crime.

En la revisión de la literatura, se presenta investigaciones realizadas a nivel nacional, regional y del extranjero a pesar que puedan responder a otros contextos y situaciones, se puede destacar por su relevancia a la realizada por Claus (2015), en su trabajo respeto a la Guardia Nacional de los Estados Unidos de Norteamérica y el Cibercomando de Estados Unidos (USCYBERCOM[8]), concluye que la ciberdefensa requiere un trabajo fuerte entre los sectores públicos y privados, proponiendo y validando al final un modelo público-privado para la ciberdefensa eficaz de infraestructuras críticas.

[8] USCYBERCOM, United States Cyber Command, Cibercomando de Estados Unidos

Wells (2017), en su obra determina que las operaciones en el ciberespacio deben integrarse con otras y apoyados con la inteligencia, así como que ninguna organización civil o militar por si sola está preparada para hacer frente a fuerzas en el ciberespacio.

Nielsen (2016), en su investigación establece que el ejército de los Estados Unidos de Norteamérica tiene un papel importante en el dominio cibernético, requiriendo que los militares innoven y realicen una colaboración con actores internacionales, de gobierno y privados.

A nivel regional se pueden citar a trabajos como de Cabral (2015), quien en su investigación define que Argentina y Brasil en seguimiento de la tendencia mundial, respecto a la protección del ciberespacio es responsabilidad de la Defensa Nacional y coordinada por FFAA.

Moreno (2015), en su trabajo identifica la ciberdefensa militar de Colombia, las implicaciones del uso del ciberespacio y los convenios o coordinaciones con entidades públicas y privadas.

Zúñiga (2017), en su investigación plantea determinar las dificultades de la ciberdefensa del ejercito del Perú, concluyendo la existencia insuficiencias en capacitación, falta de recursos, aplicación inadecuada e incumplimiento de procedimientos en ciberdefensa.

En función de situarnos en el contexto de la ciberdefensa en Ecuador y específicamente enfocada a la Fuera Terrestre, la literatura es escasa pero se ha identificado las siguientes investigaciones en el entorno nacional.

Castro (2015), en su trabajo de investigación determina lo factores fundamentales relacionados para el estudio prospectivo de la ciberdefensa en las FFAA

para el año 2017, presenta escenarios y las estrategias para la ciberdefensa para el Ecuador.

Vargas (2017), en su estudio trata sobre la ciberdefensa y ciberseguridad en el Ecuador, realiza un examen analítico conceptual de seguridad y defensa, proponiendo un modelo de gobernanza en ciberdefensa del Ecuador, sus hallazgos demuestran una incipiente reflexión respecto a esfuerzos Interagenciales para su institucionalización.

Sobre la base de la literatura expuesta, se identifican que actualmente el Ecuador está expuesto a ciberataques, ubicándose como unos de los principales objetivos de los atacantes a nivel global y entre los países más afectados a nivel Latinoamericano.

Respecto a las investigaciones o estudios relacionados con el problema, no se ha identificado trabajos aplicados a la FT del Ecuador, puesto que la conceptualización de ciberdefensa es relativamente nueva y como referencia su adopción inicia en el 2011 en la Organización del Tratado del Atlántico Norte (OTAN) con la aprobación del nuevo concepto de ciberdefensa de la Alianza (Bejarano, 2011), como otro ejemplo es España que lo adopta en el 2018 mediante el concepto de ciberdefensa que tiene la finalidad de proporcionar un marco conceptual para orientar el dearrollo doctrinal y el proceso de implementación en el área de la defensa (Centro Conjunto de Desarrollo de Conceptos [CESEDEN], 2018).

Fundamentación Teórica

Fundamentación Teórica General

Es imprescindible para una adecuada comprensión del entorno de la investigación, iniciar la fundamentación teórica con definiciones básicas en el contexto de la ciberdefensa, las cuales se describen a continuación.

A nivel global se inicia con la utilización de la terminología cibernética o cybernetic, de origen griego κυβερνήτης, cuyo significado es piloto o timón, este término es asimilado por el matemático Wiener (1948), que la define como la tecnología de los sistemas de control, de este se desprende como prefijo el termino ciber o cyber, el cual indica relación con las redes informáticas (Real Academia Española, 2019).

La conceptualización de ciberespacio es difundida por primera ocasión a través del libro Neuromancer de Gibson (1984), el cual la describe como el entorno virtual de sus escritos. Según la Real Academia Española el ciberespacio es definido como el "Ámbito virtual creado por medios informáticos" (Real Academia Española, 2019).

En la doctrina en vigencia de la FT o CCFFA del Ecuador no existe una conceptualización de ciberespacio, ciberdefensa, ciberseguridad y otros términos relacionas a los descritos. Siendo imprescindible presentar algunas conceptualizaciones de estos y otros términos.

> El ciberespacio es un dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de tecnología de la información y datos residentes, incluida Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados. (Joint Chiefs of Staff, 2018, p. 100)

En función del ámbito de aplicación en el contexto de seguridad y defensa el ciberespacio se conceptualiza como:

> Es así como surge el concepto de ciberdefensa, al agrupar el conjunto de medidas y acciones que se adaptan a este entorno dinámico y son capaces de proporcionar un tipo de protección de la información y los sistemas que la manejan acorde a este nuevo escenario.(Escuela de Altos Estudios de la Defensa de España, 2014, p. 17)

A continuación se cita a la conceptualización de ciberseguridad desarrollada por organismos internacionales.

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. (Unión Internacional de Telecomunicaciones, 2010, p. 20)

El Ministerio de Defensa de España a través de Escuela de Altos Estudios de la Defensa de España (2014), en la publicación de Documentos de Seguridad y Defensa, en función del conceto estratégico de la OTAN, desarrollado en la cumbre de Lisboa en 2010, describe la definición de ciberdefensa.

> ciberdefensa, como aplicación de medidas de seguridad para la protección y reacción frente a ataques cibernéticos contra las infraestructuras de las TIC, requiere una capacidad de preparación, prevención, detección, respuesta, recuperación y extracción de lecciones aprendidas de los ataques que podrían afectar a la confidencialidad, integridad y disponibilidad de la información, así como a los recursos y servicios de los sistemas de las TIC que la procesan (p. 41)

El Ejército de Chile por medio del Centro de Estudios Estratégicos de la Academia de Guerra (2018), en su publicación define a la ciberdefensa como:

> Contempla la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. Por ello, la ciberdefensa se relaciona con el desarrollo y aseguramiento de capacidades, preocupándose de sus recursos, actividades, tácticas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios para garantizar el libre acceso al ciberespacio. (p. 66)

La consultora de tecnología INDRA conceptualiza desde el enfoque militar a la ciberdefensa como “se centra en las medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, e incluye las capacidades de reacción y ataque propias de un conflicto armado” (Batanero, 2013, p. 16).

Ataque, se la define como “ una agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema” (Arribas, 2011, p. 8).

Ciberataque, se define como una “acciones hostiles desarrolladas en el ciberespacio con el objetivo de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica, componente lógico o interacciones de éste y pueden tener distintos niveles según su duración, frecuencia y daño generado” (Ministerio de Defensa Nacional Chile, 2015, p. 14).

Vulnerabilidad de seguridad, se define como “un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema” (Arribas, 2011, p. 8).

Política de seguridad, “es el conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema con el propósito de proteger sus recursos críticos y sensibles” (Arribas, 2011, p. 8).

Amenaza, en seguridad de TIC es, “una violación de la seguridad en potencia, que existe a partir de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún daño en el sistema” (Arribas, 2011, p. 8).

Se debe considerar también que la garantía de las propiedades de la información o datos en el ciberespacio deben cumplir ciertas propiedades que incluyen a la disponibilidad, integridad que puede incluir la autenticidad y el no repudio, y confidencialidad (Unión Internacional de Telecomunicaciones, 2010).

Fundamentación Teórica Específica

Ciberdefensa. Constituye actualmente un paradigma[9], una nueva área que se proyecta como una necesidad de los Estados, entidades y organismos públicos o privados y hasta el nivel de la ciudadanía.

El Ministerio de Defensa Nacional del Ecuador (MIDENA) ya incluye al ciberespacio, ciberseguridad, ciberataques y ciberdefensa entre otros en su política de 2018 y Plan Específico de Defensa 2019-2030. A pesar que no los conceptualiza, este desarrolla una aproximación.

Territorio Nacional. El MIDENA ya incluye al ciberespacio y lo describe como “En el dimensionamiento del territorio nacional, que incluye el ciberespacio, se presentan otros tipos de amenazas que, inevitablemente, pueden afectar la soberanía y el bienestar de la sociedad” (Ministerio de Defensa Nacional del Ecuador, 2019, p. 14).

> El ciberespacio implica ampliar la territorialidad, lo que conlleva el incremento de actividades ilegales en esta dimensión. El empleo del manejo de las tecnologías de la información y comunicaciones (TIC) y redes informáticas vulneran la

[9] Paradigma: ejemplo o ejemplar. Teoría o conjunto de teorías cuyo núcleo central se acepta sin cuestionar y que suministra la base y modelo para resolver problemas y avanzar en el conocimiento

> seguridad y defensa de los Estados, a través de ciberataques como: phishing, hacking, cracking hasta ciberterrorismo, los cuales pueden afectar la infraestructura crítica del Estado. (Ministerio de Defensa Nacional del Ecuador, 2019, p. 24)

Ciberataques. Se describen como los ataques que "se basan en la vulnerabilidad que tienen las redes informáticas, pudiendo afectar incluso la infraestructura crítica del Estado, una parte de la cual es responsabilidad de las Fuerzas Armadas" (Ministerio de Defensa Nacional del Ecuador, 2019. pp. 34-36).

Ciberdefensa. A pesar de que no existe una definición o conceptualización propia a cargo del MIDENA o CCFFA se puede referenciar un acercamiento a la misma como:

> a través de un sistema de ciberdefensa que proteja el ciberespacio; puesto que como afirma Nieto(2016) la ciberdefensa debe ser considerada como una "capacidad y una oportunidad estratégica del Estado, […] no hacerlo significaría quedar a merced de las ciberactividades destructivas y resistirse a creer que el campo de batalla del futuro estará en el ciberespacio" (Nieto, 2016, como se citó en Ministerio de Defensa Nacional del Ecuador, 2019, p. 36).

Dentro de un entorno militar, se desarrollan una serie de conferencias a nivel regional respecto a la ciberdefensa, dentro de las cuales se puede referenciar al ciclo de conferencias en línea, webinar[10] sobre ciberdefensa en el ámbito de España y Latinoamérica, CIBERDEFENSA ¿cómo enfrentar este nuevo dominio militar? (Empresa DarFe, 2019) que describe ponencias contrastadas de autores militares y de

[10] Webinar, de Web y seminario, conferencia interactiva en línea por internet, desarrollo de la web 2.0

la sociedad civil. En estas se propone una visión militar y empresarial de la ciberdefensa en los niveles táctico técnico, operacional gerencial y estratégico directivo.

Nivel Táctico – Técnico de la ciberdefensa. Desde la visión militar el Mayor Regueira (2019) del ComDCiber del Brasil propone que el contexto militar debe dirigirse a una elevada capacitación técnica mediante fuentes abiertas y pagadas, se debe compartir información mediante colaboración y entrenamientos constantes por medio de competiciones internas y externas para pensar y actuar en este ambiente con presión. El ponente proporciona fuentes de capacitación abiertas y pagadas en el área de ciberdefensa que a continuación se describen:

- Fuentes de pagos:
    - Instituto Sans.
    - Offensive Security, con cursos online o cursos presenciales.
    - Pentester Academy, con laboratorios online.
- Fuentes abiertas:
    - Open Security Training, capacitación de técnicas ofensivas como defensivas.
    - Cybray, como fuentes de pagos y cursos libres.
    - Corelan Team, conocimientos básicos.
    - Hack the Box, capacitación de seguridad ofensiva, criptografía, ataque a plataformas web, etc.

Malvacio (2019) como investigador de la facultad de Ingeniería del Ejército argentino, en su ponencia ¿Cómo enfrentar este nuevo dominio militar? Nivel Táctico y Técnico, propone que el nivel táctico-técnico como el procedimental de seguridad, ataque, defensa, forense y análisis en general; fortaleciendo la capacitación con el entrenamiento de 2 equipos Blue Team y Red Team.

El Equipo Azul como un equipo de seguridad defensiva, una analogía dentro de la ciberdefensa y un equipo rojo encargo de realizar ataques al propio organismo. El ponente propone como metodología de formación y capacitación en este nivel a los siguientes:

- Ejercicio del tipo CTF (Capture The Flag).
- Formación académica, con carreras de grados, posgrados o cursos en universidades o institutos.
- Cursos técnicos por empresas externas: penetration test, ethical hacker, linux, redes, entre otros.
- Certificación de Ethical Hacking, Penetration Test, Offensive Security, ISACA.

Nivel Operacional – Gerencial. Desde el punto de vista militar, el nivel operacional establece los modos por los cuales él se llevará adelante la campaña. Define los efectos que el nivel táctico va a tener que cumplir en las operaciones militares (Cicerchia, 2019).

Cicerchia (2019) en su ponencia describe al diseño operacional como un método común en muchas fuerzas armadas en este nivel, siendo un método de resolución de problemas, resalta que actualmente es empleado un oficial de ciberguerra o ciberdefensa, quién está vinculado con el oficial de comunicaciones y guerra electrónica, con el de operaciones de información, el de inteligencia, entre otros.

El conferencista describe los pasos del diseño operacional aplicado a la ciberdefensa, resaltando la identificación del problema, los elementos del ciber ambiente, el centro de gravedad, análisis de modos de acción y tareas, líneas de operación ciber y resolución del comandante entre otras.

En este nivel Carneiro (2019) analiza la teoría de la emulación militar, que la define como una imitación voluntaria, sistemática y deliberada para que un Estado se actualice o modernice.

En función que la innovación puede resultar arriesgada esta teoría considera tres tipos de isomorfismos. El primero es el mimético, en el cual sólo se copian los modelos considerados como exitosos; el segundo es el coercitivo, es el que sucede cuando se tiene necesidad de esfuerzos de estandarización y de interoperabilidad; y el tercero el normativo, el cual suman los estándares, lecciones aprendidas, la experiencia profesional, y se adapta (Carneiro, 2019).

Nivel Estratégico – Directivo. En función de los avances tecnológicos se ha desarrollado un ambiente virtual o del ciberespacio, que se considera un ambiente estratégico, Moresi (2019) describe en su exposición esa evolución, la influencia de la tecnología y determina que el conflicto del ciberespacio en occidente se enfoca solo a la seguridad informática y ciberdefensa, pero que conlleva un enfoque a nivel mundial que consideran tres niveles que son la Información, ciberdefensa y seguridad informática; los niveles táctico, operacional y estratégico en el ciberespacio tiene una relación, el estratégico dirige, el operacional genera las mejores condiciones y el táctico ejecuta.

El conflicto del ciberespacio es dictado por la interdisciplinaridad, en la que intervienen muchas áreas del conocimiento como la neurociencia, la psicología social, la sociología, entre otras que conforman parte de la problemática del ciberespacio. Describe como estrategias principales a crear una cultura del ciberespacio, se debe cambiar el sistema de aprendizaje, el campo de batalla en el siglo 21 es la mente de la sociedad (Moresi, 2019).

Dimensión Política.

Constitución de la República del Ecuador 2008. Es la norma jurídica en vigencia de mayor jerarquía en la República del Ecuador, en referencia a la constitución se desarrollan leyes, códigos o normas jurídicas, en esta se determina los elementos constitutivos del Estado, derechos, garantías constitucionales, participación y organización del poder, organización territorial del Estado, régimen de desarrollo, régimen del buen vivir, relaciones internacionales, entre otras (Constitución de la República del Ecuador, 2008).

En general no se especifica respecto a ciberdefensa, se determina la misión fundamental de FFAA, más información en el Apéndice A.

Código Orgánico Integral Penal. es un conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, que establece delitos y penas conforme al sistema penal ecuatoriano (Código Orgánico Integral Penal [COIP], 2014). Este código se relaciona a delitos informáticos y tecnológicos, pero no considera aspectos sobre ciberdefensa, más información en el Apéndice A.

Ley Orgánica de la Defensa. Con respecto a esta ley debemos considerar las misiones dispuestas para FFAA y el ámbito de aplicación, específicamente no se describen aspectos de ciberdefensa (Ley Orgánica de la Defensa Nacional, 2007). Más información en el Apéndice A.

Ley de Seguridad Pública y del Estado. Esta ley tiene como propósito regular la seguridad integral del Estado ecuatoriano, por medio del Sistema de Seguridad Pública y del Estado (Ley de Seguridad Pública y del Estado, 2009). No se considera a la ciberdefensa, más información en el Apéndice A.

Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público. Este código regulariza la organización, funcionamiento y regímenes administrativos y profesionales de entidades de seguridad ciudadana y orden público (Código Orgánico

de las Entidades de Seguridad Ciudadana y Orden Público, 2017). No considera temas de ciberdefensa, más información en el Apéndice A.

Política de la Defensa Nacional del Ecuador "Libro Blanco". Conceptualiza la política pública de la defensa del Ecuador, definiendo estrategias de defensa y seguridad nacional, política de relaciones exteriores y su contexto, amenazas y riesgos, el escenario de la defensa en el año 2030, planificación para la defensa, estructura militar, seguridad marítima, economía de la defensa y alianzas, y aportes de la defensa al desarrollo nacional (Política de la Defensa Nacional del Ecuador “Libro Blanco”, 2018). En la política se incluyen acercamientos a la conceptualización del ciberespacio, ciberataques, ciberseguridad y ciberdefensa, más información en el Apéndice A.

Libro Blanco de la Sociedad de la Información y del Conocimiento. El libro Blanco de la Sociedad de la Información y del Conocimiento, representa un instrumento dinámico que tiene por objetivo dar a conocer las estrategias desarrollo de la Sociedad de la Información y del Conocimiento en Ecuador (Ministerio de Telecomunicaciones y Sociedad de la Información, 2018a). En este se incluye la seguridad de la información y protección de datos personales, considerando a la ciberseguridad con propuesta de una estructura nacional y desarrollo de una política nacional de ciberseguridad; no se consideran aspectos de la ciberdefensa, más información en el Apéndice A.

Dimensión Militar.

Estructura organizacional de la Ciberdefensa. Se entiende como estructura organizacional, a las diferentes formas que una institución, organización o empresa se organiza interna y externamente tanto para los entes administrativos y operativos.

La ciberdefensa es de valor estratégico, se debe desarrollar en forma constante pero que no se ha convertido en nuestros tiempos en una política de entendimiento

(Carayannis y Campbell, 2018). Comprendiendo que su estructura jerarquía en un Estado es estratégica, pero que debe alcanzar los niveles político y militar.

El Índice Global de Ciberseguridad (GCI[11]), es presentado por la Unión Internacional de Telecomunicaciones UIT[12], como una iniciativa para proporcionar información en relación al incremento de la concientización de la seguridad en el ciberespacio (Unión Internacional de Telecomunicaciones, 2019). Este índice define en sus estudios y mediciones el compromiso que adquieren los países con la seguridad del ciberespacio, en la perspectiva global ubica en primer lugar al Reino Unido, país en el cual la ciberdefensa se encuentra regentada por el Cuartel General de Comunicaciones del Gobierno (GCHQ[13]) entidad responsable de la inteligencia de señales y garantizar la información al gobierno y las fuerzas armadas del Reino Unido.

El ejército del Reino Unido en referencia al desarrollo de su programa de transformación, ha creado un ciber regimiento con el propósito de proteger las redes de defensa y operaciones en general. Se proyecta conformar el Centro de Operaciones de Seguridad de la Información Cibernética del Ejército, teniendo como base al treceavo Regimiento de Señales (13th Signal Regiment) el cual pertenece a la primera brigada de señales (1st (UK) Signal Brigade) bajo el mando operacional de la sexta división (6th (UK) Division) la cual es la responsable de maniobras de información y guerra no convencional. El treceavo Regimiento de Señales constituirá una unidad especializada para la defensa del ciberespacio en coordinación con las fuerzas naval y aérea del Reino Unido para proporcionar redes seguras para las comunicaciones militares (Ministerio de Defensa del Reino Unido, 2020).

---

[11] GCI, Global Cybersecurity Index, Índice Global de Ciberseguridad estudio de Unión Internacional de Telecomunicaciones

[12] UIT, Unión Internacional de Telecomunicaciones o sus siglas en idioma ingles ITU de International Telecommunication Union

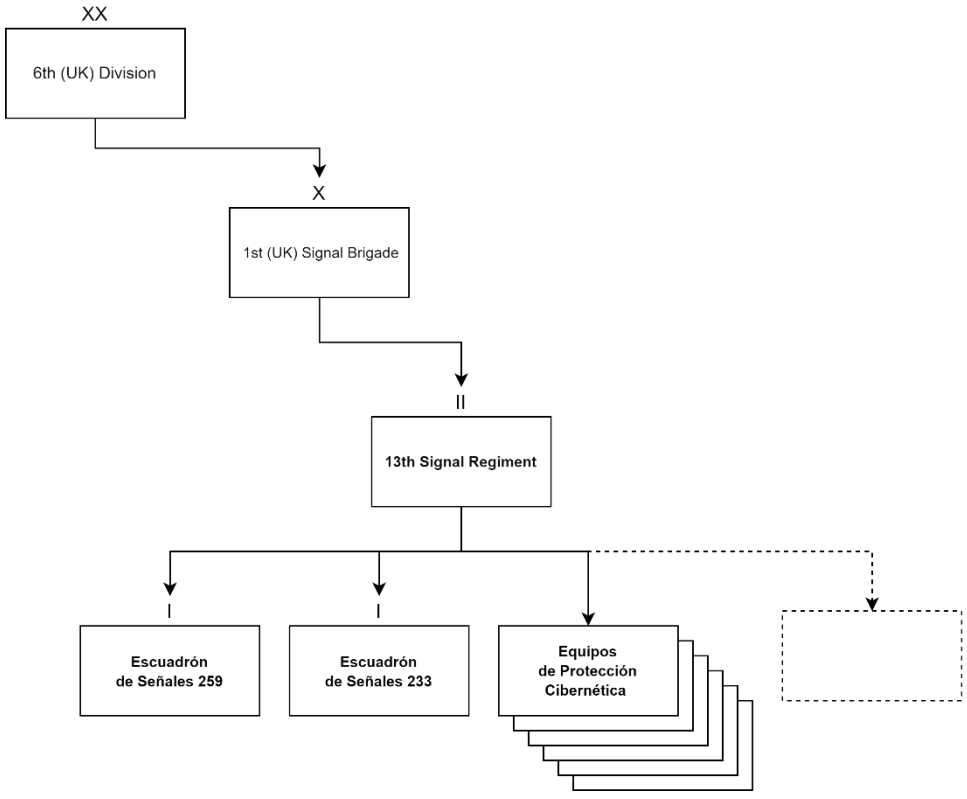
[13] GCHQ, Government Communications Headquarters, Cuartel General de Comunicaciones del Gobierno

Como primera unidad cibernética del ejército su estructura organizacional inicial se compone por el Escuadrón de Señales 259, el Escuadrón de Señales 233 y 6 Equipos de Protección Cibernética (Ejército Británico, 2020).

Este regimiento sigue en desarrollo y busca nuevas funciones cibernéticas para su completamiento con personal del ejército, marina y aviación del Reino Unido. En la figura 9 se representa la estructura organizacional con los escalones superiores y subordinados descritos.

Figura 9

Estructura del regimiento cibernético del Ejército del Reino Unido

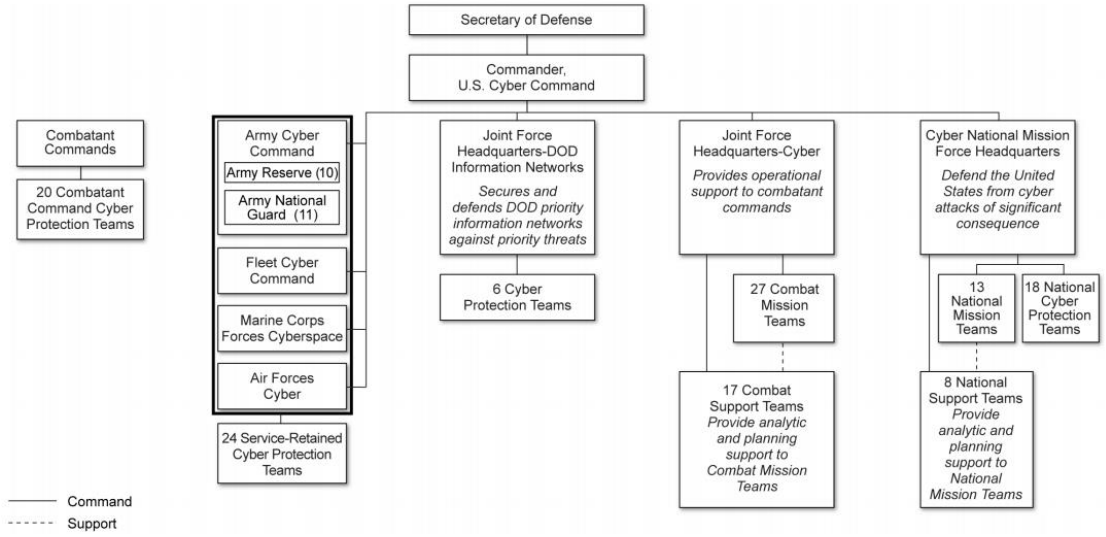


Nota. La línea entrecortada representa a las futuras unidades o elementos cibernéticos. Figura desarrollada por el autor a partir de la información de In Front (p. 31) por el Ejército de Reino Unido, 2020.

La UIT coloca en segunda ubicación a los Estados Unidos de América, en el cual el organismo que gobierna la ciberdefensa es el USCYBERCOM y presenta una estructura como se la ilustra en la figura 10.

Figura 10

Estructura del USCYBERCOM



Nota. Estructura jerárquica del USCYBERCOM. Tomado de *GAO-19-362, DOD TRAINING: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force* (p. 7), por Oficina de Responsabilidad Gubernamental, 2019.

En referencia a esta organización se encuentra como componente el Comando Cibernético del Ejército (ARCYBER[14]) el cual tiene como misión:

> Integra y realiza operaciones de ciberespacio de espectro completo, guerra electrónica y operaciones de información, asegurando la libertad de acción de

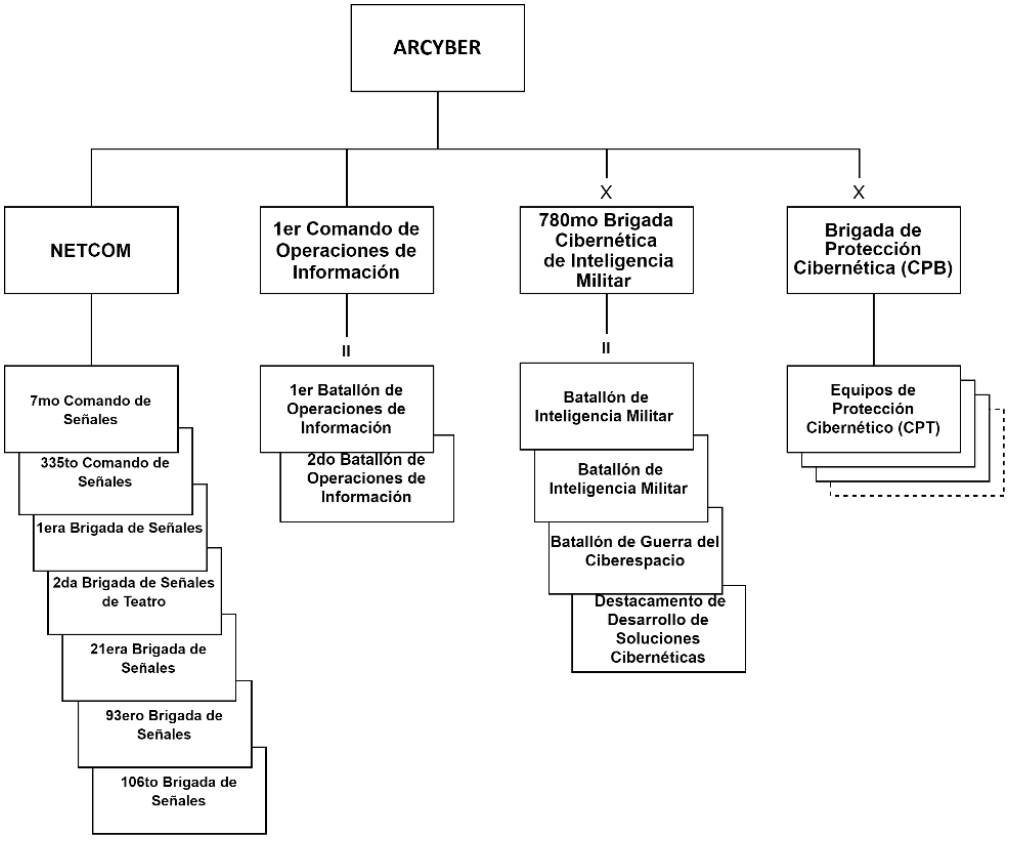
[14] ARCYBER, Army Cyber, Comando Cibernético del Ejército de Estados Unidos

las fuerzas amigas en y a través del dominio cibernético y el entorno de información, mientras niega lo mismo a nuestros adversarios". (Comando Cibernético del Ejército de los Estados Unidos, 2020)

Su estructura se ilustra en la figura 11 compuesta por el Comando de Tecnología Empresarial de Red (NETCOM[15]), Primer Comando de Operaciones de Información (1st Information Operations Command) y 780 ava Brigada de Inteligencia Militar (Cyber).

Figura 11

Estructura organizacional del ARCYBER



Nota. Figura desarrollada por el autor a partir de la información del Comando Cibernético del Ejército de los Estados Unidos, https://www.arcyber.army.mil/.

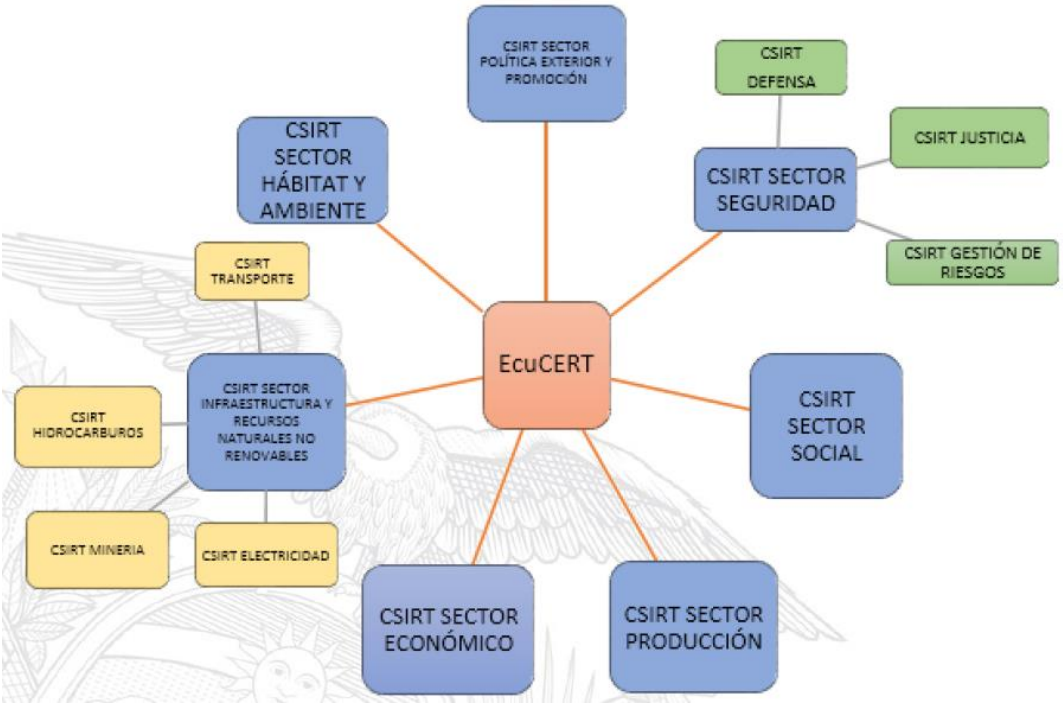
[15] NETCOM Network Enterprise Technology Command, Comando de Tecnología Empresarial de Red

En el Ecuador el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT) de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como entidad adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) es “Reconocido como un CIRT (Critical Incident Response Team) nacional oficial de acuerdo al Índice mundial de ciberseguridad y perfiles de ciberbienestar, de la UIT, 2015.” (Ministerio de Telecomunicaciones y Sociedad de la Información, 2018a, p. 41). Esta entidad define como comunidad objetivo a todos los prestadores de servicios de TIC, instituciones del sector gubernamental, empresas privadas y ciudadanía en general del Ecuador.

La misión del EcuCERT describe “Brindar a su Comunidad Objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico” (Centro de Respuesta a Incidentes Informáticos del Ecuador, 2017) . En la figura 12 se ilustra la estructura propuesta que presenta el MINTEL en base a su Proyecto – Estrategia Nacional de Ciberseguridad (Ministerio de Telecomunicaciones y Sociedad de la Información, 2018c).

Figura 12

Propuesta de la organización nacional del EcuCERT



Nota. Tomado de *Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad* (p. 27), por la ARCOTEL, 2018.

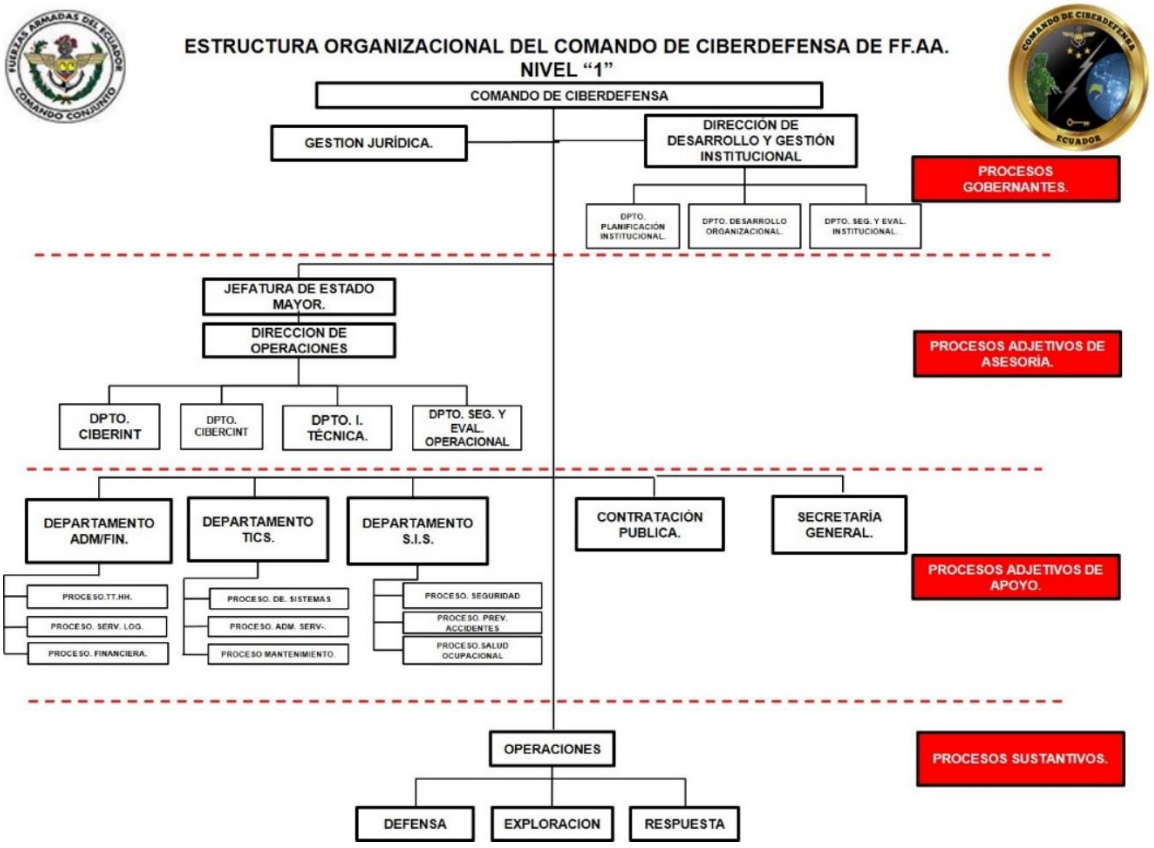
El Comando Conjunto de las Fuerzas Armadas del Ecuador (CCFFAA) en función de su estatuto orgánico por procesos en vigencia define en su estructura institucional a la Gestión de Ciberdefensa Militar, como:

> Efectuar operaciones de defensa y exploración en el Ciberespacio en forma permanente, protegiendo la infraestructura crítica tecnológica de Fuerzas Armadas y otras asignadas, degradando o neutralizando la infraestructura crítica tecnológica del adversario con orden, a fin de contribuir al cumplimiento de la misión del Comando Conjunto de las Fuerzas Armadas. (Comando Conjunto de las Fuerzas Armadas del Ecuador, 2018, p. 10).

En la figura 13, se ilustra la propuesta de estructura organizacional para el Comando de Ciberdefensa (COCIBER) de las FFAA. Esta estructura se orienta a los procesos, identificándose a los gobernantes, adjetivos de asesoría, adjetivos de apoyo y sustantivos. No se identifica en su estructura propuesta el relacionamiento estructural o en base a procesos con las Fuerzas Terrestre, Naval y Aérea.

Figura 13

Estructura organizacional propuesta del COCIBER



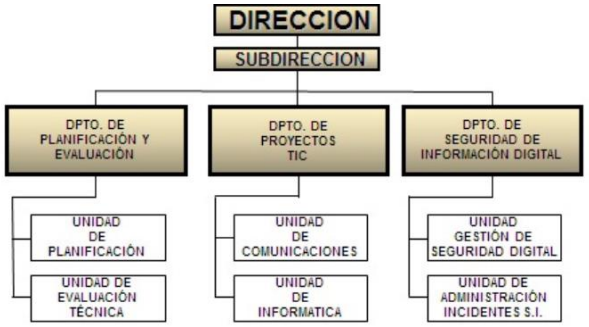
Nota. Se ilustra la estructura organizacional del COCIBER sin identificarse la relación con la FT. Tomado de *Propuesta Estructura Organizacional del COCIBER* (p. 2), por COCIBER, 2019.

En la organización actual de la FT no contempla un área o unidad específica de ciberdefensa o ciberseguridad que dependa o no del COCIBER. En la figura 14 se ilustra la organización estructural de la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), en la cual se identifica al Departamento de Seguridad de la Información Digital, el cual se rige al Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC27000[16] esta establece una serie de recomendaciones para la seguridad de la información y mejora continua (Ministerio de Telecomunicaciones y Sociedad de la Información, 2019). El esquema gubernamental no reemplaza a los estándares internacionales o nacionales referentes a la seguridad de la información.

En función del EGSI la FT emite el Esquema de Gestión de Seguridad de la Información Digital de la FT (EGSID) en la cual se define su estructura que se ilustra en la figura 15.

Figura 14

Orgánico estructural de la DTIC



Nota. En la estructura se identifica los departamentos de la DTIC y sus dependencias subordinadas. Tomado de *Orgánico estructural de la DTIC de la FT.*

[16] Es una traducción idéntica de la Norma Internacional ISO/IEC 27000:2016, Information technology - Security techniques - Information security management systems — Overview and vocabulary

Figura 15

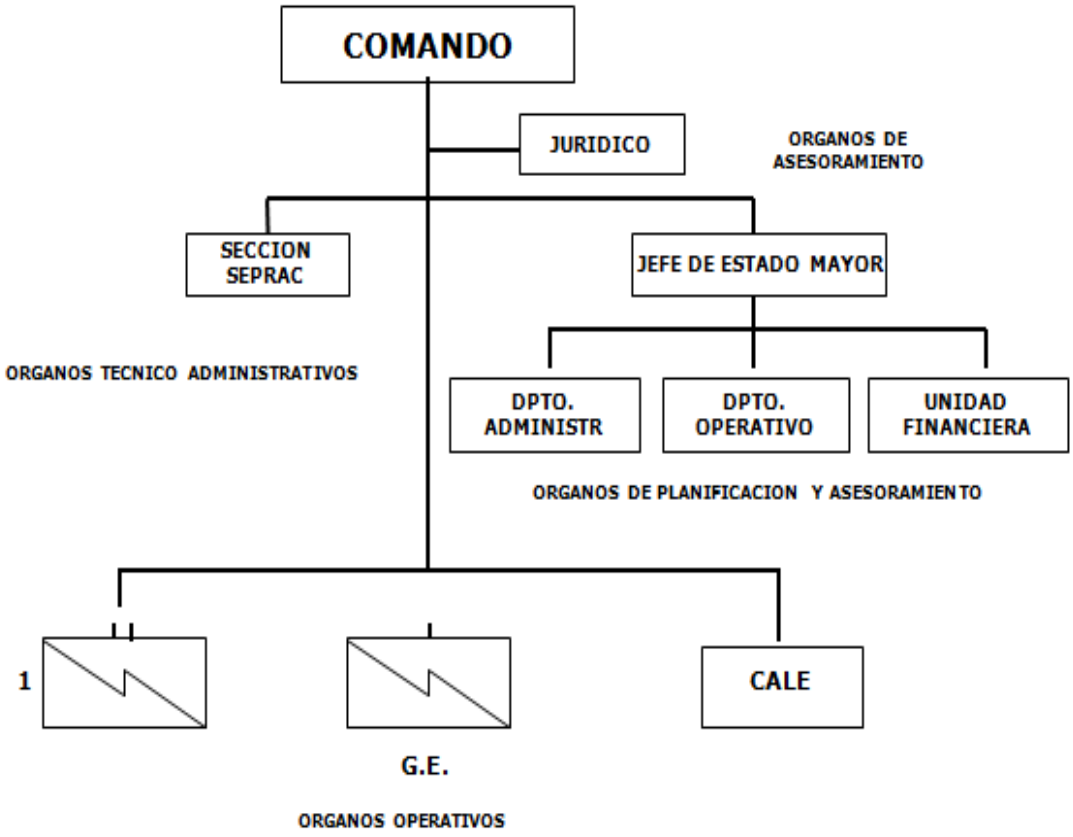
Estructura de Seguridad de la Información de la DTIC

Nota. En la figura se ilustra la estructura de seguridad de la información digital a responsabilidad de la DTIC. Tomado de *Esquema de Gestión de Seguridad de la Información Digital de la FT (EGSID) - V.1* (p. A-3), por la DTIC, 2018.

La figura 16 ilustra la organización actual del Agrupamiento de Comunicaciones y Guerra Electrónica (AGRUCOMGE) de la FT, en el cual no presenta una unidad o dependencia específica de ciberdefensa, ciberseguridad u operaciones en el ciberespacio, que dependa o no del COCIBER, en su estructura comprende a la Compañía de Guerra Electrónica la cual no tiene ninguna función de ciberdefensa o ciberseguridad. En la figura 17 se observa la organización del Batallón de Comunicaciones N° 1 (BC 1) en su estructura no incluye ninguna unidad o dependencia específica de ciberdefensa, ciberseguridad u operaciones en el ciberespacio.

Figura 16

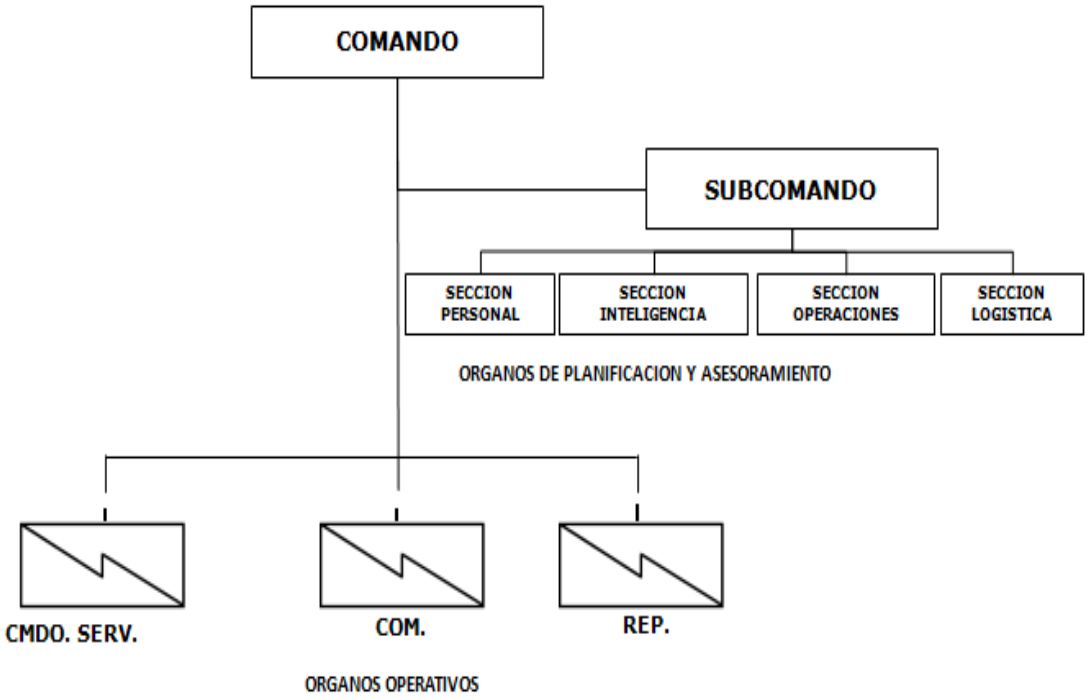
Estructura del AGRUCOMGE de la FT



Nota. La estructura del AGRUCOMGE comprende al BC 1, Compañía de Guerra Electrónica y al Comando de Apoyo Logístico Electrónico. Tomado del *Manual de Comunicaciones del Ejército* (p. 28), por la Dirección de Doctrina, 2010.

Figura 17

Estructura del BC 1



Nota. El BC 1 se estructura con una compañía servicios, compañía comunicaciones y compañía de repetidoras. Tomado del *Manual de Comunicaciones del Ejército* (p. 29), por la Dirección de Doctrina, 2010.

Dimensión de TIC.

Personal capacitado en Ciberdefensa. La capacitación en ciberdefensa en la actualidad constituye una nueva área que agrupa a diferentes áreas del conocimiento como la seguridad informática, seguridad de información, seguridad de tecnologías, seguridad de TIC, seguridad física, gestión de tecnologías, entre otras.

En la fundamentación teórica en el numeral de ciberdefensa en el contexto militar se especifica varios tipos de capacitación.

En referencia al GCI, este indicador mide la existencia de un marco aprobado a nivel gubernamental para la certificación y acreditación de profesionales por estándares de seguridad cibernética internacionalmente reconocidos, estas certificaciones, acreditaciones y estándares incluyen, entre otros, los siguientes:

> Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute, CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc. (Unión Internacional de Telecomunicaciones, 2019, p. 73)

La capacitación requiere de programación. La cual se refiere a la existencia de programas educativos y profesionales a nivel local, nacional o internacional, en el contexto de seguridad cibernética o ciberseguridad, ciberdefensa y la promoción de la certificación de la industria. La educación incluso debe considerar niveles desde la educación primaria, secundaria, superior y profesional (Unión Internacional de Telecomunicaciones, 2019).

En general las habilidades relacionadas con la seguridad cibernética o ciberseguridad y ciberdefensa incluyen profesiones que se relacionan con la seguridad

de TIC incluyendo la dimensión del ciberespacio, criptoanalistas, forenses digitales, equipos de respuesta a incidentes de seguridad de TIC, arquitectos y diseñadores de seguridad de TIC, verificadores de seguridad y programas de educación superior relacionados con las ciencias de seguridad y defensa, computación, eléctrica, electrónica y telecomunicaciones, tanto de tercer o cuarto nivel.

La capacitación debe estar relacionada a procesos y procedimientos de investigación, desarrollo e innovación (I+D+i), considerando aspectos como el análisis de malware, criptografía, identidad digital, vulnerabilidades de TIC, conceptos de seguridad y gestión de seguridad del ciberespacio.

Dimensión Recursos.

Asignación Presupuestaria e infraestructura. Se refiere a los planes operativos y techos presupuestarios señalados por el Ministerio de Economía y Finanzas (MEF), que cada institución establece con los montos para los programas a incorporarse en las proformas presupuestarias y su distribución a cada unidad ejecutora. Cada institución verificará que la agregación de los montos a cada unidad ejecutora que dependen de los programas, sin que se exceda del techo presupuestario y de excederse se deberá reformulará las metas del plan operativo y ajustará la asignación de recursos hasta igualar al techo presupuestario (Ministerio de Economía y Finanzas, 2018).

Dentro del contexto de seguridad cibernética o ciberseguridad y ciberdefensa, la infraestructura comprende todo el hardware y software que se encuentra interconectada al ciberespacio. La infraestructura en general se proyecta hacia las redes de nueva

generación (NGN[17]) estas nuevas redes son respaldadas y desarrolladas por la UIT que la definen como:

> Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios. (Unión Internacional de Telecomunicaciones, 2004, p. 8)

Esta nueva generación de infraestructura contiene sus redes basada en paquetes IP, prevé independencia entre la provisión de servicios y tecnologías de transporte de datos que incluye calidad de servicio (QoS[18]) y calidad de experiencia (QoE[19]) de extremo a extremo lo cual garantiza la calidad al usuario o cliente final.

Dimensión Normativa

Plan Nacional de Desarrollo 2017-2021. En la planificación no existe ningún aspecto o apartado que explícitamente tenga referencia a la seguridad cibernética o ciberseguridad, ciberdefensa, seguridad informática, seguridad de la información y seguridad de TIC. El lineamiento que se puede considerar de aporte y da valor para el presente documento es el objetivo 9, que describe “Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo” (Secretaría Nacional de

[17] NGN, del idioma inglés Next Generation Networks, Redes de Nueva Generación según grupo de la UIT
[18] QoS, del idioma inglés Quality of Service, Calidad de Servicio en redes y telecomunicaciones
[19] QoE, del idioma inglés Quality of Experience, Calidad de Experiencia en servicios en redes y telecomunicaciones

Planificación y Desarrollo, 2017, p. 104) , el campo de acción de este enunciado es muy amplio y sin duda implica la actuación de FFAA, más información en el Apéndice B.

Plan Específico de Defensa 2019-2030. En este plan que presenta el MIDENA se sustenta en la defensa y seguridad del Ecuador, tiene el propósito de pasar de una planificación a corto plazo a una prospectiva, para optimizar los recursos del Estado (Ministerio de Defensa Nacional del Ecuador, 2019). En el plan se presenta la importancia del ciberespacio, ciberseguridad y ciberdefensa, existiendo un acercamiento a su conceptualización, más información en el Apéndice B.

Plan de la Sociedad de la Información y del Conocimiento. Se presenta como un plan para el período 2018-2021. En su sitio web oficial el plan se exhibe como borrador. El plan constituye una herramienta de planificación para el desarrollo de las áreas de la sociedad de la información y del conocimiento. Contiene cinco ejes estratégicos, seis programas y varios proyectos.

EL plan tiene como misión fundamental "… convertirse en el instrumento de planificación y gestión de las tecnologías de la información y comunicación que articule las políticas de desarrollo sectorial e intersectorial en materia de la sociedad de la información y comunicación" (Ministerio de Telecomunicaciones y Sociedad de la Información, 2018b, p. 17). En el plan se involucra a varias instituciones gubernamentales, privadas, organizaciones sin fines de lucro, académicas entre otras, como actores en su desarrollo y conformación de mesas de trabajo. En ningún contexto consideran al Ministerio de Defensa Nacional o FFAA, como actor o miembros de mesas de trabajo, únicamente como alianzas estratégicas.

Los ejes que se relacionan a la seguridad cibernética o ciberseguridad y ciberdefensa, son el primer eje de infraestructura digital, seguridad de la información y uso responsable de las TIC y el quinto de protección de datos personales. Respecto a

los programas y proyectos específicos del primer y quinto eje, , más información en el Apéndice B.

Plan de Gestión Institucional de la Fuerza Terrestre 2017-2021. Este plan considera como un objetivo el incrementar las capacidades militares. En mencionado objetivo se enuncia el de fortalecer la capacidad de ciberdefensa, describiendo en su numeral 3 “En coordinación con el CCFFAA capacitar, entrenar y dotar de equipos de tecnología moderna que requieran las unidades del Ejército para cumplir las misiones que se le asignen en este ámbito” (Fuerza Terrestre, 2017, p. 5).

En referencia al objetivo y numeral descrito, no se ha plasmado en programas o proyectos para su desarrollo y cumplimiento, más información en el Apéndice B.

Procedimientos de Ciberdefensa o afines (directivas, planes, instructivos y/o procesos). En función de la revisión documental desarrollada en las en las unidades o dependencias de la investigación, a continuación se enumera los documentos relacionados a la seguridad cibernética o ciberseguridad, ciberdefensa, seguridad informática, seguridad de la información y seguridad de TIC, más información en el Apéndice B.

COCIBER:

- Manual Organizacional del COCIBER.

DTIC de la FT:

- Esquema Gubernamental de Seguridad de la Información EGSI.
- Esquema de Gestión de Seguridad de la Información Digital de la FT. (EGSID)–v.1.
- Manual de Procesos Gestión de Tecnologías de la Información y Comunicaciones (Seguridad Tecnológica).

- Instructivo FT-DTIC-2019-005-C-INS, asunto: Implementar medidas de seguridad informática en la Fuerza Terrestre.

En la actualidad existen diversas normas de buenas prácticas referentes al marco de seguridad cibernética o ciberseguridad, seguridad informática, seguridad de la información y seguridad de TIC. Las normas en general no consideran una normativa de ciberdefensa. Entre los estándares de mayor impacto se describen sucintamente a las siguientes:

- La UIT con sus buenas prácticas o normas NGN, seguridad en las redes de información y comunicación, GCI y conceptualización de ciberseguridad.
- Biblioteca de Infraestructura de Tecnologías de Información (ITIL), se considera la gestión de seguridad de tecnologías de información.
- Organización Internacional de Normalización (ISO) con la ISO 20000, referente a la calidad de servicios de TIC.
- La ISO y la Comisión Internacional de Electrotécnica (IEC), con la ISO/IEC 27000, respecto a la seguridad de la información.
- La Asociación de Auditoría y Control de Sistemas de Información (ISACA) con su estándar Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT), proporciona un marco de referencia para el gobierno IT y gestión de la seguridad de la información.
- Instituto Nacional de Estándares y Tecnología de los Estados Unidas (NSIT) con SP 800, constituye la serie 800 de Publicaciones Especiales (SP) respecto a la seguridad informática.
- Instituto para la Seguridad y Metodologías Abiertas (ISECOM), es una organización de usuarios abierta, no gubernamental, no lucrativa cuyo

objetivo es la concienciación, investigación y certificación en materia de seguridad de los sistemas de información, con su metodología por medio del Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM) para la auditoría de los sistemas de información.

- Proyecto Abierto de Seguridades de Aplicaciones web (OWASP), con el propósito de facilitar a las organizaciones la información y los medios para desarrollar, adquirir y mantener, de manera segura, aplicaciones basadas en tecnologías de Internet, también llamadas comúnmente aplicaciones web.
- Penetración tes de ejecución estándar (PTES) referentes a un conjunto de tipos de pruebas que, de manera más realista, evalúa la situación de la seguridad de una infraestructura TIC.
- Grupo de Servicio de Seguridad de Información Abierta (OISSG), proyecto enmarcado dentro del conjunto de metodologías surgidas del movimiento de software libre para proporcionar herramientas de auditoría de sistema.

Base Legal

El presente trabajo de investigación se fundamenta en la siguiente base legal:

- Constitución de la República del Ecuador 2008.
- Ley Orgánica de la Defensa.
- Código Orgánico Integral Penal.
- Ley de Seguridad Pública y del Estado.
- Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público.
- Política de la Defensa Nacional del Ecuador "Libro Blanco".

- Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad “Libro Blanco de la Sociedad de la Información y del Conocimiento”.
- Plan Nacional de Desarrollo 2017-2021.
- Plan Específico de Defensa 2019-2030.
- Plan de la Sociedad de la Información y del Conocimiento.
- Plan de Gestión Institucional de la FT 2017-2021.

Hipótesis

La débil o limitada Ciberdefensa de la FT incide en la seguridad datos e infraestructura de TIC.

Sistema de Variables

Variable Independiente

Ciberdefensa.

Variable Dependiente

Seguridad y defensa de datos e infraestructura de TIC.

Conceptualización y Operacionalización de las variables

En la tabla 1 se desarrolla y describe la conceptualización y operacionalización de la variable independiente y dependiente.

Tabla 1

Conceptualización y Operacionalización de las variables

Variable	Dimensión	Indicadores	Ítem
Independiente: Ciberdefensa Conceptualización: Conjunto de técnicas, métodos, procesos y gestión para la protección y defensa de datos e infraestructura.	Política	– Constitución de la República del Ecuador 2008. – Código Integral Penal – Ley Orgánica de la Defensa. – Ley de Seguridad Pública y del Estado. – Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público. – Política de la Defensa Nacional del Ecuador "Libro Blanco". – Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad “Libro Blanco de la Sociedad de la Información y del Conocimiento”.	Revisión bibliográfica Encuesta
	Militar	– Estructura organizacional de la ciberdefensa.	Revisión bibliográfica Encuesta
	TIC	– Personal capacitado en ciberdefensa.	Revisión bibliográfica Encuesta
	Recursos	– Asignación Presupuestaria e infraestructura.	Encuesta
	Normativo	– Plan Nacional de Desarrollo 2017-2021. – Plan de la Sociedad de la Información y del Conocimiento. – Plan de Gestión Institucional de la FT 2017-2021. – Procedimientos ciberdefensa o afines (Directivas, Planes o Instructivos)	Revisión bibliográfica Encuesta

Variable	Dimensión	Indicadores	Ítem
Dependiente: Seguridad y defensa de datos e infraestructura de TIC. Conceptualización: Es la protección de datos e infraestructura de TIC.	– Defesa de datos e infraestructura	Protección para datos, información e infraestructura de TIC de la FT.	Encuesta

Nota. Esta tabla describe la operacionalización de las variables de la investigación, estableciendo sus dimensiones e indicadores.

Marco Metodológico

El presente trabajo de investigación se desarrolló empleando el método científico, el cual determina las fases de planteamiento del problema, elaboración de la hipótesis, selección de la metodología, prueba de la hipótesis e interpretación de resultados (Abalde y Muñoz, 1992).

Enfoque de la Investigación

El enfoque para la presente investigación científica es la cuantitativa, empleando varios procesos como el deductivo, que va de lo general a lo particular. Se caracteriza por la recolección de datos para comprobar la hipótesis, respaldada por la comprobación numérica y análisis estadístico, este enfoque se describe por ser secuencial y probatorio, ésta parte con la idea, identificación, formulación y delimitación del problema, derivando las preguntas de investigación y objetivos de la misma, complementando una revisión de la literatura para el marco teórico, se define su alcance determinación para la determinación de la hipótesis y variables, diseñamos la investigación, para posterior realizar la recolección, mediciones, análisis e interpretación de datos estadísticos y finalmente elaborar el reporte de resultados, para la comprobación de la hipótesis planteada (Hernández et al., 2014).

Tipo de Investigación

En el presente trabajo, se emplea inicialmente la investigación exploratoria con el propósito de examinar el contexto de la ciberdefensa en la FT, en base a la literatura revisada no existe investigaciones relevantes relacionadas con el problema de estudio, posterior se desarrolla la investigación descriptiva en la cual se busca especificar y analizar las causas más importantes o predominantes de una deficiente ciberdefensa en la Fuera Terrestre, enfocados en las dependencias descritas en la delimitación espacial, se realizará la medición y recolección de datos e información respecto a las variables

operacionalizadas, para luego correlacionarlas mediante la asociación de variables este estudio, procurando responder a las preguntas de investigación planteada, con la finalidad de conocer las relaciones que se determine entre variables del contexto de la ciberdefensa en la FT, requiriendo una cuantificación, análisis y vínculos de las mismas que sustentan a la hipótesis probada, finalmente es necesario que se aplique una investigación explicativa, la cual se dirige a exponer por qué ocurre un fenómeno específico o la relación entre variables, estableciendo las causas de los sucesos (Hernández et al., 2014). Esto definirá la base para la propuesta de solución mediante nuevos conocimientos, estructuras, tecnologías, técnicas, modelos de gestión, entre otros.

Población

Campo de Acción

Ciberdefensa

Población

Las unidades de análisis corresponden a la Direcciones de Comunicaciones e Informática de la FT y Agrupamiento de Comunicaciones y Guerra Electrónica, descritas en la delimitación espacial y como población se considerarse al personal militar y de servidores públicos involucrados y especialistas en ciberdefensa, seguridad informática, seguridad de información y seguridad de TIC.

Muestra

Se define una muestra no probabilística o también llamada dirigida, en función que la investigación está orientada a un grupo específico y que no depende de la probabilidad, ni se fundamenta en formulas, se basa en las características propias de la exploración, para el presente trabajo el grupo de expertos especifico del personal militar y de servidores públicos especialistas en seguridad cibernética o ciberseguridad,

ciberdefensa, seguridad informática, seguridad de la información y seguridad de TIC. La población se define con 4 oficiales, 31 voluntarios y 5 servidores públicos, danto un total de 40.

Métodos de Investigación

El método desarrollado en el presente trabajo es el Hipotético-Deductivo, en función de su enfoque cualitativo, que inicia con el planteamiento y formulación del problema, para posteriormente elaborar la hipótesis, determinándose las consecuencias de la hipótesis para ser contrastada y comprobada.

Las características de la investigación en el contexto de la ciberdefensa en la FT, requieren una fundamentación teórica, con variables y dirigido hacia datos medibles que definirán el problema y que permitan plantear una hipótesis que puedan ser contrastadas.

Técnicas de recolección de Datos

Entre las principales técnicas de recolección de datos usados son la revisión bibliográfica, documental y encuestas en línea.

Revisión Bibliográfica o de la literatura, que inicia desde la generación de ideas y planteamiento del problema respecto al tema investigado, consiste en una revisión analítica que implica la detección, consulta y obtención de bibliografía, que son útiles para el desarrollo de la investigación (Hernández et al., 2014). La obtención debe ser selectiva en función que para las publicaciones académicas, se consideran la relevancia de revistas y autores, impacto en la comunidad académica, relación con el contexto del problema y enfoque de investigación. En la revisión y selección de la literatura, se obtiene las referencias bibliográficas, las cuales son útiles para fundamentar el marco teórico y dirigir la investigación, se utiliza fuentes primarias de base de datos cerradas y abiertas como ProQuest, Scopus, Dialnet, Web of Science, Google Scholar, Open

Directory of Open Access Journals, Hindawi, Scielo, entre otras de no menor importancia.

Revisión Documental, respecto a los documentos relacionados con la ciberdefensa, seguridad informática, seguridad de la información y/o seguridad de TIC, obtenidos en la DTIC y AGRUCOMGE, en referencia a la delimitación espacial, pero adicional también se realizó la revisión documental del escalón superior que para el contexto de la investigación es el COCIBER.

Registros de datos estadísticos, fundamentado en la base de datos de la empresa o consultora Statista, el cual es un portal de estadísticas a nivel mundial en línea, centradas en industrias, mercados, consumidores, tendencias y conocimientos especializados, que para nuestro trabajo de investigación nos centramos en las industria de la seguridad de Tecnologías de la Información, seguridad de software, Internet y Cyber Crimen, facilitando el desarrollo de la definición del problema, antecedentes, marco teórico y para los análisis de los contextos global y regional.

Encuestas, en base que el enfoque cuantitativo del trabajo de investigación, se plantea como técnica de recolección de datos a la encuesta, dirigida hacia una población específica, esta se aplica en el entorno de la FT.

Instrumentos de Recolección de Datos

La recolección de datos cuantitativos se efectúa a través de instrumentos de medición, los cuales están relacionados con las variables de la investigación, que cumplen con condiciones como confiabilidad, validez y objetividad (Hernández et al., 2014). A continuación se describen los instrumentos utilizados en la presente investigación.

Cuestionarios, que consisten en un sin número de preguntas respecto o referentes a las variables a ser medidas en la investigación, y coherentes al problema e

hipótesis planteados. Los cuestionarios se utilizaron en la encuestas desarrolladas en la FT, los cuales se describe en el Apéndice C. El cuestionario se caracteriza por presentar preguntas cerradas, que en función del contexto fueron en línea con el uso del internet. Su construcción se define en función de los fundamentos, revisión de la literatura, relación con el dominio de las variables e indicadores, se elabora el instrumento, se realizan pruebas, se verifica y elabora la versión final. El instrumento se sube a la plataforma de Microsoft Forms versión de Microsoft Office 365, que proporciona automáticamente su difusión mediante enlace web, enlace por redes sociales, correo electrónico y código de respuesta rápida (QR). Esta plataforma informática proporciona una matriz en la hoja electrónica en Microsoft Excel, que servirá para la posterior análisis de los datos.

Técnicas de Análisis e Interpretación de Datos

Como técnicas de análisis e interpretación, se entiende a la forma de procesar los datos obtenidos, es decir ordenarlos, clasificarlos y presentarlos mediante tablas, gráficos de barras, pastel, escala y/o lineal, para su comprensión, el análisis se orienta a probar la hipótesis y la interpretación proporciona un considerado general a los referentes empíricos investigados referentes al problema y marco teórico.

Se utiliza en la presente investigación el aplicativo Microsoft Forms, el cual genera una matriz de datos en Microsoft Excel, para que juntamente con el software estadístico de código abierto GNU PSPP[20] desarrollar el análisis e interpretación de datos.

Descripción y Análisis de Resultados

En este apartado se describe la recolección de datos, en base a la encuesta enviada al personal militar y de servidores públicos de la FT, que constituyen el tamaño

[20] GNU PSPP, programa para el análisis estadístico de datos muestreados, proporciona funcionalidades de estadística descriptiva e inferencial.

de la muestra de la investigación, para su posterior tratamiento y análisis de los resultados obtenidos.

Recolección de Datos

En referencia al método de investigación cuantitativo, conceptualización de las variables con la dimensión, indicadores e ítems detallada en la tabla 1 y la determinación de la muestra en función del problema e hipótesis, a continuación, se desarrolla la recolección de datos.

Como instrumento de recolección y/o medición de datos empleados, es el cuestionario aplicado a través de la encuesta, con preguntas cerradas previamente delimitadas utilizando como nivel de medición a la escala. En el Apéndice C, se define el formato del cuestionario que se aplica en la encuesta. La encuesta se remite por medio del internet con el aplicativo de Microsoft Forms.

En la presente investigación se propone el empleo de la escala de Likert en el cuestionario con la aplicación de la codificación Net Promoter Score (NPS), por su simplicidad hacia los encuestados y sobre todo sin la complicación de encuestas tradicionales. Reichheld en su investigación The One Number You Need to Grow introdujo la escala y codificación NPS, en la cual se determina una escala o puntuación de 0 a 10, que agrupa a los clientes en los siguientes rangos de 9-10 favorable, 7-8 como neutral y 0-6 desfavorable en general (Reichheld, 2003).

Por codificación de datos, se define a la asignación de un valor numérico a las opciones de respuesta contestados, en nuestro caso las preguntas del cuestionario son cerradas y están precodificadas con la escala NPS. El nivel de medición aplicado es por intervalos o escala, el cual determina un orden o jerarquía entre categorías en función de intervalos de medición.

Proceso de tratamiento y análisis

Una vez recopilados los datos en línea a través del internet, mediante el aplicativo del Microsoft Forms, a continuación, se desarrolla el tratamiento y análisis de datos.

Los datos recogidos en el aplicativo de Microsoft Forms, presentan la opción para descarga en formato de matriz en Microsoft Excel, para su análisis se ejecuta en un programa computacional estadístico. A continuación se aplica las fases del proceso de análisis de datos cuantitativos (Hernández et al., 2014):

Seleccionar el programa o software estadístico para el análisis de datos. En la actualidad existe un sin número de programas o software estadísticos para el análisis de datos, en general el funcionamiento es similar entre todos. El software a utilizarse es el GNU PSPP , es un software libre de código abierto para el análisis estadístico de datos muestreados, su licencia es GNU General Public License que permite la redistribución o modificación.

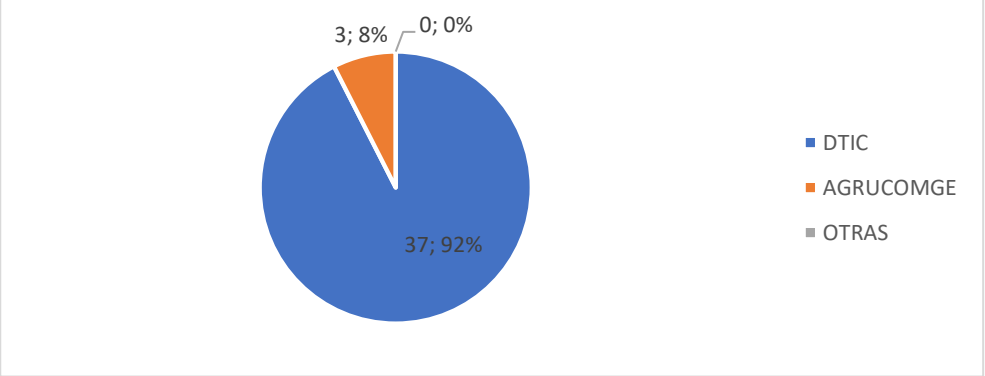
Ejecutar el programa o software estadístico. La ejecución del aplicativo se lo realiza específicamente en las opciones de la barra de menú y específicamente en la opción de Analizar.

Explorar los datos. La encuesta es aplicada a la personal específico relacionado a la ciberdefensa o áreas afines. Las preguntas demográficas o de ubicación planteadas a los participantes, se detallan a continuación con sus resultados:

1. Seleccione la unidad o dependencia a la pertenece:

Figura 18

Unidad o dependencia que pertenecen los encuestados

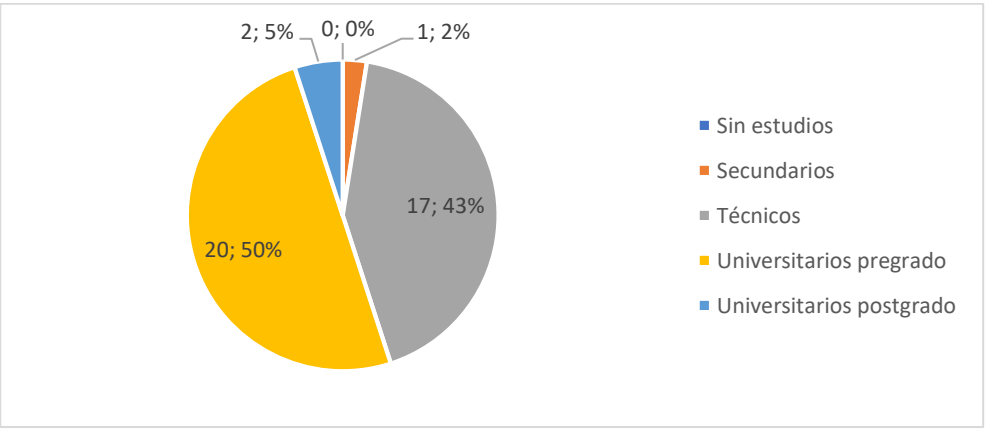


Nota. En la figura se determina que el 92 % pertenecen a la DTIC constituyendo la mayor parte de la población y el 8 % pertenecen al AGRUCOMGE, en función que según revisión documental y bibliográfica en las unidades o dependencias descritas no existe ninguna estructura y personal definido para la ciberdefensa o áreas afines.

2. Indique su nivel de estudios/instrucción (la de mayor jerarquía):

Figura 19

Nivel de estudios de los encuestados



Nota. Respecto al nivel de estudios o instrucción en la figura se define que el 50% de la población tiene estudios universitarios de pregrado y con estudios técnicos un 43%.

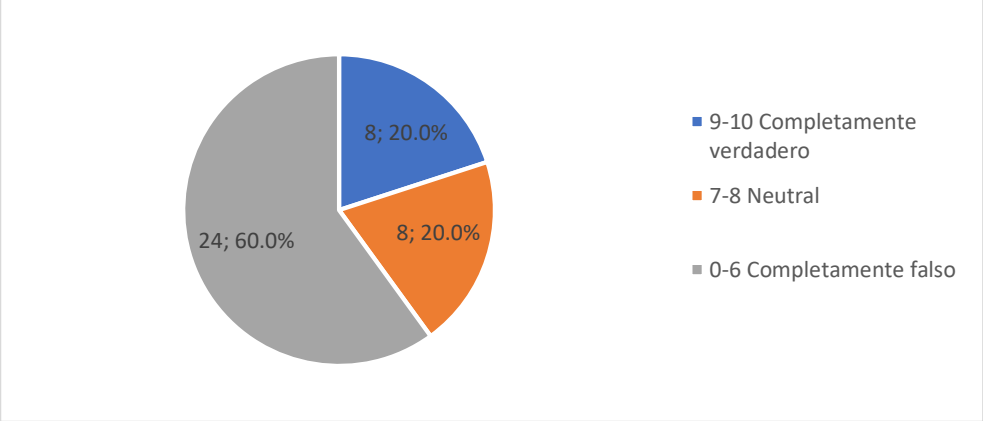
Las características demográficas o de ubicación de los encuestados, predomina la pertenencia a la DTIC y su nivel de estudios son universitarios de pregrado.

A continuación se describen los resultados de las preguntas de la encuesta aplicada a la población relacionada con las variables, dimensiones e indicadores

3. ¿Existe actualmente en su institución/Fuerza Terrestre una legislación en vigencia como Leyes, Códigos y/o Políticas sobre Ciberdefensa?

Figura 20

Legislación en vigencia sobre ciberdefensa

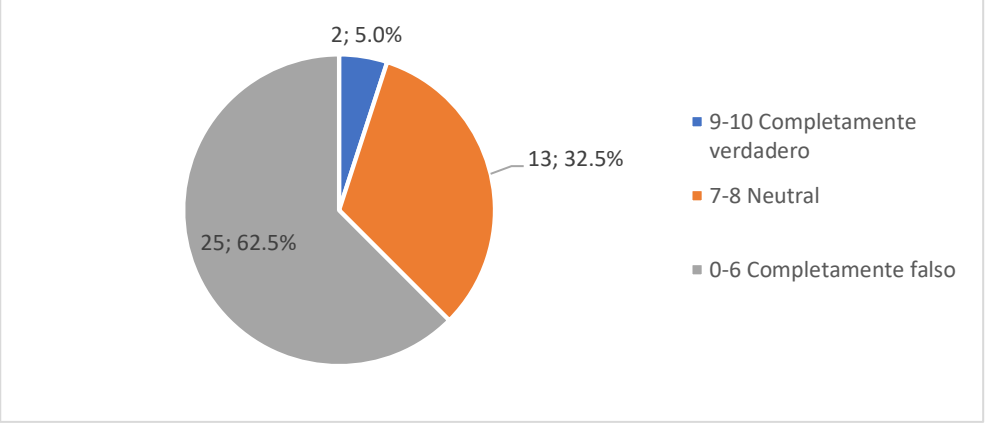


Nota. En la figura se identifica que la mayoría de los encuestados con un 60% consideran que no existe legislación sobre la ciberdefensa en la FT.

4. ¿Su institución/Fuerza Terrestre dispone de una estructura de ciberdefensa, CIRT, CSIRT o CERT/CC?

Figura 21

Estructura de Ciberdefensa en la FT

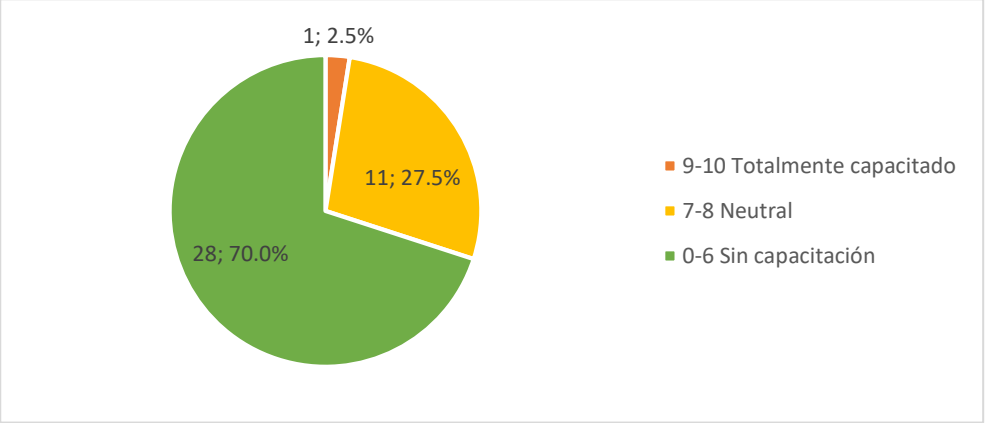


Nota. En la figura se identifica que el 62.5% de los encuestados identifican que no existe una estructura de ciberdefensa en la FT.

5. ¿Cómo considera Ud. que el personal militar y de servidores públicos de su dependencia/FT, están especializados o capacitados en ciberdefensa?

Figura 22

Especialización o capacitación en Ciberdefensa

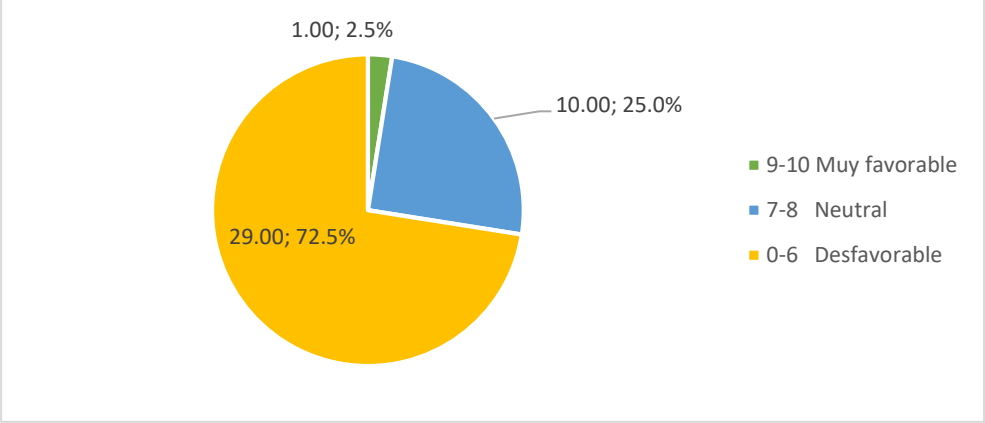


Nota. Sobre la capacitación en la figura se ilustra que el 70% considera que el personal no tiene capacitación específicamente en el área de ciberdefensa.

6. ¿Como evalúa el nivel de asignación presupuestario para mejorar la ciberdefensa y afines en su institución/Fuerza Terrestre?

Figura 23

Asignación presupuestaria para Ciberdefensa y áreas afines

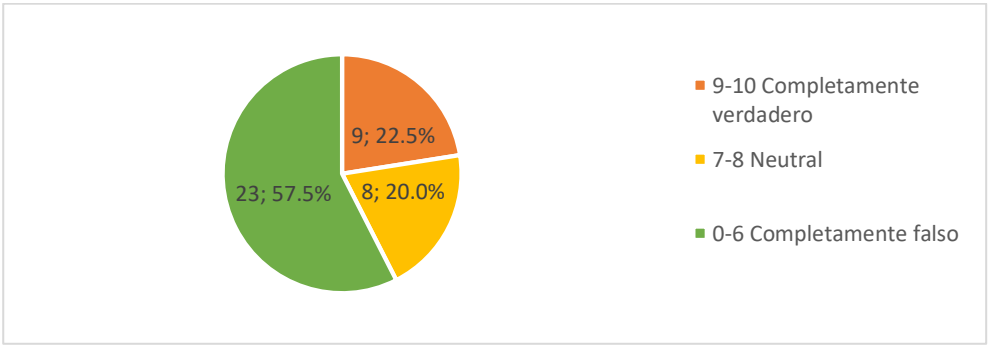


Nota. La asignación presupuestaria para la ciberdefensa y afines, se define en la figura con un 72.5% como muy desfavorable.

7. ¿Existe actualmente en su institución/Fuerza Terrestre una normativa en vigencia como Planes, Directiva, Instructivos, procesos y/o procedimientos sobre ciberdefensa?

Figura 24

Planes, directivas, instructivos y procesos en vigencia sobre ciberdefensa

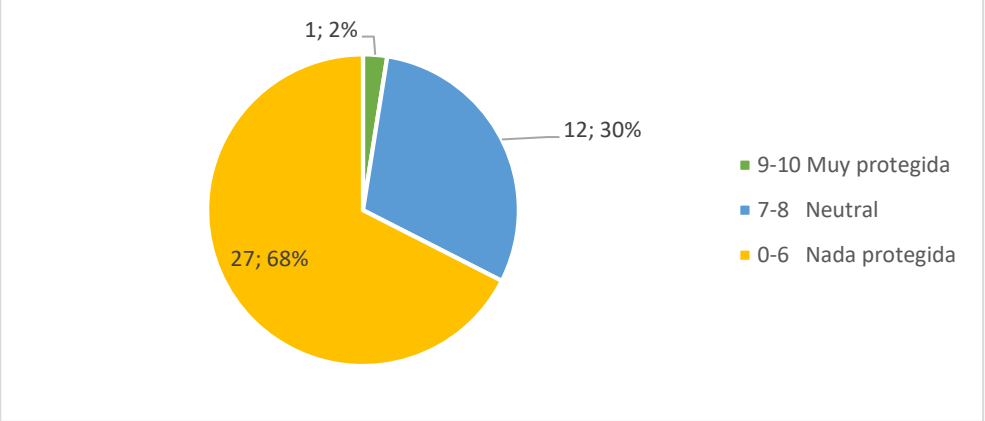


Nota. Respecto a la normativa de planes, directivas, instructivos, procesos o procedimientos de ciberdefensa el 57.5% consideran que no existen actualmente.

8. ¿Cómo considera Ud. el nivel de la seguridad y defensa de datos, información e infraestructura de TIC de su institución/Fuerza Terrestre?

Figura 25

Nivel de protección de datos, información e infraestructura de TIC



Nota. En función de los resultados, la figura representa que el nivel de protección en su mayoría tiene a nada protegida con un 70% y con un 30% medianamente protegido. Ninguno de los encuestados considera que la protección se encuentra en el nivel de muy protegida.

Evaluación de la fiabilidad del o de los instrumentos escogidos. Se evalúa a partir de los instrumentos de medición desarrollados, en función de los cuales se emplea el software estadístico GNU PSPP, a través de la medida de consistencia interna alfa de Cronbach (Hernández et al., 2014), con el resultado de $Alfa\ de\ Cronbach = 0{,}76$.

En general no existe una regla que defina el valor de la fiabilidad del instrumento, pero se puede citar a (Hernández et al., 2014), en el cual existe un variado criterio de algunos autores:

> Respecto a la interpretación de los distintos coeficientes mencionados cabe señalar que no hay una regla que indique “a partir de este valor no hay fiabilidad del instrumento”. Más bien, el investigador calcula su valor, lo declara y lo somete a escrutinio de los usuarios del estudio u otros investigadores, explicitando el método utilizado (Chen y Krauss, 2003; McKelvie, 2003; Lauriola, 2003; y Carmines y Zeller, 1991). Algunos autores consideran que el coeficiente debe estar entre 0.70 y 0.90 (Tavakol y Dennick, 2011; DeVellis, 2003; Streiner, 2003; Nunnally y Bernstein, 1994; Petterson, 1994). Nunnally (1987) por encima de 0.80. Lauriola (2003) sugiere un valor mínimo de 0.70 para la comparación entre grupos y 0.90 para escalas. Garson (2013) establece que 0.60 es aceptable para propósitos exploratorios y 0.70 para fines confirmatorios, resultando 0.80 “bueno” en un alcance explicativo. Ahora bien, también un coeficiente mayor de 0.90 puede implicar redundancia de ítems o indicadores y la necesidad de reducir el instrumento (Tavakol y Dennick, 2011). (pp. 295-296)

Para la presente investigación en función de los criterios descritos, con un valor de 0,76 el cual se considera una fiabilidad aceptable.

Análisis estadísticos de la hipótesis planteada. La prueba de la hipótesis se desarrolla en el contexto inferencial, respecto de uno o varios parámetros, una hipótesis se define un valor aceptable del parámetro, si es consistente con los datos recolectados, si no lo es, se rechaza.

El nivel de significancia, corresponde al nivel de probabilidad de que un evento ocurra, en las ciencias existe dos niveles según Hernández et al. (2014):

> El nivel de significancia de 0.05, el cual implica que el investigador tiene 95% de seguridad para generalizar sin equivocarse y sólo 5% en contra. En términos de

probabilidad, 0.95 y 0.05, respectivamente; ambos suman la unidad. Este nivel es el más común en ciencias sociales.

El nivel de significancia de 0.01, el cual implica que el investigador tiene 99% en su favor y 1% en contra (0.99 y 0.01 = 1.00) para generalizar sin temor. (p. 302)

Se ejecuta la prueba de hipótesis mediante el empleo del coeficiente de correlación de Pearson, en el aplicativo GNU PSPP. Este coeficiente analiza la relación, entre dos variables medidas en un nivel por intervalos o de razón, su denominación es r.

Hipótesis: La débil o limitada Ciberdefensa de la FT incide en la seguridad datos e infraestructura de TIC.

El coeficiente de correlación de Pearson se desarrolla entre las variables de la matriz que corresponden, a la variable independiente de investigación con la variable de la matriz que corresponde a la dependiente, estas ejecutan en el programa de análisis estadístico GNU PSPP con los siguientes resultados:

En la tabla 2 se describe los resultados en el programa de análisis estadístico GNU PSPP de la correlación entre la variable legislación y protección de datos, información e infraestructura:

Tabla 2

Correlación de variable legislación con protección

		Legislación	Protección
Legislación	Correlación de Pearson	1.00	0.69
	Significancia		0.000
	N	40	40
Protección	Correlación de Pearson	0.69	1.00
	Significancia	0.000	
	N	40	40

r = 0.69 (valor del coeficiente)

s o P = 0.000 (significativa en el nivel del 0.000, menor del 0.01)

+0.75 = Correlación positiva considerable.

En la tabla 3 se describe los resultados en el programa de análisis estadístico GNU PSPP de la correlación entre la variable estructura y protección de datos, información e infraestructura:

Tabla 3

Correlación de variable estructura con protección

		Estructura	Protección
Legislación	Correlación de Pearson	1.00	0.81
	Significancia		0.000
	N	40	40
Protección	Correlación de Pearson	0.81	1.00
	Significancia	0.000	
	N	40	40

r = 0.81 (valor del coeficiente)

s o P = 0.000 (significativa en el nivel del 0.000, menor del 0.01)

+0.90 = Correlación positiva muy fuerte.

En la tabla 4 se describe los resultados en el programa de análisis estadístico GNU PSPP de la correlación entre la variable capacitación y protección de datos, información e infraestructura:

Tabla 4

Correlación de variable capacitación con protección

		Capacitación	Protección
Legislación	Correlación de Pearson	1.00	0.41
	Significancia		0.005
	N	40	40
Protección	Correlación de Pearson	0.41	1.00
	Significancia	0.005	
	N	40	40

r = 0.41 (valor del coeficiente)

s o P = 0.005 (significativa en el nivel del 0.005, menor del 0.01)

+0.50 = Correlación positiva media.

En la tabla 5 se describe los resultados en el programa de análisis estadístico GNU PSPP de la correlación entre la variable recursos y protección de datos, información e infraestructura:

Tabla 5

Correlación de variable recursos con protección

		Recursos	Protección
Legislación	Correlación de Pearson	1.00	0.45
	Significancia		0.002
	N	40	40
Protección	Correlación de Pearson	0.45	1.00
	Significancia	0.002	
	N	40	40

r = 0.45 (valor del coeficiente)

s o P = 0.002 (significativa en el nivel del 0.002, menor del 0.01)

+0.50 = Correlación positiva media.

En la tabla 6 se describe los resultados en el programa de análisis estadístico GNU PSPP de la correlación entre la variable normas-planes y protección de datos, información e infraestructura:

Tabla 6

Correlación de variable normas-planes con protección

		Recursos	Protección
Legislación	Correlación de Pearson	1.00	0.51
	Significancia		0.000
	N	40	40
Protección	Correlación de Pearson	0.51	1.00
	Significancia	0.000	
	N	40	40

r = 0.51 (valor del coeficiente)

s o P = 0.000 (significativa en el nivel del 0.000, menor del 0.01)

+0.50 = Correlación positiva media.

El detalle de los resultados en la ejecución del programa GNU PSPP se detallan en el Apéndice D.

En función de los resultados obtenidos anteriormente, se acepta la hipótesis de investigación en base a que la significancia es menor a 0.01 y las correlaciones se encuentran en el rango de positiva media a positiva muy fuerte.

Resultados y hallazgos

En referencia a la revisión bibliográfica y documental en la FT, específicamente en la DTIC y AGRUCOMGE respecto a las dimensiones planteadas e indicadores a continuación se describen los resultados.

En referencia a las Leyes, Códigos o políticas, actualmente no existe ley o código específicos de ciberdefensa y la política a nivel nacional de ciberdefensa se encuentra regentada por el MINTEL pero en planificación y desarrollo, el MIDENA, CCFFAA y FT tienen participación mínima en función del plan de la sociedad de la información y del conocimiento.

En la dimensión militar, no existen una estructura definida para ciberdefensa en la FT, así como en la DTIC y AGRUCOMGE. La estructura está definida en el CCFFAA a través del COCIBER pero actualmente no tiene ninguna relación de estructura hacia las fuerzas respecto a estructura y a nivel nacional por medio del EcuCert a responsabilidad del MINTEL. Se presentan las estructuras de ciberdefensa del primer y segundo país según el GCI las misma que se basan en unidades militares de sus ejércitos, estructurados como componentes a niveles nacionales.

En la dimensión de TIC respecto a la capacitación esta se presenta incipiente, no existen programas de capacitación específica de ciberdefensa en la DTIC y AGRUCOMGE. En la revisión bibliográfica se presenta capacitaciones en el área de ciberdefensa y un marco aprobado para certificaciones y acreditaciones de seguridad cibernética internacionales.

Respecto a la dimensión de recursos, en función de la revisión documental en la DTIC y AGRUCOMGE la asignación presupuestaria es mínima. Al no existir una estructura organizacional en ciberdefensa la FT no existirán recursos de personal, asignaciones de presupuesto e infraestructura de hardware y software en el contexto de ciberdefensa.

La dimensión normativa en relación a planes, procesos y procedimientos, a nivel de la FT no existe ninguna relacionada específicamente a la ciberdefensa. Se puede

citar al Plan Específico de Defensa 2019-2030 del MIDENA en el cual incluye aspectos del ciberespacio, ciberdefensa y ciberseguridad.

En referencia al análisis de estadísticos y validación de la hipótesis planteada en función de la correlación de variables. Respecto a los aspectos demográficos o de ubicación, la mayoría de los encuestados pertenece a la DTIC y poseen estudios universitarios de pregrado.

En la variable de investigación definida como independiente se identifica en la dimensión política con un 60% que constituye la mayoría, consideran que no existe una legislación en vigencia sobre ciberdefensa ya sea leyes, códigos o políticas y un 20% se consideran neutrales o pasivos.

La mayoría de encuestados con 62.5% de la población consideran que no existe una estructura de ciberdefensa en la FT y con un 32.5 % se consideran neutrales o pasivos del indicador respecto a la dimensión militar planteada.

El indicador de personal capacitado determina que un 70% de la población considera que el personal militar y de servidores públicos se encuentran sin capacitación y un 27,5% se consideran neutrales o pasivos, en las áreas de ciberdefensa respecto a la dimensión de TIC.

Respecto a la dimensión de recursos, el indicador de asignación presupuestaria e infraestructura el 72.5% de los encuestados la evalúan como desfavorable y con un 25% lo consideran neutral o pasivo.

Referente al indicador de planes, directivas, instructivos, procesos o procedimientos de la dimensión de normativa, mayoría consideran que no existen con un 57.5% y con un 22.5% consideran que si existen.

Como variable dependiente se plantea a la dimensión de defensa de datos e infraestructura con el indicador de protección de datos, información e infraestructura de

TIC, dando como resultado que la mayoría con un 68% evalúan como nada protegido y un 30% se describen como neutrales o pasivos.

Se desarrolla la correlación de las variables, obteniéndose que existe correlación en el rango de positiva media a muy fuerte, que influye en la variable dependiente a las dimensiones e indicadores planteado, pero en mayor proporciona e influencia con la dimensión militar respecto a la estructura organizacional de la ciberdefensa. Los demás indicadores planteados influyen en menor proporción como son la legislación en vigencia (dimensión política), planes (dimensión normativo), Asignación presupuestaria e infraestructura (dimensión recursos) y personal capacitado (dimensión de TIC) respectivamente en función del resultado de las correlaciones entre variables.

En referencia a la estadística descriptiva desarrollada, correlación y significancia, la hipótesis planteada es aceptada, en función que de acuerdo al análisis planteado existe una alta significancia y correlación de variables.

Desarrollo de la Investigación

Primer Objetivo Especifico

Determinar las dificultades que imposibilitan el mantenimiento de la ciberdefensa en la FT.

Introducción

En referencia al primer objetivo específico este persigue establecer que dificultades que se han presentado en la FT respecto a su ciberdefensa, en función de esta identificación se puede establecer causas de la deficiente ciberdefensa en la FT.

Conocimiento del Hecho

En referencia a la revisión bibliográfica y documental descritos en la investigación, en general el Ecuador en especial el sector gubernamental presenta deficiencias en su seguridad y defensa del ciberespacio en controles, políticas de seguridad, planes de continuidad, clasificación de la información, protección de infección de malware, entre otros constituyéndose en uno de los principales países que recibe ciberataques a nivel mundial y de Latinoamérica.

En la constitución política del Ecuador no se establece ningún articulado especifico respecto a la ciberdefensa, seguridad cibernética y/o ciberespacio, únicamente se enuncia la misión de FFAA. Las leyes y códigos revisados no presentan aspectos específicos de ciberdefensa. En la política de Defensa Nacional se incluye aspectos del ciberespacio, ciberseguridad y ciberdefensa.

En referencia a la estructura organizacional, la FT actualmente no dispone de estructura de ciberdefensa. Respecto a la normativa en el plan de la sociedad de la información y del conocimiento, incluye aspectos de ciberseguridad y protección de datos, pero no de ciberdefensa sin incluir en su desarrollo y programación al MINEDA o CCFFAA. EL Plan Específico de Defensa 2019-2030 del MIDENA amplia y se acerca a

la conceptualización de aspectos como ciberespacio, ciberseguridad y ciberdefensa. El AGRUCOMGE, BC 1 y DTIC, no disponen de una normativa de ciberdefensa o defensa cibernética específica.

Respecto a los estadísticos y correlación de variables, el indicador de mayor impacto o influencia es el de estructura organización de ciberdefensa con una correlación positiva muy fuerte. El indicador que le sigue es el de legislación con una correlación positiva considerable, a continuación el indicador de normas-planes con una correlación positiva media, los indicadores recursos y capacitación se acercan a la correlación positiva media respectivamente.

Análisis

En referencia a lo desarrollado es necesario una legislación que respalde el accionar de las instituciones gubernamentales en el contexto de ciberdefensa, que actualmente no existe a nivel ley o código, existe en programas futuros del gobierno central desarrollar la política de ciberseguridad y esquemas de protección de datos. Este aspecto se encuentra en el contexto del nivel ejecutivo y legislativo, para su desarrollo.

Al no existir estructura de ciberdefensa, no existirá procesos, asignación de recursos, capacitación, procedimientos, auditorias gestión de tecnologías, entre otras, en el contexto del ciberespacio para regular los niveles estratégico, operacional y táctico.

La capacitación del personal involucrado es fundamental para el respaldo y garantía de la ciberdefensa de la FT y su deficiencia impacta en mencionada seguridad en forma directa.

Conclusiones Parciales

Se identifica como principales dificultades para el mantenimiento de la ciberdefensa en la FT a la falta de una ley o código, la estructura es inexistente, existe una deficiente capacitación, la asignación de presupuesto es reducida, lo cual influirá en el mantenimiento y garantía de la confidencialidad, integridad y disponibilidad de datos, información e infraestructura de la FT.

Segundo Objetivo Especifico

Identificar las causas de los limitados recursos para la ciberdefensa en la FT.

Introducción

El propósito fundamental del segundo objetivo es la determinación de las razones o motivos de los insuficientes recursos para la ciberdefensa de la FT, entendiéndose como recursos a los económicos, de infraestructura de hardware - software y del personal especializado, lo que permitirá fundamentar la situación actual de la ciberdefensa en la fuerza, y su incidencia o impacto para la seguridad y defensa de datos e infraestructura de TIC.

Conocimiento del Hecho

Se hace referencia a que no existe actualmente una estructura aprobada o en funcionamiento de ciberdefensa o defensa cibernética, ya sea como un órgano independiente o de dependencia directa del COCIBER del CCFFAA, para la DTIC, AGRUCOMGE y BC 1.

Por consecuencia no existirá de parte de unidades anteriormente descritas programas de capacitación, recursos económicos, recursos de infraestructura, recursos humanos capacitados o especializados.

Análisis

Tres recursos son primordiales en toda institución u organización respecto al funcionamiento como un todo, estos son recursos de personal, económicos e infraestructura, los cuales están directamente relacionados a una estructura en vigencia que actualmente no existe en la FT. Al no existir una estructura orgánica de ciberdefensa los recursos serán nulos, se identifica un aspecto fundamental que impacta en los recursos descritos, es la concepción del I+D+i, lo cual potencializan al recurso de personal, optimiza al económico e infraestructura, este aspecto debe potencializarse en la FT. lo cual incrementara los recursos impactando para una mejora de la ciberdefensa de la FT.

Conclusiones Parciales

Los recursos de personal, económicos e infraestructura de hardware – software, se encuentran relacionados directamente a una estructura legal como parte de una institución, en el presente trabajo de investigación la FT carece de dicha estructura orgánica o de procesos en el área de la ciberdefensa, que concluye que sus recursos para la ciberdefensa serán sumamente limitadas o nulas en la actualidad.

Tercer Objetivo Especifico

Diseñar una propuesta que contribuyan a la mejora de la ciberdefensa en la FT.

Introducción

El tercer objetivo específico se basa en la situación actual de la ciberdefensa en la FT, determinación de las causas para sus limitados recursos y marco teórico desarrollado, con la finalidad de establecer una propuesta que contribuya para la mejora de la ciberdefensa de la FT.

Conocimiento del Hecho

Respecto a la falta de estructura organizacional para la ciberdefensa en la FT, la propuesta se fundamenta proponer una estructura que mejore su ciberdefensa, en función que este indicador se presenta como el de mayor impacto o influencia hacia la variable dependiente. En el marco teórico se cita a las estructuras definidas por los ejércitos de Gran Bretaña y Estados Unidos.

La propuesta se complementa en base a la dimensión planteada de normas con el indicador de planes-procesos-procedimientos en función que constituye a nivel de la FT como el segundo indicador que más influye en la correlación de variables.

Análisis

Las nuevas formas de estructuras organizacionales son flexibles para enfrentar los nuevos escenarios actuales, más aún en el ambiente del ciberespacio, por lo cual es imperativo referirnos a estándares mundiales desde la visión militar y técnica-civil, el Ecuador a nivel gubernamental se alinea en general con la estandarización de la UIT, ISO e IEC en general en el contexto del ciberespacio, ciberseguridad y ciberdefensa, sin dejar de observar a otras normalizaciones internacionales.

La estructura organizacional se complementa con sistema de gestión, los cuales basan su accionar con un recursos de personal capacitado, asignación presupuestaria e infraestructura, enfocado en el trabajo grupal y colaborativo tanto interno como externo y entrenamiento bajo nuevos estándares que se relacionan a las tecnologías emergentes y disruptivas del ciberespacio.

Conclusiones Parciales

Actualmente no existe aplicación de nuevas tecnologías, técnicas o modelos de gestión en la FT en el contexto de la ciberdefensa. Se requiere una propuesta de estructura organizacional enfocada en los contextos militares y técnico-civil

fundamentado en estándares internacionales, que enlacen los niveles táctico-técnico, operacional-gerencial y estratégico-directivo, que con las base de una capacitación adecuada proyecte el empleo de la teoría de la emulación militar o la I+D+i.

Conclusiones Generales

La situación actual de la ciberdefensa en la FT, identifica a la ausencia de una legislación con jerarquía de Ley o Código, la inexistencia de una estructura organizacional de ciberdefensa en la FT, falta de normas como planes, procesos o procedimientos específicos de ciberdefensa y a una deficiente capacitación del personal militar o civil involucrado. Estos aspectos influyen e impactan en la seguridad y defensa de datos, información e infraestructura de TIC en la FT.

Al no existir una estructura organizacional de ciberdefensa en la FT, consecuentemente no existirán recursos humanos, económicos y de infraestructura. En función de la estructura no existe aplicación de nuevas tecnologías, técnicas y modelos de gestión en la FT en el contexto de la ciberdefensa.

Se requiere una propuesta de estructura organizacional, complementada con un sistema de gestión las cuales contribuirán a mejorar la ciberdefensa.

Propuesta

En referencia a los resultados de la investigación, a continuación se desarrolla la propuesta para mejorar la ciberdefensa en la FT. Esta propuesta se basa en la situación actual, indicadores de estructura organizacional y normalización como planes, procesos o procedimiento y el marco teórico desarrollado.

En general para proponer cualquier sistema se requiere una línea base o punto de inicio. Se consideran como aspectos que componen a la línea base, al análisis de la situación actual, legislación de respaldo y conocimiento del entorno.

El análisis de la situación actual de ciberdefensa en la FT se encuentra desarrollado en el presente trabajo de investigación.

Respecto a la legislación actualmente se carece de una ley o código de ciberdefensa, por lo cual como legislación de respaldo se considera principalmente a la Constitución de la República del Ecuador en referencia a la misión fundamental de FFAA, Política de la Defensa Nacional del Ecuador y los objetivos planteados en el Plan Específico de Defensa, planes estratégicos del MIDENA y CCFFAA, y plan de gestión de la FT.

EL conocimiento del entorno se refiere al comprensión de las áreas relacionadas a la ciberdefensa en la FT que en general constituye la organización de la FT y específicamente a la DTIC como AGRUCOMGE.

Objetivo

Proponer un sistema de gestión para mejorar la ciberdefensa en la FT.

Alcance

El alcance de la presente propuesta plantea un sistema de gestión de ciberdefensa que sea transversal, considerando la estructura de la FT a nivel táctico y

operacional, el cual se enlaza con su escalón técnico superior constituido por el COCIBER del CCFFAA como el nivel estratégico militar.

Sistema de Gestión de Ciberdefensa para la Fuerza Terrestre

Desarrollo

El Sistema de Gestión de Ciberdefensa propuesto para la FT está compuesto por los siguientes componentes:

- Conceptualizaciones Internas.
- Fundamentos.
- Estructura Organizacional.
- Arquitectura de la Red de Información de la FT.
- Proceso.

Marco Legal

En referencia al marco legal que respalde el accionar del sistema de gestión de ciberdefensa, se describen a continuación las más importantes.

- Constitución de la República del Ecuador 2008.
- Ley Orgánica de la Defensa.
- Política de la Defensa Nacional del Ecuador "Libro Blanco".
- Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad “Libro Blanco de la Sociedad de la Información y del Conocimiento”.
- Manual Organizacional del Comando de Ciberdefensa de las Fuerzas Armadas.
- Plan de la Sociedad de la Información y del Conocimiento.
- Plan Específico de Defensa 2019-2030.
- Plan Estratégico Institucional de Defensa.

- Plan Estratégico Institucional de Fuerzas Armadas.
- Plan de Gestión Institucional de la FT.

Marco de Referencia de Estandarización

- NTE.
- ISO/IEC 27000 o NTE INEN-ISO /IEC 27000.
- UIT con su GCI.
- Estructura del Treceavo Regimiento de Señales (13th Signal Regiment).
- Estructura del ARCYBER.

Conceptualizaciones Internas

Ciberespacio en el contexto global. Es un ambiente no físico o no natural, estructurado por elementos de TIC que producen un sin número de efectos, también se lo denominado ambiente virtual. Es un dominio global en el contexto de los datos, información y comunicaciones. Está compuesto por redes de dependencia mutua con infraestructuras[21] de TIC.

Ciberespacio de la Fuerza Terrestre. En el contexto e influencia de las redes globales, se considera a sus redes (incluye todos sus componentes) interdependientes de la infraestructura de TIC, que incluye al Internet, intranet, redes de comunicaciones, sistemas de información, sistemas informáticos, aplicativos, procesadores, controladores, entre otros, que conforman el entorno virtual de la FT.

Ciberdefensa. Es el empleo y práctica de un conjunto de medidas de protección y acciones para defender el ciberespacio de infraestructuras críticas del Estado que afecten su soberanía e integridad territorial.

[21] Se incluye el Internet, redes de computadores, telecomunicaciones, sistemas informáticos, procesadores, controladores, sensores, entre otros elementos.

Fundamentos

El sistema de gestión de ciberdefensa se basa en los siguientes fundamentos en el contexto de la defensa y seguridad.

Confidencialidad. Pertinente a la exclusividad de un usuario o grupo de usuarios registrados que están autorizados y tienen acceso a datos, información o recurso de TIC en el ciberespacio de la FT. Pero al mismo tiempo los datos, información o recurso de TIC no puedan ser revelados.

Integridad. Referida a los datos, información o recursos de TIC del ciberespacio de la FT son exactos y completos, nunca han sido manipulados sin autorización.

Disponibilidad. Si el usuario, grupo de usuarios o procesos registrados y autorizados obtienen acceso cuando lo requieran a los datos, información o recursos de TIC del ciberespacio de la FT.

Autenticidad. Referente a la seguridad o certeza de la identidad y autoría de los usuarios o procesos que ejecutan acciones con los datos, información o recursos de TIC del ciberespacio de la FT.

Trazabilidad. Registro de históricos de acciones en un usuario, proceso o procedimiento automatizado que incluye su autoría, referente al uso de datos, información o recursos de TIC del ciberespacio de la FT.

Privacidad. Referente a que los datos personales puedan ser públicos o no.

Estructura Organizacional

Se fundamenta en los objetivos estratégicos institucionales y propuesta de agencias responsables de la ciberdefensa.

Objetivos Estratégicos Institucionales (OEI). La estructura organizacional se alinea a los OEI de:

- MIDENA: “Incrementar las capacidades estratégicas conjuntas de las Fuerzas Armadas” (Ministerio de Defensa Nacional del Ecuador, 2017, p. 102).
- CCFFAA: “Incrementar las capacidades estratégicas conjuntas de Fuerzas Armadas” (Comando Conjunto de las Fuerzas Armadas del Ecuador, 2010, p. 52)
- FT: “Incrementar las Capacidades Militares” (Fuerza Terrestre, 2017, p. 4).

Agencias Responsables. Corresponden a las unidades o dependencias de la FT responsable de la ciberdefensa. Las dependencias y unidades militares que conforman la estructura del sistema de ciberdefensa son:

- Comando de Operaciones Terrestres (COT) a través de la dependencia propuesta como Centro de Operaciones de Ciberdefensa de la FT (CEOPC).
- AGRUCOMGE a través de la unidad propuesta como Unidad de Operaciones de Ciberdefensa (UOCIBER).
- Las compañías, pelotones o secciones de comunicaciones de las unidades de la FT a través de la propuesta de la conformación de los Equipo de Protección Cibernética (EPC).

En la figura 26 se ilustra la estructura del sistema con las dependencias y unidades responsables.

Centro de Operaciones de Ciberdefensa de la Fuerza Terrestre. También se puede denominar como equipo de respuesta ante emergencias informáticas (CERT[22]) o

[22] CERT del acrónimo ingles Computer Emergency Response Team

equipo de respuesta ante incidencias de seguridad informáticas (CSIRT[23]). Unidad encargada de gestionar operaciones de defensa y exploración en el ciberespacio de la FT y otras asignadas en forma permanente, protegiendo la infraestructura crítica tecnológica, degradando o neutralizando la infraestructura tecnológica del adversario con orden.

Unidad de Operaciones de Ciberdefensa. La UOCIBER constituye una fuerza militar bajo el mando del AGRUCOMGE, encargada de planificar, coordina, integrar y ejecutar operaciones de defensa y exploración en el ciberespacio de la FT y otras asignadas en forma permanente.

Unidades de Comunicaciones de la Fuerza Terrestre. En referencia a la estructura en vigencia constituyen las siguientes unidades:

- AGRUCOMGE con sus unidades orgánicas:
    - BC 1.
    - Comando de Apoyo Logístico Electrónico (CALE).
    - Compañía de Guerra Electrónica.
    - UOCIBER, como propuesta.
- Compañía de comunicaciones a nivel División y Brigada.
- Pelotones o secciones de comunicaciones a nivel Batallón o Grupo.

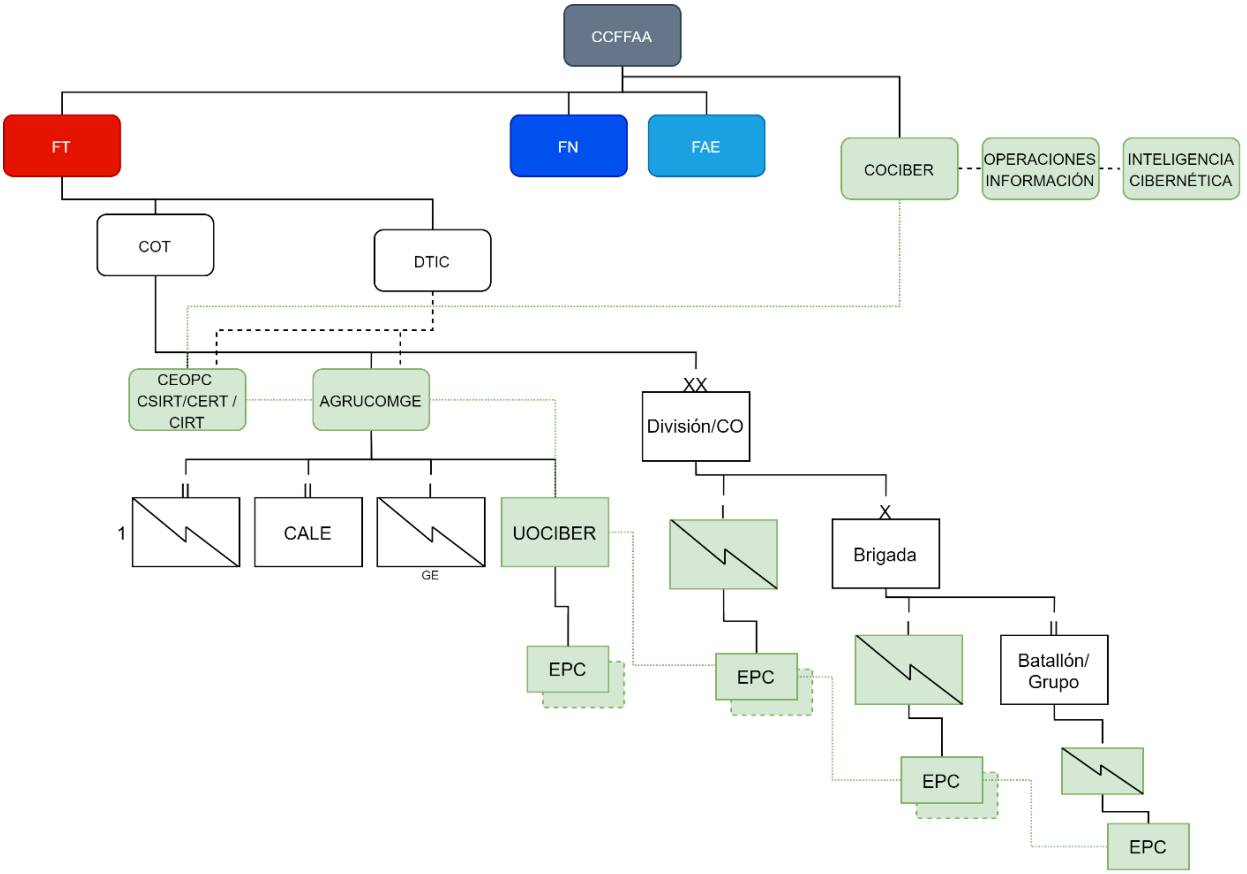
Equipo de Protección Cibernética. Son los equipos o elementos del sistema de gestión de ciberdefensa que ejecutan o accionan las operaciones de defensa, exploración y respuesta en el ciberespacio de la FT y otras que sean asignadas con orden.

[23] CSIRT del acrónimo ingles Computer Security Incident Response Team

Estos equipos forman parte de sistema y serán encargadas en general de ejecutar operaciones de defensa, exploración y respuesta.

Figura 26

Estructura para el Sistema de Gestión de Ciberdefensa de la Fuerza Terrestre



Nota. Se ilustra a las dependencias o unidades de Operaciones de Información e Inteligencia a nivel estratégico militar y DTIC de la FT, con las cuales se debe coordinar en todos los niveles del sistema de gestión de ciberdefensa.

Arquitectura de la Red de Información de la Fuerza Terrestre

La red de información de la FT está conformada por las redes de comunicaciones o telecomunicaciones, redes de datos, sistemas de información,

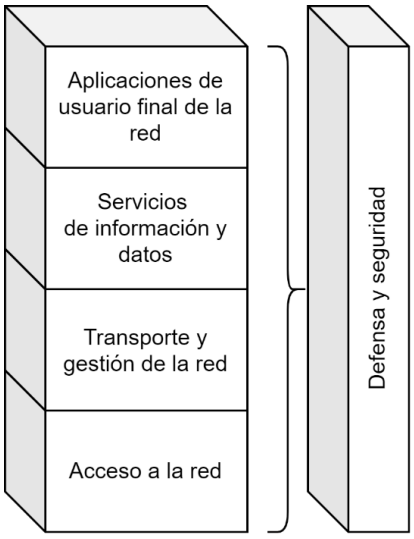
sistemas informáticos con sus aplicativos y código fuente, base y estructura de datos, sistemas de gestión, dispositivos o hardware, medios de transmisión, infraestructura de TIC, entre otros. Los cuales establecen el ciberespacio de la FT y requieren para una gestión efectiva la definición de su arquitectura.

La arquitectura describe la configuración de elementos físicos y lógicos, que contendrán al ciberespacio de la FT. En la figura 27 se ilustra las 5 capas de la arquitectura de la red.

1. Capa de acceso a la red.
2. Capa de transporte y gestión de la red.
3. Capa de servicios de información y datos.
4. Capa de aplicaciones de usuario final de la red.
5. Capa de defensa y seguridad.

Figura 27

Arquitectura de la Red de la FT



Nota. La capa de Defensa y Seguridad es transversal a las cuatro capas de la arquitectura, es decir se encuentra presente en todas.

Capa de Acceso a la Red. Comprende aspectos físicos y de enlace. Define la interfaz física entre dispositivos de TIC y el medio de transmisión físico de la FT. Los medios de transmisión son los guiados que incluyen a los cableados por cobre y fibra óptica. Como medios de transmisión no guiados a todo el conjunto de radiofrecuencia. Se caracteriza por aspectos mecánicos, eléctricos, ópticos, funcionales y de procedimientos. Referente al aspecto de enlace es responsable del intercambio entre dispositivos finales y las redes enlazadas por los medios de transmisión.

Capa de Transporte y gestión de la Red. La gestión de la red admite y transfiere datos a la red en general. Esta emplea protocolos para su gestión y control.

El transporte proporciona conectividad y traslado de datos entre dispositivos. Este emplea protocolos para garantizar que los datos lleguen secuencialmente, sin errores,

Capa de Servicios de Información y Datos. El propósito principal de los servicios de información y datos, es definir los aplicativos y servicios de la red de información de la FT. Lo cual facilitara la toma de decisiones y la ejecución, sean oportunas y precisas mediante la gestión y procesamiento de los datos e información. Los servicios y datos incluyen a servicios de información, servidores y estándares de datos.

Capa de Aplicaciones de Usuario Final de la Red. Las aplicaciones de usuario final incluyen a sistemas de información automatizados, sistemas informáticos, procesos y procedimientos, software y hardware de usuario (como dispositivos informáticos y aplicativos). Estos permiten a los usuarios visualizar y difundir información, permitiendo al personal aprovechar las capacidades de la red de información de la FT.

Capa de Defensa y Seguridad. La capa de defensa y seguridad, se aplica transversalmente a las cuatro primeras como se ilustra en la figura 27. En esta capa controla y proporciona, defensa y seguridad a la transmisión de datos en el campo de batalla.

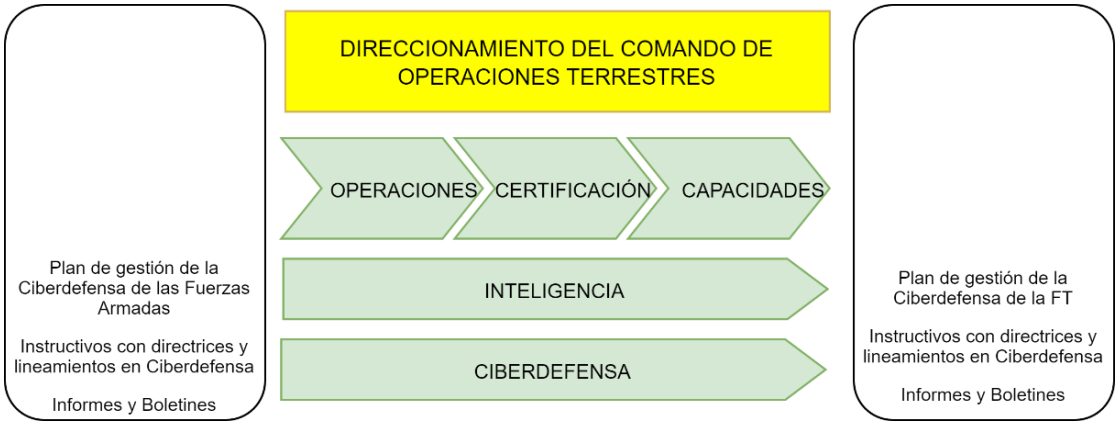
Se incluyen elementos físicos y lógicos de todas las capas, desde aspectos físicos, medios de transmisión, dispositivos de gestión que incluyen conmutadores (switches), enrutadores (routers, bridge y repeater), dispositivos o software de seguridad de la red (firewall, sistemas de alerta, detección y prevención de intrusos, sensores, entre otros), servicios de información y aplicaciones de usuario final.

Proceso

Se propone incluir el proceso de ciberdefensa en el macroproceso de gestión de las operaciones militares terrestres, perteneciente al COT como se ilustra en la figura 28.

Figura 28

Macroproceso de gestión de las operaciones militares terrestres



Nota. En la figura se ilustra las entradas y productos del proceso de ciberdefensa incluido al macroproceso de gestión de las operaciones militares terrestres. Adaptado

de *Manual de Procesos de la Fuerza Terrestre: Gestión de las Operaciones Militares Terrestres* (p. 2), por FT, 2018.

Descripción del Proceso de Ciberdefensa.

Propósito. Gestionar el sistema de ciberdefensa de la FT, mediante la planificación y empleo de operaciones en el ciberespacio de la FT y otros asignados con orden, a fin de contribuir al cumplimiento de la misión del COT.

Disparador. Constituye la condición o suceso que causa el inicio del proceso.

- Plan de gestión de la Ciberdefensa de las FFAA.
- Plan de gestión del COT.
- Directivas, planes y órdenes militares.
- Acciones en el ciberespacio de la FT y otros asignados.

Entradas.

- Plan Estratégico Institucional de Defensa.
- Plan Estratégico Institucional de FFAA.
- Plan de Gestión Institucional de la FT.
- Plan Específico de Defensa.
- Plan de gestión de la ciberdefensa de las FFAA.
- Plan de gestión del COT.
- Directivas, planes y órdenes militares.
- Instructivos con directrices y lineamientos en ciberdefensa.
- Informes y boletines de ciberdefensa.
- Requerimientos.

Subprocesos.

- Planificación.

- Empleo.

Productos o Servicios del Proceso.

- Plan de gestión de la ciberdefensa de FT.
- Instructivos con directrices y lineamientos en ciberdefensa.
- Apreciaciones de ciberdefensa.
- Informes y boletines de ciberdefensa, seguridad del ciberespacio de la FT.
- Directivas, planes y órdenes militares.
- Requerimientos

Tipo de Proceso. Sustantivo.

Responsable del Proceso. Comandante del CEOPC.

Tipo de Cliente.

Internos. Unidades militares del sistema de ciberdefensa de la FT.

Externos. Comandos, direcciones y unidades militares.

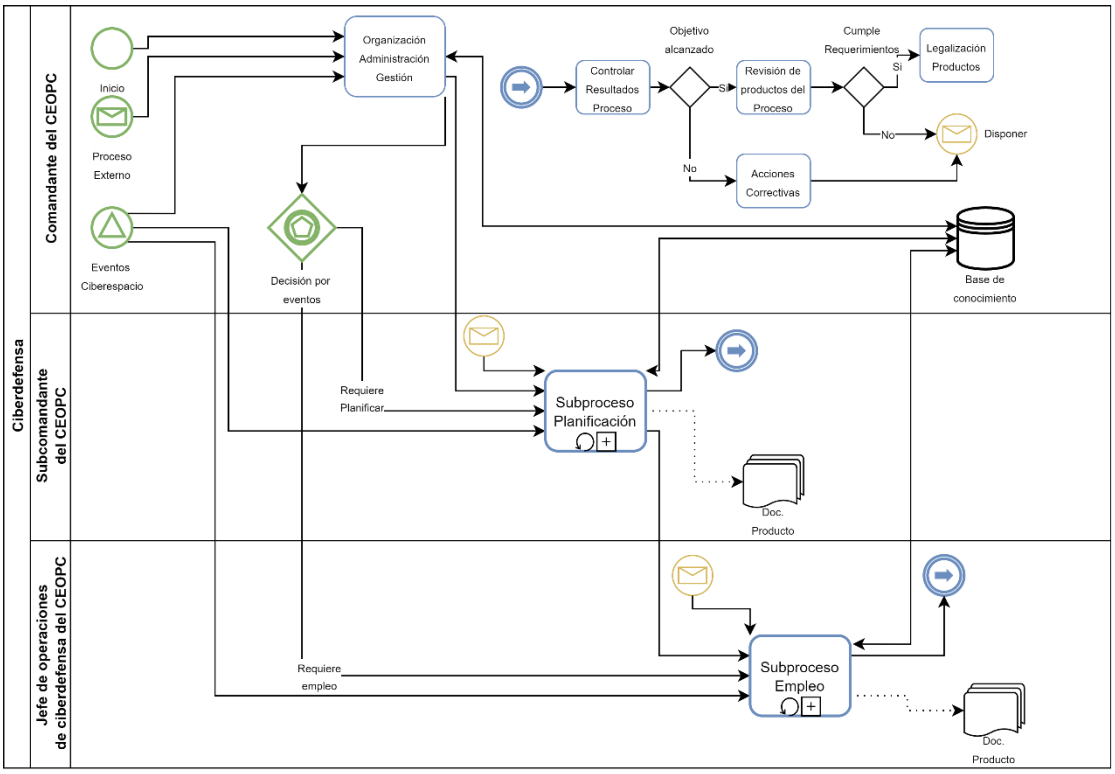
Marco Legal. La legislación descrita en el sistema de ciberdefensa y la que se detalla a continuación:

- Plan de gestión de la ciberdefensa de las FFAA.
- Plan de gestión del COT.
- Instructivos con directrices y lineamientos en ciberdefensa.
- Directivas, planes y órdenes militares.

Mapa de Interrelación de Ciberdefensa. En la figura 29 se ilustra el mapa de interrelación del proceso de ciberdefensa.

Figura 29

Mapa de interrelación del proceso de ciberdefensa de la FT



Descripción del Subproceso de Planificación de Operaciones de Ciberdefensa.

Propósito. Realizar la planificación de operaciones de defensa, exploración y respuesta en el ciberespacio de la FT y otros asignados con orden, con la finalidad de proteger la infraestructura crítica de TIC.

Disparador.

- Plan de gestión de la Ciberdefensa de las FFAA.
- Plan de gestión del COT.
- Directivas, planes y órdenes militares.
- Acciones en el ciberespacio de la FT y otros asignados.

Entradas.

- Plan de gestión de la Ciberdefensa de las FFAA.
- Plan de gestión del COT.
- Directivas, planes y órdenes militares.
- Informes.
- Requerimientos.

Productos o Servicios del Proceso.

- Plan de gestión de la ciberdefensa de FT.
- Apreciaciones de ciberdefensa.
- Planes y órdenes militares de ciberdefensa.
- Informes de operaciones de defensa, exploración y respuesta.
- Informes de propuestas de proyectos.
- Informes de requerimientos de personal, capacitación, equipos y sistemas.

Responsable del Proceso. Subcomandante del CEOPC.

Tipo de Cliente.

Internos. Unidades militares del sistema de ciberdefensa de la FT.

Externos. Comandos, direcciones y unidades militares.

Descripción del Subproceso de Empleo de Operaciones de Ciberdefensa.

Propósito. Ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio de la FT en forma permanente y otros asignados con orden, con la finalidad de proteger la infraestructura crítica de TIC.

Disparador.

- Directivas, planes y órdenes militares.
- Acciones en el ciberespacio de la FT y otros asignados.

Entradas.

- Directivas, planes y órdenes militares.
- Instructivos con directrices y lineamientos en ciberdefensa.
- Informes y boletines de ciberdefensa.
- Requerimientos.

Productos o Servicios del Proceso.

- Planes y órdenes militares en áreas de ciberdefensa.
- Informes y Boletines.
- Apreciaciones en áreas de ciberdefensa
- Reportes y registros.
- Matrices de amenazas y riesgos.
- Requerimientos.
- Doctrina y base de datos en conocimiento.

Responsable del Proceso. Jefe de operaciones de ciberdefensa del CEOPC.

Tipo de Cliente.

Internos. Unidades militares del sistema de ciberdefensa de la FT.

Externos. Comandos, direcciones y unidades militares.

Fundamentación Documental

En referencia a la revisión documental desarrollada actualmente en la FT y AGRUCOMGE no existe estructura, unidad o dependencia relacionada a la ciberdefensa o alguna relación directa con el COCIBER del CCFFAA. Los resultados de la investigación y la correlación de variables determinan que la estructura organización tienen el mayor impacto en la ciberdefensa de la FT. En función de lo cual se propone la estructura ilustrada en la figura 26 como componente del sistema.

La propuesta enlaza los niveles táctico, operacional y estratégico en el contexto militar, los cuales concuerdan con los niveles en el entorno civil técnico, gerencia y directivo respectivamente desarrollado en revisión bibliográficas.

Fundamentación Filosófica

Se propone que para el entorno militar táctico y operacional, la propuesta se basa en los fundamentos dentro del contexto de defensa y seguridad de TIC de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad. Fundamentos adoptados a nivel nacional, regional e internacional por Estados, organizaciones público o privado.

Validación de la Propuesta

Conceptualización de la Propuesta

El Sistema de Gestión de Ciberdefensa propuesto para la FT se organiza con fundamentos, estructura, arquitectura de la red y procesos. Se respaldo con el marco legal descrito y de estandarización. Propone una aproximación a conceptualizaciones de ciberespacio y ciberdefensa para la FT.

Se describe los fundamentos aplicables para el sistema en el contexto de defensa y seguridad. Se ilustra la estructura organizacional y sus componentes, que se basa en los objetivos estratégicos del MIDENA, CCFFAA y FT. Se describe las unidades o dependencias que conforman el sistema.

Se propone crear un CEOPC como parte del COT, el cual debe gestionar operaciones de defensa y exploración en el ciberespacio de responsabilidad de FT y las que se le asigne por parte del CCFFAA. Este centro tendrá como su escalón técnico superior de ciberdefensa al COCIBER del CCFFAA y como escalón técnico subordinado al AGRUCOMGE.

Como parte del AGRUCOMGE se plantea la creación de una UOCIBER, como una fuerza militar encargada de planificar, coordina, integrar y ejecutar operaciones de defensa y exploración en el ciberespacio. Esta unidad a su vez ubica al CEOPC como su escalón técnico superior de ciberdefensa y como escalones técnicos subordinados a las compañías y pelotones de comunicaciones de las unidades de la FT tipo División, Brigada, Grupo o Batallón.

Las compañías y pelotones de comunicaciones, ejecutan o accionan las operaciones de defensa y exploración a través del empleo de los EPC.

Se estructura la arquitectura de la red de información de la FT, conformada con sus cinco capas.

Se define un proceso para el sistema, el cual articula los subprocesos de gestión, planificación y ejecución.

Método y Criterios de Validación

Se aplica el análisis mediante la valoración de la matriz Positivo, Negativo e Interesante (PNI) la cual es una herramienta sencilla y creativa, desarrollando sus criterios positivo, negativo e interesantes respecto de la propuesta presentada.

La descripción de los criterios se desarrolla a continuación:

- Positivos, criterios o aspectos favorables, fortalezas, bondades.
- Negativo, criterios o aspectos inaceptables, debilidades, que presentan riesgos sin utilidad o malos.
- Interesantes, criterios o aspectos innovadores, curiosos, posibles potenciales positivos

Validación

Matriz de Validación

En la tabla 7 se desarrolla la matriz de validación de la propuesta presentada mediante el análisis PNI.

Tabla 7

Matriz de Valoración

Positivo	Negativo	Interesantes
Facilita recursos de personal, presupuesto e infraestructura.	Requiere modificaciones presupuestarias.	Marco legal de actuación.
Permite implementar técnicas, métodos, procesos y gestión en el entorno de ciberdefensa.	No existe doctrina de ciberdefensa.	Marco ético de actuación.
Proporciona la defensa de los activos de TIC. Gestión de convenios y cooperación en área de ciberdefensa. Transversalidad en el nivel táctico y operacional de las unidades de la FT respecto a la ciberdefensa.	Personal especializado.	Apoyo de otros países o instituciones internacionales.

En referencia a los aspectos descritos en la matriz PIN, que presenta un mayor número de aspectos positivos, esta permite validar la propuesta planteada de la investigación.

Conclusiones y Recomendaciones

Conclusiones

La ausencia de una norma legal y estructura organizacional, se presentan como las principales dificultades para el mantenimiento de una efectiva ciberdefensa. La estructura influye directamente en la capacitación y recursos. Estas dificultades impactan en para que la ciberdefensa en la FT sea limitada.

La hipótesis de investigación es aceptada, en función de la correlación es positiva. Al incrementar los indicadores de la variable independiente como el indicador estructura se incrementa la protección, sin estructura la protección y seguridad de los datos, información e infraestructura de TIC de la FT será débil o limitada.

En referencia que no existe actualmente una estructura en funcionamiento, aprobada o prevista de ciberdefensa en la FT, esta influirá en la conformación de unidades o dependencias, programas de capacitación, recursos y el desarrollo de procesos.

En base a los resultados y hallazgos de la investigación se requiere una estructura organizacional, la cual se encuentra incluida en la propuesta como parte del Sistema de Gestión de Ciberdefensa de la FT. En esta se aporta con la definición de conceptualizaciones y fundamentos en el contexto de la ciberdefensa que actualmente no existe en la doctrina de la FT.

La estructura propuesta se alinea a los OEI del MINEDA, CCFFAA y FT, define las agencias responsables planteando la creación del CEOPC subordinada del COT y UOCIBER subordinada del AGRUCOMGE. La base de la estructura son las unidades del sistema del arma de Comunicaciones en las cuales se conforma los EPC.

Se contribuye con la estructuración de la arquitectura de la red de información de la FT, con la definición de sus capas que conforman su ciberespacio. Se plantea un

proceso de ciberdefensa, caracterizando a los subprocesos de gestión, planificación y empleo de operaciones de ciberdefensa.

La situación actual de la FT en ámbito de la ciberdefensa impacta negativamente en la seguridad y defensa de datos, información e infraestructura de las TIC. Lo cual afecta a los fundamentos de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad en el contexto de la defensa y seguridad del ciberespacio de la FT.

Recomendaciones

Para superar las deficiencias en ciberdefensa una vez se implante un sistema de gestión que incluya una estructura tipo, se requiere desarrollar programas de capacitación para el personal involucrado en esta nueva área de conocimiento, en función que el recurso de personal constituye el recurso más valioso.

La gestión de ciberdefensa debe incluir su infraestructura, desarrollar entrenamientos, evaluaciones constantes del personal encargado, convenios de cooperación y capacitación e impulsar la cultura organizacional.

Como futuras líneas de investigación, en base a los resultados y hallazgos debe considerarse a la capacitación en esta área de conocimiento en el contexto militar, por medio de propuestas de creación o adopción de esta capacidad a escuelas o institutos de la FT.

Otra línea de investigación es la relacionada a plantear nuevos sistemas o procesos de I+D+i o la denominada Teoría de la emulación militar.

Referencias Bibliográficas

Abalde, E., & Muñoz, J. (1992). *Metodologia Cuantitativa vs. Cualitativa* (pp. 89–99). pp. 89–99. Recuperado de http://hdl.handle.net/2183/8536

Arribas, G. N. (2011). *Introducción a las vulnerabilidades* (S. FUOC Eureca Media, Ed.). Barcelona: FUOC.

Batanero, J. C. (2013). CIBERDEFENSA. *Ciberdefensa*, pp. 1–40. Recuperado de http://www.criptored.upm.es/descarga/ConferenciaJuanCarlosBataneroTASSI2013.pdf

Bejarano, M. J. C. (2011, marzo 17). Nuevo Concepto de Ciberdefensa de la OTAN. *INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS*, pp. 1–5. Recuperado de http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

Cabral, V. J. Q. (2015). *La estrategia de Argentina y Brasil para la Defensa Cibernética , una análisis por los niveles de la conducción*. Recuperado de http://190.12.101.91:80/jspui/handle/1847939/462

Carayannis, E., & Campbell, D. (2018). *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense* (C. Springer, Ed.). 2018.

Cárdenas, W. (2015). *Ciberdefensa y Ciberseguridad en el Sector Defensa de Colombia*. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2849/00002590.pdf?sequence=1

Carneiro, J. (2019). *¿Cómo enfrentar este nuevo domínio militar? Nivel operacional e gerencial – Visión Militar*. YouTube.

Castro Peralvo, E. J. (2015). *Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador* (UFA ESPE). Recuperado de http://repositorio.espe.edu.ec/bitstream/21000/7426/2/T-ESPE-047514.pdf

Centro Conjunto de Desarrollo de Conceptos [CESEDEN]. (2018). *Concepto de Ciberdefensa - Resumen Ejecutivo*.

Centro de Estudios Estratégicos de la Academia de Guerra [CEEG]. (2018). *La Ciberguerra: Sus Impactos y Desafíos* (Andros Impresores, Ed.). Recuperado de http://www.ceeag.cl/wp-content/uploads/2018/07/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf

Centro de Respuesta a Incidentes Informáticos del Ecuador. (2017). Nosotros. Recuperado el 11 de octubre de 2020, de https://www.ecucert.gob.ec/nosotros.html

Cicerchia, C. (2019). *Ciberdefensa Nivel Operacional/Gerencial*. YouTube.

Cisco Systems. (2018). Reporte Anual de Ciberseguridad de Cisco 2018. En *Reporte Anual de Ciberseguridad de Cisco 2018* (Vol. 1). Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

Cisco Systems. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. En *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*. Recuperado de http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

Claus, B., Gandhi, R. A., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. *Journal of Strategic Security*, *8*(4), 1–22. https://doi.org/10.5038/1944-0472.8.4.1441

Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público. *Ley 0 de 2017. Art. 1-2*. , (2017).

Código Orgánico Integral Penal [COIP]. *Ley 0 de 2014. Art. 229-234*. , (2014).

Comando Cibernético del Ejército de los Estados Unidos. (2020). U.S. Army Cyber Command. Recuperado el 9 de octubre de 2020, de 2 de septiembre website: https://www.arcyber.army.mil/

Comando Conjunto de las Fuerzas Armadas del Ecuador. (2010). *Plan Estratégico Institucional de Fuerzas Armadas*. Recuperado de https://www.ccffaa.mil.ec/wp-content/uploads/sites/8/2019/04/k-anexo-1-PLAN-ESTRATEGICO-FF.AA_.-2010-2021.pdf

Comando Conjunto de las Fuerzas Armadas del Ecuador. (2018). *Estatuto Orgánico por procesos Comando Conjunto Fuerzas Armadas*. Recuperado de https://www.ccffaa.mil.ec/wp-content/uploads/sites/8/2019/04/a2-anexo-23-estatuto_por_procesos_comaco.pdf

Constitución de la República del Ecuador. *Art.158*. , (2008).

Dixon. (2014). *Protecting an Organization's Most Important Asset: Information*. Recuperado de https://search-proquest-com.biblioteca-uoc.idm.oclc.org/docview/1535257890?accountid=15299

Ejército Británico. (2020). *IN FRONT*. Recuperado de https://www.army.mod.uk/media/10192/adr009405_in_front_5.pdf

El Telégrafo. (2018). Cayó red que vendía armas a "Guacho". Recuperado el 23 de octubre de 2020, de 18 de octubre de 2018 website: https://www.eltelegrafo.com.ec/noticias/judicial/12/operacion-camaleon-detenidos-provincias-ecuador

Emm, D., & Chebyshev, V. (2018). *Kaspersky: Boletín de seguridad PRINCIPALES HISTORIAS DE SEGURIDAD EN 2018*. Recuperado de https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2018/12/14040903/KSB2018_Review-of-the-year_final_SP.pdf

Empresa DarFe. (2019). Ciclo sobre Ciberdefensa Webinar 1 (nivel táctico/técnico) [Archivo de Vídeo]. Youtube. Recuperado el 24 de octubre de 2020, de 5 de octubre de 2019 website: https://www.youtube.com/watch?v=e554iMxXeOw

Escuela de Altos Estudios de la Defensa de España. (2014). Documentos de Seguridad y Defensa 60. *Estrategia de la información y seguridad en el ciberespacio*, p. 125. Recuperado de http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf

ESET. (2019). *ESET SECURITY REPORT Latinoamérica 2019*.

Fuerza Terrestre. (2017). *Objetivos Estratégicos del Ejército Ecuatooriano* (p. 9). p. 9.

Gibson, W. (1984). *Neuromancer* (Ace Books, Ed.).

Hernández, R., Fernández, C., & Baptista, M. del P. (2014). *Metdología de la Investigación* (Sexta; McGRAW-HILL, Ed.).

Joint Chiefs of Staff. (2018). *Cyberspace Operations*.

Ley de Seguridad Pública y del Estado. *Ley 0 de 2009. Art. 21-22 46*. , (2009).

Ley Orgánica de la Defensa Nacional. *Ley 74 de 2007. Art. 1-2*. , (2007).

Malvacio, E. (2019). *¿Cómo enfrentar este nuevo dominio militar? Nivel Táctico & Técnico*. YouTube.

Ministerio de Defensa del Reino Unido. (2020). Armed Forces announce launch of Cyber Regiment in major modernisation. Recuperado el 6 de octubre de 2020, de 4 de junio website: https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation

Ministerio de Defensa Nacional Chile. (2015). *Bases para una Política Nacional de Ciberseguridad* (pp. 1–15). pp. 1–15. Recuperado de https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Política-Nacional-sobre-Ciberseguridad.pdf

Ministerio de Defensa Nacional del Ecuador. (2017). *Plan Estratégico Institucional de Defensa 2017-2021*. Recuperado de https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/02/plan-estrategico-20-enero-2020-web.pdf

Ministerio de Defensa Nacional del Ecuador. (2019). *Plan Específico de Defensa 2019-2030*.

Ministerio de Economía y Finanzas. (2018). *Normas Técnicas de Presupuesto* (p. 53). p. 53. Recuperado de https://www.finanzas.gob.ec/wp-content/uploads/downloads/2018/04/Normativa-Presupuestaria-Codificación-5-de-abril-de-2018-OK-ilovepdf-compressed.pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (2018a). *Libro Blanco de la Sociedad de la Información y del Conocimiento* (Primera). Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/07/Libro-Blanco-de-la-Sociedad-del-Información-y-del-Conocimento.pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (2018b). Plan de la Sociedad de la Información y del Conocimiento borrador. Recuperado el 15 de octubre de 2020, de https://plansociedadinformacion.mintel.gob.ec/#

Ministerio de Telecomunicaciones y Sociedad de la Información. (2018c). *Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad*. Quito.

Ministerio de Telecomunicaciones y Sociedad de la Información. (2019). *Esquema Gubernamental de Seguridad de la Información [EGSI]*. Recuperado de https://www.gobiernoelectronico.gob.ec/egsi/

Moresi, A. (2019). *Ciberdefensa: ¿Cómo enfrentar este nuevo Dominio Militar?* YouTube.

Nielsen, S. (2016). The Role of the U . S . Military in Cyberspace. *Journal of Information Warfare*, *15*(2), 27–38. Recuperado de https://search-proquest-com.biblioteca-uoc.idm.oclc.org/docview/1968022194?accountid=15299

Política de la Defensa Nacional del Ecuador “Libro Blanco”. *Cap. I-V-VI*. , (2018).

Real Academia Española. (2019). Diccionario de la lengua española | Edición | RAE - ASALE. Recuperado el 2 de enero de 2020, de Real Academia Española website: https://dle.rae.es

Regueira, F. (2019). *Visión Militar*. YouTube.

Reichheld, F. (2003). The One Number You Need to Grow. *Harvard business review*, *81*(12), 46–55. Recuperado de www.hbr.org

Secretaría Nacional de Planificación y Desarrollo. (2017). *Plan Nacional de Desarrollo 2017-2021-Toda una Vida*. Recuperado de www.planificacion.gob.ec

Statista. (2019a). IT Security. En *IT Security*. Recuperado de https://www-statista-com.biblioteca-uoc.idm.oclc.org/study/15503/information-security-statista-dossier/

Statista. (2019b). *Security Software*. Recuperado de https://www-statista-com.biblioteca-uoc.idm.oclc.org/study/22270/security-software-statista-dossier/

Unión Internacional de Telecomunicaciones. (2004). Visión general de las redes de próxima generación. Recuperado el 14 de octubre de 2020, de https://www.itu.int/rec/T-REC-Y.2001-200412-I/es

Unión Internacional de Telecomunicaciones. (2010). *Ciberseguridad*. Recuperado de https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Unión Internacional de Telecomunicaciones. (2019). *Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research*. Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (20), 31. https://doi.org/10.17141/urvio.20.2017.2571

Wells, L. (2017). Cognitive-Emotional Conflict. *Prism*, *7*(2), 4–17. Recuperado de http://www.jstor.org/stable/26470514

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine* (MIT press, Ed.).

Zúñiga, J. (2017). *Ciberdefensa y su incidencia en la protección de la información del Ejército del Perú, Caso: COPERE 2013-2014*. Recuperado de http://repositorio.icte.ejercito.mil.pe/handle/ICTE/32

Apéndices