La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033

Acosta Sánchez, Bolívar Vinicio y Vizcaíno Villavicencio, Christian Michel

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 en Conducción Militar

Msc. Muñoz Morales, Bethy Andrea

13 de noviembre de 2023

Copyleaks

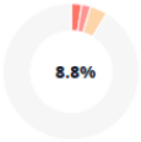
Plagiarism and AI Content Detection Report

TESIS_FINAL_MAYO_ACOSTA_BOLÍVAR...

Scan details

Scan time:	Total Pages:	Total Words:
August 27th, 2023 at 22:43 UTC	109	27190

Plagiarism Detection



Types of plagiarism		Words
Identical	2.1%	582
Minor Changes	1.8%	501
Paraphrased	3.5%	958
Omitted Words	14.3%	3885

AI Content Detection

Text coverage		Words
AI text	0%	0
Human text	100%	23305

Learn more

Firmado electrónicamente por: BETHY ANDREA MUÑOZ MORALES

Muñoz Morales, Bethy Andrea

Director

C.C.: 1714086236

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: "**La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033**" fue realizado por los señores **Tcrn EM Acosta Sánchez Bolívar Vinicio** y **Tcrn EM Vizcaíno Villavicencio Christian Michel;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 09 de noviembre de 2023

Firmado electrónicamente por:
BETHY ANDREA MUÑOZ MORALES

Muñoz Morales, Bethy Andrea

Director

C.C.: 1714086236

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Nosotros **Tcrn EM Acosta Sánchez Bolívar Vinicio** y **Tcrn EM Vizcaíno Villavicencio Christian Michel**, con cédulas de ciudadanía N° 0502334477 y 1706740600, declaramos que el contenido, ideas y criterios del trabajo de titulación*:* ***"La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033"*** 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, 09 de noviembre de 2023

Firmado electrónicamente por:
BOLIVAR VINICIO
ACOSTA SANCHEZ

Acosta Sánchez, Bolívar Vinicio

C.C.: 0502334477

Firmado electrónicamente por:
CHRISTIAN MICHEL
VIZCAINO
VILLAVICENCIO

Vizcaíno Villavicencio, Christian Michel

C.C.: 1706740600

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Nosotros **Tcrn EM Acosta Sánchez Bolívar Vinicio** y **Tcrn EM Vizcaíno Villavicencio Christian Michel**, con cédulas de ciudadanía N° 0502334477 y 1706740600, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 09 de noviembre de 2023

Firmado electrónicamente por:
BOLIVAR VINICIO ACOSTA SANCHEZ

Acosta Sánchez, Bolívar Vinicio

C.C.: 0502334477

Firmado electrónicamente por:
CHRISTIAN MICHEL VIZCAINO VILLAVICENCIO

Vizcaíno Villavicencio, Christian Michel

C.C.: 1706740600

Dedicatoria

A la Academia de Guerra de la Fuerza Terrestre, por transmitir los conocimientos necesarios en el perfeccionamiento de los oficiales de Estado Mayor. A Mi Tcrn E.M Ángelo Semanate quien es la guía más importante en la cristalización de este trabajo.

Acosta Sánchez Bolívar Vinicio & Vizcaíno Villavicencio Christian Michel

Autores

Agradecimiento

Al Todopoderoso, quien es la guía de nuestro camino por la vida, a nuestras esposas, hijos y padres por su incondicional apoyo, el cual es fundamental en nuestro progreso profesional, a la Academia de Guerra de la Fuerza Terrestre, por el aporte de sus docentes en nuestro perfeccionamiento por medio del cual se ha hecho posible alcanzar esta meta.

Acosta Sánchez Bolívar Vinicio & Vizcaíno Villavicencio Christian Michel

Autores

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

La ciberdefensa militar permite a las fuerzas armadas de un país, ejecutar ciberoperaciones en el quinto dominio del campo de batalla, la Fuerza Terrestre del Ecuador en su ámbito de acción, requiere ejecutar la defensa y exploración de sus sistemas de información, bases de datos y redes de comunicación de datos y en cualquier momento y con orden la respuesta a un ataque ciberespacial de una amenaza híbrida, interestatal o internacional. El nuevo escenario estratégico exige el desarrollo de la capacidad ciberespacial en cada una de las ramas de las Fuerzas Armadas como componentes de las operaciones militares conjuntas, es por eso que este trabajo de investigación permitirá al ejército ecuatoriano, disponer de un análisis prospectivo de la ciberdefensa con proyección al año 2033, proporcionando una orientación para el incremento del nivel de madurez de esta capacidad de una manera integral y organizada, mediante la ejecución de las estrategias planteadas para alcanzar un posible escenario apuesta. Para analizar este fenómeno de estudio, se aplicará la herramienta prospectiva de Godet que se desarrolla en tres fases: inicialmente se construirá una línea base que se puede obtener del análisis del macroambiente y microambiente, posteriormente se definen las variables estratégicas con la herramienta ábaco de Regnier y se construyen los escenarios prospectivos en la matriz morfológica, finalmente se desarrollan las estrategias de la ciberdefensa en la Fuerza Terrestre, para obtener los resultados que permitan generar respuestas a los problemas detectados en el estudio del futuro.

Palabras clave: ciberoperaciones, ciberdefensa, estudio prospectivo, estrategias.

Abstract

Military cyber defense allows the armed forces of a country to execute cyber operations in the fifth domain of the battlefield, the Ecuadorian Land Force in its field of action, requires executing the defense and exploration of its information systems, databases, and data communication networks and at any time and with order the response to a cyberspace attack of a hybrid, interstate, or international threat. The new strategic scenario requires the development of cyberspace capacity in each of the branches of the Armed Forces as components of joint military operations, which is why this research work will allow the Ecuadorian army to have a prospective analysis of cyber defense. with a projection to the year 2033, providing guidance for increasing the level of maturity of this capacity in a comprehensive and organized way, through the execution of the strategies proposed to achieve a possible bet scenario. To analyze this study phenomenon, Godet's prospective tool will be applied, which is developed in three phases: initially, a baseline will be built that can be obtained from the analysis of the macroenvironment and microenvironment, then the strategic variables are defined with the Régnier abacus tool. and the prospective scenarios are built in the morphological matrix, finally the cyber defense strategies are developed in the Land Force, to obtain the results that allow generating answers to the problems detected in the study of the future.

Keywords: cyber operations, cyber defense, prospective study, strategies.

Capítulo I

Planteamiento del Problema

Formulación del Problema

La formulación del problema se establece en base a la interrogante: ¿Cuáles son los actores del sistema, factores de cambio, hechos portadores y los posibles escenarios futuros de la ciberdefensa al año 2033 que permitan el desarrollo de la capacidad ciberespacial en la Fuerza Terrestre ecuatoriana?

Preguntas de Investigación

- ¿Qué aspectos se deben tomar en cuenta en el estudio prospectivo de la ciberdefensa en la Fuerza Terrestre al 2033?
- ¿Cuáles son las capacidades específicas de la ciberdefensa que debe desarrollar la Fuerza Terrestre al 2033?
- ¿Para construir el mejor escenario futuro de la ciberdefensa en la Fuerza Terrestre, cuáles son las mejores estrategias se deben diseñar en el presente?

Antecedentes

El avance tecnológico y el precipitado desarrollo del conocimiento extendido por todo el globo terrestre en la era digital, hace que el mundo moderno conserve una dependencia total del ciberespacio, impactando directamente a la sociedad en su conjunto.

Según lo señaló Sancho (2017), “la gobernabilidad de todo sistema político requiere de considerar tres factores básicos: seguridad como condición, institucionalidad como medio y desarrollo como objetivo” (p. 8). Por otra parte, cantidad de datos virtuales que se generan posibilita almacenar y usar gran cantidad de información con buenos o malos propósitos.

En el Estado ecuatoriano el Ministerio de Defensa Nacional no reconoce al ciberespacio como un dominio emergente, para este organismo gubernamental, se ha constituido en el quinto dominio para las operaciones militares, debido a que es un componente del territorio

ecuatoriano que se ha vinculado explícitamente en la defensa de la soberanía y la seguridad Nacional (Ministerio de Defensa Nacional, 2018).

En el Plan Nacional de Seguridad Integral (2019), se considera la aparición de los ciberataques como una amenaza y una problemática transversal por el creciente uso de la tecnología en el Ecuador, motivo por el cual la seguridad del ciberespacio dentro del Estado representa una condición ineludible para las Fuerzas Armadas, más aún, ahora que en la Declaración sobre Seguridad en las Américas de la Organización de Estados Americanos (OEA, 2003), se reconoció la multidimensionalidad de la seguridad.

Por otra parte, la Política de Defensa Nacional (2018), ha determinado que la vulneración a los sistemas informáticos de las instituciones del Estado constituye una agresión, por lo tanto, todo tipo de ciberataque a la Infraestructura Tecnológica Digital del afecta directamente a la seguridad de este.

En un estudio efectuado por la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre, se señala que actualmente ha existido un incremento de ciberamenazas a los sistemas informáticos, redes de datos, almacenamiento digital de información y plataformas tecnológicas, debido a relación o dependencia directa con este nuevo dominio, que si bien es cierto genera grandes oportunidades, también da origen al surgimiento de ciberataques, lo cual constituye un vector de ataque que impide el normal funcionamiento, las empresas y entidades públicas y privadas e incluso de los ciudadanos (Amigo, 2015).

En la actualidad, también se ha incrementado el uso del ciberespacio para almacenar datos e información sensible e importante del Estado, sus instituciones y las empresas públicas y privadas (Sancho, 2017). Dando lugar de esta manera al incremento de acciones de ciberespionaje para alcanzar información específica, ciberataques para causar pérdida de información y ciberdelitos para obtener dinero, a través de las redes, sistemas y plataformas tecnológicas e informáticas de la Fuerza Terrestre.

En este contexto, existe una marcada presencia de ciberamenazas que atentan en contra del ejército y de la seguridad del Estado, evidenciado lógicamente por una tendencia exponencial de las actividades cibernéticas en el quinto dominio de las operaciones militares. La Fuerza Terrestre consciente de que las ciberamenazas cada vez son más frecuentes, complejas, destructivas y coercitivas, busca establecer los mecanismos necesarios que le permitan garantizar un ciberespacio seguro y la protección de la infraestructura de la institución contra los ciberataques y ciberamenazas de cualquier índole.

Todos estos riesgos en el ciberespacio deben ser minimizados, por lo que es importante el desarrollo de las capacidades de ciberdefensa en la Fuerza Terrestre, que le permitan cumplir de manera efectiva con lo establecido en la Constitución de la República del Ecuador, en la Política Nacional de Ciberseguridad y en la Estrategia de Ciberdefensa, para hacer frente a los retos y amenazas que se presenten en el quinto dominio de la guerra.

Para el desarrollo de capacidades se debe construir los escenarios prospectivos futuros de la ciberdefensa. Para nuestro caso de estudio se ha determinado 10 años, debido a que la Planificación Estratégica de Fuerza Terrestre fijo este horizonte en base a tres períodos de gobierno, por ende, el planteamiento de estrategias estará alineado a los objetivos institucionales, las cuales a su vez permitan desarrollar las capacidades necesarias, estableciendo una estructura y doctrina de empleo de la ciberdefensa en las operaciones en el ámbito interno y en la defensa del territorio nacional.

El levantamiento de las estrategias de ciberdefensa con una proyección al 2033, se vuelve imperativo e imprescindible para que la Fuerza Terrestre pueda responder al incremento de ciberamenazas a su infraestructura tecnológica digital, basados en la identificación de escenarios apuesta, tendencial y cisne negro.

El desarrollo de las estrategias fundamentadas en un estudio prospectivo es una acción viable por cuanto la Fuerza Terrestre no dispone de una visión prospectiva de la ciberdefensa, para identificar los escenarios tendencial, apuesta y cisne negro que le permitirán establecer

las capacidades que el ejército debe desarrollar, a fin de disminuir el riesgo de ser blanco de un ataque en el ciberespacio, mejorar la seguridad digital de su infraestructura tecnológica y establecer los mecanismos necesarios para minimizar los ciberataques en contra de las unidades militares, contribuyendo a la solución de la temática planteada en la sub línea de investigación referente a la Ciberdefensa.

Justificación

El presente trabajo de investigación tiene una connotación sumamente importante para la seguridad digital e infraestructura crítica de la Fuerza Terrestre, considerando que permitirá establecer las estrategias necesarias para el desarrollo de las capacidades de la ciberdefensa en el Ejército proyectados al año 2033, contribuyendo a la solución de la temática planteada en la sub línea de investigación referente a Ciberdefensa; además de esta forma, coadyuva a la protección de los recursos del Estado, garantizando indirectamente al ciudadano un ciberespacio libre y seguro, para el desarrollo de sus actividades.

En función de la situación actual en la que se desarrollan las diferentes actividades en el ciberespacio, estando expuestos a un sin número de ciberamenazas, este trabajo de investigación resolverá problemas reales referentes a vulnerabilidades cibernéticas, como acciones de ciberespionaje, ciberataques y ciberdelitos de toda índole, que en la actualidad afectan a la institución.

Cabe mencionar la importancia de esta investigación, debido a que aportará con fundamentación teórica relacionada a ciberseguridad y ciberdefensa, que servirá para solventar vacíos en los conocimientos tecnológicos, los cuales pueden ser extendidos en todas las unidades o repartos de la Fuerza Terrestre, para que de esta manera se puedan identificar cuáles son las capacidades de ciberdefensa que deberán desarrollarse en el futuro en la institución, además; permitirá el incremento de la protección de los sistemas informáticos, aplicativos, equipos y plataformas tecnológicas; minimizando así los ataques cibernéticos.

Además, la investigación permitirá, definir si existe relación entre las variables que constituyen parte de este proyecto, logrando así determinar la influencia que esta causa dentro del ámbito de la ciberdefensa.

Importancia

El desarrollo de este estudio es importante debido a que la Fuerza Terrestre, en su Manual de Procesos, emplaza el macroproceso tecnologías de la información y comunicaciones como el encargado de la seguridad de la infraestructura crítica digital de la institución, además; el desarrollo y la gestión de los sistemas de información, estos a su vez, cuando son puestos en producción, permiten un eficiente mando y control de las operaciones militares, así como; la automatización de la gestión administrativa que se desarrolla en los demás procesos institucionales.

En la guía de ciberdefensa de la (Junta Interamericana de Defensa, 2020) se señala que una fuerza armada dentro de sus procesos de transformación debe contemplar al ciberespacio como quinto dominio de operaciones militares. En la Fuerza Terrestre del Ecuador, el nivel de madurez de la ciberdefensa es aún incipiente por lo tanto aún no se han desarrollado las capacidades de ciberoperaciones de defensa, exploración y respuesta, sumado a la dependencia institucional a los sistemas de información, ha propiciado a que existan intereses ilegítimos, tanto de personal externo como interno, los cuales al tener conocimiento de las vulnerabilidades en redes de datos, base de datos y aplicaciones desarrolladas por la institución para la automatización de los procesos, obtienen información crítica para alterarla, modificarla o sacar provecho causando perjuicios graves al ejército.

Todos estos aspectos generan vulnerabilidades, amenazas y riesgos en las operaciones militares que ejecuta el ejército, lo cual a su vez afecta directamente a los intereses nacionales, considerando que, desde la infraestructura tecnológica y los datos en red, se extrae información de seguridad que permite hacer más eficiente el logro de las misiones.

Bajo este contexto, el presente trabajo aportará con un estudio prospectivo que defina un escenario futuro al 2033 para la ciberdefensa en la Fuerza Terrestre, todo esto con el objetivo de establecer estrategias que se implementen en los procesos tecnológicos de la institución, los cuales pueden ser generalizados y empleados en todos los repartos de la Fuerza Terrestre, logrando así que existan controles técnicos para la prevención de ciberataques, monitoreo de infraestructuras tecnológicas tanto propias como del enemigo y además la respuesta a incidentes de seguridad informática.

Objetivo General

Determinar los actores del sistema, factores de cambio, hechos portadores y los posibles escenarios futuros de la ciberdefensa al año 2033 que permitan el desarrollo de la capacidad ciberespacial en la Fuerza Terrestre ecuatoriana.

Objetivos Específicos

- Realizar un diagnóstico sobre la situación actual de la capacidad de ciberdefensa en la FT.
- Determinar los actores y variables que influyen en la capacidad de ciberdefensa de la Fuerza Terrestre ecuatoriana, con respecto a los posibles escenarios planteados.
- Establecer los hechos portadores de futuro que influyen en las capacidades de ciberdefensa.
- Construir los escenarios apuesta, tendencial y cisne negro de la ciberdefensa en la Fuerza Terrestre ecuatoriana al año 2033.
- Proponer estrategias de ciberdefensa que permitan alcanzar el escenario apuesta al año 2033.

Capítulo II

Marco Teórico

Fundamentación Teórica

La Prospectiva y la Estrategia como Herramientas de Planeación

Las acciones futuras que serán ejecutadas por una institución siempre están ligadas a una anticipación, es por esta razón que la planificación estratégica y la prospectiva generalmente están sólidamente relacionadas.

Para (Godet M. , 2007) “la prospectiva constituye una anticipación para iluminar las acciones presentes con la luz de los futuros posibles y deseables”, este proceso sistemático fue acuñado en Francia por ciertos políticos y administradores tras la finalización de la Segunda Guerra Mundial, su preocupación por reconstruir un país devastado les permitió desarrollar planes con proyección a lo que podría ocurrir en un futuro cercano.

En la publicación “Introducción al concepto de planificación estratégica”, el autor (Pimentel, 2009) señala que el término de estrategia se deriva del griego estrategos que significa el general, que en su extensión se puede interpretar como el arte del general, es decir en la antigüedad la terminología estaba direccionada únicamente al ámbito militar y específicamente se aplicaba en el máximo grado que puede alcanzar un militar. En la actualidad, el término es utilizado por los estrategas financieros en empresas, siendo su objetivo principal el vender más que sus competidores, dejando atrás el pensamiento de las antiguas generaciones que era la destrucción de sus enemigos.

Metodología de Construcción de Escenarios

El autor de la metodología de construcción de escenarios (Godet M. , 2007) define al escenario “como un conjunto formado por la descripción de una situación futura y un camino de acontecimientos que permiten pasar de una situación original a otra futura”. Para la edificación de escenarios, esta metodología consiente en visualizar el futuro a través de hechos o escenas, los cuales se pueden clasificar de la siguiente manera:

Optimista. Proyecta un futuro posible que no tiene obstáculos ni restricciones.

Pesimista. Espera un futuro negativo con varias problemas y dificultades.

Tendencial. En el que hay un futuro hipotético si no cambian las condiciones actuales.

Apuesta. Se construye en base a planes, proyectos y programas con la estrecha participación de los actores que ponen su mayor esfuerzo para lograrlo.

Cisne Negro. Genera una probabilidad remota con un efecto sorpresa.

Una vez descritos los posibles escenarios que se pueden construir, se describirán las fases de la metodología desarrollada por el francés Michael Godet:

Primera Fase

Construir la Base. Permite realizar el análisis del problema expuesto en dos subfases:

1. Análisis del ambiente: macroambiente (dimensiones político, ambiental, social, tecnológico y militar) y microambiente (árbol de Giget o árbol de competencias).
2. FODA prospectivo: en esta subfase se recolecta la información generada en la subfase análisis del ambiente, para conseguir como efecto del macroambiente las oportunidades y amenazas y del microambiente fortalezas y debilidades.

Una vez finalizada la primera fase, se obtienen los posibles factores de cambio los cuales de acuerdo con el autor del libro “La construcción del futuro, Concepto y modelo de la prospectiva estratégica, territorial y tecnológica” (Mojica, 2005) son “las características de la organización o sistema. Son fenómenos económicos, sociales, culturales, tecnológicos, políticos etc.” Para realizar el análisis de las variables de los posibles escenarios, los conceptos que fueron encontrados en la matriz de fortalezas, oportunidades, debilidades y amenazas se deben catalogar en el presente, pasado y futuro.

Segunda Fase

Determinar las Variables Estratégicas. El ábaco de Régnier que es un instrumento que permite determinar las variables estratégicas, a través de la clasificación de un cuadro de variables claves que han sido propuestas a través de expertos en el tema. Las variables que

mejor se representen en la edificación de los escenarios futuros son escogidas. Para el autor (Mojica, 2005), para que las variables sean priorizadas en la herramienta, se debe utilizar un código de colores que permita identificar cuáles serán las más relevantes en la construcción de las distintas escenas o escenarios.

Figura 1

Código de clasificación de variables

COLOR	ACTITUD
Verde oscuro	MUY FAVORABLE
Verde claro	FAVORABLE
Amarillo	NEUTRA
Rojo	MUY DESFAVORABLE
Rosado	DESFAVORABLE
Blanco	VOTO EN BLANCO
Negro	ABSTENCIÓN

Nota. La figura el código de colores para clasificar las variables estratégicas. Tomado del libro "Prospectivas" (Mojica, 2005).

Tercera Fase

Construcción de Escenarios. Para la construcción de escenarios se realiza el análisis morfológico mediante la matriz de Zwicky o morfológica, la cual permite determinar a través de una mixtura coherente de los componentes, las posibles hipótesis de evolución o escenas (optimista, pesimista, tendencial, apuesta y cisne negro).

Las condiciones básicas para la redacción de los escenarios son las siguientes;

- Coherencia: la redacción debe estar relacionado de manera lógica y razonable.
- Pertinencia: las etapas anteriores deben estar unidos al argumento principal.
- Veracidad: la redacción debe corresponder al universo de lo probable y creíble.

Los Avances Tecnológicos vs la Ciberseguridad

La Tecnología. Un argumento importante de esta investigación es la tecnología, en este sentido es primordial dar a conocer que (Bijker, 2005):

"Existen tres niveles de significado en la palabra tecnología. En el nivel más básico, describe a un conjunto de cosas materiales o artefactos, tales como computadoras, autos, o máquinas para votar. En el siguiente nivel también se incluyen actividades humanas, tales como en la tecnología de voto electrónico, donde también se hace referencia al diseño, fabricación y el manejo de este tipo de máquinas. Por último, y más cercano a su origen griego, tecnología refiere a conocimiento, se trata tanto de aquello que la gente conoce como de lo que hace con las máquinas y los procesos de producción relacionados (p. 4)".

Bajo esta premisa, la conceptualización de tecnología en estos tres aspectos es mucho mejor que cuando se la utilizada como un todo.

La tecnología también está definida como una fuerza autónoma en la sociedad, y su funcionamiento es una propiedad intrínseca de máquinas y procesos (Bijker, 2005). Por otra parte, la tecnología en la actualidad es ampliamente usada para referirse a un conjunto variado de herramientas, instrumentos, máquinas, organizaciones, métodos, técnicas, sistemas y programas.

Para (Perozo, 2005) la tecnología es el conocimiento que se aplica sobre las áreas científicas de la ingeniería, a fin de obtener productos y servicios.

Finalmente, (Sabato & Mackenzie, 1982) caracterizó a la tecnología como un paquete de conocimientos de distintas clases científicos técnicos y empíricos.

Características de la Tecnología. La tecnología es el producto de aplicar conocimientos científico y tecnológico para satisfacer las diferentes necesidades de la humanidad, se puede establecer en términos generales como características de la tecnología a la utilidad, diversidad, servicio, impulso científico, productividad, universalidad, especialización, conectividad (Del Moral Durán & Clemenceau Figueroa, 2019).

Importancia de la Tecnología. En la era moderna, más de la mitad de la población mundial tiene acceso a la red, existen cifras alarmantes con respecto a teléfonos inteligentes, debido a que tres mil millones de personas lo poseen y en el año 2021, más de dos billones de personas han efectuado al menos una adquisición a través del ciberespacio. Estos son tan solo unos pocos ejemplos de los muchos que existen, que indican la forma como ha mutado la forma en que vivimos y además, lo lejos que ha conseguido proyectarse la tecnología actual.

La Tecnología y su Beneficio. La innovación tecnológica ha impulsado el bienestar del ser humano, proporcionando una manera de vivir de forma más cómoda. Los beneficios que la tecnología brinda son los siguientes:

- Acceso rápido a la información
- Facilita el aprendizaje
- Ofrece entrenamiento
- Aumenta la productividad y la eficacia

Sin embargo, las nuevas concepciones y prácticas científico-tecnológicas deben ser analizadas desde el aumento de la información y los nuevos conocimientos, la necesidad de capacitación tecnológica y de gestión de la ciencia y la tecnología (Arana, 2015).

Ciberespacio

En la publicación Neuromante (1984) del autor William Gibson, señala que “el ciberespacio es una representación gráfica de los datos de los bancos de cada computador en el sistema humano”. Sorprendente complicación (Gibson, 1984, p 67). No obstante es un vocablo sin existencia física, su dominio en todo ámbito se ha desarrollado exponencialmente en los actuales tiempos, inclusive está siendo destronado por el término metaverso del autor Neal Stephenson, quien describe este término como un cosmo virtual perseverante que logra afectar a la mayoría de los aspectos de la humanidad, con los que interactúa. “Era un lugar

para el trabajo y el ocio, para la autorrealización y el agotamiento físico, para el arte y el comercio". (Stephenson, 1992).

En el ámbito de la defensa, estaban claramente definidas las tres dimensiones en las que actúan las Fuerzas Armadas del Ecuador, terrestre, naval y aérea, sin embargo, con el aparecimiento del neo-término o quinto dominio (ciberespacio), ahora contamos con un nuevo campo de batalla, intangible y sin fronteras. Durante el encuentro "Ciberguerra: Amenazas de un entorno altamente conectado", para el director de ciberseguridad de Génova, el capitán de navío (Cubeiro, 2019) el ciberespacio es un contorno trasversal a los demás ámbitos; por lo que, si algo ocurre en él, se repercute considerablemente en el resto.

Ciberdefensa Militar

La (Junta Interamericana de Defensa, 2020), describe a la ciberdefensa militar en la guía de creación y progreso de esta capacidad en los países iberoamericanos, como "la capacidad de las fuerzas armadas organizada y preparada para combatir en el ciberespacio", sin embargo los autores del trabajo de grado "Un escenario prospectivo de la ciberguerra : la estructura en ciberdefensa de los Estados Unidos", catalogan a la ciberdefensa "como las actividades o procedimientos dirigidos a preservar la seguridad de los sistemas de información ya sea de una organización o a las personas de una comunidad" (Cortés Chaves y otros, 2019). Como se puede observar, la Junta Interamericana de Defensa, señala a la ciberdefensa como una capacidad exclusiva de las fuerzas armadas de una nación, siendo este criterio el más acertado, debido a que "el Estado tiene el deber de proteger a su población de amenazas de orden interno y externo" de acuerdo al autor (Moncayo Gallegos, 2012), concordante con el concepto desarrollado por Thomas Hobbes en su obra Leviatán en 1651, el poder del Estado soberano es un poder absoluto, siendo exclusivo de este el monopolio de la fuerza.

Fuerza Ciberespacial

Las fuerzas armadas de una nación deben incluir en sus filas, cibersoldados como parte de una fuerza ciberespacial con las capacidades necesarias para hacer frente a las amenazas

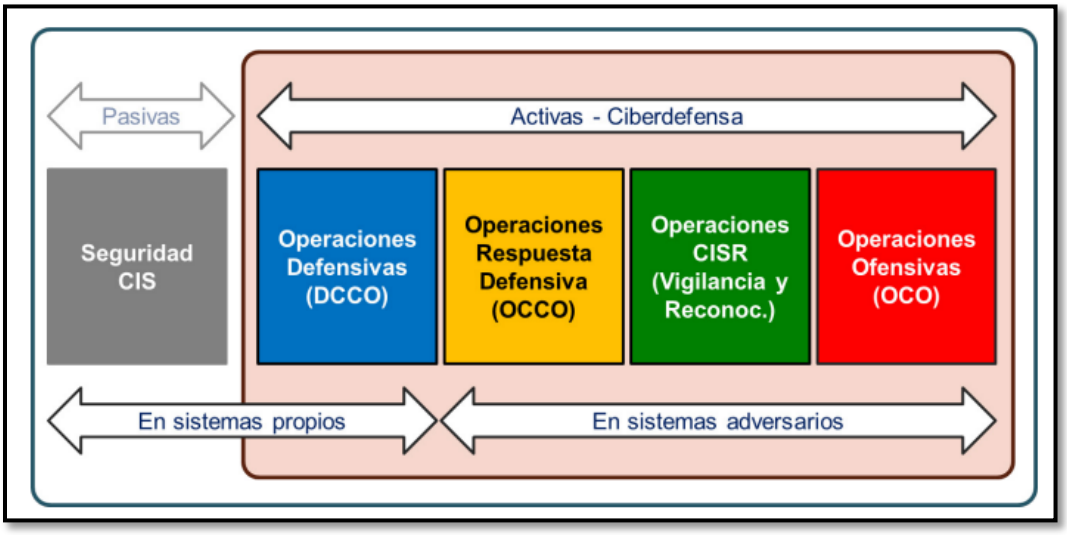
que se produzcan en el ciberespacio, así como en cualquiera de los otros ámbitos: terrestre, marítimo, aéreo y aeroespacial. De acuerdo con la (Junta Interamericana de Defensa, 2020) una fuerza ciberespacial es el conjunto de alícuotas de todas las fuerzas, las cuales se encuentran constituidas bajo un mandó único, siendo estas responsables de la planificación y conducción de las operaciones militares de defensa, explotación o exploración y ataque en el ciberespacio.

Capacidades Operativas

En una guerra cibernética la protección de la soberanía se enfoca en proteger la infraestructura crítica digital de los sectores estratégicos, gestionando o minimizando los eventos de ciberseguridad tanto de ciberamenazas internas como interestatales, la fuerza ciberespacial deberá ejecutar ciberoperaciones mediante las capacidades de defensa, explotación y ataque en el ciber dominio:

Figura 2

Gráfico de las ciberoperaciones.



Nota. El gráfico representa la ejecución de ciberoperaciones de una fuerza ciberespacial. Tomado del artículo “La dimensión cibernética en el ámbito de las fuerzas armadas” (Fojón Chamorro, 2021).

Ciberoperaciones de Defensa. El (Ministerio de Defensa de la República de Brasil, 2014) en la doctrina de operaciones señala que son “las acciones para neutralizar ataques y exploración cibernética contra nuestros dispositivos de cómputo, redes informáticas y de comunicaciones, incrementando las acciones de seguridad cibernética ante una situación de crisis o conflicto”, estas se dividen en ciberoperaciones defensivas activas y pasivas.

Ciberoperaciones de Defensa Activa. Son ciberoperaciones autorizadas por los responsables de tecnologías de la información con las cuales se ejecutan acciones intrusivas en redes propias, permitiendo la evaluación de la red para encontrar vulnerabilidades o riesgos que afecten el propio ciberespacio.

Ciberoperaciones de Defensa Pasiva. Son dirigidas a redes propias y permiten la protección del ciberespacio propio, descartando acciones contra un tercero.

Ciberoperaciones de Exploración. Consisten en acciones de búsqueda o recolección en los sistemas de tecnologías de la información de interés, con el fin de obtener conocimiento situacional del ambiente cibernético. (Ministerio de Defensa de la República de Brasil, 2014). Se dividen en ciberoperaciones de exploración activas y pasivas.

Ciberoperaciones de Exploración Pasiva. Son ciberoperaciones no intrusivas que se ejecutan en las redes de datos y de comunicaciones propias, planificadas por una fuerza ciberespacial con el objetivo de producir ciberinteligencia, en apoyo a las ciberoperaciones de defensa y respuesta (Junta Interamericana de Defensa, 2020).

Ciberoperaciones de Exploración Activa. Son ciberoperaciones intrusivas, ejecutadas en redes de datos y de comunicaciones del enemigo u oponente, ejecutadas por una fuerza ciberespacial con el objetivo de obtener información para producir ciberinteligencia necesaria para la ejecución de ciberoperaciones o en apoyo a las operaciones convencionales en el ámbito terrestre, naval y aéreo (Junta Interamericana de Defensa, 2020).

Ciberoperaciones de Respuesta. Para el (Ministerio de Defensa de la República de Brasil, 2014), comprenden las acciones para interrumpir, negar, degradar, corromper o destruir información o sistemas computacionales y comunicacionales del oponente (p.23).

Figura 3

Gráfico de las ciberoperaciones de respuesta.

Nota. El gráfico representa las ciberoperaciones de respuesta que ejecuta una fuerza ciberespacial. Tomado de la “Guía de ciberdefensa” (Junta Interamericana de Defensa, 2020).

La (Junta Interamericana de Defensa, 2020) define a estas ciberoperaciones como aquellas que se ejecutan en el ciberespacio de una amenaza o adversario con la finalidad de responder, prevenir o anticiparse a un ciberataque. Se dividen en ciberoperaciones de respuesta preventivas, anticipadas y reactivas.

Ciberoperaciones de Respuesta Preventiva. Operaciones ofensivas que ejecutan en redes de datos del enemigo para evitar un ciberataque, una vez que la ciberinteligencia tiene constancia que este último tiene planeado incurrir en un futuro cercano en el ciberespacio azul (Junta Interamericana de Defensa, 2020).

Ciberoperaciones de Respuesta Preventiva. Se ejecutan en redes de datos del enemigo para evitar un ciberataque, una vez que la ciberinteligencia tiene constancia que este último tiene planeado incurrir en un futuro cercano en el ciberespacio azul (Junta Interamericana de Defensa, 2020).

Ciberoperaciones de Respuesta Anticipada. Operaciones ofensivas que se ejecutan en redes de datos del enemigo, una vez que la ciberinteligencia tiene constancia que este último ejecutará de forma inminente un ciberataque en el ciberespacio azul (Junta Interamericana de Defensa, 2020).

Ciberoperaciones de Respuesta Anticipada. Operaciones ofensivas que se ejecutan en redes de datos del enemigo, para detener o repeler un ciberataque en curso en el ciberespacio azul (Junta Interamericana de Defensa, 2020).

Vulnerabilidad a los Ataques Cibernéticos

El siglo XXI ligado a la digitalización de los sistemas informáticos, la firme evolución tecnológica de la mano con la inteligencia artificial, el conjunto de datos de gran tamaño caracterizado por su complejidad y el desarrollo de la cuarta o ya quinta revolución industrial tiene una gran cantidad de puntos positivos, pero también perjudiciales. El mundo digitalizado ha puesto al descubierto información sensible de empresas o instituciones públicas y privadas debido a que son totalmente vulnerables a los ataques cibernéticos (Iberdrola, 2022).

Una guerra cibernética es más probable que se produzca que una guerra tradicional, tal como apuntaron los expertos Alex Ross y Karen Elazari en el Shapes de marzo de 2021. “De hecho, cada vez hay más organizaciones criminales que orientan su actividad hacia los ciberataques”. La infraestructura menos compleja y la alta rentabilidad que se obtiene producto de un ciberataque constituye un reto para las instituciones encargadas de velar por la seguridad de este dominio, debido a que es muy difícil seguir el rastro de sus acciones (Iberdrola, 2022).

Por otra parte, el Internet se ha convertido, sin duda alguna, en un elemento clave para el crecimiento económico, además de un recurso crítico del cual otros sectores económicos y productivos depende tales como las operaciones bancarias/financieras tanto nacionales como internacionales, infraestructuras y medios de transporte, el sector energético y sanitario. Debido al alto grado de dependencia que estos sectores tienen de internet y de las tecnologías de la información y de la comunicación (TIC), un fallo en la red o una incidencia sobre la misma podría suponer una vulnerabilidad y/o amenaza en materia de seguridad, bien de índole energética, sanitaria, económica, etc. (Gazapo & Machin, 2016).

"A nivel internacional, la ciberdefensa y la ciberseguridad están declaradas como una de las mayores prioridades en términos de seguridad, debido a que uno de los retos a nivel global en la actualidad es la necesidad de poder tratar adecuadamente la información, se trata de un tema de incuestionable relevancia en vista que cada vez aumenta en mayor medida la dependencia en torno a los medios cibernéticos el desarrollo de la actividad cibernética ha proporcionado innumerables beneficios a la sociedad además; la rapidez con que evolucionan las tecnologías, sumado al ritmo con el que se expande el ciberespacio, no permite desarrollar los mecanismos adecuados para prevenir de forma eficaz y eficiente las ciberamenazas: los ataques cibernéticos vulneran las políticas establecidas, por lo que se puede afirmar sin lugar a duda que es el actual talón de Aquiles de nuestra sociedad" (Gazapo & Machin, 2016).

Ciberamenazas

El vertiginoso desarrollo tecnológico ha visto surgir la internet de las cosas (IoT), La hiperconectividad (G5), el paradigma de la computación en la nube, la robotización de los procesos con los sistemas ciberfísicos (CS), la computación cuántica, el empleo de datos masivos Big Data, y la Inteligencia Artificial en todas sus manifestaciones (redes neuronales - NN, Aprendizaje profundo - Deep learning, Aprendizaje automático - Machine Learning). todas estas son fuerzas impulsoras de la transformación digital como inductor de un nuevo modelo

económico, que conlleva un sinnúmero de ventajas, fortalezas y oportunidades, pero que también trae consigo un incremento significativo de riesgos.

La cantidad de componentes tecnológicos que sostiene este nuevo ecosistema digital crece mucho más rápido que la población humana al momento hay 31,000 millones de dispositivos (sensores, actuadores, cámaras, etc.) en línea, un poco más de cuatro veces la cantidad de seres humanos. esto aumenta exponencialmente la superficie expuesta a ciberataques es más durante el año 2020, por la pandemia, los ciberataques se incrementaron un 600% a nivel mundial.

Figura 4

Amenazas en el ciberespacio.

Nota. El gráfico representa las ciberamenazas y los diferentes vectores de ataque. Tomado del artículo "Ciberguerra: El conflicto armado que se desarrolla a través del ciberespacio" (Cubeiro, 2019).

Este incremento significativo de ciberataques también se debe a que las amenazas tienen acceso a los avances tecnológicos; volviendo los cada vez más complejas y sofisticadas.

los actores detrás de los ciberataques se encuentran altamente motivados por los grandes incentivos económicos. Para la revista tecnológica (Reseller Tech&Consulting, 2023), detrás del cibercrimen existe un mercado global que se estima mueve un billón de dólares al año, lo que equivale al 1,5% del producto interno bruto mundial, superando a los tres motores económicos del crimen en el mundo, estos son trata de personas, tráfico de armas y tráfico de drogas. Los objetivos más comunes de las ciberamenazas están dirigidos a instituciones de gobierno y empresas financieras.

La proliferación de las ciberamenazas con propósitos destructivos, de espionaje y robo de información clave, ha provocado cambios trascendentales en el comportamiento de los actores sociales, políticos, financieros y militares de las naciones. El enemigo se aprovecha del anonimato y la ubicuidad.

Todas estas situaciones conllevan a una nueva y compleja encrucijada, considerando que en este nuevo escenario aparecen amenazas híbridas, que atacan deliberadamente las vulnerabilidades de los Estados y sus instituciones, utilizando el ciberespacio como herramienta más versátil para sus propósitos.

También, se debe considerar que las ciberamenazas utilizan diferentes ciberarmas para realizar sus ataques, estas se diseñan para causar daños de diferente severidad (destrucción, de negación, degradación, interrupción y exfiltración) a objetivos del ciberespacio y de otros dominios de operaciones.

¿Qué son los Ciberataques?

“Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o incluso, utilizada para extorsionar” (Iberdrola, 2022).

Para el Ecuador “es la acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información, mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan” (Estrategia de Ciberdefensa, 2021, P.75).

Existe un claro paralelismo con entre el concepto de ataque armado y un ciberataque debido a que los dos pueden producir daños físicos. “Un ciberataque es una operación tanto ofensiva como defensiva, en la que razonablemente puede esperar que cause daño o la muerte de personas o la destrucción de objetivos” (Schmitt, 2013).

Finalmente, de acuerdo con la publicación del Departamento de Defensa de los Estados Unidos de América, un ciberataque abarca toda acción llevada a cabo a través de las redes computaciones para obstaculizar, rechazar o destruir la información de un grupo de ordenadores de un oponente o enemigo (Cubeiro, 2019).

El informe de perspectivas de ciberseguridad presentado por (Latam CISO, 2023), señala que entre los vectores de ataque más comunes se encuentran los ataques de phishing1, ransomware2 y de infección por malware o programa malicioso, este último es una preocupación latente debido al aumento exponencial de incidentes y noticias destacadas relacionadas a este tipo de ataque.

---

[1] Phishing es un tipo de ciberataque dirigido a engañar a una víctima para que proporcione información a través de fuentes aparentemente confiables (Junta Interamericana de Defensa, 2020).

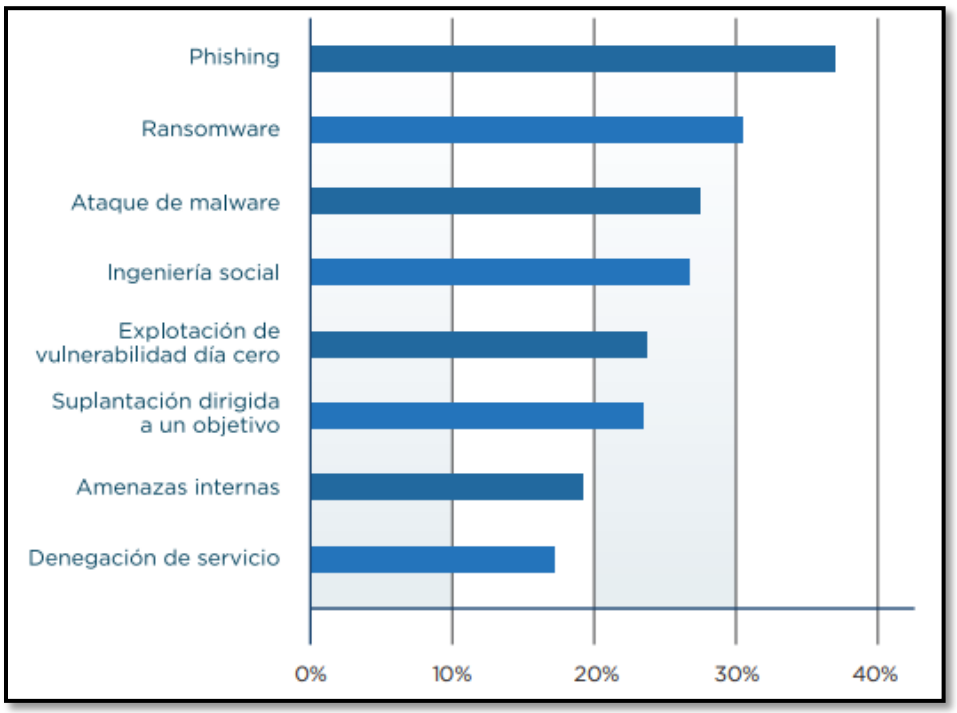
[2] Ransomware es un tipo de ciberataque que cifra archivos de la víctima y amenaza con publicar datos confidenciales, sino se paga su rescate (Junta Interamericana de Defensa, 2020).

Análisis de Vulnerabilidades

Para comprender las vulnerabilidades existentes en el ciberespacio es necesario considerar lo relativo a las ciberamenazas las mismas que son crecientes en la actualidad. “Los Estados persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo o subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales. Estos grupos aprovechan el carácter anónimo que el ciberespacio ofrece para conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución” (Junta Interamericana de Defensa, 2020). “El robo de datos e información, los ataques ransomware y de denegación de servicios como el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas” (Departamento de Seguridad Nacional, 2017).

Figura 5

Tipos de ataques cibernéticos más comunes.



Nota. En el gráfico se incorpora los tipos de ciberataques más comunes. Tomado del informe “Perspectivas de ciberseguridad de los líderes de la industria” (Latam CISO, 2023).

“La utilización del ciberespacio como medio para la realización de actividades ilícitas como acciones de desinformación como propaganda o financiación terrorista y actividades de crimen organizado entre otras, impactan en la Seguridad Nacional, amplificando la complejidad y la incertidumbre, y también pone en riesgo la propia privacidad de los ciudadanos” (Pérez & Ramos, 2020).

“Las vulnerabilidades se consideran como una debilidad en la seguridad de un entorno que puede llegar a permitir o facilitar la actuación de una amenaza; las vulnerabilidades pueden ser de naturaleza técnica, procedimental u operacional”. Habitualmente, en el ámbito TIC, la vulnerabilidad suele ir asociada a un defecto en el software o en la configuración de este, que puede permitir que se materialice una amenaza. Los entornos tecnológicos pueden describirse considerando elementos del ciberespacio en los cuales se pueden generar vulnerabilidades, tal como se describe en el libro “Comprensión y Tecnologías de información interacción y gestión” de los autores (Pérez & Ramos, 2020).

Talento Humano Competencias para Prevenir Riesgos

La gestión del conocimiento en el siglo XXI se convierte en el activo intangible más poderoso de las organizaciones modernas, por cuanto, facilita la potenciación de las competencias del talento humano, como aspectos determinantes para generar capacidad instalada para afrontar los nuevos desafíos que demandan las dinámicas de los mercados en el contexto empresarial de la sociedad actual. Sin embargo, para que esto sea posible, es necesario establecer nuevos enfoques en la gestión del talento humano y alineado con las metas y objetivos en el direccionamiento estratégico de las instituciones. Ello, con el fin de establecer políticas y procedimientos que faciliten la adquisición, distribución, almacenamiento, transformación y utilización de conocimiento, con el propósito de lograr ventajas competitivas en el mercado (Universidad Pontífica Bolivariana, 2015).

Según (Caamaño Fernández & Gil Herrera, 2020) es necesario recalcar que la economía del conocimiento y la sociedad se caracteriza por la globalización económica, la

aparición de los avances tecnológicos en varios dominios industriales y científicos y la primacía progresiva del conocimiento intensivo y tecnología basada en mercados industriales (Martín-de Castro, 2015). En este nuevo escenario competitivo el conocimiento y los activos intelectuales se están convirtiendo en los nuevos factores claves de producción. Por ello, la gestión del conocimiento se convierte en una herramienta poderosa para la toma de decisiones en los distintos sectores económicos, político, sociales, entre otros, dentro de este mundo globalizado (p.7).

Es así, que, la efectividad de la ciberseguridad organizacional tiene relación con la cantidad de profesionales y equipos de trabajo capacitados con que cuenten las organizaciones modernas en este ámbito, permitiendo disponer de herramientas que afronten las ciberamenazas con eficiencia (Caamaño Fernández & Gil Herrera, 2020).

Bajo ese contexto, la gestión del conocimiento funge como medida de prevención de los riesgos de ciberseguridad de las instituciones, por cuanto, asume relevancia en la sociedad del conocimiento donde se deben afrontar cotidianamente la complejidad y la contingencia de su entorno y para lo cual deben desarrollar la capacidad de “aprender a aprender” (Caamaño Fernández & Gil Herrera, 2020).

“Por lo tanto, la gestión del conocimiento, se potencializa a partir de las competencias del talento humano requerida, mediante la adopción e implementación de políticas y procedimientos establecidos, consolide un marco de referencia como medida de prevención y control que responda a los nuevos riesgos de la ciberseguridad generados por el uso de las TIC y se garantice la protección de las organizaciones modernas frente a actividades fraudulentas que impidan el normal desarrollo de las operaciones y la salvaguarda de las finanzas para el cumplimiento de su cometido institucional” (Caamaño Fernández & Gil Herrera, 2020).

Estado del Arte

De acuerdo con el “estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas del Ecuador”, realizado por (Peralvo, 2015) se concluye que existe un mejor escenario para la ciberdefensa en el 2017, debido que el Comando de Ciberdefensa (COCIBER) ha recibido el presupuesto adecuado para el desarrollo de capacidades con las que se pueda enfrentar, neutralizar o adaptarse a los efectos de ciberamenazas. Además; se señala que existe una debilidad en la capacitación del personal que conforma el COCIBER, esto incluido al inexistente marco legal que castigue las actividades ilícitas que se realizan en el internet y redes sociales.

En la tesis de grado de licenciatura multilingüe en negocios y relaciones internacionales de la autora (Abad, 2018), se concluye que el Ministerio de Defensa del Ecuador, ha promulgado políticas y directrices para el manejo adecuado de la información estatal sin embargo; no existen avances de ciberdefensa en el país, debido a que no se trabaja sistemáticamente entre instituciones lo que no permite la apropiada protección de la infraestructura crítica del Estado y sus sectores estratégicos. Además; se pone en evidencia que las redes de datos de los organismos gubernamentales no han minimizado sus vulnerabilidades, exponiéndose cada vez más a ciberataques y amenazas cibernéticas

Según (Jácome Guerrero, 2018) como parte de un curso de especialización, desarrolla un estudio prospectivo llamado “Proyección de la ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021, en el cual describe que Fuerzas Armadas deberá estandarizar los procedimientos de seguridad de manera que permitan prevenir y mitigar los posibles ataques en la institución castrense. Además, deberá incluir en las escuelas de formación y perfeccionamiento asignaturas que permitan entender la importancia de la ciberdefensa en las instituciones del sector público y privado del Ecuador.

Los autores del informe de tesis “Análisis de la situación actual de la ciberdefensa en la Fuerza Terrestre 2020 (Abad Páez & Sandoval Loaiza, 2020), indican que para ese año existe en la Fuerza Terrestre una limitada capacidad de ciberdefensa, debido a que actualmente no

se han implementado unidades o dependencias con estas capacidades, peor aún programas de capacitación, recursos y desarrollo de procesos, esto impacta negativamente en la seguridad de la infraestructura digital y tecnológica del ejército, por lo que se recomienda incluir una infraestructura tipo en esta área donde se deberá contemplar todos los elementos humanos y recursos tecnológicos que permitan impulsar una cultura organizacional de seguridad tecnológica.

Fundamentación Conceptual

Brecha Digital

Según la Estrategia de Ciberdefensa (2021a), “La brecha digital separa los que están conectados a la revolución digital de las TIC de los que no tienen acceso a los beneficios de nuevas tecnologías. La brecha se produce tanto a través de las fronteras internacionales como dentro de las comunidades” (p. 75).

Ciberarma

Según la Estrategia de Ciberdefensa (2021b), es el “Programa código malicioso que sirve para atacar o defenderse en el ciberespacio” (p. 75). Para la autora del artículo “Alcance y ámbito de la seguridad nacional en el ciberespacio” (Caro, 2021), “la ciberarma son programas que atacan uno o varios objetivos”. Muchos de estos sistemas de información son desarrollados por hackers de sombrero negro, quienes ponen a disposición en la dark web, ciberarmas para que sean adquiridos por países en guerra a un costo relativamente bajo. En el mercado negro de la deep web se ofrecen armas más sofisticadas.

Ciberdefensa

Según la Estrategia de Ciberdefensa (2021c), es la “Capacidad del Estado, organizada y preparada para ejecutar operaciones militares que permitan prevenir y contrarrestar las ciberamenazas, ciberataques, incidentes en el ciberespacio o actos hostiles que afecten la soberanía e integridad territorial, el orden constitucional y los intereses nacionales” (p. 75).

Ciberespacio

Según la Estrategia de Ciberdefensa (2021d), es el “Dominio caracterizado por el uso de las tecnologías de la información TI, tecnologías de operación TO, internet de las cosas loT y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de red e infraestructuras asociadas” (p. 75).

Ciberinteligencia

“Actividades de inteligencia en los procesos de la ciberseguridad que se ocupan de analizar (intenciones-oportunidades de los ciberactores y prevenir, identificar, localizar y atribuir ataques o amenazas a través del ciberespacio” (Asint360°, 2016).

Ciberseguridad

Según la Estrategia de Ciberdefensa (2021) es el conjunto de herramientas políticas, técnicas de seguridad, directrices, métodos de gestión de riesgos y tecnologías que puedan utilizarse para proteger los activos de información, durante su procesamiento, almacenamiento, transporte y uso, a fin de prevenir, reducir, neutralizar e investigar los riesgos, amenazas y delitos en el ciberespacio a las que están expuestas todas las personas naturales y jurídicas en el territorio ecuatoriano (p. 75).

Ciberriesgo

Para Guía de ciberdefensa de la (Junta Interamericana de Defensa, 2020) es la posibilidad de que una ciberamenaza aproveche una debilidad de un sistema de información o de una red de datos para causar daño a un activo valorado con una criticidad definitiva. En conclusión, es un indicador que se obtiene de dos factores: la probabilidad y el impacto.

Figura 6

Ciberriesgo

Nota. El gráfico representa el ciberriesgo, la probabilidad y el impacto de una ciberamenaza. Tomado de la Guía de ciberdefensa, (Junta Interamericana de Defensa, 2020).

Hacker

"Persona que por sus avanzados conocimientos en el área informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador" (Ramón, 2021).

Incidente de Seguridad

Según la Estrategia de Ciberdefensa (2021f), es el "Evento singular o serie de eventos de seguridad de la información inesperados o no deseados como que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información" (p. 75).

Infraestructura Crítica Digital

Según la Estrategia de Ciberdefensa (2021g), Son las "instalaciones, redes, sistemas y equipos físicos de tecnologías de información y operación sobre las qué se soporta el funcionamiento de los servicios esenciales de la infraestructura crítica y de las áreas estratégicas del Estado" (p. 75).

Unión Internacional de Telecomunicaciones (ITU)

"Es el organismo especializado en telecomunicaciones de la organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras" (Ministerio de Relaciones Exteriores de Colombia, 2028).

Seguridad de la Información

Según la Estrategia de Ciberdefensa (2021h), es el "conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información (p. 75).

Sociedad del Conocimiento

Son aquellas sociedades "inspiradas en el saber" (UNESCO, 2014).

Fundamentación Legal

Constitución de la República

"La Constitución de 2008 se establece con las normas jurídicas de mayor jerarquía dentro del ordenamiento jurídico ecuatoriano, primando inclusive sobre los convenios y tratados internacionales salvo excepciones en caso de Derechos Humanos más beneficios, leyes orgánicas y ordinarias, así como las demás normas (Asamblea Nacional, 2008). Art. 3, 16, 66 (Núm., 19 y 21), 158, 313, y 393".

Código Orgánico Integral Penal

"Conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, es decir un compendio legislativo que establece delitos y penas conforme al sistema penal ecuatoriano Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014). Art, 103,104,170, 100 178, 188, 190,194, 202.1, 202.2, 229 al 234, 262, 353.1, 415.1, 415.2 472,476, 526 y 553.2".

Ley Orgánica de la Identidad y Datos Civiles

Tiene por objeto garantizar el derecho a la identidad de las personas y normar y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación (Asamblea Nacional del Ecuador, 2016) Art. 1 y 3 (Núm., 4 y 5).

Ley de Seguridad Pública y del Estado

"Tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas comunidades, pueblos, nacionalidades y colectivos, asegurando la Defensa Nacional, previniendo los riesgos de amenazas de todo orden, a través del sistema de Seguridad Pública y del Estado Art. 2,3,10,11,38, 41y 43" (Asamblea Nacional del Ecuador, 2015).

Ley Orgánica de Telecomunicaciones

"Tiene por objeto desarrollar, en el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional bajo los principios y derechos constitucionalmente establecidos (Asamblea Nacional del Ecuador, 2015) Art, 76, 77, 78,79, 80,81, 82,83, 84,85 y 140".

Ley Orgánica de Comercio Electrónico, Firmas de Electrónicas y Mensajes de Datos.

"Regula los mensajes de datos la firma electrónica coma los servicios de certificación, la contratación electrónica y telemática, la presentación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (Asamblea Nacional del Ecuador, 2002)".

Normas Técnicas

NTE INEN- ISO/IEC especialmente sus derivadas:

- NTE INEN- ISO/IEC 27000, "Tecnologías de la información - técnicas de seguridad sistemas de gestión de la seguridad de la información guion descripción general de vocabulario".

- NTE INEN- ISO/IEC 27002:2013, “Tecnología de la información - Técnicas de seguridad - código de prácticas para controles de seguridad de la información”.
- NTE INEN- ISO/IEC 27005, “Tecnología de la información-técnicas de seguridad-gestión de riesgos de seguridad de la información”.
- NTE INEN- ISO/IEC 27032, “Tecnología de la información-técnicas de seguridad y directrices para la ciberseguridad”.
- RESOLUCIÓN ARCOTEL -2018-0652, “Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones publicada en el Registro Oficial NO 331, del 20 de septiembre de 2018” (Arcotel, 2018).
- Resolución No. SB-2018-771 de la Superintendencia de Bancos, que “reforma las normas de control para la gestión del riesgo operativo, publicado en el suplemento del Registro Oficial No. 325, del 12 de septiembre de 2018” (Super Intendencia de Bancos, 2018).

Instrumentos Internacionales

Carta de las Naciones Unidas.

Convenio de Ginebra y sus Protocolos Adicionales. “Resolución AG/RES 2014 (XXXIV-O/04) de la Organización de Estados Americanos (OEA): Adopción de Estrategia de Seguridad Cibernética” (Organización de Estados Americanos, 2014).

- “Resolución UNGA 57/63 y 56/121 de las Naciones Unidas sobre la lucha contra el uso de la tecnología de la información con fines delictivos” (ONU, 2019).
- “Resolución UNGA 57/239, 58/199 y 64/211 de las Naciones Unidas sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de la información” (UNGA, 2019).
- “Resolución UNGA 73/266 sobre Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional” (UNGA, 2019).

- “Declaración para la protección de la infraestructura crítica ante las amenazas emergentes” (CICTE, 2015).
- “Resolución CICTE/RES. 1/19 del 24 de mayo de 2019 sobre Medidas Regionales de Fomento de Confianza en el Ciberespacio (MFCS)” (Comité Interamericano Contra el Terrorismo, 2019).

Instrumentos Nacionales

El Plan Nacional de Seguridad Integral 2019-2030, “desde una visión holística de las problemáticas de seguridad para el Estado, evidencia la aparición de amenazas como los ciberataques que identifica como una problemática transversal por el creciente uso de la tecnología” (Plan Nacional de Seguridad Integral, 2018).

La Política de Defensa Nacional reconoce que los ciberataques y las vulneraciones a la infraestructura crítica tiene la capacidad de afectar al Estado. “Determina que el ciberterrorismo, ciberespionaje e infiltraciones a los sistemas informáticos son instrumentos de agresión”. Proponiendo el desarrollo de la industria de la defensa con miras a proveer productos y servicios estratégicos especializados para aportar las capacidades de la ciberdefensa (Política de Defensa Nacional, 2018).

El Plan Específico de Defensa Nacional 2019-2030, “reconoce al ciberespacio como un componente más del territorio ecuatoriano. Las implicaciones se vinculan al desarrollo de operaciones en este dominio para la defensa de la soberanía; con el fin de aportar a la ciberseguridad nacional” (Plan Específico de Defensa Nacional, 2018).

El Plan Específico de Inteligencia 2019-2030, entiende como amenaza para el Estado ecuatoriano a todo fenómeno o condición en la que uno o más actores con capacidad de fines específicos generen un daño pérdida o consecuencia negativa directa contra los ejes de protección de la seguridad integral de este, entendiendo a éstos como el ser humano y naturaleza. Con este argumento se instituye como una de las amenazas contra el estado ecuatoriano las acciones en el ciberespacio (Plan Específico de Inteligencia, 2018).

El Plan Nacional de Gobierno Electrónico 2018-2021 traza estrategias para emitir un modelo normalizado de ciberseguridad para las instituciones dependientes del gobierno central, fortalecer el equipo de respuesta ante emergencias informáticas, capacitar a los empleados y difundir los beneficios de mantener este modelo a todos los ecuatorianos (Plan Nacional de Gobierno Electrónico, 2017).

Finalmente; la Política Ecuador Digital plantea como objetivo" transformar y dirigir al país, hacia una economía basada en tecnologías digitales mediante la disminución de la brecha digital, el desarrollo de la sociedad de la información y el conocimiento, el Gobierno digital, la eficiencia de la administración pública, y la adopción digital en los sectores sociales y económicos", esta política se compone de 3 ejes:

- Ecuador conectado
- Ecuador eficiente y ciberseguro
- Ecuador innovador y competitivo.

"Cada uno incluye un conjunto de proyectos para incrementar los índices de accesibilidad a las tecnologías de la información y comunicación, el fortalecimiento de las capacidades de talento humano, la potenciación de los sectores de la economía y el impulso del emprendimiento e innovación" (Política Ecuador Digital, 2019).

Sistema de Variables

Definición Nominal

Variable dependiente: Capacidades de la Ciberdefensa

Variable independiente: Prospectiva y planificación estratégica

Definición Conceptual

Para poder establecer la definición conceptual, es necesario considerar la descripción de las variables y la unidad de análisis, cada una con su respectiva conceptualización, tal como se lo presenta en la Tabla 1.

Tabla 1

Matriz de variables

Variables	Descripción	Conceptualización
Variable Independiente:	Capacidades de la Ciberdefensa	"Es el conjunto de actividades relacionadas a la maniobra, infraestructura, recursos, adiestramiento, doctrina y organización (MIRADO) para el fortalecimiento de la ciberdefensa que la permita preservar la seguridad de mando y control de las Fuerzas Armadas". (Fernández, 2016).
Variable Dependiente:	Prospectiva y planificación estratégica	Es una herramienta gerencial que nos permite direccionar a una organización de acuerdo con su situación y al entorno cambiante, mediante el análisis y su consecuente determinación de objetivos estratégicos a ser alcanzados, a través de la ejecución de las respectivas estrategias, optimizando los recursos disponibles, para satisfacer las necesidades y deseos de la organización y de la sociedad. (Medina, 2019)
Unidad de Análisis:	Fuerza Terrestre	"Es la rama más importante de las fuerzas armadas del país tanto por ser la más numerosa y la de mayor capacidad y competencia operativa" (Wikipedia, 2022).

Nota. La matriz permite establecer una descripción y conceptualización de las variables.

Hipótesis General

Si se realiza estudios prospectivos, juntamente con una planificación estratégica de la ciberdefensa, entonces se podrá proyectar las capacidades, infraestructura y doctrina que la ciberdefensa debe seguir para enfrentarse a los nuevos restos y ciberamenazas futuras.

Hipótesis Específica

Si se establece los escenarios: tendencial, apuesta y cisne negro de la ciberdefensa, y se determinan las estrategias para el empleo de la ciberdefensa, entonces se podrá enfrentar a los riesgos y amenazas que se presenten en el ciberespacio.

Tabla 2

Operacionalización de variables

Dimensión	Conceptualización	Subdimensiones	Indicadores	Pregunta de investigación	Fuentes	Instrumento
Variable dependiente: Capacidades de la Ciberdefensa	Es el conjunto de actividades relacionadas a la maniobra, infraestructura, recursos, adiestramiento, doctrina y organización (MIRADO) para el fortalecimiento de la ciberdefensa que la permita preservar la seguridad de mando y control de las Fuerzas Armadas y de la información que manejan, permitiendo una eficiente explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y	- Defensa (MIRADO) - Exploración (MIRADO) - Respuesta (MIRADO)	**Indicador** Porcentaje de fortalecimiento de las capacidades de ciberdefensa en la Fuerza Terrestre para la defensa, exploración y respuesta ante ciberataques. **Meta** Incrementar 5% anual la capacidad de la ciberdefensa en la FT. **Fórmula** **% FCC=** %Cac - % Cca	¿Cuál es el grado/nivel de capacidades de ciber-defensa que debe alcanzar la Fuerza Terrestre para enfrentar los escenarios futuros al 2033?	- Revisión de artículos en bases indexadas (Secundaria) - Tesis de maestrías ESPE (secundaria) - Expertos en conocimiento	- Encuesta - Entrevista - Observación - Grupos focales

Dimensión	Conceptualización	Subdimensiones	Indicadores	Pregunta de investigación	Fuentes	Instrumento
	el uso eficiente de los recursos (Fernández, 2016).		**FCC=** Fortalecimiento de la capacidad de Ciberdefensa **Cac =** Capacidad actual de ciberdefensa. **Cca =** Capacidad de Ciberdefensa anterior.		tecnológico (Primaria)	
Variable independiente: Prospectiva y Planificación estratégica	La prospectiva es el estudio del futuro para intentar comprenderlo y así poder influir sobre él. (Beger,2018) Por otra parte, la prospectiva admite la investigación de los futuros posibles, para examinar, comprender y originar las fuerzas que generen el cambio, designando una acción que se realiza en un tiempo al que aún no se ha llegado (Godet,2018)	- Escenarios (Apuesta, Cisne negro, tendencial, pesimista) - Misión - Visión - Valores - Objetivos - Estrategias	**Indicador** # estrategias levantadas y aplicadas en función de los escenarios prospectivos determinados para el fortalecimiento de las capacidades de la ciberdefensa en la FT. **Meta** Actualizar anualmente las estrategias levantadas para el	¿Cuál son los escenarios prospectivos al 2033 que enfrentará la FT en el quinto dominio de la guerra? ¿Cuáles son las estrategias que debe aplicar la Fuerza Terrestre para	- Revisión de artículos en bases indexadas (Secundaria). - Tesis de maestrías ESPE (secundaria)	- Encuesta - Entrevista - Observación - Grupos focales

Dimensión	Conceptualización	Subdimensiones	Indicadores	Pregunta de investigación	Fuentes	Instrumento
	Es una herramienta gerencial que nos permite direccionar a una organización de acuerdo con su situación y al entorno cambiante, mediante el análisis y su consecuente determinación de objetivos estratégicos a ser alcanzados, a través de la ejecución de las respectivas estrategias, optimizando los recursos disponibles, para satisfacer las necesidades y deseos de la organización y de la sociedad. (Medina, 2019).		fortalecimiento de las capacidades de la ciberdefensa en la FT. **Fórmula** #ECA= #Eci - #Ecv **ECA =** Estrategias de ciberdefensa actualizadas **Eci =** Estrategias de Ciberdefensa incrementadas. **Ecv =** Estrategias de ciberdefensa vigentes.	fortalecer las capacidades de la ciberdefensa para hacer frente a las ciberamenazas en los escenarios prospectivos determinados?	- Personal de la CGE (Primaria) - Expertos en el conocimiento tecnológico (Primaria)	

Capítulo III

Marco Metodológico

Modalidad de Investigación

Según Hernández et al. (2010):

> “Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de las personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretende medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refiere, esto es, su objetivo no es indicar cómo se relacionan estas” (p. 20).

Sobre la base de lo expuesto, el presente estudio se lo realizará mediante una investigación de tipo aplicada descriptiva ya que, a través de conversatorios con expertos en ciberdefensa, se buscará determinar la relación que existe entre la variable dependiente capacidades de ciberdefensa y la variable independiente determinada por la prospectiva y planificación estratégica, las cuales se podrán analizar y cuantificar para determinar su vinculación. Además, se podrá también determinar las propiedades, características y rasgos importantes sobre las vulnerabilidades a los ataques cibernéticos, a fin de someternos a un análisis y obtener resultados para generar respuestas a los objetivos planteados en la investigación.

Tipo de Investigación

Para el desarrollo de la presente investigación se empleará algunos tipos investigación, se iniciará con la aplicación de la investigación exploratoria, esto considerando que para Hernández et al. (2010):

> “Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tiene muchas dudas o no se ha elaborado antes, valen para revelar o suponer, los estudios descriptivos son útiles

> para mostrar con precisión los ángulos o dimensiones de un fenómeno o suceso comunidad contexto o situación" (p.80).

También se aplicará una investigación correlacional, toda vez que busca determinar la relación existente entre la variable capacidades de ciberdefensa con la variable prospectiva y planificación estratégica, esto fundamentado en lo que manifiesta Cortés & Iglesias (2004) "los estudios correlacionales tienen como propósito evaluar la relación que existe entre dos o más conceptos, categorías o variables" (p. 21).

Diseño de la Investigación

Según Hernández y Mendoza (2008):

> "Los métodos mixtos representan un conjunto de procesos sistemáticos y empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta para realizar inferencias producto de toda la información recabada y lograr un mejor entendimiento del fenómeno bajo estudio" (p. 546).

Bajo este indicio, el estudio de investigación se puede desarrollar mediante una mixtura cuantitativa y cualitativa, es decir un enfoque mixto. En el caso de la presente investigación, debido a que se ha planteado el uso de varios instrumentos de prospectiva para responder el planteamiento del problema.

Población y Muestra

Población

Según López (2014) "la población o universo es el conjunto de personas u objetivos con características en común y que se pretenden conocer en una investigación" (p. 45). Es decir, contiene a todos los elementos de la variable o variables en estudio. En este contexto, en el presente estudio se ha considerado como unidad de análisis la ciberdefensa en la Fuerza Terrestre, capacidad militar que aún no se ha terminado de desarrollar en la institución, sin embargo; el estudio tomará la recomendación de los expertos en ciberseguridad, por medio de esta capacidad el ejército ecuatoriano ha adoptado políticas

de seguridad gubernamentales promovidas por el Ministerio de Telecomunicaciones, ente que gobierna la seguridad informática de las instituciones del Estado, y por medio de auditorías esta área ya alcanzado un desarrollo de madurez medio en las unidades militares.

Muestra

Los autores del libro “Generalidades sobre la metodología de la investigación” (Cortés Cortés & Iglesias León , 2004), definen a la muestra como cualquier subconjunto de la población que se puede calcular para estudiar las peculiaridades de la totalidad de la población, partiendo de una parte de la población. “De la muestra es de la que se obtiene la información para el desarrollo del estudio y sobre la cual se efectuarán la medición y la observación de las variables de la investigación a realizarse”. En este contexto en la presente investigación se ha considerado realizar un análisis profundo a través de los sujetos especialistas que nos permitan entender el fenómeno del estudio para dar contestación a las preguntas de la investigación planteadas en el capítulo anterior.

Para conocer los factores de cambio que afectan al sistema en cuestión y de acuerdo con el tipo de investigación escogida, se va a requerir seleccionar a especialistas de la Fuerza Terrestre que actualmente gestionan la ciberseguridad de la institución a través de la matriz Delphi, los expertos en cuestión laboran en la Dirección de Tecnologías de la Información y Comunicaciones (DTIC) y son quienes conocen a profundidad sobre esta capacidad militar, ellos están constituidos por el director, jefe departamental y analistas de seguridad. Además; se ha considerado que la muestra debe regirse a un número reducido de especialistas o expertos, para intentar llegar a la saturación de categorías, basados en la autora del libro Essentials of Qualitative Inquiry (Mayan, 2016) la cual señala que quizá la saturación es inalcanzable, pero que está en el investigador “llegar hasta el momento en el que considere que puede decir algo importante y novedoso sobre el fenómeno que lo ocupa”.

Técnicas de Recolección de Datos

Fuentes de Información Primarias

Observación de Campo Directo. Es el recurso principal de la observación descriptiva; se realiza en los lugares donde ocurren los hechos o fenómenos investigados (Pita y Pértegas, 2002). Esto permitirá acudir al lugar del evento y observar cómo se desarrollan los acontecimientos durante un tiempo determinado permitiendo describir el fenómeno tal cual como sucede en la realidad, en este sentido en la investigación se empleará la observación de campo directa en la (DTIC) de la Comandancia General del Ejército.

Estudio Causal Comparativo. Esta técnica permite conocer la relación causa-efecto por el tiempo en el que ocurren. Se clasifican en estudios retrospectivos y prospectivos. La investigación retrospectiva es cuando el investigador hace el análisis de un problema luego que suceden los efectos, en cambio, la prospectiva se realiza antes de que los hechos ocurran (Tesis y másters, 2018). En ese sentido esta herramienta se constituye fundamental para el desarrollo de la investigación debido a que nos ofrece toda la información útil en relación con la naturaleza del fenómeno, permitiendo recolectar información confiable y precisa para el análisis de los resultados finales.

Fuentes de Información Secundaria

Desde el inicio de esta investigación las fuentes bibliográficas han sido el soporte principal y fundamental para fundamentar y sustentar el conocimiento teórico científico del presente caso de estudio, considerando que esta técnica constituye el conjunto de elementos suficientemente detallados que permiten la identificación de la fuente documental, pudiendo ser libros, revistas, artículos científicos entre otros documentos de relevancia.

Instrumento

Entrevista. De acuerdo con los autores (Cortés Cortés & Iglesias León , 2004), la entrevista es un instrumento fundamental en las investigaciones sociales, pues a través de

ella se puede recoger información de muy diversos ámbitos relacionados con un problema que se investiga, la persona entrevistada, su familia, y el ambiente en que se halla inmersa. En nuestra investigación, por medio de este instrumento identificaremos los factores de cambio tanto internos como externos.

Discusión Grupal. "Técnica de investigación que consiste en reunir a un grupo de personas y suscitar entre ellas una conversación sobre el tema que deseamos investigar, la cual debe estar dirigida en nuestro caso por uno de los integrantes de del equipo de trabajo, con vistas a tomar notas y no dejar escapar ningún detalle útil para el desarrollo de este" (Cortés Cortés & Iglesias León , 2004). Mediante este instrumento, buscaremos construir los escenarios mediante la interacción de los actores para más adelante determinar las estrategias a alcanzar en cada uno de los escenarios.

Validez y Confiabilidad

Debido a la peculiaridad del tema, en esta investigación se empleará el criterio y experiencia del personal de expertos en ciberdefensa escogidos por los investigadores.

Técnicas de Comprobación de Hipótesis

Una vez obtenidos los datos a través de los distintos instrumentos señalados anteriormente, se utilizará el método prospectivo de grupo a través del ábaco de Regnier, el análisis de juego de actores field anomaly relaxation (FAR) combinado con el método Delphi, por medio de los cuales se pretende estructurar las opiniones de los expertos en distintos campos de interés de la ciberdefensa. El grupo de expertos seleccionados emitirán su criterio sobre el campo de la ciberdefensa y su proyección en la Fuerza Terrestre al 2033, y a través de sucesivas reuniones anónimas, llegar a un consenso autónomo entre los participantes.

Para el tratamiento de los datos cualitativos se empleará el estudio descriptivo, basados en las herramientas prospectivas de análisis PESTM con el cual se definirá los factores de cambio externos y mediante el árbol de Giget se definirán los factores de cambio internos.

Capítulo IV

Análisis de Resultados

Problemática

Este término se refiere a aquello que genera problemas o acarrea inconvenientes, es decir se refiere al conjunto de las complicaciones que forman parte de un cierto asunto, este concepto permite englobar los desafíos, los conflictos y las dificultades de algo; la problemática de un tema es el conjunto de asuntos o cuestiones que se debe solucionar o aclarar y que conllevan contradicciones o conflictos entre lo que es y lo que debe ser, debe considerarse que la problemática se encuentra llena de inconvenientes para la consecución de un fin. (Clavijo, 2004)

Entendida como los hechos o circunstancias que obstaculizan la consecución de un fin (Villacis, 2022), se dice también que es el conjunto de problemas en torno a una situación, actividad, problema u organización, el análisis de la problemática permitirá definir e identificar el problema a ser estudiado y tratado, es así que para el caso de la Fuerza Terrestre se ha considerado determinar los diversos factores y a la vez problemas que hoy afectan al quinto dominio de la guerra, entre los cuales se pueden mencionar los siguientes:

a. Falta de presupuesto para renovación de equipos (compra de equipo tecnológico).
b. Falta de presupuesto para la modernización de aplicativos.
c. Falta de presupuesto para el mantenimiento de los equipos disponibles.
d. Falta de capacitación del personal técnico de ciberdefensa.
e. Obsolescencia del equipo tecnológico (Computadores, laptop, impresoras, servidores, etc.) por haber cumplido el tiempo límite de vida útil.
f. Falta de un horizonte a mediano plazo, que permita proyectar la ciberdefensa en la Fuerza Terrestre.
g. Falta de equipamiento y material técnico para el mantenimiento de la infraestructura tecnológica.

h. Incapacidad técnica para la modernización permanente de los aplicativos y sistemas de ciberdefensa.
i. Falta de personal, material y equipo tecnológico para el cumplimiento de misiones de defensa de la infraestructura digital de la Fuerza Terrestre.
j. Falta de personal, material y equipo tecnológico para el cumplimiento de misiones de exploración del ciberespacio para identificar ciberamenazas que atenten contra la infraestructura crítica de la Fuerza Terrestre.
k. Falta de personal, material y equipo tecnológico para el cumplimiento de misiones de respuesta contra ciberamenazas que atenten contra la infraestructura crítica de la Fuerza Terrestre o la ejecución de sus operaciones en el ámbito externo e interno.
l. Falta de marco normativo en temas de ciberdefensa.
m. Falta de cultura de ciberseguridad en el personal de la Fuerza terrestre.
n. Falta de cooperación internacional en temas de ciberdefensa

Problema

El problema se manifiesta como cualquier situación o estado de dificultad, carencia, desequilibrio, conflicto, desconocimiento, disfuncionalidad, necesidad, expectativa o interés personal, que se presente o conciba en cualquier actividad humana, la sociedad misma y el conocimiento, la cual se descubre con preguntas, se crea con ideas, se trata y resuelve con procedimientos metodológicos, actuaciones profesionales, y cuyos resultados o soluciones se exponen con argumentos especializados que se validan y acreditan públicamente a través de medios diversos de comunicación y difusión. (Moreno Doris, 1994)

En el Ecuador, se pudo evidenciar la vulnerabilidad de la defensa del ciberespacio, cuando en abril de 2019 se enfrentó al mayor ataque cibernético de su historia, una vez que se tomó la decisión de retirar el asilo diplomático a Julián Assange, fundador de WikiLeaks". De acuerdo con el MINTEL, en pocos días se registraron millones de ataques a diferentes instituciones públicas y privadas, lo que puso en evidencia la vulnerabilidad del país a este

tipo de ataques (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

Con estos antecedentes, el Ministerio de Defensa Nacional en el año 2021, a través de la Estrategia de Ciberdefensa, dispone la creación de una estructura organizacional de ciberdefensa en cada una de las ramas de Fuerzas Armadas, esta decisión le permitirá al Ecuador, disponer de un sistema integrado de ciberdefensa con las capacidades necesarias para neutralizar las ciberamenazas y apoyar a la ejecución de operaciones militares convencionales en los ámbitos terrestre, naval y aéreo.

Para el diccionario militar, una capacidad es un conjunto de elementos como: infraestructura, talento humano, logística donde se contienen los sistemas de armas, con los cuales se pretenden conseguir un objetivo estratégico, operacional o táctico dentro de las misiones fijadas por el Escalón Superior (Comando de Educación y Doctrina Militar Terrestre, 2010).

La planificación estratégica nos permitirá, tener una consciencia situacional de lo que ocurre en el quinto dominio de la guerra, ya que esta incluye; el desarrollo de capacidades para detectar y analizar la naturaleza de las ciberamenazas, desarrollar la doctrina de ciberdefensa, formación de cibersoldados y por último los procedimientos organizativos y tecnológicos que deberán ser considerados por la Fuerza Terrestre para la implementación del Grupo de Ciberdefensa (GRUCIBER).

Basados en lo expuesto anteriormente, para el desarrollo de esta investigación nos hemos trazado la siguiente interrogante fundamental:

¿Qué estrategias se deben plantear en el presente para construir el mejor escenario futuro de la ciberdefensa en la Fuerza Terrestre?

Tema

Por lo tanto, una vez planteada la problemática y el problema, se puede determinar el tema de estudio a ser analizado:

“La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033”.

Fase 1 (Construir la Base)

Análisis del Macroambiente PESTM

Político

Son aspectos gubernamentales que inciden directamente en la dirección y organización de la ciberdefensa en la Fuerza Terrestre, tales como las políticas impositivas, regulaciones, convenios internacionales que afectan al desarrollo y fortalecimiento de la ciberdefensa en esta institución, entre los cuales se establecieron los siguientes:

- Actores políticos sin interés, ni comprensión en temas de ciberseguridad y ciberdefensa.
- Hipótesis de conflicto interno por poder y amenazas híbridas.
- Limitada gestión del organismo político responsable de la seguridad y defensa del Estado
- Desconocimiento político del impacto de las ciberamenazas.
- Desconocimiento político del rol que debe cumplir el Ejército en la seguridad del ciberespacio del Estado.

Económico

Se refiere al acceso a los recursos de todo tipo, y a la disponibilidad presupuestaria que inciden en el cumplimiento de las misiones que debe cumplir el ejército en el ciberespacio:

- Políticas económicas de austeridad reducen la asignación presupuestaria.
- Insuficiente presupuesto de inversión del Estado en defensa.
- No existe presupuesto para capacitación de personal técnico en ciberdefensa.
- No se cumple los planes de mantenimiento del equipo tecnológico.
- No existe presupuesto para adquisición de licencias para programas y herramientas tecnológicas.

Social

Aquí se considera las tendencias sociales, las formas o estilo de vida de la sociedad ecuatoriana, entre los cuales se determinaron los siguientes:

- Demanda regular de apoyo en temas de ciberseguridad a la sociedad civil.
- Ataques de la protesta social al ejército mediante el ciberespacio.
- Corrupción social impide ejecución de procesos de adquisición de equipos tecnológicos para ciberdefensa.
- Apoyo a las instituciones del Estado en tema de ciberseguridad y ciberdefensa minimizado por falta de equipamiento tecnológico.
- Limitado apoyo para el fortalecimiento de la cultura de ciberseguridad y ciberdefensa en la población.

Tecnológico

Son los aspectos técnico – científicos que han innovado todos los sistemas debido a su constante cambio y evolución; en este sentido se han identificado los siguientes:

- Equipos y medios tecnológicos con bajo índice de vida útil.
- Necesidad de actualizaciones permanentes en los sistemas y programas tecnológicos.
- Brecha tecnológica del conocimiento de ciberdefensa en cortos períodos de tiempo.
- Falta de Infraestructura tecnológica para la gestión de la ciberdefensa en la FT.
- Dependencia de la tecnología para todos los procesos. Administrativos y operativos que realiza la FT.

Militar

Tiene que ver específicamente con las actividades que realiza el ejército para la protección del ciberespacio, siendo estas las siguientes:

- Alta rotación del personal militar técnico.
- Vulnerabilidad de la información sensible de la FT.
- Limitada capacidad para enfrentar ciberamenazas a nivel de seguridad del Estado.

- Falta de capacitación y entrenamiento en ciberdefensa limita el óptimo empleo de los medios para la protección del ciberespacio.
- Baja capacidad desarrollada por el Grupo de Ciberdefensa (GRUCIBER) para ejecutar operaciones de protección, explotación y respuesta en el ciberespacio.
- Incremento de ciberespionaje y ciberataques a la infraestructura de la FT.

Una vez realizado el análisis del macroambiente, a continuación, se procede a elaborar la matriz PESTM del presente, pasado y futuro, esto con el fin de poder identificar los factores de cambio, lo que a su vez permitirá realizar el levantamiento de las variables estratégicas, tal como se encuentra detallado a continuación en la Tabla 3 Matriz PESTM (presente-pasado-futuro):

Tabla 3

Matriz PESTM – aspecto político

Pasado 1998	Presente 2023	Futuro 2033	Factor de cambio
Actores Políticos con interés y comprensión en temas de seguridad y defensa.	Actores Políticos sin interés, ni comprensión en temas de ciberseguridad y ciberdefensa.	Actores Políticos interesados, y con comprensión en temas de ciberseguridad y ciberdefensa.	Número de Actores Políticos comprometidos con aspectos de ciberseguridad y ciberdefensa.
Hipótesis de conflicto interestatal Ecuador Perú.	Hipótesis de conflicto interno por poder y amenazas híbridas.	Hipótesis de conflicto interno y externo por ciberamenazas.	Desarrollo de conflictos en el ciberespacio.
Moderada gestión del organismo político responsable de la seguridad y defensa del Estado.	Limitada gestión del organismo político responsable de la seguridad y defensa del Estado.	Alta gestión del organismo político responsable de la seguridad y defensa del Estado en temas de ciberdefensa.	Gestión política en temas de ciberdefensa.
Interés político ante la diversificación de amenazas internas y externas.	Desconocimiento político del impacto de las ciberamenazas en el Estado.	Adoctrinamiento del nivel político sobre ciberamenazas, y sus acciones, actores, roles e impacto ante el Estado	Accionar político ante ciberamenazas contra el Estado.
Visión política amplia sobre el empleo de Ejército en conflictos externos.	Desconocimiento político del rol del Ejército en la seguridad del Ciberespacio.	Conocimiento político del rol del Ejército en la seguridad del Ciberespacio.	Conocimiento del nivel político de la defensa del ciberespacio.

Tabla 4

Matriz PESTM – aspecto económico

Pasado 1998	Presente 2023	Futuro 2033	Factor de cambio
Políticas económicas institucionales asignan el presupuesto planificado por el Ejército.	Políticas económicas de austeridad reducen la asignación presupuestaria para el Ejército.	Emisión de políticas de optimización y racionalización de recursos para el Ejército.	Políticas para optimización y racionalización de recursos.
Moderado presupuesto de inversión del Estado en defensa.	Insuficiente presupuesto de inversión del Estado en ciberdefensa.	Suficiente presupuesto de inversión del Estado en ciberdefensa.	Asignación presupuestaria para disponer de un Grupo de ciberdefensa con capacidades de defensa exploración y respuesta.
Presupuesto para capacitación de personal técnico.	No existe presupuesto para capacitación de personal técnico en ciberdefensa.	Presupuesto para capacitación y certificación personal técnico en ciberdefensa.	Presupuesto para capacitación y certificación personal técnico en ciberdefensa.
Cumplimiento parcial de planes de mantenimiento de equipo tecnológico. .	No se cumple los planes de mantenimiento del equipo tecnológico de ciberdefensa.	Cumplimiento total de planes de mantenimiento del equipo tecnológico de ciberdefensa.	Presupuesto para la ejecución de planes de mantenimiento del equipo tecnológico de ciberdefensa.
Presupuesto disponible para adquisición parcial de licencias para programas y herramientas tecnológicas.	No existe presupuesto para adquisición de licencias para programas y herramientas tecnológicas de ciberdefensa.	Asignación presupuestaria para la adquisición de licencias para programas y herramientas tecnológicas de ciberdefensa.	Presupuesto para adquirir licencias para programas y herramientas tecnológicas de ciberdefensa.

Tabla 5

Matriz PESTM – aspecto social

Pasado 1998	Presente 2023	Futuro 2033	Factor de cambio
Poca demanda de apoyo tecnológico a la sociedad civil.	Demanda regular de apoyo en ciberseguridad a la sociedad civil.	Alta demanda de apoyo en ciberseguridad a la sociedad civil.	Capacidad de ciberseguridad para atender la demanda de la sociedad civil.
Existen ataques de la protesta social al ejército de forma física	Ataques moderados de la protesta social al ejército mediante el ciberespacio.	Ataques permanentes de la protesta social al ejército mediante el ciberespacio.	Incremento de capacidades de ciberdefensa para contrarrestar los ataques cibernéticos generados por la protesta social.
Compra de tecnología para sistemas informáticos.	Corrupción social impide ejecución de procesos de compra de equipos tecnológicos de ciberdefensa	Procesos de compra de equipos de ciberdefensa con estándares de anticorrupción.	Políticas estatales que permitan transparentar todos los procesos de compras.
Baja demanda de apoyo tecnológico a las instituciones del Estado	Mediana demanda de apoyo en ciberseguridad y ciberdefensa a las instituciones del Estado	Alta demanda de apoyo en ciberseguridad y ciberdefensa a las instituciones del Estado	Incremento de capacidad de ciberseguridad y ciberdefensa para atender la demanda de las Instituciones del Estado.
Poco demanda de apoyo al fortalecimiento de la cultura informática en la población.	Demanda moderada de apoyo para el fortalecimiento de la cultura de ciberseguridad y ciberdefensa en la población.	Alta demanda de apoyo para el fortalecimiento de la cultura de ciberseguridad y ciberdefensa en la población.	Incrementos de capacitación en ciberseguridad y ciberdefensa en el personal de la FT, para replicar en la sociedad.

Tabla 6

Matriz PESTM – aspecto tecnológico

Pasado 1998	Presente 2023	Futuro 2033	Factor de cambio
Equipos y medios de ciberdefensa con obsolescencia tecnológica en largos períodos de tiempo.	Equipos y medios de ciberdefensa con obsolescencia tecnológica en medianos períodos de tiempo.	Equipos y medios de ciberdefensa con obsolescencia tecnológica en cortos períodos de tiempo.	Desarrollo acelerado de la tecnología en ciberdefensa
Necesidad de actualizaciones permanentes en los sistemas y programas informáticos.	Necesidad de actualizaciones permanentes en los sistemas de ciberdefensa.	Necesidad de actualizaciones inmediatas en los sistemas de ciberdefensa	Sistemas de actualización on-line, virtuales o mediante red de datos
Actualización del conocimiento de ciberdefensa en largos períodos de tiempo.	Actualización del conocimiento de ciberdefensa en medianos períodos de tiempo.	Actualización del conocimiento del conocimiento de ciberdefensa en cortos períodos de tiempo.	Mejoramiento tecnológico en la capacitación en ciberdefensa.
Falta de infraestructura tecnológica para la gestión de seguridad informática en la FT.	Falta de infraestructura tecnológica para la gestión de la ciberdefensa en la FT.	Infraestructura tecnológica para la gestión de la ciberdefensa en la FT.	Mejoramiento de la Infraestructura tecnológica para la gestión de la ciberdefensa en la FT.
Dependencia relativa a la tecnología en los procesos administrativos y operativos que realiza la FT.	Dependencia permanente a la tecnología en los procesos administrativos y operativos que realiza la FT.	Total, dependencia a la tecnología en los procesos. administrativos y operativos que realiza la FT.	Incremento de la dependencia de la FT a la tecnología

Tabla 7

Matriz PESTM – aspecto militar

Pasado 1998	Presente 2023	Futuro 2033	Factor de cambio
Vulnerabilidad de la información de la FT.	Alta vulnerabilidad de la información sensible de la FT.	Vulnerabilidad de la información sensible de la FT. controlada.	Protocolos de protección de la información digital.
Poca capacidad para proteger la información a nivel de seguridad del Estado.	Limitada capacidad para enfrentar ciberamenazas a nivel de seguridad del Estado.	Suficiente capacidad para enfrentar ciberamenazas a nivel de seguridad del Estado.	Capacidad de ciberdefensa a nivel de seguridad del Estado.
Falta de capacitación en seguridad informática para las operaciones militares.	Falta de capacitación y entrenamiento en ciberdefensa para el empleo en operaciones militares.	Capacitación y entrenamiento moderado en ciberdefensa para el empleo en operaciones militares.	Capacitación y entrenamiento en ciberdefensa.
Ninguna capacidad para ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio.	Baja capacidad desarrollada por el GRUCIBER para ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio.	Capacidad desarrollada por el GRUCIBER moderada para ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio.	Capacidad moderada desarrollada por el GRUCIBER para ejecutar operaciones en el ciberespacio
Ninguna capacidad contra espionaje y ataques informáticos a la infraestructura de la FT.	Poca capacidad contra ciberespionaje y ciberataques a la infraestructura de la FT.	Moderada capacidad contra ciberespionaje y ciberataques a la infraestructura de la FT.	Capacidad contra ciberespionaje y ciberataques a la infraestructura de la FT

Análisis del Microambiente

Árbol de Giget.

El árbol de competencia pretende representar a una institución en su totalidad sin reducirla únicamente a sus productos y servicios. En este árbol, las raíces (las competencias técnicas y el saber-hacer) y el tronco (capacidad de producción de servicios) son tan importantes como las ramas (líneas de productos y servicios) (Godet M. , 2007).

Conocido también como el árbol de competencias de Giget ha sido definido por algunos entendidos como la visión integral en un determinado período de tiempo que ayuda a determinar las oportunidades y las debilidades de las diferentes áreas con relación directa a los autores, el entorno y sobre todo la estrategia a ser empleada (Giget, 1998).

Antecedentes

Fue una técnica utilizada por los japoneses para poder determinar una reflexión estratégica para evaluar las condiciones tecnológicas e industriales de una organización, la cual a partir del año de 1980 fue formalizada por Marc Giget.

Objetivo

En el marco de la metodología integrada, el objetivo del árbol es establecer una radiografía de la organización a fin de tener en cuenta, sus competencias distintivas y su dinámica, en la elaboración de las opciones estratégicas.

Metodología

Consiste en dar una visión sistemática diagnosticando el presente, pasado y futuro de una organización, fundamentado en una reflexión colectiva o por un grupo de expertos.

Para lo cual se debe tomar muy en cuenta todos los ámbitos económicos, sociales, tecnológicos políticos entre otros, de una organización durante cierto período (Monti, 1996).

Estructura

Raíces. Esta materializado por el saber hacer que constituya una competencia, las cuales pueden ser genéricas de la organización, siendo lo más importante la determinación de las fortalezas y debilidades.

Tronco. Materializado por las capacidades que no es otra cosa que la integración de las competencias mediante el respectivo análisis de las dificultades y facilidades registradas en la organización.

Ramas u Hojas. Materializado por los resultados que pretende obtener la organización.

Tabla 8

Árbol de Giget o de competencias

Componentes	Pasado 1998	Presente 2023	Futuro 2033	Factor de Cambio
Productos y servicios	Apoyo a la seguridad de la información digital de la FT.	Ejecución de operaciones de ciberseguridad para la protección de la infraestructura de la FT.	Operaciones de ciberdefensa en apoyo a las operaciones de defensa del territorio nacional y ámbito interno desarrolladas por la FT.	Cambio de teatros de operaciones para el empleo (externo e interno)
	Equipos y sistemas con tecnología analógica	Equipos y herramientas de ciberseguridad con capacidades básicas para su empleo.	Equipos y herramientas de ciberdefensa con capacidades tecnológicas modernas para el empleo.	Herramientas de ciberdefensa de última generación
Capacidades	Unidades de comunicaciones en todos los niveles de la FT.	Grupo de Ciberdefensa de la FT.	Grupo de Ciberdefensa de la FT. y unidades menores de ciberdefensa en las divisiones y brigadas de la FT.	Unidades de ciberdefensa en los niveles de la FT para cumplir misiones en el ciberespacio.
	Personal de comunicaciones capacitado para proteger la información digital de la FT.	Personal especialista capacitado para operaciones de defensa.	Personal especialista capacitado para operaciones de defensa, exploración y respuesta.	Personal de comunicaciones capacitado en operaciones de ciberdefensa.

Componentes	Pasado 1998	Presente 2023	Futuro 2033	Factor de Cambio
	Capacidades propias para el mantenimiento de los equipos informáticos de la FT.	Capacidades propias de mantenimiento preventivo de los equipos y herramientas de ciberdefensa.	Capacidades propias de mantenimiento correctivo de los equipos y herramientas de ciberdefensa.	Mantenimiento con transferencia tecnológica, certificados por organismos internacionales.
Conocimientos / recursos	Conocimientos para configurar equipos informáticos.	Conocimientos para ejecutar operaciones de defensa y exploración en el ciberespacio.	Conocimientos para ejecutar operaciones de defensa exploración y respuesta en el ciberespacio.	Capacitación en el uso de nuevas tecnologías de ciberdefensa.
	Conocimientos en: Operaciones de seguridad informática. Actividades de certificación informática.	Conocimientos en: Operaciones del Centro de Operaciones de ciberseguridad (SOC). Actividades de empleo de sistemas de ciberdefensa con certificación nacional.	Conocimientos en: Operaciones en el Centro de Fusión Cibernético. Actividades de empleo de sistemas de ciberdefensa con certificación internacional.	- Cumplimiento de operaciones de ciberdefensa. - Certificaciones de empleo de equipos de ciberdefensa.
	Conocimiento de: Mantenimiento nivel I (Básico)	Conocimiento de: Desarrollo e implementación de políticas de ciberseguridad (EGSI) en la FT.	Conocimiento de: Desarrollo e implementación de políticas de ciberdefensa con estándares internacionales en la FT.	Certificaciones tecnológicas de ciberseguridad y ciberdefensa.

Fase 2 (Variables Estratégicas)

Ábaco de Régnier

Una vez desarrollado el análisis PESTM y el árbol de Giget, se establece las variables que permitirán continuar con el estudio prospectivo. Definiéndose a una variable como un factor que cambia, que tiene atributos o características y que permite definir un problema de investigación.

Lista de Variables

- Actores políticos comprometidos con la ciberdefensa.
- Conflictos en el ciberespacio.
- Gestión política en ciberdefensa.
- Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.
- Conocimiento del nivel político de la defensa del ciberespacio.
- Políticas de optimización de recursos.
- Presupuesto para un grupo de ciberdefensa con capacidades.
- Presupuesto para capacitación en ciberdefensa.
- Presupuesto para mantenimiento de equipo de ciberdefensa.
- Presupuesto para licencias, programas y herramientas tecnológicas.
- Capacidad de ciberseguridad para atender demanda de la sociedad civil.
- Doctrina de operaciones en el ciberespacio
- Políticas estatales para transparentar procesos de compras.
- Capacidades de ciberseguridad y ciberdefensa para apoyar a instituciones del Estado.
- Desarrollar una cultura de ciberseguridad en la institución.
- Desarrollo tecnológico de ciberdefensa mundial acelerado.
- Actualización de ciberdefensa on-line, virtuales o mediante red de datos.

- Mejoramiento tecnológico de capacitación en ciberdefensa.
- Mejoramiento de infraestructura tecnológica para ciberdefensa.
- Incremento de la dependencia de la FT. a la tecnología.
- Cumplimiento de protocolos de protección de información digital.
- Capacidad de ciberdefensa a nivel de seguridad del Estado.
- Entrenamiento en operaciones de ciberdefensa.
- Capacidad del GRUCIBER para ejecutar operaciones de ciberdefensa.
- Marco regulatorio en el ciberespacio.
- Capacidad contra ciberespionaje y ciberataques.
- Equipamiento militar con tecnología de punta para ciberdefensa.
- Cambio de teatros de operaciones para el empleo de ciberdefensa.
- Equipos de ciberdefensa de última generación
- Todos los niveles de la FT con unidades militares de ciberdefensa.
- Recurso humano capacitado en operaciones de ciberdefensa.
- Mantenimiento con transferencia tecnológica, certificados por organismos internacionales.
- Capacitación en el uso de nuevas tecnologías de ciberdefensa.
- Cumplimiento de operaciones de ciberdefensa.
- Certificaciones de empleo de equipos de ciberdefensa.
- Certificaciones tecnológicas para el GRUCIBER.

Coeficiente de Competencia Experta “k”

En el artículo “Validación del diseño de una red de cooperación científico-tecnológica utilizando el coeficiente K para la selección de expertos” de la revista científica Scielo, los

autores (Marín González y otros, 2021) que el coeficiente de competencia experta se estima como referente a los elementos que inicialmente se han considerado expertos para que con su opinión y autovaloración indiquen el grado de conocimiento acerca del objeto de investigación, así como las fuentes que les permiten argumentar y justificar dicho nivel.

En la tabla 9, se presenta el cálculo del coeficiente de competencia (kc) de los expertos en ciberseguridad, que al momento se gestiona en la Dirección de Tecnologías de la Información de la Fuerza Terrestre. Basados en el método Delphi, esta información tiene origen en la autovaloración de los expertos en cuanto a su grado de conocimiento y argumentación en el tema de ciberdefensa militar, la metodología también permite calcular el coeficiente de argumentación (ka), que se obtiene de fuentes de argumentación para hallar el coeficiente k.

Tabla 9

Matriz de valoración del grado de conocimiento de expertos kc.

Valoración del grado de conocimiento	Valoración	Experto DCL	Experto DCL	Experto BAS	Experto CVV	Experto JRV	Experto GS	Experto PMS	Experto MLB	Experto PPV
No poseo ningún conocimiento del tema	0									
Tengo poco conocimiento del tema	0.3									
Tengo algún conocimiento del tema	0.6	0.6					0.6	0.6	0.6	0.6
Soy especialista en el tema y tengo bastante conocimiento del tema	0.9		0.9	0.9	0.9					
Soy especialista en el tema y tengo total conocimiento del tema	1					1				
Total		0.6	0.9	0.9	0.9	1	0.6	0.6	0.6	0.6

Nota. Elaboración propia en referencia al artículo Método Delphi - Propuesta para el cálculo del número de expertos en un estudio Delphi sobre empaques biodegradables al 2032 de la Revista Espacios (Zartha Sossa y otros, 2014)

Tabla 10

Matriz de valoración de la fuente de argumentación

Valoración de la fuente de argumentación	Grado de influencia de cada fuente		
	Alto	Medio	Bajo
Análisis teóricos realizados por el experto	0.3	0.2	0.1
Experiencia obtenida	0.5	0.4	0.2
Estudios sobre el tema	0.05	0.05	0.05
Conocimiento propio acerca del estado actual	0.05	0.05	0.05
Intuición del experto	0.05	0.05	0.05

Nota. Extraído del artículo Método Delphi – "Propuesta para el cálculo del número de expertos en un estudio Delphi sobre empaques biodegradables al 2032 de la Revista Espacios" (Zartha Sossa y otros, 2014).

Tabla 10

Matriz de coeficiente de competencia experta

Expertos	Coeficiente de conocimiento	Coeficiente de argumentación	Conocimiento de competencia experta
Henry Delgado Salvador	0,6	0,8	0,7
Diego Chiza López	0,9	0,9	0,9
Bolívar Acosta Sánchez	0,9	0,85	0,875
Christian Vizcaíno Villavicencio	0,9	0,85	0,875
José Ramos Vargas	1	0,9	0,95
Gustavo Santiago	0,9	0,95	0,925
Paúl Machado Soto	0,6	0,9	0,75
Marcelo López Báez	0,6	0,9	0,75
Pablo Paredes Valencia	0,6	0,9	0,75

Nota. Extraído del artículo "Validación del diseño de una red de cooperación científico-tecnológica utilizando el coeficiente K para la selección de expertos de la Revista Scielo". (Marín González y otros, 2021).

Priorización de Variables

Es un método que permite la revelación y representación de las opiniones de los especialistas, responsables de la elaboración, así como la percepción de los actores que interactúan cotidianamente con el entorno sobre cada una de las variables planteadas.

Las ventajas de utilizar esta herramienta en el análisis prospectivo es que permite efectuar un estudio rápido y didáctico en el tratamiento del problema en cuestión; permite la posibilidad de detectar la opinión del grupo de expertos en el tema; fomenta las ideas y opiniones a través del debate, y es una excelente herramienta de comunicación. Por otra parte, también presenta algunas desventajas como: restar protagonismo al líder del grupo y modifica el funcionamiento habitual del mismo (Godet, 2000).

Una vez establecidas las variables, se procedió a insertarlas en el ábaco de Regnier y en función del estudio realizado por cada uno de los expertos entrevistados se realizó su valoración de acuerdo con la escala determinada, dando como resultado lo que se establece en la tabla 9. Ábaco de Regnier, en esta gama de opciones planteada en esta herramienta, los colores utilizados en la leyenda se basan en los colores del semáforo (verde, amarillo y rojo), agregándose los matices intermedios entre el verde y amarillo y entre le rojo y amarillo.

Tabla 11

Ábaco de Régnier

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GS
1	Marco regulatorio en el ciberespacio.	5	4	4	5	5
2	Cumplimiento de operaciones de ciberdefensa.	5	5	5	5	5
3	Gestión política en ciberdefensa.	4	3	3	4	3
4	Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	5	4	4	5	5
5	Conocimiento del nivel político de la defensa del ciberespacio.	5	4	3	4	4
6	Presupuesto para un grupo con capacidades de ciberdefensa.	5	5	5	5	5
7	Políticas de optimización de recursos.	4	5	4	3	2
8	Presupuesto para capacitación en ciberdefensa.	4	4	5	5	3
9	Presupuesto para mantenimiento de equipo.	4	3	3	4	2
10	Presupuesto para licencias, programas y herramientas tecnológicas.	4	4	3	4	3
11	Capacidad de ciberseguridad para atender demanda de la sociedad civil.	4	4	4	4	3
12	Cambio de teatros de operaciones para el empleo de ciberdefensa	5	3	5	4	3
13	Políticas estatales para transparentar procesos de compras.	3	3	3	4	4
14	Capacidades de ciberseguridad y ciberdefensa para apoyar a instituciones del Estado.	3	3	3	2	2
15	Apoyar al desarrollo de una cultura de ciberseguridad en la sociedad.	5	5	5	5	5
16	Equipos y herramientas de ciberdefensa de última generación.	5	5	5	5	5
17	Actualización de ciberdefensa on-line, virtuales o mediante red de datos.	5	5	4	4	4

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GS
18	Mejoramiento tecnológico de capacitación en ciberdefensa.	4	3	4	4	4
19	Mejoramiento de infraestructura tecnológica para ciberdefensa.	4	2	4	3	1
20	Recurso humano capacitado en operaciones de ciberdefensa.	5	5	5	5	5
21	Cumplimiento de protocolos de protección de información digital.	5	4	4	5	4
22	Capacidad de ciberdefensa a nivel de seguridad del Estado.	4	4	4	3	2
23	Entrenamiento en operaciones de ciberdefensa.	4	4	3	4	4
24	Capacidad del GRUCIBER para ejecutar operaciones de ciberdefensa.	4	5	3	4	2
25	Capacidad contra ciberespionaje y ciberataques.	4	3	4	4	3
26	Equipamiento militar con tecnología de punta para ciberdefensa.	3	1	2	2	1
27	Doctrina de operaciones en el ciberespacio.	5	5	5	4	4
28	Desarrollo tecnológico de ciberdefensa mundial acelerado.	3	1	2	2	1
29	Incremento de la dependencia de la FT. a la tecnología.	4	4	4	4	3
30	Actores políticos comprometidos con la ciberdefensa.	4	4	4	3	2
31	Mantenimiento con transferencia tecnológica, certificados por organismos internacionales.	4	3	4	4	3
32	Capacitación en el uso de nuevas tecnologías de ciberdefensa.	5	4	4	5	5
33	Conflictos en el ciberespacio.	5	4	4	4	4
34	Certificaciones de empleo de equipos de ciberdefensa.	5	5	4	3	3
35	Certificaciones tecnológicas para el GRUCIBER.	4	4	4	2	2

Tabla 12

Ábaco de Régnier ordenado

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GSA
2	Ejecución de operaciones de ciberdefensa.	5	5	5	5	5
7	Presupuesto para un grupo con capacidades de ciberdefensa	5	5	5	5	5
15	Apoyar al desarrollo de una cultura de ciberseguridad	5	5	5	5	5
28	Equipos y herramientas de ciberdefensa de última generación	5	5	5	5	5
29	Recurso humano capacitado en operaciones de ciberdefensa.	5	5	5	5	5
30	Marco regulatorio en el ciberespacio.	5	5	5	4	4
4	Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	5	5	5	4	4
12	Doctrina de operaciones en el ciberespacio.	5	5	5	4	4
32	Capacitación en el uso de nuevas tecnologías de ciberdefensa.	5	5	5	4	4
17	Actualización de ciberdefensa on-line, virtuales o mediante red de datos.	5	5	4	4	4
21	Cumplimiento de protocolos de protección de información digital.	5	5	4	4	4
8	Presupuesto para capacitación en ciberdefensa.	5	5	4	4	3
27	Cambio de teatros de operaciones para el empleo de ciberdefensa.	5	5	4	3	3
34	Certificaciones de empleo de equipos de ciberdefensa.	5	5	4	3	3
33	Conflictos en el ciberespacio.	5	4	4	4	4
5	Conocimiento del nivel político de la defensa del ciberespacio.	5	4	4	4	3
6	Políticas de optimización de recursos.	5	4	4	3	2
24	Capacidad del GRUCIBER para ejecutar operaciones de ciberdefensa.	5	4	4	3	2
11	Capacidad de ciberseguridad para atender demanda de la sociedad civil.	4	4	4	4	3
18	Mejoramiento tecnológico de capacitación en ciberdefensa.	4	4	4	4	3

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GSA
20	Incremento de la dependencia de la FT. a la tecnología.	4	4	4	4	3
23	Entrenamiento en operaciones de ciberdefensa.	4	4	4	4	3
10	Presupuesto para licencias, programas y herramientas tecnológicas.	4	4	4	3	3
25	Capacidad contra ciberespionaje y ciberataques.	4	4	4	3	3
31	Mantenimiento con transferencia tecnológica, certificados por organismos internacionales.	4	4	4	3	3
22	Capacidad de ciberdefensa a nivel de seguridad del Estado.	4	4	4	3	2
1	Actores políticos comprometidos con la ciberdefensa.	4	4	4	3	2
35	Certificaciones tecnológicas para el GRUCIBER.	4	4	4	2	2
3	Gestión política en ciberdefensa.	4	4	3	3	3
13	Políticas estatales para transparentar procesos de compras.	4	4	3	3	3
9	Presupuesto para mantenimiento de equipo.	4	4	3	3	2
19	Mejoramiento de infraestructura tecnológica para ciberdefensa.	4	4	3	2	1
14	Capacidades de ciberseguridad y ciberdefensa para apoyar a instituciones del Estado.	3	3	3	2	2
26	Equipamiento militar con tecnología de punta para ciberdefensa.	3	2	2	1	1
16	Desarrollo tecnológico de ciberdefensa mundial acelerado.	3	2	2	1	1

LEYENDA	
Muy Probable	5
Probable	4
Duda	3
Improbable	2
Muy Improbable	1

Para la priorización de las variables con el ábaco de Régnier, se realizó el procesamiento de los datos insertados, a fin de definir las más importantes en base a los colores de la leyenda, dando como resultado las variables que más adhesiones han tenido a los expertos; este proceso permitió determinar la jerarquización de las variables y plantear 08 variables estratégicas según la tabla 12. Priorización de las variables.

El resultado generado a partir de esta priorización permite establecer algunas conclusiones; en primer lugar se puede definir las variables que son dominadas por las tonalidades verdes como las principales variables o las que tienen el consenso de los expertos con una aprobación mayoritaria; en las posiciones subsiguientes se ubican las variables que tienen una marcada tonalidad verde con verde claro, amarillos, y al final se ubican las variables que tienen poca tonalidad verde y aparecen las tonalidades amarilla y roja, indicando una zona de alto riesgo y restricciones en las variables.

Tabla 13

Priorización de Variables

Nro.	LISTA DE VARIABLES	Exp. 1 DCL	Exp. 2 BAS	Exp. 3 CVV	Exp. 4 JRV	Exp. 5 GSA
1	Ejecución de operaciones de ciberdefensa.	5	5	5	5	5
2	Presupuesto para un grupo de ciberdefensa con capacidades.	5	5	5	5	5
3	Apoyar al desarrollo de una cultura de ciberseguridad	5	5	5	5	5
4	Equipos y herramientas de ciberdefensa de última generación	5	5	5	5	5
5	Recurso humano capacitado en operaciones de ciberdefensa.	5	5	5	5	5
6	Marco regulatorio en el ciberespacio.	5	5	5	4	4
7	Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	5	5	5	4	4
8	Doctrina de operaciones en el ciberespacio.	5	5	5	4	4

Fase 3 (Construcción de Escenarios)

Matriz Morfológica

La matriz morfológica es una matriz de doble entrada, dada por las variables estratégicas (fila), por la hipótesis o posible evolución de cada variable a futuro (columnas). El análisis morfológico permite organizar las ideas para una respuesta estratégica que sea relevante y consistente, por ende, es utilizada para sistematizar la información a la vez que genera una serie de combinaciones de posibles respuestas a problemas complejos (Godet M. , 2007).

Por otra parte, el análisis morfológico se presta muy bien a la construcción de escenarios para el análisis de la prospectiva. Un sistema global puede ser descompuesto en cuestiones o variables demográficas, económicas, técnicas, sociales u organizativas. Para cada una de esas variables o cuestiones claves para el futuro se pueden identificar un cierto número de hipótesis o de respuestas posibles para el futuro (Reyes, 2010).

Las hipótesis en este estudio son cinco, las cuales originan sus respectivas escenas futuras: optimista, pesimista, tendencial, cisne negro y apuesta. Además, es necesario conocer que todos los escenarios deben cumplir con condiciones de: pertinencia, coherencia, verosimilitud, importancia y transparencia, por lo que una sencilla integración de hipótesis sin sentido no configura un escenario (Godet y Durance, 2011).

Tabla 14

Matriz Morfológica

Variables Estratégicas	Estados o hipótesis del futuro				
	Hipótesis optimista "Americano"	**Hipótesis pesimista "Brasileño"**	**Hipótesis tendencial "Ecuatoriano"**	**Hipótesis Cisne negro "Venezolano"**	**Hipótesis apuesta "Español"**
Ejecución de operaciones de ciberdefensa.	Permanente	Mínima	Parcial	Inexistente	Continua
Presupuesto para un grupo de con capacidades de ciberdefensa.	Elevado	Insuficiente	Reducido	Nulo	Suficiente
Apoyar al desarrollo de una cultura de ciberseguridad.	Estable	Mínimo	Parcial	Irreal	Continuo
Equipos de ciberdefensa de la FT de última generación	Elevado	Reducido	Bajo	Insubsistente	Alto
Recurso humano capacitado en operaciones de ciberdefensa.	Permanente	Mínimo	Parcial	Inexistente	Equilibrado
Marco regulatorio en el ciberespacio.	Excelente	Pésimo	Improcedente	Nulo	Moderado

Variables estratégicas	Estados o hipótesis del futuro				
	Hipótesis optimista "Americano"	**Hipótesis pesimista "Brasileño"**	**Hipótesis tendencial "Ecuatoriano"**	**Hipótesis Cisne negro "Venezolano"**	**Hipótesis apuesta "Español"**
Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	Permanente	Imperceptible	Limitada	Inefectiva	Continua
Doctrina de operaciones en el ciberespacio.	Elevada	Incompleta	Baja	Nula	Suficiente

Líneas de Acción

En la figura 7., se plantean las líneas de acción específicas que se identificaron como las más pertinentes para el desarrollo de la ciberdefensa en la Fuerza Terrestre en un escenario prospectivo al 2033.

Figura 7

Líneas de acción

Descripción de los Escenarios

Escenario Optimista "Americano"

El escenario optimista al 2033 se caracteriza por: tener un PERMANENTE cumplimiento de las operaciones de ciberdefensa, un ELEVADO presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un

ESTABLE apoyo de la FT al desarrollo de la cultura de ciberseguridad, un ELEVADO número de equipos y herramientas de ciberdefensa de la FT. de última generación, con un PERMANENTE recurso humano capacitado en operaciones de ciberdefensa, con un EXCELENTE marco regulatorio en el ciberespacio, con una PERMANENTE reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital y una ELEVADA doctrina de operaciones en el ciberespacio.

Escenario Pesimista "Brasileño"

El escenario pesimista al 2033 se caracteriza por: tener una MÍNIMA ejecución de las operaciones de ciberdefensa, un INSUFICIENTE presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un MÍNIMO apoyo de la FT. al desarrollo de la cultura de ciberseguridad, un REDUCIDO número de equipos de ciberdefensa de última generación, con un MÍNIMO recurso humano capacitado en operaciones de ciberdefensa, con un PÉSIMO marco regulatorio en el ciberespacio, con una IMPERCEPTIBLE reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital, una INCOMPLETA doctrina de operaciones en el ciberespacio.

Escenario Tendencial "Ecuatoriano"

El escenario Tendencial al 2033 se caracteriza por: tener una PARCIAL ejecución de las operaciones de ciberdefensa, un REDUCIDO presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un PARCIAL apoyo de la FT. al desarrollo de la cultura de ciberseguridad en la sociedad, un BAJO número de equipos y herramientas de ciberdefensa de última generación, con un PARCIAL recurso humano capacitado en operaciones de ciberdefensa., con un IMPROCEDENTE marco regulatorio en el ciberespacio, con una LIMITADA reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital y una BAJA doctrina de operaciones en el ciberespacio.

Escenario Cisne Negro "Venezolano"

El escenario Cisne Negro al 2033 se caracteriza por: tener una INEXISTENTE ejecución de las operaciones de ciberdefensa, un NULO presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un IRREAL apoyo de la FT. al desarrollo de la cultura de ciberseguridad, un INSUBSISTENTE número de equipos de ciberdefensa de la FT. de última generación, con un INEXISTENTE recurso humano capacitado en operaciones de ciberdefensa., con un NULO marco regulatorio en el ciberespacio, con una INEFECTIVA reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital, y una NULA doctrina de operaciones en el ciberespacio.

Escenario Apuesta "Español"

El escenario Apuesta al 2033 se caracteriza por: tener una CONTINUA ejecución de las operaciones de ciberdefensa, un SUFICIENTE presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un CONTINUO apoyo de la FT. al desarrollo de la cultura de ciberseguridad, un ALTO número de equipos y herramientas de ciberdefensa de la FT. de última generación, con un EQUILIBRADO recurso humano capacitado en operaciones de ciberdefensa, con un MODERADO marco regulatorio en el ciberespacio, con una CONTINUA reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital, y una SUFICIENTE doctrina de operaciones en el ciberespacio.

Matriz de Importancia y Gobernabilidad (IGO)

Herramienta que permite levantar objetivos estratégicos y sus acciones particulares, y que a través de una evaluación de la importancia y gobernabilidad a cada una de las acciones estratégicas se puede generar el diagrama donde se determina las que son urgentes, necesarias, menos urgentes e innecesarias, para priorizar de manera sencilla los proyectos (Jiménez, 2007).

Importancia

"Es el grado de influencia de cada acción en la consecución de su objetivo".

Gobernabilidad

"Es el control que la organización o los actores tienen sobre cada acción o proyecto".

Para la calificación se le asigna un puntaje a cada acción, de acuerdo con su grado gobernabilidad con una escala de 5 (fuerte), 3 (moderado) y 1 (débil), mientras que para calificar la importancia la escala será 5,10, 15, 20 y 25 donde 5 es menos importante y 25 más importante.

Estos valores se constituirán en pares ordenados dentro de un plano cartesiano formado por los valores de gobernabilidad que se constituirá en el eje de las "X", y los valores de la importancia que se constituirá como eje de las "Y". Además, con el valor de las medianas de cada uno de estos ejes, se divide en cuatro partes al área del plano cartesiano donde se ubicará los pares ordenados de cada factor. Estos cuatro subsectores son los siguientes:

Sector 1 Urgentes. Aquellas que están en el extremo superior derecho, es decir son las que tienen mayor gobernabilidad e importancia, en otras palabras, se tiene control sobre ellas y su ejecución tendrá una importante repercusión en el escenario a estudiar; por lo tanto, deben considerarse como prioritarias.

Sector 2 Necesarias. Están en el extremo superior izquierdo (mayor importancia, pero menor Gobernabilidad); es decir son aquellas que van a repercutir sobre el sistema, pero no se tiene un control total sobre ellas.

Sector 3 Innecesarias. Se ubican en el extremo inferior izquierdo entonces tienen poca Gobernabilidad y también poca Importancia, como se puede apreciar, son difíciles de manipular y además no tienen un impacto importante en el escenario.

Sector 4 Menos Urgente. Están en el extremo inferior derecho, tienen una alta gobernabilidad, pero no van a impactar notoriamente en el sistema.

Tabla 15

Matriz IGO

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario Apuesta	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Ejecución de operaciones de ciberdefensa.	Continua	Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Estableciendo un equipo de respuesta a incidentes seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.	20	5	Urgente
			Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.	25	5	Urgente
Presupuesto para un grupo con capacidades de ciberdefensa.	Suficiente	Optimizar el presupuesto suficiente para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa.	25	3	Necesaria
			Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.	20	1	Necesaria

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario Apuesta	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Desarrollo de una cultura de ciberseguridad.	Continuo	Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.	Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de Educación y Doctrina Militar Terrestre.	20	1	Necesaria
			Concientizando al personal en ciberseguridad a través de una política, impulsada del Comando General.	10	3	Innecesaria
Herramientas y equipos de ciberdefensa de última generación.	Alto	Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	Negociando con empresas pares para la implementación de herramientas de ciberdefensa a bajos costos.	15	5	Menos urgente
			Impulsando el desarrollo de conocimiento a través de los Centros de Investigación, para eliminar la dependencia extranjera.	20	1	Necesaria

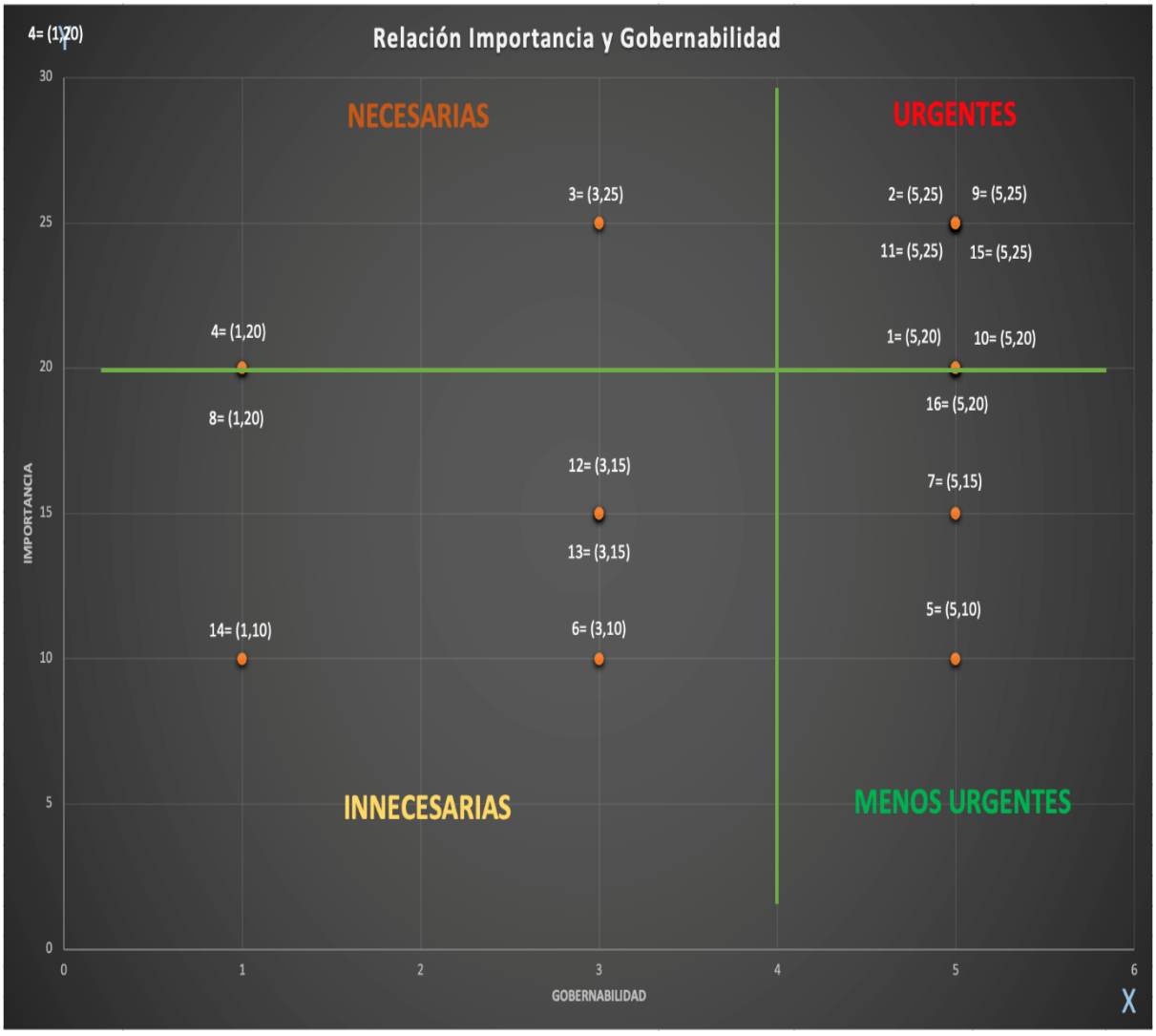
Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario Apuesta	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Recurso humano capacitado en operaciones de ciberdefensa	Equilibrado	Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa	Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre.	25	5	Urgente
			Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.	20	5	Urgente
Marco regulatorio en el ciberespacio.	Moderado	Alcanzar un moderado con marco regulatorio en el ciberespacio.	Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio.	25	5	Urgente
			Proponiendo reglas de enfrentamiento y normas de comportamiento en el ciberespacio.	20	1	Necesaria
Reducir las vulnerabilidades cibernéticas en la ITD.	Continua	Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD	Incrementando la capacidad de monitoreo, detección y eliminación de ciberamenazas en la ITD.	20	1	Necesaria
			Ejecutando ciberoperaciones conjuntas con el COCIBER y el CIES, para la reducción de vulnerabilidades cibernéticas en la ITD	10	1	Innecesaria

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario Apuesta	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Doctrina de operaciones en el ciberespacio.	Suficiente	Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Generando la doctrina básica de ciberoperaciones	25	5	Urgente
			Participando en ejercicios de ciberdefensa nacionales e internacionales en todos los niveles de mando.	20	1	Necesaria
		Total		**300**		
		Valor establecido como base		**300**		

La mediana de la columna de importancia se encuentra en un valor de 20 y de la Gobernabilidad se encuentra en un valor de 4, de donde se pueden establecer las siguientes acciones estrategias urgentes y necesarias:

Figura 8

Gráfico de Relación Importancia y Gobernabilidad



Nota. Se empleó el software MACTOR (2018) para la generación del gráfico.

Una vez generado el gráfico de relación de importancia y gobernabilidad, se clasifican las acciones estratégicas necesarias y urgentes en la siguiente tabla:

Tabla 16

Acciones estratégicas urgentes y necesarias

Acciones estratégicas urgentes		
Acciones	**Gobernabilidad**	**Importancia**
Estableciendo un equipo de respuesta a incidentes seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.	20	5
Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.	25	5
Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre.	25	5
Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.	20	5
Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio.	25	5
Generando la doctrina básica de ciberoperaciones	25	5
Acciones estratégicas necesarias		
Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa.	25	3
Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.	20	1
Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de Educación y Doctrina Militar Terrestre.	20	1
Impulsando el desarrollo de conocimiento a través de los Centros de Investigación, para eliminar la dependencia extranjera.	20	1
Proponiendo reglas de enfrentamiento y normas de comportamiento en el ciberespacio.	20	1
Incrementar la capacidad de monitoreo, detección y eliminación de ciberamenazas en la ITD.	20	1

Juego de Actores.

El juego de actores constituye una estrategia recurrente entre las actividades que se aplican en el ámbito del análisis y la investigación en todos sus niveles y disciplinas de conocimiento; sin embargo, la relativa obviedad de sus objetivos instrumentales, la oportunidad de su aplicación, el diseño metodológico, la creatividad del dispositivo, la dinámica operativa, la diversidad temática, le confieren una potencialidad inagotable, versatilidad de aplicación y multiplicidad de opciones a ser aplicados por los mismos, los cuales se manifiestan dentro de un análisis estratégico.

En este contexto, se puede considerar que el futuro nunca está totalmente establecido, sea cual sea la tendencia que proviene del pasado, este en realidad se encuentra abierto a varios escenarios posibles. De hecho, los actores determinados para el análisis prospectivo de la Ciberdefensa en la FT. disponen de múltiples grados de libertad que podrán ejercer a través de acciones estratégicas para alcanzar los fines propuestos (Arcade et al, 2004).

Tabla 17

Tabla de actores a favor y en contra.

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario apuesta	Actores	
			Favor	En contra
Ejecución de operaciones de ciberdefensa.	Continua	Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Fuerza Terrestre	Estados regionales e internacionales
Presupuesto para un grupo con capacidades de ciberdefensa.	Suficiente	Optimizar el presupuesto para el suficiente desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	AGRUCOMGE	Ministerio de Economía y Finanzas
Apoyar al desarrollo de una cultura de ciberseguridad.	Continuo	Generar un continuo apoyo al desarrollo de una cultura de ciberseguridad.	Comité de Ciberdefensa	Ciberdelincuencia
Equipos y herramientas de ciberdefensa de la FT de última generación.	Alto	Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	GRUCIBER	Ciberamenazas

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario apuesta	Actores	
			Favor	En contra
Marco regulatorio en el ciberespacio.	Moderado	Alcanzar un moderado con marco regulatorio en el ciberespacio.	Fuerza Terrestre	Ciberamenazas y ciberoponentes
Reducir las vulnerabilidades cibernéticas en la ITD.	Continua	Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD	Fuerza Terrestre	Ciberamenazas
Doctrina de operaciones en el ciberespacio.	Suficiente	Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Fuerza Terrestre	Ciberamenazas

Tabla 18

Listado de actores.

N°	Título largo	Título corto
1	Fuerza Terrestre	FT
2	Ministerio de Defensa Nacional	MDN
3	Agrupamiento de Comunicaciones y Guerra Electrónica	AGRUCOMGE
4	Comité de Ciberdefensa	CCIBER
5	Grupo de Ciberdefensa de la Fuerza Terrestre	GRUCIBER
6	Centro de monitoreo de información conjunta	CMIC
7	Estados Regionales e Internacionales	ERI
8	Ciberterroristas	CBT
9	Ciberdelincuencia	CBD
10	Ciberamenazas	CBA
11	Comando de Ciberdefensa	COCIBER
12	Crimen Organizado Transnacional	COTRA
13	Grupos Sociales Antagónicos	GSA

Tabla 19

Listado de objetivos.

N°	Título largo	Título corto
1	Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	OP.CIBER
2	Optimizar el presupuesto suficiente para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	ASG.PRE
3	Generar un continuo apoyo al desarrollo de una cultura de ciberseguridad.	A.C.CIBERS

N°	Título largo	Título corto
4	Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	EQ.UG
5	Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa	U.CIBER
6	Alcanzar un moderado con marco regulatorio en el ciberespacio.	TEC.CAP
7	Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD	ACC.POL
8	Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	CAP.CIB.

Tabla 20

Matriz de Influencia Directa (MID), calificación de la matriz actor x actor.

	FT	MDN	AGRUCOMGE	CCIBER	GRUCIBER	CMIC	ERI	CBT	CBD	CBA	COCIBER	COTRA	GSA
FT	0	2	3	1	3	1	2	3	3	3	1	3	1
MDN	1	0	0	1	0	1	2	3	3	3	1	3	1
AGRUCOMGE	1	0	0	0	3	0	0	3	3	3	1	3	1
CCIBER	1	2	1	0	1	2	2	4	4	4	1	4	1
GRUCIBER	2	0	2	0	0	0	2	4	4	4	2	4	1
CMIC	2	2	1	1	1	0	1	2	2	2	2	2	1
ERI	2	2	2	2	2	1	0	2	2	2	2	2	1
CBT	2	2	2	2	2	2	3	0	2	2	2	2	2
CBD	2	2	2	2	2	2	3	2	0	2	2	2	2
CBA	2	2	2	2	2	2	3	2	2	0	2	2	2
COCIBER	2	0	2	2	2	3	2	3	3	3	0	2	2
COTRA	2	2	2	2	2	2	2	2	2	2	2	0	2
GSA	2	2	2	2	2	3	0	1	1	1	1	1	0

Nota. Se empleó el software MACTOR (2018) para la generación de la Matriz.

Para generar las calificaciones de la influencia de los actores en la matriz de Actor por Actor (MID) se van a utilizar los nombres cortos o abreviados de los actores debido al espacio en la matriz. Esta matriz lo que busca es identificar por medio de una escala que va del 1 al 4 cuál actor influye más sobre otro, o cuál tiene más poder que otro. Para calificar la influencia de actores se utilizará la siguiente escala:

4= Fuerte influencia

3= Moderada influencia

2= Débil influencia

1= Muy débil influencia

0= Influencia nula

De esta manera, se debe discurrir que los actores que alcancen el valor de 4 serán de mayor fuerza, mientras que los que alcanzan el valor de 1 son los de muy débil poder o fuerza, con lo cual se logra relacionar los diferentes actores y determinar el nivel de influencia o poder. Cabe señalar que los actores más poderosos son aquellos que ejercen fuerte influencia sobre los demás y a la vez dependen muy poco de ellos.

Calificación de la Matriz Actor x Objetivo (2MAO).

Para determinar el nivel de involucramiento del actor frente al objetivo, se realizará a través de la matriz actor objetivo (2MAO), con la cual podremos determinar la posición que tiene el actor respecto a cada objetivo, reflejando la categoría que éste le da a cada uno.

Tabla 21

Matriz actor x objetivo (2MAO)

	OP.CIBER	ASG.PRE	A.C.CIBERS	EQ.UG	U.CIBER	TEC.CAP	ACC.POL	CAP.CIB.
FT	4	3	3	4	2	3	1	4
MDN	4	3	3	4	2	3	4	4
AGRUCOMGE	4	2	2	4	2	3	1	4
CCIBER	4	1	1	4	1	2	1	1
GRUCIBER	4	1	1	4	4	2	1	1
CMIC	4	1	1	3	1	2	2	1
ERI	4	3	3	2	1	2	4	1
CBT	-4	-4	-4	-4	-4	-4	-4	-4
CBD	-4	-4	-4	-4	-4	-4	-4	-4
CBA	-4	-4	-4	-4	-4	-4	-4	-4
COCIBER	4	3	3	4	0	3	2	2
COTRA	-4	-4	-4	-4	-4	-4	-4	-4
GSA	-2	1	1	-2	-1	-2	-2	2

Nota. Se empleó el software MACTOR (2018) para la generación de la Matriz.

Además, también la matriz (2MAO), permite identificar aquellos actores que están a favor y aquellos que están en contra de los objetivos planteados en el análisis de la ciberdefensa de la FT, para lo cual se procede a calificar mediante el uso de la escala del - 4 a 4, donde el valor de 4 positivo significa que el actor está fuertemente a favor y el 4 negativo quiere decir que está fuertemente en contra.

Tabla 22

Matriz escala de calificación de actor x objetivo (2MAO)

A FAVOR	EN CONTRA
4= Fuerte a favor	- 4= Fuerte en contra
3= Moderado a favor	- 3= Moderado en contra
2= Débil a favor	- 2= Débil en contra
1= Muy débil a favor	- 1= Muy débil en contra
0= Ninguna actitud	

Reportes Generados por el Programa Mactor

Con la calificación asignada a actores y objetivos en las matrices MID y 2MAO, el software MACTOR genera los reportes referentes al nivel poder, convergencia, divergencia y ambivalencia de los actores (Godet M. , 2007), tal como a continuación se detalla.

Poder de los Actores.

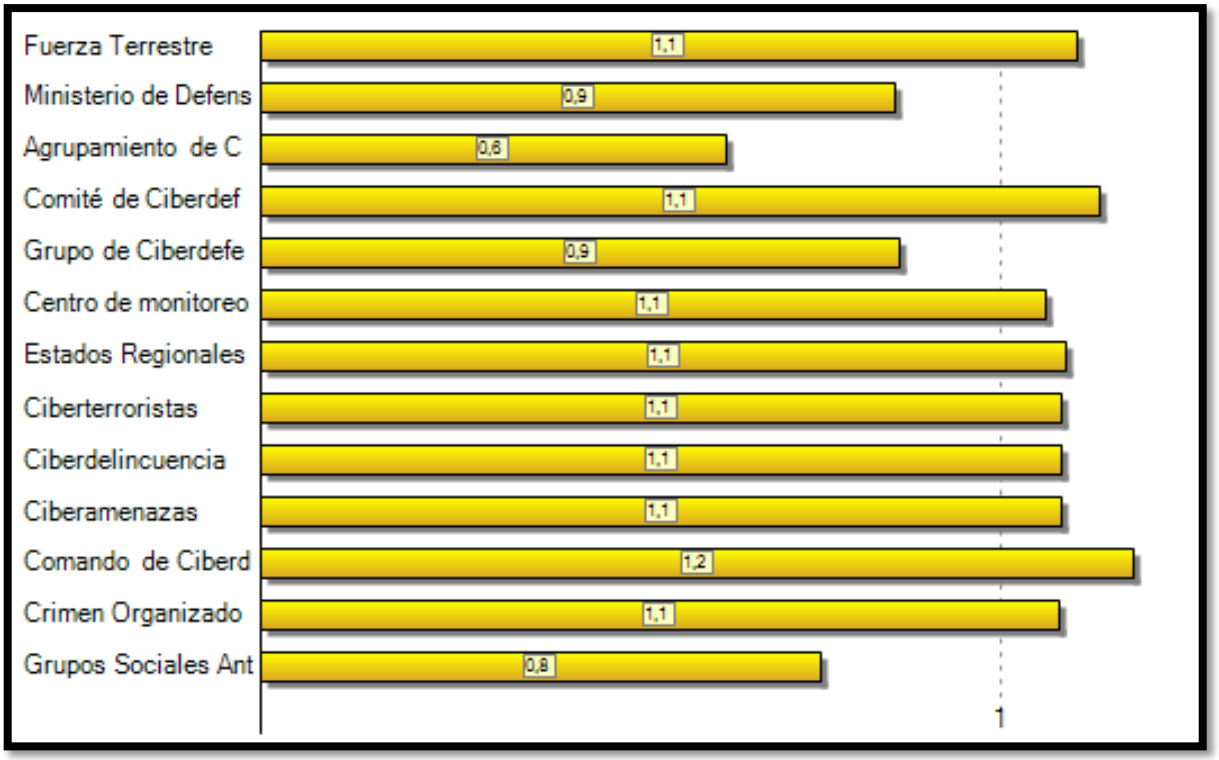
En la figura 8. Histograma de relaciones de fuerza MMIDI, se observa en forma de barras de histograma, los actores de mayor a menor influencia, priorizados por el MACTOR. La barra de mayor tamaño correspondiente al Comando de Ciberdefensa, la cual representa la mayor fuerza o poder como actor con un valor de 1.2, en consecuencia es el más influyente entre todos los actores del presente histograma, seguidos por la Fuerza Terrestre, el Ministerio de Defensa Nacional con un valor de 0,9; el Comité de Ciberdefensa, el Centro de Monitoreo Conjunto, Estados Regionales e Internacionales, ciberterroristas, ciberamenazas y el crimen organizado con un valor de 1.1; los grupos sociales antagónicos

con un valor de 0,8 y el Agrupamiento de Comunicaciones y Guerra Electrónica con un valor de 0,6.

En conclusión, el actor de mayor poder o influencia es el Comando de Ciberdefensa siendo las de mediana influencia las unidades militares, y la menor influencia son los ciberterroristas.

Figura 9

Histograma de relaciones de fuerza MMIDI



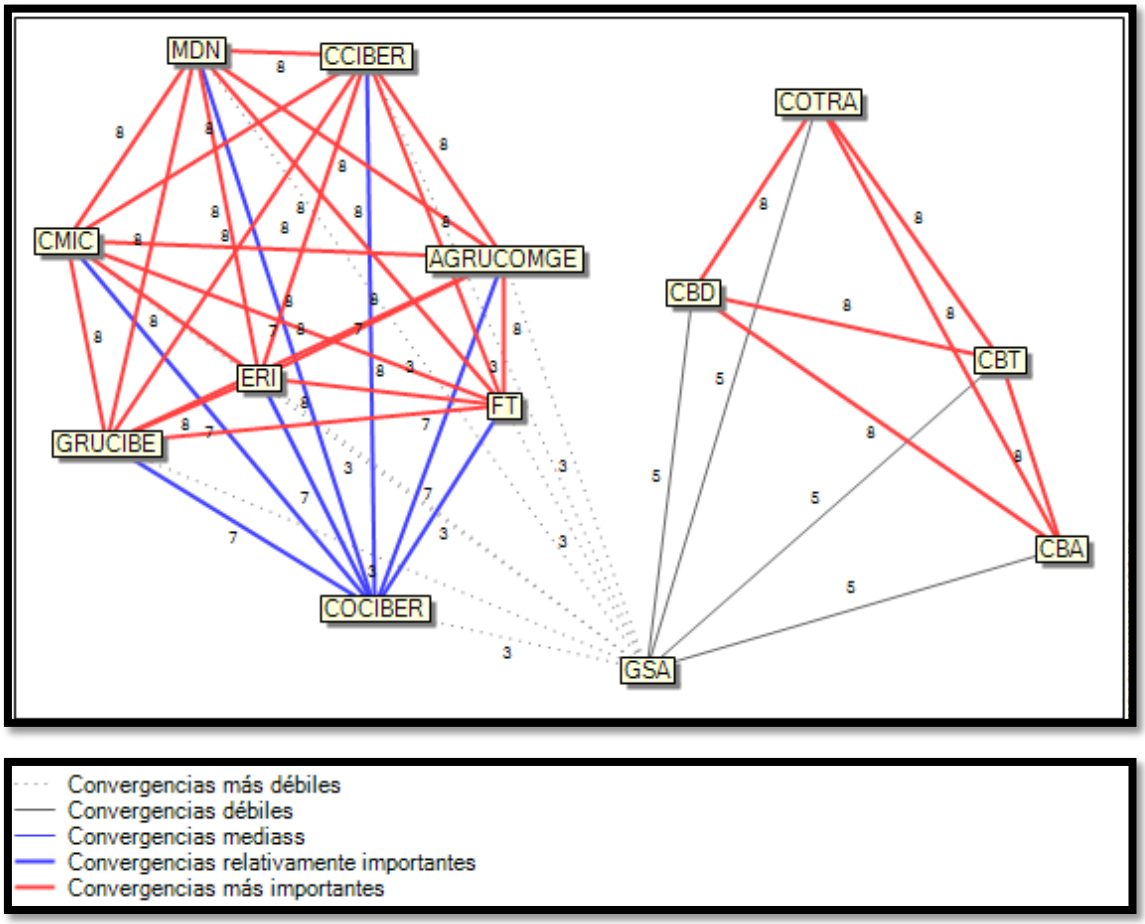
Nota. Se empleó el software MACTOR (2018) para la generación del histograma.

Convergencia o Alianza de los Actores

Para alcanzar un objetivo común, varios actores se agrupan bajo una alianza a la cual se le denomina convergencia. En la figura 9. gráfico de convergencia entre actores de orden 3, se muestra una red que representa la convergencia entre los actores (nombre corto), donde las líneas de colores indican la mayor o menor posibilidad. Es decir, se conciben las posibles alianzas.

Figura 10

Gráfico de Convergencia entre actores



Nota. Se empleó el software MACTOR (2018) para la generación del gráfico.

Las convergencias que se aprecian en el análisis del juego de actores plantean con claridad la posibilidad de las alianzas que pueden establecerse entre los diferentes actores identificados para el fortalecimiento de la ciberdefensa en la FT.

Las convergencias más importantes identificadas son:

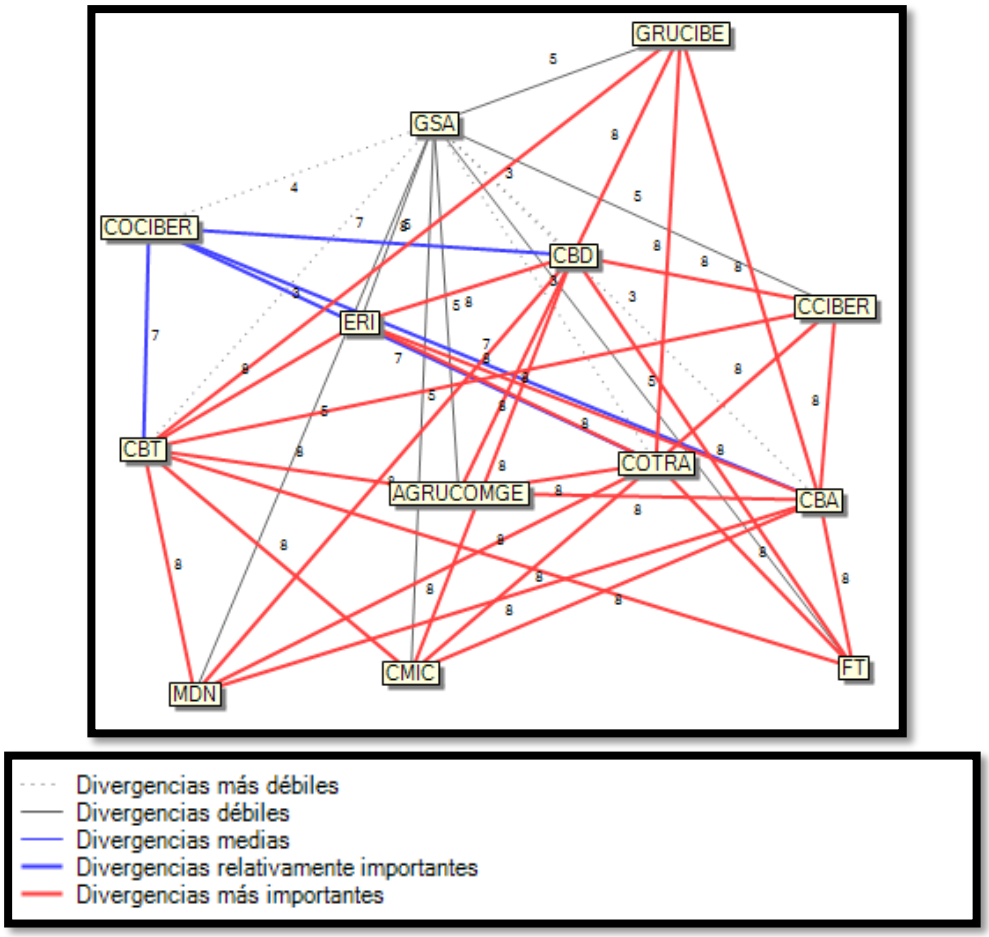
- El Ministerio de Defensa Nacional con el Comité de Ciberdefensa.
- El Ministerio de Defensa Nacional con el Centro de Monitoreo de Información Conjunta.
- El Ministerio de Defensa Nacional con el Comando de Ciberdefensa
- La Fuerza Terrestre con el AGRUCOMGE.
- La Fuerza Terrestre con el Grupo de Ciberdefensa de la FT.
- La Fuerza Terrestre con el Estados Regionales e Internacionales.

Divergencia o Conflicto de los Actores.

La divergencia se relaciona a la oposición de los actores frente a un objetivo. En la figura 10. se representa la existencia de divergencias entre actores, el gráfico permite visualizar la formación de una malla de divergencia entre estos, es decir aquellos que pueden generar conflicto.

Figura 11

Gráfico de Divergencias entre actores



Nota. Se empleó el software MACTOR (2018) para la generación del gráfico.

Los grupos de actores en conflicto en orden de importancia de acuerdo con el reporte del programa MACTOR son: el primer grupo conformado por el Ministerio de Defensa Nacional contra la Fuerza Terrestre y sus unidades de ciberdefensa además; ciberterroristas, crimen organizado transnacional, el segundo grupo lo compone el

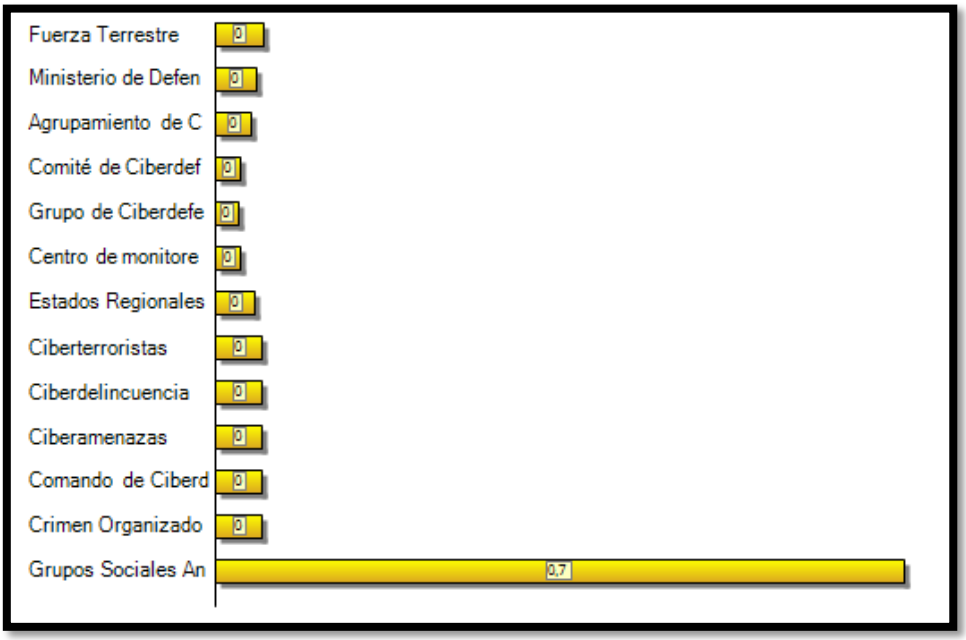
COCIBER contra los ciberterroristas, ciberamenazas y ciberdelincuencia y finalmente un tercer grupo está integrado por los grupos antagónicos contra ciberterroristas, crimen organizado transnacional y ciberamenazas.

Ambivalencia o Riesgo de los Actores

Dos actores pueden ser tanto convergentes como divergentes en relación con un objetivo. Por lo tanto, estos se denominan actores ambivalentes (Mederos, 2016).

Figura 12

Histograma de la ambivalencia entre actores.



Nota. Se empleó el software MACTOR (2018) para la generación del histograma.

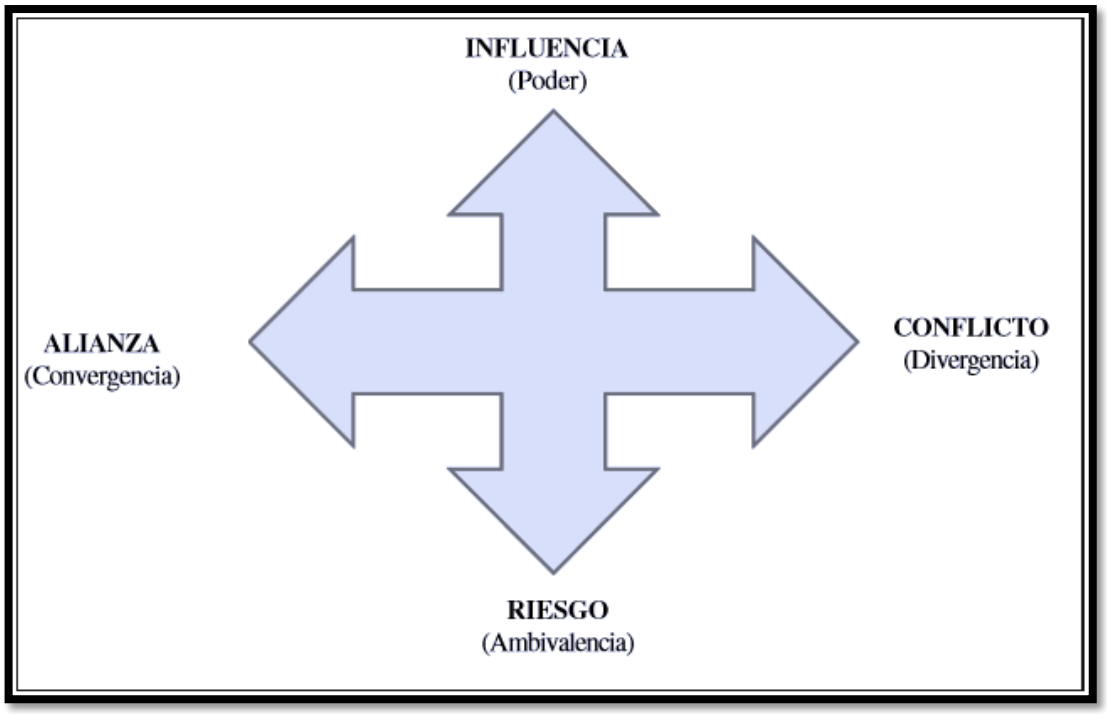
El actor de mayor riesgo por su alta ambivalencia y de acuerdo con el reporte del MACTOR es el de los grupos sociales antagónicos debido a que son los que mayor grado de ambivalencia tienen.

Análisis Estratégico de los Actores

El Análisis Estratégico de Actores (AEA), herramienta aplicada en el presente trabajo, se puede visualizar gráficamente en la figura 12.

Figura 13

Análisis Estratégico de Actores



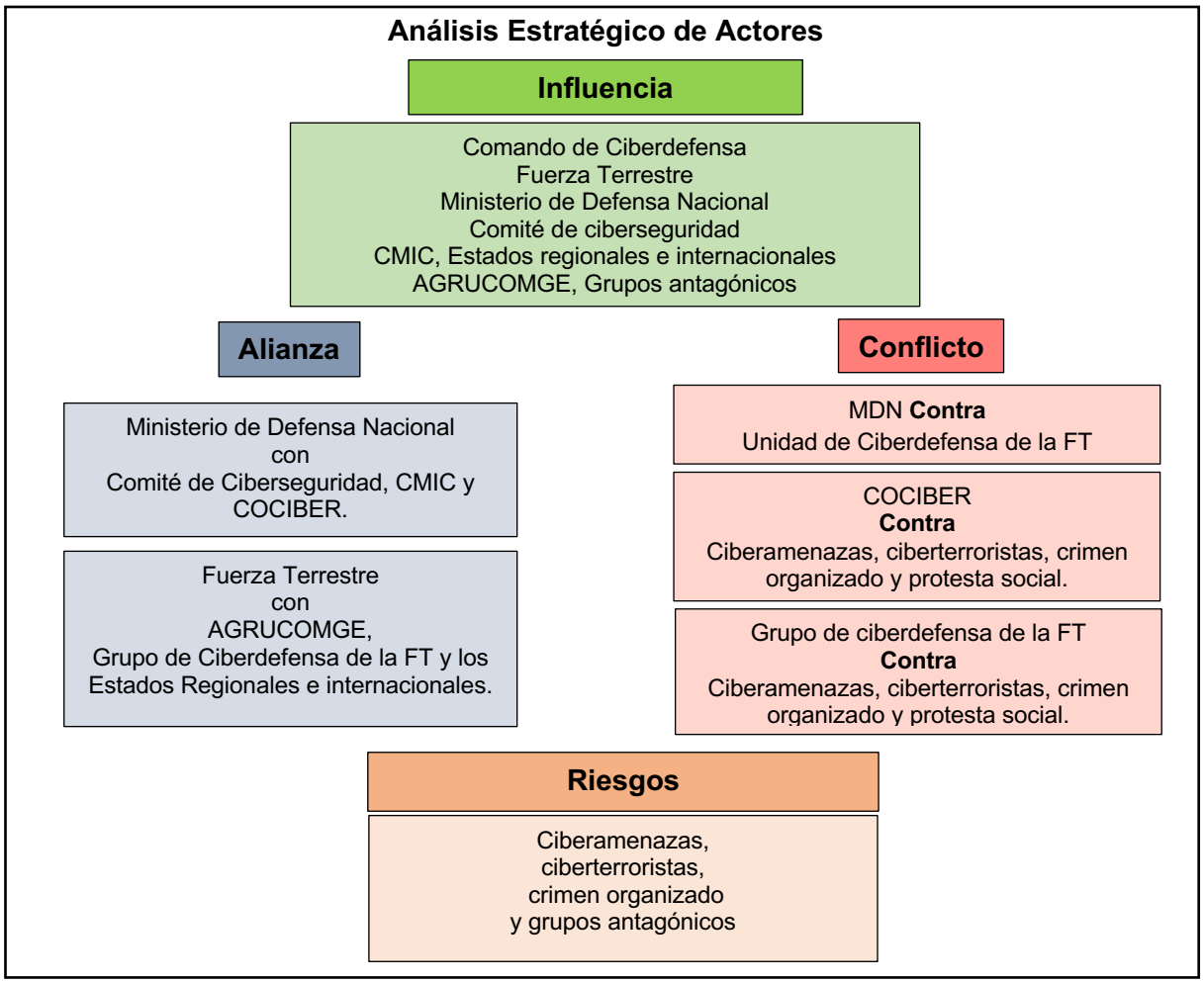
En el análisis estratégico de actores, se muestra las particularidades de los diferentes actores involucrados en un solo documento, permitiendo tener una perspectiva de los actores que tiene mayor poder e influencia sobre otros, las posibles alianzas entre ellos, así como los más riesgosos (poco confiables) por su gran ambivalencia, y los que pueden generar conflicto por su divergencia.

Para describir esta información, se genera a través de una mapeamiento de actores y sus jugadas, con lo cual se diseñan acciones estratégicas apropiadas para lograr los objetivos advertidos por la institución.

En la figura 14. se presenta la aplicación del AEA para el análisis de la ciberdefensa de la FT.

Figura 14

Análisis Estratégico de Actores de Ciberdefensa



Nota. Los datos fueron tomados de los resultados arrojados por el software MACTOR (2018).

En la figura anterior se puede identificar que el Comando de Ciberdefensa (COCIBER) es el actor que mayor influencia dispone, seguido por la Fuerza Terrestre y el Ministerio de Defensa, además las ciberamenazas, ciberterroristas, crimen organizado y grupos antagónicos se constituyen los actores que mayor riesgo pueden generar por su ambivalencia elevada. También permite identificar los actores con los cuales se puede crear alianzas y con cuales se pueden generar conflictos, permitiendo de esta manera relacionar los distintos actores, de tal manera que se pueda esclarecer sus posibles jugadas, información clave al momento de implementar estrategias para poder hacerlos frente de forma efectiva.

Capítulo V

Propuesta

Plan Estratégico Institucional de la Ciberdefensa en la Fuerza Terrestre

Introducción

Mediante una planificación estratégica adecuada, que permita al nivel político estratégico mantener una conciencia situacional de este nuevo ámbito de operación, se alcanzará una gestión eficaz, basada en el desarrollo de capacidades para que la fuerza militar actúe en el quinto dominio de la guerra y sobre todo pueda asegurar la Infraestructura Crítica Digital del Estado y la Infraestructura Tecnológica Digital del sector Defensa. Con esta premisa el Ministerio de Defensa Nacional, ha incluido en los elementos orientadores de la defensa, aspectos organizativos, procedimientos tecnológicos, así como de capacitación y desarrollo integral de profesionales plasmados inicialmente en una unidad cibernética a nivel Comando Conjunto y posteriormente con la formación de unidades tácticas en cada una de las Fuerzas Terrestre, Naval y Aérea descritos en el Anexo “A” (Línea de tiempo de la ciberdefensa en el Ecuador).

Es de suma importancia para todo grupo estructurado, empresa u organización, el determinar el rumbo u orientación que se plantea seguir en función de las actividades que le permiten desarrollar, producir u ofertar productos o servicios de “calidad”, así la planeación estratégica es una herramienta que direcciona el comportamiento organizacional e incide de forma significativa en las actividades y decisiones tanto de quienes dirigen la organización, como de quienes se constituyen en los ejecutores de las decisiones del nivel directivo de la organización; generalmente para esto se determina una “filosofía institucional” (la cual señala la misión, visión, y valores), así como una “planificación estratégica institucional” relacionada a los objetivos estratégicos, estrategias, acciones y metas a corto, mediano y largo plazo.

El ámbito militar, no es ajeno a este tipo de “estrategias” es más muchas de las herramientas de decisión empresarial fueron desarrolladas a partir del denominado “Proceso

Militar en la Toma de Decisiones" (PMTD), ante lo anterior la estructura militar en sus diversos niveles de mando y ejecución, ha establecido una planificación estructurada de tal forma, que en virtud de la realidad de su entorno y de los posibles escenarios en los cuales debe desarrollar sus actividades y acciones propias de su identidad y de la misión institucional y constitucional encomendada, establece y consolida tanto objetivos como metas, que en función de las "políticas de Estado" en el ámbito de la "Seguridad y Defensa" apoyan la consecución de metas u objetivos de carácter nacional.

El "Plan Estratégico de Ciberdefensa" es un documento que describe la estructura de una planificación estratégica, este deberá ser considerado por la Fuerza Terrestre dentro de su planificación, debido a que permite describir y orientar de forma particular tanto: la misión, visión, valores y objetivos estratégicos con sus correspondientes estrategias, estos elementos fueron determinados mediante el proceso prospectivo de Godet para el caso de objetivos y estrategias y de planificación para los demás elementos, como lo establece el Anexo "B" (Procedimiento de planificación para establecerla misión, visión, valores y principios de la ciberdefensa en la FT). Con la definición del Plan Estratégico se puede proporcionar apoyo en el ciberespacio a las diversas unidades militares, así también apuntalar la gestión del Agrupamiento de Comunicaciones y Guerra Electrónica; finalmente de lo expuesto, el presente trabajo pretende describir en forma ordenada y estructurada los diversos elementos que corresponden a la planificación estratégica institucional de Ciberdefensa de la Fuerza Terrestre, así en función del entorno, escenario del empleo y de los "elementos orientadores" de la Ciberdefensa, se han determinado factores internos (fortalezas – debilidades) y agentes externos (Oportunidades – amenazas) que han permitido establecer objetivos estratégicos institucionales y sus correspondientes estrategias, las cuales a su vez permiten desarrollar procesos, programas, proyectos e indicadores que permitirán alcanzar los objetivos institucionales planteados.

Figura 15

Ataques cibernéticos al Ecuador en tiempo real

Nota. https://cybermap.kaspersky.com/es (2023).

Misión

La Fuerza Terrestre a través del Grupo de Ciberdefensa efectuará operaciones de defensa y exploración en el ciberespacio de forma permanente en apoyo a las operaciones militares en todo el teatro de operaciones, para proteger la infraestructura tecnológica digital de la institución; operaciones de respuesta, con orden, para degradar o neutralizar la infraestructura crítica tecnológica del adversario y así contribuir con el cumplimiento de las misiones del Comando de Operaciones Terrestres.

Visión

Al 2033, la Fuerza Terrestre tendrá una elevada capacidad tecnológica, innovadora e interoperable en el ciberespacio, que le permita ejecutar acciones de defensa exploración y respuesta en el quinto dominio en apoyo a las operaciones militares, para conocer, prevenir, disuadir y responder a las ciberamenazas, en escenarios de alta incertidumbre, en el ámbito de la seguridad y defensa, proporcionando el apoyo con efectividad, cohesión institucional y trabajo en equipo, empleando personal profesional calificado, experimentado y certificado, con capacidad disuasiva, permanente y sostenible.

Figura 16

Mapa de ciberataques a nivel mundial.

Nota. https://securityinside.info/5-mapas-de-ciberataques-para-impresionar-like-a-pro/ (2023).

Valores

Responsabilidad

"Cumplimiento cabal y correcto de los deberes inherentes al grado y función que le fueron asignados, que le permita cumplir una tarea de manera exitosa" (Dirección de Planificación y Gestión Estratégica de la FT, 2021).

Integridad

"Verticalidad de carácter, firmeza de principios morales, cualidad de la verdad y honestidad absoluta, y toma sistemática decisiones positivas, incluso cuando nadie esté controlando" (Dirección de Planificación y Gestión Estratégica de la FT, 2021).

Lealtad

"Sentimiento de noble fidelidad y franqueza que permite un ambiente de confianza y seguridad en las relaciones entre los miembros de las Fuerzas Armadas y de entrega total a la institución a la que se pertenece" (Dirección de Planificación y Gestión Estratégica de la FT, 2021).

Trabajo en Equipo

"Labor que se lleva a cabo a través de un conjunto de integrantes que tienen la capacidad de participar activamente en la prosecución de una meta común subordinando los intereses personales a los objetivos del equipo" (Dirección de Planificación y Gestión Estratégica de la FT, 2021).

Cohesión Institucional

"Es el vínculo de unión, solidaridad y orgullo de pertenecer a las Fuerzas Armadas. Es el desarrollo del espíritu colectivo propio del trabajo en equipo con responsabilidad compartida" (Dirección de Planificación y Gestión Estratégica de la FT, 2021).

Principios

Los principios de la capacidad de ciberdefensa en la Fuerza Terrestre precisan la disposición en el accionar de sus miembros en el cumplimiento de las misiones asignadas, además; garantizan el fortalecimiento del conocimiento en ciberdefensa, por lo que es una obligación definirlos, practicarlos, difundirlos y hacerlos cumplir. Para el desarrollo de este trabajo, se ha tomado como referencia la Estrategia de Ciberdefensa 2021 establecida por el Ministerio de Defensa Nacional del Ecuador, la Doctrina Militar de Defensa Cibernética de Brasil y el Manual de Operaciones Militares Cibernéticas de Argentina, llegando a definir los siguientes:

Cooperación

Depende de colaboración y aporte de varios actores, es uno de los principios fundamentales de la ciberdefensa. El intercambio de información e inteligencia de ciberamenazas, permite reducir los riesgos, mejorar los controles y responder oportuna y adecuadamente a las ciberamenazas.

Disimulación

Se adoptan medidas activas para no ser detectados por las ciberoperaciones de exploración y respuesta del oponente, realizando el enmascaramiento de las ciberoperaciones ofensivas propias.

Resiliencia

Toma de decisiones orientadas a que la ciberdefensa de la FT tenga la capacidad de resistir, adaptarse y/o recuperarse de una ciberamenaza de manera oportuna y eficiente, a través de la prevención y restauración de su estructura y funciones básicas.

Adaptabilidad

Mediante proactividad, la defensa en el ciberespacio se adapta o se mantiene flexible a la capacidad de mutación del oponente.

Restricción

Limita el uso innecesario de la fuerza, para evitar los daños colaterales mediante el equilibrio de la necesidad de seguridad, la conducción de las ciberoperaciones y el estado final deseado. (Amorin, 2014)

Maniobra

La cibermaniobra se utiliza para aplicar la fuerza, negar operaciones u obtener acceso a fuentes de información clave o sistemas estratégicamente valiosos. (De Vergara & Trama, 2022)

Seguridad y Simplicidad

Principios que permiten el desarrollo de los vectores de ataque en el ciberespacio para atacar la infraestructura tecnológica digital del oponente. (Amorin, 2014)

Tempo

Principio que permite la presión constante para lograr el máximo efecto sicológico sobre el oponente.

Capacidad y Voluntad

Permite responder simétricamente a un ataque cibernético mediante ciberoperaciones de respuesta y asimétricamente atacando al régimen que gobierna el oponente mediante el apoyo de países aliados.

Objetivos Estratégicos

Los objetivos estratégicos de la ciberdefensa en la Fuerza Terrestre describen los resultados que se desean obtener o alcanzar en un tiempo determinado, se encuentran alineados a los objetivos estratégicos institucionales y guardan consistencia con la misión y visión de esta capacidad.

- Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.
- Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.
- Alcanzar una suficiente doctrina de operaciones en el ciberespacio.
- Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.
- Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa.
- Alcanzar un moderado marco regulatorio en el ciberespacio
- Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD.
- Optimizar el presupuesto suficiente para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.

Estrategias

A través de las estrategias o planes de acción, la capacidad de ciberdefensa en la Fuerza Terrestre cumplirá con los objetivos estratégicos planteados anteriormente. En la tabla 24, se describen las estrategias alineadas a los objetivos de la ciberdefensa.

Tabla 23

Estrategias

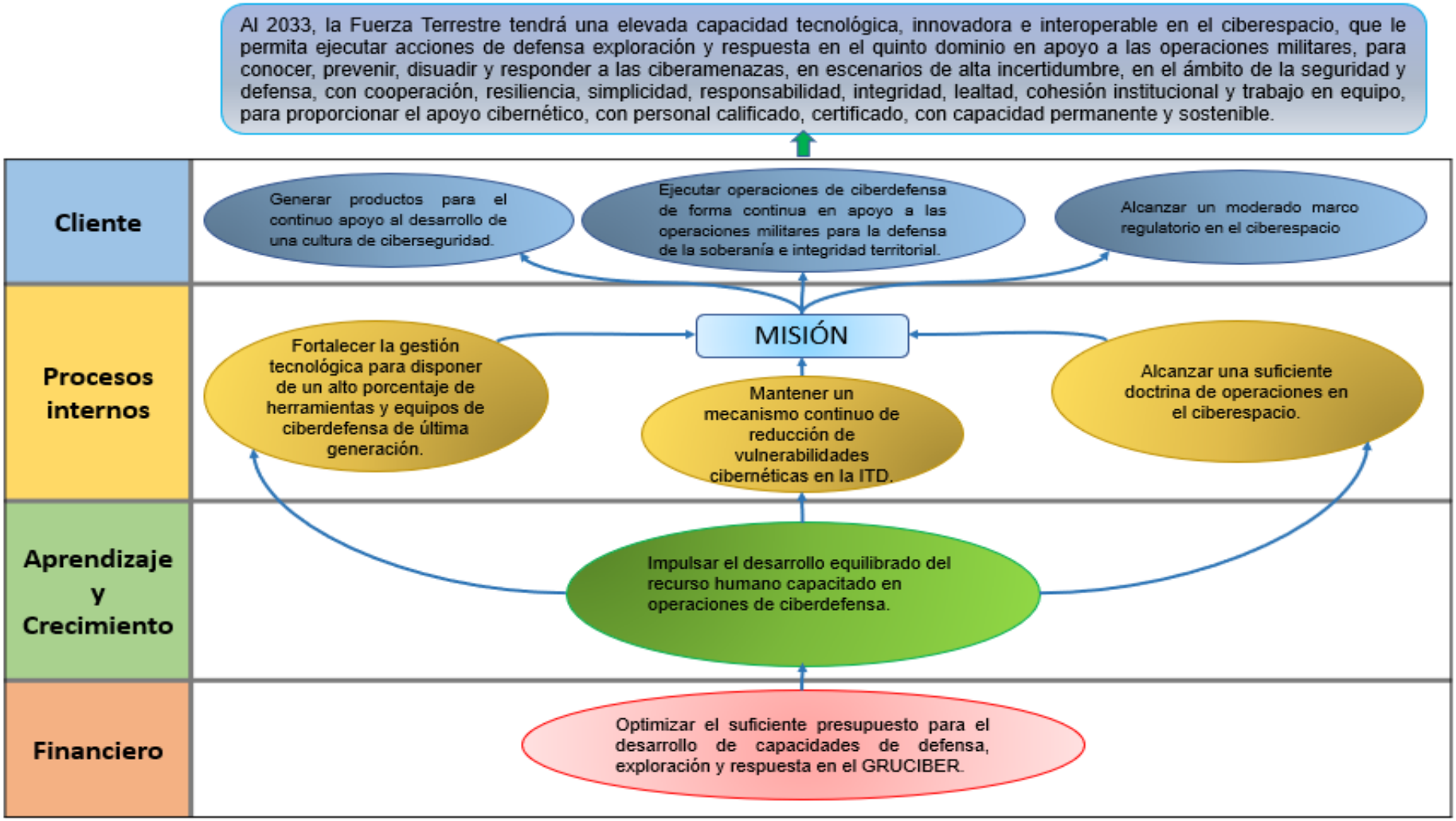
Perspectivas	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	Objetivos	**Ideas de innovación estratégica**	**Objetivo estratégico**	**Estrategias**
Cliente / Sociedad	**OBJ. 1** "Incrementar la efectividad en el control del territorio nacional".	Optimizando las operaciones militares en la defensa de la soberanía y seguridad integral.	**OBJ. 1** Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Estableciendo un equipo de respuesta a incidentes de seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.
		Estructurando unidades militares flexibles, móviles y multipropósito que puedan operar en diversos tipos de misiones y escenarios geográficos		Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.
		Proponiendo los cambios pertinentes al Marco Legal	**OBJ. 2** Alcanzar un moderado marco regulatorio en el ciberespacio.	Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio. Proponiendo reglas de enfrentamiento y normas de comportamiento en el ciberespacio.
	OBJ. 2 "Mantener la imagen institucional".	Fortaleciendo la imagen institucional y cohesión interna con el manejo adecuado de los temas legales.	**OBJ. 3** Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.	Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de Educación y Doctrina Militar Terrestre.

Perspectivas	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	Objetivos	**Ideas de innovación estratégica**	**Objetivo estratégico**	**Estrategias**
Procesos	**OBJ. 3** "Incrementar la efectividad operacional de las unidades militares".	Optimizando los procesos de difusión de información que tengan impacto estratégico Optimizando la infraestructura de las unidades militares acorde a los requerimientos operacionales Desarrollando protocolos y procedimientos que definan las condiciones de empleo, tareas específicas y coordinaciones que se deben realizar para el cumplimiento de misiones y tareas de apoyo a la seguridad integral.	**OBJ. 4** Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD.	Concientizando al personal en ciberseguridad a través de una política, impulsada del Comando General del Ejército. Incrementar la capacidad de monitoreo, detección y eliminación de ciberamenazas en la ITD. Ejecutar ciberoperaciones conjuntas con el COCIBER y el CIES, para la reducción de vulnerabilidades cibernéticas en la ITD
	OBJ. 4 "Incrementar las capacidades militares".	Fortaleciendo la capacidad de "ciberdefensa"	**OBJ. 5** Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	Negociando con empresas pares para la implementación de herramientas de ciberdefensa a bajos costos. Impulsando el desarrollo de conocimiento a través de los Centros de Investigación, para eliminar la dependencia extranjera.
	OBJ. 5 "Incrementar el alistamiento operacional".	Mejorar los niveles de entrenamiento, educación militar y generación de doctrina	**OBJ. 6** Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Generando la doctrina básica de ciberoperaciones. Participando en ejercicios de ciberdefensa nacionales e

Perspectivas	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	Objetivos	**Ideas de innovación estratégica**	**Objetivo estratégico**	**Estrategias**
				internacionales en todos los niveles de mando.
Aprendizaje y Crecimiento	**OBJ. 8** “Incrementar el desarrollo del talento humano”.	Mejorando las competencias del personal militar y de servidores públicos en función del perfil profesional.	**OBJ. 7** Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa.	Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre. Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.
Financiero	**OBJ. 9** “Incrementar el uso eficiente del presupuesto”.	Mejorar los procesos y procedimientos que permitan optimizar la planificación y ejecución presupuestaria, y el manejo administrativo de las unidades. Realizar el manejo del presupuesto y recursos institucionales bajo una política de priorización en virtud de los requerimientos operacionales y administrativos más importantes	**OBJ. 8** Optimizar el suficiente presupuesto para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa. Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.

Figura 17

Mapa Estratégico



Referencias Bibliográficas

Abad Páez, W., & Sandoval Loaiza, P. (2020). *Análisis de la situación actual de la Ciberdefensa en la Fuerza Terrestre 2020.* Universidad de Fuerzas Amadas ESPE.

Abad, N. S. (2018). *Ciberdefensa en el estado ecuatoriano periodo 2013-2016.* Pontificia Universidad Católica del Ecuador.

Amigo, A. (2015). Consideraciones sobre la ciberamenazas a la seguridad nacional. (Revista de Estrategia Nacional 125), 83-96.

Amorin, C. (2014). *Doctrina de Ciberdefensa Militar.* Ministerio de Defensa del estado.

Arana, M. (2015). La educación científico-tecnológica desde los estudios de la ciencia, tecnología, sociedad e innovación. (3), 292-313.

Arcade, J., Godet, M., & Meunier, F. (s.f.). (2004). Análisis estructural, con el método MICMAC, Estrategia de los Actores, con el método Mactor.

Asamblea Nacional. (2008). Constitución de la República del Ecuador. Quito, Pichincha, Ecuador: ANE.

Asamblea Nacional del Ecuador. (2002). Ley Orgánica de Comercio Electrónico, Firmas de Electrónicas y Mensajes de Datos. Quito, Pichincha, Ecuador: LOCE.

Asamblea Nacional del Ecuador. (2009). Ley de Seguridad Pública y del Estado. Quito, Pichincha, Ecuador: LSPE.

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Quito, Pichincha, Ecuador: COIP.

Asamblea Nacional del Ecuador. (2015). Ley Orgánica de Telecomunicaciones. Quito, Pichincha, Ecuador: LOT.

Asamblea Nacional del Ecuador. (2016). Ley Orgánica de la Identidad y datos civiles. Quito, Pichincha, Ecuador: LOIDC.

Asint360°. (16 de marzo de 2016). *Asint360°*. http://www.asint360.com/que-es-la-ciberinteligencia-la-inteligencia-en-materia-de-ciberseguridad/#:~:text=La%20Ciberinteligencia%20%28Cyberintelligence%20en%20ingl%C3%A9s%20o%20nuestro%20servicio,atribuir%20ataques%20o%20amenazas%20a%20trav%C3%A9s%20del%2

Bijker, W. (2005). ¿Cómo y por qué es importante la tecnología? Redes. Universidad Nacional de Quilmes.

Caamaño Fernández, E. E., & Gil Herrera, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. *1*(10), 61-80.

Caro, M. J. (2021). Alcance y ámbito de la seguridad nacional en el ciberespacio. MLA.

Comando de Educación y Doctrina Militar Terrestre. (2010). *Diccionario militar.* Comando de Educación y Doctrina Militar Terrestre.

Comité Interamericano Contra el Terrorismo. (24 de mayo de 2019). Medidas Regionales de Fomento de Confianza en el Ciberespacio. Washington, Estados Unidos.

Cortés Chaves , C., Herrera Álvarez, Ó., Lucero Huertas, J., & Rodríguez Forero, L. (2019). *Un escenario prospectivo de la ciberguerra: la estructura en la ciberdefensa de los Estados unidos.* Escuela de Guerra "General Reyes".

Cortés Cortés, M., & Iglesias León , M. (2004). *Generalidades sobre la Metodología de la Investigación.* Universidad Autónoma del Carmen. https://doi.org/968-6624-87-2

Cubeiro, E. (9 de junio de 2019). “Ciberguerra: Amenazas de un entorno altamente conectado”. *Defensa.com*, págs. 1-2. https://www.defensa.com/ciberseguridad/ciberguerra

De Vergara, E., & Trama, G. (2022). *Operaciones Militares Cibernéticas.* Visión Conjunta.

Del Moral Durán, M., & Clemenceau Figueroa, V. (10 de octubre de 2019). *www.ejemplode.com*. https://www.ejemplode.com/13-ciencia/3449-caracteristicas_de_la_tecnologia.html

Dirección de Planificación y Gestión Estratégica de la FT. (2021). *Plan Estratégico Institucional 2021-2033.* Instituto Geográfico Militar.

Fernández, A. M. (19 de Febrero de 2016). *Orden ministerial de creación del mando conjunto de ciberdefensa de España.* Valencia: Tirant lo blanch.

Fojón Chamorro, E. (septiembre de 2021). *La dimensión cibernética en el ámbito de las fuerzas armadas.* https://www.thiber.org/wp-content/uploads/2019/09/Numero_13_Septiembre_Analisis.pdf

Gazapo, M., & Machin, N. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. UNISCI. https://doi.org/ http://dx.doi.org/10.5209/RUNI.53786

Gibson, W. (1984). *Neuromancer.* Minotauro.

Giget, M. (1998). *La dynamique stratégique de l'entreprise.* Dunod.

Godet, M. (2007). *Prospectiva estratégica problemas y métodos.* Parque empresarial de Zuatzu.

Godet, M. (2007). *Prospectiva Estratégica: problemas y métodos. Cuaderno Nº 20, Segunda edición, 2007.*

Iberdrola. (2022). *Iberdrola.* Ataques cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos: https://www.iberdrola.com/innovacion/ciberataques

Jácome Guerrero, J. (2018). *Proyección de la ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021.* Universidad de Fuerzas Armadas ESPE.

Jiménez, D. (28 de 10 de 2012). *Que aprendemos hoy*. Retrieved 17 de diciembre de 2018, from Que aprendemos hoy: http://queaprendemoshoy.com/el-analisis-pest/

Junta Interamericana de Defensa. (2020). *Guía de ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* JID.

Knoow enciclopedia temática. (03 de Marzo de 2018). https://knoow.net/es/cieeconcom/gestion/estudio-prospectivo/

Latam CISO. (2023). *Perspectivas de ciberseguridad.* https://www.latamciso.com/Report2023SPA.pdf

Marín González, F., Pérez González, J., Senior Naveda, A., & García Guliany, J. (2021). *Validación del diseño de una red de cooperación científico-tecnológica utilizando el coeficiente K para la selección de expertos.* Scielo. Scielo. https://doi.org/http://dx.doi.org/10.4067/S0718-07642021000200079

Mayan, M. (2016). *Essentials of qualitative inquiry.* Routledge. https://doi.org/https://doi.org/10.4324/9781315429250

Ministerio de Defensa de la República de Brasil. (2014). *Doctrina militar en defensa cibernética.* MDN-MD31-M-07.

Ministerio de Defensa Nacional. (2018). *Plan Específico de Defensa Nacional.* Instituto Geográfico Militar.

Ministerio de Relaciones Exteriores de Colombia. (27 de agosto de 2028). *Cancilleria.gov.ec.* https://www.cancilleria.gov.co/international/multilateral/united-nations/itu#:~:text=La%20UIT%20es%20el%20organismo,miembros%20y%20las%20empresas%20operadoras.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Gobierno del Ecuador*. https://www.gobiernoelectronico.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

Mojica, F. (2005). *La construcción del futuro. Concepto y modelo de prospectiva estratégica, territorial y tecnológica.* (e. 1, Ed.) Universidad Externado de Colombia.

Moncayo Gallegos, P. (2012). *Poder y seguridad.* El Conejo.

Monti, R. (1996). *Prospektiker.* Prospektiker.

Moreno Doris, Á. (1994). *Relevancia de las líneas de investigación. una visión desde la Complejidad de las instituciones universitarias.* Revista Venezolana de Enfermería y Ciencias de la Salud. https://doi.org/https://orcid.org/0000-0002-4875-8211

Organización CARI. (2013). https://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Organización de Estados Americanos. (2014). *Convenio de Ginebra y protocolos adicionales.* OEA.

Peiró, R. (14 de octubre de 2020). *Economipedia*. https://economipedia.com/definiciones/trabajo-en-equipo.html

Peralvo, E. C. (2015). *Estudio prospectivo de la ciberdefensa en Fuerzas Armadas del Ecuador.* Universidad de Fuerzas Armadas ESPE.

Pérez, W., & Ramos, M. (07 de septiembre de 2020). *Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas.* https://repositorio.espe.edu.ec/bitstream/21000/23372/1/T-ESPE-044157.pdf

Perozo, E. (2005). El impacto de la gestión tecnológica en el contexto empresarial. En *Revista Venezolana de Ciencias Sociales* (págs. 488-504).

Pimentel, L. (2009). *Introducción al concepto de planificación estratégica.*

Powerdata. (junio de 2022). *Powerdata*. https://www.powerdata.es/seguridad-de-datos

Ramón, M. (19 de noviembre de 2021). *América en movimiento*. https://www.alainet.org/es/articulo/203438

Reguant Álvarez, M., & Torrado Fonseca, M. (2016). *El método Dephi.* https://revistes.ub.edu/index.php/REIRE/article/view/reire2016.9.1916/18093

Reseller Tech&Consulting. (07 de junio de 2023). *IT.* https://www.itreseller.es/seguridad/2023/06/el-cibercrimen-alcanza-un-valor-global-de-un-billon-de-dolares

Sabato, J., & Mackenzie, M. (1982). La producción de tecnología. En I. A. nacionales. Editorial Nueva Imagen.

Schmitt, C. (2013). Responsabilidad del estado por los ciberataques a la infraestructura crítica: violación de derechos humanos.

Scielo. (abril de 2021). https://doi.org/http://dx.doi.org/10.4067/S0718-07642021000200079

Stephenson, N. (1992). *Snow Crash.* Aesteria.

Tesis y masters. (2018). *Qué son las técnicas de investigación*. https://tesisymasters.com.co/tecnicas-de-investigacion/

Universidad Pontificia Bolivariana. (2015). La gestión del conocimiento: modelos de comprensión y definiciones. En *Colección Académica de Ciencias Estratégicas* (págs. 84-111). Palmira.

Wikipedia. (11 de diciembre de 2022). *Ejército del Ecuador*. https://es.wikipedia.org/wiki/Ej%C3%A9rcito_del_Ecuador

Zartha Sossa, J., Montes Hincapié, J., Toro Jaramillo, I., & Villada, H. (2014). *Método Delphi - Propuesta para el cálculo del número de expertos en un estudio Delphi sobre empaques biodegradables al 2032.* Revista Espacios.

Apéndices