ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

Capacidad Militar de Ciberdefensa en los Sistemas de Comando y Control de la Aviación del Ejército, 2022

AUTOR:

BACH. Michael Joseph Latorre Sosaya

(orcid.org/0000-0003-0270-9921)

para optar al Grado Académico de

MAESTRO EN CIENCIAS MILITARES

Con Mención en Planeamiento Estratégico y Toma de Decisiones

ASESOR:

MG. Edgard Eliseo Carmen Choquehuanca

(orcid.org/0000-0003-0841-4403)

LÍNEA DE INVESTIGACIÓN:

Empleo de GUB, GUC, Operaciones GC y GNC

2025

Página Jurado

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 083 – 2025/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veintidós (22) días del mes de diciembre del año dos mil veinticinco, siendo las ..11:14.... horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctor**	**IVAN RICARDO BARRETO BARDALES**	**Presidente**
❖	**Maestro**	**LIZET MILAGROS CACHO DE LA CRUZ**	**Secretario**
❖	**Maestro**	**ROBERTO JOAQUIN VIVANCO BURGOS**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 083-2025/SIE/DGI/ESGE-EPG** del 09 de diciembre de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"CAPACIDAD MILITAR DE CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022"**, presentado por el Bachiller **MICHAEL JOSEPH LATORRE SOSAYA**, para optar el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

Luego de atender la sustentación presencial, defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de ....dieciseis (16.00).....

En mérito del cual, el jurado .....aprueba..... (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones.

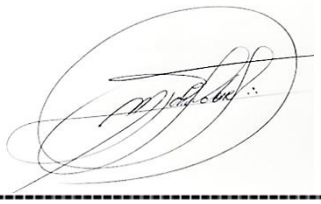
Firmado, en Chorrillos a los veintidós (22) días del mes de diciembre del año dos mil veinticinco.

DR. IVAN RICARDO BARRETO BARDALES	**MG. LIZET MILAGROS CACHO DE LA CRUZ**	**MG. ROBERTO JOAQUIN VIVANCO BURGOS**
PRESIDENTE	**SECRETARIO**	**VOCAL**

Autorización para Publicación y Uso

Con el presente documento, yo Lic. Michael LATORRE SOSAYA faculto a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado la publicidad del texto completo o parcial de la tesis de grado titulada “Capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022.” presentada para optar al grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones en el Repositorio Institucional y en el Repositorio Nacional de Tesis (RENATI) de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), de conformidad al marco legal y normativo vigente. La tesis se conservará permanente e perennemente en el repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada, exhibida y usada también con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Chorrillos, 05 de noviembre del 2023



Michael LATORRE SOSAYA
DNI: 42459772

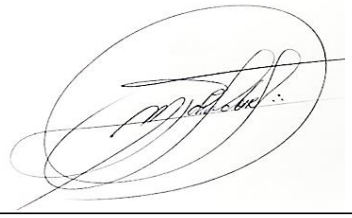
Declaración Jurada de Autoría

Mediante el presente documento, Yo, Bach. Michael Joseph LATORRE SOSAYA, identificado con Documento Nacional de Identidad N° 42459772, con domicilio Jr Riobamba N 1656 SMP, provincia de Lima y departamento de Lima, graduado de la XI Maestría en Ciencias Militares con mencion en Planeamiento Estrategico de la Escuela Superior de Guerra-Escuela de Posgrado del Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG) declaro bajo juramento que:

Soy el autor de la investigación titulada: “Capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022.” que presento a los 17 días del mes de mayo del año 2023, ante esta institución con fines de optar el grado académico de Magister en Ciencias Militares con mencion en Planeamiento Estratégico y Toma de Decisiones.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas y a otros que corresponde al suscrito o a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado y me declaro como el único responsable.



Michael Joseph LATORRE SOSAYA
DNI 42459772

Dedicatoria

Al Glorioso Ejército del Perú y cada uno de sus integrantes por el profesionalismo buscando el bien público vertido a una sociedad valiente. La sed asidua de conocer y aprender en la vida, las amplias ilustraciones adquiridas, desde prolegómeno académico hasta los estudios superiores, somos los artistas del saber, con esfuerzo, dedicación y sacrificio. En el paso fulgente por los campos del arte y ciencia militar, dirimo categóricamente que el éxito radica en la perfección del talento, prodigalidad y la disciplina. A mi venerada familia que son el acicate constante de inspiración.

ÍNDICE

Lista de Tablas

Lista de Figuras

Resumen

Los sistemas de comando y control de la Aviación del Ejército del Perú en la actualidad conllevan a analizar el empleo de las capacidades operativas de ciberdefensa para obtener como solución, una seguridad óptima. Por lo tanto, la unidad de investigación se enfoca en la Aviación del Ejército del Perú, de ahí que, la presente investigación tiene como objetivo, analizar la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército.

Al respecto, la investigación tiene un enfoque cualitativo, de tipo teórico – empírico para abordar las preguntas de investigación, por consiguiente, es Teórico en vista que contaremos con documentación orientada a la capacidad de ciberdefensa y poder establecer el marco teórico adecuado. Por otro lado, será empírico en vista que recolectaremos datos, empleando para ello diferentes herramientas metodológicas, tales como entrevistas, observación y análisis documental. Se debe mencionar que se recurrió como muestra a cuatro (04) expertos en sistemas de comando y control y cuatro (04) expertos en ciberdefensa. Este estudio se elaboró a través de entrevistas al personal que labora en la Aviación del Ejército (AE) y especialistas en ciberdefensa, desarrollándose y estableciendo categorías: sistemas de comando y control (C2), capacidad de ciberdefensa. Por lo tanto, como resultado obtenido de la investigación se desprende de establecer un marco de gobernanza en ciberdedefensa, el cual permitirá establecer una seguridad eficiente en los Sistemas de Comando y Control de la Aviación del Ejército. Del mismo modo, emplear las capacidades operativas de defensa y exploración contando para ello con procesos, personas y tecnologías de ciberdefensa acordes a establecer una seguridad optima en los Sistemas de Comando y Control de la Aviación del Ejército.

Palabras clave: capacidad de ciberdefensa, sistema de comando y control, marco de gobernanza, defensa y exploración.

Abstract

The command and control systems of the Peruvian Army Aviation currently involve analyzing the use of operational cyber defense capabilities to obtain optimal security as a solution. Therefore, the research unit focuses on the Peruvian Army Aviation, hence the objective of this research is to analyze the military cyber defense capacity in the security of the Army Aviation Command and Control Systems.

In this regard, the research has a qualitative, theoretical-empirical approach to address the research questions. Therefore, it is theoretical in view of the fact that we will have documentation aimed at cyber defense capacity and be able to establish the appropriate theoretical framework. On the other hand, it will be empirical since we will collect data, using different methodological tools, such as interviews, observation and documentary analysis. It should be mentioned that four (04) experts in command and control systems and four (04) experts in cyber defense were used as a sample. This study was prepared through interviews with personnel working in the Army Aviation (AE) and the Army Cyber Defense Center (CECIBER), developing and establishing categories: command and control systems (C2), cyber defense capacity. Therefore, as a result obtained from the research, it is clear to establish a governance framework in cyberdefense, which will allow establishing efficient security in the Army Aviation Command and Control Systems. Likewise, use the operational capabilities of defense and exploration, counting on processes, people and cyber defense technologies in accordance with establishing optimal security in the Army Aviation Command and Control Systems.

Keywords: cyber defense capability, command and control system, governance framework, defense and exploration.

Introducción

La importancia de implementar una adecuada seguridad para el sistema de comando y control que posee la Aviación del Ejército, se enfoca en que esta es una dependencia que forma parte de la estructura organizacional del Ejército, por cuanto las actividades propias de la Aviación son altamente remunerativas para este, ya que son vinculantes a las operaciones en cumplimiento a roles estratégicos que desarrolla.

En base a lo antes mencionado, podemos establecer el planteamiento del problema, toda vez que la protección de dicho activo crítico institucional es de sustancial importancia, por esta razón, de suceder un incidente sobre estos sistemas tecnológicos, llevaría consigo la disrupción de los servicios, teniendo un efecto detrimental en las operaciones y acciones militares que desarrolla la Aviación del Ejército. Justificándose que la Aviación del Ejército al poseer una plataforma denominada Blue Sky (sistema de comando y control) siendo prioritario en las operaciones aéreas; empero, representa un potencial riesgo al no tener seguridad digital y física para dicha plataforma. Definiendo como objetivo el analizar la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército.

Es necesario determinar que, en los antecedentes descritos en el marco teórico, muy poco sea investigado desde un enfoque nacional, al respecto se debe señalar que en lo establecido en las bases teóricas; buenas prácticas de ciberseguridad dentro de un marco metodológico, resulta fundamental para la implementación de la capacidad de protección en la seguridad digital de la infraestructura tecnológica de los sistemas de comando y control que posee la Aviación del Ejército, es preciso mencionar que se debe cumplir con estándares tecnológicos sobre las plataformas modernas y necesarias para la Aviación del Ejército, entre las cuales contemplan sistemas de comunicación, sistemas de rastreo satelital, sistemas tráfico aéreo, etc. Por ende, la seguridad de su tecnología radica, por un lado, en una

seguridad perimetral tanto de software y hardware; por otro lado, con procesos adecuados para la respuesta ante los incidentes contando con personal calificado.

Asimismo, al definir una metodología cualitativa, se podrá establecer una contextualización por comprender como es que se produce el fenómeno estudiado. Asimismo, se busca comprender las experiencias, significados y perspectivas de los participantes en su entorno, se debe tener en cuenta que con el crecimiento de las tecnologías, las amenazas también han avanzado desarrollando diseños disruptivos sofisticados, empleando como medio el ciberespacio, un dominio que aún se encuentra en investigación doctrinal desde el enfoque militar, la existencia de ciberamenazas hace que las infraestructuras tecnológicas que posee la Aviación del Ejército puedan ser vulnerable a diferentes vectores de ataque.

Al realizar el análisis y síntesis, se desarrolló la recolección de datos, a través de las herramientas metodológicas como la guía de entrevistas, el análisis documental y guías de observación necesarias para poder establecer una correcta organización de los datos y definición de categorías, estableciendo una triangulación que nos permita obtener una comprensión más completa y rica del fenómeno estudiado, buscando confirmar y validar los hallazgos a través de la convergencia de evidencia.

De los expuesto, podemos establecer que las ciberamenazas en la actualidad son actores definidos como estados, organizaciones, personas que, motivadas con un fin específico, buscan neutralizar, degradar infraestructuras tecnológicas, sabotear y espiar. Afectando con estas acciones, las tecnologías. Ante esta situación el empleo de la ciberdefensa a través de sus capacidades operativas de explotación y defensa se enfocan en dar soluciones en defensa y ciberinteligencia en el ciberespacio, con el fin ulterior de garantizar la funcionabilidad del sistema de C2 de la Aviación del Ejército frente a las amenazas.

CAPÍTULO I: El Problema de Investigación

1.1 Planteamiento del Problema

Los avances tecnológicos debido al IoT (Internet de las cosas) y la IA (inteligencia artificial) propio de la modernización y digitalización de la gestión de procesos de cerrar brechas en un horizonte de tiempos cortos en las organizaciones públicas y privadas; han traído consigo un impacto de inseguridad a nivel internacional, en la región, países como Brasil, Argentina y Colombia han desarrollado esta capacidad e implementado dentro sus Fuerzas Militares, pero todo ello ha comprendido una articulación entre el planeamiento estratégico y la gestión presupuestal en vista que esta capacidad obedece a la adquisición de soluciones tecnológicas y tienen un enfoque basados en escenarios actuales y futuros, todas vez que las ciberamenazas son cada vez más sofisticadas; sin embargo, poder señalar que Brasil es un país que desarrolla soluciones tecnológicas, así como diseña metodologías basados en ciberdefensa, lo que ha permitido situarse como un país que tiene un nivel de madurez en ciberdefensa alto y a su vez poder entregar una seguridad a sus sistemas C2 incluyendo dentro de esta a las operaciones aéreas, Por otro lado, muchas organizaciones privadas y militares en el mundo orientadas a la aeronáutica , han tenido que lidiar con las ciberamenazas y su evolución de una manera exponencial, empleando como medio el ciberespacio, siendo considerado como el quinto dominio, aún desconocido y en exploración.

En el Perú, la aeronáutica militar demanda de tecnologías modernas para el empleo de sus aeronaves con sistemas de comunicación robustos, sistemas de comando y control (C2) fiables e interoperables, que permita un control del tráfico aéreo proporcionando un enlace voz con los pilotos y entre controladores de manera segura, resulta que esta se puede dar a través de un enlace tierra - aire, cuando las aeronaves están en misión de vuelo, así como el enlace tierra - tierra, en las comunicaciones entre los propios controladores de tráfico aéreo militares y civiles, para coordinar gestiones administrativas y actuar alineados a reglas

convencionales ligadas a la aeronáutica como la RAP (Regulación Aéreas Peruana). Los sistemas de comando y control aéreos poseen una complejidad propia de su empleo, por cuanto son sistemas integrados de comunicación de voz, tecnología VoIP, sistemas duales, sistemas de control aéreo, sistemas distribuidores de red, la sinergia de estos sistemas que dispongan de la seguridad adecuada hace posible la operatividad de las aeronaves con el fin ulterior de cumplir con la misión establecida.

La Aviación del Ejército posee un sistema de Comando y Control denominado Blue Sky, por donde se procesa información propia del empleo de sus aeronaves. No obstante, se han identificados diferentes problemáticas en la unidad de investigación, identificando como causas directas, el desconocimiento del empleo de la capacidad de ciberdefensa en la seguridad de los sistemas de comando y control. Al respecto, La prioridad de establecer la protección del sistema de C2, radica en la importancia que asume la Aviación del Ejército dentro de la organización estructural del Ejército, que apoya en operaciones y acciones militares aéreas, acorde con los nuevos roles que ha asumido el Ejército. Sin embargo, el sistema C2 de este importante órgano de Línea, en la actualidad no posee una seguridad adecuada, asimismo se encuentra expuesto frente a las ciberamenazas, el cual tiene como consecuencia la constitución de un riesgo potencial de ocurrir un incidente digital o físico, teniendo como efecto la inoperatividad de las aeronaves por un periodo de tiempo indeterminado, sujeto al vector y magnitud de ataque empleado por la ciberamenaza.

Con referente problemática podemos resaltar que se evidencia la falta de un marco de gobernanza en ciberdefensa, esta inexistencia limita establecer procesos, procedimientos propios de las operaciones de ciberdefensa empleando la capacidades operativas de ciberdefensa, al respecto, se debe señalar que la capacidad operativa de defensa, es la que estructura una seguridad perimetral, empleando para ello tecnología acorde para neutralizar a las ciberamenazas tanto de manera digital como física, dicho empleo radica en la implementación de software tales como: AntiDDOS, Antimalware, Firewall, SIEM, lo que permitirá realizar un análisis de comportamientos anómalos, al mismo tiempo se debe establecer que dentro de la red de la plataforma que compone las tecnologías de la Aviación

del Ejército, no existen tecnologías modernas y sofisticadas materializadas en soluciones acordes a los requerimientos propios de un marco de ciberdefensa, ni a los operacionales. En consecuencia, sin esta capacidad operativa defensiva no se podrá materializar la primera línea defensiva ante ciberataques, en vista que la Aviación del Ejército no posee ninguna medida de seguridad perimetral acorde a las operaciones aéreas.

Por otro lado, la carencia de empleo de la capacidad operativa de explotación dentro de la Aviación del Ejército, limitará realizar operaciones de ciberinteligencia sobre ciberamenazas teniendo como medio el ciberespacio, es por ello, la importancia del empleo de esta capacidad de explotación radica en poder identificar vulnerabilidades, exploit de tipo "Zero day" que puedan ser utilizados frente al sistema Blue Sky y tener como efecto la disrupción del sistema, para ello se debe emplear software de tipo Inteligencia de amenazas, sofisticadas que permita identificar las ciberamenzas de manera oportuna.

Al respecto, el sistema Blue Sky, permite conocer la operatividad continua de las aeronaves, recopilar información de las tripulaciones y de alerta establecidas, la Aviación del Ejército posee aeronaves que utilizan tarjetas madres en las pantallas digitales de la cabina de mando, los cuales son actualizados mediante softwares a través del uso del internet, presentando ello una vulnerabilidad frente a una infección de malware producto de un ciberataque.

La Aviación del Ejército al carecer de estas capacidades operativas antes mencionadas, están expuestas a ciberataques y ciberincidentes, más aún si los softwares que emplean las aeronaves y torres de control en algunos casos se encuentran desactualizados, reflejando también un agravante en vista que en la dark web (red oscura) ofrecen vulnerabilidades de sistema de comando y control de tipo militar y civil, pudiendo ser esta asequible a una ciberamenaza, debemos tener en claro que el término ciberamenaza puede hacer referencia a un estado adversario, organizaciones criminales, personas motivadas con un fin emocional o económico.

Ante ello, es necesario el empleo de la capacidad de ciberdefensa para obtener una óptima seguridad del sistema C2 que dispone la Aviación del Ejército, toda vez que dicha

capacidad se implementó en el Ejército en el año 2018 a través del comando de ciberdefensa con sus tres capacidades operativas: respuesta, defensa, explotación. Sin embargo, para la presente investigación solo se enfocará en dos (02) capacidades operativas: defensa y explotación, dicho empleo se dará a través de una sección de ciberdefensa que se encontrará dentro de la estructura organizacional de la Cía. Com N°800, orgánica de la Aviación del Ejército.

En consecuencia, se hace imprescindible contar con procedimientos, técnicas y tácticas en ciberdefensa dentro de los sistemas C2 de la Aviación del Ejército, ya que, en la actualidad, esta actividad solo se guía con directivas, normas endebles y desactualizadas, carentes de una metodología de ciberdefensa frente a ciberamenazas.

Al respecto, debemos señalar que el manual de procesos de la Compañía de Comunicaciones N°800 (Cía. Com N°800) no hace referencia a las medidas pasivas y reactivas para los ciberincidentes, en base a ello la importancia de poseer una metodología frente a eventos de este tipo. La función general según, la Cía. Com N°800 (2018) “Consiste verificar la eficiencia de los medios de comunicación correspondientes y en caso de deficiencia o desperfectos, realiza las coordinaciones pertinentes para su inmediata solución” (p. 16).

En lo que refiere al Manual de Operación y Funciones (MOF) de la Cía. Com N°800 (2017) “Establece que debe coordinar con la Empresa TESAM PERU S.A.C, respecto a alguna falla en el sistema de monitoreo (Blue Sky), errores de posición u otros, formular el informe si así lo amerita” (p. 14).

A partir de lo antes mencionado se ha podido determinar que la problemática radica en tres (03) aspectos: la carencia de una tecnología acorde a los requerimientos operacionales, asimismo no disponer de personal especialista ante ciberincidentes, así como carecer de procesos, procedimientos definidos para una respuesta oportuna.

De no contar con el empleo de las capacidades operativas de ciberdefensa, cuyos pilares se ven sostenidos en los tres (03) aspectos antes mencionados, existiría una alta probabilidad de ocurrencia de un ciberataque en cual tendría como consecuencia la

inoperatividad de los sistemas de comando y control, por ende, la disrupción de las operaciones aéreas que realiza la Aviación del Ejército, de manera que no se pueda cumplimiento a la misión asignada al Ejército del Perú.

1.2 Justificación de la Investigación

La investigación decanta al propósito del investigador por hacer conocer la notabilidad que representa la protección del sistema de C2 de la Aviación del Ejército a través de las capacidades operativas de ciberdefensa, en la actualidad los sistemas de C2 constituyen un activo informático – tecnológico, para organizaciones dedicadas a la aeronáutica, en lo que refiere a la Aviación del Ejército es una dependencia que dentro de la estructura de organización del Ejército, es órgano de línea que apoya con aeronaves en operaciones aéreas; asimismo, apoya a la Institución para realizar acciones y operaciones militares, acorde con los nuevos roles estratégicos que ha asumido el Ejército.

La Aviación del Ejército al ser una dependencia que comprende de alta tecnología para el abordaje al apoyo conjunto militar y otros medios de apoyo (OMA); por otro lado, actuar enmarcado en el SINAGERD, articulado con el PESEM/PEI del sector. Por la importancia estratégica, ergo, requiere de sistemas de comando y control acorde a sus requerimientos operacionales, como también de personal especialista con procesos tanto como procedimientos con pautas técnicas adecuadas para dar una repuesta oportuna ante incidentes o amenazas cibernéticos.

La Aviación del Ejército al poseer una plataforma definida como Blue Sky (sistema de comando y control) este activo crítico es prioritario en las operaciones aéreas; empero, representa un potencial riesgo al no tener seguridad digital y física para dicha plataforma, esgrimiendo que es el único sistema de C2 que posee la Aviación del Ejército, para ello a través de la capacidad de ciberdefensa implementada en el Ejército del Perú desde el 2018 se propone el empleo de las capacidades operativas de explotación y defensa, para lo cual al tener implementada estas capacidades en la Aviación del Ejército reduciría el riesgo de un incidente cibernético por parte de las ciberamenazas.

Esta investigación se justifica metodológicamente ya que se utilizará métodos y técnicas que servirán para investigaciones futuras. Además, tendrá una justificación práctica en razón que contribuirá con acciones preventivas y reactivas contra irrupciones sobre brechas vulnerables en los sistemas, servidores, proxy, etc. También adscribirá una justificación legal por encontrarse las capacidades militares a investigar enmarcadas dentro de la Ley de Ciberdefensa Nº30999 en vigencia desde 2019. Cabe manifestar que el tema a desarrollar no ha sido indagado por la comunidad científica en el Perú, es por ello que con este estudio se dará un aporte a la metodología en la seguridad del sistema de C2 de la Aviación del Ejército proponiendo el empleo de las capacidades operativas de ciberdefensa.

1.3 Delimitación de la Investigación

La investigación tendrá por localización la provincia de Lima, debido a la recopilación de información en vista que se tiene como referencia la experiencia, observación y estudio de la seguridad del sistema de C2 de la AE y la capacidad de ciberdefensa del Ejército en el año 2022, La delimitación, la cual se produjo durante los meses de enero a diciembre del 2022.

1.4 Limitaciones de la Investigación

Algunas restricciones se darán en el hecho de acceder a los sistemas de C2 de la AE y al Centro de Ciberdefensa del Ejército, ámbitos donde se produce el problema a investigar, estos serán minimizados, puesto a que el investigador ha laborado en la AE como parte de las tripulaciones de vuelo, en adición, se desempeñó en la Cía Com Nº 800, en años anteriores y podrá obtener algunos permisos para ingresar al lugar señalado.

La carencia de trabajos de investigación y personal con experiencia en el tema tratado, dentro de la institución, se podrá minimizar gracias al estudio de otras instituciones.

1.5 Formulación del Problema

Problema 1

¿Cómo se empleó la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022?

Problema 2

¿Cómo el empleo de las capacidades operativas de ciberdefensa mejoraron la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022?

Problema 3

¿Cómo se estableció la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y la normativa de operaciones aéreas de la Aviación del Ejército el año 2022?

Problema 4

¿Cuáles son las tecnologías militares de ciberdefensa que se deben emplear en las operaciones aéreas conjuntas que realiza la Aviación del Ejército?

1.6 Objetivos de Investigación

Objetivo 1

Analizar la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022.

Objetivo 2

Comprender el empleo de las capacidades operativas de ciberdefensa en la mejora de la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022.

Objetivo 3

Analizar la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y normativa de operaciones aéreas de la Aviación del Ejército el año 2022.

Objetivo 4

Conocer las tecnologías militares de ciberdefensa para las operaciones aéreas conjuntas que realiza la Aviación del Ejército.

CAPÍTULO II: Marco Teórico

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Nacionales

Quevedo (2023), en su investigación “Ciberdefensa y ciberseguridad en el Perú” el objetivo general fue de establecer el contexto y desafíos que circunscriben a la capacidad de las FF.AA. para contrarrestar ciberataques que violenten contra la seguridad nacional. Para la configuración de la investigación se estableció un método cualitativo.

El autor concluyó en lo siguiente:

> Que los operadores de tecnología en el Perú han identificado un déficit en ciberdefensa debido a que la ejecución de los procesos o infraestructura tecnológica que fortalecen la protección de información de diferentes entidades sean estos privados como públicos aún son precarios. Esta deficiencia también es parte a la ausencia de amenazas de gran gradación, provocando ello la indolencia respecto a esta trama por parte de los gestores tecnológicos de un estado. En ese sentido, constituye uno de los lances prioritarios para cambiar la situación problemática. En otro orden de cosas, el Perú es considerado como un país que registra un volumen cimero de ataques cibernéticos en la región relacionados a información. (p.70)

La investigación citada se vincula a la planteada en vista que a pesar de los esfuerzos elaborados por la Secretaria de Gobierno Digital y su articulación con las FF. AA, no han sido suficientes dichos esfuerzos, en vista que el desinterés de los decisores en temas presupuestales, pasa por que aún poseemos una tecnología precaria, que no es capaz de identificar ataques avanzados y por ende estos puedan tener un impacto mordaz dentro de las entidades públicos, privadas y dentro de las FF. AA, por el contrario si estas amenazas fueran identificadas con un impacto exponencial en filtración de datos o dañar la imagen de

entidades vulneradas, tendría como respuesta que los decisores sean reactivos y se tome en serio esta problemática.

Carrillo (2020), en su investigación denominada “La ciberdefensa en el sistema de mando y control en la 9a Brigada Blindada, Tumbes” El objetivo fue establecer que las teorías de seguridad y defensa, tecnología y arte militar, están estrechamente relacionados con las operaciones militares y su entorno. Para la presente investigación se estableció un método cualitativo. Asimismo, el diseño fue descriptivo. Empleando técnicas de entrevista, observación y análisis. Al respecto, el autor concluye que los medios digitales son cruciales para comprender el entorno operacional y para llevar a cabo operaciones militares exitosas. La guerra, por lo tanto, se nutre de los grandes avances tecnológicos en los medios digitales y la información, los cuales son la base de los sistemas. Por consiguiente, la investigación referida se relaciona a la propuesta, en vista que establece que los sistemas C2 se soportan en tecnologías disruptivas y que están relacionados con la defensa.

Sevillano (2020), en su investigación “Implementación y optimización de un sistema de comando y control con capacidades de integración e interoperabilidad para el soporte de las operaciones en situaciones de crisis y/o emergencias nacionales” realizado en la región Tiabaya- Arequipa estableciendo como objetivo general el uso de un sistema C2 permite la supervisión, coordinación y control de las maniobras. Para la presente investigación se estableció un método cualitativo. El diseño fue descriptivo. El autor concluyó que el sistema procura capacidades de control en tiempo real y garantiza la gestión adecuada del flujo de información necesario para las unidades involucradas en dichas operaciones. Asimismo, la investigación referida se relaciona a la propuesta en establecer que los sistemas trabajan de manera concatenada y sistemática, buscando la oportunidad de la información necesaria para coadyuvar en la toma de decisiones, para evitar dilemas o nieblas mentales en escenarios discrepantes.

Bruderer (2019), en su investigación “Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial” llevado en Lima-Perú, el objetivo general fue la necesidad de identificar una lista de amenazas de ciberseguridad para dispositivos móviles y

procedimientos, son necesarios para realizar una evaluación continua y oportuna. Para la presente investigación se estableció un método cualitativo. Asimismo, el diseño de investigación fue explicativo. Al respecto, el autor infiere que para precisar el curso actual de la seguridad cibernética de la organización y poder determinar los controles necesarios que faltan implementar para lograr el nivel de protección deseado. En resumen, La investigación referida se relaciona a la propuesta en vista que es necesario contar con un marco gobernanza en ciberdefensa basado en primer lugar con buenas prácticas de ciberseguridad, dentro de ello podemos destacar NIST como el marco que establecerá controles basados en ciberriesgo, por otro lado, las amenazas cibernéticas son sofisticadas con el pasar del tiempo requiriendo para su mitigación de procedimiento basados en buenas prácticas de ciberseguridad.

Carrasco (2019), en su investigación denominada “Capacidad de respuesta del Centro de Ciberdefensa en las operaciones y acciones militares” llevado a cabo en Lima – Perú, objetivo general fue de establecer que el desarrollo de capacidades debe contribuir en las operaciones militares y avalar la seguridad en el uso de sistemas de fuerzas amigas. Para la presente investigación se estableció un método cualitativo, hermenéutico interpretativo. El tipo de investigación teórico - empírico. El autor infiere lo siguiente:

> Para lograr estos objetivos, se deben desarrollar tres capacidades operativas: defensa, explotación y respuesta. La capacidad de defensa debe abarcar acciones preventivas, la capacidad de ciberdefensa debe incluir la habilidad para detectar, reaccionar y recuperarse de posibles ataques, acciones hostiles que puedan estropear la seguridad de la información. Además, la capacidad de explotación es substancial para obtener inteligencia sobre los sistemas adversarios. Por último, la capacidad de respuesta debe contener medidas y acciones que se pueden implementar en caso de amenazas o ataques (p. 63)

Al respecto, de la investigación referida se relaciona a la propuesta que para generar libertad de maniobra en las acciones y operaciones militares y garantizar la seguridad de nuestros sistemas. Por un lado, como medida pasiva en la defensa con implementar en los

sistemas de C2, IDS (sistema de detección de intrusión) posterior al firewall. por otro lado, en la explotación y respuesta con IPS (sistema de prevención de intrusos) como medida reactiva, son aspectos clave en la protección de la información y la garantía de un entorno seguro para el uso de tecnologías en contextos militares.

2.2.2 Antecedentes Internacionales

Indra (2022), en su investigación denominada “mando, control, comunicaciones, computación, ciberdefensa, inteligencia, vigilancia y reconocimiento” llevado a cabo en España, estableció como objetivo general que los sistemas C5ISR de Indra proporcionan al mando militar la capacidad de adquisición de información y la creación de una imagen común de la situación operacional. A todo esto, el autor concluye que estos sistemas son fundamentales para la gestión de operaciones militares en ambientes complejos y diversificados como el ciberespacio, y para la integración de información de diferentes unidades militares y civiles. Además, los sistemas C5ISR permiten la generación de planes y órdenes, y la diseminación de información a diferentes niveles de mando. En conclusión, de la investigación referida se vincula a la presente, toda vez que los sistemas C5ISR de Indra proporcionan información precisa y oportuna para la gestión efectiva de operaciones y acciones militares en entornos complejos y cambiantes, donde la ciberdefensa se desarrolla en un ambiente aún poco estudiado y requiere la máxima colección de información para una toma de decisión pertinente.

Saez (2022) en su investigación “La interoperabilidad y las operaciones aéreas conjuntas en la Fuerza Aérea del Perú” llevado en Perú, objetivo principal fue establecer de qué manera la Interoperabilidad se relaciona con las operaciones Aéreas Conjuntas. Una de las condiciones que se requieren para el empleo del poder militar, se encuentra en la capacidad militar conjunta que las instituciones armadas. A propósito, el autor solventa entonces que el argumento céntrico de la interoperabilidad es exteriorizar que existen acontecimientos que tienen implicancias tanto en la dimensión material como en la virtual. Asimismo, al manifiesta el fortalecimiento de la organización de las operaciones militares a través de una Doctrina Operacional Conjunta de Operaciones Aéreas permitirá el eficiente

cumplimiento de las funciones. En consecuencia, la investigación citada se vincula a la propuesta, el dominio del de la interoperabilidad dentro de las operaciones aéreas conjuntas en vista que estas son necesarias para poder establecer un eficiente C2 entre las aeronaves y las diferentes plataformas tecnológicas.

Córdova y Pérez (2021) en su investigación “La ciberdefensa en los sistemas de información sanitarios militares” llevado en Madrid –España, cuyo objetivo fue establecer que la ciberdefensa como el vínculo de actividades, activas o pasivas, conducentes a robustecer la funcionalidad del ciberespacio en los sistemas de información sanitarios militares. Por consiguiente, el autor infiere que los sistemas de redes, equipos, personal y enlaces a fin de mantener la defensa de la información y asegurar la consecución de las acciones que estas tengan que desempeñar, soslayando que terceros implementen el exploit e irrumpan los sistemas, para utilizarlas al chantaje o vender información en la Deep Web. De manera que podemos decir que la ciberdefensa es una capacidad que establece una serie de tareas de nivel táctico en la cual articulan infraestructuras físicas y digitales, que cada vez son más avanzadas y requieren de un conocimiento calificado de los operadores. En lo que refiere a las actividades pasivas y activas dependerán mucho de la tecnología que se posea, así como del personal que emplee dicha tecnología. En la región la capacidad de ciberdefensa, está dando sus primeros pasos tanto en metodologías adaptadas a la propia realidad de cada país, como sus normativas complementarias que significarán el soporte para sus operaciones.

Cubeiro (2020), en su investigación denominada “Los sistemas de mando y control: una visión histórico prospectiva”. Realizado en España, estableció como objetivo que un sistema de C2, es una herramienta esencial para el mando en la actualidad, ya que puede multiplicar los esfuerzos en el campo de acción. Por esta razón, el autor estableció que un uso inadecuado puede tener efectos aún más negativos que su falta. Los sistemas utilizados hasta hace poco se caracterizaban por su baja en los nuevos escenarios, la interoperabilidad, la flexibilidad y la seguridad son aspectos críticos que deben ser considerados. Por consiguiente, la investigación inferida se vincula a la propuesta puesto que, en perspectiva

cercana, se espera que los sistemas se basen en estructuras distribuidas y dependan de redes comunes para agenciar mayor eficacia y eficiencia. con una amplia variedad de servicios y utilizarán principalmente tecnologías comerciales, aunque a corto plazo no se esperan mejoras significativas en la seguridad, procesamiento de información en vista que se requiere servidores ágiles respaldados contra las amenazas de hackers de sombrero de negro.

JID (2020), en su publicación realizada en la “Guía de ciberdefensa de la JID” llevado en Canadá mencionó que el objetivo principal de las ciberoperaciones es cumplir con la misión y lograr los objetivos deseados. Al respecto, el autor infiere que la fuerza ciberespacial es el conjunto de unidades de las fuerzas armadas, organizadas bajo un mismo mandó único, responsables del planeamiento y la conducción de las operaciones militares en el ciberespacio. Por lo tanto, se enfocan exclusivamente en los efectos en el ciberespacio, sin considerar los efectos físicos. En resumen, la investigación citada se vincula a la planteada en vista que acentúa la importancia de entender que las operaciones conjuntas de ciberdefensa en el ámbito aéreo son un factor importante en vista que articula las capacidades de explotación, defensa a través de la interoperabilidad eficiente y una taxonomía única ante situaciones de ciberataques por parte de agentes hostiles.

2.2 Bases Teóricas

El estudio se sustenta en la implementación de la doctrina de empleo de la ciberdefensa en los sistemas C2 de la Aviación del dentro del Ejército y su concepción propia de las operaciones en el ciberespacio y como está vinculada a la protección de plataformas de C2.

La guerra en WIFI de ciberguerra a wikiguerra: la lucha por el ciberespacio.

Rexton (2014)

Las ciberamenazas son cada vez más avanzadas y transversales a diferentes tecnologías, los sistemas de C2 para operaciones aéreas no son ajenas a los efectos de las ciberamenazas, en vista que las operaciones emplean comunicaciones a través de enlaces de voz data y video, medio por el cual se transmiten diferentes malware con la finalidad de

explotar vulnerabilidades de las tecnologías que emplean las aeronaves del Ejército del Perú, asimismo es muy importante determinar medidas preventivas de seguridad empleando para ello plataformas de software, hardware, procedimientos adecuados como personal especialista para la respuesta a diferentes ciberincidentes. Es por ello que los sistemas C2 articulados con las aeronaves de las fuerzas militares de la región poseen un sistema de seguridad tecnológica apropiado a su sistema C2, en el Perú al analizar la seguridad que ofrece el sistema el C2 del AE se pudo establecer que carece una seguridad digital y de información apropiada en las operaciones al respecto menciona Rexton (2014):

> En relación al ciberespacio y la ciberguerra, existen cinco debates persistentes y diferentes que giran en torno a este nuevo dominio y la manera de abordarlo. Uno de estos debates es quién establece los límites en el ciberespacio. Otro de los debates es la diferencia entre la guerra y el delito. (p. 30)

La ciberseguridad en el ámbito militar. Díaz del rio (2010)

Las plataformas de comando y control así como las tecnologías de hardware y software están vinculadas en su esencia, es por ello que las plataformas de C2 al emplear tecnologías son susceptibles a recibir ciberataques, teniendo en consideración que la Aviación del Ejército son objetivos militares remunerativos y que su disrupción trae como efecto el detrimento de las operaciones y acciones militares, los sistemas de C2 de los ejércitos modernos poseen sistemas cifrados que hacen difíciles la interpretación de las comunicaciones; sin embargo, las ciberamenazas al tener conocimiento que los ataques sobre sistemas de C2 militares con lleva a tener impacto exponencial y que las motivaciones de las ciberamenazas puedan ser de reputación, económico, patriótico o de espionaje, ante esta situación se debe estar constantemente actualizando las tecnologías que forman parte de los sistemas C2. Establece lo siguiente Diaz del rio (2010):

> Al principio, la mayoría de los llamados hackers solían realizar incursiones en las redes por razones intelectuales, buscando notoriedad y popularidad por haber logrado penetrar sistemas importantes a pesar de las medidas de seguridad. Sin embargo, la aparición de la ciberdelincuencia trajo un cambio significativo en las motivaciones de

> los hackers, centrándose principalmente en beneficios económicos obtenidos de manera ilegal. Este problema ha ido en aumento y se ha convertido en una amenaza preocupante. El ciberterrorismo es otra amenaza que ha ganado fuerza en los últimos años debido a su evolución y aumento de actividad. La capacidad técnica de los hackers se ha incrementado considerablemente, y se debe tener en cuenta la posibilidad de que puedan realizar ataques que dañen gravemente elementos de las infraestructuras críticas nacionales. (p. 247)

Por consiguiente, las ciberamenazas constituyen un riesgo cibernético para las organizaciones publica y privadas, cabe detallar que estas se vuelven cada día más disruptiva y cambiante en sus vectores de ataque. Y las organizaciones cada vez más pasivas en el robustecimiento de su seguridad física y digital.

2.3 Categorías y Subcategorías

La implementación de la capacidad militar de ciberdefensa en los sistemas de C2 de la Aviación del Ejército peruano representa un enfoque innovador para mejorar las operaciones de las aeronaves durante las diversas acciones y operaciones militares en las que participan las fuerzas armadas del Perú. por cuanto brinda la seguridad en los tres factores importantes disponibilidad, integridad y confidencialidad, siendo las amenazas en el ciberespacio actores y agentes de riesgo en la explotación de vulnerabilidades sobre las tecnologías aéreas que emplea la Aviación del Ejército del Perú.

2.3.1 Capacidad Militar de Ciberdefensa

En lo establecido en la Ley de Ciberdefensa, define como la capacidad de ciberdefensa “Empleo de conocimientos, habilidades y herramientas para llevar a cabo operaciones en el ciberespacio y asegurar su uso por parte de las fuerzas propias” (Congreso de la República del Perú, 2019, Ley 30999, Capítulo I).

De acuerdo a lo establecido desde el esbozo militar se infiere, que los productos que brinda la fuerza militar se adscriben en operaciones y acciones militares, esgrimiendo en el caso exclusivo de la presente investigación a la Aviación del Ejército. Empleando el

conocimiento del personal, la habilidad, los medios compuestos por hardware y software lo que permitir asegurar el empleo de la fuerza durante las operaciones a realizar.

Para la presente materia de estudio, se realizó un enfoque a las dos (02) capacidades operativas de ciberdefensa: Protección y exploración propiamente, todas vez que las mencionadas capacidades establecerán las seguridad de los sistemas de comando y control de la Aviación del Ejército, Según lo establecido en la Ley de Ciberdefensa define como capacidad de respuesta aquella “Que se encuadra a la seguridad ofensiva de los sistemas de C2, en vista que su ejecución se lleva a cabo con orden del más alto escalón que conducen las operaciones militares” (Congreso de la República del Perú, 2019, Ley 30999, Capítulo I).

En virtud de ello, es necesario señalar la teoría que tiene un enfoque de la ciberdefensa desde la perspectiva de la polivalencia, en primer lugar, la contribución referida al intercambio de información con otros países sobre las diferentes ciberamenazas existentes en el entorno digital, lo que genera un ambiente de confianza entre los diferentes países y de esta manera mejorar las relaciones multilaterales. Por otro lado, tenemos la educación en vista que diferentes países de la región han desarrollado mejores conocimientos, en consecuencia, esto permite mejorar las destrezas del personal a través de la formación. De igual forma en situaciones de catástrofe el Ejército podrá poner a disposición los equipamientos de comunicación, comando y control necesarios para mantener los enlaces necesarios de comunicación en situaciones de emergencia y catástrofe.

El enfoque de tener una visión prospectiva de la capacidad de ciberdefensa basado en la teoría de la polivalencia, conlleva a analizar que el empleo de la capacidad de ciberdefensa no necesariamente se circunscribe al ámbito de las operaciones militares. A propósito, Espina (2020) señala que:

> El Ejército de Chile cuenta con unidades de ciberdefensa, que cristalizan de forma significativa la versatilidad que tienen ciertas capacidades de las FAs para contribuir en tareas más allá del ámbito de la defensa. Incluso, el actuar de la ciberdefensa se ve beneficiado al operar en las diversas áreas de misión, ya que no se produce un cambio significativo en sus roles, respecto de lo que constituye su orientación

> principal. Se estima que estas razones, sustentan claramente la necesidad de continuar desarrollando las capacidades de ciberdefensa con que cuenta el Ejército de Chile, las que son fundamentales para enfrentar los desafíos que imponen los cambios en el ambiente operacional. (p. 62)

Como resultado de lo cual, se establece que algunos países ven a la ciberdefensa con un enfoque de polivalencia, permitiendo de esta manera tener capacidades mucho más versátiles. asimismo, se debe señalar que un factor limitante en el mejoramiento de equipamiento de ciberdefensa, es la carencia de asignación presupuestal, ante ello tener un enfoque de polivalencia de la ciberdefensa, coadyuva a tener factores posibilitantes a la asignación presupuestal y que contribuya de manera óptima a tener una capacidad de ciberdefensa con sostenibilidad de mejora continua permanente.

El Ciberespacio. Según el Consejo de Seguridad Nacional de España (2019) afirmó lo siguiente:

> El espacio digital se presenta como un escenario de conflicto en el que la información y la privacidad de los datos son activos de gran importancia en un contexto de mayor rivalidad geopolítica, cambios en el poder y empoderamiento del individuo. En este sentido, la creciente interconexión y la mayor dependencia de las redes y sistemas, así como de dispositivos y componentes digitales, generan debilidades que dificultan la protección adecuada de la información. (p. 8)

Establece la preponderancia a la información y privacidad de los datos como activos de alto valor en un entorno, dentro del ambiente operacional de la Aviación del Ejército el ciberespacio se configura como el medio en el cual se operativiza el enlace de los sistemas C2 tanto físico, lógicos y humanos.

En su investigación denominada Operaciones del Ciberespacio y guerra electrónica, estableció Waden (2019):

> El espacio digital no se limita por fronteras geográficas o geopolíticas y está estrechamente relacionado con la gestión y funcionamiento de infraestructuras vitales, así como a la realización de actividades de comercio, gobierno y defensa nacional. La

> disponibilidad de acceso a Internet y otras áreas del ciberespacio permite a los usuarios tener un alcance operativo y la capacidad de afectar directa o indirectamente la integridad de las infraestructuras críticas, todo ello sin necesidad de estar físicamente presentes. Sin embargo, estos mismos avances también han llevado a una mayor exposición a vulnerabilidades y una crítica dependencia del ciberespacio. (p. 1)

En resumen, el acceso a internet significa en la actualidad un camino de riesgos en vista que dicha accesibilidad puede ser aprovechada por amenazas para causar disrupción sobre activos físicos y lógicos por cuanto requieres de una adecuada gestión de buenas prácticas de ciberdefensa.

Tecnología Militar de Ciberdefensa. La tecnología militar constituye el equipamiento con el cual una fuerza pondrá en marcha su estrategia para el cumplimiento de sus diferentes objetivos militares, el empleo de tecnologías moderniza una fuerza militar, permite efectividad, disuasión y ventaja sobre su enemigo.

Efectivamente, la digitalización ha revolucionado las capacidades militares al permitir una mayor eficacia y diversidad de capacidades. Esto se evidencia especialmente en la aparición de nuevos dominios como el cibernético y el espectro electromagnético, que se suman a los tradicionales como el terrestre, marítimo y aéreo. La integración de estos diferentes dominios en una estrategia coordinada se conoce como multidominio, lo que permite a las fuerzas armadas operar de manera más efectiva y adaptarse a los desafíos contemporáneos. (Fojon, 2019).

Capacidades Operativas de Ciberdefensa. Se define como aquellas capacidades que permiten ejecutar las tareas de ciberdefensa en el desarrollo de operaciones (CEEAG, 2017).

Capacidad Operativa de Defensa. Esta capacidad define las medidas operativas adoptadas para certificar la seguridad, configuración, operación, extensión, mantenimiento y apoyo del ciberespacio, con el fin de crear y custodiar la confidencialidad, disponibilidad e integridad de los sistemas de C2 de la Aviación del Ejército. (CEEAG, 2017).

Capacidad Operativa de Explotación. Según la JID (2020) esta capacidad operativa que hace referencia a las actividades para obtención, análisis de información de las redes internas, así como sobre las redes el adversario, con la finalidad que sean las actividades preparatorias para las operaciones de defensa y respuesta. A través de esta capacidad operativas podremos realizar inteligencia de ciberamenazas, alertas tempranas.

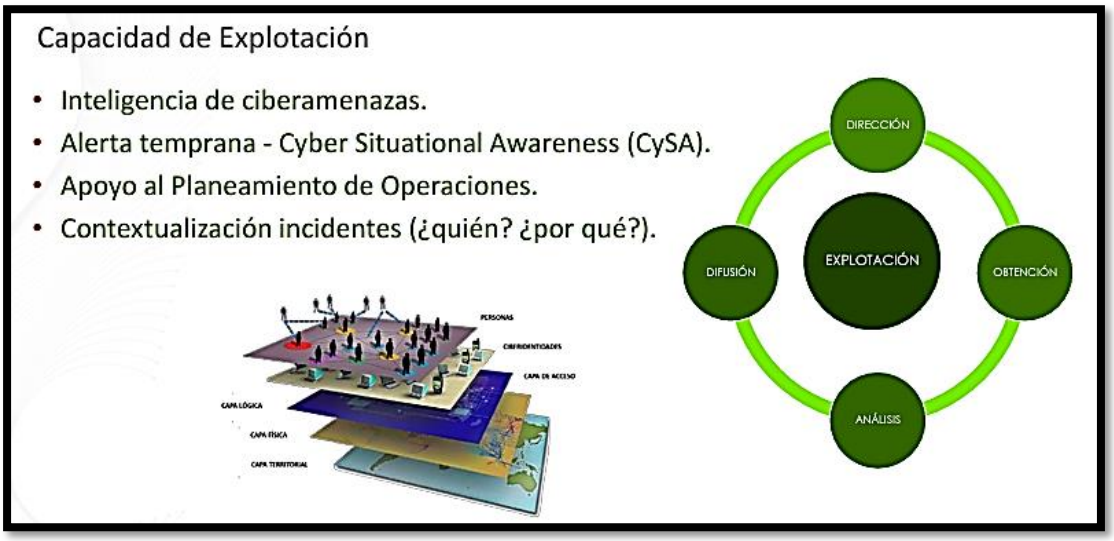
Herramientas Empleadas. Técnicas de OSINT (Inteligencia de fuente abierta): procesos que tiene por finalidad recolectar información pública a través de:

- Motores de búsqueda: obtener información a través de diferentes motores y/o buscadores tales como Google, Bing y otros, a ello también se le denomina Google hacking y doxing, asimismo existe un buscador denominado shodan cuya finalidad identificar sistemas informáticos conectados al internet, también la búsqueda la podemos realizar a través de la darkweb, Deep web y obtener información que no está indexada.
- Redes sociales: redes que la mayoría de personas utilizan a través de esta podemos obtener información de nuestros objetivos.

Existen herramientas tales como: OSINT Framework, Sherlock que permite realizar búsqueda por nombres, Foca que nos permite extraer metadatos, the harvester obtener direcciones de correos, así como subdominios, Maltego a partir de nombres teléfonos permite obtener gran cantidad de información.

Figura 1

Capacidades de explotación



Nota. *Adaptado de* la figura muestra las c*apacidades de explotación manual* de ciberdefensa. de JID, 2019, JID (https://www.jid.org/ciberdefensa-2/).

Marco de Gobernanza en Ciberdefensa

Metodología de Ciberdefensa Basado en NIST. La moldura de ciberseguridad del NIST (NIST CSF) consigna patrones, modelos y conspicuas prácticas que ayudan a las organizaciones a optimizar su gestión del riesgo de ciberseguridad.

Figura 2

Framework NIST

Marco básico (Framework Core)	Niveles de implementación del marco (Framework Implementation Tiers)	Perfiles del marco (Framework Profiles)
Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el de implementación/operación. El Framework Core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.	Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa.	Los perfiles se emplean para describir el estado actual (Current Profile) y el estado objetivo (Target Profile) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

Nota. Adaptado de *marco básico, el perfil del marco y los niveles de implementación*, de NIST, 2022, NIST (https://www.nist.gov/).

NIST Cybersecurity Framework incluye funciones, categorías, subcategorías y referencias informativas.

Las funciones del Marco de Ciberseguridad del NIST proporcionan una visión general mejores prácticas. Es importante tener en cuenta que estas funciones no son un conjunto de pasos de procedimiento, No se trata de una acción única, sino de una serie de medidas que deben implementarse constantemente para atizar la cultura operativa que aborde los riesgos cambiantes de la ciberseguridad. Las categorías y subcategorías proporcionan planes de acción específicos para departamentos o procesos dentro de una organización. Estos planes de acción son más detallados y permiten su aplicación de manera más efectiva en un contexto organizativo. Juntas, las funciones, categorías y subcategorías son componentes fundamentales del contexto de Ciberseguridad del NIST, que ayuda a las organizaciones a llevar a cabo una estrategia completa de seguridad informática.

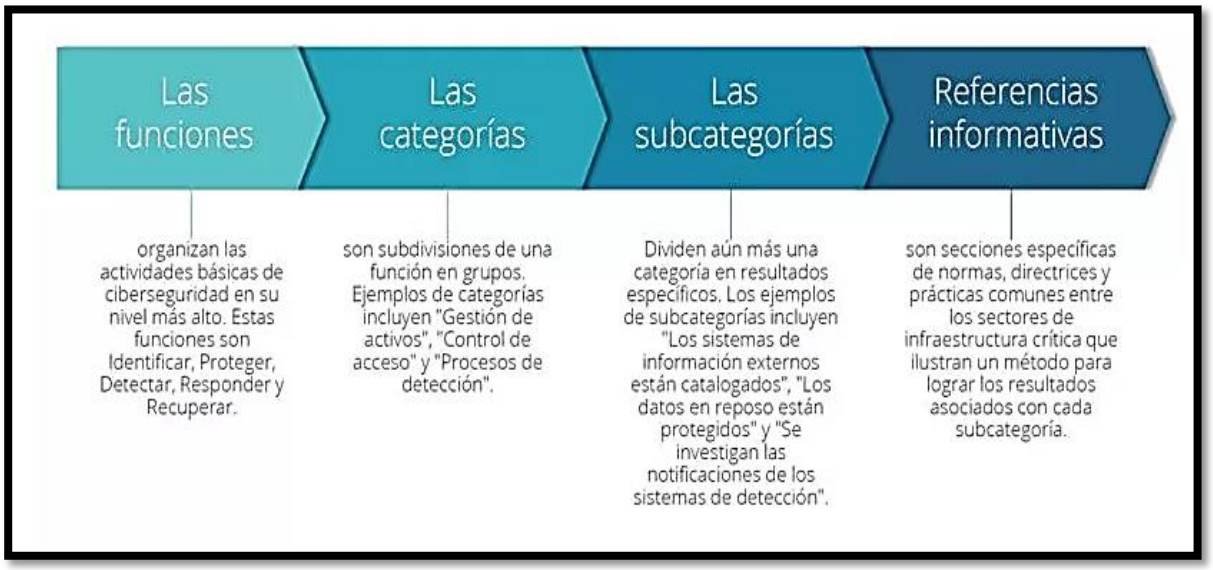
Funciones y Categorías NIST Incluyen lo Siguiente:

Identificar. Con el fin de prevenir los ataques cibernéticos, es fundamental que el equipo de ciberseguridad tenga una comprensión detallada de los recursos y activos críticos institucional. Dentro del ámbito de identificación, el Contorno de Ciberseguridad del NIST abarca una variedad de categorías que deben ser consideradas por las organizaciones. Estas categorías envuelven la gestión de activos, el entorno empresarial, la gobernanza, la evaluación de riesgos, la estrategia de gestión de riesgos y la gestión de riesgos en la cadena de suministro. Cada una de estas categorías ayuda a los equipos de ciberseguridad a identificar los activos y capitales más valiosos de la organización y a tasar los posibles riesgos y amenazas cibernéticas a los que pueden enfrentarse.

La función de identificación resulta fundamental para desarrollar una estrategia sólida de ciberseguridad y proteger a la organización de eventuales ataques (NIST, 2019).

Figura 3

Funciones NIST



Nota. Adaptado de *las f*unciones de Framework. de NIST, 2022, NIST https://www.nist.gov/).

Proteger. La función de proteger en el marco del NIST Cybersecurity Framework se enfoca la función de establecer controles de seguridad físicos y técnicos tiene como objetivo desplegar y llevar a efecto las medidas adecuadas para proteger la infraestructura crítica.

Según NIST (2019) en esta función, se identifican diferentes categorías que abordan aspectos específicos, tales como la gestión de identidad y control de acceso, la concientización y capacitación en ciberseguridad, la seguridad de datos, los procesos y procedimientos de protección de la información, así como el mantenimiento y la tecnología de protección. Todas estas categorías proporcionan un enfoque concreto para establecer medidas de seguridad que resguarden los sistemas y activos críticos institucionales.

Detectar. La función de detección se enfoca en establecer medidas que permitan a una organización detectar posibles ciberataques. Dentro de esta función, las categorías corresponden a los métodos específicos utilizados para identificar posibles amenazas, como el rastreo de anomalías y eventos, así como el monitoreo constante de la seguridad y los procesos de detección de ataques, son actividades importantes en la estrategia de ciberseguridad de una organización.

Según NIST (2019) estas acciones permiten identificar posibles amenazas o ataques en tiempo real y tomar medidas raudamente para salvaguardar los sistemas y activos críticos. En resumen, esta función busca asegurar que cualquier actividad malintencionada en el sistema sea identificada y manejada de manera oportuna.

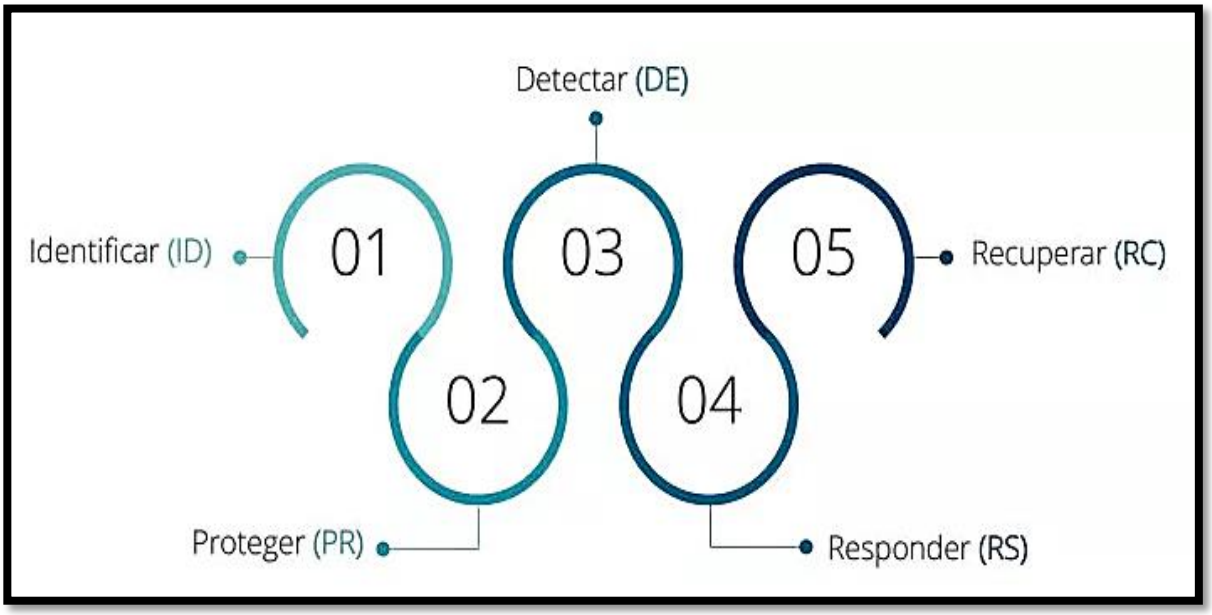
Responder. Al respecto NIST (2019) establece que las categorías dentro de la función de respuesta se enfocan en asegurar que se tenga una respuesta efectiva ante eventos relacionados con la ciberseguridad. Estas categorías específicas incluyen planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

Recuperación. La función de recuperación en el Marco de Ciberseguridad del NIST se concentra en la capacidad de la organización para recuperarse y mantener la continuidad del negocio en caso de un evento de ciberseguridad. Las actividades de recuperación incluyen la planificación de recuperación y las comunicaciones mejoradas. Además, las referencias informativas del NIST CSF establecen una conexión directa entre las funciones,

categorías y subcategorías con los controles de seguridad específicos de otros marcos, como el CIS Controls® del Center for Internet Security (CIS) y COBIT 5, la Sociedad Internacional de Automatización (ISA) 62443-2-1:2009, ISA 62443-3-3:2013, la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional 27001:2013 y NIST SP 800-53 Rev.

Figura 4

Proceso de ciberseguridad



Nota. Adaptado de *framework del proceso de ciberseguridad*. de NIST, 2022, NIST (https://www.nist.gov/).

Según NIST (2019) en el marco del NIST CSF, no se especifica cómo llevar a cabo el inventario de los dispositivos y sistemas físicos, ni tampoco se proporciona una guía detallada sobre cómo inventariar las plataformas y aplicaciones de software. En su lugar, el marco ofrece una lista de verificación de tareas que deben ser completadas para garantizar la ciberseguridad de la organización.

Cada organización es libre de elegir su propio método para realizar el inventario de acuerdo a sus necesidades de ciberseguridad. Si se necesita una orientación adicional, se puede indagar sobre las reseñas informativas relacionadas con los controles de seguridad en

otras normas agregadas. En resumen, el NIST CSF brinda una gran flexibilidad para que las organizaciones se adapten a sus necesidades específicas de ciberseguridad.

Niveles de Implementación del Marco NIST. Para ayudar a las organizaciones del sector privado a medir su progreso hacia la implementación, el marco identifica cuatro niveles de implementación:

Nivel 1. La organización tiene un conocimiento general del NIST CSF y es posible que haya aplicado algunos controles de seguridad en ciertas partes de su infraestructura. Sin embargo, la implementación de medidas y procedimientos de ciberseguridad ha sido más bien reactiva que planificada. Además, La empresa posee un conocimiento reducido acerca de las amenazas de seguridad cibernética y no cuenta con los procedimientos y recursos propicios para asegurar el resguardo de la información.

Nivel 2. La organización tiene un mayor conocimiento de los riesgos de ciberseguridad y comparte información de forma no formal. Sin embargo, aún no cuenta con una gestión de riesgos de ciberseguridad establecido y planificado que pueda aplicarse en toda la organización de forma proactiva y repetitiva. En otras palabras, aunque la organización está más informada sobre los riesgos de ciberseguridad, aún no ha desarrollado un enfoque sistemático y estratégico para gestionar y mitigar estos riesgos en toda la organización.

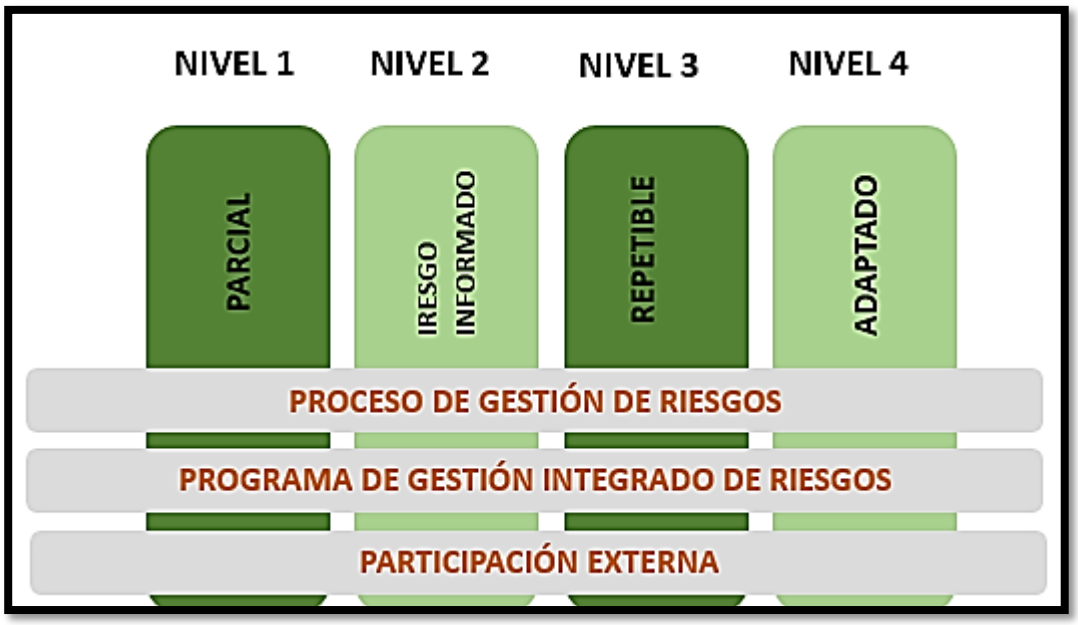
Nivel 3. Repetible: En detalle, la organización y sus altos ejecutivos tienen un alto nivel de conciencia de los riesgos de ciberseguridad. Han establecido un plan de gestión de riesgos de seguridad informática que puede ser aplicado en las diversas áreas y procesos de la compañía de manera planificada y constante. El personal a cargo de la ciberseguridad ha creado un plan de acción detallado que les permite monitorear y responder de manera efectiva a los ataques cibernéticos, lo que les permite reducir el impacto y minimizar el daño.

Nivel 4. Adaptativo: La organización ha logrado un alto nivel de resiliencia cibernética al implementar tecnologías y prácticas de ciberseguridad avanzadas, además de utilizar información predictiva para prevenir ataques cibernéticos. El equipo de ciberseguridad está en constante evolución La organización ha emprendido medidas para aumentar la seguridad y está en capacidad de responder rápidamente ante nuevas amenazas. Hay un compromiso

generalizado dentro de la empresa hacia la gestión de riesgos de seguridad de la información, con políticas, procesos y procedimientos que tienen en cuenta los riesgos existentes. Además, la diligencia de los riesgos de seguridad cibernética se ha incorporado en las decisiones presupuestarias y la cultura organizacional para garantizar que la organización sea adaptable ante posibles amenazas de ciberseguridad.

Figura 5

Niveles Framework NIST



Nota. Adaptado de *La figura muestra* el framework consta de cuatro niveles. de NIST, 2022, NIST (https://www.nist.gov/).

El NIST CSF ofrece una estructura minuciosa para instituir o corregir, se trata de un programa perfilado para la gestión de riesgos de seguridad cibernética, que ofrece un método estructurado y detallado para orientar a las organizaciones en la admisión seria de prácticas de gestión de riesgos sólidas y efectivas.

Priorizar y alcance:

En el proceso de establecer un programa según NIST, es importante crear una visión clara del alcance del proyecto y determinar las prioridades. Esto implica establecer los objetivos comerciales o de misión de alto nivel de la organización, identificar sus necesidades

comerciales y determinar su tolerancia al riesgo. Todo esto ayudará a la organización a tener una idea clara de los riesgos que enfrenta.

Orientar. Este paso implica realizar una evaluación y resulta primordial reconocer los riesgos con el propósito de identificar fortuitas coacciones y vulnerabilidades capaces de afectar los activos y sistemas. Posteriormente, se adoptarán e poner en efecto las medidas de seguridad pertinentes para contrarrestar los riesgos detectados, y se llevará a cabo una supervisión continua para comprobar la eficacia de dichas medidas. Este procedimiento de gestión de riesgos adquiere una relevancia vital para garantizar la seguridad cibernética y resguardar los activos y sistemas críticos institucionales, se debe identificar las regulaciones y leyes que puedan aplicar a la organización y las amenazas potenciales que puedan enfrentar. Se debe tomar en cuenta el enfoque de riesgo de la organización y cómo este afecta la identificación y gestión de amenazas. El objetivo de este proceso es erigir fundamentalmente una imagen completa del panorama de riesgos para la organización.

Cree un Perfil Actual. Un perfil actual se refiere a una evaluación que muestra cómo la organización está manejando el riesgo de ciberseguridad en el momento actual, basado en las categorías y subcategorías establecidas por el CSF. En otras palabras, es un análisis que describe la postura actual de la organización, el perfil vigente se puede emplear como punto de partida para determinar las áreas que requieren mejoras en acciones para tratar los riesgos detectados.

Realice una Evaluación de Riesgos. Una evaluación cuidadosa del entorno operativo, es importante tener información actualizada sobre los riesgos de seguridad cibernética, incluyendo aquellos emergentes, para poder evaluar la probabilidad y la gravedad de un aleatorio evento de seguridad cibernética que pueda impactar a la organización. Luego, se debe establecer un perfil objetivo que represente las metas en cuanto a la gestión de riesgos.

Crear un Perfil Objetivo. evaluar el cumplimiento de las iniciativas de ciberseguridad implementadas.

Determine, Analice y Priorice las Brechas. Cuando se detectan las diferencias el análisis comparativo entre el perfil actual que habilitará identificar las áreas que requieren mejoras en la gestión de riesgos. A partir de esto, el equipo de seguridad de la información podrá incluir hitos específicos y recursos necesarios, como personal, presupuesto y tiempo, para afrontar las brechas y optimizar la gestión de riesgos de la organización. Este plan de quehacer puede ayudar a la organización a progresar de manera efectiva hacia el perfil objetivo.

Implementar el Plan de Acción. Implementar el plan de acción definido en el paso 6.

2.3.2 Sistema de Comando y Control en la Aviación Militar

Sistema de Comando y Control Militar. Según Cabello (2001) señaló que este concepto se refiere a grupos de componentes que trabajan juntos para proveer al mando información relevante y actualizada sobre la situación, lo cual es fundamental para tomar decisiones, dar órdenes y supervisar su cumplimiento. Estos conjuntos de elementos están interconectados entre sí y desempeñan las acciones necesarias para lograr este objetivo en un plazo adecuado.

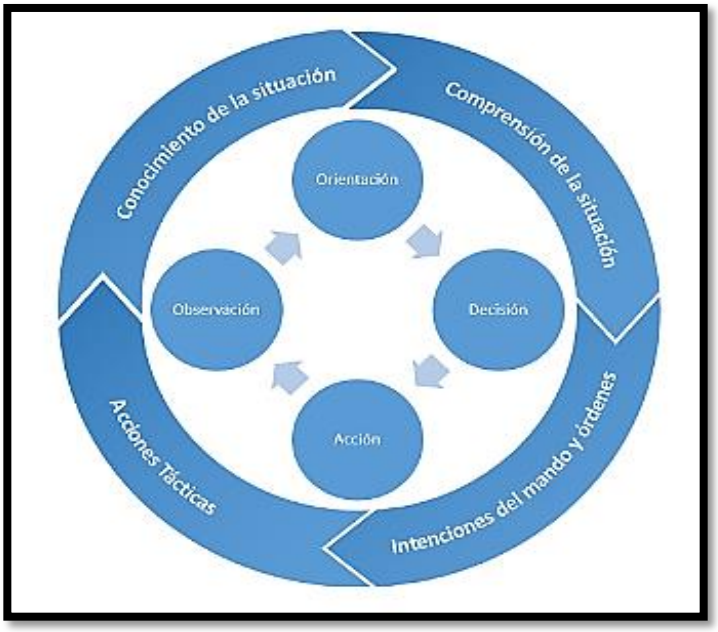
Un sistema de mando y control debe desempeñar un papel importante en:

- Adquirir información relevante para la situación.
- Procesar, analizar, sintetizar, visualizar y distribuir la información de manera efectiva tanto dentro de la estructura de mando como hacia afuera.

Se puede decir que un sistema C2 tiene como objetivos principales la planificación y a toma de decisiones, la comunicación de los subordinados y el seguimiento constante de la situación conforme se obtuvieron nuevos datos y la situación se desarrolla, son componentes clave. En su forma más completa, el sistema de mando y control (C2) comprende centros de mando, sensores y sistemas de información y comunicación. No obstante, en muchos contextos, el vocablo se esgrime específicamente para referirse al sistema de información.

Figura 6

Ciclo de comando y control



Nota. Adaptado de *la figura muestra el c*iclo de comando
y control, de U.S Army, 2019 U.S Army (https://www.army.mil/).

En la fase final del ciclo de gestión (Acción), Una tarea crítica en el ciclo de mando y control es la transmisión de órdenes, su capacidad de velocidad y conexión. Además, a lo largo de todo el proceso, el sistema debe asegurarse de que la información sea segura y confiable para garantizar una toma de decisiones efectiva esté protegida contra posibles ataques de las ciberamenazas para explotarla o destruirla.

Un sistema estratégico tiene como objetivo proporcionar información oportuna a los mandos de nivel estratégico en situaciones de conflicto, así como alertar y concertar a nivel nacional e internacional. Debido a su importancia, es fundamental que esté protegido adecuadamente su operatividad.

En el ámbito de la guerra, los sistemas tácticos desempeñan un papel fundamental al conectar diversos sistemas de armas y brindar a los líderes tácticos los recursos necesarios para dirigir sus fuerzas en tiempo real durante el combate. No obstante, tanto en el campo de batalla como en el ciberespacio, la principal meta de ambos bandos consiste en obstaculizar o impedir el ejercicio del mando y control por parte del oponente.

Para lograr este objetivo, se lleva a cabo la Guerra de Mando y Control (C2W), que tiene dos vertientes: la ofensiva y la defensiva. En la vertiente ofensiva, se pueden usar diferentes acciones, desde la destrucción física de elementos clave de los sistemas de mando, hasta la inserción de virus informáticos, en cuanto a las acciones ofensivas, se busca degradar, anular o manipular la información del adversario. Por otro lado, en el ámbito defensivo, se centra en resguardar las instalaciones, asegurar la información, implementar contramedidas de inteligencia y aplicar medidas de protección electrónica. para proteger el propio ciclo de decisión y dificultar el del adversario. En resumen, la C2W es una guerra que busca impedir el ejercicio del mando y control de la ciberamenaza, incluyendo el uso de acciones físicas o cibernéticas, tanto en objetivos ofensivos como defensivos.

Aviación del Ejército. Dentro de la organización de la Aviación se encuentra la Cía Com Nª800 responsable de establecer los enlaces de comunicaciones propios de la Aviación del Ejército dentro de dicha organización de la compañía, opera la sección Torre de Control tiene como función la de controlar el movimiento de aeronaves en superficie (plataforma) embarque, carga, descarga, de material y personal, mantenimiento, abastecimiento de combustible (recarga) de las aeronaves. Así como la conducción del curso de habilitación y recurrente para los Controladores de Tráfico Aéreo

Dentro del proceso de operaciones de la Torre de Control se identificó tres (03) procesos:

- Plan de vuelo
- Meteorología
- Remolque de aeronaves

Sin embargo, estos procesos se realizan de manera insegura al existir enlaces de comunicaciones no cifrados que emplean como medio el ciberespacio, representando ello una vulnerabilidad frente a las ciberamenazas.

Torre de Control. El jefe de la TWR HALCÓN dicta disposiciones para el funcionamiento correcto control de la navegación aérea. Dirige y controla la recepción y transmisión de los planes de vuelo local y nacional a la dependencia de Planeamiento

CORPAC (ARO) e informaciones requeridas por las tripulaciones. Asimismo, supervisa las actividades de su sección para el estricto cumplimiento de los procedimientos a adoptar. Mantiene una coordinación con las tripulaciones aéreas, sobre el encendido de motores y puesta en marcha previo al rodaje a fin de ser transferidos a las dependencias de control de tránsito aéreo CORPAC (Lima superficie/Autorizaciones. Efectuado las coordinaciones con las tripulaciones, el control local (CTA de Servicio de Torre Halcón), se mantendrá informado sobre el desarrollo del vuelo y arribo de la aeronave al aeródromo y/o aeropuerto de destino e informará a las autoridades militares autorizadas a recibir dicha información. Terminado el vuelo de la aeronave (Despegue, arribo y retorno si los hubiese), procederá a consolidar toda la información en el registro del operador (en una computadora con puertos de libre acceso al personal, sin un óptimo antivirus o software de encriptación de datos), solicitando el reporte final de las operaciones al comandante de aeronave o a su representante.

Representando la torre de control una infraestructura crítica para las operaciones aéreas, el no tener implementado un sistema C2 con una seguridad acorde a los requerimientos operacionales proporciona a las ciberamenazas que puedan ocasionar la disrupción de las operaciones.

En la actualidad todos estos procedimientos se llevan a cabo de una manera desfasada tecnológicamente.

Normativa de Operaciones Aéreas

Normativa ICAO. La Organización de Aviación Civil Internacional (ICAO) ha instaurado una serie de regulaciones para certificar la seguridad de las operaciones. La torre de control de la Compañía de Comunicaciones Nº800, utiliza estas regulaciones como referencia para asegurar la seguridad en sus operaciones. Sin embargo, debido a que la compañía no tiene una plataforma interoperable, se dificulta la aplicación coherente y adecuada de las regulaciones de ICAO en todas sus operaciones.

Según el documento 4444 de la Organización Aviación Civil Internacional (1997) estableció lo siguiente:

> Que la entidad encargada del Servicio de Tránsito Aéreo (ATS) llevará a cabo un análisis exhaustivo. Deberán generarse informes periódicos acerca del estado de los sistemas y equipos de comunicaciones, vigilancia y demás elementos pertinentes para la seguridad en las instalaciones y sistemas del Servicio de Tránsito Aéreo (ATS). Esto incluye reportar cualquier fallo o daño que pueda afectar negativamente la seguridad y detectar patrones en el funcionamiento de estos sistemas. (p. 2)

Se realiza una evaluación continua del funcionamiento normal verifica que los sistemas y equipos de comunicaciones, navegación, vigilancia y otros elementos relevantes para la seguridad cumplan con los requisitos en condiciones normales. de fiabilidad y disponibilidad establecidos por la autoridad competente. Se debe contar con medidas de detección temprana de fallas y deterioro en el sistema, incluyendo documentación sobre las consecuencias de las mismas y procedimientos para su control y solución. También se deben considerar factores importantes como el tipo de comunicación aire-tierra y el tiempo de diálogo, así como la capacidad del controlador para intervenir todas estas medidas de seguridad.

Dentro de las competencias de las torres de control de un aeródromo que establece la Organización Aviación Civil Internacional (ICAO) de 1997 señala que el propósito principal de las torres de control de aeródromo es asegurar un tráfico aéreo seguro y eficiente, a través de la entrega de información y autorizaciones a las aeronaves bajo su jurisdicción. Este objetivo se logra para evitar colisiones en situaciones diversas, como entre aeronaves dentro del espacio designado, las que se mueven en la zona de maniobras, aquellas que aterrizan y despegan, vehículos en movimiento y cualquier obstáculo en el entorno. La función de control de la torre de aeródromo es fundamental para mantener el orden y prevenir accidentes en el aeropuerto y sus alrededores.

La principal función de las torres de control de aeródromo consiste en evitar la colisión de múltiples aeronaves y vehículos que operan en diferentes zonas del aeropuerto. Esto implica no solo las aeronaves que vuelan dentro del ámbito de responsabilidad de la torre de control, sino también aquellas que se encuentran en la fase de maniobras, aterrizando o

despegando. Además, se busca prevenir choques entre aeronaves, vehículos y obstáculos presentes en el área de responsabilidad aplicando la gestión de tránsito aéreo (ATM). Para lograrlo, la torre de control proporciona información y autorizaciones a las aeronaves que están bajo su supervisión. con el fin de asegurar un tráfico aéreo seguro, eficiente y organizado en el aeropuerto y sus alrededores.

Servicios de Vigilancia ATS

Capacidades de los Sistemas de Vigilancia ATS. En cuanto a la capacidad de los sistemas de vigilancia ATS, Es importante que sean altamente confiables, disponibles e íntegros para proporcionar servicios de tránsito aéreo de manera efectiva. importante minimizar la probabilidad de fallas del sistema o degradaciones significativas para evitar interrupciones totales o parciales de los servicios. Estos sistemas generalmente están compuestos por varios elementos integrados.

Además, es crucial que los sistemas de vigilancia ATS puedan integrar los datos con diferentes sistemas automatizados utilizados en la prestación de servicios ATS.

Los Estados deben asegurar establecimiento de procedimientos de coordinación automatizados basados en acuerdos regionales de navegación aérea.

Comunicaciones. La fiabilidad y disponibilidad deberán ser tan altas que las posibilidades de fallas o degradaciones importantes sean extremadamente bajas. Se deberán proveer instalaciones de reserva adecuadas para asegurar que el servicio de comunicaciones no se interrumpa.

Empleo del Sistema de Vigilancia ATS en el Servicio de Control de Tránsito Aéreo. Los sistemas de vigilancia ATS brindan información que puede ser utilizada para diversas funciones en la prestación de servicios de control de tráfico aéreo implica llevar a cabo diversas funciones. Algunas de estas responsabilidades asegurarán una separación adecuada entre las aeronaves, gestionarán el flujo continuo del tráfico en situaciones de fallas de comunicación, optimizarán la eficiencia del espacio aéreo y disminuirán los retrasos, así como proporcionarán rutas y perfiles de vuelo óptimos con el objetivo de renovar la seguridad y mantener la vigilancia del tráfico aéreo y brindar información detallada sobre la posición de

las aeronaves bajo control, así como información adicional sobre otros tráficos y desviaciones importantes que puedan afectar la seguridad. Además, estos sistemas permiten el seguimiento de rutas autorizadas y niveles de vuelo, lo que ayuda a prevenir errores de coordinación entre el controlador y el piloto.

Transmisión de la Información. La autoridad responsable decidirá cómo se difundirá la información a las aeronaves, pudiendo utilizar uno o varios de los siguientes medios:

- Transmitir la información directamente a la aeronave, asegurándose de recibir una confirmación de recepción.
- Hacer una llamada general a todas las aeronaves interesadas, sin necesidad de confirmación de recepción.
- Utilizar la radiodifusión para difundir la información.
- Emplear un enlace de datos para transmitir la información.

Ciberseguridad y la Aviación Civil. La Asamblea reconoció que el sistema de aviación global es muy complejo e interconectado, y comprende sistemas críticos para la seguridad de las operaciones de la aviación. Además, se destacó que la confiabilidad, integridad y disponibilidad de sistemas, datos e información son cada vez más importantes para el sector de la aviación. Por lo tanto, se exhortó a las partes interesadas adoptar medidas para abordar las amenazas cibernéticas en la aviación civil.

Las aspiraciones de este documento son los siguientes:

- Ayudar a fortalecer la capacidad del sistema de aviación del estado para resistir y recuperarse de ataques y eventos cibernéticos adversos.
- Brindar apoyo para garantizar que la información crítica y sensible relacionada con la aviación esté protegida contra amenazas cibernéticas y accesos no autorizados.
- Proteger los componentes de hardware y software que son esenciales para la operación de la infraestructura de aviación del estado, con el fin de reducir el riesgo de interrupciones de los servicios estatales.

- Facilitar la implementación de procedimientos y medidas de seguridad cibernética en todos los sistemas e infraestructuras de aviación del estado.
- Contribuir a la seguridad cibernética y la capacidad de resistencia de la industria de la aviación civil.

Ciberseguridad Para la Gestión del Tráfico Aéreo. La creciente digitalización y los sistemas interconectados han aumentado la amenaza de ciberataques en todo el mundo. Debido a sus requisitos de interconectividad, la aviación civil es especialmente vulnerable a los ciberataques, lo que puede tener deletéreas consecuencias para la seguridad operacional y reputación del sector. La Organización Aviación Civil Internacional (ICAO) de 1997 esta amenaza en la aviación civil fue abordada por medio de la resolución A40-10 durante la Asamblea A40 en 2019. Por lo tanto, resulta fundamental que en torno a la aviación civil incorpore políticas de ciberseguridad en sus procesos y sistemas en todos los aspectos, como la Gestión del tránsito aéreo (ATM), los sistemas de Comunicación, Navegación y Vigilancia (CNS), la Gestión de la información (AIM) y otros sistemas críticos de aviación que están expuestos a posibles riesgos.

Las amenazas cibernéticas son una preocupación creciente para los sistemas aeronáuticos en todo el mundo debido al aumento en la digitalización y la interconexión. Estas amenazas pueden ser premeditados y hostiles, accidentales o negligentes, o pueden ser el resultado de un desastre natural. Los sistemas de aviación pueden verse afectados por diversos riesgos, incluyendo el sabotaje de TI, la corrupción de datos y software, el entorpecimiento de las comunicaciones y la interferencia en la comunicación satelital pueden ser sinónimos de perturbación de las comunicaciones y obstrucción en la comunicación vía satélite. Además, las amenazas cibernéticas pueden estar involucradas en un contubernio más amplio, como el secuestro o la toma de rehenes.

En la región de América Latina y el Caribe, las Autoridades de Aviación Civil (AAC) han expresado su preocupación sobre la acentuación de las amenazas cibernéticas debido a la falta de protección adecuada y los procedimientos de resiliencia para garantizar la seguridad requerida. Se recomienda que es fundamental que los Estados amplíen su enfoque

en ciberseguridad y consideren salvar los sistemas de navegación aérea, incluyendo los sistemas satelitales y de gestión de tráfico aéreo. La formación del personal, tanto en proveedores de servicios para estar preparado para afrontar estos desafíos. Por lo tanto, la OACI considera la ciberseguridad como un asunto interrelacionado debido a la tecnología interconectada y la amenaza potencial de un ciberataque que afecte las operaciones de aviación.

Se apunta ejecutar subsecuentes acciones para asegurar la ciberseguridad de los sistemas de tránsito aéreo:

- Identificar y dar protección de las infraestructuras críticas vinculadas con las comunicaciones, navegación y vigilancia del servicio de tránsito aéreo.
- Preservar los sistemas automatizados que respaldan las unidades de Servicio de Tránsito Aéreo (ATS), para garantizar la confidencialidad, integridad y disponibilidad de la información, y dar resiliencia a las operaciones.
- Originar la investigación prolija sobre los riesgos sobre las amenazas y fragilidades relacionadas con el impacto en los servicios de tránsito aéreo.
- Actualizar las descripciones operacionales para mitigar los riesgos cibernéticos
- Monitorear la interacción de la información y las conexiones para detectar ciberataques y establecer medidas de protección para los sistemas.
- Patrocinar con la industria que el hardware y el software que apuntalan los sistemas de tránsito aéreo estén actualizados contra un ciberataque.
- Suministrar adiestramiento y calificaciones al personal que gestiona áreas técnicas y operacionales para obtener la capacidad de realizar planes de recuperación en el caso de un incidente cibernético.

Sin embargo, La Organización Aviación Civil Internacional (2022) estableció como propósito lo siguiente:

> El principal modelo de política de ciberseguridad es asegurar la salvaguardia y la resistencia de las infraestructuras críticas de la aviación civil internacional frente a las

> amenazas cibernéticas. Para alcanzar este objetivo, es necesario establecer una cooperación multilateral tanto dentro del sector de la aviación civil como con autoridades externas del ámbito militar, de la ciberseguridad y la seguridad nacional. Este modelo tiene como objetivo servir como un faro para que los Estados y la industria puedan dirigir sus recursos y acciones hacia un enfoque sistémico de la ciberseguridad en la aviación civil, abarcando tanto los sistemas actuales como los obsoletos. El objetivo final es establecer un "sistema de sistemas" que proteja la aviación civil contra las amenazas cibernéticas, responda y se recupere de los incidentes cibernéticos de manera oportuna y maneje nuevas amenazas sin causar interrupciones importantes. (p. 1)

2.3.3 Operaciones Aéreas Conjuntas

Las operaciones aéreas conjuntas obedecen a la integración de las diferentes fuerzas para la realización de operaciones y acciones militares, al respecto debemos señalar que las nuevas amenazas son cada vez más sofisticadas es por ello que esto obliga a que las operaciones militares en el aspecto aéreo deban realizarse bajo el principio de la conjuntez.

La "conjuntez" implica una colaboración estratégica profunda entre varios elementos militares, tales como fuerzas terrestres, aéreas, navales y ciberespaciales, cada uno aportando sus habilidades particulares para lograr un objetivo compartido. Este enfoque va más allá de la simple acumulación de habilidades individuales; se trata de generar una sinergia donde el conjunto sea más eficaz que la suma de las partes por separado (Piazzini, F. et al, 2023).

Interoperabilidad de Ciberdefensa. La Interoperabilidad dentro de la capacidad de ciberdefensa obliga a tener una taxonomía en común el cual permita mantener una articulación fluida dentro de las operaciones y acciones militares es por ello que esta es fundamental, al mismo tiempo las tecnologías de poseen cada fuerza deben mantener una comunicación fluida de data que permita una respuesta oportuna ante diferentes ciberataques o incidentes cibernéticos.

La interoperabilidad desempeña un papel fundamental en la protección, permite una respuesta más ágil ante posibles amenazas, aspecto vital para resguardar a las tropas y lograr los objetivos de la misión. En un contexto donde la guerra moderna se apoya cada vez más en tecnologías avanzadas como sistemas de comunicación, drones, guerra cibernética y armamento electrónico, la interoperabilidad asegura una integración eficiente de dichas tecnologías en las operaciones militares (Piazzini, F. et al, 2023).

2.4 Definición de términos

Comunicación Aeroterrestre

Es el intercambio de información entre aviones y estaciones terrestres que se ubican en la superficie de la tierra.

Comunicación de Aire a Tierra

La comunicación se lleva a cabo desde las aeronaves hacia las estaciones ubicadas en la superficie terrestre.

Comunicación por Enlace de Datos Controlador – Piloto

Esta interacción se establece con dos actores, quienes son el controlador y el piloto por medio de enlace de datos.

Sistema de Gestión del Tránsito Aéreo

Este sistema es una integración de personas, información, tecnología e infraestructura que utiliza comunicaciones, navegación y vigilancia en la superficie terrestre, el aire y/o el espacio.

Activo

Un activo se refiere a cualquier cosa que una organización considere importante y necesaria para su funcionamiento. Este concepto abarca diversos aspectos, como el personal que trabaja en la organización, los recursos digitales, como la información y los datos almacenados en sistemas informáticos, y los recursos tecnológicos utilizados por la organización.

Operatividad

La operatividad se refiere a la capacidad de mantener en excelentes condiciones de operación un equipo, sistema o instalación industrial, garantizando su seguridad y confiabilidad, y cumpliendo con los requerimientos operativos establecidos de antemano.

Seguridad Operacional

La seguridad operacional se refiere a mantener un nivel de riesgo aceptable o inferior a él en lo que respecta a daños a la propiedad o a las personas. Se consigue a través de un proceso continuo que implica identificar los peligros y gestionar los riesgos relacionados con las operaciones para reducirlos y mantenerlos en un nivel seguro.

Vulnerabilidad

Una brecha de seguridad es la resultante de un fallo o un deleznable procedimiento de seguridad, diseño, implementación o controles internos del sistema, que pueden ser explotados de forma deliberado o accidental, y pueden conducir a la violación de las políticas de seguridad establecidas en el sistema.

Ciberamenazas

Se relata la acción planificada y deliberada de un individuo o grupo con el propósito de comprometer la seguridad y privacidad de los sistemas informáticos y redes, con el objetivo de causar daño, robar información o llevar a cabo actividades fraudulentas.

Agente de Amenaza

Esta expresión se utiliza para describir a cualquier persona, entidad o programa informático que constituye una amenaza potencial hacia la seguridad y la integridad de los sistemas informáticos y las redes. Estas amenazas pueden ser representadas por individuos, grupos, organizaciones o incluso malware diseñado para causar daño o robo de información.

Análisis de Vulnerabilidades

La evaluación de seguridad es un procedimiento que busca detectar y valorar las deficiencias en la seguridad de los sistemas y redes informáticas. Esta actividad se lleva a cabo a través de una inspección metódica de los sistemas, redes y aplicaciones para identificar posibles puntos débiles y determinar su nivel de peligro.

Denegación de Servicio

El término relata a una pericia de ataque informático que consiste en inundar un sistema o red con una cantidad de tráfico anormalmente alto para dejarlo inoperable.

Malware

El malware se refiere a cualquier tipo de software dañino que se crea con la intención de causar daño a sistemas informáticos, redes y dispositivos móviles. Puede manifestarse en diferentes formas, incluyendo virus, gusanos, troyanos, ransomware, spyware y adware, entre otros.

Riesgo Cibernético

La expresión se utiliza para describir el riesgo de que una persona u organización sufra pérdidas o daños a consecuencia de un ataque o incidente de seguridad en sus sistemas informáticos y redes.

Vector de Amenaza

Se refiere a cualquier vía o técnica empleada por una persona o entidad malintencionada para atacar o poner en compromiso la seguridad de los sistemas informáticos y redes. Los vectores de amenaza pueden variar, desde ataques de phishing y el uso de malware, hasta la explotación de vulnerabilidades en el software y los sistemas.

CAPÍTULO III: Método

3.1 Enfoque de la Investigación

La presente investigación se diseñó bajo con un enfoque cualitativo, buscando generar conocimiento por medio de la experiencia y poder generar obtención de datos e información de la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército.

Según Vargas (2011) “describe que el enfoque cualitativo es un proceso que involucra metodologías, estrategias, observables e instrumentos que permiten al investigador analizar la realidad, centrándose en las cualidades y características del objeto de estudio” (p. 35). Por otro lado, Hernández-Sampieri y Mendoza (2018) “señalan que el enfoque cualitativo puede entenderse como un conjunto de prácticas interpretativas que hacen visible al mundo, lo transforman y lo representan mediante observaciones, anotaciones, grabaciones y documentos” (p. 102).

3.2 Tipo de Investigación

Se utilizará el tipo teórico – empírico, en vista que permitirá establecer nuevas conclusiones ya se obtienen del medio a través de la observación, análisis del empleo de la ciberdefensa en los sistemas de C2 de la Aviación. Asimismo, Vargas (2011) establece “La investigación consiste en recopilar datos empíricos sobre una realidad específica, y luego analizarlos a través de un diálogo comparativo con diversos autores seleccionados” (p.76).

3.3 Método de Investigación

La metodología empleada en este estudio se basó en el enfoque hermenéutico-interpretativo, el cual se enfoca en la “búsqueda del significado y comprensión de los fenómenos a través de una interpretación subjetiva y constante de lo que les otorga sentido en relación con el todo. Para la investigación” (Vargas, 2011, p.48).

Se utilizaron datos provenientes de investigaciones previas, teorías y definiciones sobre el uso de la capacidad militar de ciberdefensa en los sistemas de C2 de la Aviación.

3.4 Objeto de Estudio

El objeto de estudio es determinar la capacidad militar de ciberdefensa y su empleo en los sistemas de C2 de la Aviación.

3.5 Muestra de Estudio

3.5.1 Población

La población de estudio de la presente investigación fue la Aviación del Ejército del Perú, en vista que representa la base de operaciones donde se encuentra los componentes tanto de equipamiento e infraestructura materializado en torres de control, hangares de aeronaves, instalaciones del estado Mayor, Compañías. Asimismo, se encuentra desplegado el equipamiento en tecnologías que representas el soporte tecnológico de las operaciones aéreas tanto de ala rotatoria como fija. La base aérea de la AE, se encuentra ubicado en la Provincia constitucional del Callao dentro de las instalaciones de CORPAC, a través de un convenio firmado entre las dos (02) entidades, se le concedió a la Aviación del Ejército ocupar esa área hasta el año 2026. Asimismo, el estudio se realizará a través de operadores propios de aviación siendo un aproximado de ochenta (80) personas entre civiles y militares especialistas en aeronáutica y responsables de ser el soporte humano para las operaciones militares aéreas, también comprenderá personal operador en ciberdefensa del Ejército, siendo un aproximado de treinta (30) especialistas, sin embargo por ser una población muy amplia y en vista que solo se enfoca al estudio de una capacidad operativa de ciberdefensa en los sistemas de comando y control de la aviación, se verá reducido tal como se establece en la muestra.

3.5.2 Muestra

Se llevará a cabo una muestra no probabilística o dirigida del estudio, toda vez que los participantes son expertos en las variables establecidas, siendo un total de ocho (08) participantes, cuatro (04) especialistas en ciberdefensa, así como cuatro (04) oficiales pilotos. Los entrevistados poseen extensa experiencia en el empleo de sistemas de comando y control aeronáutico y en la ciberdefensa. Los entrevistados son actualmente miembros en servicio activo y fueron seleccionados como expertos para obtener la información necesaria

mediante el uso de una guía de entrevista como instrumento. Así como también cinco (05) profesionales que realizaron la observación teniendo todo el grado de oficiales conocedores de investigación planteada.

3.6 Técnica e Instrumentos de Recolección de Datos

3.6.1 Técnica

Se esgrimieron para el estudio: la entrevista, la observación y el análisis documental.

La Entrevista. La entrevista es una técnica que permite la comunicación entre el entrevistador y el entrevistado o incluso con otras personas que puedan intervenir, con el fin de dialogar y compartir información. En algunos casos, la entrevista puede involucrar a parejas o grupos pequeños. A través de esta técnica, se realizan preguntas y respuestas con el objetivo de obtener una comunicación adecuada y la construcción de significados en torno al tema en cuestión.

La Observación. De acuerdo con Hernández (2017) “en el contexto de este estudio, es esencial tener una formación adecuada, especialmente en lo que respecta a la observación, que es diferente de lo que hacemos en la vida diaria que es simplemente ver” (p. 117), La observación investigativa implica una jerarquía de situaciones y requiere el uso de todos los sentidos disponibles.

Análisis Documental. Según Hernández (2017) afirma que la documentación y los materiales son fuentes esenciales de información para la investigación. Estos recursos proporcionan datos sobre el fenómeno de estudio, incluyendo las historias narradas por personas, instituciones y sociedades” (p. 120). Por consiguiente, lo que permite al investigador obtener referencias precisas sobre el entorno, las experiencias y los contextos que se desarrollan en él. De esta manera, el investigador puede obtener información detallada y fidedigna sobre el ambiente y las actividades cotidianas que se llevan a cabo en él.

3.6.2 Instrumentos

El listado de instrumentos que fueron seleccionados para el presente estudio es:

Guía de Entrevista. La entrevista utilizada en este estudio fue semi-estructurada y diseñada específicamente para la muestra seleccionada. El objetivo de esta técnica fue

obtener información relevante para responder la pregunta de investigación y comprender el contexto actual del sistema de comando y control de la Aviación del Ejército a través de las perspectivas de los miembros de la institución. Las entrevistas se llevaron a cabo mediante la plataforma Zoom o Meet.

Ficha de Contenido. La información recopilada fue organizada mediante el análisis de documentos, el cual se analizó y resumió para una mejor comprensión.

Guía de Observación. El instrumento de observación permite al investigador registrar información mientras se encuentra presente en el lugar donde ocurre el fenómeno que está siendo estudiado. Esto le permite al observador una aproximación metodológica al objeto de estudio y la posibilidad de observar detalladamente comportamientos y procesos, lo que a su vez le permite conocer la realidad en profundidad.

3.7 Rigor Científico

La investigación cualitativa, busca garantizar la efectividad, objetividad y validación de la misma a través de ciertos parámetros. En la presente investigación, se han considerado los principios de credibilidad, auditabilidad y conformabilidad en vista que estos son transversales a la investigación propuesta

La Credibilidad

Se refiere al uso preciso y verídico de los datos, esencialmente aquellos recolectados tanto en la Dirección de Inversiones del Ejército como en la Aviación del Ejército.

La Auditabilidad

Se refiere al fiel acatamiento de las normas y procedimientos establecidos para este tipo de investigación.

La Conformabilidad

Se relaciona con el uso apropiado de los datos y su veracidad para procesar la información obtenida.

3.8 Técnica de Procesamiento y Análisis de Datos

3.8.1 Procesamiento

El procesamiento para la presente investigación cualitativa, inicio con la identificación de expertos calificados en operaciones aéreas y operaciones de ciberdefensa, para la presente investigación se determinaron ocho (08) expertos, así como a cinco (05) profesionales que realizaron las observación a través de visitas a las instalaciones de la Aviación del Ejército y las instalaciones de CITELE, los mencionados profesionales tienen competencias en operaciones aéreas y de ciberdefensa, pertenecientes a la Aviación del Ejército y al Centro de Ciberdefensa del Ejército, se llevará reuniones virtuales a través de la diferentes plataformas de comunicación con la finalidad de coordinar y poner al corriente la envergadura de la presente investigación, haciendo conocer que su aporte servirá para establecer un aporte doctrinal a las operaciones de ciberdefensa y su empleo en las operaciones aéreas, después de hacer conocer la importancia de la investigación se procederá a realizar una serie de entrevistas, siguiendo la guía de entrevistas la cual será grabado de manera digital con el consentimiento de los entrevistados, el procedimiento de recolección de dato (entrevistas) se realizará empleando plataformas Zoom y Meet, en vista que son versátiles para la comunicación.

Los requerimientos para establecer la entrevista, es que ambas partes cuenten con dispositivos (Laptop, Tablet) u otro dispositivo que facilité la comunicación, con una capacidad de internet disponible para el proceso de entrevistas. La conexión de internet debe estar asegurada a fin que el proceso de grabado se lleve de la manera más óptima, dicha grabación debe ser transcrita aun documento digital con la finalidad de realizar un análisis posterior y acorde a los requerimientos de la investigación.

.*3.8.2 Método de Análisis de Datos*

Se utilizaron varias técnicas en esta investigación, incluyendo la entrevista a expertos, el análisis documental y la observación. Además, se usaron varios instrumentos, como la guía de entrevista, la ficha de contenido y la guía de observación. Estos métodos y herramientas

permitieron la clasificación y reducción de la información, lo que facilitó su categorización, síntesis y estructuración para un mejor análisis y comprensión del problema en estudio.

CAPITULO IV: Análisis y Síntesis

4.1 Recolección de Datos

Luego de la validación de los instrumentos de recolección de datos y aprobado la autorización para tener acceso al campo de estudio, la que se gestionó a través de la Dirección de la Escuela Superior de Guerra – EPG, se continuó con la recolección de datos para conocer la Capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022. Al respecto:

En el proceso de la construcción de muestras se definen datos a través un conjunto de conceptos producto de la interacción entre personas e investigadores (Izcara, 2014).

Las actividades realizadas, a través de documentos o elementos físicos, procesados por medio de ocho (08) oficiales conocedores de la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, procediendo a la recolección de los datos de una manera eficiente con un valor analítico, a través de fuentes humanas y documentos.

4.2 Organización de los Datos

Los datos se organizaron de una manera eficiente teniendo en consideración cada instrumento, según los datos obtenidos, para explicar información relevante sobre la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022.

Guía de Entrevista. Se efectuaron ocho (08) entrevistas, a través plataforma virtual meet y zoom, las mismas que fueron llevadas a un formado de documento word para una adecuada interpretación de la muestra.

Guía de Observación. Los datos obtenidos de la observación directa a través de cinco (05) profesionales observadores en las visitas a las instalaciones del AE y CITELE dichos observadores transcribieron y obtuvieron informaciones de suma relevancia con

respecto a la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022

Indagación Documental. Se seleccionó la información obtenida en la ficha de investigación, la información fue transcrita al formato Word, para su análisis.

De acuerdo al volumen de información recolectada, es importante estructurarla de manera adecuada con base en los datos, considerando el uso de herramientas complementarias incluso para llevar a cabo el análisis si resultara necesario. (Hernández-Sampieri & Mendoza, 2018)

Se organizaron los datos respectivamente por instrumentos, el cual facilitó el análisis del material, empleándose para ello el método de la Hermenéutica.

Tabla 1

Organización de los datos

	Guía de entrevista	Guía de observación	Ficha de investigación
Guía de entrevista	Entrevistado 1 Entrevistado 2 Entrevistado 3 Entrevistado 4 Entrevistado 5 Entrevistado 6 Entrevistado 7 Entrevistado 8		
Guía de Observación		Bitácora de campo con anotaciones de la observación directa (05) observadores instalaciones de la Aviación del Ejército.	
Ficha de Investigación			• Manual de ciberdefensa de la Junta Interamericana de Defensa. • Concepción de las operaciones militares. • Manual de ciberdefensa OTAN • Ley de Ciberdefensa

4.3 Definición de Categorías

En atención a la categorización es sustancial el estudio cualitativo, en vista que se eligen fragmentos importantes que se obtienen de la deducción de la investigación. La clasificación permitirá dar inicio, construir ideas para obtener luego conceptos analíticos, formando un entendimiento claro cuando se traza el problema. las codificaciones son como protocolos que entregan un nivel a las clases (Hernández-Sampieri & Mendoza, 2018).

4.3.1 Definición de Temas (Grupos de Categorías) de las Entrevistas

Tabla 2

Definición de los temas de las guías de entrevista

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad Militar de ciberdefensa	Tecnología Militar de ciberdefensa	TMC	05	La tecnología militar refleja todos los instrumentos tecnológicos que son empleados para las operaciones y acciones militares por cuanto su importancia es fundamental para operaciones, debemos señalar que Aviación del Ejército comprende una infraestructura tecnológica compleja, toda vez que es un sistema que integra aeronaves, software y personas, desde la naturaleza misma de las aeronaves para su empleo, ya que tienen en si sistemas de comando y control, sensores integrados, asimismo la torre de control comprende sistema de comando y control que permite monitorear la conducción de las aeronaves, sin embargo todo ello puede ser vulnerable a ciberataques, en vista que la Aviación no cuenta con tecnología militar de ciberdefensa que permita proteger sus activos tecnológicos que posee, por ello es necesario que la tecnología militar sea renovada constantemente a fin de evitar la explotación de vulnerabilidades de los sistemas de la Aviación del Ejército.
	Capacidades operativas	CO	06	Las capacidades operativas de ciberdefensa son necesarias dentro de la estructura tecnológica

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				que posee la Aviación en vista que aún no cuenta protección de seguridad perimetral, lo que conlleva al desconocimiento de haber sido penetrado por amenazas y que estén ex filtrando información o que en algún momento puedan sabotear alguna operación, la capacidad de defensa, hace posible implementar tecnologías de seguridad perimetral tales como SIEM, Firewall, sistemas de detector de intrusos, sistemas de prevención de intrusos, etc. La implementación de estas herramientas es fundamental en vista darían ese soporte a las operaciones que hoy no la tienen, teniendo en la actualidad un riesgo muy alto que afecten las operaciones que realiza la Aviación, por otro lado tenemos capacidad operativa de explotación que nos permite recolectar información del ciberespacio sobre amenazas potenciales, así como vulnerabilidades que poseen los sistemas aeronáuticos su implementación nos pondría siempre adelante de las intenciones de las amenazas cibernéticas, es por ello que estas dos (02) capacidades son fundamentales dentro de la Aviación permitirían que las operaciones se lleven de la mejor manera
	Marco de gobernanza	MG	04	Con referente al marco de gobernanza implica que debemos optar por obtener procesos y procedimientos claros desde la manera preventiva y reactiva frente a ciberataques, es por ello que para la presente investigación se determinó que sea NIST, el marco de gobernanza, en vista que posee un enfoque del ambiente operacional basado en el ciber riesgo enfocado a la organización en el proceso de maduración, este marco es muy importante ya que

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
Comando y control de la Aviación del Ejército	Sistema de comando y control	C2	07	facilitaría el soporte a las operaciones en vista que posee un conjunto de buenas prácticas puestas de manifiesto en diferentes organizaciones tanto militares y civiles. La Aviación del Ejército posee un sistema de Comando y Control denominado Blue Sky, por donde se procesa información propia del empleo de sus aeronaves. La prioridad de establecer la protección del sistema de C2, radica en la importancia que asume la Aviación del Ejército dentro de la organización estructural del Ejército, que apoya en operaciones y acciones militares aéreas, acorde con los nuevos roles que ha asumido el Ejército. Sin embargo, el sistema C2 de este importante órgano de Línea, en la actualidad no posee una seguridad adecuada, asimismo se encuentra expuesto frente a las ciberamenazas. Lo cual constituye un riesgo exponencial de ocurrir un incidente digital o físico, pueda tener un efecto de inoperatividad de las aeronaves por un periodo de tiempo indeterminado, sujeto al vector de ataque empleado por la ciberamenaza.
	Normativa operativa aérea	NOA	06	Al respecto debemos tener en claro que los sistemas aéreos son cada vez más interconectados, en consecuencia, han aumentado las amenazas de ciberataques. En consecuencia, la aviación civil ha sido responsable respecto a lo que puede configurar un riesgo para las operaciones. La Organización Aviación Civil Internacional (ICAO) abordo esta amenaza como un riesgo para la aviación civil resultando fundamental que la aviación civil incorpore políticas de ciberseguridad en sus procesos y sistemas en todos los aspectos, como la gestión del tránsito aéreo

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				(ATM), los sistemas de Comunicación, Navegación y Vigilancia (CNS), la Gestión de la información (AIM) y otros sistemas críticos de aviación que están expuestos a posibles riesgos. La interoperabilidad en las operaciones aéreas conjuntas resultan fundamentales para las operaciones y acciones militares, en vista que las operaciones se realizan de manera conjunta, con tecnología integrada, por cuanto tanto aeronaves, sistemas de comando y control deben ser interoperables, en base a ello se debe tener como soporte una protección cibernética óptima para las operaciones, las trasmisiones de comunicación, de la torres de control, los sistemas que operan dentro todo este proceso complejo, asimismo requieren de capacidades operativas de ciberdefensa, para ello es necesario que se implemente la capacidad de ciberdefensa en vista que podemos ser vulnerados por sistemas diferentes a la Aviación del Ejército.
Operaciones aéreas conjuntas	Interoperabilidad de ciberdefensa	IC	05	

4.3.2 Definición de Temas (Grupo de Categorías) de la Observación Directa

Tabla 3

Observación directa

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad Militar de ciberdefensa	Tecnología Militar de ciberdefensa	TMC	05	Se evidenció que la Aviación del Ejército es una organización netamente técnica, con aeronaves de ala rotatoria y fija de reciente adquisición, sin embargo esta dependencia cuenta con una compañía de comunicaciones, responsable de dar el soporte tecnológico a las operaciones, al respecto, se pudo apreciar que

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				dicha compañía no cuenta con la infraestructura adecuada para dar un soporte cibernético a las operaciones que realiza dicha dependencia, asimismo dicha compañía articula las operaciones con la torre de control, en ambos casos no se dispone de una seguridad perimetral cibernética adecuada por cuanto son vulnerables a ataques cibernéticos.
	Capacidades operativas	CO	06	Se evidencio que las capacidades de ciberdefensa no se encuentran implementados en las Aviación del Ejército, dichas capacidades de defensa y explotación son necesarias porque estas enmarcan: tecnologías, procesos y operadores, necesarios para dar un soporte cibernético adecuado mitigando el riesgo de ocurrencia de ataque cibernéticos, así como poder identificar ciberamenazas y también mantener actualizados los sistemas propios de la Aviación.
	Marco de gobernanza	MG	04	Se apreció que la Aviación a través de su compañía de comunicaciones, no cuenta con un marco de gobernanza que permita establecer procesos y procedimientos frente a ataques cibernéticos, problemas y ocurrencias, y estas puedan ser escalonadas para la solución oportuna, como también poder tener un acompañamiento de madurez como organización para lograr nivel más óptimo en ciberdenfensa, todo ello es necesario debido a que esta dependencia es técnica siendo también un objetivo de alto impacto para las ciberamenazas.
Comando y control de la Aviación del Ejército	Sistema de comando y control	C2	07	Se evidencio que la Aviación del Ejército posee un sistema de Comando y Control denominado Blue Sky, por donde se procesa información propia del empleo de

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				sus aeronaves. La prioridad de establecer la protección del sistema de C2, radica en la importancia de las operaciones y acciones militares aéreas que desarrollan, acorde con los nuevos roles que ha asumido el Ejército, asimismo dicho sistema Blue Sky es un sistema de pago y de terceros, aumentando con ellos el nivel de criticidad de ser vulnerable, toda vez que no tenemos acceso al código fuente, si este fue desarrollado de la mejor manera o que pueda tener conexiones remotas con ex filtración de data.
	Normativa operativa aérea	NOA	06	Se evidencio que la Aviación del Ejército mantiene procesos y procedimientos netamente aeronáuticos, sin embargo, esta normativa ha sido actualizada, recomendando que las organizaciones aéreas deberán de adoptar medidas de ciberseguridad necesarias para poder llevar a cabo sus operaciones, estas medidas recomendadas circunscriben a tener infraestructura tecnológica necesaria de ciberdefensa y adoptar procesos adecuados para ello.
Operaciones aéreas conjuntas	Interoperabilidad de ciberdefensa	IC	05	Se apreció que la Aviación del Ejército, también realiza operaciones conjuntas y sus sistemas de comunicación, comando y control son interoperables, por cuanto refleja ello que puede ser atacado, empleando como movimiento lateral o pivot la infraestructura de la Aviación de otra fuerza. En base a ello es necesario contar con capacidades operativas de ciberdefensa de defensa y explotación.

4.3.3 Definición de Temas (Grupo de Categorías) de la Indagación Documental

Tabla 4

Definición de los temas de indagación documental

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad Militar de ciberdefensa	Tecnología Militar de ciberdefensa	TMC	05	La tecnología ha sido un factor determinante en los diferentes dominios donde una guerra abarco, estos avances tecnológicos han generado una actualización constante de la doctrina de la guerra. Los tomadores de decisiones militares diseñan conceptos operativos que aprovechan la tecnología para aplicarla de la forma más eficaz, la Aviación del Ejército a lo largo de su existir ha empleado diversas tecnologías militares tanto para aeronaves, sistemas de armas, C2 sensores, por consiguiente, se requiere que las tecnologías deben ser actualizadas constantemente. con la aparición de este quinto dominio denominado ciberespacio, es esencial que se implementen tecnologías con el objetivo de mitigar el ciber riesgo.
	Capacidades operativas	CO	06	Las capacidades operativas narran las medidas operativas adoptadas para certificar la seguridad, configuración, operación, del ciberespacio, así como obtención de información relacionada con las ciber amenazas, con el fin de crear y custodiar la confidencialidad, disponibilidad e integridad de los sistemas de C2 de la Aviación del Ejército. Las capacidades operativas como defensa y explotación son esenciales para las operaciones aéreas, su implementación demanda de infraestructura tecnología como SIEM, detectores de intrusos, así como motores de búsqueda especializado de ciberamenazas para estar de una manera preventiva preparados y responder

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				ante cualquier incidente cibernético.
	Marco de gobernanza	MG	04	Las funciones del Marco de Ciberseguridad del NIST proporcionan una visión general mejores prácticas. Es importante tener en cuenta que estas funciones no son un conjunto de pasos de procedimiento, No se trata de una acción única, sino de una serie de medidas que deben implementarse constantemente para fomentar una cultura operativa que aborde los riesgos cambiantes de la ciberseguridad. Las categorías y subcategorías proporcionan planes de acción específicos para departamentos o procesos dentro de una organización.
Comando y control de la Aviación del Ejército	Sistema de comando y control	C2	07	Este concepto se refiere a grupos de componentes que articulan para proveer al mando información relevante y actualizada sobre la situación, lo cual es fundamental para tomar decisiones. Estos conjuntos de elementos están interconectados entre sí y desempeñan las acciones necesarias para lograr este objetivo en un plazo adecuado. Un sistema de mando y control debe desempeñar un rol importante en adquirir información relevante para la situación, procesar, analizar, sintetizar, visualizar y distribuir la información de manera efectiva tanto dentro de la estructura de mando como hacia afuera.
	Normativa operativa aérea	NOA	06	Los sistemas aeronáuticos en todo el mundo son una preocupación ante el aumento en la digitalización y la interconexión. Estas amenazas pueden ser premeditados y hostiles, accidentales, Los sistemas de Aviación pueden verse afectados

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				por diversos riesgos, incluyendo el sabotaje de TI, la corrupción de datos y software, el entorpecimiento de las comunicaciones y la interferencia en la comunicación satelital pueden ser sinónimos de perturbación de las comunicaciones. Es por ello que la Aviación del Ejército deba actualizar su normativa aérea con buenas prácticas que promuevan la protección de su infraestructura TI.
Operaciones aéreas conjuntas	Interoperabilidad de ciberdefensa	IC	05	La Interoperabilidad en las operaciones aéreas conjuntas podemos definirlas como aquellas que se realizan de una manera sinérgica para la realización de operaciones y acciones militares por cuanto es necesario determinar taxonomías de ciberdefensa en común que permitan operar con las capacidades operativas de ciberdefensa ante cualquier ciberataque o incidente cibernético que se pueda dar durante la realización de las operaciones. Las tecnologías cibernéticas de cada fuerza deben ser identificadas, así como los diferentes procesos mapeados y los operadores operar bajo la taxonomía establecida, en vista que el factor oportunidad es fundamental en este tipo de operaciones aéreas.

4.4 Soporte de Categorías

Tabla 5

Soporte de Categorías

Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad Militar de ciberdefensa	Tecnología Militar ciberdefensa	TMC	05	La tecnología militar son las herramientas y procesos que se desarrollan con la finalidad de efectivizar operaciones de tipo militar en base a ello establecemos doctrina, en el ámbito de la ciberdefensa es muy importante la tecnología, por que articula con hardware y software necesario para operativizar las capacidades operativas de ciberdefensa.
	Capacidades operativas	CO	06	Las capacidades operativas de ciberdefensa son aquellas capacidades que se ejecutan en base a tareas tácticas de ciberdefensa, en el ámbito de la Aviación, se emplearan dos (02) capacidades: defensa y explotación y ellas requieren de tecnologías acordes a los requerimientos operacionales.
	Marco de gobernanza	MG	04	El Marco de gobernanza NIST es un marco que enfoca al ciber riesgo que permite identificar nivel de madurez actual para realizar un acompañamiento y poder llegar a un nivel de madurez óptimo necesario en las operaciones de ciberdefensa dentro de la Aviación.
Comando y control de la Aviación del Ejército	Sistema de comando y control	C2	07	Los sistemas de comando y control son aquellas herramientas que nos permiten conducir, controlar las operaciones aéreas para ello se emplearan sistemas o plataformas digitales el cual permitirá establecer comunicaciones entre el operador y las aeronaves para poder llevar un monitoreo continuo.
	Normativa operativa aérea	NOA	06	La Organización de Aviación Civil Internacional (ICAO) ha instaurado

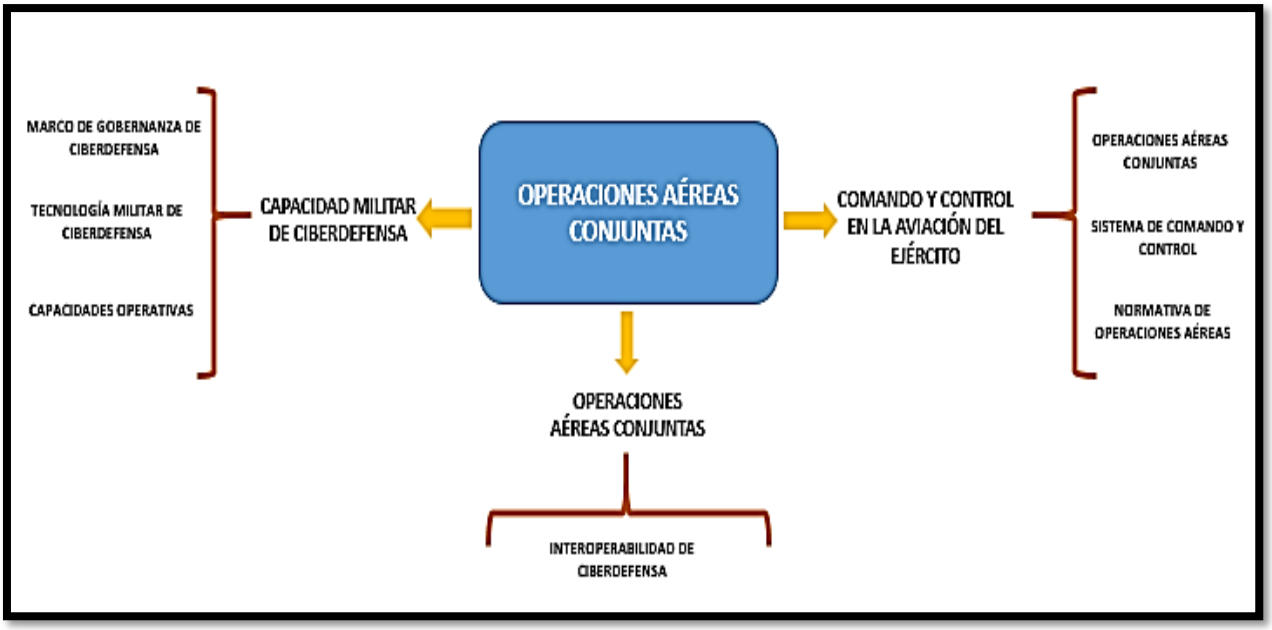
Categoría (codificación axial)	Subcategoría (Codificación abierta)	Abrev	Frec	Síntesis
				una serie de regulaciones para certificar la seguridad de las operaciones. La torre de control de la Compañía de Comunicaciones Nº 800, utiliza estas regulaciones como referencia para asegurar la seguridad en sus operaciones. Sin embargo, debido a que la compañía no tiene una plataforma interoperable, se dificulta la aplicación coherente y adecuada de las regulaciones de ICAO en todas sus operaciones. Asimismo, la actualización de las normativas de la Aviación es necesarias y deberán estar orientadas a las buenas prácticas de ciberdefensa.
Operaciones aéreas conjuntas	Interoperabilidad de ciberdefensa	IC	05	Las operaciones aéreas conjuntas con llevan a la interoperabilidad dentro de una plataforma, por consiguiente, permiten establecer comunicaciones, intercambio de información con las fuerzas que intervienen, es por ello que es necesario el empleo de una taxonomía única entre las fuerzas con la finalidad que las operaciones sean eficientes y puedan responder frente a cualquier incidente cibernético.

4.5 Red Semántica

Establece los problemas que existen en la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022, con respecto al cumplimiento de su misión asignada. Además, se analizó la capacidad militar de ciberdefensa, como medio para realizar operaciones de ciberdefensa, asimismo se incluyó los sistemas de comando y control como soporte a las operaciones, como también las operaciones aéreas conjuntas que tienen como requerimiento, la interoperabilidad de ciberdefensa.

Figura 7

Red semántica



4.6 Triangulación

En el enfoque cualitativo, sostiene Hernández-Sampieri & Mendoza (2018) que “en triangulación la indagación cualitativa se tiene una riqueza, amplitud y profundidad de datos que se obtienen de diferentes actores, de distintas fuentes y de una variedad amplia de formas de recolección” (p. 417), objetivo principal es garantizar la validez y la rigurosidad en la investigación científica. Para lograrlo, se llevaron a cabo comparaciones entre los resultados obtenidos de las entrevistas, la revisión de documentos y la observación directa.

Tabla 6

Triangulación de técnicas cualitativas

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
Capacidad militar de ciberdefensa	Las capacidades operativas de ciberdefensa son necesarias dentro de la estructura tecnológica que posee la Aviación, en vista que aún no cuenta protección de seguridad perimetral, lo que conlleva al desconocimiento de haber sido penetrado por amenazas y que se estén ex filtrando información o que en algún momento puedan sabotear alguna operación, es por ello que las capacidades son fundamentales dentro de la Aviación ya que permitiría que las operaciones se lleven de la mejor manera, por otro lado la importancia de la tecnología militar refleja	Se evidenció que la Aviación del Ejército es una organización netamente técnica, con aeronaves de ala rotatoria y fija de reciente adquisición, sin embargo esta dependencia cuenta con una compañía de comunicaciones, responsable de dar el soporte tecnológico a las operaciones, sin embargo, se pudo apreciar que dicha compañía articula las operaciones con la torre de control, en ambos casos no se dispone de una seguridad perimetral cibernética adecuada por cuanto son vulnerables a ataques cibernéticos. Asimismo, se evidencio que las capacidades de	La tecnología ha sido un factor determinante en los diferentes dominios donde una guerra abarco, estos avances tecnológicos han generado una actualización constante de la doctrina de la guerra. Los tomadores de decisiones militares diseñan conceptos operativos que aprovechan la tecnología para aplicarla de la forma más eficaz, la Aviación del Ejército a lo largo de su existencia han empleado diversas tecnologías militares, tanto para aeronaves, sistemas de armas, C2, sensores, por consiguiente, se requiere que las tecnologías deben ser actualizadas constantemente de	La capacidad militar de ciberdefensa es una convergencia de capacidades operativas definidas como explotación, defensa y respuesta, sin embargo dentro de la estructura operativa que posee la Aviación del Ejército, se ha podido evidenciar que esta dependencia no tiene implementada ninguna capacidad operativa de ciberdefensa, al respecto la Aviación es una organización netamente técnica, cuyas operaciones se enmarcan a operaciones y acciones militares, de allí la importancia de esta dependencia de tener implementada la capacidad operativa de

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
	todos los instrumentos tecnológicos que son empleados para las operaciones y acciones militares por cuanto su importancia es fundamental para operaciones, debemos señalar que la Aviación del Ejército comprende una infraestructura tecnológica compleja, toda vez que es un sistema que integra aeronaves, software y personas, ya que tienen en su sistema de comando y control, sensores integrados, asimismo la torre de control comprende sistema de comando y control que permite monitorear la conducción de las aeronaves, sin embargo todo ello puede ser vulnerable a ciberataques, en vista que la Aviación no cuenta	ciberdefensa no se encuentran implementados en las Aviación del Ejército, dichas capacidades de defensa y explotación son necesarias porque estas enmarcan: tecnologías, procesos y operadores, necesarios para dar un soporte cibernético adecuado mitigando el riesgo de ocurrencia de ataque cibernéticos, así como poder identificar ciberamenazas y también mantener actualizados los sistemas propios de la Aviación. Por otro lado, se apreció que la Aviación a través de su compañía de comunicaciones, no cuenta con un marco de gobernanza que permita establecer procesos.	información relacionada con las ciberamenazas, con el fin de crear y custodiar la confidencialidad, disponibilidad e integridad de los sistemas de C2 de la Aviación del Ejército. Las capacidades operativas como defensa y explotación son esenciales para las operaciones aéreas, su implementación demanda de infraestructura tecnología como SIEM, detectores de intrusos, así como motores de búsqueda especializado de ciberamenazas para estar de una manera preventiva preparados y responder ante cualquier incidente cibernético. Cabe mencionar que en lo que refiere a las funciones del Marco de ciberseguridad basado en NIST, proporcionan una	defensa y explotación, en vista que las ciberamenazas emplean como medio el ciberespacio, un dominio poco investigado, reflejando claramente un riesgo a las operaciones aeronáuticas, lo que conlleva a tener actualizado las tecnologías que se emplean en actualidad, como de prever nuevas tecnologías de ciberdefensa, en el aspecto de defensa, disponer de seguridad perimetral cibernética acorde a los requerimientos operaciones de la Aviación, como contar con capacidad de explotación que identifique ciberamenazas de manera oportuna para minimizar un impacto sobre los

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
	con tecnología militar de ciberdefensa que permita proteger sus activos tecnológicos que posee.		visión general mejores prácticas de ciberseguridad.	activos tecnológicos de la Aviación.
Comando y control de la Aviación del Ejército	La Aviación del Ejército posee un sistema de Comando y Control denominado Blue Sky, por donde se procesa información propia del empleo de sus aeronaves. La prioridad de establecer la protección del sistema de C2, radica en la importancia que asume la Aviación del Ejército dentro de la organización estructural del Ejército, que apoya en operaciones y acciones militares aéreas, acorde con los nuevos roles que ha asumido el Ejército. Al respecto debemos tener en claro que los sistemas aéreos son cada vez más	Se evidencio que la Aviación del Ejército posee un sistema de Comando y Control denominado Blue Sky, por donde se procesa información propia del empleo de sus aeronaves. también la Aviación del Ejército mantiene procesos y procedimientos netamente aeronáuticos, sin embargo, esta normativa ha sido actualizada, recomendando que las organizaciones aéreas deberán de adoptar medidas de ciberseguridad necesarias para poder llevar a cabo sus operaciones, estas	La Interoperabilidad en las operaciones aéreas conjuntas podemos conceptualizarlas como aquellas que se realizan de una manera sinérgica para la realización de operaciones y acciones militares en el cumplimiento de objetivos, para ello debemos tener en cuenta que las doctrinas de las tres (03) fuerzas son diferentes porque su empleo es diferente basado en su concepción propia por cuanto es necesario determinar taxonomías de ciberdefensa en común que permitan operar con las capacidades operativas de ciberdefensa ante	El sistema de comando y control mapeado en la Aviación del Ejército es un sistema denominado Blue Sky, es un sistema licenciado, es decir de terceros, sin embargo se ha evidenciado que esto representa un riesgo a las operaciones en vista que al ser un sistema de terceros, se desconoce cómo fue desarrollado y que vulnerabilidades presente dicho sistema, en vista que no ha sido sometido a pruebas de vulnerabilidades, asimismo la infraestructura tecnológica que comprende el sistema de comando y control de la aviación, es rudimentaria en vista que no posee

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
	interconectados, en consecuencia, han aumentado la amenaza de ciberataques. La Organización Aviación Civil Internacional (ICAO) abordo esta amenaza como un riesgo para la aviación civil resultando fundamental que la aviación civil incorpore políticas de ciberseguridad en sus procesos y sistemas.	medidas recomendadas circunscriben a tener infraestructura tecnológica necesarias de ciberdefensa y adoptar procesos adecuados para ello. La prioridad de establecer la protección del sistema de C2, radica en la importancia de las operaciones y acciones militares.	cualquier ciberataque o incidente cibernético que se pueda dar durante la realización de las operaciones. Las tecnologías militares de ciberdefensa de cada fuerza deben ser mapeadas, así como los diferentes procesos y operadores y establecer un esfuerzo sinérgico de taxonomía única para este tipo de operaciones.	sistemas que detecten comportamientos anómalos dentro de las redes, es por ello que el sistemas de comando y control que posee la Aviación debe tener una protección cibernética adecuada, que permita garantizar que las operaciones que realiza la aviación se llevaran a cabo de la manera más óptima.
Operaciones aéreas conjuntas	La interoperabilidad en las operaciones aéreas conjuntas resultan fundamental para las operaciones y acciones militares, en vista que las operaciones se realizan de manera conjunta, con tecnología integrada, por cuanto tanto las aeronaves, sistemas de comando y control deben ser interoperables, en base a ello se debe tener	Se apreció que la Aviación del Ejército, también realiza operaciones conjuntas con otras fuerzas como son: Marina de Guerra del Perú y Fuerza Aérea del Perú llevando a cabo operaciones militares, por otro lado también realiza acciones militares en apoyo a entidades estatales, toda esta sinergia compleja que se	La Interoperabilidad en las operaciones aéreas conjuntas podemos definirlas como aquellas que se realizan de una manera sinérgica para la realización de operaciones y acciones militares por cuanto es necesario determinar taxonomías de ciberdefensa en común que permitan operar con las capacidades	Las operaciones aéreas conjuntas comprenden una interoperabilidad entre la fuerzas que realizan la misma misión, al respecto podemos decir que la Aviación del Ejército, Marina de Guerra y Fuerza Aérea deben conceptualizar una misma taxonomía de ciberdefensa, en vista que los ataques o incidentes cibernéticos son

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
	como soporte una protección cibernética óptima para las operaciones, las trasmisiones de comunicación, de la torres de control, los sistemas que operan dentro todo este proceso complejo, requieren de capacidades operativas de ciberdefensa, para ello es necesario que se implemente la capacidad de ciberdefensa en vista que la Aviación puede ser vulnerado a través de sistemas diferentes a la Aviación del Ejército.	pudo apreciar obedece a esfuerzo y empleo de medios, tanto tecnológicos, operadores y procedimientos, lo cual refleja que las operaciones aeronáuticas requieren de un soporte de seguridad, más aún en el aspecto cibernético, donde torres de control, aeronaves y operadores emplean como medio de comunicación el ciberespacio, por cuanto los sistemas de comunicación y comando y control son interoperables, reflejando ello que puede ser atacados empleando vectores de ataques sofisticados.	operativas de ciberdefensa ante cualquier ciberataque o incidente cibernético que se pueda dar durante la realización de las operaciones. Las tecnologías cibernéticas de cada fuerza deben ser identificadas, así como los diferentes procesos mapeados y los operadores operara bajo la taxonomía establecida, en vista que el factor oportunidad es fundamental en este tipo de operaciones aéreas.	transversales a dichas fuerzas, cabe mencionar que las ciberamenazas buscan explotar vulnerabilidades en los sistemas de C2, sistemas de armas, comunicación, ante ello la interoperabilidad en el aspecto cibernético debe permitir mitigar los impactos ocasionados por las ciberamenazas, ello implica tener una tecnología interoperable, procesos mapeados así como operadores conjuntos que permitan dar respuesta oportuna a las operaciones.

CAPITULO V: Diálogo Teórico Empírico

El diálogo teórico-empírico se refiere a un proceso de investigación que combina tanto la teoría como la evidencia empírica para obtener un conocimiento más completo y riguroso sobre un fenómeno o problema en particular. El proceso de diálogo teórico-empírico es iterativo, lo que significa que se realiza una revisión constante de las hipótesis a la luz de los nuevos datos empíricos y de los desarrollos teóricos posteriores. Este enfoque es fundamental en muchas disciplinas científicas, ya que permite una integración efectiva entre la teoría y la evidencia empírica para desarrollar un juicio más profundo y preciso de los fenómenos naturales y sociales.

Según el objetivo N°01 se analizó la capacidad militar de ciberdefensa en la seguridad de los sistemas de comando y control de la Aviación del Ejército. De los resultados obtenidos se demuestra que la presente investigación enfatiza que la capacidad militar de ciberdefensa dentro del Ejército, tiene una reciente creación con su dependencia del ciberdefensa y Telemática del Ejército (CITELE), al respecto debemos señalar que su avance en la implementación no ha sido el más óptimo en lo que refiere a establecer tecnologías de ciberdefensa, especialistas y procesos que hagan viables el empleo de esta capacidad. Los resultados obtenidos concuerdan con la investigación de Quevedo (2023), en su investigación “Ciberdefensa y ciberseguridad en el Perú” define que la capacidad militar de ciberdefensa es importante, pero que todavía hay mucho trabajo por hacer para mejorarla. Ha argumentado que los operadores de tecnología en el Perú han identificado un déficit en ciberdefensa debido a que la ejecución de los procesos o infraestructura tecnológica que fortalecen la protección de información de diferentes entidades sean estos privados como públicos aún son precarios. Este resultado concuerda con la teoría de Carrasco (2019), en su investigación denominada “Capacidad de respuesta del Centro de Ciberdefensa en las operaciones y acciones militares” señala que el desarrollo de capacidades debe contribuir en las operaciones militares y avalar la seguridad en el uso de sistemas de fuerzas amigas. Con los resultados presentados

podemos señalar la Aviación del Ejército requiere de la capacidad para la seguridad propia de las operaciones, esta dependencia al carecer de tecnologías, operadores y procesos adecuados genera un riesgo ante la ocurrencia de un ciberataque a la infraestructura propia del sistema de comando y control que posee la Aviación del Ejército.

Según el objetivo N°02 se comprendió el empleo de las capacidades operativas de ciberdefensa mejoran la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército. Al respecto se demuestra que la presente investigación se enfoca que la Aviación del Ejército al poseer una plataforma definida como Blue Sky (sistema de comando y control) representa dicho activo un riesgo a las operaciones aéreas al no tener una seguridad digital y física para dicha plataforma. Siendo esta importante; sin embargo, el no tener capacidades de ciberdefensa en la infraestructura, hace que la AE se mantenga en una situación de vulnerabilidad, en vista que las aeronaves, sistema Blue Sky, así como diversas tecnologías pueden tener vulnerabilidades exponenciales durante las operaciones. Los resultados obtenidos concuerdan con la investigación de Carrillo (2020), en su investigación establece que la tecnología puede mejorar la eficacia y la eficiencia de los sistemas de C2, pero también advierte que la tecnología por sí sola no es suficiente para garantizar el éxito en las operaciones militares.

Este resultado concuerda con la teoría de Sevillano (2020), en su investigación “Implementación y optimización de un sistema de comando y control con capacidades de integración e interoperabilidad para el soporte de las operaciones en situaciones de crisis y/o emergencias nacionales” señala que el uso de un sistema C2 permite la supervisión, coordinación y control de las maniobras. Con los resultados presentados podemos señalar que el sistema blue Sky que posee la AE, requiere de sistemas de seguridad perimetral operado por especialistas en identificar anomalías, en la actualidad la AE, no cuenta con ningún requerimiento de ciberdefensa antes mencionado.

Según el objetivo N°03 se analizó la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y la normativa de operaciones aéreas de la Aviación del Ejército. Al respecto se demuestra que la presente investigación identificó la carencia de

una metodología basada en ciberdefensa, adecuada al tipo de organización en este caso al ser una organización de operaciones aéreas con una alta criticidad en las operaciones militares. Los resultados obtenidos concuerdan con la investigación de Bruderer (2019), en su investigación donde analizó que al carecer de un modelo o marco de gobernanza en ciberdefensa no permite las identificaciones de activos tecnológicos que se posee, ni el nivel de riesgo que significa para la dependencia. Este resultado concuerda con la teoría de NIST (2019) el cual establece un marco de gobernanza permite establecer el nivel de madurez que tiene la organización estableciendo indicadores de desempeño y gestión durante la mejora continua, un marco de gobernanza permite establecer un horizonte de cumplimiento de objetivos dentro de un periodo de tiempos, siendo todo ello necesario para las operaciones. Con los resultados presentados podemos señalar que el carecer de un marco de gobernanza de ciberdefensa dentro de Aviación hace que no se tenga claro la respuesta frente a ciberataques o ciberincidentes, por esta razón el periodo de escalamiento no quedaría definido en un periodo de tiempo, significando un agravante en la disrupción de las operaciones aéreas.

Según el objetivo N°04 se conoció las tecnologías militares de ciberdefensa que se deben emplear en las operaciones aéreas conjuntas que realiza la Aviación del Ejército. Al respecto se demuestra que la presente investigación establece que la AE no ha determinado que tecnologías militares necesarias para sus operaciones de ciberdefensa, se debe señalar que estás también deben de desarrollarse de manera conjunta, ser interoperables con las tecnologías que posee las otras fuerzas, y converger en una taxonomía única, se deber tener en claro que las tecnologías se deben identificar de acuerdo a los requerimientos operaciones. Los resultados obtenidos concuerdan con la investigación de La Junta Interamericana de Defensa JID (2020), en su publicación realizada en la “Guía de ciberdefensa de la JID” señala el empleo de tecnologías militares en las operaciones conjuntas de ciberdefensa en el ámbito aéreo, según el resultado de este trabajo de investigación afirma como un factor importante la articulación de las capacidades de ciberdefensa y que tienen como base la interoperabilidad eficiente y una taxonomía única

ante situaciones de ciberataques por parte de agentes hostiles. Este resultado concuerda con la teoría de Cubeiro (2020), en su investigación de sistemas de mando y control, destacando la importancia de la interoperabilidad de los sistemas, es decir, la capacidad de diferentes sistemas de C2 para comunicarse y trabajar juntos de manera efectiva. También señala que la tecnología puede ser una fuente de vulnerabilidad en los sistemas de C2, ya que los sistemas pueden ser atacados o interrumpidos. Con los resultados presentados podemos señalar que del levantamiento de información en la instalaciones de la aviación no se identificó un centro de datos, equipos de seguridad perimetral, ni mucho menos software que permita mitigar riesgos de explotación de vulnerabilidades, por otro lado se establece que el sistema de comando y control es un software comercial el cual puede determinar riesgo a las operaciones, La interoperabilidad en la Aviación del Ejército en el aspecto de ciberdefensa no se ha podido determinar, en vista que aún no se ha implementado esta capacidad y no se encuentra articulada con CITELE dentro del espectro del Ejército, ni con el CCFFAA como entidad directriz de ciberdefensa dentro de las fuerzas militares, siendo la articulación ciberdefensa importante tanto en el sector privado y público.

CAPÍTULO VI: Conclusiones y Recomendaciones

6.1 Conclusiones

Del Objetivo N°01

En relación al objetivo N°01. Los resultados obtenidos de esta investigación respaldan que la capacidad militar de ciberdefensa se vincula a través de una perspectiva de seguridad sobre los Sistemas de Comando y Control de la Aviación del Ejército. Al respecto, los protocolos basados en marcos de gobernanza con un enfoque de seguridad digital se ajustan a los requerimientos de defensa y explotación necesarios para los Sistemas de Comando y Control.

La evidencia surgida del estudio, establece que la capacidad militar de ciberdefensa requiere de una adecuada articulación de las tecnologías militares, como también de un adecuado marco de gobernanza y un empleo de capacidades operativas llevadas a través de la defensa y explotación, por lo tanto el sistema de comando y control dentro las operaciones que realiza la Aviación del Ejército constituye un activo crítico, en vista que permite mantener el enlace operacional del comandante y las operaciones que conduce.

Por otro lado, la investigación se vio limitado toda vez, que los Sistema de Comando y Control de la Aviación, carecen de marcos de gobernanza que establezcan claramente procesos y procedimientos para hacer frente a las actividades de las ciberamenazas, de esta manera se pudo establecer que el análisis correlacional de las capacidades de ciberdefensa con las medidas de seguridad actuales que poseen los Sistemas de Comando y Control no son las más óptimas.

El presente estudio realiza contribuciones, dentro de las cuales se puede señalar que al establecer un análisis desde un enfoque de empleo de capacidades de ciberdefensa sobre los Sistema de Comando y Control de la Aviación, permite identificar las capacidades operativas necesarias para la protección de los mencionados sistemas, teniendo en

consideración que las tecnologías son cada vez más avanzadas, lo cual con lleva a que las capacidades operativas se encuentren en una constante mejora continua.

Asimismo, los resultados de esta investigación proporcionan una nueva comprensión sobre el empleo de las capacidades de ciberdefensa, entendiendo que no se requiere que capacidades operativas sean implementadas en su totalidad, ni buscar un grado de madurez óptimo sobre la implementación, ya que esta puede llevarse de manera paulatina, teniendo en consideración lo complejo que comprende las infraestructuras tecnológicas compuesto por aeronaves, computadoras y redes.

Del Objetivo N°02

Con respecto al objetivo N°02. Los resultados obtenidos de esta investigación respaldan que el empleo de las capacidades operativas de ciberdefensa dentro del enfoque de la capacidad militar de ciberdefensa se establecen en dos (02) capacidades definidas: explotación y defensa conceptualizadas anteriormente, los cuales contribuyen de manera exponencial en la seguridad de los Sistemas de Comando y Control de la Aviación.

La evidencia del estudio, establece que el empleo de las capacidades operativas de ciberdefensa basadas en explotación y defensa, se conceptualizan en un conjunto de buenas prácticas, técnicas, tácticas y procedimientos el cual permiten viabilizar una adecuada gestión en la mejora de la seguridad de los Sistemas de Comando y Control.

Por otro lado, la investigación se vio limitado que desde un enfoque de ciberdefensa de empleo de capacidades operativas sobre activos críticos institucionales son muy limitados, por cuanto las buenas prácticas de las capacidades operativas de explotación y defensa poseen un enfoque basado en la ciberseguridad, a ello se debe tener en cuenta que este ámbito de ciberseguridad es el que más se ha desarrollado en la actualidad.

La presente investigación establece contribuciones, toda vez que muy pocos estudios sean realizados sobre capacidad operativas de explotación y defensa basados en ciberdefensa; sin embargo, al instaurar un enfoque en ciberseguridad nos ha permitido adoptar dichas capacidades trayendo consigo técnicas y tácticas actualizadas con herramientas digitales acordes a los requerimientos operacionales.

Asimismo, los resultados de esta investigación proporcionan una nueva comprensión sobre el empleo de las capacidades de explotación y defensa que estas pueden ser implementadas en aquellas organizaciones que disponen de una tecnología moderna dentro del ámbito del ciberespacio y de esta manera hacer frente a amenazas emergentes y avanzadas que puedan afectar las operaciones.

Del Objetivo N°03

Con respecto al objetivo N°03. Los resultados obtenidos demuestran que la pertinencia del marco de gobernanza de ciberdefensa consiste en establecer un modelamiento basado en procesos de ciberdefensa cuya implementación se enfoque en la seguridad al sistema de comando y control de la Aviación del Ejército, que permita la identificación de activos tecnológicos, identificación del nivel de riesgo e impacto en la dependencia,

La evidencia del estudio, establece que es necesario disponer de un marco de gobernanza de ciberdefensa, que permita establecer el nivel de madurez que tiene la organización estableciendo indicadores de desempeño y gestión durante la mejora continua.

Por otro lado, la investigación se vio limitada toda vez que las normativas aéreas de la Aviación del Ejército, nos disponen de lineamiento claros de respuesta frentes a ciberamenazas, de esta manera se podría establecer que el riesgo de ocurrencia de un evento es exponencial.

La presente investigación establece contribuciones dentro de las cuales se señala que la pertinencia basado en un marco de gobernanza de ciberdefensa es necesario, en vista que permitiría, llevar a cabo una adecuada gestión de la capacidad de ciberdefensa, se debe señalar que los marcos de gobernanza son empleados en el ámbito de la ciberseguridad y han funcionado y contribuido de la manera óptima. Esta investigación al señalar que un marco de gobernanza establecería la pertinencia necesaria para que los diferentes procesos y procedimientos no solo se establezcan en la Aviación del Ejército, sino en diferentes unidades militares que posean tecnologías militares modernas.

Asimismo, los resultados de esta investigación señalan que se debe tener en consideración que la AE al realizar operaciones y acciones militares se enmarca en el normativas de operativas aéreas, es pertinente entonces que la Aviación del Ejército deba poseer capacidades operativas de ciberdefensa y una metodología basada en buenas prácticas acorde a su requerimiento operacional que contribuya a que dichas operaciones y acciones militares que realiza la AE sean seguras desde un enfoque cibernético y el sistema de C2 de la Aviación del Ejército sea robusto en defensa frente a ciberataques.

Del Objetivo N°04

Con respecto al objetivo N°04. Los resultados obtenidos demuestran que las tecnologías militares de ciberdefensa son un factor importante dentro del empleo de las capacidades operativas, en vista que las dos (02) capacidades operativas de defensa y explotación se soportan en tu totalidad en soluciones tecnológicas, las cuales viabilizarán la seguridad del sistema de comando y control Blue Sky de la Aviación.

La evidencia del estudio, establece que es necesario conocer las tecnologías militares de ciberdefensa para las operaciones aéreas conjuntas que realiza la Aviación del Ejército. En vista que en la actualidad es necesario establecer una interoperabilidad que permita operaciones conjuntas y que estas posean las medidas de seguridad correspondientes.

Por otro lado, la investigación se vio limitada al no disponer de información sobre las tecnologías que poseen las Fuerzas Armadas, en lo que refiere a operaciones aéreas conjuntas, en vistas que al ser identificadas se podría conocer que tecnologías militares de ciberdefensa son acordes y definir procesos, procedimientos basados en las capacidades operativas de explotación y defensa frente a las ciberamenazas.

La presente investigación establece contribuciones, al identificar que es necesario poseer una interoperabilidad de ciberdefensa, en vista que las operaciones aéreas de la Aviación del Ejército también se realizan de manera conjunta, lo que lleva a disponer de una taxonomía que permita tener una respuesta oportuna ante cualquier situación.

Asimismo, los resultados de esta investigación señalan que la interoperabilidad de ciberdefensa es muy importante, ya que articula tecnología militar de ciberdefensa y

operaciones aéreas conjuntas, al referir de operaciones conjuntas podemos establecer las operaciones que llevan las tres (03) fuerzas así como la conducción que realiza el Comando Conjunto de las Fuerzas Armadas, es por ello que la interoperabilidad responde también a una articulación tecnológica de seguridad en el ámbito de la ciberdefensa.

6.2 Recomendaciones

De Acuerdo al Objetivo N°01

Analizar la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército.

La capacidad militar de ciberdefensa al estar articulado con un marco de gobernanza que disponga de buenas prácticas y procesos acordes a los requerimientos operacionales, una tecnología militar basado en soluciones de software y hardware robustos para un ambiente operacional complejo en la seguridad del sistema de comando y control dentro de la Aviación de Ejército del Perú, requiere que se implemente la capacidad militar de ciberdefensa a través de sus capacidades operativas de defensa y explotación, para ello la Aviación del Ejército deberá coordinar con Ciberdefensa y Telemática del Ejército (CITELE) que posee dentro de su estructura al Centro de Ciberdefensa del Ejército (CECIBER) centro responsable de la ciberdefensa dentro de la institución, para lo cual dicho centro deberá analizar los requerimientos en el ámbito de la ciberdefensa que deberán ser establecidas en el AE, para la securización del sistema de C2 de la AE, asimismo se debe tener en claro que las capacidades operativas de defensa y explotación son primordiales. Cabe mencionar que la Ley N°30999 establece que las FFAA, son garantes de la seguridad en el ámbito del ciberespacio, es por ello que es muy importante la coordinación y articulación de la aviación y el CITELE.

De Acuerdo al Objetivo N°02

Comprender el empleo de las capacidades operativas de ciberdefensa en la mejora de la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército.

Al respecto, el empleo de las capacidades operativas definidas como explotación y defensa, un marco de gobernanza basado en una adecuada gestión de la capacidad de

ciberdefensa, un escalamiento, respuesta efectiva y oportuna a ciberataques, con tecnologías de tipo militar para seguridad del C2 que posee la Aviación, hace que se recomiende que la Aviación de Ejército tome en cuenta la guía de procedimientos desarrollada con el propósito de establecer el empleo de la capacidad de ciberdefensa teniendo como capacidades operativas: defensa, explotación con el objetivo de establecer parámetros de seguridad en los sistemas de comando y control de la Aviación del Ejército, de acuerdo al anexo N°07.

Asimismo, la Aviación de Ejército en coordinación con la Dirección de Planeamiento del Ejército, implemente una sección de ciberdefensa el cual disponga de tecnologías apropiadas, metodología de seguridad física y lógica que permita que el sistema de comando y control de la Aviación opere de la manera más óptima, y con personal calificado en ciberdefensa, se debe tener en cuenta los tres (03) pilares en organizaciones que emplean infraestructuras tecnológica son fundamentales para las capacidad operativas de ciberdefensa y las operaciones en el ciberespacio, así como su articulación a los requerimientos operacionales de la Aviación, la tecnología a implementar requieren de un análisis de las ciberamenazas que se encuentran en el entorno, por cuanto se debe viabilizar infraestructuras de software y hardware como datacenter, simuladores, computadoras potentes, entornos controlados, etc. sin ello se verá limitado el cumplimiento de la misión asignada de defensa y explotación.

De acuerdo al Objetivo N°03

Analizar la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y normativa de operaciones aéreas de la Aviación del Ejército.

La importancia de contar con un marco de gobernanza que guarde pertinencia con la normativa de operaciones aéreas es fundamental para realizar operaciones de ciberdefensa, toda vez que consiste en establecer un enfoque basado en procesos de ciberdefensa cuya implementación en la seguridad al sistema de comando y control de la AE, permita la identificación de activos tecnológicos, identificación del nivel de riesgo e impacto, así como establecer el nivel de madurez que tiene la dependencia a través de indicadores de desempeño y gestión durante la mejora continua, tomando como asidero legal esta. Se

recomienda que la Dirección de Telemática del Ejército (DITELE), Ciberdefensa Telemática del Ejército (CITELE) y la AE, converjan en implementar la metodología denominada NIST con pertinencia en las normativas de operaciones aéreas, en vista que permitirán establecer un ciclo de madurez de la organización y adoptar buenas prácticas de otras organizaciones, al respecto NIST nos permite identificar los activos que posee una organización, en base a ello establecer los parámetros necesario para proteger los activos, con infraestructura tecnológica física y digital, de acuerdo a ello detectar comportamientos anómalos que se puedan realizar dentro de la infraestructura de la AE y poder obtener un respuesta acorde a las necesidades operacionales que permita que la operaciones aéreas se lleven de la manera más óptima, y por ultimo recuperarse de los daños ocasionados por incidentes o ataques cibernéticos. Esta metodología tiene un compendio de diferentes marcos en el ámbito de la ciberseguridad que han permitido que diferentes organizaciones protejan sus activos, asimismo NIST es adaptable a cualquier tipo de organización y dimensión realizando siempre un acompañamiento en su madurez, es por ello que la capacidad de ciberdefensa dentro de la Aviación del Ejército requiere de una metodología puesta práctica y con casos de éxito y que sea adaptable a cualquier dimensión y madurez de la organización.

De acuerdo al Objetivo N°04

Conocer las tecnologías militares de ciberdefensa para las operaciones aéreas conjuntas que realiza la Aviación del Ejército.

Las tecnologías militares de ciberdefensa basadas en soluciones de software y hardware, necesarias para las operaciones de ciberdefensa se enfocan en un principio de interoperabilidad para la seguridad de los sistemas de C2, es por ello que las operaciones aéreas conjuntas deben ser interoperables a fin que las operaciones y acciones militares sean ejecutadas de manera exitosa, al respecto se recomienda que la AE, Ciberdefensa Telemática del Ejército, establezcan una taxonomía de interoperabilidad con el Comando conjunto de las Fuerzas Armadas, toda vez que la Aviación del Ejército llevará operaciones aéreas con las diferentes fuerzas militares, debiendo tener en consideración que cada fuerza ha determinado sus propias tecnologías para sus operaciones, en el aspecto de ciberdefensa

también pasa que cada fuerza emplea su propia tecnología militar de ciberdefensa, siendo una prioridad que durante las operaciones militares las tecnologías deben ser interoperables a fin que se pueda llevar un C2 adecuado durante el proceso de las operaciones.

Referencias

Aguilar, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/4007

Alvarez, P. (2018). *Ética e investigación.* Colombia: Universidad Santiago de Cali.

Bruderer, R. S. (2019). *Diseño de un modelo de ciberseguridad para dispositivos.* Lima. Obtenido de https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/15134/BRUDERER_VEGA_RAMON_DISE%C3%91O_MODELO_CIBERSEGURIDAD.pdf?sequence=1&isAllowed=y

Cabello, E. C. (2001). *Los sistemas de mando y control: una vision histórico prospectiva.* Obtenido de file:///C:/Users/j/Downloads/Dialnet-LosSistemasDeMandoYControl-4602258%20(1).pdf

Carrasco, E. (2019). *Capacidad de respuesta del centro de ciberdefensa en las operaciones y acciones militares. Lima [Tesis de Maestria, Escuela de Guerra del Perú].* Obtenido de http://repositorio.esge.edu.pe/handle/20.500.14141/251

Carrillo, C. (2020). *La Ciberdefensa en el sistema de mando y control en la 9na Brigada Blindada. Lima. [Tesis de Maestria, Escuela de guerra del Perú].* Lima. Obtenido de http://repositorio.esge.edu.pe/handle/20.500.14141/246

CEEAG. (2017). *La ciberguerra: sus impactos y desafíos. Chile.* Andros.

COCID. (2019). *Operaciones de Ciberdefensa.* CCFFAA.

Congreso de la República del Perú. (2019). *Ley 30999 de 2019. Por lo cual se expide Ley de Ciberdefensa.*

Cordova, J., & Perez, L. (2021). La ciberdefensa en los sistemas de información sanitarios militares. *Scielo*. Obtenido de https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140

CSN. (2019). *Informe Anual de Seguridad Nacional.* Madrid. Obtenido de https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2019

Damasceno. (2019). *Evoluciòn del comando y control el caso BRABAT/MINUSTAH (2004-2017).*

De Vergara, E., & Trama, G. A. (2017). *Operaciones militares ciberneticas.* Vertra.

Diaz del rio, J. (2010). *LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR.* Imprenta del Ministerio de Defensa-España.

Ejército de Estados Unidos. (2018). *C2 Manual .* US ARMY.

España, C. d. (2019). *Estrategia Nacional de Ciberseguridad.* España.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación las rutas cuantitativa, cualitativa y mixta.* McGRAW-HILL Interamericana.

ICAO. (2022). *Abordar la ciberseguridad en la aviación civil.* Obtenido de https://www.icao.int/aviationcybersecurity/Pages/default.aspx

Indra. (2022). *mando, control, comunicaciones, computación, ciberdefensa, inteligencia, vigilancia y reconocimiento.* España.

Izcara, S. P. (2014). *Manual de investigacion cualitativa.* Mexico, Mexico: fontamara.

JID. (2020). II Conferencia de Ciberdefensa 2020. Bogotá, Colombia. Obtenido de https://www.iadfoundation.org/es/2020/05/28/ii-conferencia-de-ciberdefensa-2020/

Karpesky. (2021). *Las amenazas avanzadas persistentes. Recuperado el 05 enero 2022.* Obtenido de https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Mertens, D. (2015). *Diseño fenomenológico*. (S. gordillo, Productor) Obtenido de Scribd: https://es.scribd.com/document/483714258/Diseno-Fenomenologico

NIST. (2019). *Núcleo del marco.* Obtenido de https://www.nist.gov/

Quevedo, R. (2023). Ciberdefensa y ciberseguridad en el Perú. (CAEN, Ed.)

Rexton, P. (2014). *Como analizar la guerra en WIFI de ciberguerra a wikiguerra: la lucha por el ciberespacio.Recuperado el 25 octubre 2022.* REX. Obtenido de https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20141231_art007SPA.pdf.

Roberto, H., Carlos, F., & Pilar , B. (2014). *Metodologia de la Investigacion.* Mexico: McGRAW-HILL / INTERAMERICANA EDITORES. Obtenido de https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Saez, M. G. (2022). *La interoperabilidad y las operaciones aéreas conjuntas en la Fuerza Aérea del Perú, año 2022.* Lima: FAP.

Sevillano, M. A. (2020). *Implementaciòn y òptimizaciòn de un sistema de comando y control con capacidades de integraciòn e interoperabilidad para el soporte de operaciones.* EMCH.

Torres, R. (2016). *Estructuración de un sistema C4i y la innovacion [Tesis de Maestria, Centro de Altos Estudios Nacionales]. Obtenido de http://repositorio.caen.edu.pe/handle/20.500.14141/251.*

Urrutia, F. D. (2019). *Ciberseguridad marco NIST, un abordaje integral a la ciberseguridad. OEA.* Obtenido de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Vargas, X. (2011). *Cómo hacer una investigacion cualitativa.* México. Obtenido de http://www.paginaspersonales.unam.mx/files/981/94805617-Xavier-Vargas-B-COMO-HACER-INVESTIGA.pdf

Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (06 de Agosto de 2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de.* Lima, Perú: UPC.

Villegas, J. (1998). *el futuro del sistema integrado de mando y control aereo SIMCA.* España.

Waden, N. (2019). *CYBER1: El libro SMARTbook de Operaciones y Guerra Electrónica.* The Lightning Press.

Anexos

ANEXO 1

MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

TÍTULO: CAPACIDAD MILITAR DE CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022

Preguntas de Investigación	Objetivos	Teorías	Categorías	Subcategorías	Metodología	Análisis de datos
¿Cómo se empleó la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022? ¿Cómo el empleo de las capacidades operativas de ciberdefensa mejoraron la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022? ¿Cómo se estableció la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y la normativa de operaciones aéreas de la Aviación del Ejército el año 2022? ¿Cuáles son tecnologías militares de ciberdefensa que se deben emplear en las operaciones aéreas conjuntas que realiza la Aviación del Ejército?	Analizar la capacidad militar de ciberdefensa en la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022. Comprender el empleo de las capacidades operativas de ciberdefensa en la mejora de la seguridad de los Sistemas de Comando y Control de la Aviación del Ejército el año 2022. Analizar la pertinencia del marco de gobernanza de ciberdefensa del Ejército del Perú y normativa de operaciones aéreas de la Aviación del Ejército el año 2022. Conocer las tecnologías militares de ciberdefensa para las operaciones aéreas conjuntas que realiza la Aviación del Ejército.	La presente investigación se sustenta en la teoría basada en la implementación de la doctrina de empleo de la ciberdefensa en los sistemas de comando y control de la Aviación del Ejército y su concepción propia de las operaciones en el ciberespacio y como está vinculada a las operaciones aéreas en apoyo a las acciones y operaciones militares que realiza el Ejército.	Capacidad militar de ciberdefensa Comando y control en la Aviación militar . Operaciones aéreas conjuntas	• Tecnología militar de ciberdefensa • Capacidades operativas. • Marco gobernanza en ciberdefensa • Sistemas de comando y control militar • Normativa operaciones aéreas • Interoperabilidad de ciberdefensa	**Enfoque:** Cualitativo **Tipo:** Teórico- empírica **Diseño**: Fenomenológico **Método:** Hermenéutico **Muestra**: Muestra de expertos, teniendo previsto la entrevista a 08 oficiales expertos con amplios conocimientos del tema y 05 oficiales observadores	**Técnicas:** Entrevista Observación Análisis documental **Instrumentos:** Guía de entrevistas Guía de observación Ficha documental **Técnica de análisis de datos:** Se desarrollará de manera artesanal

ANEXO 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

Buenos días/tardes, expreso mi agradecimiento por el tiempo y la atención prestada para poder realizar esta entrevista, cuya información y comentarios proporcionados serán muy valiosos para profundizar la presente investigación.

Entrevistado: Grado Académico: DNI: Lugar – fecha: Experiencia alcanzada:	
Título de la investigación: Capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022	
N°	GUÍA DE ENTREVISTA
01	Conociendo que los sistemas de comando y control de la aviación se soportan en tecnologías modernas ¿Que opina de la capacidad militar de ciberdefensa en la protección de los sistemas de C2 de la Aviación del Ejército?
	Rpta
02	¿Cómo considera Ud., que debería emplearse las capacidades operativas de ciberdefensa en la seguridad de los sistemas de C2 de la Aviación del Ejército?
	Rpta
03	¿Cómo enfocaría Ud., la pertinencia del marco de gobernanza de ciberdefensa y la normativa de operaciones aéreas?
	Rpta
04	En la protección de los sistemas de C2 ¿Qué tecnologías militares de ciberdefensa se emplean actualmente para identificar ciberamenazas en el ciberespacio en Aviación del Ejército?
	Rpta
05	Conociendo que la doctrina de ciberdefensa es limitada en el EP, ¿Qué estándares normativos de ciberdefensa emplearán para la seguridad de los sistemas de C2?
	Rpta
06	Sabiendo que las operaciones aéreas conjuntas son importantes para operaciones militares ¿Qué tecnologías militares de ciberdefensa deben emplearse?
	Rpta
07	¿Cómo sería la interoperabilidad de las capacidades operativas de ciberdefensa con las diferentes plataformas tecnológica que utiliza el sistemas de C2 de la aviación del Ejército?
	Rpta
08	¿Cómo definiría Ud., en la actualidad el nivel de seguridad del sistema de comando y control que posee la Aviación del Ejército?
	Rpta

FICHA DE ANÁLISIS DOCUMENTAL

Se seleccionó los documentos que contenían información que está relacionada a la capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército.

TIPO DE DOCUMENTO	PAÍS	REFERENCIA	TEMAS
Ley	Perú	Ley de Ciberdefensa Ley N°30999.	Capacidad de ciberdefensa de las FF. AA
Libro	Chile	La Ciberguerra: sus impactos y desafíos	Ciberguerra
Informe	EE. UU	II Conferencia de Ciberdefensa	Operaciones de ciberdefensa
Libro	Argentina	Operaciones militares ciberneticas	Capacidades de ciberdefensa
Libro	EE. UU	Ciberseguridad Marco NIST.	Marco de trabajo
Tesis	España	El futuro del sistema integrado de mando y control aereo SIMCA	Sistema de comando y control
Tesis	Perú	Capacidad de respuesta del centro de ciberdefensa en las	Capacidad de respuesta de ciberdefensa

		operaciones y acciones militares	
Manual	Perú	Operaciones de Ciberdefensa	Ciberdefensa
Manual	España	mando, control, comunicaciones, computación, ciberdefensa, inteligencia, vigilancia y reconocimiento	C4I
Guía	EEUU	Núcleo del marco NIST	Framework de ciberseguridad
Tesis	Perú	Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones	Modelo de ciberseguridad
Guía	Perú	Ciberdefensa y ciberseguridad en el Perú	Ciberdefensa y ciberseguridad
Tesis	Perú	Implementaciòn y òptimizaciòn de un sistema de comando y control con capacidades de integraciòn e	Sistema de comando y control

		interoperabilidad para el soporte de operaciones	
Informe	EEUU	Las amenazas avanzadas persistentes	Ciberamenazas
Manual	EEUU	C2 Manual	Comando y control norteamericano
Tesis	Perú	Diseño de un modelo de ciberseguridad para dispositivos	Modelo de ciberseguridad
Tesis	Perú	Estructuración de un sistema C4i y la innovacion	Comando y control
Articulo	España	La ciberdefensa en los sistemas de información sanitarios militares	ciberdefensa
Artículo	Ecuador	Proyección de la Ciberdefensa en el Ecuador al 2021	Ciberespacio, Defensa nacional, seguridad interna, sistemas de seguridad y política de seguridad
Revista	Chile	Ciberseguridad en América Latina y ciberdefensa en Chile	Ciberseguridad y Ciberdefensa.

Guía	Europa	Abordar la ciberseguridad en la aviación civil	Ciberseguridad en la aviación
Guía	EEUU	Ciberseguridad marco NIST, un abordaje integral a la ciberseguridad. OEA	Marco NIST

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN:

CAPACIDAD MIUTAR DE CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022

I. *DATOS DEL EXPERTO:*

a. Apellidos y nombres: Talavera Virado Samuel
b. Grado académico-profesión: Dr en educación
c. D.N.I.: 09771027
d. N° de teléfono: 996132050
e. Lugar y fecha: Chorrillos 23 F.
L Firma: [firma]

3

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor(es) del instrumento: Michael Joseph Latorre sosaya
b. Institución a la que pertenece: Ejército del Perú
c. Método de imrestígadón: Hermeneútico
d. Tipo de entrevista: Semi estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración e: 0 a 1
01	Diseño	Convocatoria: Lugar - tiempo. Cootenidoo: Propuesta de temas- preguntas - respuestas.	9
02	Organización	Selección, informantes - representación de temas - tipo de respuesta - número de entrevistas.	9
03	Estructuración	Guía de entrevista: Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista. Contexto de los datos: Conocer experiencias del entrevistado. Tema pro ios: Aspectos que interesen	8
04	Secuencial	C-Orrelación a variables - dimer>.siones e indicadores. Sigue un orden lógico y pre-requísítoriaL	9
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con !as experiencias que esperan ser revaloradas en el cuestionario.	9
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las **variables de investigación**.	9
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en e! marco de doctrina, leyes, teorjas vi entes.	9
08	Cootra.«tación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	9
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	9
iO	Análisis e interpretación	Se ha adecuado algún ínstrmmento o herramienta para verter los resultados *de la entrevista y analizarlos /interpretarlos.*	

IV. RESULTADO DE VALORACIÓN:

88%

V. OPINIÓN D-E APUCACIÓN

Instrumento | Aplicable

Aspectos para la valoración

Validada por TRES expertos, con grado academice de maestro/doctor.
Debe aplicarse la prneba de la "V" de Aiken
Resultado mínimo aprobatorio: 0.85 u 85%
La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN:
CAPACIDAD MILITAR DE CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : Dr. Lozo Mata Miguel
b. Grado académico-profesión : Magister en Ciberseguridad
c. D.N.I. : 09961682
d. N° de teléfono : 969766138
e. Lugar y fecha : Chorrillos 9 Jun 23
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor(es) del instrumento : Michael Joseph Latorre Sosaya
b. Institución a la que pertenece: Ejército del Perú
c. Método de investigación : Hermenéutico
d. Tipo de entrevista : Semi estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: 0 a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	9
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	10
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	10
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitorial.	9
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	9
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	9
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	9
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	9
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	9
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	9

IV. RESULTADO DE VALORACIÓN:

92 %

V. OPINIÓN DE APLICACIÓN

Instrumento Aplicable.

Aspectos para la valoración

- Validada por TRES expertos, con grado academico de maestro/doctor.
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN: CAPACIDAD MILITAR DE CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : OLAYA MORENO MÁXIMO VICENTE
b. Grado académico profesión : DOCTOR EN ADMINISTRACIÓN Y EXPERTO EN COMUNICACIONES
c. D.N.I. : 43296212
d. N° de teléfono : 944459555
e. Lugar y fecha : LIMA, 21 DE JUNIO DE 2023
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor(es) del instrumento : MICHAEL JOSEPH LATORRE SOSAYA
b. Institución a la que pertenece: EJÉRCITO
c. Método de investigación : HERMENEÚTICO
d. Tipo de entrevista : SEMIESTRUCTURADA

III. ASPECTOS DE EVALUACIÓN

°	Criterios	Indicadores	Valoración De: 0 a 1
1	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	9
2	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	10
3	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	9
4	Secuencial	Con relación a variables – dimensiones o indicadores. Sigue un orden lógico y pre-requisitorial.	10
5	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	8
6	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	9
7	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	9
8	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	9
9	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	9
0	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	9

IV. RESULTADO DE VALORACIÓN:

91 %

V. OPINIÓN DE APLICACIÓN

INSTRUMNENTO APLICABLE

Aspectos para la valoración

- Validada por TRES expertos, con grado académico de maestro/doctor.
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

ANEXO 4

AUTORIZACIÓN PARA RECOLECCIÓN DE DATOS

PERÚ | Ministerio de Defensa | Ejército del Perú | Aviación del Ejército

"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

Callao, 23 de octubre del 2023

Oficio N° 210 /AE/DIEDOC/05.00.

Señor General de Brigada
Director de la Escuela Superior de Guerra del Ejército.

Asunto : Facilidades para el levantamiento de datos e informaciones.

Ref : Oficio N° 61 – 2023/ESGE-EPG/U-26.e.a. del 04 de abril 2023

Tengo el honor de dirigirme a Ud., para manifestarle que este comando autoriza al: **MY EP LATORRE SOSAYA Michael Joseph**, estudiante de la XI Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército para el levantamiento de datos e informaciones relacionadas a la investigación titulada: **"DOCTRINA DE EMPLEO DE LA CIBERDEFENSA EN LOS SISTEMAS DE COMANDO Y CONTROL DE LA AVIACIÓN DEL EJÉRCITO, 2022".**

Aprovecho la oportunidad para expresarle los sentimientos de mi especial consideración y estima personal

Dios guarde a Ud.

AVIACIÓN DEL EJÉRCITO - COMANDANCIA

O-224347267-04
LUIS EDUARDO CARRANZA VILAHUR
General de Brigada
Comandante General de la Aviación del Ejército

DISTRIBUCIÓN
- ESG.....01
- ARCHIVO.....01/02

ANEXO 5

COMPROMISO ÉTICO

Declaración de Compromiso Ético

El presente trabajo de investigación titulado: **Capacidad militar de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército, 2022**, se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación en Ciencias Militares promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado.

En vista de lo anterior:

Yo Bach Michael La torre Sosaya, egresado de la XI Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado esta investigación siguiendo las instrucciones brindadas por el Departamento de Gestión de la Investigación, desde la elaboración del marco referencial y recolección de la información, hasta el análisis de datos y elaboración del informe final.

En tal sentido la información contenida en el presente documento es producto de mi trabajo personal, apegándome a la legislación sobre propiedad intelectual, sin haber incurrido en falsificación de la información o cualquier tipo de fraude, por lo cual me someto al marco legal y normativo vigente relacionado a dicha responsabilidad, así como a las normas disciplinarias establecidas en la ESGE-EPG.

Michael LATORRE SOSAYA
DNI: 42459772

ANEXO 6

HOJA DE DATOS PERSONALES

HOJA DE DATOS PERSONALES

GRADO **TTE CRL EP**

NOMBRES **MICHAEL JOSEPH**

APELLIDOS **LATORRE SOSAYA**

EMAIL **michaeljosephlatorre21@gmail.com**

DIRECCIÓN **Jr. Riobamba 1656 S.M.P**

TELEFONO **+51 993334474**

FIRMA

ANEXO 7

APORTE A LA INVESTIGACIÓN

Aporte de Investigación

7.1 Título del aporte a la investigación

Guía de procedimiento del empleo de la capacidad de ciberdefensa en defensa y explotación en los sistemas de comando y control de la Aviación del Ejército.

7.2 Objetivos del aporte de investigación

Esta guía de procedimientos ha sido desarrollada con el propósito de establecer el empleo de la capacidad de ciberdefensa teniendo como capacidades operativas: defensa, explotación con el objetivo de establecer parámetros de seguridad en los sistemas de comando y control de la Aviación del Ejército, con la finalidad para que dicha dependencia lleve a cabo sus operaciones aéreas en apoyo a las operaciones y acciones militares, es por ello que identificar que las aeronaves son un activo institucional requieren que estas sean protegidas en el ámbito digital, ya que su transmisión de data se realiza a través del ciberespacio y su infraestructura nativa se encuentra articulada a este ámbito, pudiendo ser vulnerable a los diferentes vectores de ataque de las ciberamenazas teniendo como efecto final las disrupción de las operaciones, todo este marco de ciberdefensa tiene como soporte al factor humano, tecnológico y de procesos establecidos

7.3 Justificación del aporte de investigación

La capacidad de ciberdefensa en los sistemas de comando y control de la Aviación del Ejército son necesarias ya que este activo es soporte a las operaciones y acciones militares que realiza el Ejército del Perú, por cuanto requiere de infraestructuras tecnológicas seguras y fiables para las operaciones, debemos tener en consideración que el medio de enlace de las aeronaves se establece también a través del ciberespacio, siendo este medio aun poco estudiado desde el enfoque militar, el ciberespacio al ser un medio poco estudiado es aprovechado por ciberamenazas cuya finalidad radica a muchas motivaciones pudiendo ser estas económicas, espionaje, etc. Por cuanto el empleo de las capacidades operativas de explotación, defensa es importante toda vez que la Aviación de Ejército dentro de su estructura organizacional dispone de una compañía de comunicaciones, por cuanto se recomienda que dentro de esta compañía se implemente una sección de ciberdefensa el cual disponga de tecnologías apropiadas, metodología de seguridad física y lógica que permita que el sistema de comando y control de la Aviación del Ejército opere de la manera más óptima, y con personal calificado en ciberdefensa

Asimismo, en un estado de ciberguerra, que demandaría la realización de operaciones militares, requeriría que las capacidades operativas de ciberdefensa dentro de la Aviación sean las más optimas, lo que demandaría tiempo esfuerzo y recursos para que estos sean lo más oportunos posibles.

7.4 Aporte de investigación

Introducción

La transformación digital de los sistemas militares, particularmente aquellos vinculados al comando y control aeronáutico, ha incrementado significativamente la superficie de exposición a amenazas cibernéticas. En la Aviación del Ejército del Perú, la interconectividad de redes operacionales (OT), redes corporativas (IT) y sistemas de comunicaciones tierra-aire exige la adopción de una arquitectura integral de defensa cibernética.

La presente Guía de Procedimientos constituye una propuesta estructurada orientada a fortalecer la seguridad perimetral, la ciberinteligencia y la capacidad de respuesta ante incidentes, garantizando la continuidad de las operaciones aéreas militares.

Finalidad y Objetivo

Finalidad. Establecer procedimientos técnicos y organizacionales para proteger el Sistema de Comando y Control (C2) Blue Sky y la infraestructura tecnológica crítica de la Aviación del Ejército, asegurando la confidencialidad, integridad y disponibilidad de la información.

Objetivo General. Implementar una arquitectura de defensa en profundidad que permita prevenir, detectar, contener y recuperar oportunamente ante ciberamenazas que afecten los sistemas operacionales.

Marco Normativo y Referencial

La Guía se encuentra alineada con:

- Ley N.° 30999 – Ley de Ciberdefensa.
- Política Nacional de Ciberseguridad.
- Directivas del Comando Conjunto de las FF.AA.
- Estándares internacionales como:
    - National Institute of Standards and Technology (NIST SP 800-53 y SP 800-207 – Zero Trust).
    - International Organization for Standardization (ISO/IEC 27001:2022).
    - Marco MITRE ATT&CK.

Arquitectura de Seguridad Propuesta

La propuesta adopta un modelo de **defensa en profundidad**, estructurado en cuatro capas principales:

1. Seguridad Perimetral

- Firewalls de Nueva Generación (NGFW).
- Sistemas IDS/IPS.
- Protección Anti-DDoS.
- WAF para aplicaciones críticas.

- Segmentación de red y zonas desmilitarizadas (DMZ).
- VPN seguras con cifrado IPsec o TLS 1.3.

2. Segmentación IT/OT

Se establece una separación lógica y física entre:

- Red corporativa de servidores.
- Red corporativa de usuarios.
- Red operacional de supervisión.
- Red operacional de control (PLC/HMI).

El monitoreo inter-VLAN e IT/OT reduce el movimiento lateral y limita el impacto de intrusiones.

3. Monitoreo y Centro de Operaciones de Seguridad (SOC)

- Implementación de SIEM para correlación de eventos.
- Integración de telemetría de red, endpoints y sistemas críticos.
- Búsqueda proactiva de amenazas (Threat Hunting).
- Indicadores clave de desempeño: MTTD y MTTR.

4. Modelo de Confianza Cero (Zero Trust)

En concordancia con NIST SP 800-207, se adopta el principio de:

- Verificación continua.
- Mínimo privilegio.
- Control granular de accesos.
- Monitoreo constante de identidad y dispositivos.

Capacidad de Explotación Cibernética e Inteligencia de Amenazas

La Guía incorpora un componente proactivo basado en inteligencia de amenazas (CTI), que incluye:

- Integración de feeds de vulnerabilidades (CVE).
- Análisis bajo la matriz MITRE ATT&CK.
- Uso de plataformas colaborativas como MISP para intercambio de Indicadores de Compromiso (IoC).
- Automatización mediante herramientas SOAR.
- Simulaciones Red Team / Blue Team.

Este enfoque permite anticipar amenazas avanzadas persistentes (APT) y reducir riesgos estratégicos y operacionales.

Plan de Respuesta a Ciberincidentes

Se establece un ciclo estructurado de gestión de incidentes:

- Preparación
- Detección y análisis
- Contención

- Erradicación
- Recuperación
- Lecciones aprendidas

Se define un Equipo de Respuesta a Incidentes (CSIRT) con roles claramente establecidos (Coordinador, Analista de Seguridad, Administrador de Sistemas, Comunicaciones y Área Legal).

Los incidentes se clasifican en niveles: Bajo, Medio, Alto y Crítico, según su impacto en las operaciones aéreas y sistemas estratégicos.

Asimismo, se contemplan:

- Simulacros semestrales.
- Revisión anual del plan.
- Preservación de evidencia digital.
- Intercambio interinstitucional de información.

Impacto Estratégico Esperado

La implementación de la Guía permitirá:

- Incrementar la resiliencia cibernética institucional.
- Proteger el sistema C2 Blue Sky y redes operacionales.
- Reducir tiempos de detección y respuesta.
- Minimizar riesgos de interrupción de operaciones aéreas.
- Integrar la dimensión cibernética al planeamiento militar.
- Consolidar una cultura organizacional de seguridad digital.

Conclusión

La presente propuesta establece un modelo integral de defensa y explotación cibernética para la Aviación del Ejército, combinando seguridad perimetral, segmentación IT/OT, inteligencia de amenazas, arquitectura Zero Trust y un plan robusto de respuesta a incidentes.

Su adopción permitirá evolucionar hacia una postura de seguridad proactiva, resiliente y alineada con estándares internacionales, contribuyendo directamente a la protección de los activos estratégicos y a la continuidad de las operaciones aéreas del Estado.

Nota. La Guía de Procedimientos completa con el nombre de “Guía de procedimiento del empleo de la capacidad de ciberdefensa en defensa y explotación en los sistemas de comando y control de la Aviación del Ejército” se encuentra en versión digital en el repositorio de la

ANEXO 8

CD CONTENIENDO LA TESIS EN PDF

ESCUELA SUPERIOR DE GUERRA

DEL EJÉRCITO - ESCUELA DE POSTGRADO

TESIS

Capacidad Militar de Ciberdefensa en los Sistemas de Comando y Control de la Aviación del Ejército, 2022

AUTOR:

Bach. Latorre Sosaya Michael Joseph

2025

ANEXO 9

REPORTE DE SIMILITUD TURNITÍN

EF_MLATORRES_29NOV25_INFORME resuelto (1).docx

AÑO 2026

AÑO 2026

Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:566943321

Fecha de entrega
12 mar 2026, 4:49 p.m. GMT-5

Fecha de descarga
12 mar 2026, 4:54 p.m. GMT-5

Nombre del archivo
EF_MLATORRES_29NOV25_INFORME resuelto (1).docx

Tamaño del archivo
7.5 MB

122 páginas

26.172 palabras

150.220 caracteres

16% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

14% Fuentes de Internet

1% Publicaciones

9% Trabajos entregados (trabajos del estudiante)