ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

La capacidad de Ciberdefensa del Ejército del Perú y su influencia en el Ciberespacio, 2024

AUTORES:

BACH. José Raúl Tineo Arenas

(orcid.org/0009-0004-8476-7678)

BACH. Nicéforo Gutiérrez Chávez

(orcid.org/0009-0008-4820-4041)

Para optar el Grado Académico de

MAESTRO EN ESTRATÉGIA Y GEOPOLÍTICA

ASESOR:

DR. Iván Ricardo Barreto Bardales

(orcid.org/0009-0006-7908-9459)

LÍNEA DE INVESTIGACIÓN:

Evaluación Estratégica

2025

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 011 – 2025/ DGI/PAME

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los diecisiete (17) días del mes de diciembre del año dos mil veinticinco, siendo las 08:55 horas, se reunió el jurado evaluador conformado por los docentes:

- **Doctor** **GAMALIEL MANUEL GUSTAVO TALAVERA PRADO** **Presidente**
- **Maestro** **ROBERTO JOAQUIN VIVANCO BURGOS** **Secretario**
- **Maestro** **JOSE LUIS AGUILAR OBLITAS** **Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 011-2025/SIE/DGI/ESGE-EPG** del 08 de diciembre de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"LA CAPACIDAD DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ Y SU INFLUENCIA EN EL CIBERESPACIO, 2024"**, presentado por los Bachilleres **NICEFORO GUTIERREZ CHAVEZ y JOSE RAUL TINEO ARENAS**, para optar el Grado Académico de Maestro en Estrategia y Geopolítica, 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).

En mérito del cual, el jurado APRUEBA (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Estrategia y Geopolítica.

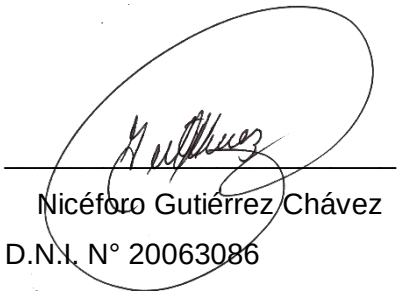
Firmado, en Chorrillos a los diecisiete (17) días del mes de diciembre del año dos mil veinticinco.

DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO PRESIDENTE	MG. ROBERTO JOAQUIN VIVANCO BURGOS SECRETARIO	MG. JOSE LUIS AGUILAR OBLITAS VOCAL

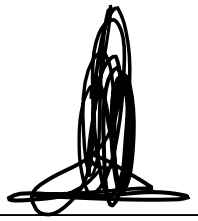
Autorización de Publicación y Uso

Nosotros, Bach. Nicéforo Gutiérrez Chávez y Bach. José Raúl Tineo Arenas, a través del presente documento, autorizamos la Escuela Superior de Guerra del Ejército – Escuela de Postgrado, la publicación del texto completo o parcial de la tesis de grado titulada: **"La Capacidad de Ciberdefensa del Ejército del Perú y su Influencia en el Ciberespacio, 2024"**, presentada para optar el grado académico de Maestros en Maestros en Estrategia y Geopolítica 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 mantendrá permanente y definitivamente 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, 10 de julio de 2024



Nicéforo Gutiérrez Chávez
D.N.I. N° 20063086



José Raúl Tineo Arenas
D.N.I. N° 10381102

Declaración Jurada de Autoría

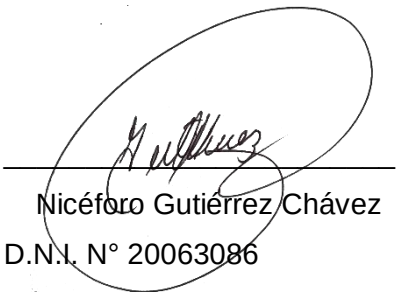
Mediante el presente documento, nosotros, Bach. Nicéforo Gutiérrez Chávez, identificado con Documento Nacional de Identidad N° 20063086, con domicilio en Pasaje los Descalzos N° 185, Rimac, y Bach. José Raúl Tineo Arenas, identificado con Documento Nacional de Identidad N° 10381102, con domicilio en Villa Militar Oeste Avenida Elena fray de Pastor, Casa N° 65, Chorrillos, egresados de la maestría en Estrategia y Geopolítica, declaramos bajo juramento que:

Somos los autores de la investigación que presentamos ante esta institución con fines de optar al grado académico de Maestro en estrategia y Geopolítica.

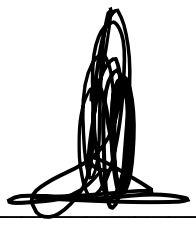
Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por los suscritos, para optar otro grado académico ni título profesional alguno. Declaramos que se ha citado debidamente toda idea, texto, figura, formulas, tablas u otros que corresponde a los suscritos u a otro en respecto irrestricto a los derechos del autor. Declaramos conocer y nos sometemos al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaramos bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicados, ni copiados. Que no hemos cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximimos de toda responsabilidad a la Escuela Superior de Guerra del Ejército – Escuela de Postgrado y nos declaramos como los únicos responsables.

Chorrillos, 10 de julio de 2024



Nicéforo Gutiérrez Chávez
D.N.I. N° 20063086



José Raúl Tineo Arenas
D.N.I. N° 10381102

Dedicatoria:

A Dios Todopoderoso, por brindarnos fortaleza, esperanza y guía a lo largo de este proceso, especialmente en medio de las dificultades que se presentaron durante este año. Su presencia nos permitió seguir adelante y valorar el apoyo constante de nuestras familias, quienes con su comprensión, motivación y respaldo incondicional nos impulsaron a continuar trabajando para alcanzar nuestras metas profesionales.

Índice

Página

Capítulo I: El Problema de la Investigación

Capítulo II: Marco Teórico

Capítulo III. Método

Capítulo IV: Resultados

Capítulo V: Discusión de Resultados

Capítulo VI: Conclusiones y Recomendaciones

Anexos:

Lista de tablas

Lista de figuras

Resumen

La presente investigación titulada "La Capacidad de Ciberdefensa del Ejército del Perú y su Influencia en el Ciberespacio, 2024" tiene como objetivo determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio durante el año 2024. Para ello, se empleó un enfoque cuantitativo, con un estudio de tipo básico, nivel explicativo y diseño no experimental de corte transversal. La población de estudio estuvo conformada por 52 integrantes del personal militar, entre oficiales superiores, oficiales subalternos, técnicos y suboficiales pertenecientes al Centro de Ciberdefensa del Ejército, Centro de Informática del Ejército y la Dirección de Telemática del Ejército. La investigación analiza cuatro dimensiones clave de la capacidad de ciberdefensa: defensa, explotación, respuesta e investigación digital, evaluando su impacto en las redes interconectadas e interdependientes de infraestructura tecnológica y de datos almacenados. La metodología contempló la aplicación de encuestas como técnica principal de recolección de datos, las cuales fueron procesadas y analizadas con el software estadístico SPSS (versión 25). El análisis permitió identificar una correlación estadísticamente significativa entre las capacidades de ciberdefensa y su influencia en el ciberespacio, evidenciándose variaciones relevantes en las distintas dimensiones evaluadas. Específicamente, se encontró una correlación baja en la capacidad de defensa (0.207), correlaciones moderadas en las capacidades de explotación (0.540) y respuesta (0.513), y una correlación alta en la capacidad de investigación digital (0.804). Estos hallazgos sugieren áreas críticas que requieren atención y mejora en la estructura de ciberdefensa del Ejército. El estudio contribuye significativamente al entendimiento de las fortalezas y debilidades en las capacidades de ciberdefensa del Ejército Peruano, proporcionando una base sólida para el desarrollo de estrategias que fortalezcan la postura de defensa en el ciberespacio frente a las crecientes amenazas cibernéticas.

Palabras clave: Ciberdefensa, ciberespacio, capacidad militar, seguridad digital, infraestructura tecnológica, Ejército del Perú.

Abstract

This research titled "The Cyber Defense Capability of the Peruvian Army and its Influence on Cyberspace, 2024" aims to determine the influence of the Peruvian Army's cyber defense capability in cyberspace during 2024. The study adopts a quantitative approach, basic type, explanatory level, and non-experimental cross-sectional design. The population consists of 52 military personnel including senior officers, junior officers, technicians, and non-commissioned officers working at the Army Cyber Defense Center, Army Computer Center, and the Army Telematics Directorate. The research analyzes four key dimensions of cyber defense capability: defense, exploitation, response, and digital investigation, evaluating their impact on interconnected and interdependent networks of technological infrastructure and stored data. The methodology includes surveys as the main data collection instrument, with statistical analysis using SPSS25 software. The results reveal a significant correlation between cyber defense capabilities and their influence in cyberspace, with important variations among the different dimensions analyzed. Specifically, a low correlation was found in defense capability (0.207), moderate correlations in exploitation (0.540) and response (0.513) capabilities, and a high correlation in digital investigation capability (0.804). These findings suggest critical areas requiring attention and improvement in the Army's cyber defense structure. The study significantly contributes to understanding the strengths and weaknesses in the Peruvian Army's cyber defense capabilities, providing a solid foundation for developing strategies to strengthen the defense posture in cyberspace against growing cyber threats.

Keywords: Cyber defense, cyberspace, military capability, digital security, technological infrastructure, Peruvian Army.

Introducción

El vertiginoso desarrollo de las tecnologías de la información y de las comunicaciones ha modificado de manera significativa el escenario de la seguridad y la defensa nacional. El ciberespacio se ha convertido en el quinto dominio de interacción humana, presentando nuevos desafíos y amenazas para los Estados y sus instituciones militares. En este contexto, la capacidad de ciberdefensa se configura como un factor esencial para resguardar los intereses nacionales y garantizar la soberanía en el entorno digital. Casos emblemáticos como el ataque cibernético a Estonia en 2007 y el incidente de Ecuador en 2019 demuestran la vulnerabilidad de los estados ante estas nuevas formas de agresión.

La problemática central radica en la necesidad de evaluar e impulsar el fortalecimiento de las capacidades de ciberdefensa en el Ejército del Perú. Si bien la promulgación de la Ley N° 30999 de Ciberdefensa en 2019 marcó un hito importante al definir la ciberdefensa como una capacidad militar esencial, es fundamental determinar la efectividad de estas capacidades y su influencia real en el ciberespacio. Surge entonces la interrogante sobre cómo las diferentes dimensiones de la capacidad de ciberdefensa - defensa, explotación, respuesta e investigación digital - influyen en la protección del ciberespacio nacional.

En este contexto, el objetivo central de esta investigación es determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio durante el año 2024. A través de un análisis cuantitativo que involucra a 52 efectivos militares pertenecientes al Centro de Ciberdefensa, Centro de Informática y la Dirección de Telemática del Ejército, se pretende aportar evidencia empírica acerca de la eficacia de las capacidades actuales y establecer las bases para el diseño de estrategias que fortalezcan la defensa en el ciberespacio.

Capítulo I: El Problema de Investigación

1.1. Planteamiento del Problema

Es ampliamente reconocido que el avance tecnológico se desarrolla de manera acelerada, especialmente en el ámbito de las comunicaciones, lo que genera preocupación para la seguridad y defensa de los Estados. Este escenario representa un desafío frente a las amenazas que emergen desde el ciberespacio, esto demuestra que la seguridad de los Estados no depende únicamente de su dimensión territorial, ya que el ámbito digital también representa un espacio vulnerable a amenazas desestabilizadoras.

Nagurney & Shukla (2017) señalan que las nuevas tecnologías de información y comunicación han dado origen al ciberespacio (Internet). Este constituye el quinto dominio de interacción humana y cada día se hace más extenso.

En definitiva, al aparecer nuevas amenazas que pueden ser creadas por individuos, organizaciones o Estados, pueden causar efectos negativos en las víctimas, obteniendo beneficios al perpetrador. Este escenario ha generado un clima de hostilidad que puede ser utilizado por estrategas para evaluar la situación de los Estados en el ámbito de la guerra. En consecuencia, los gobiernos, cuya responsabilidad es garantizar la seguridad de sus ciudadanos, se ven obligados a adaptar sus estructuras y marcos normativos a fin de enfrentar y prevenir estas nuevas amenazas. Es necesario reconocer que los ciberataques son reales y que su magnitud puede llegar a afectar gravemente la economía, las instituciones y las estructuras de aquellos Estados que carecen de una defensa nacional enfocada en el ciberespacio, convirtiéndolos en blancos vulnerables para ciberterroristas, hackers y otros actores que disponen de herramientas digitales para ejecutar sus planes.

En ese sentido, la estructura social y política del estado- nación constituye una respuesta orientada a la seguridad y debe contar con las condiciones necesarias para enfrentar todo tipo de amenaza, riesgo. De Vergara, (2009) asegura que el desarrollo de un Estado está íntimamente ligado a su condición de seguridad y a las acciones que se ejecuten para mantener esa condición, es decir, su capacidad de defensa.

El trinomio seguridad, defensa y desarrollo presentan una relación de interdependencia marcada por intereses y dinámicas de poder de carácter geopolítico y estratégico, con ello, el desarrollo de la tecnología se ha configurado como una nueva forma de poder ejercido a través de internet, las telecomunicaciones, los sistemas informáticos y el software, dando origen al ciberespacio como escenario virtual que

incide directamente en los ámbitos de la seguridad y la defensa.

La Organización de las Naciones Unidas (ONU) se ha manifestado al respecto, planteando amplios debates nacionales e internacionales en torno a las tensiones geopolíticas donde se advierte de una “gran fractura” entre las principales potencias del mundo, las cuales desarrollan sus propias políticas sobre internet e inteligencia artificial, manteniendo normativas financieras internas y diseñan estrategias geopolíticas y militares acordes a sus intereses, mencionó además la importancia que de la cooperación digital entre los Estados y un ciberespacio universal que refleje las normas mundiales para la paz y la seguridad, los derechos humanos y el desarrollo sostenible se considera crucial para garantizar un mundo unido. Un “compromiso global para la cooperación digital” (ONU, 2020).

La defensa nacional en todo país tiene como finalidad garantizar la seguridad nacional, protegiendo los derechos fundamentales y el Estado constitucional de derecho, mediante la aplicación de normas, técnicas, instrumentos y procedimientos propios del Estado. Actualmente, esta tarea no se limita al ámbito terrestre, sino que también se extiende al ciberespacio, como ya se ha señalado.

En abril de 2007, Estonia fue escenario del primer ciberataque de gran magnitud dirigido contra un Estado. Las principales instituciones públicas y privadas quedaron paralizadas tras una serie de ataques masivos que afectaron al Parlamento, varios ministerios, partidos políticos, bancos y medios de comunicación. Ante esta situación, el gobierno se vio con la necesidad de interrumpir el servicio de internet y a restablecer sus sistemas informáticos. El entonces director del Centro de Seguridad Informática de Estonia informó que los hackers reemplazaron portales oficiales con imágenes ofensivas contra el primer ministro, mientras que el tráfico digital aumentó hasta saturar los servidores. No solo fueron afectadas las agencias de noticias, sino también los grandes bancos, lo que generó alarma en un país de dimensiones reducidas. La crisis estuvo a punto de desencadenar un conflicto interno, ya que sectores de la población de origen ruso protagonizaron disturbios en la capital, mientras los bloqueos tecnológicos interrumpieron la distribución de productos básicos como la gasolina y el pan.

Ecuador**,** vivió una experiencia sobre ataque cibernético en abril del 2019, luego que su gobierno retirara el asilo diplomático a Julián Assange fundador de Wikileaks, a partir de ahí surgieron más de 40.000.000 ataques a diferentes instituciones públicas y privadas ecuatorianas en pocos días, lo que puso en evidencia la vulnerabilidad del país en el aseguramiento del ciberespacio (Rivadeneira, 2019).

La ciberdefensa es un complemento de la ciberseguridad, que proporciona la

defensa contra las amenazas en el ciberespacio, siendo parte de la acción estratégica de la Política de Defensa 2018 de Ecuador, que se articula con el inciso segundo del Art. 158 de la Constitución Política del Ecuador que establece: "… Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía e integridad territorial y, complementariamente, apoyar en la seguridad integral del Estado de conformidad con la ley". Basado en este mandato constitucional, el Ministerio de Defensa publica mediante Acuerdo Ministerial N° 199 del 11 de mayo del 2021 y articulándose con los objetivos de la política de ciberseguridad, la Guía Político Estratégica de Ciberdefensa, que busca orientar el accionar en el nivel político estratégico de la ciberdefensa, su relación con los otros sectores gubernamentales y su aplicación en los ejes de la seguridad integral en general y de la defensa en particular; y la Estrategia de Ciberdefensa con el propósito fundamental de establecer lineamientos para fortalecer a la ciberdefensa como una capacidad estratégica del Estado. (Semanate y Lenin 2023).

En el Perú, la Ley N.° 30999, promulgada el 26 de agosto de 2019, establece que la ciberdefensa constituye una capacidad de carácter militar destinada a responder ante amenazas o ataques provenientes del ciberespacio, siempre que estos comprometan la Seguridad Nacional (El Peruano, 2019).

Durante 2017, el Ministerio de Defensa, a través de la Dirección de Política y Planeamiento Estratégico, preparó un proyecto de Directiva que proponía lineamientos de Ciberdefensa para el Sector Defensa. Si bien este proyecto no fue oficializado mediante Resolución Ministerial, fue considerado como referencia en la elaboración del Plan Estratégico Sectorial Multianual (PESEM) 2017-2021 (Castillo, 2021).

El 25 de marzo de 2019, el CCFFAA activó el Comando Operacional de Ciberdefensa (COCID), cuyas instalaciones fueron inauguradas el 20 de enero de 2020. Este comando cuenta con tres componentes: terrestre, naval y aéreo. El Componente Terrestre está constituido por el Centro de Ciberdefensa del Ejército, inaugurado el 29 de octubre de 2018; el Componente Naval, por la Comandancia de Ciberdefensa de la Marina de Guerra, inaugurada el 21 de febrero de 2019; y el Componente Aéreo, por el Grupo de Operaciones en el Ciberespacio de la Fuerza Aérea, inaugurado el 21 de diciembre de 2019 (Castillo, 2021).

Considerando la importancia del ciberespacio y que en esta se pueden recibir ataques o a través de ella, además, teniendo en cuenta que diariamente se realizan millones de ciberataques de diversa índole, con la finalidad de obtener algún tipo de beneficio que afectarían los activos críticos nacionales y los recursos claves, que podrían desestabilizar al país, por lo que es importante considerar una adecuada capacidad de ciberdefensa debidamente organizada y estructurada que permita la

defensa nacional del ciberespacio.

1.2. Justificación de la Investigación

Los Estados, las organizaciones regionales y los órganos de seguridad y defensa han comenzado a modificar sus estrategias con el propósito de enfrentar las amenazas en el ciberespacio o, al menos, reducir su impacto. Los ejemplos de acciones emprendidas son numerosos; entre ellos destacan: (1) Alemania, que en 2011 lanzó su Estrategia de Seguridad Cibernética, creó el Centro Nacional de Ciberdefensa y publicó el Plan Nacional para la Protección de Infraestructuras de Información (NPIIP) (Acosta, 2009); y (2) España, que en ese mismo año implementó un Centro y un Plan Nacional de Protección de Infraestructuras Críticas, además de establecer en 2013 un Mando Conjunto de Ciberdefensa. En consecuencia, se hace necesaria una mirada estratégica orientada a diseñar un modelo de intervención, gestión y evaluación que permita garantizar la seguridad de la información en los procesos, sistemas e infraestructuras de los que depende el Estado para su economía y desarrollo (Vargas et al., 2017).

En el caso peruano, persiste la percepción de que la defensa se limita exclusivamente a la protección del territorio nacional. Esta visión es confirmada en el Plan Estratégico de Desarrollo Nacional – Plan Bicentenario al 2021, donde se advierte que la sociedad peruana carece de una adecuada conciencia de seguridad y tiende a considerar la defensa como una función exclusiva de las Fuerzas Armadas. Asimismo, el documento señala que la Defensa Nacional no constituye una prioridad para la ciudadanía y que existe una falta de claridad respecto a la relación entre defensa y desarrollo. Ante esta situación, se plantea la necesidad de fortalecer el Sistema de Seguridad y Defensa Nacional (reconocido constitucionalmente como Sistema de Defensa Nacional), teniendo como pilar fundamental la educación (Bautista, s.f.).

Por un lado, la ciberdefensa se entiende como el conjunto de operaciones y acciones, tanto pasivas como activas, desarrolladas en el marco de los sistemas de información, equipos, redes, enlaces y personal vinculados a los recursos teleinformáticos e informáticos de la defensa. Su propósito es garantizar el cumplimiento de las misiones o servicios para los cuales fueron creados, al mismo tiempo que busca impedir que las fuerzas enemigas logren los suyos (Becerra et al., 2019).

Por otro lado, la Defensa Nacional comprende el conjunto de medidas, previsiones y acciones que el Estado genera, adopta y ejecuta de manera integral y permanente, abarcando tanto el ámbito interno como el externo. En este marco, toda persona natural o jurídica tiene la obligación de participar en la Defensa Nacional (Ministerio de Defensa, 2005).

1.3. Delimitación de la Investigación

La investigación estuvo delimitada a evaluar la influencia de las capacidades actuales de ciberdefensa del Ejército del Perú en el ciberespacio en el año 2024, considerando la importancia estratégica para la seguridad nacional y el desarrollo del país. El estudio se realizó en las instalaciones del Ejército del Perú, (específicamente en el Centro de Ciberdefensa del Ejército, el Centro de Informática del Ejército, y la Dirección de Telemática del Ejército, centrado en el personal de oficiales superiores, oficiales subalternos, técnicos y suboficiales involucrados en ciberdefensa, con una muestra igual al tamaño de la población debido a su tamaño manejable, además, que se llevó a cabo en el período específico del año 2024. Por lo tanto, esta delimitación aseguró que el estudio se concentró en un ámbito específico y relevante, permitiendo un análisis detallado y enfocado.

1.4. Limitaciones de la Investigación

Dado que la información tecnológica solía ser de acceso público, se esperó que la investigación no encontrara limitaciones significativas en este aspecto. Sin embargo, la confidencialidad en los procesos de adquisición de equipamiento militar y adquisición de las capacidades presentó un desafío considerable, ya que el acceso a detalles específicos estuvo restringido por razones de seguridad y protección de intereses estratégicos. Por lo tanto, fue crucial considerar estrategias que permitieran abordar este aspecto sin comprometer la sensibilidad de la información militar.

1.5. Formulación del Problema

1.5.1. Problema General

¿Cuál es la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio, 2024?

1.5.2. Problemas Específicos

¿Cuál es la influencia de la capacidad de defensa del Ejército del Perú en el ciberespacio, 2024?

¿Cuál es la influencia de la capacidad de explotación del Ejército del Perú en el ciberespacio, 2024?

¿Cuál es la influencia de la capacidad de respuesta del Ejército del Perú en el ciberespacio, 2024?

¿Cuál es la influencia de la capacidad de investigación digital del Ejército del Perú en el ciberespacio, 2024?

1.6. Objetivos de la Investigación

1.6.1. Objetivo General

Determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio, 2024.

1.6.2. Objetivos Específicos

Determinar la influencia de la capacidad de defensa del Ejército del Perú en el ciberespacio, 2024.

Determinar la influencia de la capacidad de explotación del Ejército del Perú en el ciberespacio, 2024.

Determinar la influencia de la capacidad de respuesta del Ejército del Perú en el ciberespacio, 2024.

Determinar la influencia de la capacidad de investigación digital del Ejército del Perú en el ciberespacio, 2024.

Capítulo II: Marco Teórico

2.1. Antecedentes de la Investigación

2.1.1. Antecedentes Nacionales

Rossi (2021) desarrolló la tesis titulada “La seguridad y defensa en la era de la cuarta revolución industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas”, presentada en la Academia Diplomática del Perú “Javier Pérez de Cuéllar” para optar el grado de Maestro en Diplomacia y Relaciones Internacionales. Su propósito fue analizar mecanismos que permitan al país establecer alianzas y convenios orientados a la capacitación y entrenamiento de las instituciones competentes, además, de explorar alternativas para la transferencia tecnológica y el desarrollo conjunto de nuevas capacidades. El estudio sostiene que tanto la ciberseguridad como la ciberdefensa resultan indispensables para prevenir y contrarrestar ciberataques dirigidos a la infraestructura crítica, las redes de comunicación y los sistemas digitales de organismos estatales, militares y del sector privado, con la finalidad de garantizar la seguridad y defensa nacional. Desde el punto de vista metodológico, se aplicó un enfoque deductivo, analítico y cualitativo. Como resultado, se identificaron los elementos fundamentales para formular una estrategia de política exterior que fortalezca las capacidades del Perú en materia de ciberseguridad, ciberdefensa y amenazas híbridas. Finalmente, se evidenció que el país carece de capacidades cibernéticas consolidadas, situación que se repite en gran medida en los Estados de América Latina.

Quevedo (2022) publicó en el Centro de Altos Estudios Nacionales (CAEN) el artículo “Ciberdefensa y ciberseguridad en el Perú: Realidad y retos en torno a la capacidad de las Fuerzas Armadas para neutralizar ciberataques que atenten contra la seguridad nacional”. El objetivo central de este trabajo fue destacar que la ciberdefensa y la ciberseguridad se han convertido en pilares fundamentales para garantizar la estabilidad y el funcionamiento de los Estados modernos, constituyéndose en ejes prioritarios dentro de los estudios estratégicos. Sin embargo, el autor señala que el Perú no ha logrado consolidar un desarrollo adecuado en este ámbito y que, además, carece de inversión específica destinada a fortalecer sus sistemas de seguridad y defensa cibernética. El estudio, basado en una metodología de revisión documental, resalta que, aunque en América Latina los conflictos cibernéticos de gran escala aún son limitados, la seguridad nacional peruana corre el riesgo de verse comprometida si no se avanza al ritmo de las exigencias internacionales. En sus conclusiones, Quevedo plantea que el

diseño de estrategias efectivas en materia de ciberseguridad y ciberdefensa requiere de un sistema articulado que integre la cooperación entre los sectores público, privado y militar. Asimismo, enfatiza que las Fuerzas Armadas no solo deben cumplir con la misión de resguardar las fronteras terrestres, marítimas y aéreas, sino también ejercer un rol activo en la protección del ciberespacio.

Huayapa (2022) elaboró la tesis “Aportes para la política exterior peruana en materia de amenazas híbridas en el ciberespacio”, presentada en la Academia Diplomática del Perú “Javier Pérez de Cuéllar”. El objetivo de este trabajo fue establecer lineamientos que orienten el diseño de la política exterior nacional frente a las amenazas híbridas en el ciberespacio, partiendo del reconocimiento de que el desarrollo tecnológico ha generado nuevas modalidades de conflictividad y riesgos para la seguridad de los Estados.

El estudio se desarrolló bajo un enfoque cualitativo con alcance descriptivo y se sustentó en un diseño de teoría fundamentada. Para la obtención de información se aplicaron entrevistas estructuradas y un análisis documental apoyado en listas de verificación. Estas herramientas metodológicas permitieron examinar las definiciones doctrinarias de amenazas híbridas y su vinculación con conceptos como conflicto híbrido y guerra híbrida, así como su relación con el ciberespacio, las ciberoperaciones y los ciberataques.

La investigación concluyó que existen diversos tipos de ciberoperaciones que representan riesgos significativos para la seguridad de los Estados, como el ciberespionaje y el cibercrimen, siendo los ciberataques los más relevantes. Estos se definieron como acciones que utilizan el ciberespacio como medio no tradicional y las ciberoperaciones como método no tradicional, con el objetivo de comprometer la infraestructura tecnológica y digital de un Estado, afectando tanto al gobierno como a la población.

Muñoz (2023) presentó su tesis titulada "La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033" en la Universidad de las Fuerzas Armadas como parte de su programa de magíster en defensa y seguridad. El objetivo principal de esta investigación fue determinar los actores del sistema, los factores de cambio, los eventos clave y los posibles escenarios futuros de la ciberdefensa hasta el año 2033, con el fin de fortalecer la capacidad ciberespacial en la Fuerza Terrestre ecuatoriana.

Para desarrollar este análisis, se aplicó la metodología prospectiva de Godet, la cual se dividió en tres fases: la construcción de una línea base a partir del análisis del macroambiente y microambiente, la definición de variables estratégicas utilizando la

herramienta ábaco de Regnier, y la elaboración de escenarios prospectivos mediante la matriz morfológica. Como resultado, se formularon estrategias específicas para mejorar la ciberdefensa dentro de la Fuerza Terrestre, con el objetivo de proporcionar respuestas efectivas a los desafíos identificados en el estudio.

Chivilches (2023) presentó su tesis titulada “Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú”, presentada en la Escuela Superior de Guerra Naval. El propósito central de este trabajo fue diseñar una estrategia integral que permita enfrentar de manera efectiva la ciberdelincuencia y mitigar sus repercusiones sobre la Seguridad Nacional. La investigación resalta la necesidad de articular esfuerzos institucionales y fortalecer las capacidades del Estado para responder a este tipo de amenazas en constante evolución.

La investigación se sustentó en un enfoque cualitativo, de carácter básico y descriptivo, con un alcance transversal. Se empleó un diseño de análisis documental para recolectar y analizar la información relevante.

Los resultados obtenidos resaltaron que la ciberdelincuencia afecta directamente la Seguridad Nacional peruana mediante ataques dirigidos a instituciones clave y vulnerabilidades en sistemas de salud, lo cual tiene repercusiones significativas en la seguridad ciudadana. Se enfatizó la necesidad crítica de contar con personal altamente capacitado en ciberseguridad, la implementación de recursos tecnológicos avanzados, y la mejora de la infraestructura. Además, se destacó la importancia de establecer acuerdos internacionales para combatir eficazmente la ciberdelincuencia. Asimismo, se subrayó la urgencia de desarrollar e implementar una Estrategia Nacional de Ciberseguridad, así como la promulgación de una Ley de Ciberseguridad que fortalezca el marco legal en esta área. Mejorar los recursos humanos especializados y la infraestructura también fue identificado como un paso crucial para abordar estas amenazas de manera efectiva.

Villón (2024) publicó el artículo “Seguridad Nacional, Relaciones Internacionales y Bienestar Social en la Era Digital” en el Centro de Estudios Estratégicos del Ejército del Perú. El texto analiza cómo la revolución digital incide en la seguridad nacional, las dinámicas internacionales y el bienestar social en el contexto peruano. La autora examina tanto los retos como las oportunidades que acompañan a la digitalización, poniendo énfasis en aspectos como la ciberseguridad, la gestión de la desinformación, la protección de datos, la aplicación de la Inteligencia Artificial (IA) y la cooperación internacional. Asimismo, identifica amenazas emergentes como el cibercrimen, el espionaje digital y las debilidades en infraestructuras críticas. Finalmente, resalta la urgencia de que el Estado implemente políticas eficaces para enfrentar dichos riesgos,

subrayando el rol de la educación pública en ciberseguridad y la necesidad de promover alianzas internacionales en este campo estratégico.

2.1.2. Antecedentes Internacionales

Santos (2022), en su tesis titulada “Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento”, presentada en la Universidad Andina Simón Bolívar (Ecuador) para obtener el grado de maestría en Relaciones Internacionales, analizó la respuesta de los Estados latinoamericanos frente al incremento de amenazas en el ciberespacio. El estudio puso especial atención en el caso ecuatoriano, examinando el marco normativo que regula la ciberseguridad y la ciberdefensa en el contexto de la sociedad actual caracterizada por el uso intensivo de la información y el conocimiento. La investigación también se orientó a identificar los factores que originan las amenazas en el entorno digital, así como los escenarios y actores que intervienen en este tipo de riesgos, elementos que resultan fundamentales para la formulación de políticas y estrategias internacionales en materia de seguridad digital. De igual manera, se analizó el desarrollo de instrumentos estratégicos implementados por el Estado ecuatoriano —como políticas públicas, normativa jurídica e instituciones especializadas— destinados a prevenir y enfrentar los riesgos y ataques cibernéticos que afectan la seguridad nacional. El estudio se desarrolló bajo un enfoque cualitativo, apoyado principalmente en el análisis y recopilación de fuentes bibliográficas especializadas. Entre sus principales conclusiones se destaca la responsabilidad del Estado en la protección del ciberespacio, lo que implica salvaguardar la infraestructura crítica digital, los servicios esenciales y los sistemas de defensa, además de garantizar la seguridad de los datos personales y el respeto de los derechos de los ciudadanos en el entorno digital.

García y Herrero (2020) presentaron el artículo “La ciberdefensa en los sistemas de información sanitarios militares”, el cual tiene como objetivo la sensibilización del personal militar que son el factor esencial en estos sistemas, pero a la vez son el factor más débil para la protección de los sistemas informáticos. Este artículo hace una descripción analítica de los sistemas informáticos de la sanidad del Ejército de España, teniendo en consideración el ciberespacio, los diferentes tipos de ciberataques para el cual los atacantes podrían usar diferentes tipos de vectores como los malware, exploits, ingeniería social o phishing, keyloggers hardware y memorias USB; y las vulnerabilidades de los sistemas de información. Además, hace una descripción de la existencia de una diversidad de agentes de la ciberamenaza que pueden atentar contra los estados tales como el ciberespionaje, ciberdelincuencia organizada, hacktivistas,

ciberpatriotas, ciberterrorismo, económicos, políticos entre otros. Asimismo, se concluye que en internet no existe una seguridad absoluta, sin embargo, esto no significa que no haya que buscarla, por lo que se debe estar siempre alertas, con la finalidad de reducir estos riesgos y consecuencias. Este artículo permitió identificar a las Fuerzas Armadas Españolas con tres tipos de capacidades de ciberdefensa: la capacidad de defensa, capacidad de explotación y la capacidad de ataque que permita realizar acciones ofensivas en el ciberespacio, frente a las agresiones o amenazas que puedan atentar contra su seguridad nacional.

Muñoz (2023) presentó su tesis titulada "La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033" en la Universidad de las Fuerzas Armadas como parte de su programa de magíster en defensa y seguridad. El objetivo principal de esta investigación fue determinar los actores del sistema, los factores de cambio, los eventos clave y los posibles escenarios futuros de la ciberdefensa hasta el año 2033, con el fin de fortalecer la capacidad ciberespacial en la Fuerza Terrestre ecuatoriana. Para llevar a cabo este análisis, se empleó la metodología prospectiva de Godet, la cual se dividió en tres fases: la construcción de una línea base a partir del análisis del macroambiente y microambiente, la definición de variables estratégicas utilizando la herramienta ábaco de Regnier, y la elaboración de escenarios prospectivos mediante la matriz morfológica. Como resultado, se formularon estrategias específicas para mejorar la ciberdefensa dentro de la Fuerza Terrestre, con el objetivo de proporcionar respuestas efectivas a los desafíos identificados en el estudio.

Mogollón (2021) llevó a cabo la investigación titulada “La adaptación asimétrica de las doctrinas de Defensa en torno al Ciberespacio: los casos de Chile y Ecuador (2014-2018)”, desarrollada en FLACSO. El propósito central del estudio fue analizar las causas que explican la asimetría en los procesos de adecuación doctrinaria de la Defensa en relación con el ciberespacio entre Chile y Ecuador, a pesar de que ambos comparten principios dogmáticos semejantes.

El estudio empleó una metodología cualitativa. Los resultados revelaron que Chile ha desarrollado un proceso avanzado de adaptación en la defensa del ciberespacio, destacándose la influencia significativa de la política pública de ciberdefensa del país. En contraste, Ecuador no cuenta con una política formal de ciberdefensa, a pesar de haber implementado extensivamente servicios públicos en línea. Esta falta de preparación ha expuesto a Ecuador a múltiples incidentes cibernéticos, comprometiendo la seguridad nacional del país.

Urtasun (2021) realizó un estudio titulado "Cibersecuritización: un análisis de discurso, instituciones y documentos oficiales para los casos de Estonia y Reino Unido".

El objetivo de la investigación fue abordar la pregunta de por qué algunos países logran securitizar la respuesta a las amenazas relacionadas con la ciberseguridad. El estudio utilizó un enfoque comparativo de estudio de caso y aplicó como metodología el análisis de discurso. Se analizaron diversas fuentes discursivas como entrevistas, diarios, discursos y documentos oficiales. La investigación examinó específicamente los casos de Reino Unido, un país que enfrenta constantemente ciberdelitos, y Estonia, reconocida por iniciar un enfoque avanzado hacia la ciberseguridad que la posicionó en el contexto internacional como protagonista, especialmente después de los eventos de 2007, considerados como uno de los primeros incidentes importantes de guerra en el ciberespacio.

2.2. Bases Teóricas

2.2.1. Base Teórica que Sustenta la Investigación

El poder de las redes y las redes del poder en el entorno tecnológico de la comunicación

Castells (2005) presenta su reconocida propuesta sobre la sociedad red, entendida como un rasgo distintivo de la estructura social a inicios del siglo XXI. Plantea que la manera en que se configura y ejerce el poder se ve profundamente transformada en el nuevo contexto organizacional y tecnológico, impulsado por la expansión de las redes digitales de comunicación global. Estas se constituyen en el principal sistema de procesamiento simbólico de nuestra época (pp. 24-25). Con ello, fortalece y amplía su concepto de sociedad red, incorporando un examen detallado de las fuentes contemporáneas de poder, especialmente en el apartado “Redes” (pp. 45-50).

Castells (2005) centra su atención en la comunicación, el diálogo y las diversas formas de debate en la sociedad, más que en la red misma y sus capacidades informáticas, como una vía para redescubrir un nuevo protagonismo social. Al plantear un modelo de análisis e interpretación basado en las redes digitales, el autor sugiere que este sistema permite comprender el funcionamiento integral de la sociedad actual, la cual trasciende los aspectos puramente tecnológicos y se ve atravesada por múltiples factores sociales que exceden las innovaciones y limitaciones propias del ámbito informático.

El autor reconoce que los cambios en los tiempos, modos e intensidades de las relaciones sociales han transformado aspectos centrales como la autonomía y la privacidad, que quedan expuestos a los “controladores invisibles globales” de la red, actores claves del capitalismo informacional (pp. 144-146). A partir de ello, surgen cuestionamientos sobre los alcances de las políticas reguladoras vigentes y sobre si la

llamada “convergencia cultural” constituye realmente una forma de resistencia frente al control monopólico de las prácticas comunicativas. Castells concluye que el sistema de comunicación digital global refleja las relaciones de poder, pero no se sustenta en la mera difusión jerarquizada de una cultura dominante (pp. 188-189).

Tras su influyente trilogía la era de la información: economía, sociedad y cultura (1999), con la que formuló una teoría sistemática acerca de los impactos de la tecnología de la información en el mundo contemporáneo, Castells, considerado por algunos como el “Marshall McLuhan de nuestro tiempo”, vuelve a sorprender con una obra que busca descifrar, y al mismo tiempo problematizar, uno de los dilemas centrales del siglo XXI: la intersección estratégica entre tecnología, comunicación y poder.

De acuerdo con Castells (2001), las redes constituyen la nueva morfología social, ya que sus formas de interacción, conexión y comunicación transforman de manera significativa los procesos de producción, la experiencia, el ejercicio del poder y la cultura. Una red puede entenderse como un conjunto de nodos interconectados que funcionan como estructuras abiertas, capaces de expandirse sin límites siempre que conserven los mismos códigos que permiten sostener una comunicación eficaz.

En este marco, Castells concibe la Sociedad en Red no como una simple denominación de un fenómeno tecnológico, sino como una nueva forma de organización social, donde la identidad de las personas se define más por su pertenencia y conexión a una red que por vínculos tradicionales como la familia, el clan, la tribu o el Estado. Así, las sociedades modernas se estructuran sobre la base de la complementariedad entre Red y Ego.

Además, el autor sostiene que las redes impulsadas por las tecnologías de la información representan las estructuras más eficientes y adaptables de la historia, debido a su flexibilidad, estabilidad y capacidad de supervivencia. Estas redes siguen la lógica de los denominados “mundos pequeños”, capaces de integrarse globalmente a partir de la interconexión de redes locales, siempre que exista compatibilidad en los códigos y protocolos de comunicación. En este contexto, las nuevas tecnologías han dado lugar a organizaciones sustentadas en nodos, en las cuales las jerarquías tradicionales tienden a diluirse.

La hipótesis teórica que emerge de estos planteamientos es las relaciones de poder que surgen del sistema de comunicación digital global establecen una nueva sociedad denominada sociedad en red.

La tecnología digital no solo está cambiando la forma en que nos comunicamos y nos relacionamos, sino que también está transformando fundamentalmente la

estructura misma de la sociedad, dando lugar a nuevas formas de organización social, participación y gobernanza. Esta teoría sugiere que la interconexión global a través de la tecnología digital está redefiniendo la estructura social y las dinámicas de poder, creando una red interconectada de individuos, instituciones y tecnologías.

"El poder de las redes y las redes del poder en el entorno tecnológico de la comunicación" de Manuel Castells es una obra seminal que explora la intersección entre la tecnología de la comunicación y el poder en la era digital. Castells, un sociólogo y académico reconocido mundialmente, examina cómo las redes de comunicación, especialmente internet, están transformando las dinámicas de poder en la sociedad contemporánea.

Castells argumenta que las redes de comunicación no solo son herramientas tecnológicas, sino que también son estructuras sociales que moldean y son moldeadas por las relaciones de poder. Examina cómo estas redes afectan la política, la economía, la cultura y otras esferas de la vida social.

Uno de los conceptos clave que Castells desarrolla en su trabajo es el de "redes de poder", que son las interconexiones de individuos, instituciones y organizaciones que ejercen influencia en la sociedad a través de la comunicación y la tecnología. Castells analiza cómo estas redes operan en diferentes contextos, desde la política hasta los negocios y la cultura, y cómo las estructuras de poder tradicionales están siendo desafiadas y reconfiguradas por la naturaleza descentralizada y globalizada de las redes de comunicación.

Castells ofrece una perspectiva profunda y perspicaz sobre la relación entre la tecnología de la comunicación y el poder en la era digital, y es una lectura fundamental para comprender los cambios sociales y políticos en el mundo contemporáneo.

La teoría de Manuel Castell nos proporciona un marco significativo que salen de las relaciones de poder que surgen del sistema de comunicación digital global, que establecen una nueva sociedad denominada sociedad en red y que influyen en la ciberdefensa en el espacio terrestre y en el ciberespacio de un país. Frente a esta postura Castell aborda el poder de las redes en el ámbito militar en redes de información y vigilancia que son altamente sofisticadas y permiten recopilación, análisis y distribución en tiempo real, con ello podemos definir a una revolución tecnológica en esta área que permiten llevar a cabo la vigilancia militar y la inteligencia estratégica. Por otra parte, Castell con su teoría nos permite analizar conflictos militares, el poder gira en utilizar las redes de comunicación para confrontar e iniciar una guerra cibernética, la propaganda en línea y la capacidad de coordinar operaciones militares a través de sistemas de comunicación digital. Castells también examina el papel de las redes

sociales y digitales en la organización y la difusión de grupos terroristas y movimientos insurgentes. Destaca cómo estas plataformas pueden facilitar la radicalización y la coordinación de ataques.

Finalmente queremos exponer que la teoría de Castell proporciona respaldo para analizar y entender que existen nuevos desafíos en la seguridad nacional y ciberseguridad en los países. Castells hace hincapié en la adaptación que deben tener los gobiernos y las organizaciones militares para protegerse contra amenazas como el hackeo, el espionaje cibernético y los ataques informáticos.

Como hemos podido analizar la teoría de Castell en "El Poder de las Redes", a modo de conclusión Castells ofrece una visión detallada de cómo la revolución digital ha impactado en diversos aspectos de la sociedad, incluido el ámbito militar. Su análisis destaca la importancia cada vez mayor de comprender y gestionar las dinámicas de poder en un mundo interconectado digitalmente.

Teorías de alcance medio

Niklas Luhmann: El ciberespacio como sistema y entorno social. El sistema social se reproduce a través de la comunicación, del mismo modo que los sistemas biológicos generan vida y los sistemas psíquicos producen conciencia. Todo aquello que no constituye comunicación se ubica en su entorno. Al tratarse de un sistema cerrado, el individuo no dispone de mecanismos directos para intervenir o dirigir el sistema social. A su vez, la modernidad ha estado marcada por un proceso de diferenciación expresado en la conformación de subsistemas opacos, que se perciben entre sí como elementos externos.

Este planteamiento responde a una inquietud central: la complejidad, entendida como el principio que orienta la lógica evolutiva de los sistemas. Sin embargo, a partir de la década de 1990, esta perspectiva comienza a desplazarse gradualmente hacia enfoques basados en la observación y la distinción. Dicho giro permite a Luhmann reformular la teoría de sistemas como un marco que concibe a los propios sistemas en calidad de observadores. En este proceso, se produce un cambio conceptual significativo, que sustituye la clásica oposición sistema/entorno por la relación forma/medio.

Luhmann cuestiona la idea de que detrás de la comunicación social exista necesariamente un actor o una acción. Su planteamiento trasciende esta noción al concebir los proyectos teóricos no como identidades cerradas (sistemas), sino como diferencias que surgen en la relación entre el sistema y su entorno. De este modo, el sistema no posee una existencia autónoma, sino que se define y se mantiene

únicamente a partir de la distinción con aquello que lo rodea. El valor de dicha diferencia, sin embargo, depende del sistema específico que se observe. En otras palabras, se abandona la aspiración de explicar el mundo como una totalidad unificada, ya sea desde fundamentos antropológicos o desde la idea de un contrato social, para que en su lugar, comprenderlo como una trama de observadores múltiples, interconectados y horizontales, cuyo sentido no puede ser reducido a una mirada totalizante.

Luhmann cuestiona la premisa de que la comunicación social tenga necesariamente un actor o una acción como fundamento. En lugar de concebir los sistemas como identidades autónomas, los entiende como diferencias que emergen en la relación con su entorno. Así, un sistema solo existe y se mantiene a partir de esa distinción, cuyo valor depende siempre de la perspectiva desde la que se observe. Con ello, se descarta la aspiración de interpretar la sociedad como una totalidad unificada y se propone, en cambio, comprenderla como una red de observadores múltiples y horizontales, imposible de reducir a una visión totalizante.

En otros contextos académicos, sin embargo, se le reprocha su inclinación a describir la sociedad sin ofrecer una crítica normativa ni propuestas de corrección frente a los problemas sociales y ecológicos derivados de su evolución.

La hipótesis teórica que emerge de estos planteamientos es superar el antropocentrismo como un obstáculo epistemológico, cuyo elemento característico de los sistemas sociales no eran los individuos sino las comunicaciones. Esta perspectiva epistemológica amplía nuestra comprensión de los sistemas sociales al reconocer la importancia de los procesos comunicativos en la construcción de la realidad social. Además, permite analizar cómo se producen, mantienen y cambian las estructuras sociales a través de las interacciones simbólicas entre diferentes unidades sociales. Además de ello, aunque Luhmann no aborda el ciberespacio en la esfera militar, constituye esta teoría fundamental para considerar al ciberespacio como un sistema social en sí mismo, con sus propias reglas, normas y estructuras de comunicación.

Niklas Luhmann, un destacado sociólogo alemán conocido por su teoría de sistemas sociales, también abordó el tema del ciberespacio y su relación con los sistemas sociales en la era digital. Aunque no escribió específicamente sobre el ciberespacio como tal, su enfoque en los sistemas sociales ofrece una perspectiva interesante para comprender cómo el ciberespacio puede ser conceptualizado dentro de su marco teórico.

Luhmann argumentaba que los sistemas sociales son sistemas autopoiéticos, es decir, sistemas que se autorregulan y se reproducen a sí mismos a través de la comunicación digital y que influye en otros sistemas sociales al proporcionar un entorno

para la interacción humana y la creación de significado. Según su teoría, la sociedad está compuesta por una variedad de sistemas sociales, como el sistema político, el sistema económico, el sistema educativo, entre otros. Cada uno de estos sistemas tiene su propia lógica interna y opera de manera independiente, pero al mismo tiempo están interconectados a través de la comunicación.

Además, Luhmann habría analizado cómo el ciberespacio afecta y es afectado por otros sistemas sociales, como la política, la economía y la cultura. Por ejemplo, el ciberespacio puede influir en la política al facilitar la participación ciudadana a través de plataformas en línea, o puede afectar la economía al cambiar la forma en que se realizan las transacciones comerciales. Al mismo tiempo, los sistemas sociales existentes también pueden influir en la estructura y el desarrollo del ciberespacio a través de la regulación, la legislación y otras formas de intervención.

Hemos mencionado que Niklas Luhmann no discutió específicamente el ciberespacio como un sistema y entorno social en el ámbito militar, sin embargo, consideramos que su teoría se puede aplicar en el ámbito militar, por ello se concibe al ciberespacio como un dominio crítico para la seguridad nacional y las operaciones militares. Siguiendo el marco de la teoría de sistemas de Luhmann, podríamos considerar al ciberespacio como un sistema social en sí mismo, con sus propias reglas, normas y estructuras de comunicación. Dentro de este sistema, los actores militares y no militares interactúan a través de redes digitales, plataformas en línea y sistemas de información. Las operaciones militares ahora dependen en gran medida de la capacidad de controlar y proteger el ciberespacio, así como de utilizarlo para llevar a cabo actividades como la vigilancia, el espionaje y la guerra cibernética. En consecuencia, el ciberespacio puede ser visto como un entorno social que rodea y afecta las operaciones militares. Las amenazas cibernéticas, como los ataques informáticos y el espionaje cibernético, pueden tener consecuencias significativas para la seguridad nacional y la efectividad militar.

En este contexto, la teoría de sistemas sociales de Luhmann puede ayudarnos a entender cómo el ciberespacio interactúa con otros sistemas sociales, como el político, el económico y el cultural, en el ámbito militar. Las dinámicas de poder, la toma de decisiones y la coordinación de operaciones militares pueden estar influenciadas por las interacciones en el ciberespacio y viceversa.

Teorías ambientales sobre ciberdefensa: La frontera de Friederich Ratzel y Spykman.

Las Teorías Ambientales se refieren a los enfoques que consideran a la

geografía, la demografía, la distribución de los recursos y el desarrollo tecnológico como factores centrales para el análisis de las relaciones internacionales. Dichas teorías resultan fundamentales para la comprensión y planificación de la geopolítica y la geoestrategia.

En este marco, el ciberespacio y su utilización han introducido nuevas dinámicas para interpretar los escenarios geopolíticos. Este dominio ha cuestionado los tradicionales postulados de supremacía terrestre y marítima, al tiempo que plantea retos a las concepciones clásicas de dominación espacial (y también temporal).

El ciberespacio se presenta como una frontera inédita, carente de limitaciones físicas: sin montañas, ríos u océanos; sin estaciones ni climas que condicionen su existencia. Tampoco intervienen en él factores tangibles que, en otros contextos, influyen en las decisiones políticas o militares ni en la formación del carácter nacional. Por ello, este nuevo escenario trasciende los enfoques tradicionales de la geopolítica, desde los planteamientos de Aristóteles hasta las formulaciones de autores del siglo XX como Harold y Margaret Sprout.

Existen ciertos paralelismos con la noción de frontera desarrollada por Frederick Jackson Turner, quien sostuvo que la expansión hacia el oeste configuró el pensamiento norteamericano al dotarlo de dinamismo, creatividad e innovación. Trasladado al ciberespacio, este concepto adquiere un matiz distinto: los individuos no solo deben avanzar hacia esa frontera, sino también perseguirla de manera constante, ya que implica actualizar permanentemente sus conocimientos para mantener una nueva distancia intelectual. Se trata de una frontera virtual en continuo movimiento que, desde la perspectiva de la ciberdefensa, puede entenderse en dos dimensiones: la primera corresponde a la frontera establecida para contener y proteger los recursos estratégicos; y la segunda, a aquella diseñada para superar dichas defensas.

En sintonía con esta perspectiva, otros autores también reflexionaron sobre la noción de frontera. Friederich Ratzel introdujo el concepto de lebensraum (“espacio vital”), entendido como el esfuerzo del Estado por expandir sus fronteras territoriales, lo que implica que estas se encuentran en permanente transformación. Por su parte, Nicholas Spykman desarrolló la idea de las “fronteras dinámicas”, las cuales representan zonas donde la expansión se ha detenido de manera temporal, pero sin perder su carácter de cambio y movimiento constante.

Otra peculiaridad de la ciberdefensa vinculada a las teorías ambientalistas se observa en los enfoques darwinianos de la “supervivencia de los más aptos”, particularmente en la teorización de Thomas Robert Malthus, quien sostenía que el crecimiento poblacional era diametralmente opuesto a la disponibilidad de alimentos.

Trasladado al ámbito de la ciberdefensa, pueden señalarse tres factores distintivos: a) en el ciberespacio no existen recursos en vías de extinción, sino que, por el contrario, se generan de manera constante y acelerada; b) no hay una “ética” o “moral” que limite los ejercicios de acción y manipulación de dichos recursos; y c) no existe una noción de justicia que resulte aplicable de manera relevante ni a los recursos ni a los agentes o actores que operan en ese entorno.

Los planteamientos de Malthus llevaron a considerar al Estado como una entidad orientada hacia la expansión imperialista, resultado de la pulsión utilitarista sobre los objetos existentes, que no se limitan a los alimentos, sino que incluyen cualquier recurso material. En el ámbito de la ciberdefensa, se perciben semejanzas con esta lógica. ¿Cómo no asociar la figura imperial con un suelo cuya extensión depende de la voluntad, el deseo o la interpretación de los actores que lo habitan? Existe un darwinismo intrínseco en la operativa del ciberespacio en términos de ciberdefensa, pues lo que existe (información y conocimiento) debe ser ocupado, comprendido y aprehendido. Las conciliaciones y alianzas se orientan a la ocupación, la competencia y el conflicto. Este fenómeno puede observarse en colectivos como Anonymous o LulzSec, cuya acción se legitima en la cooperación de los individuos que los integran, aunque ninguno de ellos sea un actor legítimo por sí solo. En este sentido, tales grupos no se entienden como una simple suma de individuos, sino como un todo articulado.

Otra característica relevante proviene de los estudios de Quincy Wright, quien analizó las transformaciones demográficas y señaló que el incremento de la población favorecía la interpenetración cultural. Este proceso, acompañado por el aumento de la comunicación, reducía la brecha tecnológica entre los pueblos, aunque al mismo tiempo intensificaba las fricciones entre ellos.

En el ámbito de la ciberdefensa se observa un fenómeno comparable, caracterizado por una creciente interconexión entre actores y sistemas. Esta dinámica surge de manera natural debido a que la información ya no permanece bajo un control claramente delimitado, sino que tiende a difundirse cada vez más en el espacio público. Como consecuencia, aumenta el número de actores con acceso a dicha información y, paralelamente, la brecha tecnológica entre ellos se reduce progresivamente. Este escenario fortalece la dinámica de interacción en las fronteras del ciberespacio, lo que incrementa las posibilidades de fricción y conflicto entre distintos actores.

La hipótesis teórica que se desprende de estos planteamientos es entender al ciberespacio en términos de territorio, y que su uso y manipulación han marcado nuevas pautas para entender las aristas de la geopolítica. Esta hipótesis sugiere que el ciberespacio no es simplemente un espacio abstracto de comunicación digital, sino que

tiene dimensiones territoriales y geopolíticas que influyen en las relaciones entre estados, actores no estatales y empresas multinacionales.

Las teorías ambientales sobre ciberdefensa exploran cómo el entorno geográfico y geopolítico influye en las estrategias y capacidades de defensa cibernética de un país. Estas teorías toman prestado el concepto de "frontera" de teóricos como Friedrich Ratzel y Nicholas Spykman para analizar cómo las características físicas y políticas de un territorio pueden afectar la seguridad cibernética de una nación.

Friedrich Ratzel: Ratzel fue un influyente geógrafo alemán del siglo XIX y XX, conocido por desarrollar la teoría del determinismo geográfico. Según esta teoría, los factores geográficos, como el clima, la topografía y los recursos naturales, determinan en gran medida el curso de la historia y la política de una nación.

En el contexto de la ciberdefensa, las teorías ambientales podrían aplicar el concepto de "espacio vital" de Ratzel para argumentar que los países con vastas fronteras físicas tienen desafíos únicos en la protección de sus infraestructuras críticas contra ataques cibernéticos. Por ejemplo, países con fronteras extensas podrían enfrentar dificultades para monitorear y proteger sus redes y sistemas de información de manera efectiva.

Nicholas Spykman: Spykman fue un geógrafo político estadounidense conocido por su teoría del "Rimland" en geopolítica. Según Spykman, la región costera de Eurasia, que abarca desde Europa occidental hasta el este de Asia, es la región geopolíticamente más significativa del mundo debido a su accesibilidad marítima y su proximidad a importantes centros de poder.

Las teorías ambientales sobre ciberdefensa podrían aplicar el concepto de "Rimland" de Spykman para argumentar que las naciones que controlan las rutas marítimas y los puntos de acceso estratégicos en el ciberespacio tienen una ventaja geopolítica en términos de defensa cibernética. Esto se debe a que el control sobre las redes de comunicación y los cables submarinos puede influir en la capacidad de un país para llevar a cabo operaciones ofensivas o defensivas en el ciberespacio.

En resumen, las teorías ambientales sobre ciberdefensa utilizan conceptos geográficos y geopolíticos, como la frontera de Ratzel y el Rimland de Spykman, para analizar cómo el entorno físico y político de una nación puede influir en su capacidad para protegerse contra amenazas cibernéticas y mantener la seguridad en el ciberespacio.

Con esta teoría, podemos concebir al ciberespacio como un territorio, se reconocen varios aspectos importantes dentro de ellos está el control y soberanía: los

estados siempre están en constante búsqueda de hegemonía geopolítica y autoridad y jurisdicción sobre el ciberespacio; es en este sentido, que intentan controlar y ejercer soberanía sobre el ciberespacio, ya sea a través de la legislación, la regulación o el uso de herramientas técnicas como cortafuegos y sistemas de filtrado. Por otra parte, existe una creciente dependencia de la infraestructura digital, como consecuencia hace que el ciberespacio sea un campo de batalla potencial, donde se debilita la seguridad nacional, economía y estabilidad política, lo que lleva a la aparición de nuevas formas de conflicto y guerra cibernética entre estados y actores no estatales. El ciberespacio también se ha convertido en un espacio para la diplomacia y las relaciones internacionales. Los estados negocian acuerdos y tratados sobre cuestiones como la ciberseguridad, la protección de datos y la privacidad en línea, lo que refleja la creciente importancia de las relaciones internacionales en el contexto digital.

El ciberespacio en términos de territorio implica reconocer su importancia en la geopolítica contemporánea y en las relaciones de poder a nivel internacional. El ciberespacio no es simplemente un espacio virtual, sino un terreno estratégico que influye en la política, la seguridad y la economía a nivel global.

2.2.2. Base Teórica de la Variable 1

La capacidad de ciberdefensa constituye la respuesta de los gobiernos para garantizar la seguridad en el ciberespacio. En el contexto peruano, la Ley N.º 30999, promulgada el 26 de agosto de 2019, define la ciberdefensa como la capacidad militar orientada a actuar frente a amenazas o ataques realizados en y a través del ciberespacio cuando estos comprometen la seguridad nacional. Asimismo, en su artículo 6, la norma establece que las capacidades de ciberdefensa comprenden el uso de conocimientos, habilidades y medios destinados a ejecutar operaciones en y mediante el ciberespacio con el propósito de asegurar su empleo por las fuerzas propias (Ley Nº 30999, 2019).

2.2.3. Base Teórica de la Variable 2

El ciberespacio se entiende como un entramado de redes interconectadas e interdependientes que conforman la infraestructura de tecnología de la información. Este ámbito incluye internet, redes de telecomunicaciones, sistemas aislados (es decir, redes, sistemas y dispositivos de almacenamiento que no se conectan directamente a la red global), software, datos, protocolos de transporte, suministro eléctrico, sistemas informáticos, procesadores y controladores integrados, así como las personas que interactúan con dichos elementos. En términos generales, puede considerarse un

entorno digital sin límites físicos y que se encuentra fuera de la jurisdicción exclusiva de cualquier Estado (Ley Nº 30999, 2019).

2.3. Definición de Términos

Capacidad de Ciberdefensa

La Ley N.° 30999 establece que la ciberdefensa constituye una capacidad militar destinada a responder ante amenazas o ataques ejecutados en y a través del ciberespacio, cuando estos comprometen la seguridad nacional. Además, precisa que las capacidades de ciberdefensa comprenden el uso articulado de conocimientos, destrezas y recursos para desarrollar operaciones en dicho entorno digital, con el propósito de garantizar su uso seguro por parte de las fuerzas propias (Ley Nº 30999, 2019).

La ciberdefensa puede entenderse como el conjunto de estrategias, acciones y medidas adoptadas por un Estado para asegurar su seguridad en el entorno digital y prevenir amenazas cibernéticas. Estas amenazas abarcan desde el acceso indebido a datos sensibles de organizaciones hasta ciberataques dirigidos a infraestructuras críticas o actos de ciberterrorismo (UNIR, 2023).

Entre sus principales funciones preventivas se incluyen: proteger la integridad territorial de un país, salvaguardar infraestructuras esenciales como el suministro eléctrico o de gas, mantener la vigilancia permanente de las redes, asegurar la confidencialidad y disponibilidad de los datos de ciudadanos, empresas y entidades públicas, implementar controles y medidas de seguridad en el ciberespacio, responder ante incidentes y recuperar información comprometida, así como identificar y corregir vulnerabilidades (UNIR, 2023).

Capacidad de Defensa

El modelo integra todas estas dimensiones de la capacidad para que las personas no se dejen seducir, bajo la presión de limitaciones de recursos u otras, a pensar que el cambio de un elemento, como la redacción de una nueva doctrina, da como resultado automáticamente la generación de los efectos respectivos de las condiciones de funcionamiento deseadas (Glosario Militar, s.f.)..

Griffiths (2011) señala que “la defensa nacional no solo existe para la defensa de la soberanía e integridad territorial, sino que también, para otorgar paz, seguridad y estabilidad internacionales” (pp. 578-579), identificando así un campo de acción más amplio para la función defensa, que abarca desde hacer frente a las amenazas de naturaleza militar externas hasta objetivos asociados a la política exterior del Estado. En esa misma línea, el Libro de la Defensa Nacional (2017) afirma que para garantizar

el efecto que busca la función defensa “es necesario que se satisfaga, entre otras, la siguiente condición: que el ejercicio de la función abarque la suma de actividades de los organismos del Estado necesarios para la defensa, ya que su ámbito excede los límites de lo estrictamente militar” (p. 98).

Ciberespacio

El concepto “ciberespacio” nace en la literatura con la novela Neuromancer de Gibson (1984), y posteriormente es acogido por la informática, dado el parecido de la obra con lo que sucede en el mundo actual y las redes de ordenadores de distintos tipos sustentadas en Internet.

En el ámbito informático, el término “ciberespacio” suele abordarse desde una perspectiva jurídico-política vinculada con la ciberseguridad, dado que los Estados buscan preservar la confianza ciudadana en unos procesos gubernamentales cada vez más digitalizados y, al mismo tiempo, protegerse de los efectos derivados de un entorno digital globalizado. A la par, este enfoque informático responde también al interés de las corporaciones por resguardar la confiabilidad y seguridad de sus operaciones, incluidas las transacciones económicas y el tratamiento de datos, frente a socios, inversores y clientes (Harari, 2016; Letho, 2015).

Desde la perspectiva filosófica, el ciberespacio se ha abordado buscando reconstruir su evolución histórica y su impacto tanto en los individuos como en la sociedad. No obstante, su conceptualización resulta ambigua, pues no se delimita con precisión si alude a infraestructuras tecnológicas concretas, a los flujos de información, a las interacciones sociales, a dimensiones culturales, a cuestiones legales o a la combinación de todos estos aspectos. Esta indefinición dificulta su aplicación en diferentes campos del conocimiento, aun cuando, por su naturaleza multifactorial, exige ser examinado desde un enfoque interdisciplinario que integre diversas ciencias.

El término ciberespacio incorpora, además, una complejidad filosófico-semántica vinculada al propio concepto de “espacio”. Este ha sido objeto de prolongados debates tanto en la filosofía como en las ciencias, tal como se evidencia en la histórica controversia entre Newton y Leibniz en el siglo XVIII (Rada, 1980). Para efectos de este estudio, se adopta una noción de espacio de carácter intuitivo y cotidiano que se aproxima a la perspectiva leibniziana, entendiendo el espacio como el entramado de relaciones de proximidad y adyacencia entre diversas entidades. Desde este enfoque, el ciberespacio se concibe como un ámbito que posibilita múltiples interacciones entre entidades mediadas y condicionadas por entornos artificiales con base material (Santana & Báez, 2022).

Partiendo del principio de que la precisión conceptual favorece el progreso científico y tecnológico (Romero, 2017, 2018; Bunge, 2017), resulta necesario delimitar aquellos términos de gran relevancia para que puedan emplearse con un sentido y una referencia uniformes en las distintas disciplinas en que se utilicen. Esta delimitación, además de permitir un uso plural, facilita que los conceptos puedan adaptarse a transformaciones futuras que los afecten directa o indirectamente.

De acuerdo con la Estrategia Nacional para la Seguridad del Ciberespacio (2023), el ciberespacio puede concebirse como una suerte de “sistema nervioso” o “sistema de control” de un país, conformado por una extensa red de ordenadores interconectados, servidores, enrutadores, conmutadores y cables de fibra óptica, que en conjunto sustentan el funcionamiento de infraestructuras críticas (Kuehl, 2009, p. 27).

Cibernética

El término cibernética proviene del vocablo griego kybernetes, utilizado en la Antigua Grecia para referirse al arte de gobernar un navío. Esta noción fue retomada por Wiener y Rosenblueth, quienes la ampliaron para aludir no solo al control y regulación de embarcaciones, sino a la capacidad de autorregulación y control de cualquier sistema. Así, la cibernética pasó a entenderse como el estudio de las estructuras y mecanismos de los sistemas reguladores (Barbosa Martínez, 2004; Merejo, 2021). Dicho enfoque interdisciplinario toma como modelo la regulación propia de los organismos vivos para replicarla en sistemas artificiales u organizacionales. Entre sus fundamentos teóricos se encuentran: la teoría de la información, orientada a la medición y representación de datos, así como a la capacidad de los sistemas de comunicación para procesarlos y transmitirlos; la teoría de algoritmos, dedicada a explicar y gestionar el flujo interno de información en los sistemas; y la teoría de autómatas, centrada en el estudio de máquinas abstractas y de los problemas que estas pueden resolver (Téllez, 2016).

Posteriormente, sobre la base de los planteamientos de Wiener y Rosenblueth, Heinz von Foerster (1991) desarrolla la denominada cibernética de segundo orden. Esta perspectiva sitúa al sujeto observador en un plano distinto del fenómeno analizado, aun cuando dicho sujeto forme parte de él, con el fin de generar explicaciones más completas y reflexivas. A partir de este enfoque se configuran antecedentes y marcos conceptuales que facilitan la interpretación de los actuales procesos sociotécnicos y científicos.

La cibernética, en sus vertientes de primer y segundo orden, se ocupa tanto del diseño de sistemas concebidos como heteroorganizaciones, es decir, aquellos en los que un agente externo interviene para organizar su funcionamiento, como del análisis y

comprensión de sistemas que no han sido configurados deliberadamente por un sujeto, sino que se presentan ya constituidos. En esta última categoría se ubican los organismos vivos, incluidos los seres humanos, así como los sistemas sociales en los que estos participan; sistemas que, si bien reciben aportes de sus integrantes, no han sido estructurados en su totalidad por ellos.

Tal como se ha expuesto, el desarrollo histórico de la cibernética estuvo atravesado por las nociones de autonomía y autorreferencia. En este sentido, puede inferirse que la cibernética alude a sistemas regidos por sus propias normas, con la capacidad de autorreferenciarse en sus procesos de autorregulación. Esto implica que tales sistemas toman sus propias operaciones como objeto de análisis para asegurar su correcto funcionamiento, corrigiendo internamente cada proceso mediante mecanismos de retroalimentación constante que permiten verificar si las acciones ejecutadas contribuyen al cumplimiento de los objetivos establecidos (Pakman, 2009).

Las referencias y normas que rigen estos sistemas están constituidas esencialmente por mensajes, es decir, por información, conformando en última instancia un sistema de comunicación (Weiner, 1989). Desde esta perspectiva, la cibernética se configura como una herramienta conceptual valiosa para explicar el funcionamiento de los sistemas informáticos, cuyo desarrollo se sustenta precisamente en la información y la comunicación. Además, en términos de apropiación social, el prefijo “ciber” adquirió mayor relevancia para describir estas relaciones informáticas con la introducción y posterior popularización del término cyberspace (ciberespacio) por William Gibson en su novela Neuromancer (1984), donde se presenta al ciberespacio como un entorno emergente no material en el que los usuarios interactúan mediante redes de ordenadores para realizar actividades sociales diversas, incluidas las de carácter ilícito.

En la actualidad, es posible observar que todo término —ya sea sustantivo o adjetivo— que incorpore el prefijo “ciber” alude a interacciones que superan el contacto físico directo. Dichas interacciones están mediadas por sistemas informáticos y remiten a procesos relacionados con máquinas, información digitalizada o, en general, con el uso de ordenadores en un espacio emergente de interacción no tangible ni material.

Amenaza Cibernética

Las amenazas cibernéticas pueden entenderse como acciones maliciosas dirigidas a obtener acceso no autorizado a información sensible de organizaciones, incluyendo datos personales de empleados, clientes o información estratégica vinculada al funcionamiento institucional (Canvia, 2023). Este tipo de amenazas compromete directamente la seguridad y defensa de los Estados.

Un ejemplo significativo es el ransomware CryptoLocker, que apareció

inicialmente en 2007. Este malware se difundía principalmente mediante correos electrónicos con archivos adjuntos infectados y, una vez instalado en el equipo, localizaba y cifraba los archivos más valiosos. Se calcula que llegó a afectar a aproximadamente 500 000 computadoras. Su propagación se realizaba a través de una extensa red de equipos domésticos infectados. Tras una operación conjunta de empresas y organismos de seguridad, se logró tomar control de esta red, lo que permitió interceptar la información enviada a los ciberdelincuentes sin que estos lo advirtieran.

Seguridad Digital

El concepto de seguridad posee múltiples acepciones. En términos amplios, proviene del latín securitas y se asocia con la idea de protección o resguardo frente a peligros, daños o riesgos. Algo seguro se considera firme, confiable y cierto; por lo tanto, la seguridad puede entenderse también como sinónimo de certeza (Avenía, 2017).

En el ámbito digital, la seguridad se refiere a la protección de los dispositivos conectados a Internet y de la información que contienen, frente a intrusiones como la piratería, el phishing u otros ataques. Esta práctica es esencial para salvaguardar datos personales y sensibles, así como para mantener la integridad de los sistemas y la privacidad de los usuarios.

2.4 Hipótesis

2.4.1 Hipótesis General

La capacidad de ciberdefensa del Ejército del Perú influye significativamente en el ciberespacio, 2024.

2.4.2 Hipótesis Específicas

La capacidad de defensa del Ejército del Perú influye significativamente en el ciberespacio, 2024.

La capacidad de explotación del Ejército del Perú influye significativamente en el ciberespacio, 2024.

La capacidad de respuesta del Ejército del Perú influye significativamente en el ciberespacio, 2024.

La capacidad de investigación digital del Ejército del Perú influye significativamente en el ciberespacio, 2024.

Capítulo III: Método

3.1. Enfoque de Investigación

La investigación de enfoque cuantitativo se sustenta en los paradigmas del positivismo, neopositivismo y pospositivismo, priorizando la objetividad como un principio esencial en la producción del conocimiento (Hernández & Mendoza, 2018). Este tipo de investigación parte del supuesto de que la realidad es estable y puede describirse mediante observaciones y mediciones sistemáticas, lo que permite obtener resultados verificables y replicables.

El enfoque cuantitativo se encuadró en la obtención y un posterior análisis de datos numéricos que permitió la descripción, explicación y predicción de los fenómenos. Buscó establecer relaciones causales o correlacionales mediante el uso de métodos estadísticos; utilizando datos que pudieron ser medidos numéricamente, los cuales fueron recolectados mediante instrumentos estandarizados como encuestas, cuestionarios, y experimentos. Asimismo, se emplearon técnicas estadísticas para analizar los datos, y se utilizaron modelos matemáticos para interpretar los resultados obtenidos y validar la hipótesis propuesta.

Para efectos de nuestra investigación el enfoque cuantitativo nos permitió conocer, medir y analizar de una manera estadística las capacidades de ciberdefensa y su influencia en el ciberespacio. Esto incluyó datos sobre recursos, capacidades técnicas y resultados de ciberdefensa.

3.2. Tipo de Investigación

Las investigaciones de tipo básica, igualmente conocidas como investigaciones teóricas o puras. Las cuales tienen un fin puramente cognoscitivo, repercutiendo en algunos casos en las correcciones de los conocimientos, y en otros en su perfeccionamiento, pero definitivamente con la finalidad de perfeccionar el conocimiento (Consejo Nacional de la Universidad Peruana, 1974).

Una investigación básica es esencial para el progreso en el conocimiento científico, la validación de teorías y la provisión de evidencia empírica que tuvo importantes implicaciones prácticas en campos como la ciberdefensa del Ejército del Perú. De este modo, nos permitió comprender cómo la inversión en tecnología, la formación del personal y la adopción de políticas influyen en el ciberespacio.

3.3. Nivel de Investigación

Las investigaciones de nivel explicativo se enfocan en identificar las causas y

efectos de los fenómenos analizados, intentando comprender las razones subyacentes a ciertos eventos y cómo se interrelacionan. Este enfoque va más allá de simplemente describir los fenómenos; profundiza en las relaciones causales mediante el uso de métodos cuantitativos para probar hipótesis y establecer conexiones causales. Kerlinger y Lee (2002) subrayan que este tipo de estudio es fundamental para la evolución de las teorías científicas, puesto que ofrece una visión detallada de los mecanismos subyacentes y las relaciones entre diferentes variables.

3.4. Diseño de Investigación

La investigación no experimental se caracteriza por analizar fenómenos sin manipular de forma deliberada las variables involucradas. Esto implica que no se introducen cambios intencionales en las variables independientes para observar su efecto en otras, sino que se registran y analizan en su contexto natural tal como se presentan (Hernández & Mendoza, 2018). En este tipo de estudio, las situaciones no son creadas ni inducidas por el investigador, sino que se examinan acontecimientos ya existentes, con el fin de describirlos y comprender sus relaciones sin intervenir en ellos.

En ese sentido, la investigación que realizamos tiene un diseño no experimental, ya que nos permitió estudiar y describir los fenómenos existentes sin la manipulación de la variable, la capacidad de ciberdefensa del Ejército del Perú, ni de la variable del ciberespacio, ya que no pudieron ser manipuladas, además, de la no intervención directa en las situaciones reales; asimismo, se ha determinado que es de corte transeccional o transversal porque recolectamos los datos en un exclusivo momento o en un único tiempo, definido por un único año (2024), en el cual realizamos la investigación.

3.5. Población y Muestra de Estudio

3.5.1. Población de Estudio

La población de estudio estuvo integrada por oficiales superiores, oficiales subalternos, técnicos y suboficiales del Ejército del Perú que desempeñan funciones en el Centro de Ciberdefensa del Ejército, el Centro de Informática del Ejército y la Dirección de Telemática del Ejército. En total, la población estuvo constituida por 52 integrantes pertenecientes a dichas dependencias.

3.5.2. Muestra de Estudio

La selección del tamaño de la muestra se consideró el tamaño de la población. Dado que la población es homogénea y relativamente pequeña, estamos tratando con

una población muestral. En este caso, el tamaño de la muestra fue igual al tamaño de la población, es decir es una muestra censal.

$$P<100$$

$$n=P=30$$

Donde n = muestra

P = población

3.6. Variables de Investigación

Variable X: La capacidad de ciberdefensa del Ejército del Perú

Variable Y: Ciberespacio

3.7. Operacionalización de las Variables

Variables	Dimensiones	Indicadores
X: La capacidad de ciberdefensa del Ejército del Perú	X1Capacidad de defensa	• Eficiencia en la prevención de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. • Eficiencia en la prevención de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas.
	X2 Capacidad de explotación	• Eficiencia en la protección de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. • Eficiencia en la protección de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas.
	X3 Capacidad de respuesta	• Eficiencia en la resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. • Eficiencia en la resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas.
	X4 Capacidad de investigación digital	• Eficiencia en la búsqueda de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas.

		• Eficiencia en la identificación de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. • Eficiencia en el reconocimiento de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. • Eficiencia en la vigilancia de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. • Eficiencia en el seguimiento de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. • Eficiencia en limitar o negar, temporal o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, impactando en sus capacidades; recurriendo a medidas activas. • Eficiencia en el análisis de la evidencia digital para determinar su funcionalidad, a través de un proceso de ingeniería inversa. • Eficiencia en el análisis de la evidencia digital para determinar su comportamiento, a través de un proceso de ingeniería inversa. • Eficiencia en el análisis de la evidencia digital para determinar su origen, a través de un proceso de ingeniería inversa. • Eficiencia en el análisis de la evidencia digital para determinar su impacto, a través de un proceso de ingeniería inversa. • Eficiencia en el análisis de la evidencia digital para determinar su explotación futura, a través de un proceso de ingeniería inversa.
Y: Ciberespacio	Y1 Redes interconectadas e interdependientes de infraestructura de tecnología de la información	• Eficiencia en el empleo del Internet a través de las Redes interconectadas e interdependientes de infraestructura de tecnología de la información. • Eficiencia de las Redes de telecomunicaciones. • Eficiencia de los Sistemas informáticos en el Cecyber • Eficiencia de los procesadores en las Redes interconectadas e interdependientes de infraestructura de tecnología de la información

	Y2 Redes interconectadas e interdependientes de infraestructura de datos almacenados	• Eficiencia de los controladores integrados de las Redes interconectadas e interdependientes de infraestructura de datos almacenados. • Eficiencia de los usuarios Redes interconectadas e interdependientes de infraestructura de datos almacenados.

3.8. Técnicas e Instrumentos de Recolección de Datos

En esta investigación se utilizó la encuesta como técnica principal de recolección de datos, aplicada al personal militar del Ejército del Perú perteneciente al Centro de Ciberdefensa, el Centro de Informática y la Dirección de Telemática. Esta herramienta posibilitó analizar el nivel de conocimiento, las motivaciones, las actitudes y las percepciones de oficiales superiores, oficiales subalternos, técnicos y suboficiales en relación con la capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio. La encuesta se aplicó de manera individual mediante una encuesta escrita, diseñada específicamente para obtener datos detallados y opiniones fundamentadas sobre el tema de estudio. Este enfoque garantizó que se analice adecuadamente las hipótesis planteadas, asegurando así la validez y confiabilidad de los datos recogidos. La encuesta que se utilizó se encuentra como parte de los anexos de este trabajo, el cual fue validado por tres expertos.

3.9. Técnicas de Procesamiento y Análisis de Datos

Para el procesamiento de los datos se diseñó una base de datos estructurada que incorporó variables esenciales, tales como las percepciones sobre la capacidad de ciberdefensa y el impacto en el ciberespacio del personal militar del Ejército del Perú. Se llevó a cabo un proceso riguroso de limpieza y preparación de los datos, eliminando respuestas incompletas y estandarizando formatos con el fin de asegurar la coherencia y fiabilidad de la información recolectada. Posteriormente, se aplicaron estadísticas descriptivas y técnicas de organización para resumir y visualizar los datos de manera clara y comprensible.

Para el análisis se utilizó el software estadístico SPSS versión 26, que permitió responder al objetivo e hipótesis general mediante análisis descriptivo, así como establecer comparaciones para los objetivos e hipótesis específicos a través de pruebas estadísticas no paramétricas. Entre estas, se empleó la prueba Chi-cuadrado de

Pearson para la contrastación de hipótesis y el coeficiente alfa de Cronbach para evaluar la fiabilidad de las escalas y de los datos obtenidos. Los resultados fueron presentados en tablas y gráficos acompañados de descripciones breves.

Asimismo, se utilizaron medidas de frecuencia, tablas y gráficos para comprender el comportamiento de los datos en cada variable. La interpretación de estos resultados resultó esencial para integrar de manera científica los datos obtenidos y las inferencias derivadas de ellos. De esta forma, el análisis y la interpretación, enmarcados en teorías y doctrinas pertinentes, proporcionaron la base necesaria para la elaboración de las conclusiones finales del estudio.

Capítulo IV: Resultados

En este capítulo se presentan los resultados obtenidos a partir de la aplicación de los cuestionarios a la muestra integrada por oficiales, técnicos y suboficiales que laboran en el Centro de Ciberdefensa, el Centro de Informática y la Dirección de Telemática del Ejército del Perú durante el semestre 2024-II. El instrumento de recolección de datos fue elaborado considerando las dos variables de la investigación: Capacidad de Ciberdefensa del Ejército del Perú y Ciberespacio.

Para el procesamiento y análisis de la información se utilizó el software estadístico IBM SPSS Statistics 26, mediante el cual se generaron tablas estadísticas como frecuencias y tablas de contingencia y representaciones gráficas, incluyendo gráficos de barras y diagramas de dispersión, con el fin de facilitar la interpretación de los resultados.

4.1. Análisis Descriptivo

VI: Capacidad de Ciberdefensa del Ejército del Perú
D1: Capacidad de Defensa (3 ITEMS)
D2: Capacidad de Explotación (3 ITEMS)
D3: Capacidad de Respuesta (3 ITEMS)
D4: Capacidad de Investigación Digital (5 ITEMS)
Total 14 ítems

Tabla 1

Baremos para la Variable Capacidad de Ciberdefensa en el Ejército del Perú y sus dimensiones

NIVEL	VI	D1	D2	D3	D4
BAJO	(14-32)	(3-6)	(3-6)	(3-6)	(5-11)
MODERADO	(33-51)	(7-11)	(7-11)	(7-11)	(12-18)
ALTO	(52-70)	(12-15)	(12-15)	(12-15)	(19-25)
VALOR.MAX	70	15	15	15	25
VALOR.MIN	14	3	3	3	5
RANGO	57	12	12	12	21
INTERVALO	19	4	4	4	7

4.1.1. Variable 1: Capacidad de Ciberdefensa del Ejército del Perú

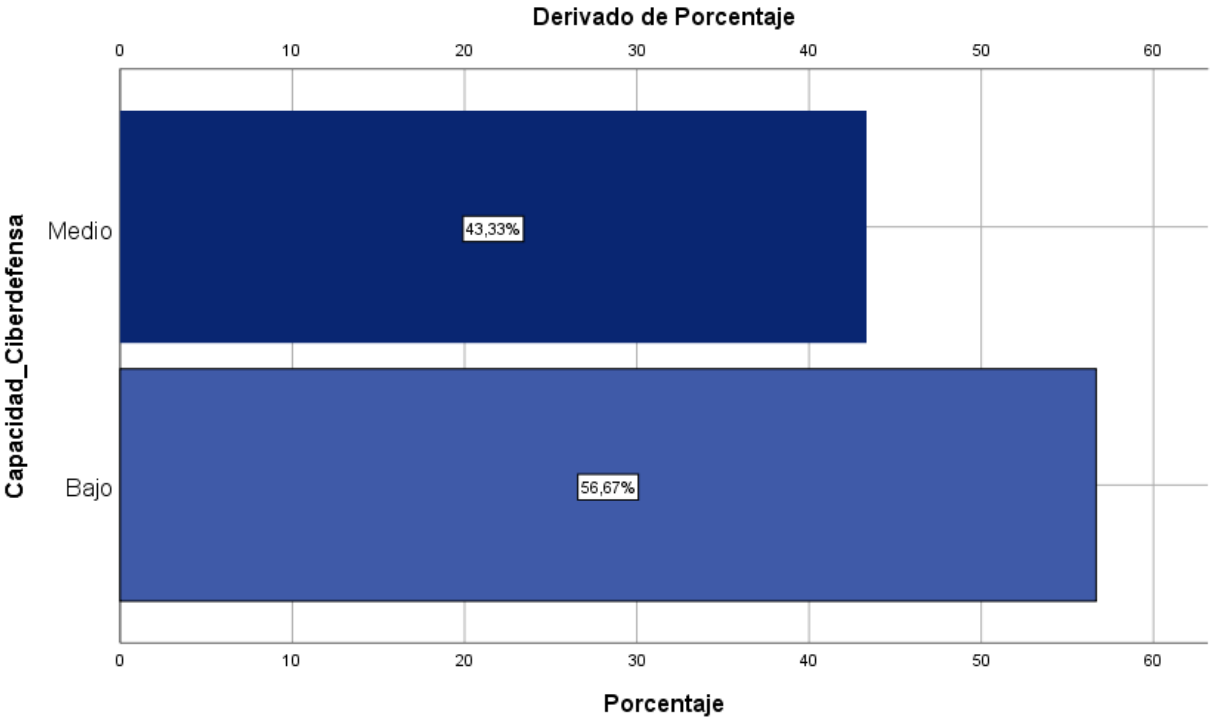
Tabla 2

Tabla de frecuencias para la Capacidad de Ciberdefensa del Ejército del Perú según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	17	56,7	56,7	56,7
MODERADO	13	43,3	43,3	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 1

Figura de frecuencias para la Capacidad de Ciberdefensa del Ejército del Perú según niveles



El análisis de la tabla revela información importante sobre la distribución de niveles en la variable de la Capacidad de Ciberdefensa del Ejército del Perú. De un total de 30 encuestados, se observa que 17 personas, es decir, el 56.7%, se clasificaron en

la categoría "Bajo". Esto indica que más de la mitad de los participantes perciben la Capacidad de Ciberdefensa en un nivel de desempeño que podría considerarse insatisfactorio.

Por otro lado, 13 encuestados (43.3%) se encuentran en la categoría "Moderado", lo que sugiere que una parte significativa de los participantes muestra un desempeño aceptable, aunque aún hay margen para mejorar. Es notable, sin embargo, que no hubo encuestados en la categoría "Alto", lo que indica que ningún participante considera que la Capacidad de Ciberdefensa alcanza un nivel destacado en la evaluación.

Esta distribución resalta áreas críticas que requieren atención y desarrollo, dado que una alta proporción de los encuestados se encuentra en niveles bajos y moderados. La ausencia de niveles altos sugiere que hay una oportunidad significativa para implementar estrategias que fomenten el crecimiento y la mejora de la Capacidad de Ciberdefensa.

4.1.2. Dimensión 1: Capacidad de Defensa

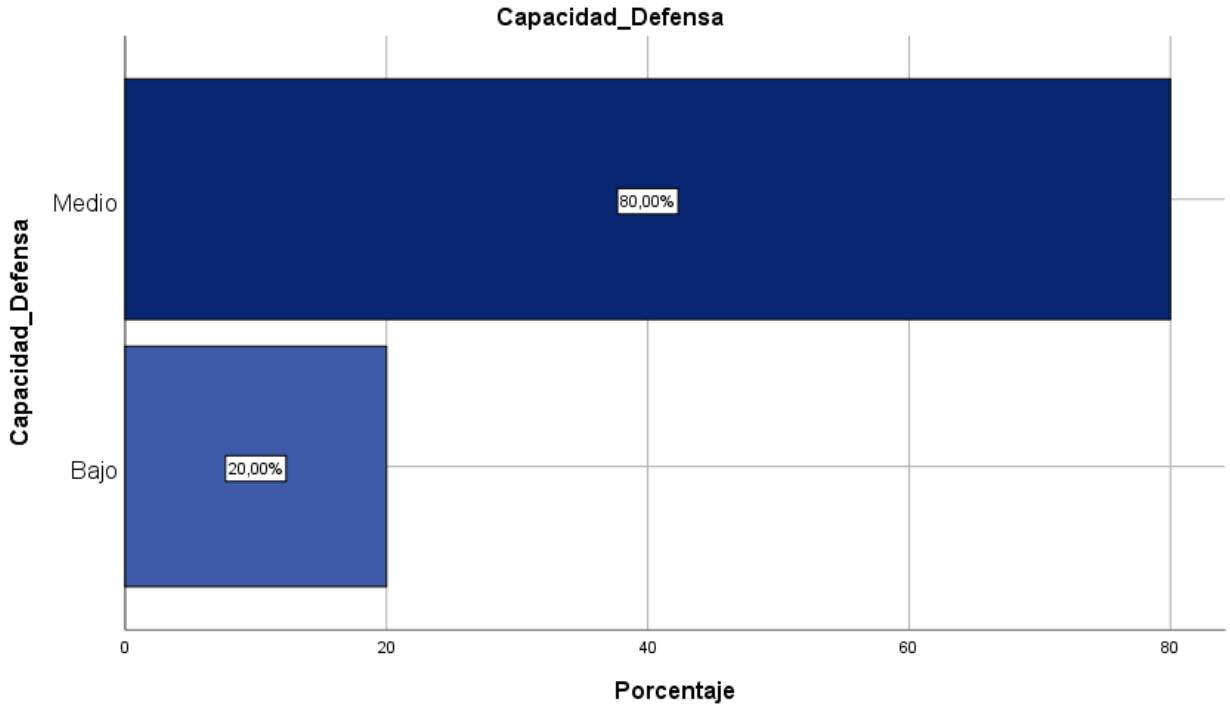
Tabla 3

Tabla de frecuencias para la dimensión Capacidad de Defensa según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	06	20,0	20,0	20,0
MODERADO	24	80,0	80,0	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 2

Figura de frecuencias para la dimensión Capacidad de Defensa según niveles



El análisis de la tabla revela información significativa sobre la distribución de niveles en la variable de la Capacidad de Defensa del Ejército del Perú. De un total de 30 encuestados, se observa que 6 personas, es decir, el 20%, se clasificaron en la categoría "Bajo". Esto indica que solo una pequeña proporción de los participantes percibe la Capacidad de Defensa en un nivel insatisfactorio.

En contraste, la mayoría de los encuestados, 24 personas (80%), se encuentra en la categoría "Moderado". Esto sugiere que una parte significativa de los participantes muestra un desempeño aceptable, aunque todavía existe un margen considerable para la mejora. Es importante señalar que no hubo encuestados en la categoría "Alto", lo que implica que ninguno considera que la Capacidad de Defensa alcanza un nivel destacado en la evaluación.

Esta distribución pone de relieve áreas que requieren atención y desarrollo, ya que, aunque la mayoría de los participantes se encuentran en un nivel moderado, la falta de niveles altos sugiere que hay oportunidades importantes para implementar estrategias que fortalezcan y optimicen la Capacidad de Defensa.

4.1.3. Dimensión 2: Capacidad de Explotación

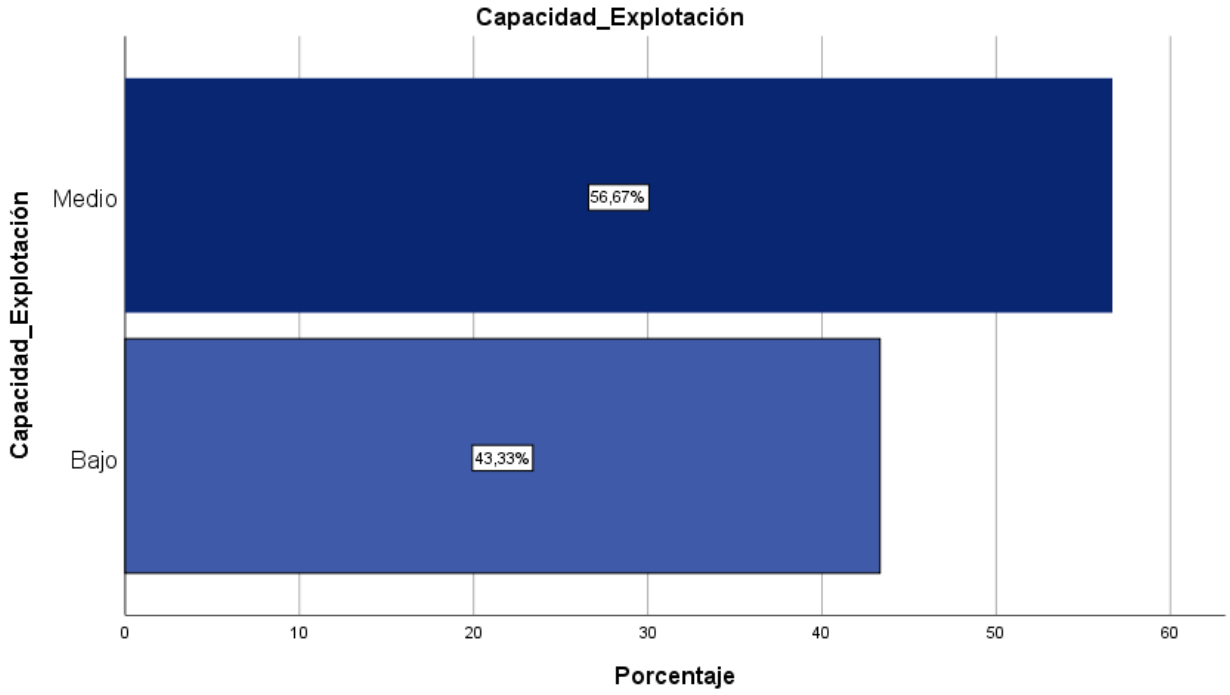
Tabla 4

Tabla de frecuencias para la dimensión Capacidad de Explotación según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	13	43,3	43,3	43,3
MODERADO	17	56,7	56,7	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 3

Figura de frecuencias para la dimensión Capacidad de Explotación según niveles



El análisis de la tabla revela información relevante sobre la distribución de niveles en la variable de Capacidad de Explotación del Ejército del Perú. De un total de 30 encuestados, se observa que 13 personas, es decir, el 43.3%, se clasificaron en la

categoría "Bajo". Esto indica que una proporción considerable de los participantes percibe la Capacidad de Explotación en un nivel que podría considerarse insatisfactorio.

Por otro lado, 17 encuestados (56.7%) se encuentran en la categoría "Moderado", lo que sugiere que la mayoría de los participantes muestra un desempeño aceptable, aunque todavía hay espacio para mejoras. Sin embargo, es importante destacar que no hubo encuestados en la categoría "Alto", lo que significa que ningún participante considera que la Capacidad de Explotación alcanza un nivel destacado en la evaluación.

Esta distribución subraya áreas críticas que requieren atención y desarrollo, ya que una parte significativa de los encuestados se sitúa en niveles bajos y moderados. La ausencia de niveles altos indica que hay una oportunidad valiosa para implementar estrategias que potencien y optimicen la Capacidad de Explotación.

4.1.4. Dimensión 3: Capacidad de Respuesta

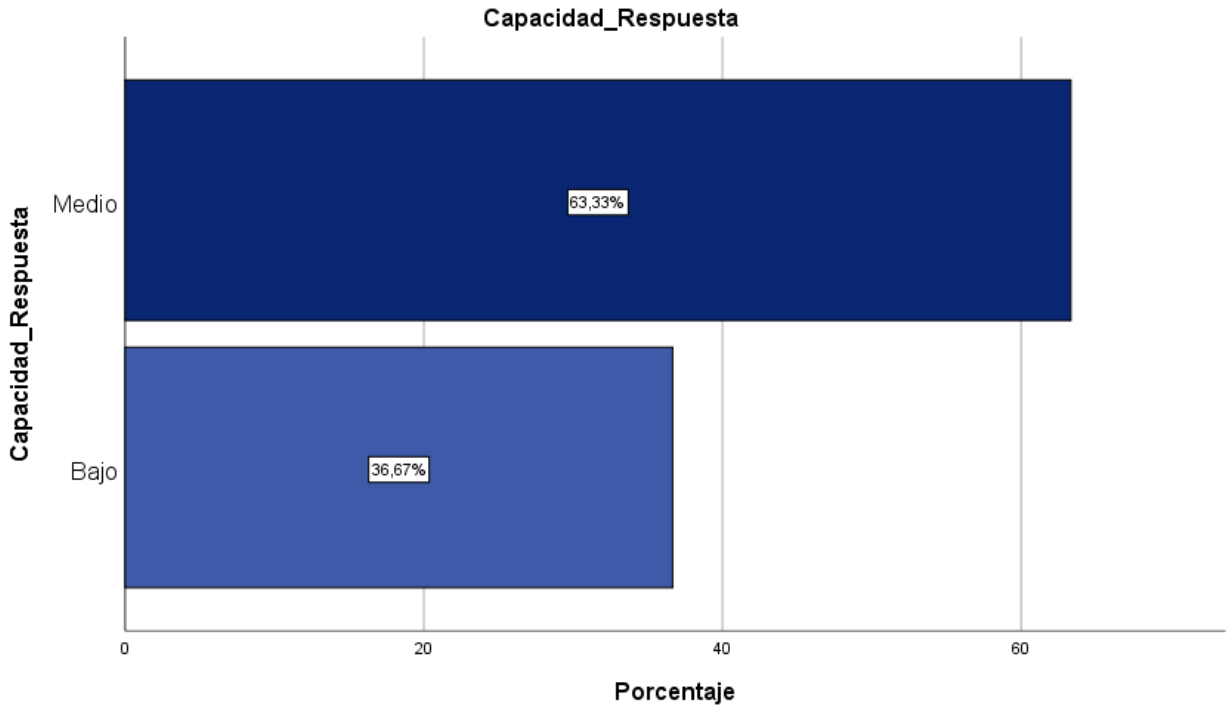
Tabla 5

Tabla de frecuencias para la dimensión Capacidad de Respuesta según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	11	36,7	36,7	36,7
MODERADO	19	63,3	63,3	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 4

Figura de frecuencias para la dimensión Capacidad de Respuesta según niveles



El análisis de la tabla revela información importante sobre la distribución de niveles en la variable de Capacidad de Respuesta del Ejército del Perú. De un total de 30 encuestados, se observa que 11 personas, es decir, el 36.7%, se clasificaron en la categoría "Bajo". Esto indica que una porción considerable de los participantes percibe la Capacidad de Respuesta en un nivel que podría considerarse insatisfactorio.

Por otro lado, 19 encuestados (63.3%) se encuentran en la categoría "Moderado", lo que sugiere que la mayoría de los participantes muestra un desempeño aceptable, aunque todavía existe un margen significativo para la mejora. Es importante resaltar que no hubo encuestados en la categoría "Alto", lo que implica que ningún participante considera que la Capacidad de Respuesta alcanza un nivel destacado en la evaluación.

Esta distribución destaca áreas críticas que requieren atención y desarrollo, ya que la percepción de una Capacidad de Respuesta baja o moderada puede afectar la efectividad del Ejército en situaciones críticas. La ausencia de niveles altos sugiere que hay una oportunidad significativa para implementar estrategias que fortalezcan la capacidad de reacción ante incidentes cibernéticos.

Dado que la Capacidad de Respuesta es esencial para mitigar y gestionar ciberamenazas de manera efectiva, es crucial que se realicen intervenciones, tales

como entrenamientos específicos y mejoras en los protocolos de respuesta, para elevar los niveles de competencia en esta dimensión. La evaluación sugiere que la atención a estos aspectos podría resultar en una respuesta más ágil y efectiva ante desafíos en el ciberespacio.

4.1.5. Dimensión 4: Capacidad de Investigación Digital

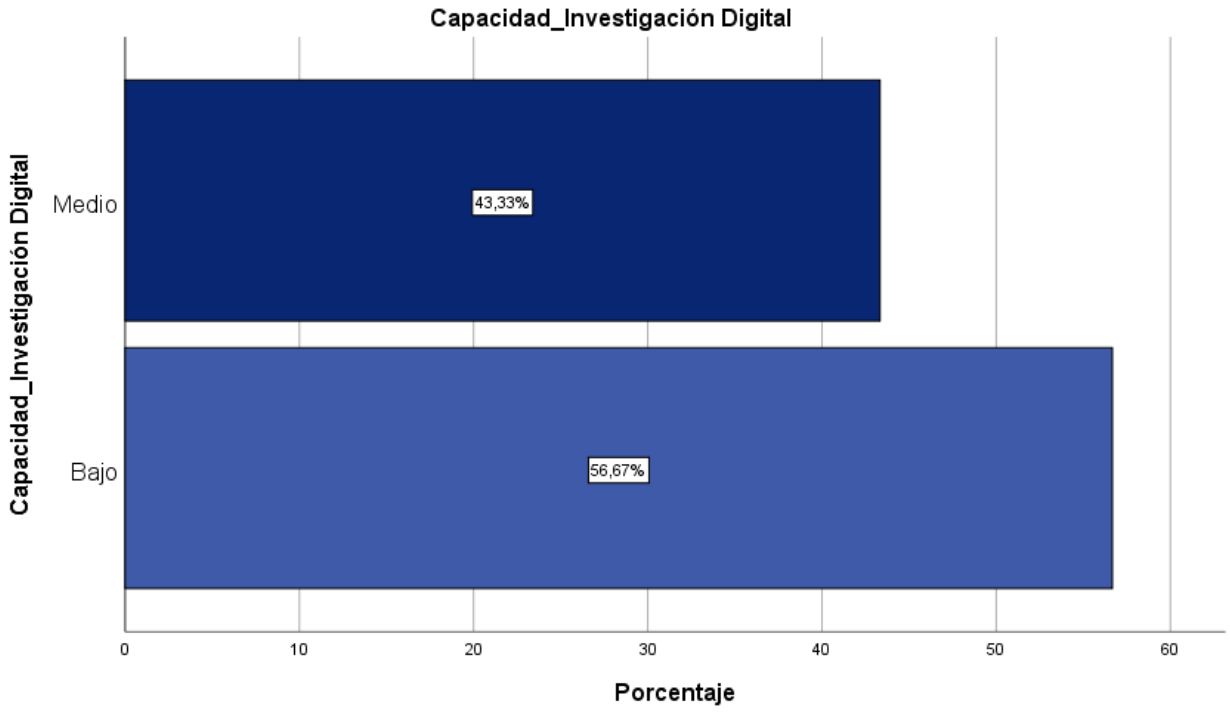
Tabla 6

Tabla de frecuencias para la dimensión Capacidad de Investigación Digital según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	17	56,7	56,7	56,7
MODERADO	13	43,3	43,3	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 5

Figura de frecuencias para la dimensión Capacidad de Investigación Digital según niveles.



El análisis de la tabla revela información importante sobre la distribución de niveles en la variable de Capacidad de Investigación Digital del Ejército del Perú. De un total de 30 encuestados, se observa que 17 personas, es decir, el 56.7%, se clasificaron en la categoría "Bajo". Esto indica que una mayoría significativa de los participantes percibe la Capacidad de Investigación Digital en un nivel que podría considerarse insatisfactorio.

Por otro lado, 13 encuestados (43.3%) se encuentran en la categoría "Moderado", lo que sugiere que una parte significativa de los participantes muestra un desempeño aceptable en esta dimensión, aunque aún queda un amplio margen para la mejora. Notablemente, no hubo encuestados en la categoría "Alto", lo que implica que ningún participante considera que la Capacidad de Investigación Digital alcanza un nivel destacado en la evaluación.

Esta distribución pone de relieve áreas críticas que requieren atención y desarrollo. La Capacidad de Investigación Digital es fundamental para la identificación y análisis de ciberamenazas, y la escasez de niveles altos indica que hay oportunidades significativas para implementar estrategias de formación y recursos que fortalezcan esta capacidad.

Dado que la investigación digital es clave para el desarrollo de tácticas defensivas efectivas, es crucial realizar intervenciones, como entrenamientos específicos en herramientas digitales y metodologías de investigación, para elevar los niveles de competencia en esta dimensión. Mejorar la Capacidad de Investigación Digital no solo aumentará la efectividad del Ejército en el ciberespacio, sino que también contribuirá a una defensa más robusta contra amenazas cibernéticas.

Resultados Descriptivos de la Segunda Variable

VD: Ciberespacio

D1: Redes Interconectadas de Infraestructura de Tecnología de la Información (09 Ítems)

D2: Redes Interconectadas de Infraestructura de Datos Almacenados (05 Ítems)

Total 14 ítems

Tabla 7

Baremos para la Variable Ciberespacio y sus dimensiones

NIVEL	VD	D1	D2
BAJO	(14-32)	(9-20)	(5-11)
MODERADO	(33-51)	(21-33)	(12-18)
ALTO	(52-70)	(34-45)	(19-25)
VALOR.MAX	70	45	25
VALOR.MIN	14	9	5
RANGO	57	36	21
INTERVALO	19	12	7

4.1.6. Variable 2: Ciberespacio

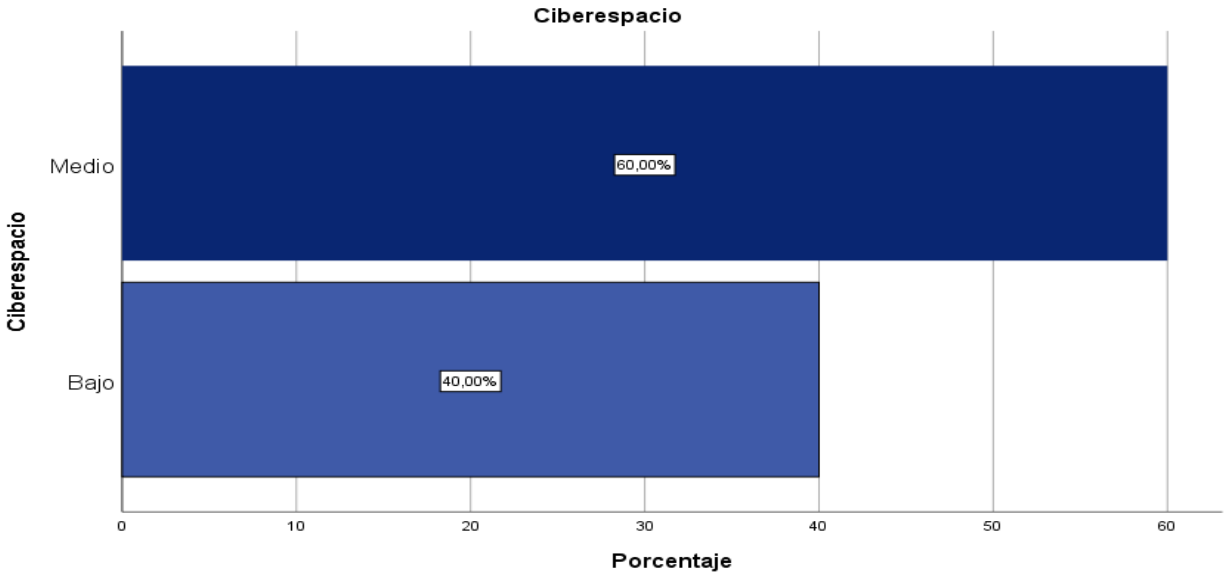
Tabla 8

Tabla de frecuencias para la variable Ciberespacio según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	12	40,0	40,0	40,0
MODERADO	18	60,0	60,0	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 6

Figura de frecuencias para la variable Ciberespacio según niveles



El análisis de la tabla revela información relevante sobre la distribución de niveles en la variable Ciberespacio del Ejército del Perú. De un total de 30 encuestados, se observa que 12 personas, es decir, el 40%, se clasificaron en la categoría "Bajo". Esto indica que una parte considerable de los participantes percibe el manejo del ciberespacio en un nivel que podría considerarse insatisfactorio.

En contraste, 18 encuestados (60%) se encuentran en la categoría "Moderado", lo que sugiere que la mayoría de los participantes muestra un desempeño aceptable en esta área, aunque aún existe un margen significativo para la mejora. Es importante resaltar que no hubo encuestados en la categoría "Alto", lo que implica que ninguno considera que la capacidad del Ejército para operar en el ciberespacio alcanza un nivel destacado en la evaluación.

Esta distribución destaca áreas que requieren atención y desarrollo. La capacidad de operar efectivamente en el ciberespacio es crucial para la defensa y seguridad cibernética, y la alta proporción de encuestados en niveles bajos y moderados sugiere la necesidad de implementar estrategias específicas para mejorar esta habilidad.

Se recomienda establecer programas de capacitación en ciberseguridad y en el uso de herramientas y tecnologías relacionadas con el ciberespacio. Al mejorar la competencia en esta dimensión, el Ejército no solo podrá optimizar su capacidad de respuesta ante ciberamenazas, sino que también fortalecerá su posición general en el ámbito de la defensa cibernética.

4.1.7. Dimensión 1: Redes Interconectadas de Infraestructura de Tecnología de la Información

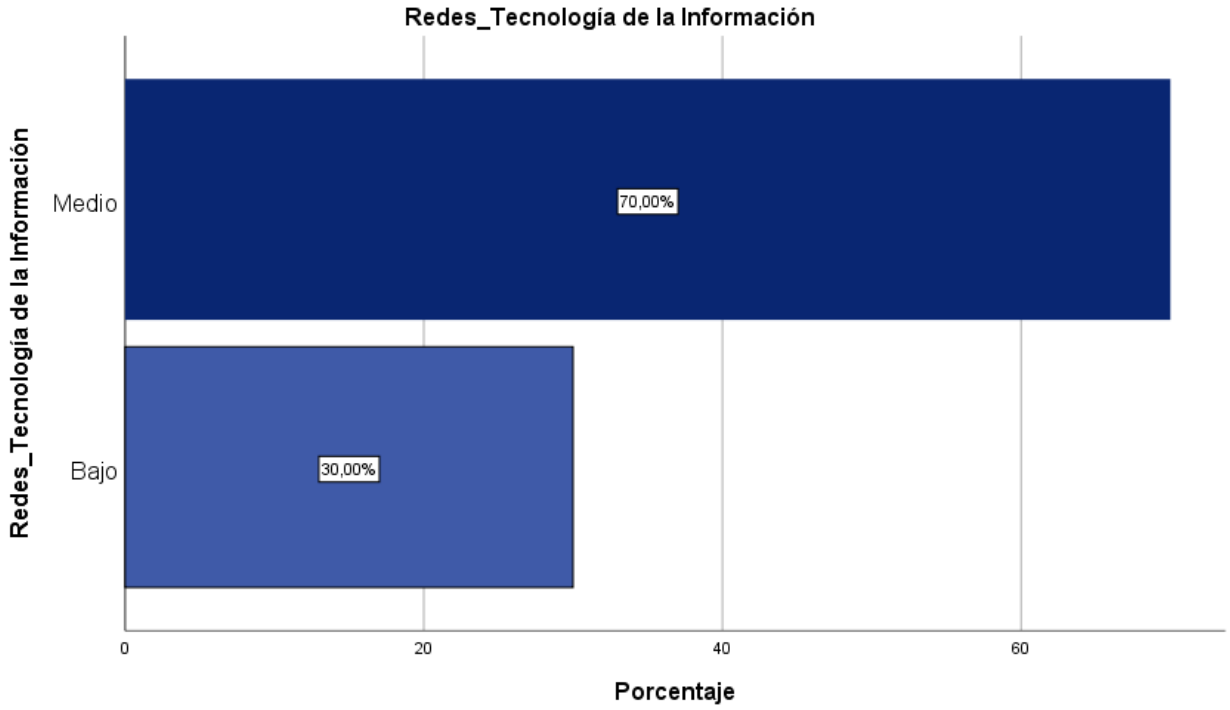
Tabla 9

Tabla de frecuencias para la dimensión Redes Tecnologías de Información según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	09	30,0	30,0	30,0
MODERADO	21	70,0	70,0	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 7

Figura de frecuencias para la dimensión Redes de Tecnologías de Información según niveles



El análisis de la tabla revela información significativa sobre la distribución de niveles en la variable Redes y Tecnologías de Información del Ejército del Perú. De un total de 30 encuestados, se observa que 9 personas, es decir, el 30%, se clasificaron

en la categoría "Bajo". Esto indica que una proporción considerable de los participantes percibe su competencia en esta área en un nivel que podría considerarse insatisfactorio.

Por otro lado, 21 encuestados (70%) se encuentran en la categoría "Moderado", lo que sugiere que la mayoría de los participantes muestra un desempeño aceptable, aunque todavía hay un margen considerable para la mejora. Es importante señalar que no hubo encuestados en la categoría "Alto", lo que implica que ningún participante considera que las competencias en Redes y Tecnologías de Información alcanzan un nivel destacado en la evaluación.

Esta distribución destaca áreas críticas que requieren atención y desarrollo. Dado que las redes y tecnologías de información son fundamentales para la operación eficiente del Ejército en el contexto actual, la alta proporción de encuestados en niveles bajos y moderados sugiere la necesidad de implementar estrategias específicas para mejorar esta competencia.

Se recomienda la implementación de programas de capacitación en el uso de tecnologías de información y comunicación, así como en la gestión de redes, para elevar los niveles de competencia en esta dimensión. Mejorar las habilidades en redes y tecnologías de información no solo optimizará la capacidad del Ejército para operar y comunicarse eficazmente, sino que también fortalecerá su defensa cibernética en un entorno cada vez más complejo.

4.1.8. Dimensión 2: Redes Interconectadas de Infraestructura de Datos Almacenados

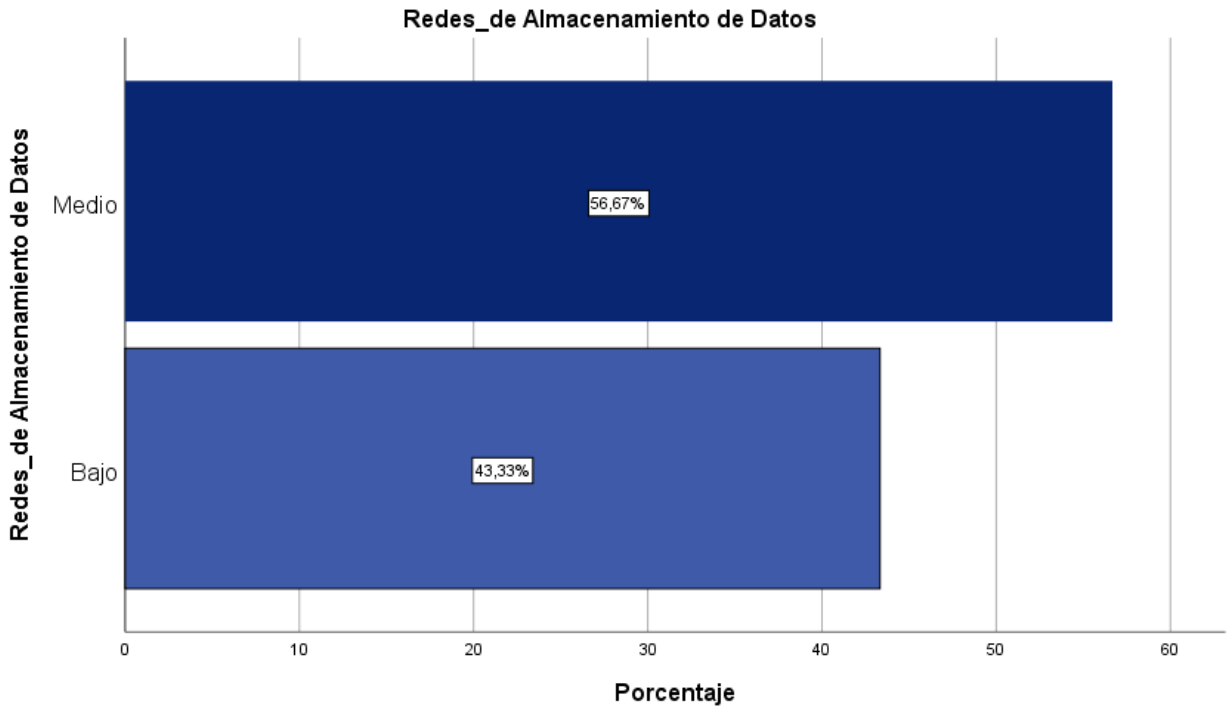
Tabla 10

Tabla de frecuencias para la dimensión Redes de Datos Almacenados según niveles

NIVEL	FRECUENCIA	%	% VÁLIDO	%ACUMULADO
BAJO	13	43,3	43,3	43,3
MODERADO	17	56,7	56,7	100,0
ALTO	0	0	0	100,0
TOTAL	30	100,0	100,0	

Figura 8

Figura de frecuencias para la dimensión Redes de Datos Almacenados según niveles



El análisis de la tabla revela información relevante sobre la distribución de niveles en la variable Redes de Datos Almacenados del Ejército del Perú. De un total de 30 encuestados, se observa que 13 personas, es decir, el 43.3%, se clasificaron en la categoría "Bajo". Esto indica que una proporción significativa de los participantes percibe su competencia en esta área como insatisfactoria.

Por otro lado, 17 encuestados (56.7%) se encuentran en la categoría "Moderado", lo que sugiere que la mayoría de los participantes muestra un desempeño aceptable, aunque todavía existe un margen considerable para mejorar. Es importante destacar que no hubo encuestados en la categoría "Alto", lo que implica que ninguno de los participantes considera que sus competencias en Redes de Datos Almacenados alcanzan un nivel destacado en la evaluación.

Esta distribución pone de manifiesto áreas críticas que requieren atención y desarrollo. Dado que la gestión y protección de los datos almacenados son esenciales para la seguridad y eficacia operativa del Ejército, la alta proporción de encuestados en niveles bajos y moderados sugiere la necesidad urgente de implementar estrategias para mejorar esta capacidad.

4.2. ANÁLISIS INFERENCIAL

Análisis Bivariado

Las hipótesis se verificaron mediante el coeficiente de correlación r de Pearson, teniendo en cuenta que es una investigación básica explicativa en donde se busca determinar la influencia de la Capacidad de Ciberdefensa del Ejército en el Ciberespacio.

Tabla 11

Resumen de los resultados de la prueba de hipótesis

Hipótesis	p valor o nivel de significancia	Coeficiente	Decisión
General	0,000	0,908	Aceptar
Específica 1	0,273	0,207	No aceptar
Específica 2	0,002	0,540	Aceptar
Específica 3	0,004	0,513	Aceptar
Específica 4	0,000	0,804	Aceptar

Tabla 12

Interpretación del coeficiente de correlación

Coeficiente	Interpretación
0,00	No existe correlación
0,10	Correlación positiva muy débil
0,25	Correlación positiva débil
0,50	Correlación positiva media
0,75	Correlación positiva considerable

0,90	Correlación positiva muy fuerte
1,00	Correlación positiva perfecta

Variable Ciberespacio y variable Capacidad de Ciberdefensa en el Ejército del Perú

La hipótesis general sometida a prueba fue la siguiente:

"La capacidad de ciberdefensa del Ejército del Perú influye significativamente en el ciberespacio, 2024".

Tabla 13

Correlaciones VD y VI

		CAPACIDAD DE CIBERDEFENSA	CIBERESPACIO
CAPACIDAD DE CIBERDEFENSA	Correlación de Pearson	1	,908**
	Sig. (bilateral)		,000
	N	30	30
CIBERESPACIO	Correlación de Pearson	,908	1
	Sig. (bilateral)	,000	
	N	30	30

Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).

El valor de la correlación de Pearson entre las variables "Capacidad de Ciberdefensa del Ejército del Perú" y "Ciberespacio" es de 0,908. Este valor indica una correlación positiva muy fuerte entre ambas variables. En otras palabras, cuando la "Capacidad de Ciberdefensa" del Ejército del Perú aumenta, también lo hace la influencia que tiene sobre el "Ciberespacio".

La correlación positiva de 0,908 implica que ambas variables tienden a variar en la misma dirección: a medida que la capacidad de ciberdefensa mejora, la presencia o influencia en el ciberespacio también aumenta. Esto es coherente con la hipótesis general, que postula que la capacidad de ciberdefensa influye significativamente en el ciberespacio.

El valor de sig. (bilateral) = 0,000 (p < 0,01) indica que la relación observada entre las variables no es producto del azar, sino que es estadísticamente significativa al nivel de confianza del 99%. En otras palabras, podemos confiar en que la correlación entre la "Capacidad de Ciberdefensa" y el "Ciberespacio" es real y no fruto de variaciones aleatorias.

De acuerdo con los criterios establecidos por Hernández y Mendoza (2018), esta correlación es muy fuerte. En la práctica, esto significa que existe una fuerte relación entre el incremento de la capacidad de ciberdefensa y el aumento de la influencia en el ciberespacio, lo que podría tener implicaciones muy importantes en la formulación de políticas y estrategias para mejorar la Ciberdefensa en el Ejército del Perú.

La muestra consta de 30 casos, lo cual es adecuada para este tipo de análisis. Teniendo en cuenta que es una población pequeña, por lo que se puede considerar suficiente para que los resultados sean representativos y confiables en cuanto a la validez de la correlación obtenida.

Variable Ciberespacio y D1 de VI Capacidad de Defensa

Tabla 14

Correlaciones VD y D1 VI

		CIBERESPACIO	CAPACIDAD DE DEFENSA
CIBERESPACIO	Correlación de Pearson	1	,207
	Sig. (bilateral)		,273
	N	30	30
CAPACIDAD DE DEFENSA	Correlación de Pearson	,207	1
	Sig. (bilateral)	,273	
	N	30	30

La correlación de Pearson es de 0,207, lo que indica una correlación positiva muy débil entre ambas variables. Esto significa que hay una relación positiva entre la Capacidad de Defensa y el Ciberespacio, pero esa relación es muy débil. Es decir, aunque existe una ligera tendencia de que a medida que la Capacidad de Defensa mejora, también podría haber un aumento en la influencia sobre el Ciberespacio, esta relación es débil y probablemente no tenga un impacto significativo.

El nivel de significación bilateral obtenido es 0,273, valor que supera el umbral de 0,05, lo cual indica que la correlación encontrada no presenta significancia estadística. En consecuencia, no es posible rechazar la hipótesis nula, la cual plantea la inexistencia de relación entre las variables analizadas. Esto sugiere que la asociación observada entre Ciberespacio y Capacidad de Defensa podría deberse a efectos aleatorios dentro de la muestra estudiada. La ausencia de significancia estadística ($p > 0,05$) implica que no se puede afirmar con evidencia suficiente la existencia de una relación real entre ambas variables en la población, por lo que los resultados obtenidos no permiten establecer conclusiones definitivas ni sustentar decisiones basadas en dicha correlación.

Variable Ciberespacio y D2 de VI Capacidad de Explotación

Tabla 15

Correlaciones VD y D2 VI

		CIBERESPACIO	CAPACIDAD DE EXPLOTACIÓN
CIBERESPACIO	Correlación de Pearson	1	,540**
	Sig. (bilateral)		,002
	N	30	30
CAPACIDAD DE EXPLOTACIÓN	Correlación de Pearson	,540**	1
	Sig. (bilateral)	,002	
	N	30	30

Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).

La correlación de Pearson es de 0,540, lo que indica una correlación positiva moderada entre ambas variables. Una correlación de 0,540 es una correlación moderada, lo que sugiere que existe una relación positiva entre la Capacidad de Explotación y el Ciberespacio. Es decir, a medida que la Capacidad de Explotación mejora, también tiende a mejorar la influencia sobre el Ciberespacio, aunque esta relación no es tan fuerte como la que se encontró entre Ciberespacio y Capacidad de Ciberdefensa (que era mucho más fuerte en el análisis anterior). En resumen, hay una relación notable, pero no tan intensa como la que vimos entre el Ciberespacio y la Capacidad de Ciberdefensa.

El valor de 0,002 para la significación bilateral es menor que 0,01. Como la significación es menor que 0,01, podemos afirmar con un alto nivel de confianza (99%) que la correlación observada entre Ciberespacio y Capacidad de Explotación no es producto del azar. Por lo tanto, hay una relación significativa y real entre estas dos variables en la población de estudio.

Variable Ciberespacio y D3 de VI Capacidad de Respuesta

Tabla 16

Correlaciones VD y D3 VI

		CIBERESPACIO	CAPACIDAD DE RESPUESTA
CIBERESPACIO	Correlación de Pearson	1	,513**
	Sig. (bilateral)		,004
	N	30	30
CAPACIDAD DE RESPUESTA	Correlación de Pearson	,513**	1
	Sig. (bilateral)	,004	
	N	30	30

Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).

La correlación de Pearson es de 0,513, lo que indica una correlación positiva moderada entre ambas variables, lo que sugiere que existe una relación positiva entre la Capacidad de Respuesta y el Ciberespacio. Es decir, cuando la Capacidad de Respuesta del Ejército del Perú (en cuanto a su capacidad para reaccionar ante incidentes o amenazas en el ciberespacio) aumenta, también aumenta la influencia o el control que se ejerce sobre el Ciberespacio. Aunque la correlación no es tan fuerte como la que observamos en el análisis con la Capacidad de Explotación, sigue siendo significativa y moderada.

El valor de 0,004 para la significación bilateral es menor que 0,01, lo que indica que la correlación es estadísticamente significativa al nivel del 99%. Como la significación es menor que 0,01, podemos afirmar con un alto nivel de confianza (99%) que la correlación observada entre Ciberespacio y Capacidad de Respuesta no es producto del azar. Por lo tanto, hay una relación significativa entre ambas variables en la población de estudio. Esto refuerza la validez de los resultados obtenidos y sugiere que la Capacidad de Respuesta tiene un impacto real sobre el Ciberespacio.

Variable Ciberespacio y D4 de VI Capacidad de Investigación Digital

Tabla 17

Correlaciones VD y D4 VI

		CIBERESPACIO	CAPACIDAD DE INVEST. DIGITAL
CIBERESPACIO	Correlación de Pearson	1	,804**
	Sig. (bilateral)		,000
	N	30	30
CAPACIDAD DE INVEST. DIGITAL	Correlación de Pearson	,804**	1
	Sig. (bilateral)	,000	
	N	30	30

Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).

La correlación de Pearson es de 0,804, lo que indica una correlación positiva fuerte entre ambas variables, lo que sugiere que hay una relación significativa y positiva entre la Capacidad de Investigación Digital y el Ciberespacio. Esto significa que a medida que mejora la Capacidad de Investigación Digital del Ejército del Perú (por ejemplo, en cuanto a habilidades para analizar datos, detectar amenazas o realizar investigaciones en el ciberespacio), también aumenta su influencia sobre el Ciberespacio.

El valor de 0,000 para la significación bilateral es menor que 0,01, lo que indica que la correlación es estadísticamente significativa al nivel del 99%. Por lo que podemos afirmar con un nivel de confianza del 99% que la correlación observada no es producto del azar. Esto nos permite concluir que la relación entre Ciberespacio y Capacidad de Investigación Digital es real y confiable.

4.2.1. Hipótesis general o principal

Regresión Lineal Simple: (VD: Ciberespacio VI: Capacidad de Ciberdefensa del Ejército del Perú)

Tabla 18

Variables entradas/eliminadas

Modelo	Variables entradas	Variables eliminadas	Método
1	Capacidad de Ciberdefensa en el Ejército del Perú		Introducir

Nota: a. Variable dependiente: CIBERESPACIO

b. Todas las variables solicitadas introducidas.

Tabla 19

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,908 [a]	,825	,819	1,191

Nota: a. Predictores: (Constante), CAPACIDAD DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ

Tabla 20

Anova[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig
1	Regresión	187,093	1	187,093	131,933	,000 [b]
	Residuo	39,707	28	1,418		
	Total	226,800	29			

Nota: a. Variable dependiente: CIBERESPACIO

b. Predictores: (Constante), CAPACIDAD DE CIBERDEFENSA DEL EP.

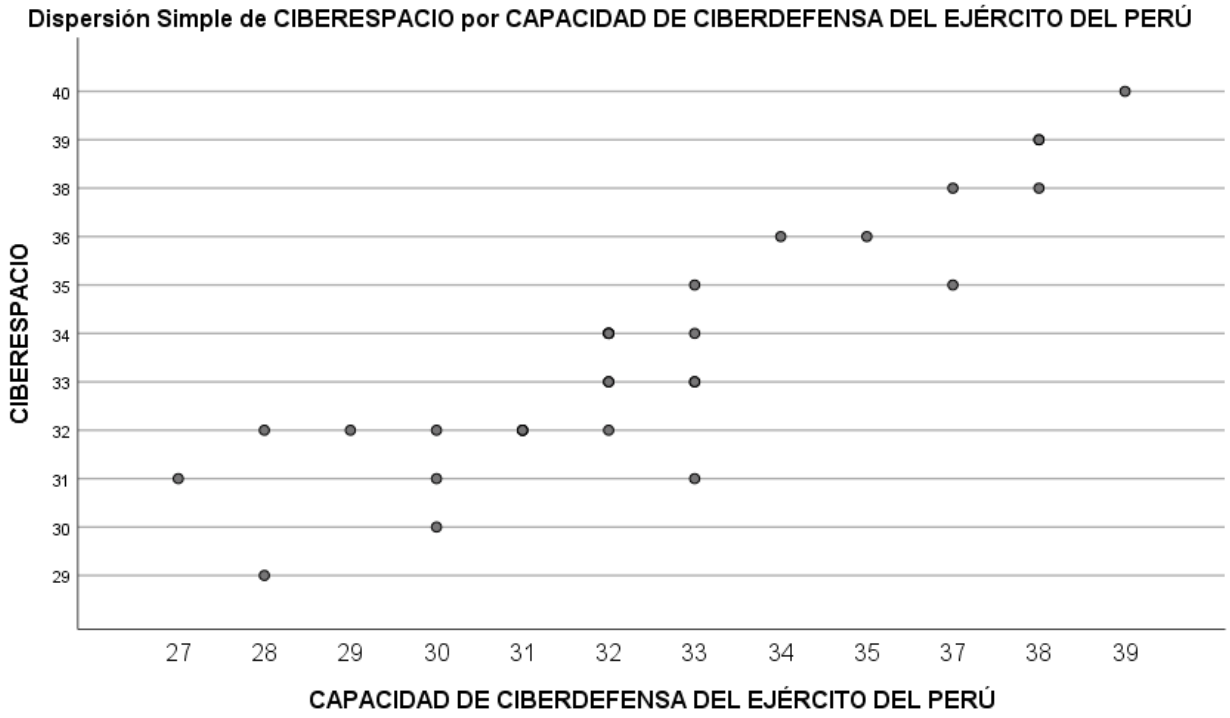
Tabla 21

Coeficiente[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig
		B	Desv. Error	Beta		
1	(Constante)	7,682	2,284		3,363	,002
	CAPACIDAD DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ	,800	,070	,908	11,486	,000

Nota: a.Variable dependiente: CIBERESPACIO

Figura 09



Interpretación:

El modelo de regresión muestra que la Capacidad de Ciberdefensa del Ejército del Perú tiene una relación fuerte y significativa con la influencia sobre el Ciberespacio. La Capacidad de Ciberdefensa explica el 82,5% de la variabilidad del Ciberespacio, lo cual es un excelente ajuste.

El valor F = 131,933 y el valor p = 0,000 indican que el modelo es altamente significativo, lo que refuerza la importancia de la Capacidad de Ciberdefensa en la

influencia sobre el Ciberespacio.

El coeficiente Beta de 0,908 indica que la Capacidad de Ciberdefensa tiene un gran impacto en el Ciberespacio, lo que valida tu hipótesis general de que la capacidad de ciberdefensa influye significativamente en el ciberespacio.

Este análisis apoya la hipótesis general de que la Capacidad de Ciberdefensa del Ejército del Perú tiene una influencia significativa en el Ciberespacio, y proporciona un fuerte respaldo empírico de la investigación.

4.2.2. Hipótesis especifica 1

Regresión Lineal Simple: (VD: Ciberespacio D1VI: Capacidad de Defensa)

Tabla 22

Variables entradas/eliminadas

Modelo	Variables entradas	Variables eliminadas	Método
1	Capacidad de Defensa		Introducir

Nota: a. Variable dependiente: CIBERESPACIO

b. Todas las variables solicitadas introducidas.

Tabla 23

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,207 [a]	,043	,009	2,785

Nota: a. Predictores: (Constante), CAPACIDAD DE DEFENSA

Tabla 24

Anova[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig
1	Regresión	9,694	1	9,694	1,250	,273 [b]
	Residuo	217,106	28	7,754		
	Total	226,800	29			

Nota: a. Variable dependiente: CIBERESPACIO

b. Predictores: (Constante), CAPACIDAD DE DEFENSA

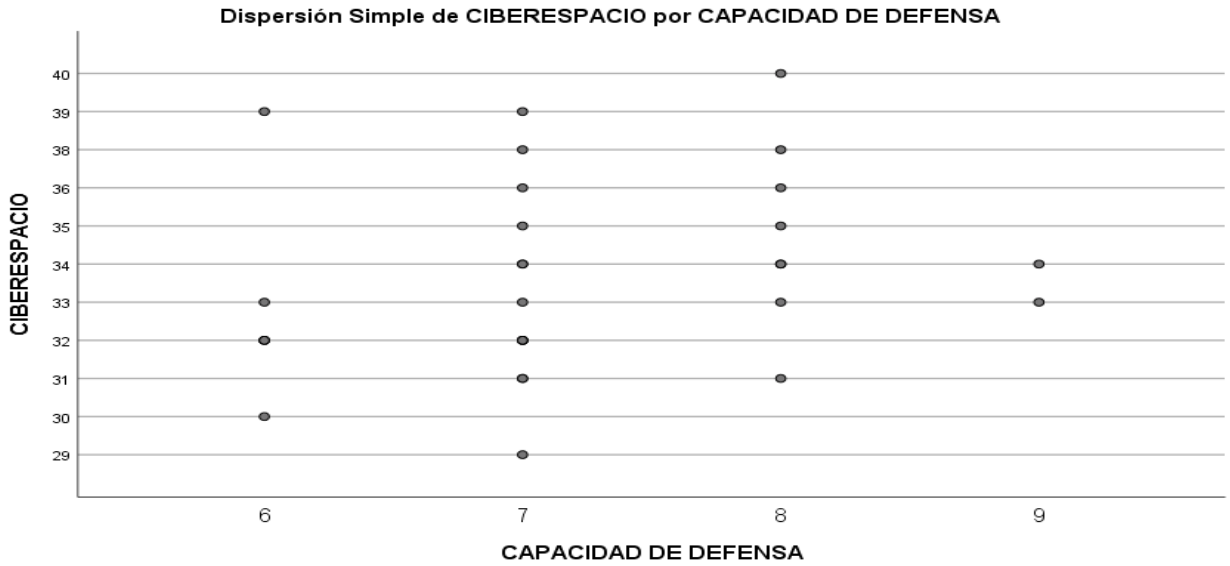
Tabla 25

Coeficiente[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig
		B	Desv. Error	Beta		
1	(Constante)	28,885	4,425		6,527	,000
	CAPACIDAD DE DEFENSA	,683	,611	,207	1,118	,273

Nota: Variable dependiente: CIBERESPACIO

Figura 10



Interpretación:

El modelo de regresión muestra que la Capacidad de Defensa tiene una relación débil y no significativa con la influencia sobre el Ciberespacio. El coeficiente de determinación ($R^2 = 0,043$) indica que la Capacidad de Defensa explica solo el 4,3% de la variabilidad del Ciberespacio, lo cual es un ajuste bastante pobre. Este bajo porcentaje de explicación sugiere que el modelo no es adecuado para predecir la influencia del Ciberespacio a partir de la Capacidad de Defensa.

El valor F = 1,250 y el valor p = 0,273 son indicadores de que el modelo no es estadísticamente significativo. Específicamente, el valor p superior a 0,05 confirma que la Capacidad de Defensa no tiene un impacto significativo en el Ciberespacio en este modelo.

El coeficiente Beta de 0,207 indica que la relación entre Capacidad de Defensa y Ciberespacio es positiva pero débil. Esto refuerza la conclusión de que, aunque hay una relación entre ambas variables, no es lo suficientemente fuerte como para validar una influencia significativa.

Este análisis no respalda la hipótesis específica 1 de que la Capacidad de Defensa influye significativamente sobre el Ciberespacio. Los resultados sugieren que existen otros factores no considerados en este modelo que podrían tener un impacto más relevante en la relación entre la Capacidad de Defensa y el Ciberespacio. Por lo tanto, se recomienda revisar otros elementos que puedan ser determinantes en este contexto, como aspectos de ciberseguridad, infraestructura tecnológica o políticas de defensa digital.

En resumen, la hipótesis específica 1 (que la Capacidad de Defensa influye significativamente en el Ciberespacio) no es respaldada por los datos de este modelo de regresión. Esto sugiere que se deben explorar otros factores o enfoques para entender mejor la relación entre estas dos variables.

4.2.3. Hipótesis especifica 2

Regresión Lineal Simple: (VD: Ciberespacio D2VI: Capacidad de Explotación)

Tabla 26

Variables entradas/eliminadas

Modelo	Variables entradas	Variables eliminadas	Método
1	Capacidad de Explotación		Introducir

Nota: a. Variable dependiente: CIBERESPACIO

b. Todas las variables solicitadas introducidas.

Tabla 27

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,540 [a]	,292	,267	2,395

Nota: Predictores: (Constante), CAPACIDAD DE EXPLOTACIÓN

Tabla 28

Anova[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	66,227	1	66,227	11,548	,002 [b]
	Residuo	160,573	28	5,735		
	Total	226,800	29			

Nota: a. Variable dependiente: CIBERESPACIO

b. Predictores: (Constante), CAPACIDAD DE EXPLOTACIÓN

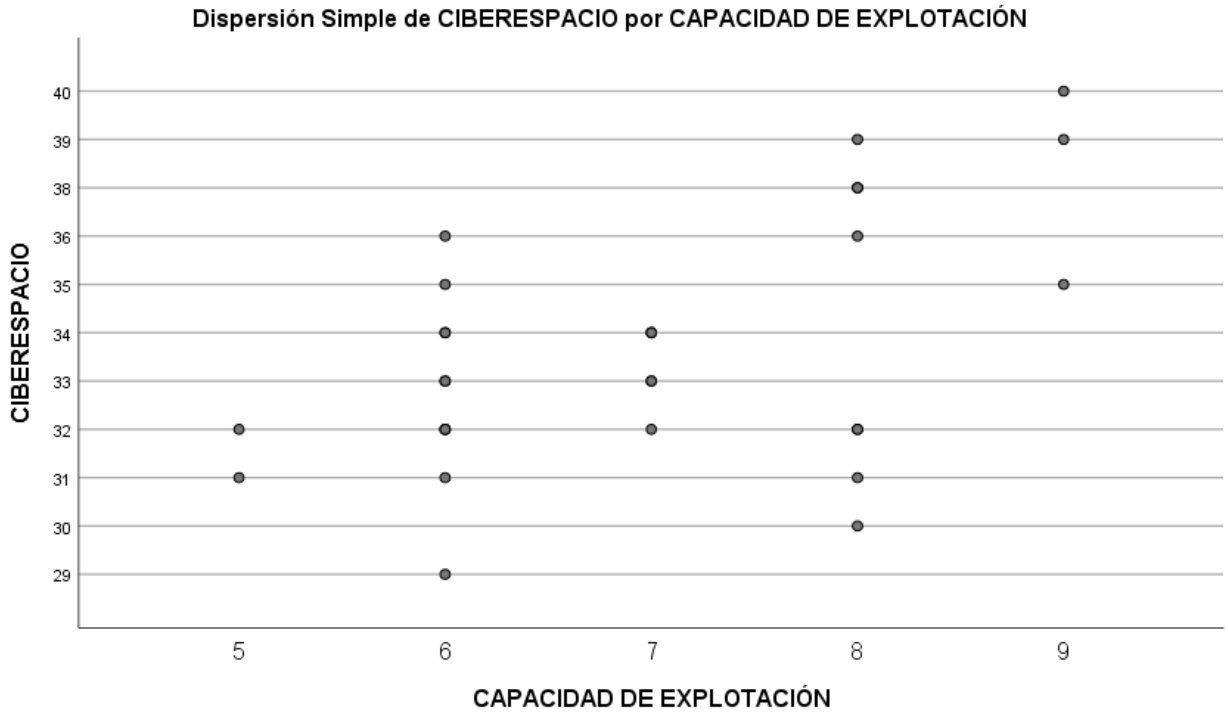
Tabla 29

Coeficiente[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig
		B	Desv. Error	Beta		
1	(Constante)	24,718	2,708		9,127	,000
	CAPACIDAD DE EXPLOTACIÓN	1,304	,384	,540	3,398	,003

Nota: Variable dependiente: CIBERESPACIO

Figura 11



Interpretación:

El modelo de regresión muestra que la Capacidad de Explotación tiene una relación moderada y significativa con la influencia sobre el Ciberespacio. La Capacidad de Explotación explica el 29,2% de la variabilidad del Ciberespacio, lo cual es un ajuste moderado pero significativo.

El valor F = 11,548 y el valor p = 0,002 indican que el modelo es estadísticamente significativo, lo que respalda la hipótesis de que la Capacidad de Explotación tiene un impacto significativo sobre el Ciberespacio.

El coeficiente Beta = 0,540 indica que la Capacidad de Explotación tiene una relación positiva y moderada con el Ciberespacio, lo que valida la hipótesis específica 2 de que la Capacidad de Explotación influye significativamente en el Ciberespacio.

Este análisis respalda la hipótesis específica 2 de que la Capacidad de Explotación tiene un impacto significativo en la influencia sobre el Ciberespacio, proporcionando un sólido respaldo empírico de la investigación.

4.2.4. Hipótesis especifica 3

Regresión Lineal Simple: (VD: Ciberespacio D3VI: Capacidad de Respuesta)

Tabla 30

Variables entradas/eliminadas

Modelo	Variables entradas	Variables eliminadas	Método
1	Capacidad de Respuesta		Introducir

Nota: a. Variable dependiente: CIBERESPACIO

b. Todas las variables solicitadas introducidas.

Tabla 31

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,513 [a]	,263	,237	2,443

Nota: Predictores: (Constante), CAPACIDAD DE RESPUESTA

Tabla 32

Anova[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	59,654	1	59,654	9,993	,004 [b]
	Residuo	167,146	28	5,970		
	Total	226,800	29			

Nota: a. Variable dependiente: CIBERESPACIO

b. Predictores: (Constante), CAPACIDAD DE RESPUESTA

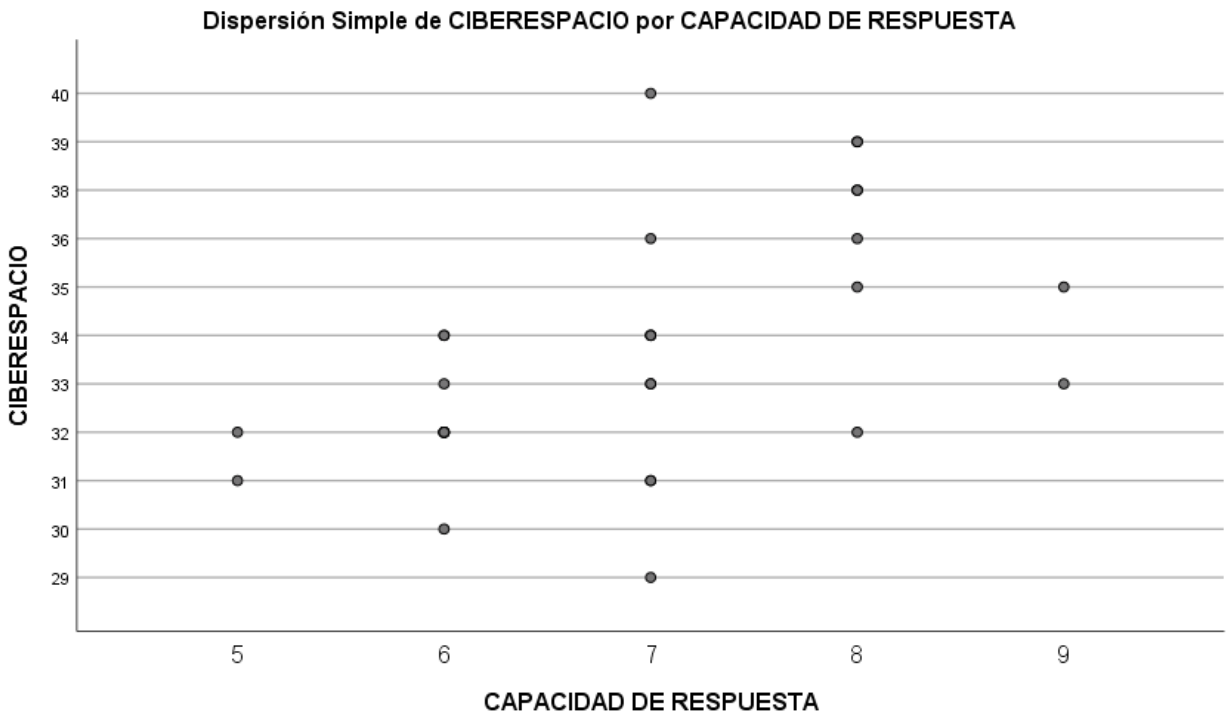
Tabla 33

Coeficiente[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig
		B	Desv. Error	Beta		
1	(Constante)	24,314	3,034		8,014	,000
	CAPACIDAD DE RESPUESTA	1,368	,433	,513	3,161	,004

Nota: Variable dependiente: CIBERESPACIO

Figura 12



Interpretación:

El modelo de regresión muestra que la Capacidad de Respuesta tiene una relación moderada y significativa con la influencia sobre el Ciberespacio. La Capacidad de Respuesta explica el 26,3% de la variabilidad del Ciberespacio, lo que es un ajuste aceptable.

El valor F = 9,993 y el valor p = 0,004 indican que el modelo es estadísticamente significativo, lo que refuerza la importancia de la Capacidad de Respuesta en la

influencia sobre el Ciberespacio.

El coeficiente Beta = 0,513 indica que la Capacidad de Respuesta tiene una relación moderada y positiva con el Ciberespacio, lo que valida la hipótesis específica 3 de que la Capacidad de Respuesta influye significativamente en el Ciberespacio.

Este análisis proporciona un respaldo empírico a la hipótesis específica 3, confirmando que la Capacidad de Respuesta tiene un impacto moderado pero significativo en el Ciberespacio, y refuerza la importancia de esta variable en el contexto de la Ciberdefensa.

4.2.5. Hipótesis especifica 4

Regresión Lineal Simple: (VD: Ciberespacio D3VI: Capacidad de Investigación Digital)

Tabla 34

Variables entradas/eliminadas

Modelo	Variables entradas	Variables eliminadas	Método
1	Capacidad de Invest. Digital		Introducir

Nota: a. Variable dependiente: CIBERESPACIO

b. Todas las variables solicitadas introducidas.

Tabla 35

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,804 [a]	,646	,633	1,694

Nota: Predictores: (Constante), CAPACIDAD DE INVESTIGACIÓN DIGITAL

Tabla 36

Anova[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	146,462	1	146,462	51,046	,000 [b]
	Residuo	80,338	28	2,869		
	Total	226,800	29			

Nota: a. Variable dependiente: CIBERESPACIO

b. Predictores: (Constante), CAPACIDAD DE INVESTIGACIÓN DIGITAL

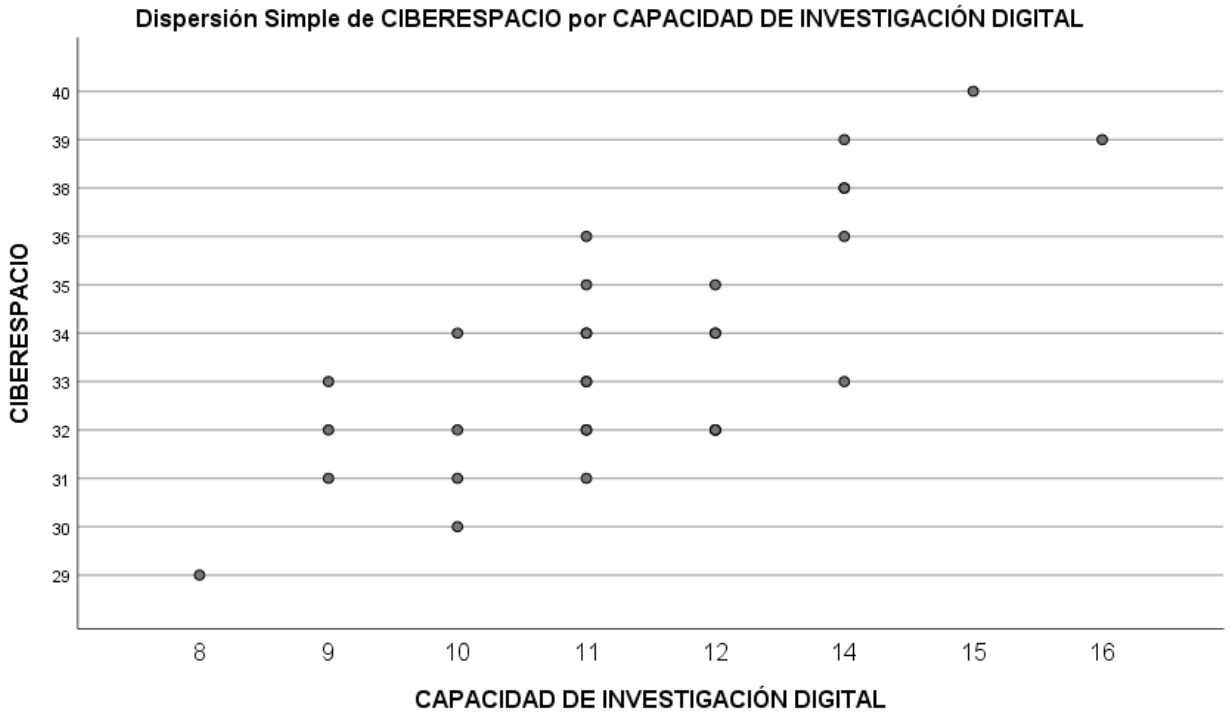
Tabla 37

Coeficiente[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig
		B	Desv. Error	Beta		
1	(Constante)	20,291	1,916		10,590	,000
	CAPACIDAD DE RESPUESTA	1,168	,163	,804	7,145	,000

Nota: Variable dependiente: CIBERESPACIO

Figura 13



Interpretación:

El modelo de regresión muestra que la Capacidad de Investigación Digital tiene una relación fuerte y significativa con la influencia sobre el Ciberespacio. La Capacidad de Investigación Digital explica el 64,6% de la variabilidad del Ciberespacio, lo que indica un excelente ajuste del modelo.

El valor F = 51,046 y el valor p = 0,000 indican que el modelo es altamente significativo, lo que resalta la relevancia de la Capacidad de Investigación Digital en la influencia sobre el Ciberespacio.

El coeficiente Beta = 0,804 demuestra que la Capacidad de Investigación Digital tiene un gran impacto sobre el Ciberespacio, lo que valida la hipótesis específica 4 de que la Capacidad de Investigación Digital influye significativamente en el Ciberespacio.

Este análisis proporciona un respaldo empírico fuerte a la hipótesis específica 4, destacando la Capacidad de Investigación Digital como un factor crucial en el Ciberespacio y subrayando su importancia en la ciberdefensa del Ejército del Perú.

Capítulo V: Discusión de resultados

El concepto de Ciberdefensa se puede entender a través de la teoría de redes de poder de Castells, que destaca cómo los actores interconectados (gobiernos, empresas, instituciones) deben colaborar de manera flexible y descentralizada para proteger el ciberespacio. Al igual que las redes digitales descritas por Castells, la Ciberdefensa debe ser un sistema interconectado y adaptable que responda rápidamente a las amenazas cibernéticas en tiempo real, manteniendo la resiliencia frente a la constante evolución de los ataques. Además, la Ciberdefensa no debe depender de un solo actor, sino que debe involucrar una cooperación interinstitucional entre diferentes nodos para fortalecer la seguridad. En este contexto, el ciberespacio es un territorio estratégico donde se libran batallas por la influencia y el control, lo que subraya la importancia de contar con una defensa sólida para proteger la soberanía digital, tal como indica el estudio que muestra que la capacidad de ciberdefensa influye significativamente en el estado del ciberespacio.

El análisis de los resultados obtenidos a través de la regresión lineal entre la Capacidad de Ciberdefensa y el Ciberespacio revela una relación estadísticamente significativa y robusta entre ambas variables. El coeficiente Beta de 0,908 indica que por cada unidad de cambio en la capacidad de ciberdefensa, se espera un cambio de 0,908 unidades en el ciberespacio, lo cual es una asociación muy fuerte. Este resultado es respaldado por el R^2 de 0,825, lo que sugiere que el 82,5% de la variabilidad del ciberespacio puede ser explicada por la capacidad de ciberdefensa, una proporción notablemente alta. Estos indicadores son claves para reafirmar que la capacidad de ciberdefensa tiene un impacto considerable sobre el ciberespacio y que las estrategias cibernéticas juegan un papel fundamental en la seguridad nacional.

El análisis se alinea con los estudios de autores como Rossi (2021) y Quevedo (2022), quienes han resaltado la creciente necesidad de fortalecer las capacidades cibernéticas en países como Perú para protegerse frente a amenazas cibernéticas emergentes. Estos autores coinciden en la importancia de mejorar las infraestructuras digitales y establecer marcos regulatorios sólidos para garantizar una defensa efectiva en un entorno global cada vez más dependiente de la tecnología digital. De manera similar, Huayapa (2022) y Quevedo (2022) coinciden en que las Fuerzas Armadas deben considerar a la ciberseguridad como un pilar central en su estrategia de defensa, dada la convergencia entre las amenazas tradicionales y las cibernéticas.

Los resultados de este estudio también confirman que la Capacidad de Ciberdefensa es un factor determinante para asegurar la protección del ciberespacio. Este hallazgo se vuelve aún más relevante cuando se considera que el ciberespacio no es solo una infraestructura tecnológica, sino un territorio estratégico en términos de soberanía nacional y geopolítica. En este sentido, las teorías geopolíticas de Friedrich Ratzel y Nicholas Spykman pueden ser útiles para entender cómo la expansión y control del ciberespacio se ha convertido en un nuevo frente de competencia global. Tal como Ratzel postuló en su concepto de espacio vital para los países, el control de las infraestructuras cibernéticas de una nación se ha convertido en una necesidad primordial para asegurar la soberanía digital.

Además, el ciberespacio ha evolucionado para convertirse en una arena clave en las dinámicas de poder internacionales. En este contexto, los nodos cibernéticos estratégicos, como los cables submarinos y otros puntos de conexión críticos, se han convertido en objetivos de interés geopolítico. La ciberdefensa, por lo tanto, no solo se trata de proteger infraestructuras locales, sino de fortalecer las capacidades globales para resistir a actores adversarios que intentan desestabilizar sistemas nacionales a través de ataques cibernéticos. Esta perspectiva se integra perfectamente con la visión de Spykman sobre el Rimland en el ciberespacio, donde las rutas de datos y conexiones actúan como nuevas fronteras geopolíticas.

Los resultados del análisis de regresión refuerzan la premisa de que la capacidad de ciberdefensa es un elemento clave en la seguridad nacional moderna y en la gestión del ciberespacio. A medida que el ciberespacio se convierte en un nuevo campo de batalla geopolítico, el fortalecimiento de las capacidades cibernéticas se vuelve esencial no solo para mitigar los riesgos de ciberamenazas, sino también para garantizar la soberanía digital y la seguridad nacional frente a actores hostiles.

En conclusión, la relación significativa entre la Capacidad de Ciberdefensa y el Ciberespacio sugiere que la inversión estratégica en ciberdefensa debe ser una prioridad para los países en el contexto actual de globalización digital. Esto no solo permitirá a las naciones proteger sus infraestructuras críticas, sino también mantener su competitividad geopolítica en un mundo cada vez más interconectado y vulnerable a los riesgos del ciberespacio.

Hipótesis Específica 1: Relación entre la Capacidad de Defensa y el Ciberespacio

Los resultados obtenidos para la relación entre la Capacidad de Defensa y el Ciberespacio muestran una correlación baja (0,207) y un valor p mayor a 0,05, lo que evidencia que no existe una relación estadísticamente significativa

entre ambas variables. Este hallazgo resulta relevante, ya que indica que la Capacidad de Defensa, entendida conforme al Reglamento de la Ley N.° 30999 como el conjunto de acciones orientadas a la prevención, protección y resiliencia de las plataformas tecnológicas y sistemas de información frente a amenazas cibernéticas, no está generando un impacto directo y medible sobre el ciberespacio en el contexto analizado.

La baja correlación observada sugiere que las medidas orientadas a la prevención, protección y resiliencia, si bien son necesarias, no resultan suficientes por sí solas para influir de manera significativa en la dinámica del ciberespacio. Ello evidencia que dichas acciones defensivas no están siendo articuladas de forma efectiva con otras capacidades operativas que permitan enfrentar amenazas cibernéticas complejas y en constante evolución, lo que limita su alcance frente a escenarios de riesgo digital cada vez más sofisticados.

Este resultado coincide con lo señalado por Quevedo (2022), quien advierte que en diversos países latinoamericanos, incluido el Perú, los enfoques de defensa han priorizado históricamente esquemas tradicionales de seguridad, relegando el desarrollo integral de capacidades específicas para el ciberespacio. El autor sostiene que, si bien las acciones de protección y prevención son indispensables, su efectividad se reduce cuando no se insertan dentro de una estrategia cibernética más amplia y articulada.

En este sentido, la Capacidad de Defensa, entendida estrictamente como la capacidad para prevenir, proteger y fortalecer la resiliencia frente a incidentes cibernéticos, requiere evolucionar en función de la creciente complejidad del entorno digital. La naturaleza dinámica del ciberespacio, caracterizada por amenazas persistentes, ataques coordinados y actores no estatales altamente especializados, demanda que dichas capacidades defensivas sean complementadas con mecanismos que permitan una actuación más integral frente a los riesgos emergentes.

La baja correlación observada también pone en evidencia limitaciones relacionadas con la inversión en tecnologías de ciberseguridad, la capacitación especializada en ciberdefensa y el fortalecimiento de infraestructuras digitales resilientes. Estas carencias reducen la efectividad de las acciones defensivas y

limitan su impacto real sobre el control y la seguridad del ciberespacio, aun cuando existan marcos normativos y doctrinarios que las respalden.

Asimismo, resulta necesario actualizar y fortalecer las doctrinas de defensa vigentes para incorporar la ciberdefensa como un componente estructural de la seguridad nacional. Tal como sostienen Huayapa (2022) y Rossi (2021), la ciberdefensa no debe ser concebida como un ámbito accesorio, sino como un eje estratégico que requiere coherencia doctrinal, capacidades operativas especializadas y una adecuada integración institucional.

En consecuencia, los resultados confirman que la Capacidad de Defensa, en los términos definidos por la Ley N.° 30999, constituye una condición necesaria pero no suficiente para influir de manera significativa en el ciberespacio, lo que evidencia la necesidad de fortalecer su articulación con capacidades de explotación, respuesta e investigación digital. Esta integración permitirá consolidar una ciberdefensa más dinámica, resiliente y acorde con las exigencias del entorno digital contemporáneo.

Hipótesis Específica 2: Relación entre la Capacidad de Explotación y el Ciberespacio

Los resultados obtenidos respecto a la Capacidad de Explotación, con una correlación moderada de 0,540 y un valor p de 0,002, destacan la relevancia de las actividades de búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciberamenazas dentro del contexto de la ciberdefensa. Esta capacidad refleja el proceso de detección y monitoreo continuo en el ciberespacio para reconocer amenazas emergentes y prevenir ataques cibernéticos antes de que ocurran. La Capacidad de Explotación incluye tanto medidas pasivas como activas, lo que implica un enfoque integral que abarca desde la observación pasiva de patrones de tráfico hasta la intervención activa para neutralizar amenazas.

Este hallazgo refuerza la idea de que la capacidad para detectar, identificar y rastrear ciberamenazas es esencial para una defensa efectiva. Como subraya Huayapa (2022), la habilidad para monitorear el ciberespacio y rastrear actividades sospechosas es crítica para prevenir los ataques antes de que causen daños significativos. La búsqueda y seguimiento de estas amenazas, a través de herramientas de análisis avanzadas y la inteligencia cibernética, no solo permite una intervención rápida, sino que también ayuda a las instituciones a comprender la naturaleza de los ataques y sus posibles orígenes.

Además, este resultado está alineado con las recomendaciones de Quevedo (2022) y Rossi (2021), quienes destacan la importancia de fortalecer las capacidades de inteligencia de amenazas y monitoreo de ciberespacio. El uso de tecnologías como la inteligencia artificial (IA) y machine learning para analizar grandes volúmenes de datos y detectar patrones anómalos puede mejorar considerablemente la capacidad de explotación, permitiendo la detección de ciberamenazas en fases tempranas. Estas tecnologías no solo permiten identificar amenazas conocidas, sino también prever y adaptarse ante nuevas técnicas de ataque, haciendo que las defensas sean más dinámicas y adaptativas.

En términos prácticos, la Capacidad de Explotación implica un enfoque integral que no solo se centra en la detección pasiva, sino también en la implementación de medidas activas que intervienen para mitigar y neutralizar amenazas identificadas. Las medidas activas incluyen el uso de herramientas de defensa de red como cortafuegos avanzados, sistemas de prevención de intrusiones (IPS) y técnicas de análisis forense que permiten no solo identificar la amenaza, sino también reconstruir el ataque para prevenir futuros incidentes similares.

Este enfoque también destaca la necesidad de contar con equipos especializados en ciberinteligencia y respuesta ante incidentes, que sean capaces de llevar a cabo operaciones de vigilancia y seguimiento de forma constante. El reconocimiento y vigilancia en tiempo real proporcionan una visión panorámica de las actividades cibernéticas que ocurren en las redes, lo que ayuda a detectar comportamientos inusuales y posibles indicadores de compromiso. Estos indicadores pueden ser utilizados para actuar de forma preventiva, antes de que se materialice un ataque.

La Capacidad de Explotación también subraya la importancia de la colaboración interinstitucional y la compartición de información en torno a las ciberamenazas. Las redes de inteligencia y las plataformas de colaboración cibernética juegan un papel crucial en la identificación rápida de nuevas amenazas y en el intercambio de mejores prácticas para su neutralización.

En conclusión, los resultados de la correlación moderada entre la Capacidad de Explotación y el Ciberespacio refuerzan la importancia de integrar tecnologías avanzadas de monitoreo y análisis en las estrategias de ciberdefensa. La capacidad para identificar, rastrear y seguir las ciberamenazas de manera efectiva es crucial para mejorar la prevención de ataques y la resiliencia del sistema. La combinación de medidas pasivas y activas permite una defensa más completa y adaptativa ante las amenazas cibernéticas, y representa un pilar fundamental para la seguridad nacional en

el ciberespacio.

Hipótesis Específica 3: Relación entre la Capacidad de Respuesta y el Ciberespacio

Los resultados obtenidos para la Capacidad de Respuesta, con una correlación moderada de 0,513 y un valor p de 0,004, subrayan la importancia crítica de la habilidad para neutralizar o mitigar las ciberamenazas. Aunque este hallazgo indica un impacto significativo de la Capacidad de Respuesta en el Ciberespacio, también revela que aún existen desafíos operativos que dificultan la implementación de respuestas rápidas y eficaces ante incidentes cibernéticos.

La Capacidad de Respuesta se refiere a la habilidad de actuar de manera rápida y eficiente frente a incidentes cibernéticos para contener y recuperar sistemas afectados, restaurando así las capacidades de operación lo más rápido posible. Esta capacidad se basa en la coordinación efectiva entre diferentes actores, el uso de herramientas avanzadas de mitigación de amenazas y la flexibilidad operativa para adaptarse a los distintos tipos de ataques. Sin embargo, la moderada correlación sugiere que, aunque las capacidades de respuesta están presentes, hay aspectos críticos que aún deben ser mejorados para garantizar una intervención más ágil y eficaz.

En este sentido, el hallazgo es consistente con las observaciones de Muñoz (2023), quien destaca que la respuesta frente a incidentes cibernéticos, aunque esencial, todavía enfrenta limitaciones operativas en muchos países. Uno de los principales retos es la integración de las fuerzas cibernéticas dentro de un sistema de defensa integral. La capacidad para responder a ciberincidentes de manera efectiva depende no solo de la disponibilidad de tecnologías adecuadas, sino también de una estructura organizativa sólida, la capacidad de colaboración interinstitucional y la formación continua de los equipos de respuesta ante incidentes.

Además, el reto de la capacidad de respuesta no se limita solo a la velocidad de intervención, sino también a la calidad de las acciones tomadas durante la mitigación de una amenaza. La respuesta activa requiere una comprensión clara de la naturaleza del ataque y de las estrategias de neutralización que deben aplicarse en cada caso. Sin una planificación anticipada y una estructura organizada para manejar los incidentes, las respuestas pueden ser incoherentes y, en algunos casos, pueden empeorar la situación.

Otro factor clave para mejorar la Capacidad de Respuesta es la integración de sistemas avanzados de inteligencia cibernética que permitan identificar y mitigar rápidamente amenazas nuevas y complejas, como las amenazas persistentes avanzadas (APT). Como lo mencionan varios expertos en ciberseguridad, la integración

de capacidades de detección automatizada y resolución de incidentes basadas en inteligencia artificial (IA) y machine learning puede acelerar significativamente la capacidad de respuesta ante ataques cibernéticos y mejorar la coordinación entre los distintos actores involucrados.

Además, la resiliencia organizacional juega un papel crucial en la Capacidad de Respuesta. En muchas ocasiones, los sistemas cibernéticos deben ser capaces de recuperarse rápidamente tras un ataque. La planificación de la recuperación ante desastres y la continuidad de negocio es clave, especialmente en infraestructuras críticas, donde la rapidez de la respuesta puede determinar la magnitud del daño causado. La gestión de crisis y los protocolos de respuesta rápida son aspectos fundamentales para mejorar esta capacidad.

En conclusión, los resultados de la correlación moderada de la Capacidad de Respuesta con el Ciberespacio refuerzan la idea de que, aunque existe una capacidad significativa para mitigar y neutralizar ciberamenazas, aún hay áreas que requieren una mejora sustancial, especialmente en términos de integración organizativa, coordinación interinstitucional y la aplicación de tecnologías avanzadas para la detección y respuesta ante incidentes. La Capacidad de Respuesta es un componente esencial para mantener la seguridad cibernética, pero su efectividad depende de la preparación continua, la adaptación de las fuerzas cibernéticas a nuevas amenazas, y la mejora constante de las infraestructuras y procedimientos de respuesta.

Hipótesis Específica 4: Relación entre la Capacidad de Investigación Digital y el Ciberespacio

Los resultados para la Capacidad de Investigación Digital, con una alta correlación de 0,804 y un valor p de 0,000, refuerzan de manera sólida la hipótesis de que las capacidades de investigación son esenciales para el control efectivo del ciberespacio. Esta correlación positiva y significativa indica que una capacidad robusta de investigación digital tiene un impacto directo y considerable sobre la capacidad de gestionar y proteger el ciberespacio de amenazas emergentes, mostrando que las capacidades de análisis forense y de investigación cibernética no solo son cruciales para responder a incidentes, sino también para prevenirlos de manera proactiva.

La Capacidad de Investigación Digital se refiere a la habilidad de investigar, analizar y rastrear ciberincidentes, utilizando herramientas forenses avanzadas y métodos de análisis para identificar y reducir los riesgos de ciberamenazas. Esta capacidad permite desentrañar la naturaleza de los ataques, determinar su origen, y desarrollar estrategias de defensa para proteger a las organizaciones o naciones de

futuras amenazas. Además, la capacidad de investigar ataques previos también brinda valiosos insights sobre vulnerabilidades y patrones de ataque, lo que ayuda a construir sistemas de defensa más sólidos y a anticipar ataques futuros.

Este hallazgo se alinea con los estudios de García y Herrero (2020), quienes subrayan la importancia de la capacitación del personal encargado de la investigación digital y la necesidad de contar con sistemas avanzados que respalden estas labores de análisis forense. La investigación digital no solo contribuye a responder a incidentes cibernéticos, sino que también permite a las organizaciones entender cómo y por qué un ataque fue exitoso, lo que se traduce en una mejora continua de las defensas cibernéticas.

Además, la Capacidad de Investigación Digital también juega un papel fundamental en la prevención de incidentes cibernéticos, ya que el análisis de ataques previos y la recopilación de inteligencia sobre ciberamenazas pueden ayudar a identificar tendencias emergentes en el ciberespacio y a adaptar las estrategias de defensa ante amenazas nuevas o evolucionadas. Los resultados refuerzan la necesidad de crear equipos especializados en ciberinteligencia y ciberinvestigación dentro de las organizaciones, equipados con las últimas herramientas digitales y entrenados en las mejores prácticas de análisis forense y respuesta a incidentes.

Este enfoque proactivo también es respaldado por el énfasis que ponen diversos estudios, como el de Huayapa (2022), en la importancia de contar con equipos bien capacitados y con infraestructuras adecuadas para llevar a cabo investigaciones exhaustivas y efectivas. La investigación digital no solo facilita una respuesta rápida y eficaz ante un ataque, sino que también permite a las organizaciones aprender de los incidentes previos para mejorar sus estrategias de prevención.

Además, una investigación digital de alta calidad contribuye al desarrollo de una cultura de ciberseguridad dentro de las instituciones, pues al identificar patrones y técnicas de los atacantes, se puede formar al personal y a los usuarios sobre las mejores prácticas para prevenir ataques y mejorar la resiliencia frente a futuras amenazas. La capacitación continua del personal y la mejora de las herramientas forenses disponibles son cruciales para garantizar que las investigaciones no solo sean reactivas, sino también proactivas en el sentido de identificar vulnerabilidades antes de que los atacantes las exploten.

En resumen, la alta correlación de la Capacidad de Investigación Digital con el Ciberespacio confirma que las capacidades de investigación y análisis forense son pilares esenciales no solo para contener los ataques cibernéticos, sino para prevenirlos a través de un enfoque continuo de mejora y adaptación a las amenazas emergentes.

Este hallazgo resalta la necesidad de un enfoque integral en el cual la capacitación, el uso de herramientas avanzadas y el análisis proactivo de ciberincidentes sean elementos clave para proteger el ciberespacio de futuras amenazas.

Finalmente, desde una perspectiva doctrinaria, los resultados obtenidos pueden interpretarse a la luz de los Factores de la Capacidad Militar establecidos para el ámbito de la defensa. En ese sentido, la influencia diferenciada de las capacidades analizadas sobre el ciberespacio no depende únicamente de su definición funcional, sino del grado de desarrollo e integración de factores como el equipamiento tecnológico, la organización institucional, el personal especializado, la infraestructura digital, la educación y capacitación en ciberdefensa, la logística de soporte, la doctrina vigente y los procesos de instrucción y entrenamiento. La evidencia empírica sugiere que aquellas capacidades que articulan de manera coherente estos factores, especialmente en los componentes tecnológico, humano y doctrinario, generan un mayor impacto sobre la dinámica del ciberespacio, mientras que las capacidades centradas predominantemente en enfoques normativos o preventivos constituyen condiciones necesarias pero insuficientes cuando no se integran sistémicamente con los demás factores de la capacidad militar.

Capítulo VI: Conclusiones y Recomendaciones

6.1. Conclusiones

Respecto al objetivo general, se puede concluir que la investigación revela que la capacidad de ciberdefensa del Ejército del Perú tiene una influencia significativa sobre el ciberespacio nacional en 2024, la que está respaldada por datos estadísticos sólidos. Esto sugiere que una mejora en las capacidades de ciberdefensa incrementa de manera considerable la seguridad y estabilidad del ciberespacio, protegiendo las infraestructuras digitales (protección de la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves) y asegurando la soberanía digital del país. Esta influencia es aún más relevante en el contexto geopolítico actual, donde el ciberespacio se ha convertido en un territorio estratégico clave para la competencia global, tal como lo plantean las teorías geopolíticas de Ratzel y Spykman. Los hallazgos subrayan la necesidad de fortalecer la ciberdefensa no solo en términos nacionales, sino también a nivel internacional, ya que los nodos cibernéticos estratégicos son cada vez más objetivos de interés geopolítico. En este sentido, el Ejército del Perú debe continuar invirtiendo en ciberdefensa, no solo para proteger sus infraestructuras, sino también para mantener su competitividad y resiliencia frente a actores hostiles que buscan desestabilizar el ciberespacio nacional. Por lo tanto, las políticas y estrategias cibernéticas deben ser una prioridad estratégica para el país, garantizando una defensa robusta que resista las crecientes amenazas cibernéticas en un entorno digital globalizado.

Del primer objetivo específico se puede concluir que la capacidad de defensa del Ejército del Perú no ejerce una influencia estadísticamente significativa sobre el ciberespacio, como lo evidencia la baja correlación observada (0,207) y el valor p mayor a 0,05, lo que confirma la ausencia de una relación directa y significativa entre ambas variables. Este resultado demuestra que la Capacidad de Defensa, entendida conforme al marco normativo vigente como el conjunto de acciones orientadas a la prevención, protección y resiliencia de las plataformas tecnológicas y sistemas de información, no genera por sí sola un impacto medible sobre la dinámica del ciberespacio. El hallazgo pone de manifiesto la necesidad de reorientar las estrategias de defensa incorporando al ciberespacio como un dominio prioritario dentro de las doctrinas de seguridad y defensa. Asimismo, las brechas en la integración de la ciberseguridad, la capacitación especializada y el desarrollo de infraestructuras resilientes incrementan la vulnerabilidad de las infraestructuras críticas frente a ciberamenazas. En consecuencia, se concluye que la Capacidad de Defensa constituye una condición necesaria pero insuficiente,

siendo indispensable su articulación con las capacidades de explotación, respuesta e investigación digital para consolidar una ciberdefensa integral frente a los riesgos presentes y futuros.

En relación con el segundo objetivo específico, se determina que la capacidad de explotación del Ejército del Perú ejerce una influencia significativa sobre el ciberespacio, sustentada en una correlación moderada (0,540) y un valor p de 0,002. Este hallazgo confirma que las actividades de búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciberamenazas son componentes clave para la gestión y protección del ciberespacio nacional, al permitir la detección anticipada de amenazas y fortalecer la toma de decisiones estratégicas en ciberdefensa. No obstante, la magnitud moderada de la correlación revela limitaciones relacionadas con la integración de tecnologías avanzadas, la interoperabilidad de los sistemas de monitoreo y la especialización del personal en ciberinteligencia. En consecuencia, el fortalecimiento de esta capacidad resulta esencial para consolidar una defensa cibernética proactiva y dinámica, siendo prioritario invertir en inteligencia cibernética, vigilancia continua y capacitación especializada para incrementar la resiliencia del ciberespacio y proteger la soberanía digital del país.

En cuanto al tercer objetivo específico, se determina que la capacidad de respuesta del Ejército del Perú influye significativamente en el ciberespacio, evidenciado por una correlación moderada de 0,513 y el valor p de 0,004. Esto confirma que la habilidad para neutralizar y mitigar ciberamenazas es un componente clave en la defensa cibernética nacional. No obstante, también se evidencian áreas críticas que requieren mejora, especialmente en términos de la velocidad de respuesta, la calidad de las intervenciones y la integración de sistemas de inteligencia cibernética avanzados. A pesar de los esfuerzos, persisten limitaciones operativas relacionadas con la coordinación interinstitucional, la formación continua de equipos especializados y la adopción de tecnologías emergentes. La capacidad de respuesta es esencial para proteger las infraestructuras críticas, pero su efectividad dependerá de una mayor preparación, adaptación a nuevas amenazas y una mejora constante en la infraestructura y los protocolos de respuesta ante incidentes. La mejora de estas áreas fortalecerá la resiliencia del Ejército del Perú frente a los riesgos cibernéticos, asegurando una defensa más robusta en el ciberespacio en 2024 y más allá.

En relación con el cuarto objetivo específico, se establece que la capacidad de investigación digital del Ejército del Perú presenta una influencia significativa y directa en el ciberespacio, lo cual se evidencia en la alta correlación obtenida (0,804) y el valor p de 0,000 demuestran que las capacidades de análisis forense y de investigación

cibernética son fundamentales para la gestión y protección del ciberespacio frente a amenazas emergentes, no solo en la respuesta a incidentes cibernéticos, sino también para prevenirlos de manera proactiva, mediante la identificación de patrones y vulnerabilidades que pueden anticipar futuros ataques. La investigación digital, a través de herramientas avanzadas y técnicas de análisis forense, permite desentrañar la naturaleza de los ataques y mejorar las defensas cibernéticas, proporcionando información crucial sobre el origen y las características de las amenazas. Además, este enfoque proactivo contribuye al desarrollo de una cultura de ciberseguridad dentro de las instituciones, mejorando la resiliencia frente a ciberamenazas. En este sentido, es fundamental fortalecer la capacitación del personal y proporcionar las infraestructuras necesarias para llevar a cabo investigaciones exhaustivas y efectivas, lo que asegura no solo una respuesta rápida ante incidentes, sino también una prevención continua de posibles ciberataques. En resumen, la Capacidad de Investigación Digital constituye un pilar clave en la defensa del ciberespacio, permitiendo una protección más efectiva y adaptativa ante las amenazas cibernéticas.

6.2. Recomendaciones

Dado el impacto significativo de la ciberdefensa en la seguridad del ciberespacio nacional y la protección de la soberanía digital, se recomienda que el Ejército del Perú priorice la inversión y el fortalecimiento de la capacidad de ciberdefensa, por lo que es crucial mejorar la coordinación interinstitucional, promoviendo la cooperación tanto a nivel nacional como internacional, y fortalecer la capacitación continua de los equipos especializados. Esto garantizará una respuesta ágil y efectiva ante amenazas emergentes, permitiendo a Perú fortalecer su posición geopolítica y asegurar la estabilidad de su ciberespacio, protegiendo sus activos críticos y recursos clave en un entorno digital cada vez más complejo.

Se recomienda que el Ejército del Perú reoriente y actualice su enfoque doctrinario de la Capacidad de Defensa, incorporando explícitamente al ciberespacio como un dominio operativo prioritario dentro de la seguridad y defensa nacional. En ese sentido, la Capacidad de Defensa, centrada actualmente en acciones de prevención, protección y resiliencia normativa, debe articularse de manera sistémica con las capacidades de explotación, respuesta e investigación digital, a fin de generar un impacto efectivo sobre la dinámica del ciberespacio. Asimismo, resulta necesario cerrar las brechas identificadas mediante el fortalecimiento de la capacitación especializada en ciberseguridad, la inversión en infraestructuras digitales resilientes y la integración

operativa de la ciberdefensa dentro de las doctrinas militares vigentes, con el objetivo de reducir la vulnerabilidad de las infraestructuras críticas frente a ciberamenazas presentes y futuras.

Se recomienda que el Ejército del Perú fortalezca de manera prioritaria la Capacidad de Explotación, orientando sus esfuerzos al desarrollo e integración de tecnologías avanzadas de monitoreo, análisis y vigilancia del ciberespacio, así como a la mejora de la interoperabilidad entre los sistemas de detección de ciberamenazas. Asimismo, resulta indispensable potenciar la especialización del personal en ciberinteligencia, mediante programas de capacitación continua y formación especializada, a fin de optimizar las actividades de búsqueda, identificación, reconocimiento y seguimiento de amenazas. El fortalecimiento de esta capacidad permitirá consolidar una ciberdefensa proactiva, incrementando la resiliencia del ciberespacio nacional y contribuyendo a la protección efectiva de la soberanía digital del país.

Resulta necesario que el Ejército del Perú fortalezca la Capacidad de Respuesta ante ciberincidentes, priorizando la optimización de los tiempos de reacción, la mejora de la calidad de las intervenciones y la integración de sistemas avanzados de inteligencia cibernética para la gestión de incidentes. Asimismo, resulta fundamental reforzar la coordinación interinstitucional, estandarizar y actualizar los protocolos de respuesta, e impulsar la formación continua de equipos especializados, con énfasis en escenarios de amenazas complejas y emergentes. Estas acciones permitirán incrementar la eficacia operativa de la respuesta cibernética, fortalecer la resiliencia de las infraestructuras críticas y consolidar una defensa cibernética más robusta y adaptativa frente a los riesgos presentes y futuros.

Es crucial fortalecer la capacidad de investigación digital del Ejército del Perú mediante la formación de equipos especializados en análisis forense digital y el uso de herramientas avanzadas para la recolección y preservación de evidencias. Estos equipos deben ser entrenados en ingeniería inversa para identificar patrones de ataque y anticipar futuros incidentes, promoviendo una cultura organizacional enfocada en la prevención proactiva de ciberamenazas. Además, es fundamental fomentar la colaboración entre las instituciones clave, garantizando una respuesta integral y eficiente ante incidentes cibernéticos. La integración de estos equipos permitirá desarrollar estrategias de defensa más robustas, mejorando la resiliencia y la protección del ciberespacio nacional.

Se recomienda que futuras investigaciones profundicen en el análisis del impacto de los Factores de la Capacidad Militar sobre el fortalecimiento de la ciberdefensa,

considerando de manera integral el equipamiento tecnológico, la organización institucional, el personal especializado, la infraestructura digital, la educación y capacitación en ciberdefensa, la logística de soporte, la doctrina vigente y los procesos de instrucción y entrenamiento. En particular, resulta pertinente evaluar cómo el nivel de desarrollo, articulación e integración de estos factores incide en la eficacia de las capacidades de defensa, explotación, respuesta e investigación digital frente a ciberamenazas. Asimismo, futuros estudios podrían analizar comparativamente qué factores generan mayor influencia en la protección del ciberespacio, a fin de orientar la toma de decisiones estratégicas, la asignación de recursos y el diseño de políticas de ciberdefensa más coherentes y sostenibles en el ámbito militar.

Referencias

Aiken, L. (1980). Content validity and reliability of single items or questionnaires. Educational and Psychological Measurement, 40, 955–959. https://doi.org/10.1177/001316448004000419

Bernal-García, M., Salamanca, D., Pérez, N. y Quemba, M. (2018). Validez de contenido por juicio de expertos de un instrumento para medir percepciones físico-emocionales en la práctica de disección anatómica. Educación Médica, 21(6), 349-356. https://doi.org/10.1016/j.edumed.2018.08.008

Castells, M. (2005). La Era de la Información: economía, sociedad y cultura. Volumen 1, La Sociedad Red. México: Siglo XXI.

Castells, M. (2011). “Introducción al Taller: La Promesa de la Teoría de Redes Universidad del Sur de California”. Revista Internacional de Comunicación 5, págs. 794–795. Disponible en http://ijoc.org/index.php/ijoc/article/view/1104/555

Castells, M (2001) La ciudad de la nueva economía. Disponible en: http://www.lafactoriaweb.com/default2.htm

Castillo, E., (18 de noviembre de 2021). Política Sectorial de Ciberdefensa: una necesidad impostergable. CEEEP. https://ceeep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/

Chivilches, F. (2023) Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú. (Tesis para obtener el título de maestría en Estrategia Marítima) Escuela Superior de Guerra Naval. https://repositorio.esup.edu.pe/handle/20.500.12927/335

De Vergara, E., (2009). Las diferencias conceptuales entre seguridad y defensa. Argentina: Instituto de Estudios Estratégicos de Buenos Aires.

Escuela Superior de Guerra del Ejército (2023). Guía metodológica para la elaboración de trabajos de investigación (2023-2025). ESGE-EPG. https://esge.edu.pe/wp-content/uploads/2023/05/3.-GUIA-METODOLOGICA-PARA-ELABORACION-DE-TRABAJOS-DE-INVEST.-2023-2025.pdf

Friederich Ratzel: “Anthropogeography” 2° ed. (Stuttgart, J. Engelhorn, 1899), parte I, p.2; ver Kirstof, op. cit., p 22.

García, J., y Herrero, L. (2020). La ciberdefensa en los sistemas de información sanitarios militares. Sanidad Militar. Scielo https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140&lang=es

Huayapa, D. (2022). Aportes para la política exterior peruana en materia de amenazas híbridas en el ciberespacio (Tesis para Obtener el grado de Maestro en

Diplomacia y Relaciones Internacionales). Academia Diplomática Del Perú Javier Pérez De Cuéllar. http://repositorio.adp.edu.pe/bitstream/handle/ADP/209/2022%20Tesis%20Huapaya%20Noriega%2c%20Daniel.pdf?sequence=3&isAllowed=y

Landis, J. y Koch, G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33(1). 159-174. https://doi.org/10.2307/2529310

Ley N° 30999. (09 de agosto de 2019). Ley de Ciberdefensa. Lima, Lima, Perú: Normas Legales.

Martínez, J. (17 de abril de 2018). EEUU y Reino Unido denuncian una campaña de ciberespionaje mundial dirigida por Rusia. El País. https://elpais.com/internacional/2018/04/17/estados_unidos/1523982825_454866.html

Mogollón, F. (2021). La adaptación asimétrica de las doctrinas de Defensa en torno al ciberespacio: los casos de Chile y Ecuador (2014 -2018) (Tesis para obtener el título de maestría de investigación en Relaciones Internacionales con mención en Seguridad y Derechos Humanos). FLACSO- Ecuador. https://repositorio.flacsoandes.edu.ec/bitstream/10469/17358/2/TFLACSO-2021FSMF.pdf

Muñoz, B. (2023). La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033 (Tesis para obtener la Maestría en Defensa y Seguridad mención en Conducción Militar). ESPE-Universidad de las fuerzas armadas. https://repositorio.espe.edu.ec/bitstream/21000/37424/1/T-ESPE-058471.pdf

Nagurney, A. & Shukla, S. (2017). Multiform models of cybersecurity investment competition vs. cooperation and network vulnerability. European Journal of Operational Research. https://doi.org/10.1016/j.ejor.2016.12.034

Nicholas J. Spykman y Abbie A. Rollins: “Geographic Objectives in Goreign Policy I”, American Political Science Review, XXXIII (junio de 1939), pp. 391-393.

Niklas Luhmann’s. (2008) La teoría de sistemas de Niklas Luhmann. https://www.uma.es/contrastes/pdfs/015/contrastesxv-16.pdf

Organización de las Naciones Unidas. Influencia de las Tecnologías Digitales. https://ceeep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidadimpostergable/#:~:text=En%20el%20Per%C3%BA%2C%20la%20Ley,estos%20afecten%20la%20Seguridad%20Nacional.

Quevedo, Ch. (17 de febrero de 2023). Ciberdefensa y Ciberseguridad en el Perú: Realidad y retos en torno a la capacidad de las Fuerzas Armadas para neutralizar ciberataques que atenten contra la seguridad nacional. Revista de

Ciencia e Investigación en Defensa – CAEN. https://doi.org/10.58211/recide.v4i1.99

Rivadeneira G. (2019). Ecuador ha recibido 40 millones de ataques cibernéticos. El universo. Disponible en: https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuadorha-recibido-40-millones-ataques-ciberneticos-revela

Rossi, G. (2021). La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas [Tesis de Maestría, Academia Diplomática del Perú Javier Pérez de Cuéllar]. Renati.

Santos, M. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento Respuestas del Estado ecuatoriano en el período 2013-2022 [Tesis de Maestría, Universidad Andina Simón Bolívar]. La Referencia.

Semanate, A., y Lenin, L., (2023). El Estado y la Defensa del Ciberespacio. Academia de Guerra del Ejército Ecuatoriano. https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.07

Soto, C. y Livia, J. (2009). Intervalos de confianza asimétricos para el índice la validez de contenido: Un programa Visual Basic para la V de Aiken. Anales de Psicología, 25(1), 169-171. https://revistas.um.es/analesps/article/view/71631

Urtasun, M. (2021) Cibersecuritización: un análisis de discurso, instituciones y documentos oficiales para los casos de Estonia y Reino Unido (Tesis para obtener el título de licenciado en Ciencia Política y Relaciones Internacionales) Universidad de San Andrés https://repositorio.udesa.edu.ar/jspui/handle/10908/19000

Vargas, R., Recalde, L., y Reyes, R. (20 de junio de 2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. Revista Latinoamericana de Estudios de Seguridad. http://dx.doi.org/10.17141/urvio.20.2017.2571

Villón, M. (2024) "Seguridad Nacional, Relaciones Internacionales y Bienestar Social en la Era Digital": Revista Seguridad y Poder Terrestre,3(1)https://ceeep.mil.pe/2024/05/16/seguridad-nacional-relaciones-internacionales-y-bienestar-social-en-la-era-digital/

ANEXOS

ANEXO 1

MATRIZ DE CONSISTENCIA

MODELO DE MATRIZ DE CONSISTENCIA (CUANTITATIVA)

Título: La capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio, 2024

Preguntas de investigación	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores	Metodología
Problema general: ¿Cuál es la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio, 2024? **Problemas específicos:** ¿Cuál es la influencia de la capacidad de defensa del Ejército del Perú en el ciberespacio, 2024? ¿Cuál es la influencia de la capacidad de explotación del Ejército del Perú en el ciberespacio, 2024? ¿Cuál es la influencia de la capacidad de respuesta del Ejército del	**Objetivo general:** Determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio, 2024. **Objetivos específicos:** Determinar la influencia de la capacidad de defensa del Ejército del Perú en el ciberespacio, 2024. Determinar la influencia de la capacidad de explotación del Ejército del Perú en el	**Hipótesis General:** La capacidad de ciberdefensa del Ejército del Perú influye significativamente en el ciberespacio, 2024. **Hipótesis específicas:** La capacidad de defensa del Ejército del Perú influye significativamente en el ciberespacio, 2024. La capacidad de explotación del Ejército del Perú influye significativamente en el ciberespacio, 2024.	**Variable 1:** La capacidad de ciberdefensa del Ejército del Perú **Variable 2:** Ciberespacio	X1Capacidad de defensa X2 Capacidad de explotación X3 Capacidad de respuesta X4 Capacidad de investigación digital Y1 Redes interconectadas e interdependientes de infraestructura de tecnología de la información Y2 Redes interconectadas e interdependientes de infraestructura de datos	•Eficiencia en la prevención de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. •Eficiencia en la prevención de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas. •Eficiencia en la protección de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. •Eficiencia en la protección de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas. •Eficiencia en la resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, recurriendo a medidas pasivas y activas. •Eficiencia en la resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante actos hostiles u otros incidentes de seguridad digital; recurriendo a	**Enfoque:** Cuantitativa **Tipo:** Básica **Nivel:** Explicativo **Diseño de investigación:** No experimental y transversal

Perú en el ciberespacio, 2024? ¿Cuál es la influencia de la capacidad de investigación digital del Ejército del Perú en el ciberespacio, 2024?	ciberespacio, 2024. Determinar la influencia de la capacidad de respuesta del Ejército del Perú en el ciberespacio, 2024. Determinar la influencia de la capacidad de investigación digital del Ejército del Perú en el ciberespacio, 2024.	La capacidad de respuesta del Ejército del Perú influye significativamente en el ciberespacio, 2024. La capacidad de investigación digital del Ejército del Perú influye significativamente en el ciberespacio, 2024.		almacenados	medidas pasivas y activas. •Eficiencia en la búsqueda de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. •Eficiencia en la identificación de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. •Eficiencia en el reconocimiento de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. •Eficiencia en la vigilancia de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas. •Eficiencia en el empleo del Internet a través de las Redes interconectadas e interdependientes de infraestructura de tecnología de la información. •Eficiencia de las Redes de telecomunicaciones. •Eficiencia de los Sistemas informáticos en el Cecyber •Eficiencia de los procesadores en las Redes interconectadas e interdependientes de infraestructura de tecnología de la información •Eficiencia de los controladores integrados de las Redes interconectadas e interdependientes de infraestructura de datos almacenados. •Eficiencia de los usuarios Redes interconectadas e interdependientes de infraestructura de datos almacenados.	

ANEXO 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO DEL PERÚ
MAESTRÍA DE ESTRATEGIA Y GEOPOLÍTICA

INTRODUCCIÓN

Buenos días (tardes),
Estamos trabajando en el estudio que servirá para elaborar una tesis de maestría en Estrategia y Geopolítica del PAME de la ESGE-EPG acerca de: “La capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio, 2024”.
El objetivo de este cuestionario tradicional es determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio en el año 2024. La encuesta está diseñada para evaluar diferentes aspectos de la ciberdefensa, incluyendo la capacidad de defensa, explotación, respuesta e investigación digital, y cómo estos afectan la eficiencia y efectividad en el ciberespacio.

INSTRUCCIONES

1. La encuesta es autoadministrada, además, los participantes deben completar el cuestionario de forma individual.
2. Emplee un bolígrafo de tinta para responder el cuestionario.
3. Todas las respuestas serán tratadas de manera confidencial y se utilizarán únicamente para fines de investigación. Su identidad no será revelada.
4. El cuestionario cuenta con 16 preguntas. La encuesta puede tardar aproximadamente veinte (20) minutos en completarse.
5. Responda las siguientes preguntas marcando la opción que mejor describa la situación o que se ajuste a la realidad. En algunas preguntas, puede marcar solo una respuesta, mientras que en otras puede seleccionar varias respuestas si considera que son aplicables.
6. Si no puede contestar una pregunta o si la pregunta no tiene sentido para usted, por favor pregúntele a la persona que le entregó este cuestionario y le explicará.

De antemano, ¡MUCHAS GRACIAS POR SU COLABORACIÓN!

Sección 1: Capacidad de Defensa

1. **¿Qué medidas pasivas se implementan para prevenir amenazas cibernéticas en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. Mantenimiento regular de sistemas y actualizaciones de seguridad
    b. Establecimiento de políticas y procedimientos de seguridad
    c. Monitoreo continuo de redes y sistemas
    d. Capacitación en ciberdefensa
    e. Ninguna de las anteriores

2. **¿Qué medidas activas se aplican para proteger las plataformas tecnológicas del Ejército del Perú contra amenazas cibernéticas?** *(Puede seleccionar más de una opción)*

    a. Análisis proactivo de vulnerabilidades
    b. Evaluación y respuesta a amenazas emergentes
    c. Acciones cibernéticas para neutralizar amenazas
    d. Implementación de contramedidas de seguridad
    e. Ninguna de las anteriores

3. **¿Cómo se asegura la resiliencia de los sistemas de información del Ejército del Perú frente a incidentes de seguridad digital?** *(Puede seleccionar más de una opción)*

    a. Implementación de redundancias y copias de seguridad
    b. Realización de pruebas de recuperación ante desastres
    c. Evaluación continua de riesgos y vulnerabilidades
    d. Establecimiento de planes de continuidad operativa
    e. No se realizan medidas específicas

Sección 2: Capacidad de Explotación

4. **¿Qué herramientas utiliza el Ejército del Perú para buscar y reconocer ciberamenazas?** *(Puede seleccionar más de una opción)*

    a. Herramientas de análisis de tráfico de red
    b. Sistemas de inteligencia de amenazas
    c. Plataformas de monitoreo de eventos de seguridad
    d. Herramientas de análisis forense
    e. Ninguna de las anteriores

5. **¿Cómo se lleva a cabo la identificación de amenazas en el ciberespacio?** *(Puede seleccionar más de una opción)*

    a. Revisión manual de registros
    b. Uso de sistemas automatizados de detección
    c. Análisis de patrones de comportamiento

d. Investigación de inteligencia de amenazas
e. No se realiza identificación sistemática

6. **¿Qué métodos se utilizan para la vigilancia continua de ciberamenazas?** *(Puede seleccionar más de una opción)*

    a. Vigilancia manual por personal especializado
    b. Herramientas automatizadas de monitoreo
    c. Análisis en tiempo real de eventos y tráfico
    d. Evaluaciones periódicas de amenazas
    e. Ninguna de las anteriores

Sección 3: Capacidad de Respuesta

7. **¿Qué procedimientos se siguen para responder a incidentes de ciberseguridad en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. Procedimientos básicos de notificación
    b. Planes detallados con roles y responsabilidades
    c. Respuesta automatizada a incidentes
    d. Simulacros y ejercicios de respuesta
    e. No existen procedimientos formales

8. **¿Cómo se realiza la recuperación de sistemas después de un incidente de ciberseguridad?** *(Puede seleccionar más de una opción)*

    a. Restauración desde copias de seguridad
    b. Uso de herramientas automatizadas de recuperación
    c. Implementación de planes de continuidad
    d. Evaluación y ajuste post-incidente
    e. No se siguen procedimientos específicos

9. **¿Qué tipo de formación recibe el personal en la gestión de incidentes de ciberseguridad?** *(Puede seleccionar más de una opción)*

    a. Capacitación básica
    b. Entrenamiento en procedimientos específicos
    c. Simulacros regulares
    d. Formación avanzada en gestión de incidentes
    e. No se proporciona formación específica

Sección 4: Capacidad de Investigación Digital

10. **¿Qué métodos se emplean para el análisis de evidencia digital en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

a. Análisis manual de datos
b. Herramientas forenses digitales
c. Técnicas de ingeniería inversa
d. Evaluación de origen e impacto
e. Ninguna de las anteriores

11. **¿Cómo se realiza la recolección y preservación de evidencias digitales?** *(Puede seleccionar más de una opción)*

    a. Procedimientos manuales
    b. Uso de herramientas automatizadas
    c. Técnicas avanzadas de preservación
    d. Evaluación post-incidente
    e. No se realizan procesos específicos

12. **¿Qué técnicas se aplican para analizar incidentes maliciosos en el ciberespacio?** *(Puede seleccionar más de una opción)*

    a. Análisis forense digital
    b. Evaluación de patrones de comportamiento
    c. Análisis de tráfico en tiempo real
    d. Investigación de vulnerabilidades
    e. Ninguna de las anteriores

13. **¿Qué enfoques se utilizan para la ingeniería inversa de amenazas digitales?** *(Puede seleccionar más de una opción)*

    a. Reversión manual de código
    b. Uso de herramientas especializadas
    c. Evaluación de funcionalidad y comportamiento
    d. Investigación de origen e impacto
    e. No se realiza ingeniería inversa

14. **¿Cómo se integra la investigación forense digital con otras capacidades de ciberdefensa?** *(Puede seleccionar más de una opción)*

    a. Coordinación con respuesta a incidentes
    b. Integración con medidas de prevención
    c. Apoyo a la explotación de ciberamenazas
    d. Evaluación y ajuste de estrategias
    e. No hay integración formal

Sección 5: Evaluación General

15. **¿Cuál considera que es el área más crítica para mejorar en la capacidad de ciberdefensa del Ejército del Perú?** *(Seleccione solo una opción)*

    a. Prevención y protección

b. Explotación y reconocimiento de amenazas
c. Respuesta a incidentes
d. Investigación y análisis digital
e. Todas las áreas requieren igual atención

16. **¿Cuántos años de experiencia tiene en el campo de la ciberseguridad y ciberdefensa?** *(Seleccione solo una opción)*

a. Menos de 1 año
b. 1-3 años
c. 4-6 años
d. Más de 6 años

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO DEL PERÚ

MAESTRÍA DE ESTRATEGIA Y GEOPOLÍTICA

INTRODUCCIÓN

Buenos días (tardes),

Estamos trabajando en el estudio que servirá para elaborar una tesis de maestría en Estrategia y Geopolítica del PAME de la ESGE-EPG acerca de: “La capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio, 2024”.

El objetivo de este cuestionario tradicional es determinar la influencia de la capacidad de ciberdefensa del Ejército del Perú en el ciberespacio en el año 2024. La encuesta está diseñada para evaluar diferentes aspectos de la ciberdefensa, incluyendo la capacidad de defensa, explotación, respuesta e investigación digital, y cómo estos afectan la eficiencia y efectividad en el ciberespacio.

INSTRUCCIONES

1. La encuesta es autoadministrada, además, los participantes deben completar el cuestionario de forma individual.
2. Emplee un bolígrafo de tinta para responder el cuestionario.
3. Todas las respuestas serán tratadas de manera confidencial y se utilizarán únicamente para fines de investigación. Su identidad no será revelada.
4. El cuestionario cuenta con 19 preguntas. La encuesta puede tardar aproximadamente veinte (20) minutos en completarse.
5. Responda las siguientes preguntas marcando la opción que mejor describa la situación o que se ajuste a la realidad. En algunas preguntas, puede marcar solo una respuesta, mientras que en otras puede seleccionar varias respuestas si considera que son aplicables.
6. Si no puede contestar una pregunta o si la pregunta no tiene sentido para usted, por favor pregúntele a la persona que le entregó este cuestionario y le explicará.

De antemano, ¡MUCHAS GRACIAS POR SU COLABORACIÓN!

Sección 1: Redes Interconectadas e Interdependientes de Infraestructura de Tecnología de la Información

1. **¿Qué tan eficiente es el empleo del Internet a través de las redes interconectadas e interdependientes de infraestructura de tecnología de la información en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. La conexión es intermitente y poco confiable
    b. El acceso es estable pero con algunas limitaciones
    c. La conexión es generalmente confiable y adecuada para la mayoría de las operaciones
    d. Se implementan medidas para optimizar el uso del Internet
    e. Existen capacidades avanzadas para asegurar la alta disponibilidad de Internet

2. **¿Cómo se valora la eficiencia de las redes de telecomunicaciones en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. Las redes de telecomunicaciones presentan fallos frecuentes
    b. Las redes son funcionales con algunas interrupciones
    c. Las redes de telecomunicaciones operan de manera eficiente para la mayoría de las necesidades
    d. Se aplican medidas para mejorar la eficiencia y reducir fallos
    e. Se cuenta con tecnología avanzada que asegura una alta eficiencia en las telecomunicaciones

3. **¿Cómo calificaría la eficiencia de los sistemas informáticos en el Cecyber?** *(Puede seleccionar más de una opción)*

    a. Los sistemas presentan problemas frecuentes de rendimiento
    b. Los sistemas son funcionales pero con algunas limitaciones
    c. Los sistemas informáticos operan eficientemente para la mayoría de los procesos
    d. Se realizan mantenimientos regulares para asegurar su buen funcionamiento
    e. Los sistemas informáticos están optimizados y actualizados con las últimas tecnologías

4. **¿Qué nivel de eficiencia presentan los procesadores en las redes interconectadas e interdependientes de infraestructura de tecnología de la información?** *(Puede seleccionar más de una opción)*

    a. Los procesadores sufren de lentitud y retrasos frecuentes
    b. Los procesadores tienen un desempeño aceptable con algunas limitaciones
    c. Los procesadores funcionan eficientemente para las tareas comunes
    d. Se implementan mejoras y actualizaciones para optimizar el rendimiento

e. Los procesadores están a la vanguardia y gestionan eficientemente las cargas de trabajo

5. **¿Cuál es su percepción sobre la efectividad de la infraestructura de tecnología de la información en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. La infraestructura es insuficiente para las necesidades actuales
    b. La infraestructura cubre las necesidades básicas, pero requiere mejoras
    c. La infraestructura es adecuada para las operaciones actuales
    d. La infraestructura está bien desarrollada y optimizada
    e. La infraestructura es avanzada y supera las expectativas actuales

6. **¿Cómo se gestiona actualmente la resiliencia de las redes interconectadas e interdependientes de infraestructura de tecnología de la información ante incidentes de seguridad digital?** *(Puede seleccionar más de una opción)*

    a. Se tienen procedimientos estandarizados para la recuperación
    b. Se realizan simulacros de respuesta ante incidentes
    c. Se cuenta con un equipo dedicado a la gestión de incidentes
    d. Se mantiene un registro actualizado de incidentes y respuestas
    e. No se aplican medidas específicas para la resiliencia

7. **¿Qué tan eficaz es la integración de diferentes sistemas tecnológicos en el ciberespacio para las operaciones militares?** *(Puede seleccionar más de una opción)*

    a. Existen problemas de interoperabilidad frecuentes
    b. La integración es funcional con algunas limitaciones
    c. Los sistemas están bien integrados y apoyan las operaciones militares
    d. Se realizan mejoras continuas para la integración de sistemas
    e. La integración es avanzada y soporta de manera óptima las operaciones

8. **¿Qué impacto tiene el nivel de concientización del personal sobre ciberseguridad en la eficiencia del ciberespacio?** *(Puede seleccionar más de una opción)*

    a. El personal tiene una baja conciencia sobre ciberseguridad
    b. El personal recibe formación básica en ciberseguridad
    c. La concientización es adecuada y apoya la seguridad del ciberespacio
    d. Se realizan sesiones regulares de formación avanzada en ciberseguridad
    e. El personal está altamente capacitado en prácticas de ciberseguridad

9. **¿Qué papel juegan las políticas y procedimientos institucionales en la eficiencia del ciberespacio?** *(Puede seleccionar más de una opción)*

a. Las políticas y procedimientos son insuficientes o desactualizados
b. Existen políticas básicas pero no completamente implementadas
c. Las políticas y procedimientos son adecuadas y bien implementadas
d. Se revisan y actualizan regularmente para adaptarse a nuevas amenazas
e. Las políticas y procedimientos son exhaustivos y se aplican de manera rigurosa

10. **¿Cuál considera que es el área más crítica para mejorar en el manejo del ciberespacio en el Ejército del Perú?** *(Seleccione solo una opción)*

    a. Empleo del Internet
    b. Redes de telecomunicaciones
    c. Sistemas informáticos
    d. Procesadores
    e. Controladores integrados de datos
    f. Usuarios de datos almacenados

11. **¿Qué medidas se podrían tomar para mejorar la eficiencia de la infraestructura de tecnología de la información?** *(Puede seleccionar más de una opción)*

    a. Implementar nuevas tecnologías de red
    b. Realizar actualizaciones regulares de sistemas
    c. Mejorar la formación del personal en el uso de tecnología
    d. Optimizar la configuración de los procesadores
    e. Aumentar la capacidad de los controladores de datos

12. **¿Qué acciones serían efectivas para incrementar la eficiencia en la gestión de datos almacenados?** *(Puede seleccionar más de una opción)*

    a. Mejorar las técnicas de almacenamiento y recuperación
    b. Incrementar la seguridad en la protección de datos
    c. Optimizar los procesos de acceso y utilización de datos
    d. Capacitar mejor a los usuarios en el manejo de datos
    e. Implementar soluciones avanzadas para el análisis de datos

---

Sección 2: Redes Interconectadas e Interdependientes de Infraestructura de Datos Almacenados

13. **¿Cómo calificaría la eficiencia en la gestión de redes interconectadas y sistemas informáticos en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. La gestión es deficiente y presenta muchos problemas
    b. La gestión es aceptable pero con áreas de mejora
    c. La gestión es eficiente y cumple con los requisitos operativos
    d. La gestión es muy eficiente con medidas proactivas en lugar

e. La gestión es ejemplar y lidera en buenas prácticas

14. **¿Cómo se valora la eficiencia de los controladores integrados de las redes interconectadas e interdependientes de infraestructura de datos almacenados?** *(Puede seleccionar más de una opción)*

    a. Los controladores tienen problemas de rendimiento y confiabilidad
    b. Los controladores funcionan adecuadamente pero con algunas limitaciones
    c. Los controladores operan de manera eficiente para el almacenamiento de datos
    d. Se realizan actualizaciones periódicas para mantener la eficiencia
    e. Los controladores están optimizados para manejar grandes volúmenes de datos sin problemas

15. **¿Qué nivel de eficiencia presentan los usuarios en las redes interconectadas e interdependientes de infraestructura de datos almacenados?** *(Puede seleccionar más de una opción)*

    a. Los usuarios encuentran dificultades frecuentes en el acceso y uso de datos
    b. Los usuarios tienen un acceso razonable con algunas limitaciones
    c. Los usuarios pueden acceder y utilizar los datos eficientemente
    d. Se proporciona capacitación regular para asegurar el uso efectivo de los datos
    e. Los usuarios están bien equipados y capacitados para maximizar el uso de los datos

16. **¿Qué medidas de seguridad se aplican para proteger la infraestructura de datos almacenados?** *(Puede seleccionar más de una opción)*

    a. Se utilizan medidas básicas de protección de datos
    b. Existen protocolos establecidos para la seguridad de datos
    c. Se implementan tecnologías avanzadas de seguridad de datos
    d. Se realizan auditorías regulares de seguridad
    e. Se proporcionan entrenamientos y concientización en seguridad de datos para el personal

17. **¿Qué tan adecuada considera que es la protección de datos almacenados en el ciberespacio del Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. La protección es mínima y hay riesgos significativos
    b. La protección es básica y podría mejorarse
    c. La protección es adecuada para las necesidades actuales
    d. Se aplican medidas avanzadas de protección de datos
    e. La protección de datos es de alta calidad y cumple con estándares rigurosos

18. **¿Cuál es el nivel de resiliencia de la infraestructura de datos almacenados ante ataques cibernéticos?** *(Puede seleccionar más de una opción)*

    a. La infraestructura tiene una baja capacidad de recuperación
    b. La infraestructura puede recuperarse de incidentes menores
    c. La infraestructura está diseñada para una recuperación efectiva ante incidentes importantes
    d. Se implementan estrategias avanzadas para asegurar una alta resiliencia
    e. La infraestructura tiene mecanismos robustos para asegurar la recuperación completa y rápida

19. **¿Qué tipo de mejoras considera más necesarias para optimizar el ciberespacio en el Ejército del Perú?** *(Puede seleccionar más de una opción)*

    a. Mejora en la infraestructura tecnológica
    b. Refuerzo en las medidas de seguridad de datos
    c. Actualización y mantenimiento de sistemas informáticos
    d. Capacitación y concientización del personal
    e. Mejoras en la integración y eficiencia de las redes

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VALIDACIÓN POR EXPERTOS DEL INSTRUMENTO DE LA PRIMERA VARIABLE

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
Gonzales Cáceres Percy	Jefe del Centro de Ciberdefensa	Encuesta	Cels Gutierrez-Tineo

Título de la Investigación:
La capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio -2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1 CLARIDAD	Esta formulado con lenguaje apropiado																			X	
2 OBJETIVO	Está expresado en Capacidades observables																			X	
3 ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			X	
4 ORGANIZACIÓN	Existe una organización lógica en el instrumento																			X	
5 SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			X	
6 INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			X	
7 CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			X	
8 COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			X	
9 METODOLOGÍA	La estrategia responde al propósito de la investigación																			X	
10 PERTINENCIA	El inventario es aplicable																			X	

II. OPINIÓN DE APLICACIÓN:
El instrumento es efectivo, claro y fácil de aplicar.

IV. PROMEDIO DE VALORACIÓN: 95.00

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
Chorrillos, 25 ago 2024	43517097		997616575

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
MARTINEZ ROSALES MIGUEL	JEFE - CINFE	ENCUESTA	Cnl. Gutierrez - TINEO

Titulo de la Investigación:
LA CAPACIDAD DE CIBERDEFENSA DEL EJERCITO DEL PERÚ Y SU INFLENCIA EN EL CIBERESPACIO, 2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1 CLARIDAD	Esta formulado con lenguaje apropiado																			X	
2 OBJETIVO	Está expresado en Capacidades observables																				X
3 ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				X
4 ORGANIZACIÓN	Existe una organización lógica en el instrumento																			X	
5 SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																				X
6 INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				X
7 CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				X
8 COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			X	
9 METODOLOGÍA	La estrategia responde alpropósito de la investigación																			X	
10 PERTINENCIA	El inventario es aplicable																			X	

II. OPINIÓN DE APLICACIÓN:

EXISTE UNA RELACIÓN MUY ALTA ENTRE LAS VARIABLES PARA EL DESARROLLO DE LA INVESTIGACIÓN

IV. PROMEDIO DE VALORACIÓN: 97.50

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
CHORRILLOS 22 Ago 2024	16125380		998736772

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
VEGA CASTRO HUGO EDWIN	DIRECTOR - ECOHE	ENCUESTA	CALS. GUTIERREZ - TIRCO

Título de la Investigación:
LA CAPACIDAD DE CIBERDEFENSA DEL EJERCITO DEL PERÚ Y SU INFLUENCIA EN EL CIBERESPACIO 2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				X
2. OBJETIVO	Está expresado en Capacidades observables																				X
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			X	
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																			X	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				X
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			X	
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																				X
9. METODOLOGÍA	La estrategia responde alpropósito de la investigación																				X
10. PERTINENCIA	El inventario es aplicable																				X

II. OPINIÓN DE APLICACIÓN:

EXISTE UNA RELACION MUY DIRECTA ENTRE LAS VARIABLES PARA EL DESARROLLO DE LA INVESTIGACION

IV. PROMEDIO DE VALORACIÓN: 98.00

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
Chorrillos 27 ago 2024	09933773		980374956

VALIDACIÓN DEL INSTRUMENTO DE LA PRIMERA VARIABLE

Los resultados o calificaciones otorgadas por los expertos se someten a análisis estadísticos para estimar un coeficiente de validación de contenido, para ello se utiliza con frecuencia la prueba V de Aiken (Aiken, 1980).

$$V = \frac{\overline{X} - I}{k}$$

Nota. $\bar{X}$ es la media de las calificaciones de los jueces en la muestra, *I* es la calificación más baja posible, y *k* es el rango de los valores posibles de la escala Likert utilizada. Por ejemplo, si *I* = 1 y *k* = 5, entonces *k* = 5 – 1= 4. Fuente: Tomado de Merino y Livia (2009).

Tabla 38

Escala de valores y puntaje de calificaciones

Escala	Rango del puntaje otorgado por los jueces/expertos
1	De 0 a 20
2	De 21 a 40
3	De 41 a 60
4	De 61 a 80
5	De 81 a 100

Tabla 39

Interpretación del coeficiente

Rango del coeficiente	Interpretación del nivel
0,00	Pobre (Poor)
0,1-0,20	Leve (Slight)
0,21-0,40	Aceptable (Fair)
0,41-0,60	Moderada (Moderate)
0,61-0,80	Considerable (Substantial)
0,81-1,0	Casi perfecta (Almost perfect)

VALIDACIÓN POR EXPERTOS DEL INSTRUMENTO DE LA SEGUNDA VARIABLE

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
Gonzales Cáceres Percy	Jefe del Centro de Ciberdefensa	Encuesta	Cels Gutierrez-Tineo

Título de la Investigación:
La capacidad de ciberdefensa del Ejército del Perú y su influencia en el ciberespacio – 2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																			X	
2. OBJETIVO	Está expresado en Capacidades observables																			X	
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			X	
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																			X	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			X	
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			X	
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			X	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																			X	
10. PERTINENCIA	El inventario es aplicable																			X	

II. OPINIÓN DE APLICACIÓN:

El instrumento es efectivo, claro y fácil de aplicar.

IV. PROMEDIO DE VALORACIÓN: 95.00

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
Chorrillos, 25 ago 2024	43517097		997616575

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
MARTINEZ NOBLES MIGUEL ANGEL	JEFE - CINFE	ENCUESTA	Chc. Gutierrez - Tineo

Título de la Investigación:
LA CAPACIDAD DE CIBERDEFENSA DEL EJERCITO DEL PERÚ Y SU INFLUENCIA EN EL CIBERESPACIO, 2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				X
2. OBJETIVO	Está expresado en Capacidades observables																				X
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				X
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																			X	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			X	
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				X
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			X	
9. METODOLOGÍA	La estrategia responde alpropósito de la investigación																				X
10. PERTINENCIA	El inventario es aplicable																			X	

II. OPINIÓN DE APLICACIÓN:

EXISTE UNA RELACIÓN MUY ALTA ENTRE LAS VARIABLES PARA EL DESARROLLO DE LA INVESTIGACIÓN

IV. PROMEDIO DE VALORACIÓN: 97.50

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
CHORRILLOS 22 Ago 2024	16125380		998731672

1. Validación de instrumentos

JUICIO DE EXPERTO DEL INSTRUMENTO DE EVALUACIÓN

Apellido y Nombre del Informante	Cargo o Institución donde	Nombre del instrumento	Autor del Instrumento
VEGA CASTRO HUGO CESAR	DIRECTOR - ECOMG	ENCUESTA	CRIS GUTIERREZ - TINGO

Título de la Investigación:
LA CAPACIDAD DE CIBERDEFENSA DEL EJERCITO DEL PERÚ Y SU INFLUENCIA EN EL CIBERESPACIO 2024

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	5	10	11 15 16 20	21	25	30	31 35 36 40	41	45	50	51 55 56 60	61	65	70	71 75 76 80	81	85	90	91 95 96 100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				X
2. OBJETIVO	Está expresado en Capacidades observables																				X
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				X
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																				X
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																				X
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				X
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				X
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																				X
9. METODOLOGÍA	La estrategia responde alpropósito de la investigación																				X
10. PERTINENCIA	El inventario es aplicable																				X

II. OPINIÓN DE APLICACIÓN:

EXISTE UNA BUENA CONCORDANCIA ENTRE LAS VARIABLES PARA DESARROLLAR LA INVESTIGACIÓN

IV. PROMEDIO DE VALORACIÓN: 97.50

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
CHORRILLOS 22 AGO 2024	09933373		988032956

VALIDACIÓN DEL INSTRUMENTO DE LA SEGUNDA VARIABLE

Para la validación del instrumento de la segunda variable también se ha tenido en cuenta las tabla 1 y tabla 2, asimismo, se consultó a tres expertos quienes otorgaron el puntaje siguiente:

Tabla 40

Escala de valores asignados por los expertos para el instrumento de la segunda variable

Expertos	***Puntaje asignado de acuerdo a la tabla 1***	**Puntaje otorgado por el experto**
Experto 1	5	95.00
Experto 2	5	97.50
Experto 3	5	97.50
Media	5	

V= (5 – 1) / 4 = 1

De acuerdo al juicio de expertos y a la tabla 2 el coeficiente de validación es de 1, por lo tanto, el nivel de interpretación es casi perfecta.

Para la validación del instrumento se consultó a tres expertos quienes otorgaron el puntaje siguiente:

Tabla 41

Escala de valores asignados por los expertos para el instrumento de la primera variable

Expertos	***Puntaje asignado de acuerdo a la tabla 1***	**Puntaje otorgado por el experto**
Experto 1	5	95.00
Experto 2	5	97.50
Experto 3	5	98.00
Media	5	

V= (5 – 1) / 4 = 1

De acuerdo al juicio de expertos y a la tabla 2 el coeficiente de validación es de 1, por lo tanto, el nivel de interpretación es casi perfecta.

ANEXO 4

CONFIABILIDAD DEL INSTRUMENTO

CONFIABILIDAD DEL INSTRUMENTO DE LA PRIMERA VARIABLE

Como criterio general, George y Mallery (2003, p. 231) sugieren las recomendaciones siguientes para evaluar los coeficientes de alfa de Cronbach:

Coeficiente alfa > .9 es excelente

Coeficiente alfa > .8 es bueno

Coeficiente alfa > .7 es aceptable

Coeficiente alfa > .6 es cuestionable

Coeficiente alfa > .5 es pobre

Coeficiente alfa < .5 es inaceptable

Nunnally (1967, p.226): en las primeras fases de la investigación un valor de la fiabilidad de 0.6 o 0.5 puede ser suficiente. Con investigación básica se necesita al menos 0.8 y en investigación aplicada entre 0.9 y 0.95.

Por lo tanto, para nuestra investigación necesitamos un coeficiente de alfa de Cronbach de un mínimo de 0.8 para que el instrumento sea bueno y confiable.

I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	
1	1	5	1	1	1	5	1	5	1	1	5	5	5	5	2	45
3	2	3	3	2	2	5	1	5	4	2	5	5	5	5	2	54
1	1	5	1	5	1	5	2	2	1	4	3	5	5	5	2	48
1	1	5	1	5	1	3	1	5	1	1	5	5	5	5	2	47
3	2	3	3	2	2	4	1	1	4	2	5	5	5	5	1	48
1	1	3	1	2	1	4	1	1	1	1	3	5	2	1	1	29
1	2	5	3	5	2	4	2	5	4	4	5	5	5	5	2	59
0.8	0.2	1	1	2.7	0.2	0.5	0.2	3.4	2.2	1.6	0.8	0	1.1	2	0.2	75

K	=	El número de ítems
Si2	=	Sumatoria de Varianzas de los Ítems
St2	=	Varianza de la suma de los Ítems
α	=	Coeficiente de Alfa de Cronbach

K	=	16
Si2	=	17.8776
St2	=	74.6939
α	=	**0.811**

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

De acuerdo al cálculo realizado nuestro resultado de alfa de Cronbach es igual a 0.811, por lo tanto, nuestro instrumento es confiable y puede ser aplicado para nuestra investigación.

CONFIABILIDAD DE INSTRUMENTO DE LA SEGUNDA VARIABLE

Como criterio general, George y Mallery (2003, p. 231) sugieren las recomendaciones siguientes para evaluar los coeficientes de alfa de Cronbach:

Coeficiente alfa > .9 es excelente

Coeficiente alfa > .8 es bueno

Coeficiente alfa > .7 es aceptable

Coeficiente alfa > .6 es cuestionable

Coeficiente alfa > .5 es pobre

Coeficiente alfa < .5 es inaceptable

Nunnally (1967, p.226): en las primeras fases de la investigación un valor de la fiabilidad de 0.6 o 0.5 puede ser suficiente. Con investigación básica se necesita al menos 0.8 y en investigación aplicada entre 0.9 y 0.95.

Por lo tanto, para nuestra investigación necesitamos un coeficiente de alfa de Cronbach de un mínimo de 0.8 para que el instrumento sea bueno y confiable.

I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	
2	2	2	1	1	1	1	1	2	3	1	5	2	2	2	1	1	1	1	32
2	2	2	1	1	4	2	1	4	3	1	2	2	2	2	1	2	2	2	38
3	2	2	2	1	5	2	1	2	3	1	3	2	2	2	2	3	2	1	41
2	5	2	2	1	5	2	5	2	5	2	5	3	2	2	2	3	2	2	54
2	2	2	1	1	1	1	1	2	3	1	5	2	2	2	1	1	1	1	32
2	2	2	2	1	4	2	1	4	3	1	2	2	2	2	1	2	2	1	38
3	2	2	1	1	5	2	1	2	3	1	3	2	2	2	2	3	2	1	40
0.2	1.1	0	0.2	0	2.8	0.2	2	0.8	0.5	0.1	1.7	0.1	0	0	0.2	0.7	0.2	0.2	47

K	=	El número de ítems
Si2	=	Sumatoria de Varianzas de los Ítems
St2	=	Varianza de la suma de los Ítems
α	=	Coeficiente de Alfa de Cronbach

K	=	19
Si2	=	11.1020
St2	=	47.0612
α	=	**0.807**

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

De acuerdo al cálculo realizado nuestro resultado de alfa de Cronbach es igual a 0.807, por lo tanto, nuestro instrumento es confiable y puede ser aplicado para nuestra investigación.

ANEXO 5

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Postgrado

Chorrillos, 21 de julio del 2023

Oficio Nº 490/U-26.e.a/DGI

Señor Gral Div Jefe del Estado Mayor General del Ejército.- **San Borja**

Asunto : Solicita brindar facilidades a personal que se indica

Ref : a. Reglamento para la obtención del grado académico de Maestro en Ciencias Militares.
b. Reglamento de Investigaciones de la ESGE-EPG

Tengo el honor de dirigirme a Ud en relación a los documentos de la referencia para solicitarle se digne brindar las facilidades para el levantamiento de datos e informaciones en la Dirección de Telemática del Ejército, Centro de Ciberdefensa del Ejército y en el Centro de Informática del Ejército, al **Crl EP José Raúl TINEO ARENAS y al Crl EP Nicéforo GUTIERREZ CHAVEZ**, estudiantes de la XV Maestría en Estrategia y Geopolítica de esta casa de estudios, quienes realizan la investigación titulada: "**LA CAPACIDAD DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ Y SU INFLUENCIA EN EL CIBERESPACIO, 2024".**

Agradeciendo de antemano por las facilidades brindadas, asimismo, es propicia la oportunidad para expresarle mis consideraciones y deferente estima.

Dios guarde a Ud.

ESCUELA SUPERIOR DE GUERRA DEL EJERCICIO
ESCUELA DE POST GRADO
DIRECCION

O -224724171 – A+
JUAN KENNET VALVERDE VIRHUEZ
General de Brigada
Director de la Escuela Superior de Guerra del Ejército
Escuela de Posgrado

Distribución:
JEMGE…… 01
CITELE…… 01 C' Informativa
Archivo…….. 01/03

ANEXO 6

COMPROMISO ÉTICO

COMPROMISO ÉTICO

El presente trabajo de investigación titulado: **La Capacidad de Ciberdefensa del Ejército del Perú y su Influencia en el Ciberespacio, 2024**.

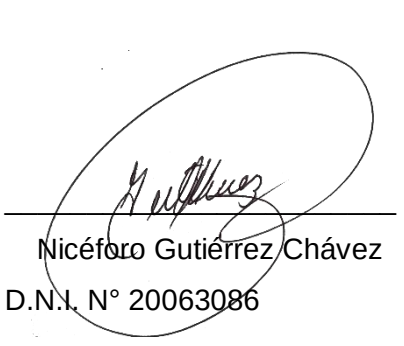
Se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación en la Escuela Superior de Guerra del Ejército, promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado.

En vista de lo anterior:

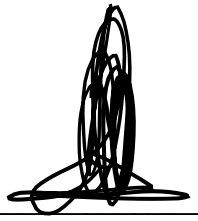
Nosotros, Bach. Nicéforo Gutiérrez Chávez, identificado con Documento Nacional de Identidad N° 20063086, con domicilio en Pasaje los Descalzos N° 185, Rimac, y Bach. José Raúl Tineo Arenas, identificado con Documento Nacional de Identidad N° 10381102, con domicilio en Villa Militar Oeste Avenida Elena fray de Pastor, Casa N° 65, Chorrillos, egresados de la Maestría en Estrategia y Geopolítica de la Escuela Superior de Guerra del Ejército – Escuela de Postgrado (ESGE-EPG), declaramos bajo juramento que hemos 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 nuestro trabajo personal, apegándonos a la legislación sobre propiedad intelectual, sin haber incurrido en falsificación de la información o cualquier tipo de fraude, por lo cual nos sometemos al marco legal y normativo vigente relacionado a dicha responsabilidad, así como a las normas disciplinarias establecidas en la ESGE-EPG.

Chorrillos, 10 de julio de 2024



Nicéforo Gutiérrez Chávez
D.N.I. N° 20063086

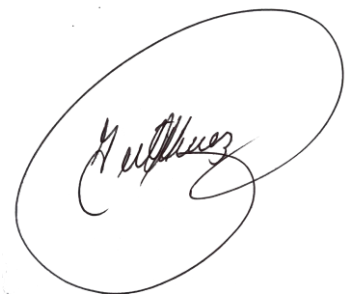


José Raúl Tineo Arenas
D.N.I. N° 10381102

ANEXO 7

HOJA DE DATOS PERSONALES

HOJA DE DATOS PERSONALES

GRADO	**:**	**Coronel**
NOMBRES	**:**	**Nicéforo**
APELLIDOS	**:**	**Gutiérrez Chávez**
EMAIL	**:**	**niceforog32@gmail.com**
DIRECCIÓN	**:**	**Pasaje Los Descalzos N° 185 – Rímac.**
CELULAR	**:**	**945105433**
FIRMA	**:**	

HOJA DE DATOS PERSONALES

GRADO	**:**	**Coronel**
NOMBRES	**:**	**José Raúl**
APELLIDOS	**:**	**Tineo Arenas**
EMAIL	**:**	cesarinfante111@hotmail.com
DIRECCIÓN	**:**	VMO. Avenida Elena Fray de Pastor, Casa 65 – Chorrillos.
CELULAR	**:**	963145593
FIRMA	**:**	

ANEXO 8

APORTE DE LA INVESTIGACIÓN

“LINEAMIENTOS ESTRATÉGICOS PARA EL FORTALECIMIENTO DE LA CAPACIDAD DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ: RESULTADOS DE LECCIONES APRENDIDAS”

1. Objetivo

El presente aporte doctrinario tiene como finalidad sintetizar las lecciones aprendidas derivadas de la investigación titulada “La Capacidad de Ciberdefensa del Ejército del Perú y su Influencia en el Ciberespacio, 2024”. Su propósito es establecer lineamientos estratégicos que contribuyan al fortalecimiento doctrinario de la ciberdefensa institucional, identificando los factores que limitan la influencia efectiva de la capacidad de ciberdefensa en el ciberespacio y proponiendo directrices orientadas a las necesidades operativas, tecnológicas y organizacionales reveladas en el estudio. Esta presentación resume el problema analizado, las recomendaciones centrales y la relevancia de los aportes a desarrollar.

2. Desarrollo

El análisis realizado permitió determinar que la capacidad de ciberdefensa del Ejército del Perú no presenta un impacto uniforme en todas sus dimensiones. La evidencia estadística demostró que la capacidad de defensa cibernética no ejerce una influencia significativa sobre el ciberespacio, reflejando una correlación baja y una limitada articulación entre los mecanismos actuales de defensa y las exigencias del entorno digital moderno. Esta primera lección aprendida muestra que el enfoque institucional aún mantiene rasgos convencionales, donde los recursos, procesos y doctrinas no se integran de manera suficiente para contrarrestar amenazas avanzadas y persistentes.

Asimismo, la investigación reveló que la capacidad de respuesta cibernética presenta una correlación moderada y estadísticamente significativa, lo que evidencia la existencia de una base operativa funcional. Sin embargo, la dispersión de responsabilidades, la falta de integración interinstitucional y la limitada estandarización de protocolos generan demoras y reducen la eficiencia en la atención de incidentes. Esta segunda lección aprendida resalta la necesidad de establecer procedimientos más ágiles, interoperables y adaptativos que permitan mejorar la capacidad de respuesta.

La dimensión más sólida identificada fue la capacidad de investigación digital, que presentó una correlación alta y significativa respecto a la influencia en el ciberespacio. Esta tercera lección aprendida demuestra que las capacidades de análisis forense, reconstrucción de incidentes y detección de vulnerabilidades constituyen un pilar estratégico para fortalecer la ciberdefensa. Sin embargo, el estudio determinó que estas capacidades aún no cuentan con una infraestructura tecnológica adecuada ni con una estructura organizacional que permita maximizar su impacto en el entorno militar cibernético.

A partir de estas tres lecciones aprendidas, el aporte doctrinario propone lineamientos estratégicos que buscan fortalecer la ciberdefensa institucional:

Priorizar la inversión en tecnologías de defensa cibernética y fortalecer las capacidades pasivas y activas de protección

El Ejército del Perú debe consolidar un sistema robusto de protección cibernética que incorpore capacidades pasivas (firewalls avanzados, segmentación de redes militares, cifrado, antivirus de grado militar, modelos Zero Trust) y capacidades activas (detección en tiempo real, análisis de tráfico,

ciberinteligencia táctica). Esto requiere inversiones orientadas a: modernizar las plataformas del Centro de Ciberdefensa, la Dirección de Telemática y el Centro de Informática; implementar sistemas EDR/XDR con monitoreo permanente; establecer una red militar con blindaje criptográfico propio; y reforzar la protección digital de los sistemas de mando y control. Estas medidas reducirán la superficie de ataque y permitirán detectar amenazas con anticipación.

Desarrollar un sistema de respuesta interoperable con protocolos institucionales y conjuntos

El Ejército debe fortalecer su capacidad de respuesta mediante un sistema interoperable que articule sus centros especializados, manteniendo alineación doctrinaria con los lineamientos del CCFFAA, entidad responsable de la conducción conjunta en operaciones cibernéticas. Esto implica: protocolos unificados de mitigación entre EP, Marina, FAP y CCFFAA; ejercicios conjuntos de ciberseguridad; integración de plataformas de alerta temprana; y la construcción de un Manual de Respuesta Conjunta frente a Ciberincidentes. La interoperabilidad permite enfrentar amenazas de manera coordinada, evitando brechas y duplicidades.

Consolidar unidades de investigación digital especializadas dentro del Ejército

La investigación digital es una capacidad esencial para rastrear y neutralizar amenazas complejas. Se propone consolidar unidades especializadas exclusivamente dentro del EP, enfocadas en análisis forense digital, ingeniería inversa, cacería de amenazas con herramientas de aprendizaje automático y laboratorios de simulación de ataques. Estas capacidades

permitirán anticiparse a adversarios, fortalecer investigaciones internas y elevar el nivel táctico-operativo de la ciberdefensa.

Incorporar tecnologías emergentes como inteligencia artificial para detección temprana y automatización

El Ejército debe integrar tecnologías emergentes, especialmente inteligencia artificial, aprendizaje automático y automatización, para mejorar la velocidad y precisión en la defensa cibernética. Ello incluye sistemas de IA para detección temprana, plataformas SOAR para respuestas automáticas, integración con estándares nacionales establecidos por el CCFFAA y algoritmos de predicción de comportamientos hostiles. Estas herramientas fortalecen la capacidad predictiva y reducen tiempos de respuesta.

Promover la capacitación continua y la cultura de ciberseguridad en la organización militar

El fortalecimiento de la ciberdefensa requiere una cultura institucional sólida. Se propone establecer programas permanentes de formación para todos los niveles del personal, impulsar certificaciones internacionales, implementar ciberentrenamiento para operadores de sistemas críticos, promover prácticas de seguridad digital y desarrollar evaluaciones periódicas para medir la madurez cibernética de las unidades. Una cultura fortalecida reduce errores, consolida disciplina digital y mejora la postura de defensa.

3. Conclusión

Las lecciones aprendidas permiten concluir que la capacidad de ciberdefensa del Ejército del Perú influye de manera diferenciada en el ciberespacio, siendo indispensable reforzar principalmente las capacidades de

defensa y respuesta para alcanzar un desempeño adecuado frente a las exigencias del entorno digital. Asimismo, el alto impacto de la investigación digital evidencia un potencial institucional significativo que, al ser potenciado doctrinaria, tecnológica y organizacionalmente, puede consolidar un sistema de ciberdefensa más robusto, integrado y proactivo.

Este aporte doctrinario propone lineamientos estratégicos que contribuyen a una postura moderna y resiliente, orientada a proteger el ciberespacio nacional, salvaguardar la soberanía digital y enfrentar con eficacia las amenazas cibernéticas emergentes. Representa, por tanto, un insumo doctrinario relevante para la actualización de políticas, procedimientos y capacidades del Ejército del Perú.

ANEXO 9

CD CONTENIENDO LA TESIS

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO - ESCUELA DE POSTGRADO

TESIS

La capacidad de Ciberdefensa del Ejército del Perú y su influencia en el Ciberespacio, 2024

AUTORES:
Bach. José Raúl TINEO ARENAS
Bach Nicéforo GUTIÉRREZ CHÁVEZ

2025

ANEXO 10

REPORTE DE SIMILITUD DE TURNITIN

IFI TINEO - GUTIERREZ.corregido.docx

AÑO 2026

AÑO 2026

Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:564385775

Fecha de entrega
6 mar 2026, 8:37 a.m. GMT-5

Fecha de descarga
6 mar 2026, 9:27 a.m. GMT-5

Nombre del archivo
IFI TINEO - GUTIERREZ.corregido.docx

Tamaño del archivo
10.8 MB

141 páginas

31.107 palabras

180.442 caracteres

20% 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

17% Fuentes de Internet

5% Publicaciones

12% Trabajos entregados (trabajos del estudiante)