ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

TESIS

Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de Información en el Ejército del Perú – 2024

AUTORES:
BACH. Maribel Jenny Mendoza Barreto De Ruiz
(orcid.org/0009-0003-1378-3761)
BACH. Marco Antonio Ruiz Hurtado
(orcid.org/0009-0009-8730-5096)

Para optar al Grado Académico de
MAESTRO EN CIENCIAS MILITARES
Con mención en Gestión Pública y Planeamiento Estratégico

ASESOR:
DRA. Yessenia Solier Castro
(orcid.org/ 0000-0002-1121-7112)

LÍNEA DE INVESTIGACIÓN
Empleo de GUB. GUC, Operaciones GC y GNC

2025

ACTA DE SUSTENTACIÓN

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 051 – 2025/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veinte (20) días del mes de noviembre del año dos mil veinticinco, siendo las 11:50 horas, se reunió el jurado evaluador conformado por los docentes:

❖	Doctor	IVAN RICARDO BARRETO BARDALES	Presidente
❖	Maestro	ROBERTO JOAQUIN VIVANCO BURGOS	Secretario
❖	Doctor	JOSE MANUEL PALACIOS SANCHEZ	Vocal

Designados según Resolución de Expedito para Sustentación de Tesis **N° 051-2025/SIE/DGI/ESGE-EPG** del 10 de noviembre de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"CENTRO DE CIBERDEFENSA DEL EJÉRCITO Y SU APORTE A LAS OPERACIONES DE INFORMACIÓN EN EL EJÉRCITO DEL PERÚ - 2024"**, presentado por los Bachilleres **MARIBEL JENNY MENDOZA BARRETO DE RUIZ y MARCO ANTONIO RUIZ HURTADO,** para optar el Grado Académico de Maestro en Ciencias Militares con mención en Gestión Pública y Planeamiento Estratégico, 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 APROBADO POR EXCELENCIA

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

Firmado, en Chorrillos a los veinte (20) días del mes de noviembre del año dos mil veinticinco.

DR. IVAN RICARDO BARRETO BARDALES PRESIDENTE	MG. ROBERTO JOAQUIN VIVANCO BURGOS SECRETARIO	DR. JOSE MANUEL PALACIOS SANCHEZ VOCAL

DEDICATORIA

A nuestro amado hijo, Dante, que siempre ilumina y motiva nuestro camino para poder alcanzar nuestras metas; a nuestros amados padres y familiares, por su infinito apoyo que facilitaron este proceso de investigación.

AGRADECIMIENTOS

Debemos reconocer el apoyo y seguimiento de nuestro docente en metodología de la investigación y al Centro de ciberdefensa que nos brindó todas las facilidades para la recolección de datos.

ÍNDICE

Página

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente tesis analiza el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información del Ejército del Perú durante el año 2024. El estudio se desarrolló bajo un enfoque cuantitativo, con un diseño no experimental de tipo correlacional, aplicando el coeficiente de correlación de Pearson para evaluar la relación entre la percepción sobre el CCE (variable independiente) y la eficiencia y eficacia de las operaciones de información (variable dependiente), considerando cinco dimensiones: nivel de actividad, capacitación, aplicación de estrategias, eficiencia operativa y eficacia informacional. Los resultados obtenidos demuestran que existe correlación positiva significativa entre la percepción del nivel de actividad del CCE y su eficiencia operativa ($r = 0.695$, $p = 0.000$), lo que indica que hay una mayor visibilidad y eficacia en sus acciones, que se relacionan con una gestión más eficaz de recursos. De igual forma, se encontró que hay una fuerte correlación entre la capacitación en ciberseguridad y la eficacia operativa ($r = 0.742$, $p = 0.000$), demostrando la influencia de la formación técnica especializada. No obstante, las correlaciones moderadas en la dimensión estratégica nos indican desafíos de alineación entre planificación y ejecución operativa. En conjunto, estos hallazgos confirman que el CCE cumple un rol importantísimo en el desarrollo de las operaciones de información. Para ampliar los beneficios, se requiere tomar medidas como: fortalecer la doctrina vigente, modernizar el equipamiento y materializar programas de capacitación dirigido al personal. El fortalecimiento del CCE es esencial para responder eficazmente a amenazas cibernéticas crecientes y mejorar el soporte a la toma de decisiones militares.

Palabras clave: Ciberdefensa; Operaciones de Información; Eficiencia Operativa; Ejército del Perú; Seguridad Cibernética.

ABSTRACT

This thesis analyzes the contribution of the Army Cyber Defense Center (CCE) to the Information Operations (IO) of the Peruvian Army during the year 2024. The study was developed under a quantitative approach with a non-experimental, correlational design, applying Pearson's correlation coefficient to evaluate the relationship between the perception of the CCE (independent variable) and the efficiency and effectiveness of information operations (dependent variable). Five dimensions were considered: level of activity, training, application of strategies, operational efficiency, and informational effectiveness.

The results demonstrate a significant positive correlation between the perceived level of activity of the CCE and its operational efficiency ($r = 0.695$, $p = 0.000$), indicating greater visibility and effectiveness in its actions, which are related to a more efficient management of resources. Likewise, a strong correlation was found between cybersecurity training and operational effectiveness ($r = 0.742$, $p = 0.000$), highlighting the influence of specialized technical training. However, moderate correlations in the strategic dimension reveal challenges in aligning planning with operational execution.

Overall, these findings confirm that the CCE plays a crucial role in the development of information operations. To expand its impact, it is necessary to take measures such as strengthening existing doctrine, modernizing infrastructure, and implementing comprehensive training programs for personnel. Strengthening the CCE is essential to effectively respond to emerging cyber threats and to enhance support for military decision-making processes.

Keywords: **Cyber Defense; Information Operations; Peruvian Army; Operational Efficiency; Cybersecurity.REPORTE DE SIMILITUD**

REPORTE DE SIMILITUD

IFI - BACH. RUIZ Y BACH. MENDOZA.docx

TESIS 2025

TESIS 2025

Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:545608085

Fecha de entrega
12 ene 2026, 7:14 p.m. GMT-5

Fecha de descarga
12 ene 2026, 7:22 p.m. GMT-5

Nombre del archivo
IFI - BACH. RUIZ Y BACH. MENDOZA.docx

Tamaño del archivo
70.0 MB

145 páginas

33.240 palabras

194.045 caracteres

turnitin Página 2 de 156 - Descripción general de integridad Identificador de la entrega trn:oid:::12350:545608085

9% 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

7% Fuentes de Internet
4% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

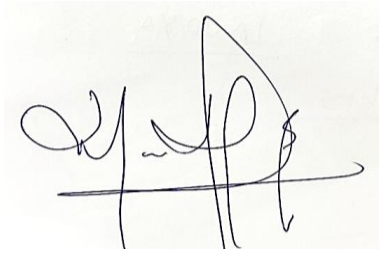
DECLARACIÓN JURADA DE AUTENTICIDAD Y NO PLAGIO

Por el presente documento, yo Marco Antonio Ruiz Hurtado, identificado con DNI N° 70470633, y la Sra. Maribel Jenny Mendoza Barreto de Ruiz, identificada con DNI N° 70470624, egresados del programa de la XIII Maestría en Ciencias Militares mención en Gestión Pública y Planeamiento Estratégico, informo que he elaborado el trabajo de Investigación denominado “Centro de Ciberdefensa del Ejército y su aporte a las Operaciones de Información en el Ejército del Perú – 2024”; para optar por el Grado Académico de Magister en la maestría de Ciencias Militares con mención en Gestión Pública, y declaro que este trabajo ha sido desarrollado íntegramente por los autores que lo suscriben y afirmamos que no existe plagio de ninguna naturaleza. Así mismo, dejamos en constancia de que las citas de otros autores han sido debidamente identificadas en el trabajo, por lo que no se ha asumido como propias las ideas vertidas por terceros, ya sea de fuentes encontradas en medios escritos como en Internet.

Así mismo, afirmamos que somos responsable solidariamente de todo su contenido y asumimos, como autores, las consecuencias ante cualquier falta, error u omisión de referencias en el documento. Sé que este compromiso de autenticidad y no plagio puede tener connotaciones éticas y legales. Por ello, en caso de incumplimiento de esta declaración, nos sometemos a lo dispuesto en las normas académicas que dictamine la Escuela Superior de Guerra del Ejército – Escuela de Postgrado y a lo estipulado en el Reglamento interno.

Marco Antonio Ruiz Hurtado

DNI: 70470633



Maribel Jenny Mendoza Barreto de Ruiz

DNI: 70470624

INTRODUCCIÓN

Dentro del contexto de la defensa y la seguridad nacional como fenómeno contemporáneo, que incluye la creciente digitalización de las funciones estatales junto con la aparición del ciberespacio como un nuevo ámbito operacional, la ciberdefensa se ha convertido en un área de enfoque crítico para las Fuerzas Armadas. En este escenario, el Ejército del Perú reconoció la creciente necesidad de mejorar su capacidad para operar y defenderse en este entorno, lo que llevó a la creación del Centro de Ciberdefensa del Ejército (CCE), una unidad especializada diseñada para contrarrestar amenazas cibernéticas sofisticadas a la infraestructura crítica y la integridad de las operaciones de información (Moya, 2023).

Las Operaciones de Información (OI), según la doctrina militar moderna, constituye un conjunto de acciones sistemáticas orientadas a proteger, influir, interrumpir y explotar los sistemas de información del adversario, integrando capacidades como guerra electrónica, guerra psicológica y ciberdefensa (Department of Defense, 2021). Sin embargo, en el caso de la ciberdefensa, esta capacidad se ha visto limitada en el CCE, por diversos factores: como estructurales y doctrinarios, entre ellos la escasez de personal especializado, ausencia de marco normativo, deficiencias de interoperabilidad tecnológica, y el rápido avance de amenazas cibernéticas, impactando en la eficiencia y eficacia operativa.

Como indican Zambrano y Tamayo (2024), las tecnologías de información y comunicaciones son hoy componentes activos de la defensa, y su adecuada integración no solo incrementa la capacidad de reacción, sino que también eleva el prestigio y proyección de las Fuerzas Armadas (p.162). bajo esta perspectiva comprender el rol del CCE, implica analizar su estructura, capacidades y aporte a las Operaciones de información que realiza el Ejército.

Esta investigación surge de la percepción que tiene el personal militar en relación con el desempeño del CCE, con el propósito de identificar los factores y su aporte a las OI durante el año 2024. Su objetivo principal es Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024, considerando las dimensiones nivel de actividad, la capacitación y entrenamiento en ciberseguridad, el desarrollo y aplicación de estrategias de ciberdefensa, y la eficiencia y eficacia institucional.

El estudio se contextualiza en un enfoque cuantitativo, con el uso de instrumentos validados para captar la percepción del personal militar sobre el desempeño del CCE en el contexto de las OI. La metodología seleccionada permitió identificar relaciones significativas entre variables consideradas fundamentales, a partir de la construcción de evidencia

empírica que sustentó las propuestas de mejora para la percepción del CCE y su aporte a las OI.

La tesis se divide en seis capítulos. En el Capítulo I, se presenta la declaración del problema junto con los objetivos y la hipótesis, y se proporciona la justificación del estudio en su esquema como dimensiones social, institucional, teórica y práctica. El Capítulo II contiene la descripción del marco teórico que incorpora los antecedentes nacionales e internacionales, así como fundamentos doctrinarios sobre ciberdefensa, operaciones de información y evaluación institucional. En el Capítulo III, se explica con mayor detalle la metodología de investigación, especificando el tipo de estudio, la población, muestra y las técnicas y herramientas para la recolección y procesamiento de datos. El Capítulo IV presenta los resultados obtenidos dentro de las dimensiones e hipótesis especificadas. Esos resultados se discuten en el Capítulo V en relación con la teoría y otros estudios relevantes que permiten evaluar el impacto institucional de esos resultados. Finalmente, se extraen los pensamientos finales, conclusiones y recomendaciones que buscan fortalecer el CCE como el punto focal desde el cual se desarrollará un enfoque estratégico integral de ciberdefensa para el Ejército del Perú, formulando una Matriz de indicadores de Ciberdefensa, concebida como una herramienta para medir, evaluar y mejorar el desempeño del CCE, dentro del marco de las OI.

Esta tesis busca contribuir al desarrollo de una doctrina de ciberdefensa más integral sugiriendo modificaciones específicas relacionadas con la eficiencia operativa e informacional del CCE. En un entorno donde las amenazas cibernéticas evolucionan con rapidez e impactan directamente con la seguridad nacional. Robustecer el CCE no solo constituye una necesidad militar, sino que también es un imperativo estratégico y doctrinario para garantizar la soberanía digital del Estado.

Esta tesis busca demostrar que las operaciones del centro de ciberdefensa contribuyen directamente en la generación de operaciones de información, así mismo busca mejorar la forma de asignar tareas y poder medir las mismas empleando KPI’s que permitan mejorar la eficiencia de los procesos y la eficacia de los productos o resultados que deseamos obtener por el centro de ciberdefensa.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1 Descripción de la Realidad Problemática

En la actualidad, el escenario global enfrenta diversos tipos de conflicto donde el concepto de Defensa Nacional ha debido de ampliarse hacia nuevas dimensiones especialmente a la perspectiva tecnológica y la necesidad de mantener una conectividad global en tiempo real. En ese contexto, el ciberespacio se ha convertido en un nuevo dominio en donde las operaciones cibernéticas realizada por diversos actores estatales como no estatales (Rutz, 2021). En este contexto, los ataques y las campañas de desinformación se han convertido en acciones de sabotaje digital, situando a la ciberdefensa como un componente esencial de la seguridad nacional y obligando a los Estados a modernizar doctrinas, técnicas y marcos normativos.

A estos cambios, potencias como Estados Unidos, China y Rusia han tomado la iniciativa. Por su parte, la Organización de Tratado Atlántico Norte (OTAN) también ha declarado importantes avances, estableciendo al ciberespacio como un dominio operativo, reafirmando que un ciberataque a gran escala podría activar los mecanismos de defensa colectiva.

En el caso de América Latina, el desarrollo de capacidades de ciberdefensa tuvo un avance muy lento, pero varios países comenzaron a institucionalizar funciones de ciberdefensa dentro de sus sistemas de seguridad. En Perú, se promulgó la Ley de Ciberdefensa Nº 30999 en el año 2019 que, en conjunto con la Estrategia Nacional de Ciberseguridad, constituía el marco normativo para la defensa nacional en el ciberespacio y establecía los lineamientos para la protección de infraestructuras críticas (Torres y Albújar, 2024). A nivel militar, se creó el Centro de Ciberdefensa del Ejército (CCE) como unidad especializada cuya misión es garantizar la seguridad de los sistemas informáticos del Ejército del Perú. Sin embargo, en la práctica, el operacional del CCE presentaba deficiencias que lo hicieron poco efectivo en el aprovechamiento de los defensivos digitales a pesar del marco legal existente.

Desde una dimensión institucional, se evidenció que el CCE tuvo una serie de problemas interrelacionados de carácter estructural y funcional: faltante de personal calificado, escasa dedicación de recursos a los sistemas tecnológicos, una nula cohesión doctrinal y pobre cooperación con otras unidades operativas (Félix y Suñagua, 2013). Estas deficiencias de orden institucional tuvieron el mayor impacto en el desempeño de las Operaciones de Información, donde su función debería haber sido fundamental. Pese a la normativa impulsada, no se consolidó una cultura operativa robusta en ciberdefensa que

posibilitara el diseño de un plan coordinado ante contingencias cibernéticas internas o externas.

Durante un período aproximado de cinco años, se identificaron problemas de vulnerabilidad y demoras en la respuesta ante incidentes informáticos dentro del Ejército del Perú. Éstos afectaron la conexión con sistemas estratégicos como SISCOBAM, SISPER y las redes VSAT, que reportaban incidentes de vulnerabilidad y falta de respuesta en tiempo. La actividad del CCE fue productiva, sin embargo, limitada por falta de un sistema de monitoreo avanzado, sumado a la reducida capacitación del personal que integra los equipos de respuesta de ciberdefensa, afectando la eficacia operacional y aumento de los riesgos de filtraciones, interrupciones o la manipulación de datos sensibles (Fonfría y Duch, 2020).

Este problema se viene suscitando periódicamente dentro del CCE, por no tener claramente definidos los objetivos y metas por conseguir dentro del ámbito de la ciberdefensa, a pesar de estar concebido como uno de los problemas más grandes para las organizaciones militares las operaciones de redes informáticas, resulta inverosímil creer que el CCE no han definido claramente sus objetivos y metas habiendo priorizado el cumplimiento financiero y administrativo, lo cual ha reducido al mínimo el cumplimiento de metas operativas relacionadas a los ataques, respuestas, explotación del ciberespacio y análisis forense; no existiendo métricas de seguimiento o cumplimiento de objetivos que le permitan mejorar tanto la eficacia de los resultados como la mejora del proceso, esto a su vez no les permite orientar claramente las acciones y actividades que deben realizar para alcanzar una efectividad plena en el cumplimiento de su labor.

Las Operaciones de información (IO) dentro del ámbito estratégico requiere ampliamente el trabajo de CCE, como parte de la capacidad de Operaciones de Informática, sin embargo; esto se viene afectando por la deficiente productividad de actividades de ciberdefensa al no tener claro que estos productos o resultados deben contribuir en las operaciones de información (IO) y permitir la toma de decisiones por parte del comando. Al no contar con “Indicadores Claves de rendimiento” (KPI) el CCE, se enfrenta a un futuro incierto que no le permitan la mejora continua, establecer metas claras relacionadas a las operaciones de información, mejorar el uso de recursos y aumentar la productividad de ciberdefensa.

1.2 Formulación del problema

1.2.1 Problema General

¿En qué medida el Centro de Ciberdefensa del Ejército (CCE) aporta a las Operaciones de Información en el Ejército del Perú durante el año 2024?

1.2.2 Problemas Específicos

¿Qué factores influyen en el nivel de actividad del Centro de Ciberdefensa del Ejército (CCE) que se relacione con las Operaciones de Información en el Ejército del Perú durante el año 2024?

¿En qué medida el nivel de capacitación y entrenamiento en ciberseguridad del Centro de Ciberdefensa del Ejército (CCE) influye en la eficiencia de su aporte a las operaciones de información en el Ejercito del Perú?

¿Cómo contribuye el desarrollo y aplicación de estrategias de ciberseguridad en el Centro de Ciberdefensa del Ejército (CCE) a la eficacia de las Operaciones de Información en el Ejército del Perú?

1.3 Objetivo de la investigación

1.3.1 Objetivo general

El objetivo general de esta investigación es: Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024.

1.3.2 Objetivos específicos

Los objetivos que nos permitirán llegar al objetivo general son: Analizar los factores que influyen en el nivel de actividad del CCE en las Operaciones de Información en el Ejército del Perú durante el año 2024.

Determinar el nivel de capacitación y entrenamiento en ciberseguridad del CCE y su influencia con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú durante el año 2024.

Evaluar como el desarrollo y aplicación de estrategias del CCE en la ejecución contribuyen a la eficacia en las Operaciones de Información en el Ejército del Perú durante el año 2024.

1.4 Justificación de la investigación

1.4.1 Justificación teórica

Desde el punto de vista teórico, esta investigación se basa en la necesidad de adaptación para ampliar el marco conceptual respecto a la ciberdefensa militar y su conexión con las Operaciones de Información (OI) (García, 2017). A pesar de la extensa literatura internacional sobre guerra cibernética, ciberseguridad y conflicto híbrido, existe una falta de investigación sistemática sobre estos temas en el contexto peruano. Particularmente, en la relación entre el Centro de Ciberdefensa del Ejército (CCE) y la

infraestructura informática del Ejército del Perú y su relación con la efectividad y eficiencia de las Operaciones de Información, las cuales no ha sido profundamente estudiado. Este estudio buscó abordar esta brecha de conceptos doctrinales, estrategias militares elaboradas y marcos evaluativos que analizan cuantitativamente el rendimiento del CCE desde perspectivas integrales. Además, este estudio propone construir un marco teórico que sirva para futuras investigaciones sobre ciberdefensa en el contexto militar, brindando definiciones claras, dimensiones analíticas y criterios de evaluación aplicado a unidades militares de otras ramas de las Fuerzas Armadas o del sector Defensa en su conjunto. En ese sentido, esta tesis servirá como un recurso valioso destinado a avanzar en la literatura sobre gestión estratégica de la ciberdefensa en países en vías de desarrollo.

1.4.2 Justificación práctica

En el ámbito práctico, como indica Pampa Urieta (2023), es necesario identificar los factores que afectan el funcionamiento efectivo del CCE dentro del marco de operaciones de información del Ejército, así como, la evaluación del nivel de actividad, eficiencia y efectividad del CCE, así como otros parámetros relevantes, lo cual proporcionará insumos concretos para la mejora de procesos, reestructuración operativa y toma de decisiones, todo ello destinado a mejorar las capacidades de respuesta del CCE ante amenazas cibernéticas.

De igual manera, el estudio de Zamorato (2022) nos ofrece criterios, objetivos y evidencia empírica que pueden ser utilizados por el Comando del Ejército, el Estado Mayor Conjunto y las Divisiones de Planificación Estratégica para rediseñar estrategias, reasignar recursos de una manera más eficiente, priorizando en inversiones tecnológicas y crear mecanismos de coordinación y control interinstitucional ante amenazas de ciberataques que evolucionan rápidamente, para contar con diagnósticos exactos y propuestas fundamentadas en datos reales es fundamental para la acción inmediata.

1.4.3 Justificación social

Desde la dimensión social, esta investigación atiende a una necesidad esencial del Estado: proteger la información en el uso de sus mecanismos en función de salvaguardar el interés nacional. Aunque la ciberdefensa pueda parecer un ámbito restringido a lo técnico-militar, su funcionamiento íntegro resguarda activos estratégicos que impactan significativamente en la estabilidad institucional, la confianza de los ciudadanos y en la defensa de la soberanía nacional (Cásale, 2022).

Un CCE fortalecido no solo mejora la seguridad operacional del Ejército, sino también la salvaguarda de los sistemas logísticos, las comunicaciones de emergencia y

otras plataformas empleadas en operaciones de apoyo a la población en desastres, acciones contrarias a amenazas transnacionales, o misiones de mantenimiento de la paz. Así, la mejora de las funcionalidades de los centros de mando operacional modernos C4i (CCE 4i) también contribuye a proteger a la sociedad peruana de vulnerabilidades orquestadas digitalmente que impactan en la vida civil.

1.4.4 Justificación metodológica

Justamente desde la metodología, el estudio se justifica por su diseño cuantitativo, correlacional no experimental, el cual posibilita establecer relaciones objetivas entre las variables más estratégicas como: grado de actividad, eficiencia y eficacia del CCE y su influencia en las órdenes de emisión (OI) correspondientes (Rodríguez et al., 2021). La aplicación de instrumentos validados y el empleo de técnicas estadísticas como el coeficiente de correlación de Pearson aseguran la rigurosidad del análisis, posibilitando resultados medibles, reproducibles y comparables en otros contextos institucionales (Hernández - Sampieri y Mendoza, 2018). Este enfoque metodológico, se encuentra centrado en la percepción del personal militar que participa en operaciones de ciberdefensa, también busca innovar en relación con asuntos de defensa, ya que combina la experiencia práctica con un análisis técnico-científico, transformando la opinión del personal en una fuente primaria de información de especialistas.

1.4.5 Justificación institucional

La relevancia institucional del estudio es estratégica dirigida al Ejército del Perú, como a otros IIAA, que está experimentando una transformación progresiva en términos de digitalización y modernización de sus capacidades militares. En ese sentido, la mejora del CCE (Centro de Ciberdefensa del Ejército) es importante para asegurar la ciberseguridad de sus sistemas y la eficiencia operacional en el dominio de la información (Maximiliano et al., 2024).

Esta investigación proporcionará al alto mando una evaluación del estado actual del CCE, cuáles son sus principales limitaciones y recomendaciones dirigidos a la optimización de la estructura del CCE junto con procesos de gestión, así como de recursos humanos y tecnología. Así, el objetivo es contribuir al desarrollo de una doctrina militar para la ciberdefensa que responda a los paradigmas de conflicto en evolución y esté alineada con los estándares de seguridad internacional.

1.5 Viabilidad de la investigación

La viabilidad específica de la investigación actual se basó en la disponibilidad y asignación de información, recursos logísticos y humanos para su efectiva implementación. Los investigadores tuvieron acceso a fuentes de información primaria a través de encuestas estructuradas con personal militar del Ejército del Perú que estaban funcionalmente

relacionados con el Centro de Ciberdefensa del Ejército y participaron en Operaciones de Información. Su aporte se complementó con documentos secundarios de naturaleza doctrinal, normativa y científica de expertos nacionales y extranjeros para proporcionar el marco teórico relevante para la investigación. Además, el acceso a bases de datos institucionales, manuales operativos e informes internos brindó la oportunidad para un análisis contextualizado, preciso y actualizado.

La investigación fue ejecutada cuidadosamente de acuerdo con el presupuesto y tiempo establecido en el cronograma académico. Para las actividades de recolección de información, análisis estadístico, así como la redacción de informes, se aplicaron técnicas que no requieren costos adicionales, tales como herramientas digitales de acceso libre y software ya poseído por el investigador. Esta distribución de tareas redujo la logística externa y, por tanto, autonomía, lo cual asegura que el estudio se complete sin retrasos. También, la naturaleza del enfoque cuantitativo y el diseño no experimental facilitaron la realización del trabajo de campo de una manera organizada, respetando el horario institucional de los empleados involucrados.

El investigador se preparó intelectualmente para los fenómenos en el estudio al poseer las competencias requeridas que incluían un trasfondo profesional militar, experiencia en gestión organizacional y conocimientos profesionales en seguridad informática. Su conocimiento previo sobre la estructura y funcionamiento del Ejército Peruano le ayudó a entender el área operativa del CCE y a desarrollar instrumentos contextualizados relevantes. Además, hubo apoyo institucional para obtener la información necesaria y contactar a los participantes de la muestra dentro del marco de ética, confidencialidad y respeto jerárquico. Juntos, estos aspectos aseguraron la viabilidad del estudio desde las perspectivas metodológica y organizacional, cumpliendo rigurosamente con los objetivos articulados.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes nacionales

Rivero (2023), en su artículo académico Ciberdefensa: Los Desafíos del Mundo Virtual, llevó a cabo un análisis doctrinal y estratégico relacionado con los problemas nacionales de ciberseguridad, considerando las amenazas emergentes en el ciberespacio en relación con la seguridad y soberanía del estado peruano. Su estudio se centró en la evolución de las Tecnologías de la Información y la Comunicación (TIC) y la creciente utilización de estas tecnologías en los sectores clave del país, que han escalado las vulnerabilidades a las amenazas cibernéticas. A través de su investigación teórica y normativa, el autor criticó el marco legal que rige a las Fuerzas Armadas, especialmente el cumplimiento del Artículo 51 de la Carta de la ONU, la adhesión a la Declaración Universal de Derechos Humanos (DDHH) y el Derecho Internacional Humanitario (DIH). El estudio identificó el punto débil de los sistemas digitales institucionales como el problema central; estos sistemas son susceptibles a ciberataques, que podrían escalar al grado de emergencia nacional. También pudo describir las operaciones militares a través del ciberespacio, relatando los casos en el que el país fue atacado por ciberdelincuentes, y enfatizó la necesidad de mejorar las capacidades de respuesta del sector. Dentro de sus principales contribuciones, hizo recomendaciones centradas en la mejora de la detección y neutralización de ciberataques, incluyendo la necesidad del desarrollo de doctrina, la capacitación especializada del personal y la inversión sostenible en tecnologías para la defensa digital. Este contexto es relevante para la investigación actual porque ofrece un marco conceptual sobre los desafíos de la ciberdefensa en Perú y justifica la necesidad de analizar el papel del Centro de Ciberdefensa del Ejército (CCE) en el apoyo a las Operaciones de Información y los factores que limitan la efectividad y eficiencia operativa.

Quevedo (2023), en su artículo académico Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional, realizó un estudio analítico y doctrinal centrado en la capacidad operativa de las Fuerzas Armadas en relación con las amenazas a la seguridad nacional en forma de ciber perturbaciones. Aunque el autor desarrolló su investigación desde una realidad peruana, el trabajo fue considerado un precedente internacional debido a su comparación con modelos extranjeros y discusión de estándares internacionales de ciberseguridad y defensa. El estudio abordó los problemas que enfrentan

los estados y, específicamente, sus instituciones militares, en la prevención, detección y neutralización de ciberataques organizados provenientes de actores estatales y no estatales. Esto se realizó mediante un análisis crítico del entorno digital global y el marco legal internacional existente. El estudio también destacó ciertas brechas estructurales en la organización de la ciberdefensa en Perú, particularmente la ausencia de un sistema civil-militar integrado, bajos niveles de interoperabilidad entre dominios y la falta de doctrinas operativas en el ciberespacio. Como parte de su análisis comparativo, el autor estudió las mejores prácticas internacionales de Israel, Estados Unidos y Estonia, enfatizando la necesidad de una estrategia nacional integrada, centros de ciberdefensa con independencia táctica y alta disposición técnica del personal militar. Como propuesta, sugirió enmarcar un sistema conjunto de ciberdefensa que incorporara a lo militar, sectores civiles especializados y agencias de inteligencia operando con una postura proactiva, reactiva y resiliente. Este contexto es fundamental para el desarrollo del presente estudio de caso porque ofrece un enfoque comparativo para entender el nivel de madurez actual del Centro de Ciberdefensa del Ejército del Perú (CCE) y sus deficiencias en relación con el marco de operaciones de información. También reafirma la necesidad de evaluar las capacidades operativas considerando los nuevos desafíos que plantea el dominio cibernético como un teatro operativo militar contemporáneo.

Huertas (2023), en su tesis denominada La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, realizó un estudio de investigación aplicada que examinó la vinculación entre la ciberdefensa y la gestión de la tecnología de la información en la Fuerza Aérea Peruana en su sede de Lima en el año 2022. Esta investigación empleó un enfoque cuantitativo con un diseño correlacional transversal no experimental no experimental, cuyo objetivo planteado fue medir el impacto de las capacidades de ciberdefensa en la eficiencia, seguridad y sostenibilidad de los sistemas de información institucionales. Para ello empleó, se administraron cuestionarios estructurados a una muestra representativa del personal técnico y administrativo en las unidades de tecnología e infraestructura digital de la Fuerza Aérea. En ese estudio se encontró una relación significativa y positiva entre la ciberdefensa y la gestión efectiva de tecnologías de información, especialmente en lo relacionado a la prevención de intrusiones, recuperación de incidentes y gestión de vulnerabilidades. Asimismo, el autor destacó las brechas existentes entre la política de seguridad digital y los planes operativos internos, lo que limitaba la capacidad de respuesta en tiempo real para contrarrestar amenazas cibernéticas. Como parte de las recomendaciones, indicó que es necesario fortalecer los protocolos de ciberdefensa, para ello es necesario regular las actualizaciones tecnológicas y crear marcos fortalecidos en planificación de contingencias los cuales deben de cumplir estándares de seguridad de las informaciones con certificación internacional. Este caso es

especialmente relevante para la investigación actual porque contribuye con evidencia empírica desde dentro del país sobre la importancia de la integración efectiva de la ciberdefensa en las operaciones de las Fuerzas Armadas. También apoya la hipótesis sobre la necesidad de evaluar sistemáticamente el centro de ciberdefensa del ejército (CCE) en su función como componente activo en el diseño y ejecución de las Operaciones de Información, que es el enfoque principal de esta investigación.

Dobbertin (2023), realizó una investigación aplicada, denominada Perfil profesional del personal militar que compone el Grupo de Operaciones Cibernéticas de la Fuerza Aérea Peruana en 2022. El estudio buscó establecer en qué medida las competencias profesionales del personal influían en la capacidad operativa de la unidad, especialmente en el ámbito de la ciberdefensa. El estudio utilizó un enfoque cuantitativo con un diseño no experimental y de alcance correlacional. Se aplicaron instrumentos de medición estructurados a una muestra de oficiales y especialistas en seguridad informática, inteligencia electrónica y administración de redes. Los resultados demostraron una correlación significativa entre el nivel de formación técnica del personal y el rendimiento general en tareas asociadas con la ciberdefensa. Específicamente, se encontró que el personal militar que estaba mejor capacitado en ciberseguridad, análisis de amenazas digitales y respuesta a incidentes tenía un rendimiento mejor en actividades de protección de infraestructuras críticas, detección de intrusiones y gestión de plataformas computacionales. Además, el estudio señaló vacíos asociados con una falta de estrategia para la formación continua del personal, la baja disponibilidad de programas educativos específicos a nivel militar y el escaso acceso a certificaciones técnicas reconocidas internacionalmente. Como parte de sus recomendaciones, el autor sugirió desarrollar un perfil profesional estandarizado para los miembros de las unidades de ciberdefensa, así como formalizar programas de formación técnica de nivel avanzado. Este antecedente es relevante para esta investigación porque ilustra cómo el factor humano impacta la efectividad operativa dentro de las unidades responsables de supervisar la ciberseguridad. También contribuye con factores críticos a contemplar respecto a la preparación y el trabajo realizado por el personal del Centro de Ciberdefensa del Ejército (CCE), particularmente en lo que concierne a su efectividad en defender y apoyar las Operaciones de Información Institucional que trascienden las fronteras definidas del Ejército Peruano.

Cadillo (2021), realizó un estudio de investigación aplicada, denominado La concientización en ciberseguridad y su relación con la seguridad informática en el servicio de informática de la Fuerza Aérea del Perú, 2020, cuyo enfoque fue evaluar el impacto de la conciencia sobre ciberseguridad en el nivel de seguridad informática del Servicio de Computo de la Fuerza Aérea Peruana para el año 2020. El estudio se situó dentro de un marco cuantitativo con un diseño no experimental, transversal y correlacional. El autor

intentó determinar el nivel de conocimiento, comprensión, adopción de medidas de protección de ciberseguridad aplicables y su impacto directo en las prácticas del personal militar y civil para salvaguardar los activos de información institucional a través de encuestas estructuradas administradas al personal técnico y administrativo en las áreas de sistemas, redes y soporte. Los resultados indicaron que había una correlación positiva significativa entre el nivel de conciencia del personal y la mejora de la seguridad informática. Más específicamente, los usuarios que estaban más informados sobre amenazas digitales, uso responsable de sistemas, gestión de contraseñas y respuesta a incidentes redujeron significativamente las vulnerabilidades operativas y frustraron infiltraciones o ataques externos. Sin embargo, también se identificaron vacíos críticos en la cultura de ciberseguridad institucional, que se deben a la escasa sensibilización colectiva dirigida a la ciberseguridad, la falta de protocolos vigentes, así como la baja contratación del personal en los programas para el adiestramiento en seguridad digital. Este antecedente resulta relevante para el presente estudio, porque evidencia el impacto que tiene la cultura organizacional y la capacitación institucional del personal en la efectividad de las medidas de ciberdefensa. Le permite reflexionar sobre la necesidad de cultivar más intensamente los factores humanísticos en el Centro de Ciberdefensa del Ejército (CCE) en lo que concierne a su impacto en la realización efectiva de las Operaciones de Información y en la defensa de los sistemas críticos del Ejército del Perú contra ciber amenazas emergentes.

2.1.2 Antecedentes internacionales

Cano (2024), en su artículo académico “Ciberdefensa basada en datos” realizó una investigación basada en la implementación de defensa cibernética, tomando como base, información obtenida para fortalecer la seguridad de las informaciones en marcos institucionales. Empleó una metodología analítica y descriptiva, el autor estudió el papel de los grandes datos y la analítica moderna en la facilitación de medidas proactivas y respuestas a ciberataques. Sus hallazgos se enfocaron en la necesidad de sistemas de monitoreo continuo y análisis predictivo, que permitan anticipar vulnerabilidades emergentes para diseñar estrategias en el ciberespacio con la suficiente antelación para reaccionar ante esos ataques. La investigación, aunque contextualizada ampliamente, consideró un escenario latinoamericano, destacando la urgencia de la defensa cibernética y que ésta sea activa para las instituciones públicas y privadas; y que se adopten paradigmas que prioricen eficiencia de datos y la planificación estratégica dentro del marco de toma de decisiones. Cano además señaló la importancia de especializar al personal en el uso de tecnologías de inteligencia artificial y aprendizaje automático para optimizar las operaciones de ciberseguridad. Por lo tanto, esta justificación proporciona un fuerte respaldo al estudio actual por los enfoques innovadores centrados en la gobernanza de datos que buscan

fortalecer el marco regulatorio de defensa cibernética. Además, enfatiza la necesidad de integrar tecnologías emergentes y capacidades analíticas avanzadas dentro del Centro de Defensa Cibernética del Ejército (CCE) para mejorar su efectividad en la detección y neutralización de amenazas en Operaciones de Información.

Locatelli (2023), en su tesis Ciberdefensa y ciberseguridad en las operaciones militares en el Comando de Operaciones de Defensa interna de Paraguay, evaluó las capacidades operativas y estratégicas para confrontar amenazas cibernéticas en la realidad militar paraguaya, prestando especial atención a sus activos críticos y la continuidad operativa de la institución. El autor empleó un enfoque descriptivo cualitativo incorporando análisis de doctrina y revisiones de marcos legales internacionales de ciberseguridad. El estudio destaca la necesidad no solo de una estructura organizacional adecuada, sino también de personal capacitado y políticas definidas en relación con la gestión de incidentes en el ciberespacio. Además señala que, los países de la región, como Paraguay, enfrentan obstáculos significativos referentes a la coordinación interinstitucional y el uso de tecnologías modernas y seguras. Además, enfatizó la necesidad de reforzar las operaciones de información como parte de la estrategia nacional de defensa global, proponiendo un modelo de defensa cibernética adaptado a la región considerando las peculiaridades del marco regional y los activos disponibles. Este contexto proporciona una perspectiva regionalmente relevante para el estudio actual en cuanto a que permite comparar y contextualizar el desarrollo chileno de capacidades de defensa cibernética en los países de América Latina, subrayando importantes desafíos compartidos y enfoques constructivos. Estas consideraciones podrían aplicarse para fortalecer el Centro de Defensa Cibernética del Ejército del Perú (CCE).

Girón (2021), en su tesis doctoral titulada Necesidad de una política nacional de ciberseguridad para infraestructuras críticas en Guatemala, desarrolla un análisis sobre la vulnerabilidad estructural del Estado guatemalteco frente a amenazas cibernéticas y la ausencia de mecanismos institucionales que aseguren la continuidad de los servicios nacionales. El autor plantea un enfoque analítico–propositivo orientado a demostrar que la carencia de políticas, capacidades técnicas y marcos normativos específicos impide que el país pueda responder adecuadamente a incidentes que afectan redes, sistemas críticos y procesos de toma de decisiones gubernamentales. Su estudio enfatiza que, sin una estructura de ciberdefensa consolidada, las instituciones públicas no logran proteger la disponibilidad, integridad y confidencialidad de su información, afectando tanto la gobernabilidad como la seguridad nacional.

Un aspecto central del trabajo de Girón Figueroa es la identificación de tres factores determinantes: la falta de doctrina técnica articulada a nivel nacional, la limitada formación especializada en ciberseguridad del personal responsable, y la obsolescencia de la

infraestructura tecnológica destinada a proteger sistemas críticos. El autor sostiene que estas brechas generan un entorno informacional altamente susceptible a ataques y campañas de desestabilización, lo que compromete la capacidad estatal para ejercer control sobre el dominio cibernético. En consecuencia, propone la formulación de una política nacional integral que fortalezca la protección de infraestructuras críticas y articule esfuerzos interinstitucionales mediante estándares técnicos, capacitación continua y mecanismos de coordinación estratégica. Estos hallazgos, guardan una relación directa con la presente investigación, dado que las debilidades observadas en Guatemala se asemejan a los desafíos identificados en nuestro país, así como al Ejército del Perú respecto al desempeño del CCE. Al igual que en el estudio guatemalteco, la evidencia de esta tesis demuestra que la percepción institucional sobre el CCE está fuertemente influida por factores como el nivel de actividad operacional, la capacitación especializada del personal y el grado de desarrollo de las estrategias de ciberseguridad. Asimismo, ambas investigaciones coinciden en que la eficiencia y eficacia de los esfuerzos de ciberdefensa determinan la capacidad del Estado —en este caso, del Ejército— para sostener Operaciones de Información en un entorno donde las amenazas informáticas adquieren protagonismo estratégico. En este sentido, el antecedente de Girón Figueroa refuerza el argumento de que la consolidación doctrinaria, el fortalecimiento de capacidades y la modernización tecnológica son condiciones indispensables para que el CCE se constituya en un habilitador efectivo del dominio informacional.

Realpe y Cano (2020), en su estudio Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia presentado en el Congreso Iberoamericano de Seguridad Informática, analizaron la evolución de las amenazas cibernéticas en América Latina y resaltaron el incremento de ataques complejos como ransomware, intrusiones APT y campañas de desinformación. Los autores adoptaron un enfoque estratégico, señalando que la región enfrenta riesgos crecientes debido a la limitada capacidad institucional para integrar vigilancia, defensa técnica e inteligencia en un sistema unificado de ciberseguridad. Asimismo, enfatizaron que la ciberdefensa moderna no puede entenderse únicamente como un mecanismo de protección tecnológica, sino como un componente habilitador de la seguridad nacional y de la gestión del entorno informacional.

Este antecedente se vincula directamente con la presente investigación, ya que coincide en destacar la importancia de contar con organismos especializados como el Centro de Ciberdefensa del Ejército del Perú capaces de sostener operaciones tanto defensivas como informacionales. Las conclusiones de Realpe y Cano respaldan la premisa central de este estudio: el desempeño del CCE depende de factores como la disponibilidad tecnológica, la capacitación del personal y la existencia de una doctrina consolidada,

dimensiones que se examinan empíricamente para determinar su relación con la eficiencia y eficacia de las Operaciones de Información. En ese sentido, su aporte confirma que el fortalecimiento de la ciberdefensa es indispensable para asegurar la superioridad informacional en el ámbito militar contemporáneo.

Olayinka (2020), en su tesis Ciberguerra y seguridad nacional en Nigeria: análisis de las capacidades de las Fuerzas Armadas para enfrentar las amenazas del ciberespacio, investigó a las capacidades de las Fuerzas Armadas de Nigeria para confrontar amenazas en el ciberespacio, midiendo el impacto de la guerra cibernética en la seguridad nacional. Empleó un enfoque cualitativo y descriptivo, este estudio examinó las acciones tomadas por el sector militar nigeriano para evitar riesgos cibernéticos, enfocándose en la preparación organizacional, la capacitación del personal y la infraestructura tecnológica. Este estudio reveló diversas brechas como la coordinación interinstitucional y la modernización de la tecnología en ciberseguridad que debilitaron la capacidad de respuesta ante amenazas. Sin embargo, destacó algunos esfuerzos realizados para mejorar la ciberseguridad a través de la adopción de políticas nacionales y la colaboración con organismos internacionales. La tesis enfatiza la necesidad de formular una doctrina que siga la línea de los planes estratégicos planteados para la defensa cibernética basados en dinámicas regionales y amenazas geopolíticas cambiantes. Este contexto, es relevante para el estudio que realizan los autores porque ofrece una perspectiva contrastando enfoques y marcos regulatorios de defensa cibernética internacional transfronteriza, especialmente en países en desarrollo con estructuras organizativas militares comparables a la nuestra. Además, contribuye con elementos para abordar las consideraciones necesarias respecto a las mejoras requeridas en el Centro de Defensa Cibernética del Ejército Peruano (CCE) en términos de su capacidad de respuesta ante amenazas cibernéticas en el ámbito de las Operaciones de Información.

2.2 Bases teóricas

La presente investigación se fundamentó en la teoría de la Convergencia Estratégica en el Ciberespacio, desarrollado en el Concepto de las Operaciones de Información habilitadas por ciberseguridad estudiada por Hatch (2019), este paradigma permitió explicar la relación funcional entre el Centro de Ciberdefensa del Ejército (CCE) y su aporte a las Operaciones de Información (OI). En la literatura empleada, la ciberdefensa se entendió como un componente que había evolucionado más allá del soporte técnico para consolidarse como un dominio operacional autónomo, vital para la seguridad nacional y para la conducción moderna de los conflictos (Clarke y Knake, 2019; Libicki, 2007). En el caso peruano, la creación del CCE respondió a los lineamientos estratégicos del Estado

orientados a fortalecer la protección de las infraestructuras críticas. Este marco operativo se fundamenta en la Ley N° 30999, Ley de Ciberdefensa (2019), y ha sido optimizado recientemente mediante el Decreto Legislativo Nº 1640 (2024), el cual introduce modificaciones para fortalecer las capacidades del Estado en el ciberespacio. Dichas normas se integran de manera sistémica con las funciones institucionales del Ejército del Perú, reguladas por el Decreto Legislativo N° 1137, permitiendo la articulación de la defensa tradicional con las nuevas exigencias de la seguridad digital

Desde esta perspectiva teórica, el aporte del CCE a las OI se explicó a partir de la relación entre sus capacidades internas y la eficacia institucional. De acuerdo con doctrina militar contemporánea, incluida la estadounidense, que sirve como referente funcional para el Ejército del Perú. Las OI dependen directamente de entornos digitales protegidos, información confiable y mecanismos integrados de defensa y respuesta (Departamet Of Defense, 2021). En consecuencia, el desempeño del CCE se entendió a través de cinco dimensiones clave, identificadas en la literatura: el nivel de actividad, vinculado al despliegue funcional, equipamiento e infraestructura; la capacitación y entrenamiento en ciberseguridad, orientada al fortalecimiento del capital humano; y el desarrollo y aplicación de estrategias de ciberseguridad, que comprende la actualización doctrinal y la implementación de medidas técnicas y operativas (Quevedo, 2023).

Asimismo, la teoría sobre eficiencia y eficacia institucional permitió comprender cómo el rendimiento del CCE influía en la capacidad del Ejército para operar en el entorno informacional. Según los enfoques administrativos clásicos, la eficiencia se refiere a la correcta utilización de los recursos y la eficacia al logro de los objetivos estratégicos (Chiavenato, 2011; Drucker, 2006). Ambos elementos, aplicados al contexto militar, se integran con la modernización estatal y la gestión orientada a resultados establecida en la Ley Nº 27658 (2001), que establece un marco normativo para la Modernización en la Gestión Pública.

En este contexto, se propone que la capacidad del CCE para sostener operaciones continuas, entrenar a su personal y actualizar sus estrategias determina directamente la efectividad de las OI y la superioridad informacional de la institución. Bajo estos fundamentos teóricos, el análisis realizado en esta investigación basado en la percepción del personal militar sobre el CCE permitió comprender cómo las capacidades internas del Centro condicionaron su rol como habilitador de las OI, reafirmando que la fortaleza percibida del CCE se traduce en una mayor eficiencia y eficacia dentro del dominio de la información del Ejército del Perú.

2.2.1 Centro de Ciberdefensa del Ejército

Según Chamorro (2023), el ciberespacio, como concepto, ha tomado forma a

medida que las tecnologías y las comunicaciones digitales evolucionan. No se trata únicamente de un espacio virtual o de la agregación de computadoras interconectadas, sino más bien de un entorno dinámico e intangible en el que fluye la información y donde se desarrollan actividades que impactan lo cotidiano y lo estratégico. Para Zamorato (2022), menciona que una red global sin límites físicos que integre sistemas informáticos, plataformas, dispositivos y usuarios en perpetua interacción, representa al ciberespacio.

En ese sentido Kasper et al. (2021) indica que el ciberespacio no solo se limita a hardware y software, sino también incluye reglas y normas que rigen las interacciones sociales, así como individuos y organizaciones conectadas a él; además, para los militares es un área operativa fundamental, un nuevo escenario que comprende desde simples comunicaciones hasta operaciones defensivas y ataques complejos, a través de medios remotos y automatizados.

Dado la naturaleza del ciberespacio: intangible y dinámico, su medición se realiza a través de evaluación perceptiva, estimando su actitud y comportamiento con relación a la operación y seguridad en este nuevo dominio. En ese contexto, se aplicará un cuestionario tipo escala Likert que ha probado su efectividad en las ciencias sociales y en estudios organizacionales que permite medir de manera cuantitativa la intensidad de oficinas o niveles de consenso en su respuesta a diferentes afirmaciones.

2.2.1.1 Teorías. Para poder comprender el ciberespacio como un nuevo teatro de guerra, es necesario tener en consideración algunas teorías que expliquen su origen y el impacto que tienen sobre la seguridad y defensa nacional, entre estas teorías las más importantes son el arte operacional, la cibernética y la teoría de la complejidad.

Para Zamorato (2022), la teoría relacionada al arte operacional aborda tanto el nivel estratégico - operacional. Por lo que, define que el ciberespacio no es solo un espacio virtual, sino también un dominio estratégico, muy al igual que la tierra, el mar o el aire. A su vez, indica que, al igual que en estos otros dominios, las fuerzas militares tienen la necesidad de desarrollar capacidades específicas para maniobrar y obtener ventajas. Esto nos permite comprender que la ciberdefensa no es periférica ni secundaria, sino un componente fundamental en la estrategia militar moderna (Cásale, 2022, p. 30). Para el Ejército, esto significa que el CCE debe gestionar las amenazas digitales con la misma seriedad y compromiso que otros tipos de operaciones reciben.

La teoría de redes enfatiza cómo se presenta el ciberespacio como una red ricamente compleja de nodos interconectados, como una telaraña por sobre la cual la información y las comunicaciones viajan (Poot, 2022, p.89). Dentro de esta telaraña donde se forman múltiples puntos críticos, existe la posibilidad de que una falla en uno de estos nodos críticos provoque consecuencias catastróficas para el sistema completo. Esta noción es fundamental para tener claro cómo priorizar los esfuerzos de defensa y asegurarse que

la falla estructural en la redundancia del sistema no resulte en la incapacidad de este a soportar ataques. Como todo sistema, es necesario definir las áreas que al ser atacadas generen un colapso en el sistema sin la necesidad de defender cada uno de sus niveles.

La teoría de la complejidad brinda un nuevo enfoque respecto al comportamiento del ciberespacio. Esta teoría argumenta que el ciberespacio es impredecible y, por ende, en constante transformación debido a su enorme volumen de elementos y la aceleración de cambios que lo caracterizan (Mora y Parra, 2021, p. 17). Esto no está limitado a una sola red sino es un sistema donde hay una interacción continua en todos los niveles. Esto permite que cada una de las acciones emprendidas da como resultado la posibilidad enfrentar resultados que no han sido anticipados. Por consiguiente, con la naturaleza del momento requiriendo más de uno, cada estrategia de defensa debe ser a la vez elástica, adaptable y en la capacidad de responder a las nuevas amenazas que pueden repetirse en el futuro además de aprender en cada intento en como realizarlo de manera más eficiente.

Estas tres teorías juntas nos acercan a entender que el ciberespacio ya es un dominio sofisticado que requiere una defensa especializada, inteligente y dinámica que pueda defender los intereses nacionales en un mundo interconectado y cada vez más frágil.

2.2.1.2 Dimensionamiento. El dimensionamiento del ciberespacio es útil para evaluar las capacidades operativas y estratégicas de las organizaciones que operan dentro de este dominio, y especialmente en el contexto militar como el CCE. Este proceso giró en torno a cinco dimensiones fundamentales: nivel de actividad, capacitación y entrenamiento en ciberseguridad en el CCE, desarrollo y aplicación de estrategias en el CCE, la eficiencia y efectividad de las OI.

a. Nivel de actividad. Se refiere a los niveles de frecuencia e intensidad de las operaciones realizadas en el ciberespacio, además del monitoreo constante de amenazas potenciales, la identificación y análisis de debilidades, posteriormente, la respuesta inmediata a incidentes de ciberseguridad, así como acciones defensivas y ofensivas, contramedidas orientadas a salvaguardar los sistemas de información (González, 2022, p. 10). Para Tafur (2022), un alto nivel de actividad demuestra que la entidad tiene capacidad operativa, y asertividad, así como una postura proactiva que es fundamental para sostener la integridad y disponibilidad de los activos digitales. También Oliveira et al (2025), indica que el nivel de actividad mide tanto la adaptabilidad del Centro de Ciberdefensa ante amenazas y la capacidad de predecir y prevenir ciberataques y, por lo tanto, refuerza su papel como el núcleo digital de las defensas del Ejército.

Es decir, un alto nivel de actividad en el ciberespacio es un indicador de eficiencia y resiliencia de las instituciones, por lo que posicionaría al CCE como un actor critico en la ciberseguridad. Este enfoque nos permite comprender que la ciberdefensa no solo se basa en respuesta a incidentes sino en la gestión continua, preventiva en el más alto nivel.

b. Capacitación y entrenamiento en ciberseguridad en el CCE. La capacitación cubre tanto la enseñanza teórica como práctica, ejercicios y simulacros de respuesta a incidentes, así como exámenes de certificación internacionales que validan los conocimientos y habilidades requeridas en seguridad informática (Dobbertin, 2023). El cambio y desafío presentado por nuevas y emergentes tecnologías, junto con tácticas adversariales nuevas, evolutivas, más sofisticadas, agresivas y maliciosas exige una educación y formación continua (Valencia et al., 2020). Un equipo bien entrenado no solo tiene la capacidad de responder de manera eficiente a un ataque, sino que también puede ayudar proactivamente a anticipar y defender a la institución, mejorando así la resiliencia institucional frente a amenazas digitales (Galushchenko et al., 2024).

Por lo tanto es de vital importancia la especialización del personal que desarrolla sus actividades en el CCE, de manera teoría y práctica, con certificaciones internacionales, y sobre todo que la capacitación sea actualizada, todo ello sumara para que el CCE sea resiliente a ataques cibernéticos.

c. Desarrollo y aplicación de estrategias de ciberseguridad en el CCE. El desarrollo de estrategias según la Presidencia de Consejo de ministros (2022) incluye la creación de políticas, doctrinas y procedimientos destinados a regular comprensivamente todas las acciones de defensa cibernética y promover la integración y cohesión en todos los niveles operativos. De la misma manera Villamil et al. (2020) manifiesta que la aplicación de estas estrategias se desarrolla en cada actividad de defensa cibernética en relación con los mecanismos internos de comando y control, así como la colaboración interinstitucional con otros actores civiles y militares.

De acuerdo con Calderón y Sánchez (2023), una estrategia efectiva engloba la previsión, el reconocimiento, la mitigación y la recuperación de incidentes, así como sistemas actualizados que afronten nuevas amenazas. Adicionalmente, dicha estrategia contempla la protección de infraestructuras críticas, la protección del intercambio seguro de información y la ciberseguridad, lo que permite conservar la ciberseguridad y la soberanía nacional.

2.2.2 Aporte a las Operaciones de Información

Para Percca (2024), las Operaciones de Información (OI) se han consolidado como un componente fundamental en el contexto de la guerra moderna y la seguridad nacional. La información es un bien esencial para el desarrollo de las actividades esenciales por lo que su control, protección e influencia sobre él pueden determinar el éxito o fracaso de una misión militar o de la política de un Estado (Cruz, 2019, p.15). Para el análisis que se está realizando sobre el papel que cumple en el Perú, en especial en su relación con el Centro de Ciberdefensa del Ejército (CCE) se necesita conocer los fundamentos teóricos, los

métodos de medición, la aplicación y sus dimensiones (Soares et al., 2025).

Según Lin y Kerr (2021), las Operaciones de Información son el conjunto de acciones coordinadas que tienen por objetivo influir, proteger y controlar la información y los sistemas relacionados, para apoyar la consecución de objetivos militares y estratégicos. Además, el Departamento de Defensa de Estados Unidos, indica que estas operaciones incluyen la guerra electrónica, las operaciones psicológicas, la seguridad de la información y las operaciones cibernéticas, entre otras (Díaz, 2022). En síntesis, buscan asegurar la superioridad informacional, es decir, la capacidad de manejar a voluntad la información para obtener ventajas sobre el adversario. En ese contexto, para el Ejército del Perú, las OI adquieren especial importancia como un medio para fortalecer la defensa nacional, contrarrestar amenazas híbridas y garantizar la integridad de las comunicaciones y el flujo informativo en entornos operacionales complejos (Percca, 2024).

Tratar de medir la efectividad de las Operaciones de Información (OI) presenta un desafío metodológico, porque los efectos no necesariamente son consistentes con una relación de causa y efecto palpable o un impacto observable. Sin embargo, hay estudios que nos permiten acercarnos y proporcionan una evaluación sistemática del rendimiento, particularmente para organizaciones militares que buscan medir la eficiencia de la actividad operacional, así como los niveles de influencia de las informaciones (Albornoz, 2024). Para los propósitos de este estudio, las mediciones se tomarán empleando un cuestionario estructurado basado en la escala de Likert dirigido a obtener información relevante del personal del Ejército sobre sus percepciones relacionadas con el desarrollo y la ejecución de las Operaciones de Información (OI) (De Lunetta y Guerra, 2023). Este instrumento evaluará el grado de influencia de las OI dentro de las operaciones militares, la preparación y formación del personal, la existencia de guías claramente definidas o doctrinas institucionales, la utilidad de las OI a nivel operacional y sus efectos percibidos en el adversario (Centurión y Rodríguez, 2023).

2.2.2.1 Teorías. Una de las teorías más relevantes que se ha tomado como base para este estudio es la de la guerra psicológica, ya que sostiene que la información puede ser utilizada para impactar la mente, emociones y decisiones del oponente, debilitando su moral, induciendo a la confusión y alterando a su comportamiento. Esto nos permite comprender cómo el lado contrario de las OI tiene un impacto más allá de lo técnico y puede influir en el estado de ánimo de las tropas enemigas o en el sentimiento público durante guerras híbridas (Villagra, 2024). En términos militares la guerra psicológica, tiene como objetivo no solo erosionar la voluntad del adversario, sino también mejorar la posición estratégica de nuestras fuerzas proyectando información e imágenes cuidadosamente elaboradas.

La teoría de la seguridad de la información brinda el cimiento necesario para las

acciones que se realizan resguardando la confidencialidad, integridad y disponibilidad de datos sensibles. En el ámbito de las Operaciones de Información, esta teoría resulta importante porque garantiza el desarrollo continuo de procesos operativos, sin interrupciones, filtraciones o manipulaciones (Jiménez y López, 2023). En ese sentido, mantener sin interrupciones las OI se torna efectiva al considerarse que, la pérdida de información crítica o exposición de planes anularía cualquier ventaja estratégica construida. Estas teorías abordan las Operaciones de Información como un campo multidimensional que fusiona elementos psicológicos con tecnología y estrategia, integrando la ejecución técnica con conocimiento doctrinario y coordinación institucional (Torres et al., 2022).

2.2.2.2 Dimensionamiento. Onetto (2024), determina que dimensionar las OI permite definir el verdadero nivel de desarrollo digital y los indicadores de rendimiento operacionales dentro de cualquier aparato militar (p. 65). Al mencionar al Ejército del Perú, su estudio se vuelve determinante para entender hasta qué punto estas operaciones están internalizadas, su capacidad de respuesta y su impacto general en el entorno operativo. En este caso, para lograr la precisión se requiere de dos dimensiones interrelacionadas entre sí: nivel de eficiencia y nivel de efectividad. Ambos permiten no solo examinar la disponibilidad de los activos y recursos necesarios, sino también la asignación y los resultados obtenidos en las operaciones de información.

a. Nivel de eficiencia. El nivel de eficiencia en las Operaciones de Información se define en la capacidad de hacer uso de los recursos disponibles tales como tiempo, personal, tecnología y la infraestructura digital en el momento preciso (Rodríguez-Barboza et al., 2024). Así mismo, se necesita tomar medidas con relación a las OI que se alineen con los planes a nivel operacional o estratégico, minimizando así posibles eventos en contra de las OI. La fluidez que caracteriza a las operaciones de información eficientes son el bajo número de errores de ejecución, así como la respuesta a lo cambiante del entorno informacional. Para determinar este nivel, es necesario observar la definición de procesos, existencia de normativa, calidad de los trabajos en sinergia, así como la formación del personal asociado y la selección de los recursos técnicos y digitales a emplear (Betancur, 2023).

Así como en los procesos o procedimientos informacionales, la eficiencia define que se brinde respuesta a eventos inesperados. En este sentido, el Centro de Ciberdefensa del Ejército (CCE) cumple un rol clave en la asignación de recursos comunicacionales e inteligencia como facilitador técnico y doctrinario. Una unidad eficiente es aquella que se toma el cuidado no solo de planificar, sino también de una ejecución correcta de la misma, utilizando herramientas y capital humano sin sobrecargas o demoras (Jiménez, 2023).

b. Nivel de eficacia. En este caso, la efectividad trata sobre el logro de los efectos deseados por las Operaciones de Información en la audiencia objetivo o en el entorno operativo. Mientras que la eficiencia se enfoca en el cómo del procesamiento, la efectividad analiza el por qué se hizo y qué se ha logrado (Bolaños, 2020). Dentro del contexto militar, se considera efectiva una campaña operacional de información cuando ayuda directamente a alcanzar objetivos tácticos u operacionales, cambia positivamente la percepción del entorno, influencia adversamente la toma de decisiones o mejora la moral y la cohesión dentro de la fuerza.

La evaluación de la efectividad requiere monitorear el impacto de la información enviada, verificar si hay algún cambio de actitud o comportamiento hacia la institución objetivo, y analizar la reputación narrativa institucional en el espacio informativo (Sales et al., 2017). Estos incluyen operaciones de influencia, contrainformación, defensa de la imagen institucional y protección del personal militar frente a un entorno cognitivo manipulado. La efectividad también se demuestra en la capacidad de predecir y tomar contramedidas contra campañas de información diseñadas de manera hostil (Guerrero et al., 2022).

2.3 Marco conceptual

El marco conceptual sirve como guía para el desarrollo de la investigación ya que permite delinear con precisión los conceptos claves, sus dimensiones y relaciones para erigir un fundamento que posibilite la elaboración de un análisis y posterior comparación de resultados. En el caso de esta tesis, el estudio está centrado en el Centro de Ciberdefensa del Ejército (CCE) en su papel de soporte para las Operaciones de Información (OI), lo que demanda comprender con precisión qué es el ciberespacio, la ciberdefensa, la eficiencia, la eficacia y las operaciones de información y cómo estos elementos interrelacionan atributos dentro de un contexto institucional y operacional.

En este sentido, se entiende el concepto de ciberespacio como un entorno global y virtual compuesto por redes interconectadas, dispositivos digitales y plataformas de información, donde se llevan a cabo actividades técnicas, sociales, comerciales y militares. Para Huaman (2021), en la defensa, el ciberespacio es reconocido como un dominio operacional al igual que la tierra, el aire, el mar y el espacio, lo que significa que es susceptible a operaciones militares específicas, como la vigilancia, la defensa o la acción ofensiva. En ese sentido los autores conceptualizan a este dominio, la defensa cibernética militar se refiere a la totalidad de capacidades, doctrinas, procedimientos y recursos destinados a asegurar los sistemas informáticos institucionales, mantener la confidencialidad y disponibilidad de la información y neutralizar amenazas. Esta

investigación asume que la ciberdefensa cumple no solo funciones técnicas, sino que tiene consecuencias estratégicas directas en la conducción de operaciones en la guerra de la información al proporcionar una plataforma segura, confiable y persistente desde la cual pueden llevarse a cabo estas operaciones.

Las operaciones de información, al igual que otras operaciones militares, se define como acciones planificadas y coordinadas destinadas a influir, proteger, interdictar o explotar la información y los sistemas de información para ventajas operativas o tácticas (Abarca y Barreto, 2020). En el Ejército Peruano, OI abarca la gestión de la mensajería institucional, la mitigación de campañas de desinformación, la protección de redes de comunicación y la colaboración entre unidades para la defensa del entorno informático. En cuanto a esta tesis, a OI le asignamos dos dimensiones principales de análisis: la eficiencia, entendida como la ejecución de estas operaciones de manera oportuna dentro de un plazo razonable, coherentemente y con un gasto mínimo de recursos; y la eficacia, entendida como el grado en que tales operaciones logran sus objetivos, impactan al adversario o defienden la imagen de la institución de daños durante un conflicto informático.

De acuerdo con Maximiliano et al. (2024) sostiene que, el Centro de Defensa Cibernética del Ejército (CCE) se describe como la unidad especializada encargada de llevar a cabo la seguridad informática, la monitorización cibernética y el apoyo técnico en los niveles estratégico y operacional para el Ejército del Perú. En cuanto a su rol en la OI, no solo proporciona asistencia técnica, sino también doctrinal, ya que participa en la planificación, instrucción, protección de redes y el diseño de respuestas coordinadas a amenazas críticas dirigidas hacia las operaciones militares (Lin y Kerr, 2021). Por esta razón, esta tesis intenta determinar en qué medida el CCE contribuye de manera identificable y cuantificable al logro efectivo y eficiente de las Operaciones de Información.

Este marco teórico logra delimitar con precisión las variables del estudio: por un lado, la variable independiente, que en este caso es el aporte del CCE, estructurado en cinco dimensiones: nivel de actividad, ciberseguridad, capacitación y entrenamiento, aplicación de estrategias, eficiencia y eficacia en las OI; y, por el otro, la dependiente, que son las Operaciones de Información, que se dimensionan en términos de eficiencia y eficacia. Esta construcción debe facilitar el diseño del instrumento de recolección de datos, la ejecución del análisis estadístico posterior y la coherencia metodológica que debe primar en el planteamiento de hipótesis, objetivos e interpretación de resultados para garantizar la consistencia en la metodología. En otras palabras, el marco conceptual aquí descrito, además de identificar los ejes centrales de la investigación, explica lo indispensable para comprender cómo se relaciona la defensa en el ciberespacio con las nuevas guerras informacionales, y qué rol desempeña el Ejército del Perú en esta realidad tan dinámica.

2.4 Definición de términos

2.4.1 Amenazas cibernéticas

Se entienden como acciones hostiles orientadas a explotar vulnerabilidades en sistemas digitales con el fin de interrumpir, manipular o comprometer información y servicios esenciales. Agrupan actividades como intrusiones, software malicioso, fraudes electrónicos o ataques dirigidos de complejidad avanzada. En el entorno militar, estas amenazas se caracterizan por su potencial de afectar la continuidad operativa y la infraestructura crítica, especialmente en unidades que dependen de redes seguras para ejecutar tareas en el ámbito operacional.

2.4.2 Centro de Ciberdefensa del Ejército (CCE)

Unidad orgánica especializada responsable de prevenir, detectar, responder y gestionar incidentes de seguridad digital que afecten los sistemas de información del Ejército del Perú. Su actuación comprende vigilancia tecnológica, soporte a operaciones, gestión de incidentes y protección de infraestructura crítica. En esta investigación, el CCE se concibe como el componente técnico-operacional que habilita la ejecución segura de actividades informativas militares.

2.4.3 Centro de Ciberdefensa del Ejército y aporte a las operaciones de información

Expresa la contribución efectiva del CCE al asegurar el entorno digital en el que se desarrollan las Operaciones de Información. Este aporte se materializa cuando la unidad garantiza un espacio informacional confiable, reduce vulnerabilidades, integra capacidades técnicas y proporciona soporte para acciones de influencia, protección y control del flujo de información militar. La percepción sobre este aporte refleja el grado en que el personal reconoce su importancia para alcanzar efectos operacionales.

2.4.4 Ciberseguridad militar

Conjunto de políticas, procesos, tecnologías y prácticas orientadas a preservar la integridad, disponibilidad y confidencialidad de las plataformas digitales empleadas en defensa. Abarca capacidades preventivas, defensivas y reactivas destinadas a proteger redes, comunicaciones y sistemas de mando y control. Su función es crítica para sostener operaciones en todos los dominios y garantizar la continuidad operativa de las fuerzas militares.

2.4.5 Eficacia institucional

Hace referencia al grado en que una organización alcanza los resultados establecidos en su misión. En el caso del CCE, implica la capacidad de generar efectos tangibles en el éxito de las Operaciones de Información, asegurando que las acciones de defensa digital contribuyan decisivamente a los objetivos estratégicos del Ejército. La eficacia se evalúa mediante resultados medibles vinculados con el impacto operativo.

2.4.6 Eficiencia operativa

Corresponde al uso óptimo de recursos humanos, tecnológicos y procedimentales para cumplir funciones con el mínimo desperdicio. En el ámbito del CCE, se relaciona con la capacidad para gestionar incidentes, operar infraestructura digital y ejecutar tareas especializadas de manera oportuna y con adecuada asignación de insumos.

2.4.7 Gestión estratégica

Proceso mediante el cual una organización orienta sus actividades hacia el cumplimiento de su misión considerando capacidades internas y condiciones del entorno. Involucra la formulación de objetivos, la asignación de recursos y la evaluación permanente de resultados. En el contexto militar, la gestión estratégica permite articular capacidades tecnológicas, operativas y doctrinarias para enfrentar amenazas en constante evolución.

2.4.8 Infraestructura crítica

Conjunto de sistemas, plataformas, redes e instalaciones cuya alteración o destrucción generaría perjuicios severos para la seguridad nacional o la continuidad del Estado. Incluye activos militares relacionados con comunicaciones, mando y control, logística y protección de datos. Su defensa constituye una prioridad de la ciberseguridad nacional.

2.4.9 Nivel de actividad

Define el grado de ejecución real de las tareas asignadas a una unidad durante un periodo determinado. En esta investigación se entiende como la frecuencia y alcance de las acciones realizadas por el CCE en materia de vigilancia, respuesta a incidentes, soporte técnico y coordinación institucional. Representa un indicador del dinamismo operativo de la unidad.

2.4.10 Operaciones de Información

Conjunto de acciones desarrolladas para influir, proteger o controlar el entorno

informacional con fines militares. Integran capacidades como seguridad de la información, operaciones psicológicas, gestión de redes y acciones contra la desinformación. Su propósito es afectar la percepción, la toma de decisiones y la libertad de acción del adversario, protegiendo al mismo tiempo los sistemas propios.

2.4.11 Percepción institucional

Apreciación que tiene el personal respecto al desempeño, credibilidad y utilidad de una unidad dentro de la organización. Esta percepción influye en el compromiso, la aceptación de procesos y la valoración del aporte institucional. En el caso del CCE, refleja cómo el personal interpreta su rol como habilitador de las OI.

2.4.12 Seguridad de la información

Actividad continua orientada a resguardar datos y sistemas contra accesos no autorizados, pérdida, exposición o alteración. Comprende controles físicos, administrativos y tecnológicos para asegurar la confidencialidad, integridad y disponibilidad de la información. Es parte esencial de la gestión del riesgo en el entorno digital militar.

2.5 Formulación de las Hipótesis

2.5.1 Hipótesis General

El Centro de Ciberdefensa del Ejército (CCE) aporta significativamente a las Operaciones de Información en el Ejército del Perú durante el año 2024.

2.5.2 Hipótesis Derivadas

El nivel de actividad del CCE se relacionan de manera significativa con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú, 2024.

La capacitación y entrenamiento en ciberseguridad del CCE influye de manera significativa con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú, 2024.

El Desarrollo y aplicación de estrategias de ciberseguridad en el CCE aporta de manera significativa en la eficacia de las Operaciones de Información en el Ejército del Perú, 2024.

CAPÍTULO III: METODOLOGÍA

3.1 Enfoque de investigación

La investigación es de tipo cuantitativa, ya que pretende analizar de manera objetiva, sistemática y medible la contribución del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024. Ello es apropiado, ya que permite medir a través de datos numéricos lo que opinan y juzgan el personal militar que trabaja directamente en el CCE, convirtiéndolo en datos estadísticos susceptibles de comprobación de hipótesis.

En la recolección de datos se emplearán encuestas estructuradas, que han sido elaboradas en base a las dimensiones de los objetivos de la investigación: nivel de actividad, capacitación y entrenamiento en ciberseguridad en el CCE, desarrollo y aplicación de estrategias de ciberseguridad en el CCE, eficiencia y efectividad en el CCE, en apoyo a las operaciones de información. Estas encuestas irán dirigidas a oficiales, técnicos y suboficiales relacionados con el CCE, garantizando así una muestra representativa del fenómeno a estudiar. Luego, los datos serán analizados con estadísticas descriptivas para encontrar patrones, correlaciones y grados de asociación entre las variables estudiadas, como la preparación técnica del personal, la capacidad de respuesta del CCE y su coordinación con otras agencias de la defensa.

Hernández - Sampieri y Mendoza (2018), señala que el enfoque cuantitativo explica y predice fenómenos a través de pruebas estadísticas, logrando asegurar la validez y confiabilidad de los resultados obtenidos. En ese sentido, el empleo de este enfoque permitirá a esta investigación describir de manera descriptiva la situación en la que se encuentra el CCE, generando evidencia empírica para posteriormente poder concluir con base, y brindar recomendaciones aplicables y coherentes que permitan fortalecer la misión del CCE.

3.2 Tipo de investigación

Esta investigación se ha considerado del tipo aplicada, ya que se busca crear una base de conocimientos que sea útil en el tiempo, y sirva a otros investigadores sobre el CCE, y su aporte hacia Operaciones de Información. Zúñiga et al. (2023) indica que, la investigación aplicada está orientada sobre problemas específicos en un contexto definido y proporciona resultados que serán aplicables, en contraste a una investigación básica, que solo busca ampliar conocimiento teórico sin aplicación práctica.

Esta investigación tiene como objetivo examinar el aporte del CCE y su aporte a las Operaciones de Información en el Ejército del evaluando el nivel de actividad, capacitación y entrenamiento en ciberseguridad, desarrollo y aplicación de estrategias de ciberseguridad, eficiencia y efectividad del CCE en la ciberdefensa militar y proporcionar insumos estratégicos para la consideración en la toma de decisiones. En ese sentido, los hallazgos podrán ser empleado para desarrollar estrategias y políticas que servirán para mejorar las capacidades del Ejército del Perú en el dominio cibernético, fortaleciendo así el carácter aplicado.

3.3 Nivel de investigación

Esta investigación emplea el nivel correlacional, ya que, esta tipo de estudios permite examinar el grado de asociación entre variables previamente medidas y descritas, para luego ser cuantificadas y analizar la relación existente entre ellas, tal como lo señala Hernández - Sampieri y Mendoza (2108). De acuerdo con estos autores, los estudios correlacionales resultan útiles por que permiten participar el comportamiento de una variable con base en el comportamiento de otra que está vinculada, pudiendo estas relaciones ser positivas, cuando ambas variables aumentan de manera conjunta, o negativas, cuando el incremento de una implica la disminución de la otra.

En este estudio, se midieron las percepciones del personal militar sobre el CCE y sobre su aporte a las OI, ambos constructos evaluados mediante el instrumento validado por juicio de expertos, aplicado a la muestra poblacional de cincuenta y siete participantes. Posteriormente, estas variables fueron descritas y sometidas a un análisis correlacional para determinar su nivel de asociación. Este enfoque permitió identificar a los investigadores, en base a los datos recolectados, como variaba la percepción del aporte de las OI en función del desempeño percibido del CCE, lo que justificó plenamente la elección del nivel correlacional para responder al problema planteado.

3.4 Diseño de la Investigación

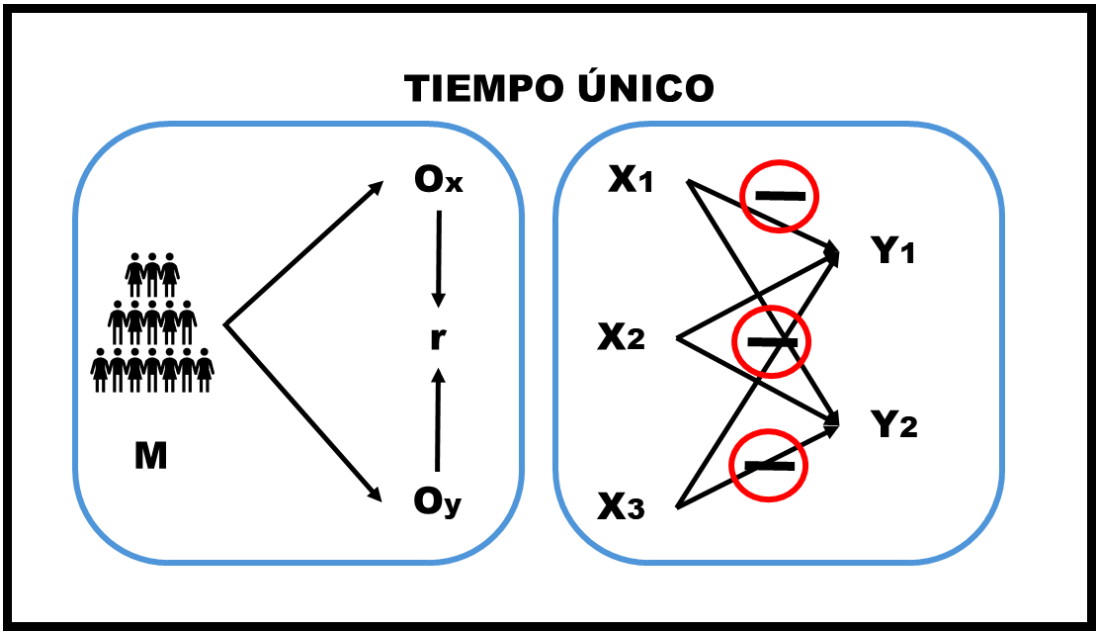
La investigación empleo un diseño no experimental, debido a que las variables analizadas, no pueden ser manipuladas de manera intencional así como sus dimensiones, tal como lo señala Hernández - Sampieri y Mendoza (2018), en los estudios no experimentales el investigador observa los fenómenos tal como ocurren en su entorno, sin que se pueda manipular porque éstos ya sucedieron. En ese contexto, el estudio de nivel de actividad, capacitación y entrenamiento y aplicación de estrategias se encuentran preestablecidas en la práctica que realiza el Ejército del Perú, por ello, el análisis se centró en recoger la percepción del personal y cuantificarlo, sin alterar las condiciones existentes.

Así mismo, el estudio adoptó un diseño transeccional correlacional, dado que la

recolección de datos se realizó en un único momento, mediante un cuestionario aplicado a cincuenta y siete integrantes del CGE. Este tipo de diseño permite describir simultáneamente las variables de interés y analizar el grado de asociación entre ellas. Para este caso, el diseño fue pertinente porque se buscó determinar cómo se comportaban las dimensiones del CCE, frente a los niveles percibidos de eficiencia y eficacia, en su aporte a las OI.

Figura 1

Esquema del diseño de la Investigación.



Nota. Ox= Variable 1 Centro de ciberdefensa del Ejército, Oy= Variable 2 Aporte a las OI, r=correlación entre las variables, todo ello tomado en un tiempo único a población muestral. X1,X2, X3, representan a las dimensiones de la Variable 1, Y1 y Y2, representan a las dimensiones de la variable 2. Fuente: Hernández - Sampieri y Mendoza (2018).

La aplicación de este diseño permitió identificar relaciones significativas entre las variables, tal como lo evidenció el análisis inferencia, donde se encontró una correlación fuerte y significativa ($r = 0.887$, $p < 0.001$) entre el CCE y su aporte a las OI, así como correlaciones específicas moderadas o muy fuertes entre sus dimensiones (actividad: $r = 0.572$; capacitación: $r = 0.839$; estrategias: $r = 0.840$). Estos resultados validaron la pertinencia del diseño correlacional, ya que permitió cuantificar de forma objetiva el comportamiento conjunto de las variables, determinando que a mayores niveles percibidos de actividad, capacitación y estrategias, correspondían mayores niveles de eficiencia y eficacia percibidas en el aporte a las Operaciones de Información.

3.5 Población y Muestra del Estudio

3.5.1 Población

La población es, según De Lunetta y Guerra (2023), “conjuntos de individuos con características comunes que habitan un mismo espacio” (p. 74) y, para evitar la complejidad que implica investigar una población en su totalidad, se recurre a la selección de una muestra. En este caso, la estrategia seleccionada no solamente ahorró recursos, sino que mejoró la exactitud y precisión de la información obtenida. En este caso, se utilizó el muestreo de tipo probabilístico, tomando en cuenta la variabilidad de horarios y lugares donde se trabajaba, así como la multifuncionalidad de los participantes.

Tabla 1

Población según jerarquía.

Jerarquía	Cantidad
Oficiales	21
Técnicos y Suboficiales	53
TOTAL	74

Nota. Se visualiza la muestra estratificada, tomada de acuerdo con el cálculo matemático, de los cuales se extraerán la información.

Con esto se quiere expresar que esta población es finita y, por lo tanto, accesible, lo que permite llevar a cabo un estudio directo y representativo de la situación específica analizada.

3.5.2 Muestra

La muestra se deriva de la población compuesta por dos estratos que se encuentran perfectamente definidos de acuerdo con su jerarquía institucional, por lo que se empleó un muestreo probabilístico estratificado proporcional con el fin de que cada grupo estuviera representado adecuadamente dentro del total poblacional. Este tipo de muestreo permite además reducir el error estándar y mejorar la precisión de las estimaciones al tener en cuenta la variabilidad interna de los estratos. La muestra fue calculada empleando la fórmula para poblaciones finitas:

$$n = Z^2 * p * q * N / [e^2 * (N-1) + Z^2 * p * q]$$

Donde:

- n = tamaño de la muestra
- Z = nivel de confianza 95 % (Z = 1,96)

- p = proporción esperada de la población con el atributo de interés (0,5)
- q = 1 – p = 0,5
- e = margen de error aceptado (0,05)
- N = tamaño de la población total (74)

Aplicando los valores mencionados, se obtuvo un tamaño de muestra de n = 57 individuos en total (De Lunetta y Guerra, 2023). Esta muestra fue distribuida proporcionalmente entre los dos estratos jerárquicos identificados.

Tabla 2

Población y muestra por estrato

Jerarquía	Población (N)	Porcentaje (%)	Muestra (n)
Oficiales	21	28.4 %	16
Técnicos y Suboficiales	53	71.6 %	41
TOTAL	74	100 %	57

Nota. Población total y muestra.

Esta muestra representa de manera proporcional y confiable a la población total y permite obtener resultados estadísticamente válidos, asegurando la representatividad de ambos estratos jerárquicos involucrados en la ejecución de tareas vinculadas a la ciberdefensa y operaciones de información.

3.6 Técnicas e Instrumentos de Recolección de datos

3.6.1 Técnica de Recolección de datos

La técnica de recolección de datos es una manera para recabar datos que serán trasformados en investigación para un estudio especifico. Rodríguez et al. (2021) plantea diversas ventajas en cuanto a las diversas metodologías, por la cual los investigadores pueden escoger la técnica que le ayude a entablar un mejor análisis para su estudio. Para esta investigación los autores emplearon una encuesta estructurada a través de medios informáticos como método principal para recolectar datos. Esta herramienta se aplicó a la muestra seleccionada, cuya dirección de enlace fue remitida a los correos electrónicos, en un momento determinado.

3.6.2 Instrumento de Recolección de Datos

Para la recolección de datos en la presente investigación, se empleó un cuestionario estructurado como principal instrumento de medición. Este cuestionario estuvo compuesto por preguntas cerradas en escala tipo Likert, lo que permitió calcular el nivel de acuerdo o

desacuerdo de los participantes, respecto al Centro de Ciberdefensa del Ejército (CCE) y su aporte en las Operaciones de Información del Ejército del Perú. La utilización de escalas Likert facilita la recopilación de información cuantitativa y su análisis mediante técnicas estadísticas (Hernández - Sampieri y Mendoza, 2018, p. 250).

El cuestionario se diseñó considerando las dimensiones de: nivel de actividad, capacitación y entrenamiento en ciberseguridad en el CCE, desarrollo y aplicación de estrategias de ciberseguridad en el CCE, eficiencia y eficacia del CCE. Cada dimensión incluyó indicadores específicos previamente definidos en la matriz de consistencia, con el fin de garantizar que la medición sea válida y (Hernández - Sampieri y Mendoza, 2018, p. 250). La administración del cuestionario se llevó a cabo de manera digital, con el objetivo de maximizar la tasa de respuesta y minimizar sesgos en la recolección de datos.

Tabla 3

Escala de Likert.

Alternativas según escala de Likert.	
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

Nota. Se representa los valores de 1 al 5. Fuente: Bazán, 2021.

3.7 Validez y confiabilidad de los instrumentos de medición

3.7.1 Validez

La validación del cuestionario en escala de Likert se realizó mediante juicio de cinco expertos, con la participación de especialistas en ciberdefensa, operaciones militares e investigación cuantitativa, Oficiales de gran trayectoria de conocimiento en el tema, de acuerdo con lo recomendado por Reyes (2022), este método permitió evaluar la claridad, coherencia y pertinencia de los ítems, asegurando que las preguntas reflejen convenientemente los constructos que se procuraron calcular.

Se les proporcionó el cuestionario junto a la matriz de evaluación diseñada para valorar los criterios actitudinales, de consistencia, intencionalidad, metodología, objetividad de organización y suficiencia, siendo válido para estos expertos, de acuerdo al coeficiente de V de Aiken, ya que según Reyes (2022), para cuantificar la validez del instrumento, el coeficiente de V de Aiken, permite determinar el grado de concordancia y la importancia de este coeficiente señalando valores superiores a 0.75, que es considerado como adecuado para aceptar la pertinencia del ítem.

3.7.1.1 Validez de Contenido (Índice de Validez de Contenido – CVR). Con la finalidad de que los ítems del instrumento de recolección de datos fuesen pertinentes y coherentes, con las dimensiones establecidas en esta investigación, se ha llevado una evaluación de validez de contenido, para ello se empleó el método de Índice de validez de Contenido (Content Validity Ratio – CVR) propuesto por Lawshe (1975), esta técnica permite cuantificar el nivel de consenso entre los expertos en base a la relevancia de cada ítem del cuestionario.

Para la realización de validez de contenido se solicitó el apoyo de un selecto panel conformado por cinco especialistas con una amplia experiencia en la especialidad de Comunicaciones, tecnología, así como en gestión pública, derecho militar, derecho administrativo, ciberdefensa institucional y planificación estratégica en contextos operacionales. A cada uno de los expertos se le solicitó evaluar los 27 ítems del cuestionario, indicando para cada uno si lo consideraban: (1) esencial, (2) útil pero no esencial, o (3) no esencial, la fórmula de Lawshe aplicada es la siguientes:

Donde N representa el número de expertos, se calculó el coeficiente CVR. Según

$$CVR = \frac{n_e - (N/2)}{N/2}$$

los estándares establecidos por Lawshe (1975), para un universo de cinco expertos, para ser considerado aceptable a un valor mínimo de CVR ≥ 0.62, para que un ítem sea considerado válido en términos de contenido. Los resultados que se han obtenido revelan que los ítems presentaron un CVR entre 0.80 y 1.00, lo que nos indica que existe un alto grado de consenso profesional, sobre su relevancia teórica y operativa. Sin embargo tres ítems registraron valores de CVR de 0.60, que se encuentran ligeramente por debajo del umbral, por lo que éstos fueron sometidos a una revisión y reformulación para la mejora de su redacción y posteriormente adecuarlo al marco institucional del Ejército del Perú. De manera general la calificación de los expertos, de manera cualitativa fue favorable.

Tabla 4

Relación de expertos y calificación

N°	EXPERTOS	CALIFICACION
01	Mg. FLORES MOZOMBITE Víctor Mahatma	Valido
02	Mg. ESPINOZA LUPUCHE Félix Junior	Valido
03	Mg. CACHO DE LA CRUZ Lizet Milagros	Valido
04	Mg. VIZARRETA PACHECO Daniel Gerardo	Valido
03	Mg ESPINOZA VELA Jorge Luis	Valido
	Promedio	Valido

Nota. Se muestra la calificación dada por los expertos.

El promedio CVR obtenido fue de 0.91, este resultado nos da a comprender que el instrumento presenta una alta validez de contenido, respaldando la opinión de los expertos. Esta calificación garantiza que el cuestionario es adecuado a las dimensiones que se han propuesto y que es pertinente para medir la percepción del desempeño del CCE en su aporte a las operaciones de información.

3.7.1.2 Validez estructural (Análisis Factorial Exploratorio – EFA). Se ha realizado la validez estructural del instrumento mediante la aplicación de un Análisis Factorial Exploratorio (EFA, por sus siglas en inglés), es una técnica estadística multivariada que permite a los investigadores identificar la estructura subyacente de los datos y verificar si los ítems del cuestionario se han agrupado adecuadamente en las dimensiones propuestas. Esta técnica resulta útil en investigaciones que buscan confirmar empíricamente la correspondencia entre ítems y los constructos que representan.

Antes del desarrollo del EFA, se comprobó la adecuación muestral a través del índice de Kaiser-Meyer-Olkin (KMO) y la prueba de esfericidad de Bartlett. El valor obtenido del índice KMO fue de 0.872, lo cual, según los criterios de Kaiser (1974), indica una adecuación meritoria para aplicar el análisis factorial (valores > 0.80 son considerados muy buenos). Por su parte, la prueba de esfericidad de Bartlett arrojó un valor de $\chi^2 = 1325.76$, $gl = 630$, $p < 0.001$, confirmando que las correlaciones entre los ítems son suficientemente significativas para proceder con la extracción de factores.

Para la extracción de los factores se utilizó el método de componentes principales (principal components) con rotación varimax, a fin de facilitar la interpretación de los factores y maximizar la varianza explicada por cada uno. El criterio de retención fue el autovalor mayor a 1 (criterio de Kaiser) y se complementó con el análisis del gráfico de sedimentación (scree plot). Los resultados del análisis factorial permitieron identificar cuatro factores principales, que en conjunto explican el 72.3% de la varianza total acumulada, lo cual es estadísticamente aceptable, ya que supera el umbral mínimo del 60% sugerido por Hair et al. (2014) para estudios en ciencias sociales. Cada factor agrupó ítems con cargas factoriales superiores a 0.60, confirmando una adecuada saturación y coherencia interna dentro de cada dimensión.

Los factores identificados coincidieron con las dimensiones teóricas propuestas en el diseño del instrumento, a saber: Nivel de actividad del CCE, capacitación y entrenamiento en ciberseguridad, desarrollo y aplicación de estrategias y percepción del aporte a las Operaciones de Información.

Este resultado evidencia que el instrumento no solo es válido en contenido (como se mostró en el CVR), sino que además posee una estructura factorial consistente con el marco conceptual, lo que permite afirmar que los ítems miden de manera confiable y diferenciada

los constructos latentes definidos en la investigación.

En conclusión, el análisis factorial exploratorio respalda la validez estructural del cuestionario y justifica su uso en la medición de percepciones respecto al rol y desempeño del Centro de Ciberdefensa del Ejército (CCE) en las Operaciones de Información, garantizando robustez metodológica y soporte empírico para los análisis estadísticos posteriores.

3.7.2 Confiabilidad

Para comprobar la calidad técnica y estadística del sondeo elaborado, se utilizó la confiabilidad Alpha de Cronbach, una estadística que intenta aproximar el grado de confianza que despierta un instrumento al medir su consistencia interna. Este índice es de especial interés en las pesquisas cuantitativas por determinar el nivel de correlación que existe entre los ítems que conforman una misma dimensión, lo que es necesario para comprobar que todos los subgrupos de preguntas realmente capturen el mismo concepto.

De Lunetta y Guerra (2023), indican que los rangos del Alpha de Cronbach deben de encontrarse en el parámetro de 0 y 1, donde los valores cercanos a 1 representan alta confiabilidad. Según la literatura experta, un puntaje inferior a 0.6 se considera deficiente, mientras que puntajes entre 0.70 y 0.90 indican una confiabilidad aceptable o buena. Resultados que superan 0.90 demuestran una excepcional consistencia interna, lo cual es especialmente importante en investigaciones aplicadas desarrolladas sobre poblaciones institucionales o técnicas, como es el caso de este estudio enfocado en personal del Ejército del Perú.

Al aplicar el coeficiente de Alfa de Cronbach, el resultado en la presente investigación fue de $\alpha = 0.974$ en relación con 27 ítems. Este valor es interpretado como un nivel de confiabilidad excelente, lo que implica que los ítems del cuestionario están correlacionados entre sí y, por tanto, están homogéneamente construidos respecto a las dimensiones del estudio. La consistencia interna obtenida refleja gracia en los detalles del instrumento en su redacción y, sobre todo, en la lógica bajo la cual fueron organizadas las preguntas por dimensiones (aporte del CCE, eficiencia, eficacia, nivel de actividad y estrategias de ciberseguridad). Esto también indica que los encuestados contablemente, al menos en los enunciados, los entendieron de la misma manera, validando, junto con los otros hallazgos, la validez del proceso de recolección de datos.

Tabla 5

Criterio de confiabilidad

Intervalo al que pertenece el coeficiente de Alpha de Cronbach	Valoración de la fiabilidad de los ítems analizados
“0 < 0.50”	Inaceptable
“0.50 < 0.60”	Pobre
“0.60 < 0.70”	Cuestionable
“0.70 < 0.80”	Aceptable
“0.80 < 0.90”	Bueno
“0.9 < 1”	Excelente

Nota. Intervalo de valores de Alpha de Cronbach.

Tabla 6

Estadísticos de confiabilidad del instrumento.

Alfa de Cronbach	N de elementos
0,974	27

Nota. Valor obtenido del alfa de Cronbach.

El instrumento ha sido diseñado con claridad para que la población muestral pueda comprenderlo, y se considera que es relevante y alineada a las variables de esta investigación. La encuesta ha incluido ítems relacionados al nivel de actividad, capacitación y entrenamiento en ciberseguridad, desarrollo y aplicación de estrategias de ciberseguridad así como la eficiencia y efectividad organizacional institucional en el contexto de las Operaciones de Información. El nivel de fiabilidad estadística alcanzado permite aplicar el instrumento a la muestra definida con confianza, asegurando que los resultados obtenidos serán significativos y relevantes. Por lo tanto, el valor alcanzado en el coeficiente Alfa de Cronbach ($\alpha = 0.974$) ha demostrado que la confiabilidad del cuestionario fue excelente, de acuerdo con los parámetros de la Tabla 5, garantizando la consistencia en la medición de los constructos teóricos definidos y su alineación con los objetivos, preguntas de investigación e hipótesis. En ese sentido, se aplicó la prueba de normalidad Kolmogórov-Smirnov y Shapiro-Wilk, los resultados mostraron que las variables se ajustan a una distribución normal ($p > 0.05$), lo que justifica el empleo de pruebas paramétricas como la correlación de Pearson.

De igual modo, se establecieron baremos de interpretación, los cuales permitieron categorizar los puntajes obtenidos en niveles bajo, medio y alto de percepción respecto al aporte del CCE a las Operaciones de Información, facilitando la interpretación práctica de los resultados. Finalmente, se elaboró la ficha técnica del instrumento, donde se especificaron sus características principales: 27 ítems distribuidos en cinco dimensiones

(actividad, capacitación y entrenamiento, aplicación de estrategias, eficiencia y eficacia), escala tipo Likert de cinco puntos, validez de contenido avalada por cinco expertos y confiabilidad medida estadísticamente. Estos elementos en conjunto aseguraron la validez y pertinencia del instrumento como herramienta de recolección de datos.

3.8 Técnica de Procesamiento y Análisis de Datos

3.8.1 Técnica para el Procesamiento de Datos

Al administrar el cuestionario a los Oficiales, Técnicos y Suboficiales del Ejército del Perú que forman parte de las unidades relacionadas con el CCE (Centro de Ciberdefensa del Ejército), realizamos una meticulosa edición de cada instrumento para comprobar que cada una de las respuestas se haya proporcionado de forma completa y precisa. Esta etapa de limpieza permitió verificar y omitir datos que eran inexistentes, incompletos o que contenían patrones de respuesta inválidos, lo que aseguró una base de datos fiable.

Como siguiente paso, se asignó códigos a cada respuesta del cuestionario, empleando la escala de Likert, asignando del 1 al 5 a cada ítem; donde 1 significa total desacuerdo y 5 significa total acuerdo. Este enfoque facilitó la comprensión y organización sistemática de los datos en el software estadístico. El procesamiento estadístico se ha realizado empleando el software estadístico IBM SPSS Statistics versión 26. Este software es reconocido por ser flexible para el análisis de datos cuantitativos, tanto para investigaciones del tipo ciencias sociales y militares.

Complementariamente, se empleó Microsoft Excel, para la organización primigenia y verificación cruzada, además de ser un interfaz sencillo que permite elaborar gráficos con datos estadísticos extraídos del SPSS Statitics versión 26. Para la validación final, se empleó de la base de datos realizada en el SPSS, cuyo trabajo de análisis fue la detección de valores atípicos, verificación de consistencia entre variables interrelacionadas y eliminación de errores causados por la entrada manual de datos; todo ello para evitar la manipulación deliberada de algún dato obtenido. Este proceso de limpieza de datos garantizó que la base de datos resultante no estuviese sesgada metodológicamente.

3.8.2 Análisis de datos

El análisis realizado a esta investigación se ha dividido en dos etapas: análisis descriptivo y análisis inferencial, con la finalidad de formular una explicación coherente y fundamentada con los datos obtenidos.

Análisis descriptivo. Como primera fase, después de aplicado el cuestionario, se calcularon las estadísticas descriptivas con relación a la base de datos obtenidos de la población muestral, permitiendo resumir las propiedades de las variables; así mismo, para cada dimensión: nivel de actividad, capacitación y entrenamiento en ciberseguridad,

desarrollo y aplicación de estrategias de ciberseguridad, eficiencia y efectividad. Del procesamiento, se obtuvieron frecuencias absolutas y relativas, porcentajes, medias aritméticas y desviaciones estándar. Para luego construir gráficos de barras e histogramas que nos ayudaron denostar las tendencias, variabilidad y distribución de las respuestas recogidas de los encuestados de la población muestral.

Análisis inferencial. Para este tipo de análisis se tomó como base las hipótesis del estudio, empleándose técnicas inferenciales. Se utilizó la correlación de Pearson porque las variables analizadas se consideran continuas y están aproximadamente distribuidas normalmente. Esta técnica nos permitió determinar la fuerza y dirección de las relaciones lineales de la variable independiente (contribución del CCE) con las variables dependientes (eficiencia y efectividad de las Operaciones de Información). Además, también se realizó un análisis de regresión lineal simple para evaluar la extensión de la influencia de la variable independiente en cada una de las dimensiones de la variable dependiente y para construir un modelo predictivo de su comportamiento.

Los pasos tomados para el proceso inferencial final fueron: primero, verificar la escala y tipo de datos para cada variable para asegurar que las pruebas aplicadas eran adecuadas; segundo, realizar los cálculos de correlación y regresión utilizando SPSS versión 26 y, por último, analizar los coeficientes obtenidos (r y R^2) y el nivel de significancia del valor p ($p < 0.05$) para probar las hipótesis formuladas en el estudio.

El empleo de técnicas descriptivas e inferenciales permitió describir de manera detallada la realidad del CCE, así como, identificar relaciones estadísticamente significativas entre la mejora del CCE y su aporte a las Operaciones de información, dentro del Ejército del Perú. Estos hallazgos ofrecen evidencia cuantitativa para una mejor toma de decisiones para el personal del CCE y brindar recomendaciones para la mejora de las capacidades cibernéticas del Ejército.

3.9 Aspectos éticos

Esta investigación ha sido desarrollada respetando los principios éticos que rigen la investigación científica, garantizando la autonomía de los autores de las diferentes referencias bibliográficas, así como la privacidad y libertad de opinión de los participantes

Con respecto a los participantes, previo a la aplicación de los instrumentos de recolección se informó a los encuestados sobre: objetivos y propósito de la investigación así mismo, se garantizó que su participación era voluntaria y anónimo; para ello, se les solicitó el compromiso consentimiento informado digital. De igual modo, se hizo de conocimiento a los participantes que, el tratamiento de datos será de carácter confidencias empleando bases de datos codificados y de acceso solo al personal de investigadores. Se garantiza

que los resultados no han sido alterados.

Se evitó el plagio mediante el uso adecuado de las fuentes bibliográficas y se respetaron los derechos de autor en todos los materiales utilizados. En concordancia con los principios de la ética militar y académica, el estudio se enmarca en los valores de responsabilidad, transparencia, veracidad y contribución al bien institucional, promoviendo una cultura de investigación ética dentro del entorno castrense.

CAPÍTULO IV: RESULTADOS

4.1 Análisis descriptivo

En esta investigación se realizó un análisis descriptivo de los datos coleccionados a través de encuestas dirigidas al personal de Oficiales, Técnicos y Suboficiales de la especialidad de Comunicaciones que laboran en el Cuartel General del Ejército. Este análisis tiene como objetivo proporcionar un enfoque general de los juicios y actitudes de los encuestados en relación con la eficacia del CCE en las operaciones de información.

El análisis descriptivo inicial se centró en la caracterización de las variables cuantitativas continuas fundamentales para la presente investigación la percepción sobre el Centro de Ciberdefensa del Ejército (V1) y la percepción sobre el aporte a las Operaciones de Información en el Ejército del Perú (V2). Para la V1, operacionalizada a través del cuestionario correspondiente a 15 preguntas con una escala de Likert (valores de 1 a 5), se obtuvo una media de 39.53. Considerando el rango potencial de puntuaciones (15 -75), este valor central sugiere una tendencia general de los participantes a ubicarse ligeramente por debajo del punto medio teórico de la escala. La mediana correspondiente fue de 39.00, indicativa de una distribución aproximadamente simétrica. No obstante, la moda de 30, junto con la identificación de múltiples modos, señala una concentración de respuestas en valores inferiores del rango. La distribución de las puntuaciones para la V1 exhibió una dispersión considerable igual a 11.50, y una curtosis de -0.621, clasificándose como platicúrtica lo que implica una menor concentración de valores en las colas de distribución.

En relación con la V2, evaluada mediante el cuestionario instrumento de recolección de datos que consta de 12 preguntas, obteniendo un rango de 12 a 60, la media registrada fue 34.05 equivalente a 9.91. Similar a la V1, este valor promedio se sitúa marginalmente por debajo del punto medio teórico. La mediana de 35.00 y un coeficiente de 0.285 sugieren una distribución relativamente simétrica, con una ligera propensión hacia valores superiores a la media. La moda para la V2 se identificó en 48, lo que denota una mayor frecuencia de percepciones que indican un aporte más favorable. La dispersión de las puntuaciones fue ligeramente inferior a la observada en la V1 (DE=9.91), y la distribución presento una curtosis de -0.733, también de tipo platicúrtico.

Tabla 7

Estadísticos descriptivos del Centro de Ciberdefensa del Ejército (V1) y la percepción sobre el aporte a las Operaciones de Información en el Ejército del Perú (V2)

Tipo de Estadística		Centro De Ciberdefensa Del Ejército	Aporte a las Operaciones de Información en el Ejército del Perú
Media		39,53	34,05
Mediana		39,00	35,00
Moda		30[a]	48
Desviación		11,500	9,906
Varianza		132,254	98,122
Asimetría		0,036	-0,285
Curtosis		-0,621	-0,733
Percentiles	25	30,00	26,00
	50	39,00	35,00
	75	45,50	42,50

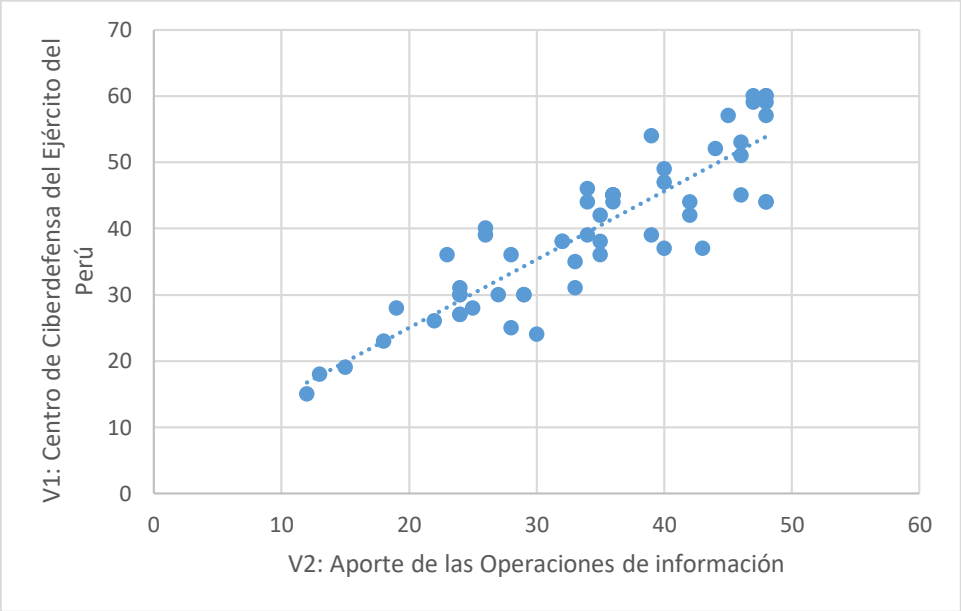
Nota. La moda marcada con superíndice ([a]) corresponde a un valor repetido en mayor frecuencia dentro del conjunto de datos. Las estadísticas fueron calculadas con base en los puntajes obtenidos de las variables V1 (Centro de Ciberdefensa del Ejército) y V2 (Aporte a las Operaciones de Información).

La relación entre la percepción sobre el Centro de Ciberdefensa del Ejército (V1) y la percepción sobre el Aporte a las Operaciones de información en Ejército del Perú (V2), fue analizada a través de un gráfico de dispersión con una línea de ajuste lineal (ver figura N° 2). Como se ilustra en la figura, se observó una tendencia positiva, indicando que a medida que aumentan las puntuaciones en la percepción del aporte a las operaciones de información, tienden a aumentar también las puntuaciones en la percepción del Centro de Ciberdefensa.

El coeficiente de determinación lineal obtenido es de un aproximado de 78.7% (R^2=0.787), de la varianza en la percepción del Centro de Ciberdefensa del Ejército del Perú, puede ser explicada por su relación lineal, con la percepción del aporte de las Operaciones de información, lo que denota una asociación fuerte entre ambas variables, considerando que valores de R^2 cercanos a 1 indican una mayor proporción considerable de la variabilidad, la dispersión de los puntos alrededor de la línea de ajuste indica que otros factores también influyen en estas percepciones.

Figura 2

Dispersión simple con ajuste de línea por V2 por la V1



Nota. Datos del resultado del SPSS, al analizar ambas variables de Ruiz y Mendoza (2025).

4.1.1 Análisis descriptivo de la variable N° 1: El Centro de Ciberdefensa del Ejército.

Se calcularon frecuencias y porcentajes para cada una de las preguntas de la encuesta, lo que permitió identificar las respuestas más comunes y sus respectivas proporciones dentro de la muestra. Para la variable N° 1: El Centro de Ciberdefensa del Ejército.

Tabla 8

Distribución de las frecuencias orientadas según personal militar del Centro de Ciberdefensa del Ejército, 2025

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	1	1,8%
En desacuerdo	15	26,3%
Ni de acuerdo ni desacuerdo	27	47,4%
De acuerdo	14	24,6%
Total	57	100,0%

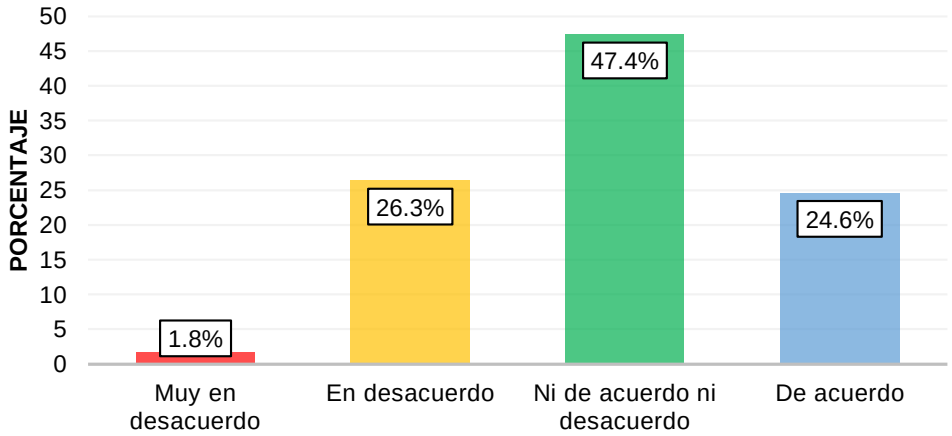
Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

La tabla N° 8, denota la distribución general de la percepción del personal militar en relación con el Centro de Ciberdefensa del Ejército (V1). Como se observa, la categoría con la mayor proporción de respuestas fue “Ni de acuerdo ni en desacuerdo”, representando el

47.4% de los participantes de la encuesta (n=27). Un porcentaje considerable del personal se inclinó hacia el desacuerdo con un 26.3% (n=15) ubicándose en la categoría “En desacuerdo” y un moderado 1.8% (n=1) expresando estar “Muy en desacuerdo”. En contraste, la postura de acuerdo fue manifestada por el 24.6% de los participantes (n=14) en la categoría de “De acuerdo”, sin representación en la categoría “Totalmente de acuerdo”. En términos generales, la distribución sugiere una tendencia central hacia la neutralidad, con una proporción notable de respuestas que indican algún nivel de desacuerdo, y una representación de menor acuerdo. La percepción de “Muy en desacuerdo” fue la menos presente entre los participantes.

Figura 3

Resultados del Centro de Ciberdefensa del Ejército



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Respecto a la variable El Centro de Ciberdefensa del Ejército el 1.8% de los encuestados manifiestan encontrarse muy en desacuerdo en que existen problemas en que el centro de ciberdefensa aporte a las operaciones de información, el 26.3% manifiestan están en desacuerdo, el 47.4% se encuentran ni en acuerdo ni en desacuerdo, el 24.6% de acuerdo.

Dimensión 1: Nivel de Actividad. Con sus correspondientes indicadores: Cantidad de instalaciones equipadas para los Hub.

Tabla 9

Nivel de Actividad para la Variable N° 1

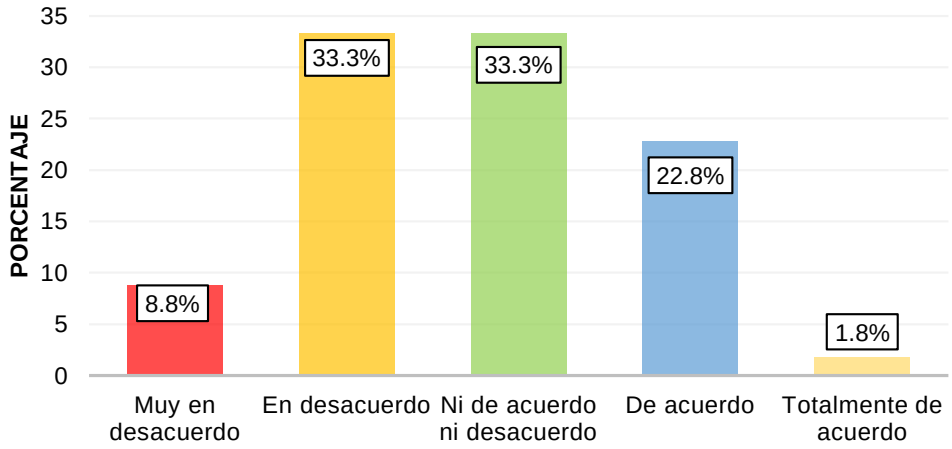
Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	5	8,8%
En desacuerdo	19	33,3%
Ni de acuerdo ni desacuerdo	19	33,3%
De acuerdo	13	22,8%
Totalmente de acuerdo	1	1.8%

Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 4

Frecuencia de Nivel de Actividad.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

La Tabla N°4, presenta la distribución de la percepción del personal militar en relación con el Nivel de Actividad del Centro de Ciberdefensa del Ejército. Los resultados revelan una distribución donde las categorías de "En desacuerdo" y "Ni de acuerdo ni en desacuerdo" comparten la mayor frecuencia, con 19 participantes cada una (33.3%). Una proporción considerable del personal percibe un nivel de actividad que no cumple con sus expectativas o sobre el cual no tienen una opinión definida. En contraste, un 22.8% de los participantes (n=13) manifestó estar "De acuerdo" con el nivel de actividad, mientras que una minoría del 1.8% (n=1) expresó estar "Totalmente de acuerdo". Las percepciones más negativas se encuentran en las categorías de desacuerdo, con un 8.8% (n=5) indicando estar "Muy en desacuerdo". En general, la distribución sugiere una percepción predominantemente neutral o negativa respecto al nivel de actividad del Centro de Ciberdefensa, con una representación limitada de opiniones positivas.

Dimensión 2: Capacitación y entrenamiento en ciberseguridad en el CCE. Con sus correspondientes indicadores: Incremento en las capacidades técnicas del CCE y Cantidad de Programas de capacitación Ofrecidos en el CCE.

Tabla 10

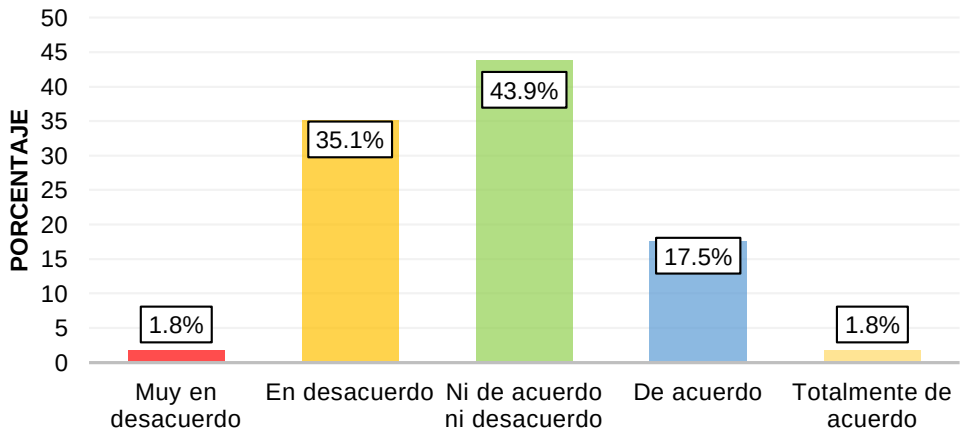
Nivel de Capacitación y entrenamiento de la Variable N° 1.

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	1	1,8%
En desacuerdo	20	35,1%
Ni de acuerdo ni desacuerdo	25	43,9%
De acuerdo	10	17,5%
Totalmente de acuerdo	1	1.8%
Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 5

Frecuencia de Nivel de Capacitación y entrenamiento.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

La Tabla N° 10 presenta la distribución de la percepción del personal militar en relación con la Capacitación y Entrenamiento proporcionados por el Centro de Ciberdefensa del Ejército. Los resultados indican que la categoría más frecuente fue "Ni de acuerdo ni en desacuerdo", con 25 participantes (43.9%), lo que sugiere una proporción considerable del personal que no tiene una opinión definida o se mantiene neutral respecto a este aspecto. Una parte importante de los encuestados expresó su desacuerdo, con 20 participantes (35.1%) ubicándose en la categoría "En desacuerdo". En contraste, las opiniones favorables hacia la capacitación y el entrenamiento fueron menos prevalentes, con 10 participantes (17.5%) manifestando estar "De acuerdo" y solo 1 participante (1.8%) expresando estar "Totalmente de acuerdo". Al igual que en otras dimensiones de la V1, la postura de "Muy en desacuerdo" tuvo una baja representación, con 1 participante (1.8%). En general, la distribución de las percepciones sobre la capacitación y el entrenamiento del Centro de Ciberdefensa tiende a inclinarse hacia la neutralidad o el desacuerdo, con una

representación limitada de opiniones positivas.

Dimensión 3: Desarrollo y aplicación de estrategias de ciberseguridad en el CCE. Con sus correspondientes indicadores: objetivos alcanzados por el CCE y frecuencia de actualización de estrategias en ciberseguridad del CCE.

Tabla 11

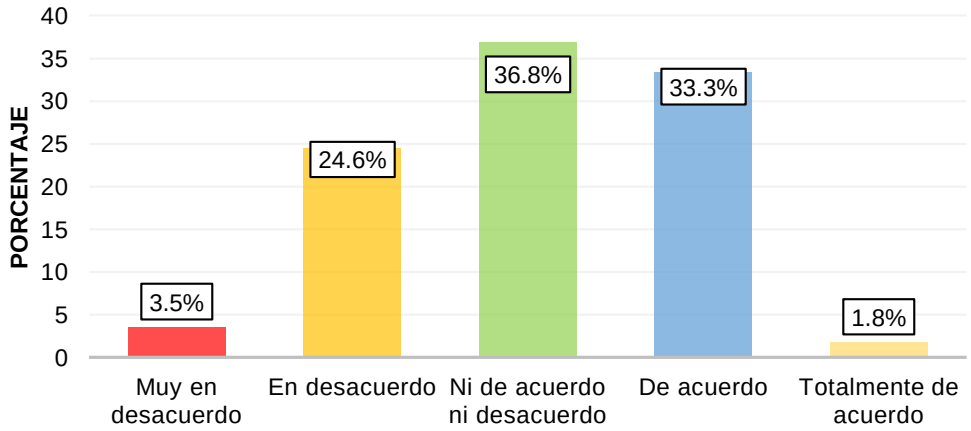
Nivel de Desarrollo y aplicación de estrategias de ciberseguridad de la Variable N° 1.

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	2	3,5%
En desacuerdo	14	24,6%
Ni de acuerdo ni desacuerdo	21	36,8%
De acuerdo	19	33,3%
Totalmente de acuerdo	1	1.8%
Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 6

Frecuencia de Desarrollo y aplicación de estrategias de ciberseguridad.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

La Tabla N° 11 presenta la distribución de la percepción del personal militar en relación con el Nivel de desarrollo y aplicación de estrategias de Ciberseguridad en el Centro de Ciberdefensa del Ejército. Los resultados muestran que la categoría más frecuente fue "Ni de acuerdo ni en desacuerdo", con 21 participantes (36.8%), indicando una proporción considerable del personal que se mantiene neutral o no tiene una opinión definida sobre

este aspecto. Le sigue de cerca la categoría "De acuerdo", con 19 participantes (33.3%), lo que sugiere una parte importante del personal que percibe un nivel adecuado de desarrollo y aplicación de estrategias. En contraste, el desacuerdo se manifestó en un 24.6% (n=14) en la categoría "En desacuerdo" y un 3.5% (n=2) en la categoría "Muy en desacuerdo". La opinión de "Totalmente de acuerdo" fue la menos representada, con solo 1 participante (1.8%). En general, la distribución de las percepciones sobre el nivel de desarrollo y aplicación de estrategias de ciberseguridad en el Centro de Ciberdefensa tiende a inclinarse hacia la neutralidad o el acuerdo, con una representación menor de opiniones negativas.

4.1.2 Análisis descriptivo de la variable N°2: Aporte a las Operaciones de Información en el Ejército del Perú, 2024.

Se calcularon frecuencias y porcentajes para cada una de las preguntas de la encuesta, lo que permitió identificar las respuestas más comunes y sus respectivas proporciones dentro de la muestra. Para la variable N° 2: Aporte a las Operaciones de Información en el Ejército del Perú - 2024.

La tabla N° 7, presenta la distribución general de la percepción militar en relación con el aporte a las Operaciones de la Información en el Ejército del Perú (V2). Al igual que en la V1, la categoría con mayor proporción de respuestas fue “Ni de acuerdo ni en desacuerdo”; representando el 42.1% de los participantes (n=24). Sin embargo, en contraste con la V1, se observa una mayor proporción de respuestas que indican acuerdo, con una 36.8% de los participantes (n=21), ubicándose en la categoría “De acuerdo”. Las posturas de desacuerdo fueron menos relevantes con un 19.3% (n=11) manifestando estar en “En desacuerdo” y un 1.8% (n=1), expresando estar “Muy en desacuerdo”. En términos generales la distribución sugiere una tendencia central hacia la neutralidad, pero con una inclinación notable hacia el acuerdo en comparación con la V1, y una menor representación del desacuerdo. La percepción “Muy en desacuerdo”, fue al igual que en la V1 es la menos frecuente.

Tabla 12

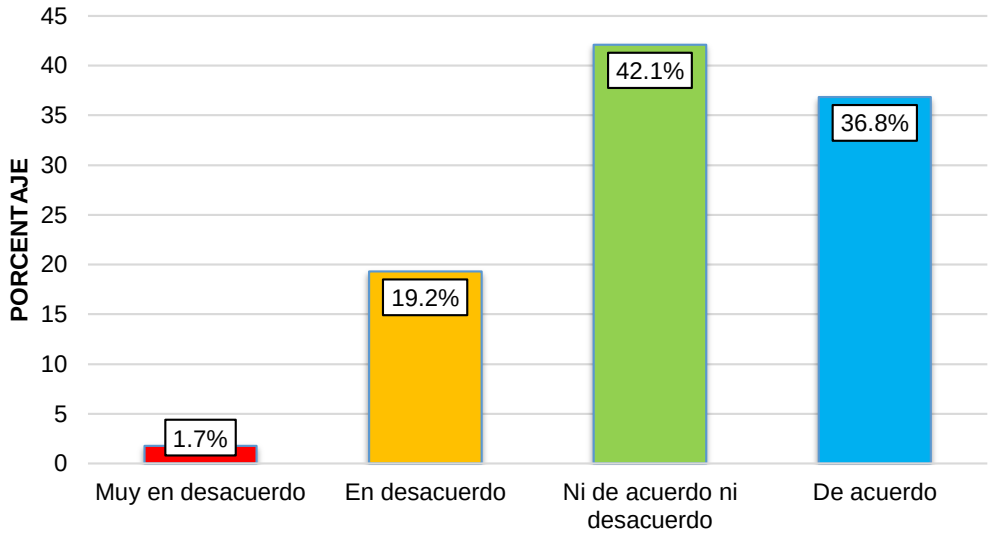
Distribución de las frecuencias orientadas según personal militar al Aporte a las Operaciones de Información en el Ejército del Perú.

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	1	1,8%
En desacuerdo	11	19,3%
Ni de acuerdo ni desacuerdo	24	42,1%
De acuerdo	21	36,8%
Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 7

Resultados del Aporte a las Operaciones de Información en el Ejército del Perú.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Respecto a la variable Aporte a las Operaciones de información el 1.7% de los encuestados manifiestan encontrarse muy en desacuerdo en que el centro de ciberdefensa aporte a las operaciones de información, el 19.2% manifiestan están en desacuerdo, el 42.1% se encuentran ni en acuerdo ni en desacuerdo, el 36.8% de acuerdo.

Dimensión 1: Nivel de eficiencia. Con sus correspondientes indicadores: percepción positiva de la población y empleo adecuado de los recursos asignados.

Tabla 13

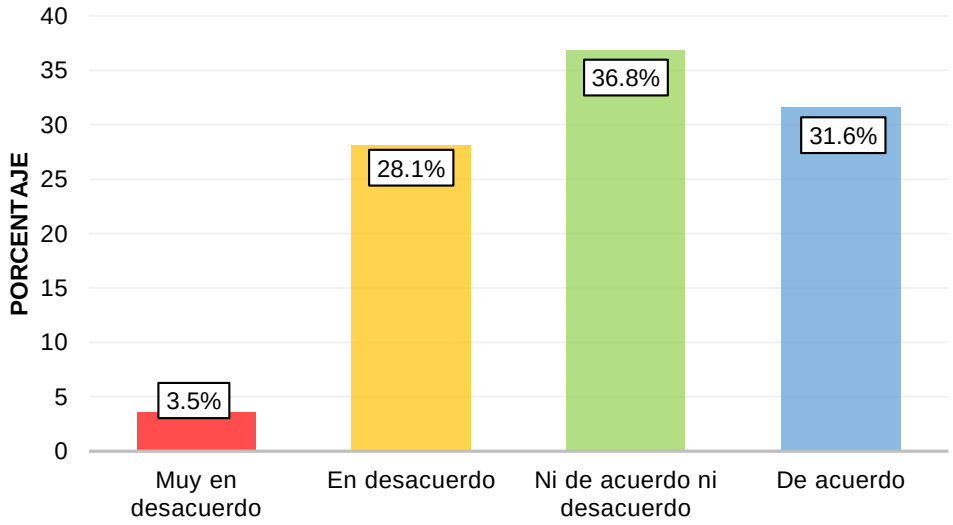
Distribución de las frecuencias orientadas al Nivel de eficiencia respecto a la V2.

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	2	3,5%
En desacuerdo	16	28,1%
Ni de acuerdo ni desacuerdo	21	36,8%
De acuerdo	18	31,6%
Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 8

Frecuencia de Nivel de Eficiencia.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

La Tabla N° 13 presenta la distribución de la percepción del personal militar en relación con el Nivel de eficiencia del aporte a las Operaciones de Información en el Ejército del Perú. Los resultados indican que la categoría más frecuente fue "Ni de acuerdo ni en desacuerdo", con 21 participantes (36.8%), lo que sugiere una proporción considerable del personal que se mantiene neutral o no tiene una opinión definida sobre la eficiencia de dicho aporte. Le sigue en frecuencia la categoría "De acuerdo", con 18 participantes (31.6%), lo que denota una parte importante del personal que percibe un nivel de eficiencia adecuado. En contraste, las opiniones que expresan desacuerdo se distribuyen entre 16 participantes (28.1%) en la categoría "En desacuerdo" y 2 participantes (3.5%) en la categoría "Muy en desacuerdo". En general, la distribución de las percepciones sobre el nivel de eficiencia del aporte a las Operaciones de Información tiende a concentrarse en la neutralidad y el acuerdo, aunque una proporción no despreciable del personal manifiesta algún nivel de desacuerdo.

Dimensión 2: Nivel de eficacia. Con sus correspondientes indicadores: cantidad de operaciones de información realizadas y cantidad de normas y disposiciones a nivel institucional promulgadas.

En la Tabla N° 9 presenta la distribución de la percepción del personal militar en relación con el Nivel de eficacia del aporte a las Operaciones de Información en el Ejército del Perú. Los resultados revelan que la categoría más frecuente fue "Ni de acuerdo ni en desacuerdo", con 22 participantes (38.6%), lo que indica una proporción considerable del

personal que mantiene una postura neutral o no tiene una opinión definida sobre la eficacia de dicho aporte. Le sigue en frecuencia la categoría "De acuerdo", con 19 participantes (33.3%), sugiriendo que una parte importante del personal percibe un nivel de eficacia adecuado. Las opiniones que expresan desacuerdo se distribuyen entre 12 participantes (21.1%) en la categoría "En desacuerdo" y 1 participante (1.8%) en la categoría "Muy en desacuerdo". Por otro lado, una minoría del personal expresó un acuerdo fuerte, con 3 participantes (5.3%) ubicándose en la categoría "Totalmente de acuerdo". En general, la distribución de las percepciones sobre el nivel de eficacia del aporte a las Operaciones de Información tiende a concentrarse en la neutralidad y el acuerdo, con una representación limitada de opiniones negativas y positivas extremas.

Tabla 14

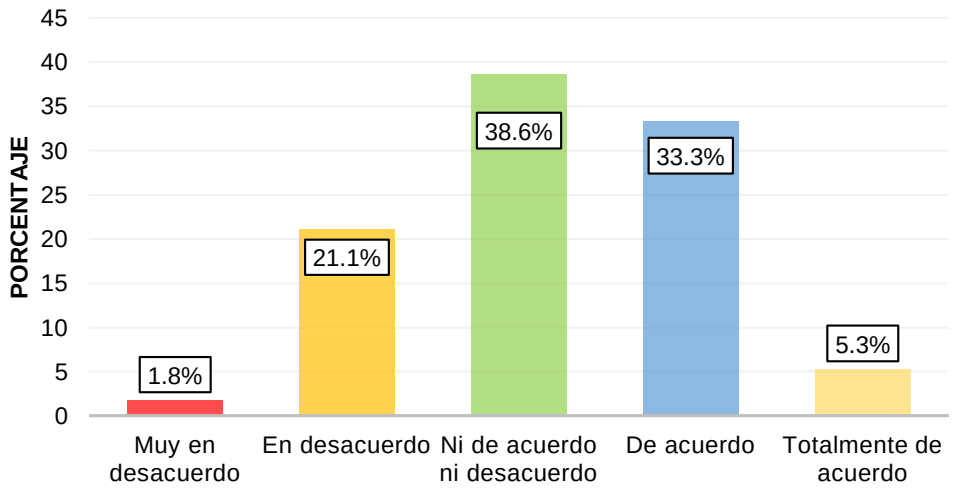
Distribución de las frecuencias orientadas al Nivel de eficiencia respecto a la V2.

Percepción del personal militar	Frecuencia	Porcentaje
Muy en desacuerdo	1	1,8%
En desacuerdo	12	21,1%
Ni de acuerdo ni desacuerdo	22	38,6%
De acuerdo	19	33,3%
Totalmente de acuerdo	3	5,3%
Total	57	100,0%

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Figura 9

Frecuencia de Nivel de Eficacia.



Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

4.2 Análisis Inferencial

Luego de haber realizado un análisis descriptivo de las variables, la siguiente fase de orienta a la realización de inferencias sobre la población a partir de los datos muestrales recibidos del instrumento de recolección de datos. En ese sentido se buscó examinar la relación lineal existente entre el Centro de Ciberdefensa del Ejército (V1) y su aporte a las Operaciones de Información en el Ejército del Perú (V2) no obstante, previamente se necesitó comprobar que los datos se comporten de una manera normal para aplicar un estadístico ya sea paramétrico o no. Ya que cuando se realiza una investigación del tipo cuantitativo se tienen dos tipos de pruebas estadísticas, las paramétricas y las no paramétricas. (Escobar et al., 2018), las pruebas paramétricas permiten analizar que el comportamiento de las variables por la situación existente, a diferencia de las pruebas no paramétricas que son eventos a raíz de una intencionalidad.

Tabla 15

Tabla de Pruebas de Normalidad

Variable	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Centro de Ciberdefensa del Ejército	0,087	57	0,200*	0,974	57	0,255
Aporte a las Operaciones de Información en el Ejército del Perú	0,080	57	,200*	0,954	57	0,031

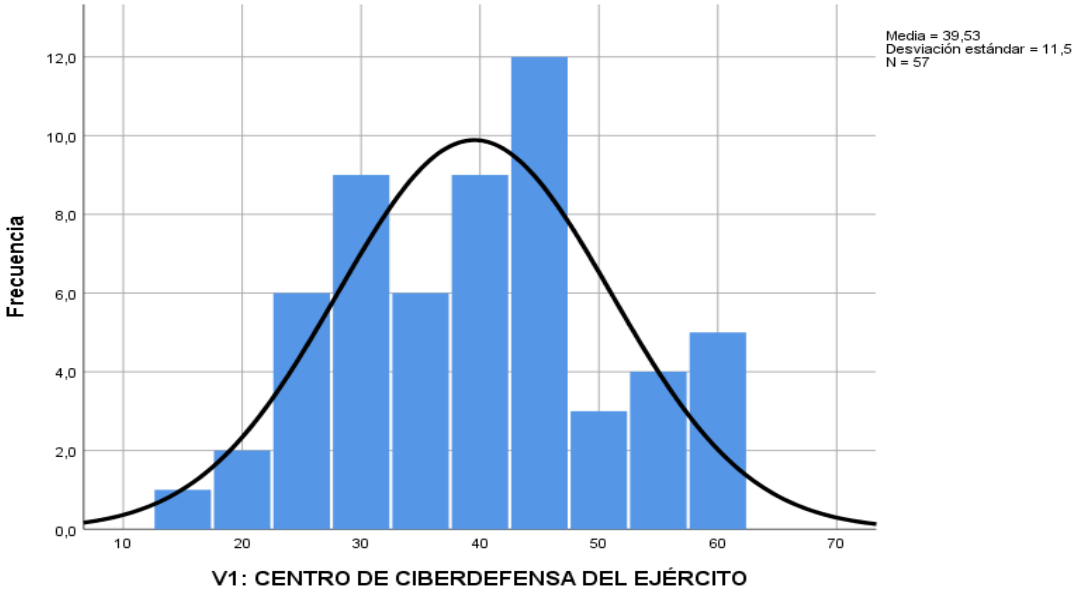
*. Esto es un límite inferior de la significación verdadera.

Nota. Los porcentajes fueron calculados sobre la base de 57 participantes encuestados del Centro de Ciberdefensa del Ejército en 2025.

Para este caso la prueba de normalidad elegida fue Kolmogórov-Smirnov, ya que el número de muestra es superior a 50 casos, según lo recomendado por Galindo (2020), la muestra resultante es de 57 individuos. Esta prueba arrojo un valor de significancia (Sig.) de 0.200 para ambas variables, ver la tabla N° 15, superior al umbral de 0.05, lo que sugiere que, según esta prueba no se encontraron desviaciones significativas en las distribuciones de ambas variables. Así mismo en las figuras 10 y 11 podemos ver el comportamiento normal que tienen las variables respecto a la frecuencia. Debido al comportamiento normal de las variables se tomarán pruebas paramétricas.

Figura 10

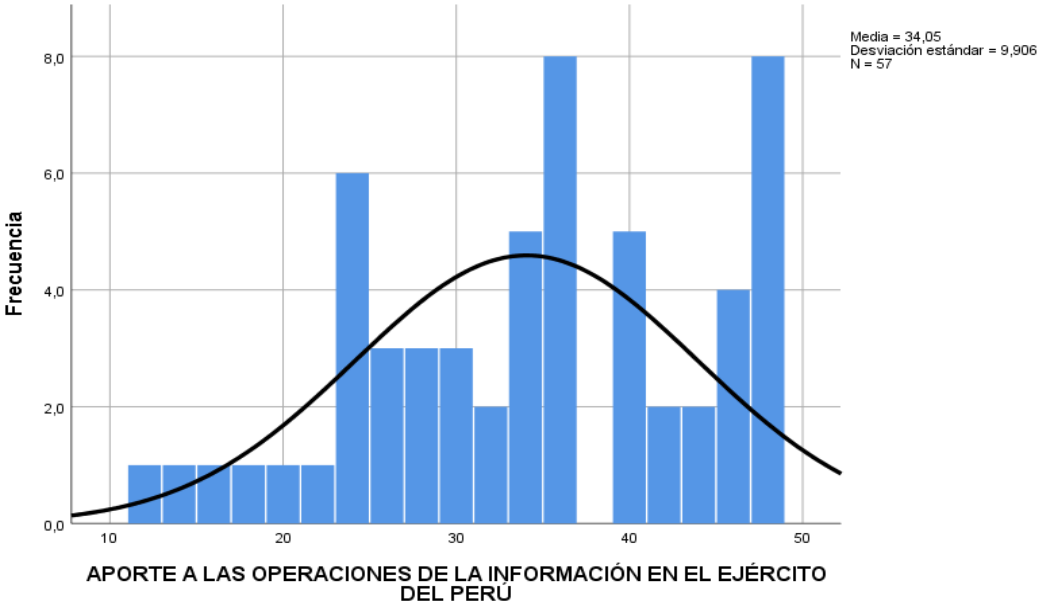
Curva de Normalidad para la V1: Centro de Ciberdefensa del Ejército.



Nota. La figura presenta el histograma y la curva de normalidad correspondientes a la variable V1 (Centro de Ciberdefensa del Ejército), basada en 57 observaciones. La media fue 39.53 y la desviación estándar 11.5.

Figura 11

Curva de normalidad de la V2: Aporte a las OI en el EP.



Nota. La figura presenta el histograma y la curva de normalidad correspondientes a la variable V2 (Aporte a las OI en el EP), basada en 57 observaciones. La media fue 34.05 y

la desviación estándar 9.9.

4.2.1 Prueba de hipótesis general

Para determinar el grado de correlación entre las variables se han planteado las hipótesis siguientes:

Hipótesis Alterna H1: El Centro de Ciberdefensa del Ejército (CCE) aporta significativamente a las Operaciones de Información en el Ejército del Perú durante el año 2024.

Hipótesis Nula Ho: El Centro de Ciberdefensa del Ejército (CCE) no aporta significativamente a las Operaciones de Información en el Ejército del Perú durante el año 2024.

Existen diversas pruebas de correlación, las pruebas correlacionales son herramientas estadísticas fundamentales para examinar la fuerza y la dirección de la asociación lineal entre dos o más variables (Hernández - Sampieri y Mendoza, 2018). El objetivo principal de estas pruebas no es establecer causalidad, sino determinar en qué medida los cambios en una variable se relacionan con los cambios en otra. La elección de la prueba correlacional apropiada depende del nivel de medición de las variables involucradas (Arispe et al., 2015).

Para variables a nivel de intervalo o razón, la prueba más comúnmente utilizada es el coeficiente de correlación de Pearson (r). Este coeficiente varía de -1.00 a +1.00, donde los valores cercanos a cero indican una correlación débil o nula, mientras que los valores cercanos a los extremos indican una correlación fuerte. El signo indica la dirección de la relación: positivo (a medida que una variable aumenta, la otra también tiende a aumentar) o negativo (a medida que una variable aumenta, la otra tiende a disminuir) (Field, 2018). La significancia estadística del coeficiente de Pearson se evalúa mediante una prueba t o un valor p asociado.

Para esta investigación se empleará el Coeficiente de correlación de Pearson, ya que es una prueba estadística que sirve para analizar la relación existente entre 2 variables, también es conocido como “coeficiente producto-momento” (Hernández - Sampieri y Mendoza, 2018, p. 346), de la misma manera que buscamos analizar el aporte que realiza el Centro de Ciberdefensa del Ejército a las Operaciones de información.

Tabla 16

Correlación de Pearson

Correlación de Pearson		Centro de Ciberdefensa del Ejército	Operaciones de Información en el Ejército del Perú
Centro de Ciberdefensa del Ejército	Correlación de Pearson	1	0,887**
	Sig. (bilateral)		0,000
	N	57	57
Operaciones de Información en el Ejército del Perú	Correlación de Pearson	0,887**	1
	Sig. (bilateral)	0,000	
	N	57	57

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

Nota. N = 57. La correlación de Pearson se calculó entre las variables "Centro de Ciberdefensa del Ejército" y "Operaciones de Información en el Ejército del Perú". **p < .01** indica significancia estadística bilateral al 1%.

La prueba revelo una correlación positiva y fuerte estadísticamente significativa entre ambas variables, con un coeficiente de Pearson r= 0.887 donde p<0.001, como se puede observar en la tabla N° 11, este resultado indica que existe una asociación lineal considerable entre la variable Centro de Ciberdefensa del Ejército sobre el aporte a las operaciones de Información en el Ejercito del Perú, de manera de que a percepciones más positivas en una variable se asocian percepciones igualmente positivas en la otra.

La significancia estadística (p<0.001) inferior al nivel de α=0.01, permite rechazar la hipótesis nula (Arispe et al., 2020, p. 82), finalmente se intuye que esta relación es altamente significativa en la población.

4.2.2 Prueba de hipótesis especificas 1

Hipótesis alterna H_1: Los factores que influyen en el nivel de actividad del CCE se relacionan de manera significativa con su participación en las Operaciones de Información en el Ejército del Perú durante el año 2024.

Hipótesis Nula H_0: Los factores que influyen en el nivel de actividad del CCE no se relacionan de manera significativa con su participación en las Operaciones de Información en el Ejército del Perú durante el año 2024.

Tabla 17

Prueba de Hipótesis especifica 1

Correlación de Pearson		Nivel de actividad.	Nivel de eficiencia
Nivel de actividad.	Correlación de Pearson	1	0,572**
	Sig. (bilateral)		0,000
	N	57	57
Nivel de eficiencia	Correlación de Pearson	0,572**	1
	Sig. (bilateral)	0,000	
	N	57	57
**. La correlación es significativa en el nivel 0,01 (bilateral).			

Nota. N = 57. La correlación de Pearson se calculó entre las dimensiones “Nivel de actividad” y “Nivel de Eficiencia”. p < .01 indica significancia estadística bilateral al 1%.

Para contrastar la Hipótesis Específica 1, la cual postulaba que el nivel de actividad del Centro de Ciberdefensa del Ejército se relaciona de manera significativa con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú, se realizó la prueba de correlación Pearson, obteniendo como resultados (ver Tabla N° 12) revelaron una correlación positiva y moderada estadísticamente significativa entre ambas dimensiones ($r=0.572$, $p<0.001$).

Este coeficiente de correlación indica que existe una asociación lineal entre el nivel de actividad percibido del Centro de Ciberdefensa y la eficiencia percibida de su aporte a las Operaciones de Información: a mayor nivel de actividad percibido, tiende a haber una mayor percepción de eficiencia en el aporte, y viceversa. La significancia estadística ($p < 0.001$), inferior al nivel de $\alpha=0.01$, permite rechazar la hipótesis nula de no correlación entre estas dimensiones y confirma la existencia de una relación significativa en la muestra.

4.2.3 Prueba de hipótesis especificas 2

Hipótesis alterna H_2: El nivel de capacitación y entrenamiento del personal del CCE influye de manera significativa en la eficiencia de su aporte a las Operaciones de Información en el Ejército del Perú durante el año 2024.

Hipótesis Nula H_0: El nivel de capacitación y entrenamiento del personal del CCE no influye de manera significativa en la eficiencia de su aporte a las Operaciones de Información en el Ejército del Perú durante el año 2024.

Tabla 18

Prueba de Hipótesis especifica 2

Correlación de Pearson		Capacitación y entrenamiento en ciberseguridad en el CCE.	Nivel de Eficiencia
Capacitación y entrenamiento en ciberseguridad en el CCE.	Correlación de Pearson	1	0,839**
	Sig. (bilateral)		0,000
	N	57	57
Nivel de Eficiencia	Correlación de Pearson	0,839**	1
	Sig. (bilateral)	0,000	
	N	57	57

Nota. N = 57. La correlación de Pearson se calculó entre las dimensiones “Capacitación y entrenamiento en ciberseguridad en el CCE” y “Nivel de Eficiencia”. p < .01 indica significancia estadística bilateral al 1%.

Para contrastar la Hipótesis Alterna 2, se examinó la correlación de Pearson entre la dimensión Capacitación y entrenamiento en ciberseguridad en el CCE y la dimensión Nivel de Eficiencia del aporte a las Operaciones de Información. Los resultados (ver Tabla N° 13) revelaron una correlación positiva y muy fuerte estadísticamente significativa (r=0.839, p<0.001). Este elevado coeficiente de correlación indica una asociación lineal sustancial entre la capacitación y entrenamiento percibidos en ciberseguridad en el CCE y el nivel de eficiencia percibido en su aporte a las Operaciones de Información: a mayor percepción de capacitación y entrenamiento, se asocia una percepción significativamente mayor de eficiencia en el aporte, y viceversa.

La significancia estadística (p < 0.001), inferior al nivel de α=0.01, permite rechazar la hipótesis nula de no correlación entre estas dimensiones y confirma la existencia de una relación altamente significativa en la muestra. Por lo tanto, se puede concluir que la capacitación y entrenamiento en ciberseguridad del CCE se relacionan de manera positiva y muy fuerte con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú.

4.2.4 Prueba de hipótesis especificas 3

Hipótesis alterna H3: El desarrollo y aplicación de estrategias de ciberseguridad en el CCE se relacionan de manera significativa con la eficacia de las Operaciones de Información en el Ejército del Perú durante el año 2024.

Hipótesis Nula H0: El desarrollo y aplicación de estrategias de ciberseguridad en el CCE no se relacionan de manera significativa con la eficacia de las Operaciones de Información en el Ejército del Perú durante el año 2024.

Tabla 19

Prueba de Hipótesis especifica 3

Correlación de Pearson		Desarrollo y aplicación de estrategias de ciberseguridad en el CCE	Nivel de eficacia
Desarrollo y aplicación de estrategias de ciberseguridad en el CCE	Correlación de Pearson	1	0,840**
	Sig. (bilateral)		0,000
	N	57	57
Nivel de eficacia	Correlación de Pearson	0,840**	1
	Sig. (bilateral)	0,000	
	N	57	57

Nota. N = 57. La correlación de Pearson se calculó entre las dimensiones “Desarrollo y aplicación de estrategias de ciberseguridad en el CCE” y “Nivel de Eficacia”. p < .01 indica significancia estadística bilateral al 1%.

Para divergir la Hipótesis Alterna 3, la cual demandaba que el Desarrollo y aplicación de estrategias de ciberseguridad en el CCE aporta de manera significativa en la eficacia de las Operaciones de Información en el Ejército del Perú, se examinó la correlación de Pearson entre la dimensión "Desarrollo y aplicación de estrategias de ciberseguridad en el CCE" y la dimensión "Nivel de eficacia" del aporte a las Operaciones de Información. Los resultados (ver Tabla N° 14) revelaron una correlación positiva y muy fuerte estadísticamente significativa (r=0.840, p<0.001). Este elevado coeficiente de correlación indica una asociación lineal sustancial entre el desarrollo y aplicación de estrategias de ciberseguridad percibidos en el CCE y el nivel de eficacia percibido en su aporte a las Operaciones de Información: a mayor percepción de desarrollo y aplicación de estrategias, se asocia una percepción significativamente mayor de eficacia en el aporte, y viceversa. La significancia estadística (p < 0.001), inferior al nivel de α=0.01, permite rechazar la hipótesis nula de no correlación entre estas dimensiones y confirma la existencia de una relación altamente significativa en la muestra. Por lo tanto, se puede concluir que el Desarrollo y aplicación de estrategias de ciberseguridad en el CCE se relacionan de manera positiva y muy fuerte con la eficacia en el aporte a las Operaciones de Información en el Ejército del Perú.

4.3 Análisis complementarios

Para esta investigación, para evaluar la consistencia interna de los instrumentos empleados se usó el coeficiente de Cronbach, obteniéndose un resultado de 0.984, esto significa que existe una excelente fiabilidad entre las escalas de medición para las variables

Centro de ciberdefensa del Ejercito y aporte a las operaciones de información en el Ejército del Perú 2024, resultando que es coherente y se mide de manera efectiva el constructo teórico propuesto.

Finalmente, se obtuvo el coeficiente de correlación de Pearson 0.906 ($p < 0.01$), lo que significa que, existe una correlación positiva fuerte y significativa; implicando que a medida se aumente el nivel de actividad del Centro de Ciberdefensa, capacitación y estrategias, también se incrementará el nivel de eficiencia y eficacia. Estos hallazgos proporcionan evidencia empírica sobre la relación de las variables estudiadas; así como, la validez del instrumento empleado, fortaleciendo así las recomendaciones de los investigadores.

CAPÍTULO V: DISCUSIÓN

En el presente capitulo se analiza los resultados obtenidos a partir del tratamiento estadístico de los datos, en relación con los objetivos y las hipótesis formuladas, interpretando los hallazgos desde un punto de vista metodológico y doctrinario, para posteriormente contrastarlo con los fundamentos teóricos, antecedentes regionales, nacionales e internacionales, para si comprender de manera holística como el Centro de Ciberdefensa del Ejército aporta a las Operaciones de Información Ejército del Perú durante el año 2024, considerando las dimensiones: nivel de actividad, capacitación y entrenamiento en ciberseguridad, desarrollo y aplicación de estrategias de ciberseguridad, nivel de eficiencia y nivel de eficacia. Así mismo, esta discusión está orientada en poner en perspectiva la importancia del CCE dentro del sistema de defensa nacional, su aporte a la seguridad digital del Ejército y su relación con el proceso de modernización de la Gestión del Estado y el Plan de Transformación Institucional del Ejército, cuyo objetivo estratégico N° 5, Desarrollar la Ciberdefensa en el Ejército del Perú (Ejército del Perú, 2022).

Con relación al objetivo general: Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024, los resultados estadísticos mostraron una correlación positiva fuerte y significativa entre la percepción del personal militar sobre el funcionamiento del CCE y su aporte a las Operaciones de información ($r = 0.887$; $p < 0.001$), este hallazgo indica que la actuación del CCE constituye un componente importante para la gestión de información y la protección del ciberespacio. El coeficiente de determinación $R^2 = 0.787$, demostró que el 78.7% de la variabilidad observada en las percepciones sobre el CCE puede explicarse por el grado de participación del CCE en las OI, lo que confirma su relevancia estrategia en el Ejército del Perú. No obstante un 47.4% de los participantes manifestó una posición neutral y un 26.3% expreso desacuerdo con el funcionamiento general del CCE, lo que denota la existencia de brechas de resultados del CCE y de visibilidad operativa, esta percepción coincide con el estudio de Quevedo (2023), quien plantea que las capacidades de ciberdefensa de las instituciones militares alcanzan su máximo potencial cuando se integran efectivamente el sistema de comando y control, y cuando sus resultados son conocidos por la estructura organizacional. En consecuencia, como menciona Onetto (2024), determina que dimensionar las OI permite definir el verdadero nivel de desarrollo digital y los indicadores de rendimiento operacionales dentro de cualquier aparato militar (p.65), es necesario conocer cómo se va desempeñando el CCE, por lo que es importante conocer cuáles son

los indicadores que van a señalar como va avanzando en el desarrollo de la ciberdefensa y a su vez en el aporte a las Operaciones de información.

Respecto al Objetivo Específico 1: Analizar los factores que influyen en la actividad del CCE en las Operaciones de Información en el Ejército del Perú durante el año 2024, los resultados revelaron correlación moderada pero significativa ($r = 0.572$; $p < 0.001$), lo que sugiere que la frecuencia de ejercicios de ciberdefensa, disponibilidad tecnológica, coordinación interinstitucional, y la ausencia de objetivos institucionales claramente definidos influyen directamente en el desempeño. Sin embargo, el 66.6% del personal encuestado manifestó percepciones neutrales o negativas, lo que indica que el CCE no dispone de una cobertura efectiva en todo el territorio ni mantienen una operatividad sostenida. En ese sentido la baja frecuencia de ejercicios de ciberdefensa constituye un factor limitante para su contribución a las OI. Asimismo, la falta de objetivos y metas institucionales ha restringido el desarrollo de capacidades técnicas y estratégicas, dificultando su aporte en las OI. Estos hallazgos concuerdan con lo señalado por Dobbertin (2023), quien sostiene que la actividad de un centro de ciberdefensa no solo se mide por la infraestructura disponible, sino también por su capacidad de anticipar y neutralizar amenazas mediante simulaciones y ejercicios continuos. Además los resultados sugieren que la infraestructura física y tecnológica del CCE, particularmente para los hubs periféricos, cuando se instalasen, requerirán de una modernización continua así como distribución geoestratégica que permita extender su alcance operativo. La limitada actualización en hardware, software y conectividad constituyen un obstáculo directo a la efectividad institucional. Por consiguiente es prioritario, definir los objetivos y metas del CCE así como la realización periódica de ejercicios interinstitucionales de ciberdefensa.

Con relación al Objetivo Específico 2: Determinar el nivel de capacitación y entrenamiento en ciberseguridad del CCE y su influencia con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú durante el año 2024, se obtuvo como resultado que existe una correlación muy fuerte y significativa ($r = 0.839$; $p < 0.001$) entre la capacitación y entrenamiento en ciberseguridad del CCE y su nivel de eficiencia en las OI. Este hallazgo permite inferir que la formación técnica del personal y la gestión del conocimiento son factores decisivos para alcanzar un desempeño eficiente, sin embargo, el análisis descriptivo demostró que el 43.9% del personal encuestado se mantuvo neutral y el 35.1 % expreso desacuerdo respecto a la suficiencia de programas de capacitación, esto revela una debilidad estructural de profesionalización continua del personal especializado. Estos resultados coinciden con Cadillo (2021), quien argumenta que la eficiencia operativa en las organizaciones de ciberdefensa está directamente vinculada con el nivel de profesionalización y certificación de sus integrantes, que garanticen estándares operativos comparables a los de la OTAN. En ese sentido, Huertas (2023), advierte que las

instituciones militares peruanas presentan deficiencias en la gestión del conocimiento y en la actualización técnica lo que limita su capacidad de respuesta frente a incidentes cibernéticos.

Así mismo la doctrina internacional enfatiza que la sostenibilidad de las capacidades en el dominio cibernético está estrechamente ligada a la formación constante del personal y la práctica operativa continua según lo señala la U.S. Joint Chiefs of Staff (JCS, 2018), los centros de ciberdefensa deben de mantener programas permanentes de entrenamiento técnico basado en simulaciones y ejercicios colaborativos, para garantizar que la fuerza mantenga su capacidad de disuasión y respuesta ante entornos híbridos.

Así mismo, para el Objetivo Específico 3: Evaluar cómo el desarrollo y la aplicación de estrategias de ciberseguridad en el Centro de Ciberdefensa del Ejército (CCE) contribuyen a la eficacia de las Operaciones de Información en el Ejército del Perú durante el año 2024, la correlación de Pearson entre el desarrollo y aplicación de estrategias de ciberseguridad en el CCE y la eficacia de las OI fue muy fuerte y estadísticamente significativa ($r = 0.840$; $p < 0.001$). este resultado demuestra que la adecuada planificación y ejecución de estrategias de protección cibernética tiene un impacto directo en la percepción de eficacia institucional. No obstante, los resultados descriptivos evidenciaron que el 36.8% del personal se mantuvo neutral y el 24.6% expresó desacuerdo, respecto a la efectividad de las estrategias implementadas lo que sugiere una limitada difusión interna o ausencia de mecanismos de evaluación de impacto. Esto sugiere la necesidad de fortalecer los procesos de planificación y evaluación de estrategias cibernéticas, asegurando su alineación con los objetivos planteados en el Plan de Transformación Institucional del Ejército, así como Objetivos sectoriales y nacionales. En esa línea. Locatelli (2023), sostiene que en la mayoría de los países latinoamericanos los centros de ciberdefensa enfrentan dificultades debido a la falta de una doctrina operacional consolidada. Asimismo, Percca (2024) resalta que la eficacia institucional requiere de manuales de operación estandarizados y protocolos claros de actualización. Por lo tanto, es recomendable crear una Manual que sea el cimiento de las operaciones de Ciberdefensa, basados en los principios de eficiencia y eficacia, basado en la Estrategia Nacional de Ciberseguridad.

Finalmente, los indicadores: recursos utilizados por operación, tiempo medio de respuesta, Objetivos estratégicos alcanzados, Normas generadas tras intervención y Satisfacción operativa con el CCE, permitieron medir las dimensiones finales del instrumento eficiencia y eficacia, los resultados mostraron una asociación significativa entre la eficiencia ($r = 0.795$; $p < 0.001$) y la eficacia ($r = 0.853$; $p < 0.001$) en relación con el aporte del CCE a las OI. Estos hallazgos indican que la interacción de los indicadores influye directamente con el desempeño del CCE. Según Chiavenato (2011), la eficiencia y eficacia

deben de coexistir, ya que la primera garantiza el uso racional de medios, mientras que la segunda refleja el logro de los fines, así mismo, en el marco de la modernización publica Ley N° 27658, refuerza la obligación de las entidades estatales en orientar su gestión a resultados medibles y sostenibles.

Cuando se estableció la relación de las actividades cibernéticas por parte del CCE y su aporte a las OI, primero se tuvo que definir cuales eras las capacidades básicas que componen a las OI (Operaciones psicológicas, Operaciones de seguridad, decepción militar, Guerra Electrónica y Operaciones sobre redes informáticas), esta última capacidad básica es donde confluye el accionar y aporte del CCE, durante la investigación se demostró que tanto la madurez del sistema de ciberdefensa como las políticas y estrategias en el campo de ciberdefensa aún son muy reducidas y con niveles inferiores a las necesarias para brindar un servicio eficiente y eficaz a los diferentes niveles de comando en la toma de decisiones, teniendo repercusión en las decisiones tanto Estratégicas como operacionales, de no corregirse o impulsar el fortalecimiento de esta capacidad militar afectara directamente las operaciones militares, desde los niveles pre operacionales, donde se centra los esfuerzo por persuadir al oponente a iniciar acciones y más aún durante el conflicto se espera la confianza de la información y sus disponibilidad sostenida.

Por lo tanto el fortalecimiento del CCE, debe centrarse en una gestión basada es resultados, optimizando los recursos humanos y tecnológicos, asegurando el cumplimiento de objetivos, para ello la necesidad imperativa de tener indicadores que permitan medir el avance del CCE en el aporte a las OI, trabajar con indicadores de medición conocidos como KPI (Key Performance Indicator), ayudan a la mejora continua del desarrollo de ciberdefensa, clarifican los objetivos y metas, así como permiten mejorar la productividad por parte de CCE, lo que dará como resultado mejorar la toma de decisiones por parte del comando dentro de las acciones realizadas por las Operaciones de Información.

CONCLUSIONES

La investigación permitió demostrar que el CCE cumple un papel estratégico en el aporte a las OI, siendo ésta una capacidad esencial para la defensa nacional. Los resultados han evidenciado que existe correlación positiva y fuerte entre la percepción de personal militar y el aporte del CCE a las OI, lo que confirma su relevancia dentro del sistema digital del Ejército. Sin embargo, el estudio también reveló limitaciones estructurales y doctrinarias que restringen el pleno desarrollo de su potencial entre ellas la ausencia de objetivos estratégicos claramente definidos, carencia de mecanismos de evaluación del desempeño, la insuficiente capacitación del personal técnico, falta de infraestructura así como ausencia de ejercicios cibernéticos. Esta situación reafirma la necesidad de fortalecer la doctrina institucional de ciberdefensa, modernizar la infraestructura tecnológica y establecer indicadores clave de rendimiento (KPI) que permitan medir de forma objetiva y continua la eficiencia y eficacia de las operaciones del CCE. Dichos indicadores deben servir como herramientas de control y retroalimentación para orientar las acciones hacia la mejora del desempeño y la consecución de los objetivos estratégicos vinculados a las OI.

Por lo tanto, se concluye de manera general que para que el CCE consolide su aporte a las Operaciones de Información de manera sostenible y verificable, resulta imprescindible que establezca objetivos claros, metas precisas y métricas cuantificables que aseguren una gestión eficiente y eficaz. Solo así podrá convertirse en una capacidad militar aprovechable para el Ejército, de acuerdo con las demandas estratégicas de un entorno de guerra híbrida cada vez más complejo y digitalizado.

Respecto al Objetivo Específico N° 1, al análisis de los factores que influyen en la actividad del CCE, los resultados revelaron una correlación moderada y significativa ($r = 0.572$; $p < 0.001$), indicando que la frecuencia de ejercicios de ciberdefensa, la disponibilidad tecnológica, la coordinación interinstitucional y la falta de objetivos institucionales definidos influyen directamente en su desempeño operativo. Se concluye que la baja frecuencia de ejercicios prácticos y la falta de metas claras han limitado la capacidad del CCE para integrarse de manera efectiva en las OI. Por tanto, el fortalecimiento de su estructura operativa requiere una planificación sostenida, modernización tecnológica y un sistema de indicadores que mida el grado de actividad cibernética en apoyo a las operaciones militares.

Respecto al Objetivo Específico N° 2: En relación con el nivel de capacitación y entrenamiento en ciberseguridad, se verificó una correlación muy fuerte y significativa ($r = 0.839$; $p < 0.001$) con la eficiencia en el aporte del CCE a las OI. Esto confirma que la

profesionalización del personal constituye un factor decisivo en el desempeño institucional. Sin embargo, las percepciones neutrales y negativas sobre la suficiencia de los programas de formación evidencian una brecha en la actualización técnica. Se concluye que la eficiencia operativa del CCE depende directamente de la capacitación continua, de la implementación de programas de certificación internacional y del fortalecimiento de convenios académicos y tecnológicos con instituciones especializadas.

Respecto al Objetivo Específico N° 3: En cuanto al desarrollo y aplicación de estrategias de ciberseguridad, se estableció una correlación muy fuerte ($r = 0.840$; $p < 0.001$) entre dichas estrategias y la eficacia de las OI. No obstante, la falta de difusión interna y de mecanismos de evaluación limita la efectividad de las acciones implementadas. Se concluye que el CCE debe consolidar un marco normativo y operativo uniforme, sustentado en un Manual de Operaciones de Ciberdefensa, que integre procesos de planificación, ejecución y control, con énfasis en la medición del impacto institucional. De igual modo, la alineación de las estrategias con los objetivos del Plan de Transformación Institucional del Ejército y la Estrategia Nacional de Ciberseguridad permitirá fortalecer la eficacia organizacional y su contribución al entorno informacional del país.

RECOMENDACIONES

Para que el Centro de Ciberdefensa del Ejército (CCE) consolide su papel como una capacidad esencial dentro de las Operaciones de Información (OI) y garantice un aporte sostenible, verificable y medible, se recomienda establecer un sistema integral de gestión por resultados sustentado en indicadores clave de rendimiento (KPI). Este sistema debe permitir la evaluación continua del desempeño institucional en términos de eficiencia, eficacia y sostenibilidad operativa.

En relación con la realidad problemática identificada esta investigación plantea la elaboración de una Matriz de Indicadores de Ciberdefensa como herramienta metodológica y estratégica que permita superar dichas limitaciones. Esta matriz vinculará el Nivel de actividad, capacitación y entrenamiento en ciberseguridad en el CCE, desarrollo y aplicación de estrategias de ciberseguridad en el CCE así como las capacidades técnicas, la frecuencia, eficiencia y efectividad de los ejercicios de ciberdefensa, buscando que las acciones del CCE puedan evaluarse de manera objetiva y en función de su impacto real en las OI.

Con respecto al Objetivo Especifico N° 1, se recomienda que, se debe desarrollar un cronograma permanente de ejercicios cibernéticos conjuntos, tanto internos como con entidades civiles y policiales, que fortalezcan la interoperabilidad y permitan evaluar la capacidad de respuesta ante incidentes en tiempo real. Modernizar la infraestructura tecnológica y de conectividad de los hubs periféricos del CCE, priorizando la redundancia operativa y la expansión geoestratégica, a fin de garantizar cobertura nacional y sostenibilidad del sistema.

Con respecto al Objetivo Especifico N° 2, se recomienda que: se debe de buscar institucionalizar un programa permanente de formación y certificación en ciberseguridad, con niveles progresivos de especialización técnica y doctrinaria, adaptados a las funciones específicas del personal. Establecer convenios de cooperación interinstitucional con universidades, centros de investigación y organismos internacionales, que permitan la actualización continua en normas ISO, estándares NIST y marcos MITRE ATT&CK.

Incorporar métricas de desempeño individual y colectivo, vinculadas a los resultados operativos del CCE en apoyo a las OI, como el porcentaje de misiones exitosas, el tiempo medio de respuesta y reducción de vulnerabilidades. Crear un repositorio institucional de lecciones aprendidas y buenas prácticas en ciberdefensa, que permita consolidar conocimiento táctico y estratégico y sirva de base para la formación de nuevas generaciones

de especialistas y disminuir errores de aplicación.

Con respecto al Objetivo Especifico N° 3, se recomienda: Elaborar un Manual de Operaciones de Ciberdefensa del Ejército del Perú, que integre doctrinas, protocolos de actuación, y mecanismos de evaluación de impacto, alineado a los planes estratégicos sectoriales y a estándares internacionales de gestión de incidentes.

Implementar un sistema de monitoreo y evaluación de las estrategias cibernéticas, con indicadores que midan la eficacia de las políticas aplicadas, el cumplimiento de objetivos estratégicos y la generación de normas derivadas de cada intervención.

Fortalecer la difusión interna de las estrategias del CCE, garantizando que los mandos operativos y las grandes unidades de batalla comprendan su rol en el ecosistema informacional del Ejército.

PROPUESTA PARA ENFRENTAR LA REALIDAD PROBLEMÁTICA

5.1 Introducción

El Centro de Ciberdefensa del Ejército (CCE), como unidad operativa del Comando de Operaciones Cibernéticas del Ejército (COCIBER), tiene la responsabilidad de desarrollar operaciones de ciberdefensa orientadas a la detección, ataque, respuesta, explotación del ciberespacio y análisis forense. No obstante, se ha identificado una brecha significativa en la implementación efectiva de esta capacidad militar, necesaria para el desarrollo de Operaciones de Información (OI), las cuales constituyen un componente estratégico para la toma de decisiones del comando, así como influir, interrumpir o contrarrestar la información proveniente de un posible adversario, fortaleciendo de este modo la disuasión estratégica.

Los resultados de la investigación demostraron que los principales problemas en el aporte del CCE a la Operaciones de Información, se relacionan a cinco dimensiones: nivel de actividad, Capacitación y entrenamiento, desarrollo y aplicaciones de estrategias de ciberseguridad, Nivel de Eficacia y el Nivel de Eficiencia. Estas limitaciones restringen la capacidad del CCE para generar resultados que fortalezcan las OI, y apoyen a una efectiva toma de decisiones .

Esta situación problemática deberá de enfrentarse con acciones integrales en los ámbitos doctrinarios, tecnológico y gestión del conocimiento. En ese sentido el CCE deberá establecer objetivos claros, metas alcanzables y medibles, que permitan orientar la planificación y evaluación de su desempeño. La carencia de indicadores vinculados directamente a los objetivos estratégicos ha generado una percepción negativa institucional, particularmente por en las unidades de comunicaciones, debido a la falta de evidencia sobre el impacto real de sus actividades en el cumplimiento de la misión del CCE.

Por ello, la propuesta planteada en este acápite consiste en la implementación de Indicadores Claves de desempeño (KPI), diseñados a base de objetivos operativos y metas alcanzables, con el propósito de mejorar la eficacia y eficiencia del CCE. Para ello, se ha considerado la metodología propuesta en la Guía para la elaboración de indicadores 2024 del Centro Nacional de Planeamiento Estratégico (CEPLAN, 2024), adaptándola al contexto de ciberdefensa en el Ejército. Esta propuesta permitirá fortalecer la gestión por resultados, mejorar la percepción de desempeño del CCE y sobre todo, garantizar una contribución sostenida y verificable a las OI que realiza el Ejército del Perú, bajo el principio de que no se puede mejorar lo que no se puede medir.

5.2 Fundamentación teórica – metodológica de la propuesta

Sustento teórico

La propuesta se sustenta en el principio de modernización institucional, establecido en la Ley N° 27658, Ley Marco de la Modernización de la Gestión del Estado (PCM, 2001), la cual orienta a las entidades públicas hacia una gestión eficiente, eficaz y basada en resultados. En ese marco, la medición del desempeño institucional mediante indicadores constituye un instrumento para la toma de decisiones. Su aplicación en el ámbito militar responde a la necesidad de garantizar la efectividad institucional y la sostenibilidad de las capacidades militares.

En el Plan de transformación Institucional del Ejército del Perú, refuerza esta visión de establecer al establecer en su Objetivo Estratégico N° 5: Desarrollar la Ciberdefensa en el Ejército, orientando sus esfuerzos hacia la consolidación de capacidades digitales y la integración de tecnologías emergentes en la conducción de las operaciones militares (Ejército del Perú, 2022). En ese contexto el CCE, constituye un componente esencial para la defensa del ciberespacio institucional y la ejecución de las OI, las cuales comprenden acciones destinadas a influir, interrumpir, o proteger los sistemas informáticos y de comunicaciones del adversario, integrando capacidades como la guerra electrónica, operaciones psicológicas y seguridad de las informaciones.

El fundamento teórico de la propuesta reconoce que la eficacia institucional se mide por el grado en que las acciones realizadas alcanzan los objetivos planificados (Rodríguez et al., 2024), mientras que la eficiencia se asociada con el uso racional de los recursos disponibles para lograr esos objetivos (Chiavenato, 2011). Así pues, los indicadore claves de desempeño (KPI) se presentan como objetivos estratégicos otorgando visibilidad a los resultados alcanzados por el CCE en términos de eficiencia y eficacia.

Huertas (2023) y Quevedo (2023), destacan que, en las instituciones de defensa el desarrollo de capacidades cibernéticas no depende únicamente de la infraestructura o tecnología, sino también de la capacidad para medir el impacto real de las acciones, lo que convierte a los indicadores en un elemento fundamental para el fortalecimiento de la gestión militar y la consolidación de una doctrina de ciberdefensa.

Sustento metodológico

Desde un punto de vista metodológico, la propuesta adopta los lineamientos de la Guía para la elaboración de indicadores 2024 del Centro Nacional de Planeamiento Estratégico (CEPLAN, 2024), la cual plantea que todo indicador debe construirse siguiendo los criterios SMART: especifico medible, alcanzable, relevante y limitado en el tiempo. Este enfoque permite que los indicadores de ciberdefensa sean claros verificables y orientados

a la mejora del desempeño del CCE.

La matriz de indicadores de ciberdefensa que se propone, para que sea empleada como herramienta de planificación y control estratégico que permitirá ingresar los resultados de la investigación en un sistema de medición formal. Su diseño toma en cuenta las cinco dimensiones analizadas: *nivel* de actividad*,* Capacitación y entrenamiento, desarrollo y aplicaciones de estrategias de ciberseguridad, Nivel de Eficacia y el Nivel de Eficiencia. Cada dimensión se vinculará con indicadores cuantitativos y cualitativos, que logren el cumplimiento de los objetivos del CCE.

Metodológicamente, la propuesta se estructura en fases, que abarcan desde el diagnóstico y formulación de indicadore, hasta la evaluación de resultados. Este proceso se apoyará por herramientas del CEPLAN, para garantizar la coherencia con los objetivos, acciones y resultados.

Finalmente esta propuesta, responde a la necesidad identificada: ausencia de indicadores que midan el desempeño del CCE. La implementación de esta matriz de indicadores permitirá transformar esta limitación en una oportunidad de mejora continua, asegurando la trazabilidad, optimización de recursos y toma de decisiones acertada y fundamentada en evidencia empírica.

5.3 Desarrollo de la propuesta

La propuesta para fortalecer el desempeño del CCE, se desarrollará a través de la implementación de una Matriz de indicadores de Ciberdefensa, integrada a otros documentos de gestión. Pero básicamente es te instrumento, permitirá medir de forma objetiva la eficiencia y eficacia, de las operaciones cibernéticas y su aporte a las OI que realiza el Ejército del Perú. El desarrollo de la propuesta se efectuará en cuatro fases, para una implementación progresiva y adaptable a la situación de la institución.

5.3.1 Diagnóstico inicial del CCE

El análisis de los resultados de la investigación permito identificar que el CCE, enfrenta limitaciones operativas y doctrinarias que reducen su aporte a las OI. Entre las principales deficiencias se encuentran la baja frecuencia de ejercicios de ciberdefensa, escasa capacitación del personal especialista , y la ausencia de objetivos e indicadores que permitan medir el desempeño. Estas deficiencias impiden consolidar una estructura eficiente. Por lo tanto se requiere de una herramienta de gestión que oriente sus acciones y permita evaluar los resultados.

5.3.2 Estrategia general

Se orienta a la implementación de Matriz de Indicadores de Ciberdefensa, concebida como instrumento de gestión por resultados que permitan evaluar de manera objetiva al CCE. Esta matriz vinculará las dimensiones definidas, con los indicadores, para

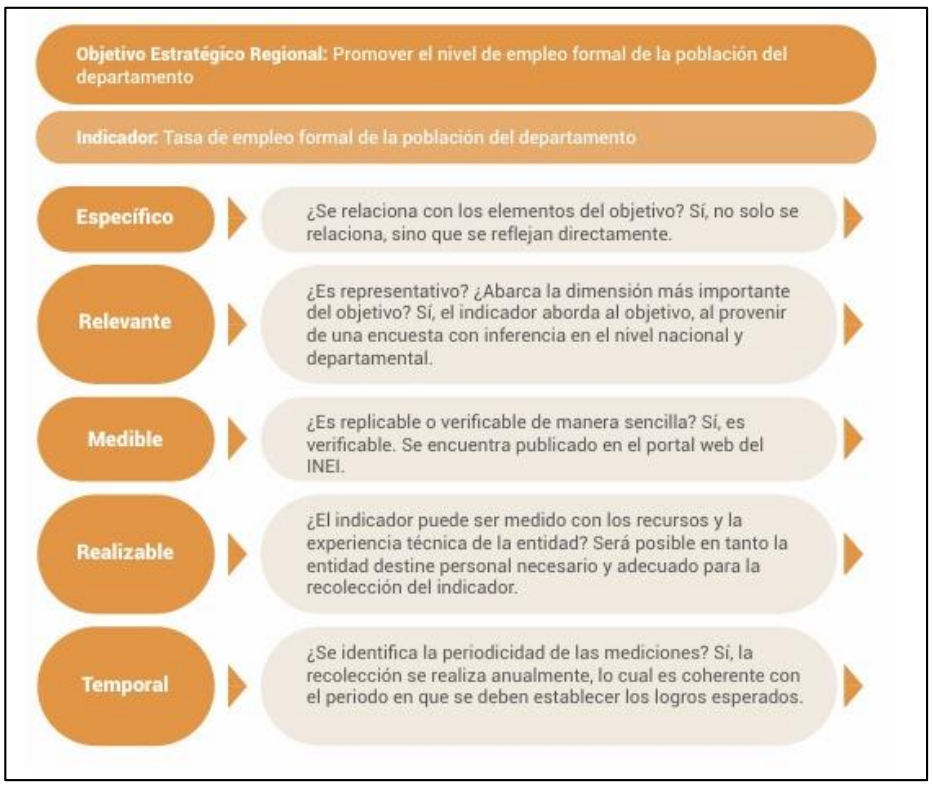
proporcionar información confiable que fomente la mejora continua y permita alinear las actividades que realice el CCE.

5.3.3 Fases de implementación

5.3.3.1 Diseño de objetivos. En base al diagnóstico inicial del CCE y revisión de los procesos, se elaborarán los objetivos de acuerdo con la metodología de CEPLAN (CEPLAN, 2024), y luego metas e indicadores. Para ello, los investigadores plantean esta Matriz de Objetivos e Indicadores de Ciberdefensa, incluida en el anexo 9 del informe de investigación, la cual es perfectible para que sea tomado como base por los especialistas del COCIBER o la Dirección de Planeamiento del Ejército (DIPLANE).

Figura 12

Ejemplo de Preguntas tipo para validar las características deseables.



Nota. La figura muestra que preguntas realizarse para la elaboración de indicadores. Fuente: CEPLAN (2024).

En base a la Figura 12 se plantearos 2 objetivos con sus respectivas metas, las cuales pueden verse en la tabla N° 20.

Tabla 20

Tabla de Objetivos y metas.

Objetivos	Metas
Objetivo 1: Capacitar al personal del CCE, a fin de que cuenten con las competencias de ciberdefensa necesarias para desarrollar ataque, respuesta, explotación y análisis forense.	Meta 1.1: Capacitar al personal de Oficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.
	Meta 1.2: Capacitar al personal de Técnicos y Suboficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.
Objetivo 2: Realizar Operaciones de ciberdefensa que permitan el uso efectivo del ciberespacio.	Meta 2.1: Reducir el tiempo de respuesta ante incidentes por parte del CCE.
	Meta 2.2: Incrementar la cobertura y aplicación de ciberdefensa del CCE en las redes del Ejército.
	Meta 2.3: Incrementar las operaciones y acciones de ciberdefensa por parte el CCE.

Nota. Se presentan las tablas con sus respectivas metas.

5.3.3.2 Diseño de Matriz de indicadores de Ciberdefensa. Para lo cual se plantearon dos objetivos.

***Objetivo 1*.** Capacitar al personal del CCE, a fin de que cuenten con las competencias de ciberdefensa necesarias para desarrollar ataque, respuesta, explotación y análisis forense.

Tabla 21

Tabla de Metas e indicadores del objetivo N° 1.

	SMART	
METAS	**1.1**Capacitar al personal de Oficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.	**1.2** Capacitar al personal de Técnicos y Suboficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.
ESPECIFICO	Mejorar el nivel de capacitación del personal de oficiales en ciberdefensa.	Mejorar el nivel de capacitación del personal de Técnicos y Suboficiales en ciberdefensa.
MEDIBLE	% de Oficiales Capacitados en desarrollar ataque, respuesta, explotación y análisis forense.	% de Técnicos y SSOO, capacitados en desarrollar ataque, respuesta, explotación y análisis forense.
ALCANZABLE	Alcanzar el 85 % de Oficiales Capacitados en ataque, respuesta y explotación.	Alcanzar el 70 % de Técnicos y Suboficiales Capacitados en ataque, respuesta y explotación.
	Alcanzar el 30% de Oficiales capacitados en análisis forense de redes.	Alcanzar el 50% de Técnicos y Sub Oficiales capacitados en análisis forense de redes.
RELEVANTE	Mejora las competencias del personal y permite desarrollar Ciberdefensa por parte del CCE.	Mejora las competencias del personal y permite desarrollar Ciberdefensa por parte del CCE.
TIEMPO	Mediciones Semestrales y Anuales.	Mediciones Semestrales y Anuales.

Nota. Indicadores elaborados en base a las metas.

***Objetivo 2*.** Realizar Operaciones de ciberdefensa que permitan el uso efectivo del ciberespacio.

Tabla 22

Tabla de Metas e indicadores del objetivo N° 2.

SMART			
METAS	2.1 Reducir el tiempo de respuesta ante incidentes por parte del CCE.	2.2 Incrementar la cobertura y aplicación de ciberdefensa del CCE en las redes del Ejército.	2.3 Incrementar las operaciones y acciones de ciberdefensa por parte el CCE.
ESPECIFICO	Optimizar el proceso de respuesta por parte del CCE frente a un incidente de seguridad informática.	Ampliar el área de cobertura actual de las operaciones de ciberdefensa realizadas por CCE.	Asegurar las redes informáticas del Ejército mediante la ciberdefensa.
MEDIBLE	% de reducción en la respuesta por parte de CCE, frente a incidente de seguridad informática.	% de incremento de la cobertura de ciberseguridad en redes informáticas por parte del CCE.	% de incremento de las operaciones de ciberdefensa realizadas por el CCE.
ALCANZABLE	Reducir en 30 % el tiempo de respuesta frente a incidentes de seguridad Informática.	Alcanzar el incremento de un 25 % de redes informáticas coberturadas por el CCE	Alcanzar el incremento del 35 % de las operaciones y acciones de ciberdefensa por el CCE.
RELEVANTE	Permite mejorar la eficiencia de la producción del CCE.	Permite mejorar la eficacia Toma de decisiones por parte de los diferentes niveles de comando.	Mejora la eficacia en la Toma de decisiones por parte de los diferentes niveles de comando.
TIEMPO	Medición Semestral y Anual.	Medición Semestral y Anual.	Medición Semestral y Anual.

Nota. Indicadores elaborados en base a las metas.

5.3.3.3 Ejecución de prueba piloto y capacitación del personal. Se recomienda implementar un plan piloto que permite comprobar la operatividad de indicadores, para ello los investigadores proponen un “Plan de Implementación 3/6/12”, incluida en el anexo 10 del informe de investigación. Así mismo, se debe de desarrollar un programa de capacitación orientado al personal del CCE, enfocado en el manejo de herramientas de seguimiento, para la realización de ajustes.

5.3.3.4 Implementación en el CCE y monitoreo. Contando con los indicadores validados, se propone que se establezcan directivas para que los Hubs regionales también las implementen, de igual forma se recomienda que se elabore tableros de control digital que permitan visualizar los avances, establecer alertas y niveles de cumplimiento de objetivos y metas del CCE.

5.3.3.5 Evaluación y Mejora continua. El monitoreo de la propuesta se llevará a cabo empleando la Matriz de objetivos e indicadores de Ciberdefensa, la cual integrará los resultados derivados de la ejecución de actividades orientadas al cumplimiento de los objetivos del CCE. Este proceso permitirá verificar el avance institucional y el grado de eficacia en cada fase. En concordancia con el Plan de Implementación 3/6/12, se establecerá un cronograma de seguimiento que incluirá la elaboración de informes, trimestrales, semestrales y un informe anual consolidado.

5.4 Recursos necesarios para la implementación

5.4.1 Recursos humanos

El desarrollo de la propuesta exigirá de un equipo multidisciplinario conformado por personal especialista en ciberseguridad, Planeamiento estratégico, gestión pública y analista de datos. Responsables de validar, aplicar y monitorear los indicadores propuestos en las matrices.

5.4.2 Recursos tecnológicos

La implementación de los indicadores propuestos en los indicadores requiere de la actualización de servidores seguros, adquisición de software de gestión de indicadores, plataformas de análisis de datos y otros sistemas de respaldo. Para que se integrado a un tablero de mando que visualice el avance de metas.

5.4.3 Recursos Financieros

La propuesta demandará una planificación presupuestal destinada prioritariamente a infraestructura tecnológica, capacitación de personal, e implementación de softwares digitales.

5.5 Resultados esperados en la implementación de KPI por el CCE.

Para concretar la propuesta de implementación de KPI orientados a medir la eficiencia, eficacia y resultados en el CCE, será necesario establecer un plan estructurado que defina acciones prioritarias de primer orden, complementadas con acciones de segundo orden que sean alcanzables dentro de un horizonte temporal definido. Esto permitirá realizar un seguimiento y una evaluación posterior mediante medidores claros y verificables, identificando áreas de mejora y fortaleciendo la definición de objetivos y metas

institucionales.

La implementación de este sistema también contribuirá a optimizar el uso de recursos humanos, tecnológicos y financieros del CCE incrementando su productividad y desempeño. Como consecuencia, se espera una mejora significativa en la percepción del personal de las Unidades de Comunicaciones respecto a la efectividad del CCE dentro del Ejército del Perú.

Así mismo, podrán establecerse indicadores complementarios a los propuestos en este estudio, siempre que se mantengan alineados y/o relacionados directa o indirectamente con los objetivos que tiene el CCE y con los productos que sirvan de insumo para las OI, las cuales tienen como capacidad básica las operaciones de redes informática. La correcta articulación de estos indicadores permitirá en un corto plazo, consolidar el aporte del CCE al fortalecimiento de las OI y con ello la defensa del ciberespacio.

REFERENCIAS BIBLIOGRÁFICAS

Abarca Sánchez, Y., & Barreto Rivera, U. (2020). Capacidad de absorción del conocimiento, aprendizaje y tecnologías de la información en las organizaciones: estado del arte y evolución de la investigación. *Apuntes Universitarios*, *11*(1). https://doi.org/10.17162/au.v11i1.558

Albornoz, S. J. (2024). *Conducción de las operaciones de información en el nivel componente terrestre del teatro de operaciones* [Trabajo final integrador, Escuela Superior de Guerra "Tte. Grl. Luis María Campos", Ciudad Autónoma de Buenos Aires]. https://cefadigital.edu.ar/handle/1847939/2732

Anca, L. J. (2015). *La conducción de las operaciones de ciberdefensa: Principios básicos en el campo de combate moderno* [Trabajo final integrador, Instituto de Enseñanza Superior del Ejército, Escuela Superior de Guerra "Tte. Grl. Luis María Campos"]. https://cefadigital.edu.ar/bitstream/1847939/430/1/TFI%20ECS%202015%20A3C4_39.pdf

Bazán, L. G. S. (2021). La metodología de indagación y el aprendizaje de las Ciencias Naturales. *Revista multidisciplinaria de innovación y estudios aplicados, Polo del Conocimiento*. https://polodelconocimiento.com/ojs/index.php/es/article/view/3406/html

Bermúdez, J. D., Castro, J. J., Peralta, D. A., y Guacaneme, P. A. (2023). *Técnicas avanzadas de ciberseguridad: Integración y evolución de la Kill Chain en diversos escenarios* [Cornell University]. https://arxiv.org/pdf/2306.09242

Betancur Betancur, O. A. (2023). *Plan de eficiencia administrativa y cero papel* [Trabajo académico, Universidad de Antioquia, Escuela Interamericana de Bibliotecología, Programa de Archivística].https://bibliotecadigital.udea.edu.co/bitstream/10495/35233/2/BetancurOscar_2023_PlanCeroPapel.pdf

Bolaños Cerón, Á. D. (2020). Eficacia y eficiencia en los procesos de reclutamiento y selección de personal. *Revista Biumar*, *4*(1), 134–146. https://doi.org/10.31948/BIUMAR4-1-art11

Cadillo Duran, R. E. (2021). *La concientización en ciberseguridad y su relación con la seguridad informática en el servicio de informática de la fuerza aérea del Perú, 2020* [Tesis de

maestría, Escuela Superior de Guerra Aérea]. Repositorio Institucional FAP. http://repositorio.fap.mil.pe/handle/fap/263

Calderón Arregui, D., y Sánchez Gordon, W. (2023). El Camino hacia el Liderazgo Militar de Excelencia: Estrategias para formar Líderes Efectivos en la Escuela Superior Militar "Eloy Alfaro." *Revista de Ciencias de Seguridad y Defensa*, *8*(03), 18. https://doi.org/10.24133/RCSD.VOL08.N03.2023.02

Cano Martínez, J. J. (2024). Ciberdefensa basada en datos. *Revista Sistemas*, *(170)*, 49–60. https://doi.org/10.29236/SISTEMAS.N170A6

Cásale, C. G. (2022). *La ciberdefensa como factor crítico en el desarrollo de operaciones militares en el nivel operacional* [Tesis de Maestría, Escuela Superior de Guerra Tte Grl Luis María Campos]. Repositorio Cefa Digital. http://cefadigital.edu.ar/handle/1847939/2585

Centurión, E. S. O., & Rodríguez, J. E. P. (2023). Gestión de incidentes para la seguridad de la información en una empresa: una revisión sistemática. *Revista de Investigación Multidisciplinaria CTSCAFE*, *7*(20), 19. https://www.ctscafe.pe/index.php/ctscafe/article/view/242

Chamorro, I. A. R. (2023). La ciberseguridad como factor estratégico en la defensa nacional. *Revista de Seguridad y Defensa*. https://doi.org/10.25062/2955-0270.4819

Chiavenato, I. (2011). *Planeación estratégica: Fundamentos y aplicaciones* (2da ed.). McGraw-Hill Interamericana. https://bluebooksoft.com/GESTION_ADMINISTRATIVA/2216.pdf

Clarke, R. A., y Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press. https://books.google.com.pe/books/about/The_Fifth_Domain.html?id=F1X4DwAAQBAJ&redir_esc=y

CEPLAN. (2024). *Guía para la elaboración de indicadores*. https://www.ceplan.gob.pe/guia-indicadores-2024

Cruz García, M. A. (2019). Fuentes de Información. *Boletín Científico de Las Ciencias Económico Administrativas Del ICEA*, *8* (15). https://doi.org/10.29057/icea.v8i15.4864

Decreto Legislativo N° 1137 (2012). *Ley del Ejército del Perú*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/883445-1

Decreto Legislativo N° 1640 (2024). *Decreto Legislativo que modifica la Ley N° 30999, Ley de Ciberdefensa, para fortalecer las capacidades de ciberdefensa del Estado peruano*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2324483-1

De Lunetta, A., y Guerra, R. (2023). Metodologia da pesquisa científica e acadêmica. *Revista OWL (OWL Journal)-Revista Interdisciplinar de Ensino e Educação*, *1*(2), 149–159. https://doi.org/10.5281/zenodo.8240361.

Department of Defense. (2017). *Military information support operations*. Joint Chiefs of Staff. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf

Department of Defense. (2021). *Joint Publication 3-13, Information operations*. Joint Chiefs of Staff. https://informationsecurity.info/wp-content/uploads/2021/04/jp3_13.pdf

Díaz, C. A. (2022). *Estudios de posgrado de utilidad para la Fuerza en articulación con el Plan de Carrera* [Trabajo final integrador, Escuela Superior de Guerra “Tte. Grl. Luis María Campos”]. https://cefadigital.edu.ar/jspui/bitstream/1847939/2850/1/TFI%2023-2022%20DIAZ.pdf

Dobbertin Guerrero, E. B. (2023). *Perfil profesional del personal militar y la ciberdefensa en el grupo de operaciones en el ciberespacio de la Fuerza Aérea del Perú, año 2022* [Tesis de maestría, Escuela Superior de Guerra Aérea]. Repositorio Institucional FAP. http://repositorio.fap.mil.pe/handle/fap/332

Drucker, P. F. (2006). *La gerencia en la sociedad futura*. Editorial Norma. https://politecnicometro.edu.co/wp-content/uploads/2021/08/Drucker-PeterLa-Gerencia-en-La-Sociedad-Futura.pdf

Ejército del Perú. (2022). *Plan de Transformación Institucional V 2.0*. Ejército del Perú.

Escobar, A. A. H., Rodríguez, M. P. R., López, B. M. P., Ganchozo, B. I., Gómez, A. J. Q., y Ponce, L. A. M. (2018). *Metodología de la investigación científica*. 3Ciencias. ISBN 978-84-948257-0-5. https://3ciencias.com/wp-content/uploads/2018/02/MIC_breve.pdf

Félix, Á., y Suñagua, D. (2013). Auditoria de seguridad de información. *Fides et Ratio - Revista de Difusión Cultural y Científica de La Universidad La Salle En Bolivia*, *6*(6), 19–30. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2013000100004&lng=es&nrm=iso&tlng=es

Fonfría, A., & Duch-Brown, N. (2020). Elementos para una política de ciberseguridad efectiva. Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/elementos-para-una-politica-de-ciberseguridad-efectiva/

Galushchenko, O., Pidbereznykh, I., Piroh, O., Khrapach, D., y Tolmachov, O. (2024). Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current trends [Ciberseguridad y dimensiones geopolíticas de las intervenciones informativas externas en Ucrania: Análisis de las tendencias actuales]. *Data and Metadata*, *3*. https://doi.org/10.56294/dm2024.345

García, M. A. P. (2017). La individualización en la preparación técnica: un análisis teórico. *Arrancada, 17*(31), 28–37. https://dialnet.unirioja.es/servlet/articulo?codigo=9119951

Girón Figueroa, W. F. (2021). *Necesidad de una política nacional de ciberseguridad para infraestructuras críticas en Guatemala* [Tesis doctoral, Universidad de San Carlos de Guatemala]. Universidad de San Carlos de Guatemala. http://biblioteca.usac.edu.gt/tesis/04/04_15455.pdf

González, G. M. (2022). *Influencia de las capacidades satelitales en el nivel operacional y su aplicación al componente naval argentino en función a los objetivos generales de la DPDN* [Tesis, Escuela Superior de Guerra Conjunta]. Repositorio Cefa Digital. https://cefadigital.edu.ar/handle/1847939/2355

Guerrero, R. E. A., Guerrero, B. E. C., Carrasco, J. C. B., & Gonzáles, K. E. B. (2022). La ciberseguridad como herramienta de defensa nacional. *Revista Científica Multidisciplinaria*. https://doi.org/10.37811/cl_rcm.v6i5.3724

Hatch, B. (2019). The Future of Strategic Information and Cyber-Enabled Information Operations. *Journal of Strategic Security*, *12*(3), 112-135. https://www.researchgate.net/publication/337807264_The_Future_of_Strategic_Information_and_Cyber-Enabled_Information_Operations

Hernández-Sampieri, R., y Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. Universidad Nacional Autónoma de México. https://doi.org/10.22201/fesc.20072236e.2019.10.18.6

Huamán Baltazar, J. L. (2021). *Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército, Lima, 2020* [Tesis de maestría, Escuela de Guerra del Ejército]. Repositorio de la Escuela de Guerra del Ejército. http://repositorio.esge.edu.pe/handle/ESGEEPG/692

Huertas Espíritu, P. R. (2023). *La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022* [Tesis de Maestría, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/118434/Huertas_EPR-SD.pdf?sequence=1

Jiménez Fabian, A. L. (2023). *Propuesta para incrementar la eficiencia operacional y validación del proceso de producción por control numérico* [Tesis de Doctorado, Universidad Autónoma del Estado de México]. Repositorio Institucional RIAA. https://riaa.uaem.mx/xmlui/bitstream/handle/20.500.12055/4070/JIFABD08.pdf?sequence=1&isAllowed=y

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *(E62)*, 16–31. https://dialnet.unirioja.es/servlet/articulo?codigo=10050181

Kasper, A., Osula, A.-M., & Molnár, A. (2021). EU cybersecurity and cyber diplomacy [Ciberseguridad y ciberdiplomacia de la UE]. *Revista de Internet, Derecho y Política*, *(34)*. https://doi.org/10.7238/idp.v0i34.387469

Ley N° 27658 (2002), *Ley Marco de Modernización de la Gestión del Estado*. (2002, 30 de enero). *Diario Oficial El Peruano. https://www.leyes.congreso.gob.pe/Documentos/Leyes/27658.pdf*

Ley N° 30999 (2019). *Ley de Ciberdefensa*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/1771966-1

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press. https://api.pageplace.de/preview/DT0400.9780511282959_A23677009/preview-9780511282959_A23677009.pdf

Lin, H., & Kerr, J. (2021). On cyber-enabled information warfare and the need for a national strategy. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680

Locatelli, O. (2023). *Ciberdefensa y ciberseguridad en las operaciones militares en el Comando de Operaciones de Defensa interna de Paraguay* [Trabajo de Investigación, Institución

de Defensa de Argentina]. Repositorio Cefa Digital. https://cefadigital.edu.ar/handle/1847939/2598

Maximiliano, C., Ravera, L., y Moresi, M. A. (2024). *El rol y las capacidades cibernéticas de las Fuerzas Armadas de la República Argentina en el marco de los conflictos futuros* [Trabajo de Investigación, Institución de Defensa de Argentina]. Repositorio Cefa Digital. https://cefadigital.edu.ar/handle/1847939/2657

Mora Arroyo, J. E., **y** Parra Mogollón, H. J. (2021). Asignación dinámica de espectro en redes inalámbricas de nueva generación: una aproximación al estado del arte. *Publicaciones e Investigación*, *15*(4). https://doi.org/10.22490/25394088.5590

Moya, J. G. (2023). La seguridad digital en el marco de la defensa nacional. *Revista Iberoamericana de Investigación y Formación*, 2(2). https://doi.org/10.62465/riif.v2i2.11

Olayinka Are, J. (2020). *Ciberguerra y seguridad nacional en Nigeria: análisis de las capacidades de las Fuerzas Armadas para enfrentar las amenazas del ciberespacio (2009-2018)* [Tesis de Maestría, Institución de Defensa de Argentina]. Repositorio Cefa Digital. https://cefadigital.edu.ar/handle/1847939/2168

Oliveira, C. C. R. B., Carneiro, B. R., Santos, I. S. C., Marinho, C. S., Silva, E. P. E., Coelho, A. C. C., **y** Pires, C. G. da S. (2025). Sociodemographic factors and level of physical activity in military police officers at work [Fatores sociodemográficos e nível de atividade física em policiais militares no trabalho; Factores sociodemográficos y nivel de actividad física de los policías militares en el trabajo]. *Cogitare Enfermagem*, *30*. https://doi.org/10.1590/ce.v30i0.95375pt

Onetto, R. K. (2024). Evolución doctrinaria de las operaciones de información y los desafíos para un empleo integral. En *Las operaciones de información en el contexto de las operaciones militares* (pp. 64–89). Publicaciones Acague. https://publicacionesacague.cl/index.php/tica/issue/view/40

Pampa Urieta, A. B. (2023). *Capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021* [Tesis de maestría, Escuela Superior de Guerra del Ejército]. Repositorio Institucional ESGE. https://repositorio.esge.edu.pe/items/523e6215-36b4-4b8a-8f90-59212b881fa6

Percca Trejo, R. N. (2024). *Capacidades de Operaciones de Información y su Influencia en las Operaciones y Acciones Terrestres Unificadas, 2021* [Tesis de Maestría, Escuela

Superior de Guerra del Ejército]. Repositorio Institucional ESGE. https://hdl.handle.net/20.500.14141/291

Pérez, A. L., y Cela, K. (2022). *Validación de un cuestionario de evaluación de actitud y autopercepción del pensamiento crítico de estudiantes universitarios* [Tesis de Licenciatura, Universidad Central del Ecuador]. Repositorio de la Universidad Central del Ecuador. http://www.dspace.uce.edu.ec/handle/25000/27079

Poot Poot, J. E. (2022). Seguridad en redes 5G. En *Exploraciones, Intercambios y Relaciones Entre El Diseño y La Tecnología* (pp. 57–79). Universidad de Quintana Roo. https://risisbi.uqroo.mx/bitstreams/dac4a3ce-2bb8-44ec-85ad-674fa4cd3b08/download

Presidencia del Consejo de Ministros. (2022). *Estrategia Nacional de Seguridad y Confianza Digital*. Secretaría de Gobierno y Transformación Digital. https://www.gob.pe/institucion/pcm/informes-publicaciones/3252954-estrategia-nacional-de-seguridad-y-confianza-digital

Presidencia del Consejo de Ministros. (2022). *Política Nacional de Modernización de la Gestión Pública al 2030*. https://cdn.www.gob.pe/uploads/document/file/3531092/POL%C3%8DTICA%20NACIONAL%20DE%20MODERNIZACI%C3%93N%20DE%20LA%20GESTI%C3%93N%20P%C3%9ABLICA%20AL%202030%281%29.pdf.pdf?v=1661208943

Quevedo Lezama, C. (2023). Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional. *Revista de Ciencia e Investigación En Defensa*, *4*(1), 55–76. https://www.researchgate.net/publication/368609127_Ciberdefensa_y_ciberseguridad_en_el_Peru_realidad_y_retos_en_torno_a_la_capacidad_de_las_FF_AA_para_neutralizar_ciberataques_que_atenten_contra_la_seguridad_nacional

Reyes, E. (2022). *Metodología de la investigación científica*. Page Publishing Inc. https://books.google.com.pe/books?id=SmdxEAAAQBAJ

Rivero Belveder, E. S. (2023). Ciberdefensa: Los Desafíos del Mundo Virtual. *Revista Seguridad y Poder Terrestre*, *2*(2). https://doi.org/10.56221/SPT.V2I2.29

Rodríguez, C. R., Oré, J. L. B., y Vargas, D. E. (2021). *Las variables en la metodología de la investigación científica* (Vol. 78). 3Ciencias. https://doi.org/10.17993/IngyTec.2021.78

Rodríguez-Barboza, J. R., Vásquez-Pajuelo, L., Andrade-Díaz, E. M., Bartra-Rivero, K. R., Sánchez-Aguirre, F. de M., y Ruiz-Villavicencio, R. E. (2024). Evaluación de la Eficiencia de la Gestión Pública en la Productividad Laboral. *Revista InveCom*, *4*(2). https://doi.org/10.5281/zenodo.10574091

Rojas Martínez, O. A. (2022). Educación e institucionalidad: Fuerzas Militares de Colombia y los Objetivos de Desarrollo Sostenible de la Agenda 2030. *Estudios En Seguridad y Defensa*, *17*(34), 247–266. https://dialnet.unirioja.es/servlet/articulo?codigo=9832175

Rutz, A. (2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. *Revista Defensa Nacional-Nro. 6*. https://www.studocu.com/es-ar/document/universidad-siglo-21/ciberdelitos/aportes-a-la-ciberdefensa-y-ciberseguridad-para-la-gestion-de-las-infraestructuras-criticas-de-la-informacion-en-argentina/69374439

Sales, C. M. D., Saraiva, A., y Faísca, L. (2017). Resiliency training in portuguese army basic instruction: The role of military cohesion, self-esteem and anxiety [Treino da resistência psicológica na recruta militar em Portugal: O papel da coesão militar, da autoestima e da ansiedade na resiliência; Entrenamiento de la Resistencia Psicológica en el Reclutamiento Militar en Portugal: El Papel de la Cohesión Militar, de la Autoestima y de la ansiedad en la resiliencia]. *Avances En Psicologia Latinoamericana*, *35*(2), 317–337. https://doi.org/10.12804/revistas.urosario.edu.co/apl/a.3626

Sandoval, Ó. J. M., Roque, V. M. P., y Urieta, A. B. P. (2024). El enfoque estratégico de la planificación y gestión de implementación de las capacidades militares. *Pensamiento Conjunto*, *12*(2), 18. https://pensamientoconjunto.com.pe/index.php/PC/article/view/145

Soares-Santeugini, M. J., Rodriguez-Prieto, I. E., Alfonso-Mora, M. L., y Sandoval-Cuellar, C. (2025). Relationship between physical activity and the sense of coherence in healthy adults [Relación entre el nivel de actividad física y el sentido de coherencia en adultos sanos]. *Atención Primaria*, *57*(5). https://doi.org/10.1016/j.aprim.2024.103106

Tafur Puerta, J. (2022). El derecho del acceso a la información, transparencia de la gestión pública y datos abiertos en los gobiernos locales del Perú. *Revista Científica de Sistemas e Informática*, *2*(1), e274. https://portal.amelica.org/ameli/journal/535/5353228004/5353228004.pdf

Torres, B., Antonio, M., Romaní, L., y Lima, A. (2022). *Importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde el sétimo ciclo de la EBR*

en el Perú [Tesis de Licenciatura, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/23667

Torres, A. M., y Albújar, D. P. M. (2024). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones* [Tesis de Licenciatura, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/27284

Valencia-Arias, A., Patiño-Toro, O., Arenas-Fernández, A., Garcés-Giraldo, L. F., Umba-López, A. M., y Benjumea-Arias, M. L. (2020). Research trends in the study of cyber defense: A bibliometric analysis [Tendencias investigativas en el estudio de la ciberdefensa: Un análisis bibliométrico]. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *2020*(E29), 366–379. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083520208&partnerID=40&md5=9a22a0b4cbfff01cd9021da69265d987

Vásquez, S. P. F., y Lira, L. A. N. (2021). Gestión por procesos en el marco de la Modernización de la Gestión Pública en el Perú. *Alpha Centauri*, *2*(3), 140–164. https://journalalphacentauri.com/index.php/revista/article/view/54

Villagra, M. E. (2024). La Imperiosa Necesidad de Modernizar las Fuerzas Armadas del Perú: Un Análisis Estratégico. *Pensamiento Conjunto*, *12*(2), 14. https://pensamientoconjunto.com.pe/index.php/PC/article/view/151

Villamil, X. A. C., Jara, M. L. B., Venegas, J. C. P., y Aguilar, J. A. Q. (2020). Cybersecurity and cyber defense in Colombia: A possible model for civil-military relations [Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares]. *Revista Científica General José María Córdova*, *18*(30), 357–377. https://doi.org/10.21830/19006586.588

Zambrano, H. M. R., y Tamayo, C. H. M. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas Revista Científica y Académica*, *4*(1), 159–178. https://doi.org/10.61384/r.c.a..v4i1.90

Zamorato, C. E. (2022). *Las operaciones en el Ciberespacio y sus limitaciones legales para el nivel operacional* [Trabajo de Investigación, Institución de Defensa de Argentina]. Repositorio Cefa Digital. https://cefadigital.edu.ar/handle/1847939/2926

Zúñiga, P. I. V., Cedeño, R. J. C., y Palacios, I. A. M. (2023). Metodología de la investigación científica: guía práctica. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(4), 9723–9762. https://doi.org/10.37811/cl_rcm.v7i4.7658

ANEXOS

1. Matriz de consistencia.
2. Matriz de Operacionalización.
3. Ficha técnica del Instrumento.
4. Validación de Instrumentos
5. Confiabilidad del Instrumento.
6. Instrumento de Recolección de Datos.
7. Autorización para la Recolección de Datos.
8. Consentimiento informado
9. Matriz de Objetivos, metas e Indicadores del Centro de Ciberdefensa del Ejército (CCE):
10. Plan de implementación de indicadores en el CCE 3 / 6 / 12.

.

Anexo 1. Matriz de Consistencia Título: Centro de Ciberdefensa del Ejército y su aporte a las operaciones de información en el Ejército del Perú- 2024.

Preguntas de Investigación	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores	Metodología
Problema general: ¿En qué medida el Centro de Ciberdefensa del Ejército (CCE) aporta a las Operaciones de Información en el Ejército del Perú durante el año 2024? **Problemas específicos:** ¿Qué factores que influyen en el nivel de actividad del CCE en las Operaciones de Información en el Ejército del Perú durante el año 2024? ¿En qué medida el nivel de capacitación y entrenamiento en ciberseguridad del CCE influyen en la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú en el año 2024? ¿Cómo contribuyen el desarrollo y la aplicación de estrategias de ciberseguridad en el CCE a la eficacia de las Operaciones de la información en el Ejército del Perú en el año 2024?	**Objetivo general:** Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024. **Objetivos específicos:** Analizar los factores que influyen en la actividad del CCE en las Operaciones de Información en el Ejército del Perú durante el año 2024. Determinar el nivel capacitación y entrenamiento en ciberseguridad del CCE y su influencia con la eficiencia en el aporte a las Operaciones de Información en el Ejército del Perú en el año 2024 Evaluar como el nivel de desarrollo y la aplicación de estrategias de ciberseguridad en el CCE contribuyen a la eficacia de las Operaciones de Información en el Ejército del Perú durante el año 2024 .	**Hipótesis general:** El Centro de Ciberdefensa del Ejército (CCE) aporta de manera significativa a las Operaciones de Información en el Ejército del Perú durante el año 2024. **Hipótesis específicas:** Los factores que influyen en el nivel de actividad del CCE no se relacionan de manera significativa con su participación en las Operaciones de Información en el Ejército del Perú durante el año 2024. El nivel de capacitación y entrenamiento del personal del CCE no influye de manera significativa en la eficiencia de su aporte a las Operaciones de Información en el Ejército del Perú durante el año 2024 El desarrollo y aplicación de estrategias de ciberseguridad en el CCE no se relacionan de manera significativa con la eficacia de las Operaciones de Información en el Ejército del Perú durante el año 2024.	**Variable 1:** El Centro de Ciberdefensa del Ejército (CCE). **Variable 2:** Operaciones de Información	Nivel de actividad. Capacitación y entrenamiento Desarrollo y aplicación de estrategias Nivel de eficiencia. Nivel de eficacia.	- Instalaciones del CCE. - Ubicación de hub - Equipamiento de hub - Capacidades técnicas del CCE. - Número de programas de capacitación ofrecidos. - Objetivos alcanzados por el CCE. - Frecuencia de actualización de estrategias de ciberseguridad. - Percepción positiva de la población. - Empleo adecuado de los recursos asignados. - Número de operaciones de información realizada. - Normas y disposiciones a nivel institucional	**Enfoque:** Cuantitativo **Tipo:** Investigación aplicada. **Alcance:** Correlacional. **Diseño:** No experimental, de corte transeccional correlacional **Población**: Personal de Oficiales, técnicos y Suboficiales **Muestra**: 57 **Técnica e Instrumento:** Encuesta**-**cuestionario **Forma de análisis de datos:** Descriptivo- Inferencial

Anexo 2. Matriz de Operacionalización de variables

VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA DE VALORES	NIVELES Y RANGO	TIPO DE VARIABLE ESTADÍSTICA
Centro de Ciberdefensa del Ejército	Nivel de actividad.	Instalaciones del CCE.	1	Muy en desacuerdo. (1) En desacuerdo. (2) Ni de acuerdo ni desacuerdo.(3) De acuerdo. (4) Totalmente de acuerdo. (5)	Alto [75 – 60> Medio <59 – 30> Bajo <29 – 15]	Ordinal.
		Ubicación de hub	2			
		Equipamiento de hub	3			
	Capacitación y entrenamiento	Capacidades técnicas del CCE	4,5, 6			
		Número de programas de capacitación ofrecidos	7,8,9			
	Desarrollo y aplicación de estrategias	Objetivos alcanzados por el CCE.	10, 11, 12			
		Frecuencia de actualización de estrategias de ciberseguridad	13, 14, 15			
Operaciones de Información	Nivel de eficiencia.	Percepción positiva de la población.	16,17, 18	Muy en desacuerdo. (1) En desacuerdo. (2) Ni de acuerdo ni desacuerdo.(3) De acuerdo. (4) Totalmente de acuerdo. (5)	Alto [75 – 60> Medio <59 – 30> Bajo <29 – 15]	Ordinal.
		Empleo adecuado de los recursos asignados	19, 20, 21			
	Nivel de eficacia.	Número de operaciones de información realizada	22, 23, 24			
		Normas y disposiciones a nivel institucional	25, 26, 27			

Anexo 3. Ficha Técnica del Instrumento

Denominación del instrumento	Cuestionario sobre el Aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú.
Autor original	Bach. Maribel Jenny Mendoza Barreto Bach. Marco Antonio Ruiz Mendoza
Autor de adaptación	Bach. Maribel Jenny Mendoza Barreto Bach. Marco Antonio Ruiz Mendoza
Año de elaboración	2024
Dimensiones	Nivel de actividad. Capacitación y entrenamiento en ciberseguridad en el CCE. Desarrollo y aplicación de estrategias de ciberseguridad en el CCE. Nivel de eficiencia. Nivel de eficacia.
Objetivo	Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024.
Administración	Autoadministrado mediante encuestas digitales dirigidas a personal del Ejército del Perú.
Duración aproximada	15 - 20 minutos
N° de ítems	27 preguntas distribuidas en cinco dimensiones, con escala tipo Likert.
Descripción	El cuestionario consta de preguntas estructuradas con escala de valoración de 1 a 5 (Muy en desacuerdo a Totalmente de acuerdo) para medir la actividad, capacitación y entrenamiento en ciberseguridad en el CCE, desarrollo y aplicación de estrategias de ciberseguridad en el CCE, nivel de eficiencia y nivel de eficacia.
Adaptación	Se ajustó la redacción de preguntas con base en normativa y doctrina actual de ciberdefensa aplicadas en el contexto del Ejército del Perú.
Validez	Validado por juicio de expertos en ciberseguridad y operaciones militares. Se utilizó el coeficiente V de Aiken con resultados superiores a 0.80.
Confiabilidad	Se empleó el coeficiente de Alfa de Cronbach, obteniendo un valor de 0.984, lo que indica alta consistencia interna.
Otros que considere	Instrumento diseñado bajo estándares de ética en investigación, asegurando el anonimato y confidencialidad de los encuestados.

Anexo 4. Validación de Instrumentos

JUICIO DE EXPERTOS

INFORMACIÓN DEL ESPECIALISTA

Apellidos y nombres del juez	Lizet Milagros CACHO DE LA CRUZ
Profesión	Militar
Especialidad	Ingeniero de comunicaciones
Grado académico	Magister en Ciencias Militares
Años de experiencia en temática	17 años
Institución donde labora	Escuela de Guerra del Ejército – Escuela de Post Grado.
Cargo que desempeña actualmente	Docente de maestria.

INFORMACIÓN DEL INVESTIGADOR

Titulo de la investigación	Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de información en el Ejército del Perú
Linea de investigación	Empleo de GUB,GUC, Operaciones GC y GNC.
Autor de investigación	BACH. RUIZ HURTADO Marco Antonio / BACH MENDOZA BARRETO Maribel Jenny
Nombre del instrumento	Cuestionario

Para efectos de la evaluacion de los items del instrumento:

CRITERIOS	INDICADORES
Claridad	Utiliza un lenguaje adecuado, lo que permite su comprensión con facilidad. Es decir, su sintaxis y semántica son adecuadas.
Coherencia	Tiene relación lógica con la dimensión y el indicador que se evalúa.
Importancia	Es esencial, significativo que sí contribuye a entender bien el objeto de estudio.
Pertinencia	Es relevante por su estrecha relación con el propósito establecido y pertenecen a una misma dimensión.

VALORACIÓN DEL INSTRUMENTO. Marcar con una "X" donde corresponda cada item:

N°	ÍTEMS	CLARIDAD		COHERENCIA		IMPORTANCIA		PERTINENCIA		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	SI	NO	
1	¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?	X		X		X		X		
2	¿Los Hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?	X		X		X		X		
3	¿El equipamiento de los Hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?	X		X		X		X		
4	¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?	X		X		X		X		
5	¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?	X		X		X		X		
6	¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?	X		X		X		X		
7	¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?	X		X		X		X		
8	¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?	X		X		X		X		

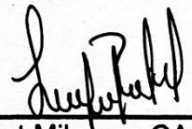
9	¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?	X		X		X		X		
10	¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?	X		X		X		X		
11	¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?	X		X		X		X		
12	¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?	X		X		X		X		
13	¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?	X		X		X		X		
14	¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?	X		X		X		X		
15	¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?	X		X		X		X		
16	¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?	X		X		X		X		
17	¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?	X		X		X		X		

18	¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?	X		X		X		X		
19	¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?	X		X		X		X		
20	¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?	X		X		X		X		
21	¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?	X		X		X		X		
22	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
23	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
24	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		
25	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
26	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
27	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		

CRITERIOS	INDICADORES	MUY INADECUADO (CUMPLE UN 25 %)	INADECUADO (CUMPLE UN 50%)	ADECUADO (CUMPLE UN 75%)	MUY ADECUADO (CUMPLE UN 100%)	OBSERVACIONES
ACTITUDINAL	Es adecuado a la descripción y alcance de la variable de la investigación.				X	
CONSISTENCIA	Está basados en aspectos teóricos-científicos del conocimiento				X	
INTENCIONALIDAD	Es adecuado para valorar aspectos de la variable de investigación				X	
METODOLOGÍA	Responde al propósito del diagnóstico.				X	
OBJETIVIDAD	Está expresado en conductas observables.				X	
ORGANIZACIÓN	Existe una organización lógica en el instrumento.				X	
SUFICIENCIA	Los ítems comprenden los aspectos en cantidad y calidad adecuada con respecto a la variable de investigación.				X	

NOTA. Luego de establecer la validez, aplicar promedio o Valor Aiken para determinar la validez del instrumento, luego administrar una prueba piloto con elementos muestrales similares a su muestra y obtener el valor Alfa de Cronbach.
El Juez, Mag. Lizet Milagros CACHO DE LA CRUZ, que suscribe recomienda que el instrumentos es:

- ➢ Válido __x__,
- ➢ Válido, luego de corregir las observaciones indicadas_____,
- ➢ No es válido____ para su administración.



Mag. Lizet Milagros CACHO DE LA CRUZ
CÓDIGO ORCID 0000-0002-5311-7670

JUICIO DE EXPERTOS

INFORMACIÓN DEL ESPECIALISTA

Apellidos y nombres del juez	Victor Mahatma FLORES MOZOMBITE
Profesión	Militar
Especialidad	Ingeniero de Telecomunicaciones
Grado académico	Magister en Ciencias Militares
Años de experiencia en temática	20 años
Institución donde labora	Batallon de Comunicaciones N° 111
Cargo que desempeña actualmente	Comandante de Batallón

INFORMACIÓN DEL INVESTIGADOR

Titulo de la investigación	Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de información en el Ejército del Perú.
Linea de investigación	Empleo de GUB,GUC, Operaciones GC y GNC.
Autor de investigación	BACH. RUIZ HURTADO Marco Antonio / BACH MENDOZA BARRETO Maribel Jenny
Nombre del instrumento	Cuestionario

Para efectos de la evaluacion de los items del instrumento:

CRITERIOS	INDICADORES
Claridad	Utiliza un lenguaje adecuado, lo que permite su comprensión con facilidad. Es decir, su sintaxis y semántica son adecuadas.
Coherencia	Tiene relación lógica con la dimensión y el indicador que se evalúa.
Importancia	Es esencial, significativo que sí contribuye a entender bien el objeto de estudio.
Pertinencia	Es relevante por su estrecha relación con el propósito establecido y pertenecen a una misma dimensión.

VALORACIÓN DEL INSTRUMENTO. Marcar con una "X" donde corresponda cada ítem:

N°	ÍTEMS	CLARIDAD		COHERENCIA		IMPORTANCIA		PERTINENCIA		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	SI	NO	
1	¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?	X		X		X		X		
2	¿Los Hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?	X		X		X		X		
3	¿El equipamiento de los Hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?	X		X		X		X		
4	¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?	X		X		X		X		
5	¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?	X		X		X		X		
6	¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?	X		X		X		X		
7	¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?	X		X		X		X		
8	¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?	X		X		X		X		

9	¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?	X		X		X		X		
10	¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?	X		X		X		X		
11	¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?	X		X		X		X		
12	¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?	X		X		X		X		
13	¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?	X		X		X		X		
14	¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?	X		X		X		X		
15	¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?	X		X		X		X		
16	¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?	X		X		X		X		
17	¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?	X		X		X		X		

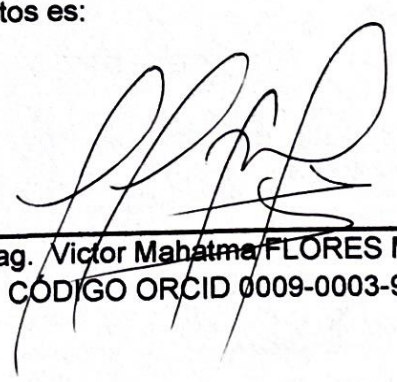
18	¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?	X		X		X		X		
19	¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?	X		X		X		X		
20	¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?	X		X		X		X		
21	¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?	X		X		X		X		
22	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
23	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
24	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		
25	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
26	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
27	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		

CRITERIOS	INDICADORES	MUY INADECUADO (CUMPLE UN 25 %)	INADECUADO (CUMPLE UN 50%)	ADECUADO (CUMPLE UN 75%)	MUY ADECUADO (CUMPLE UN 100%)	OBSERVACIONES
ACTITUDINAL	Es adecuado a la descripción y alcance de la variable de la investigación.				X	
CONSISTENCIA	Está basados en aspectos teóricos-científicos del conocimiento				X	
INTENCIONALIDAD	Es adecuado para valorar aspectos de la variable de investigación				X	
METODOLOGÍA	Responde al propósito del diagnóstico.				X	
OBJETIVIDAD	Está expresado en conductas observables.				X	
ORGANIZACIÓN	Existe una organización lógica en el instrumento.				X	
SUFICIENCIA	Los ítems comprenden los aspectos en cantidad y calidad adecuada con respecto a la variable de investigación.				X	

NOTA. Luego de establecer la validez, aplicar promedio o Valor Aiken para determinar la validez del instrumento, luego administrar una prueba piloto con elementos muestrales similares a su muestra y obtener el valor Alfa de Cronbach.

El Juez, Mag. Victor Mahatma FLORES MOZOMBITE, que suscribe recomienda que el instrumentos es:

- ➢ Válido __X__,
- ➢ Válido, luego de corregir las observaciones indicadas_____,
- ➢ No es válido____ para su administración.



Mag. Victor Mahatma FLORES MOZOMBITE
CÓDIGO ORCID 0009-0003-9966-0403

JUICIO DE EXPERTOS

INFORMACIÓN DEL ESPECIALISTA

Apellidos y nombres del juez	Félix Junior ESPINOZA LUPUCHE
Profesión	Militar
Especialidad	Ingeniero de comunicaciones
Grado académico	Magister en Ciencias Militares
Años de experiencia en temática	17 años
Institución donde labora	Escuela de Comunicaciones del Ejército del Perú
Cargo que desempeña actualmente	Docente de Diplomados en Comunicaciones

INFORMACIÓN DEL INVESTIGADOR

Titulo de la investigación	Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de información en el Ejército del Perú
Linea de investigación	Empleo de GUB,GUC, Operaciones GC y GNC.
Autor de investigación	BACH. RUIZ HURTADO Marco Antonio / BACH MENDOZA BARRETO Maribel Jenny
Nombre del instrumento	Cuestionario

Para efectos de la evaluacion de los items del instrumento:

CRITERIOS	INDICADORES
Claridad	Utiliza un lenguaje adecuado, lo que permite su comprensión con facilidad. Es decir, su sintaxis y semántica son adecuadas.
Coherencia	Tiene relación lógica con la dimensión y el indicador que se evalúa.
Importancia	Es esencial, significativo que sí contribuye a entender bien el objeto de estudio.
Pertinencia	Es relevante por su estrecha relación con el propósito establecido y pertenecen a una misma dimensión.

VALORACIÓN DEL INSTRUMENTO. Marcar con una "X" donde corresponda cada ítem:

N°	ÍTEMS	CLARIDAD		COHERENCIA		IMPORTANCIA		PERTINENCIA		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	SI	NO	
1	¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?	X		X		X		X		
2	¿Los Hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?	X		X		X		X		
3	¿El equipamiento de los Hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?	X		X		X		X		
4	¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?	X		X		X		X		
5	¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?	X		X		X		X		
6	¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?	X		X		X		X		
7	¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?	X		X		X		X		
8	¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?	X		X		X		X		

9	¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?	X		X		X		X		
10	¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?	X		X		X		X		
11	¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?	X		X		X		X		
12	¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?	X		X		X		X		
13	¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?	X		X		X		X		
14	¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?	X		X		X		X		
15	¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?	X		X		X		X		
16	¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?	X		X		X		X		
17	¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?	X		X		X		X		

18	¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?	X		X		X		X		
19	¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?	X		X		X		X		
20	¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?	X		X		X		X		
21	¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?	X		X		X		X		
22	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
23	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
24	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		
25	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
26	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
27	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		

CRITERIOS	INDICADORES	MUY INADECUADO (CUMPLE UN 25 %)	INADECUADO (CUMPLE UN 50%)	ADECUADO (CUMPLE UN 75%)	MUY ADECUADO (CUMPLE UN 100%)	OBSERVACIONES
ACTITUDINAL	Es adecuado a la descripción y alcance de la variable de la investigación.				X	
CONSISTENCIA	Está basados en aspectos teóricos-científicos del conocimiento				X	
INTENCIONALIDAD	Es adecuado para valorar aspectos de la variable de investigación				X	
METODOLOGÍA	Responde al propósito del diagnóstico.				X	
OBJETIVIDAD	Está expresado en conductas observables.				X	
ORGANIZACIÓN	Existe una organización lógica en el instrumento.				X	
SUFICIENCIA	Los ítems comprenden los aspectos en cantidad y calidad adecuada con respecto a la variable de investigación.				X	

NOTA. Luego de establecer la validez, aplicar promedio o Valor Aiken para determinar la validez del instrumento, luego administrar una prueba piloto con elementos muestrales similares a su muestra y obtener el valor Alfa de Cronbach.

El Juez, Mag. Félix Junior ESPINOZA LUPUCHE, que suscribe recomienda que el instrumentos es:

- Válido __X__,
- Válido, luego de corregir las observaciones indicadas_____,
- No es válido____ para su administración.

Mag. Félix Junior ESPINOZA LUPUCHE
CÓDIGO ORCID 000-0003-1426-634

JUICIO DE EXPERTOS

INFORMACIÓN DEL ESPECIALISTA

Apellidos y nombres del juez	Daniel Gerardo VIZARRETA PACHECO
Profesión	Militar
Especialidad	Ingeniero de Telecomunicaciones
Grado académico	Magister en Gestión Pública
Años de experiencia en temática	20 años
Institución donde labora	Fuerzas Especiales Conjuntas
Cargo que desempeña actualmente	Oficial del Estado Mayor

INFORMACIÓN DEL INVESTIGADOR

Titulo de la investigación	Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de información en el Ejército del Perú.
Linea de investigación	Empleo de GUB,GUC, Operaciones GC y GNC.
Autor de investigación	BACH. RUIZ HURTADO Marco Antonio / BACH MENDOZA BARRETO Maribel Jenny
Nombre del instrumento	Cuestionario

Para efectos de la evaluacion de los items del instrumento:

CRITERIOS	INDICADORES
Claridad	Utiliza un lenguaje adecuado, lo que permite su comprensión con facilidad. Es decir, su sintaxis y semántica son adecuadas.
Coherencia	Tiene relación lógica con la dimensión y el indicador que se evalúa.
Importancia	Es esencial, significativo que sí contribuye a entender bien el objeto de estudio.
Pertinencia	Es relevante por su estrecha relación con el propósito establecido y pertenecen a una misma dimensión.

VALORACIÓN DEL INSTRUMENTO. Marcar con una "X" donde corresponda cada ítem:

N°	ÍTEMS	CLARIDAD		COHERENCIA		IMPORTANCIA		PERTINENCIA		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	SI	NO	
1	¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?	X		X		X		X		
2	¿Los Hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?	X		X		X		X		
3	¿El equipamiento de los Hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?	X		X		X		X		
4	¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?	X		X		X		X		
5	¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?	X		X		X		X		
6	¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?	X		X		X		X		
7	¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?	X		X		X		X		
8	¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?	X		X		X		X		

9	¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?	X		X		X		X		
10	¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?	X		X		X		X		
11	¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?	X		X		X		X		
12	¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?	X		X		X		X		
13	¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?	X		X		X		X		
14	¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?	X		X		X		X		
15	¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?	X		X		X		X		
16	¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?	X		X		X		X		
17	¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?	X		X		X		X		

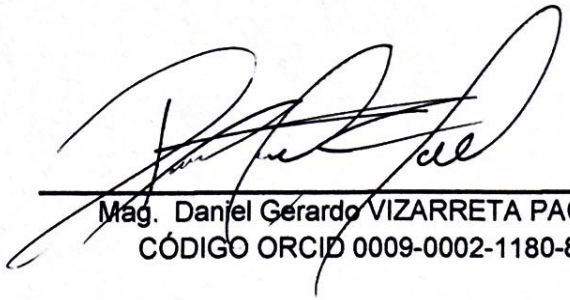
18	¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?	X		X		X		X		
19	¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?	X		X		X		X		
20	¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?	X		X		X		X		
21	¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?	X		X		X		X		
22	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
23	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
24	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		
25	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
26	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
27	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		

CRITERIOS	INDICADORES	MUY INADECUADO (CUMPLE UN 25 %)	INADECUADO (CUMPLE UN 50%)	ADECUADO (CUMPLE UN 75%)	MUY ADECUADO (CUMPLE UN 100%)	OBSERVACIONES
ACTITUDINAL	Es adecuado a la descripción y alcance de la variable de la investigación.				X	
CONSISTENCIA	Está basados en aspectos teóricos-científicos del conocimiento				X	
INTENCIONALIDAD	Es adecuado para valorar aspectos de la variable de investigación				X	
METODOLOGÍA	Responde al propósito del diagnóstico.				X	
OBJETIVIDAD	Está expresado en conductas observables.				X	
ORGANIZACIÓN	Existe una organización lógica en el instrumento.				X	
SUFICIENCIA	Los ítems comprenden los aspectos en cantidad y calidad adecuada con respecto a la variable de investigación.				X	

NOTA. Luego de establecer la validez, aplicar promedio o Valor Aiken para determinar la validez del instrumento, luego administrar una prueba piloto con elementos muestrales similares a su muestra y obtener el valor Alfa de Cronbach.

El Juez, Mag. Daniel Gerardo VIZARRETA PACHECO, que suscribe recomienda que el instrumentos es:

- ➢ Válido __X__,
- ➢ Válido, luego de corregir las observaciones indicadas_____,
- ➢ No es válido____ para su administración.



Mag. Daniel Gerardo VIZARRETA PACHECO
CÓDIGO ORCID 0009-0002-1180-8614

JUICIO DE EXPERTOS

INFORMACIÓN DEL ESPECIALISTA

Apellidos y nombres del juez	Jorge Luis ESPINOZA VELA
Profesión	Militar
Especialidad	Ingeniero de comunicaciones
Grado académico	Magister en Ciencias Militares
Años de experiencia en temática	29 años
Institución donde labora	CENTRO DE CIBERDEFENSA DEL EJÉRCITO (CCE)
Cargo que desempeña actualmente	JEFE

INFORMACIÓN DEL INVESTIGADOR

Titulo de la investigación	Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de información en el Ejército del Perú
Linea de investigación	Empleo de GUB,GUC, Operaciones GC y GNC.
Autor de investigación	BACH. RUIZ HURTADO Marco Antonio / BACH MENDOZA BARRETO Maribel Jenny
Nombre del instrumento	Cuestionario

Para efectos de la evaluacion de los items del instrumento:

CRITERIOS	INDICADORES
Claridad	Utiliza un lenguaje adecuado, lo que permite su comprensión con facilidad. Es decir, su sintaxis y semántica son adecuadas.
Coherencia	Tiene relación lógica con la dimensión y el indicador que se evalúa.
Importancia	Es esencial, significativo que sí contribuye a entender bien el objeto de estudio.
Pertinencia	Es relevante por su estrecha relación con el propósito establecido y pertenecen a una misma dimensión.

VALORACION DEL INSTRUMENTO. Marcar con una "X" donde corresponda cada item:

N°	ITEMS	CLARIDAD		COHERENCIA		IMPORTANCIA		PERTINENCIA		OBSERVACIONES
		SI	NO	SI	NO	SI	NO	SI	NO	
1	¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?	X		X		X		X		
2	¿Los Hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?	X		X		X		X		
3	¿El equipamiento de los Hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?	X		X		X		X		
4	¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?	X		X		X		X		
5	¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?	X		X		X		X		
6	¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?	X		X		X		X		
7	¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?	X		X		X		X		
8	¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?	X		X		X		X		

9	¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?	X		X		X		X		
10	¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?	X		X		X		X		
11	¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?	X		X		X		X		
12	¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?	X		X		X		X		
13	¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?	X		X		X		X		
14	¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?	X		X		X		X		
15	¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?	X		X		X		X		
16	¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?	X		X		X		X		
17	¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?	X		X		X		X		

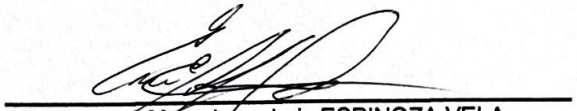
18	¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?	X		X		X		X		
19	¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?	X		X		X		X		
20	¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?	X		X		X		X		
21	¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?	X		X		X		X		
22	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
23	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
24	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		
25	¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?	X		X		X		X		
26	¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?	X		X		X		X		
27	¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?	X		X		X		X		

CRITERIOS	INDICADORES	MUY INADECUADO (CUMPLE UN 25 %)	INADECUADO (CUMPLE UN 50%)	ADECUADO (CUMPLE UN 75%)	MUY ADECUADO (CUMPLE UN 100%)	OBSERVACIONES
ACTITUDINAL	Es adecuado a la descripción y alcance de la variable de la investigación.				X	
CONSISTENCIA	Está basados en aspectos teóricos-científicos del conocimiento				X	
INTENCIONALIDAD	Es adecuado para valorar aspectos de la variable de investigación				X	
METODOLOGÍA	Responde al propósito del diagnóstico.				X	
OBJETIVIDAD	Está expresado en conductas observables.				X	
ORGANIZACIÓN	Existe una organización lógica en el instrumento.				X	
SUFICIENCIA	Los ítems comprenden los aspectos en cantidad y calidad adecuada con respecto a la variable de investigación.				X	

NOTA. Luego de establecer la validez, aplicar promedio o Valor Aiken para determinar la validez del instrumento, luego administrar una prueba piloto con elementos muestrales similares a su muestra y obtener el valor Alfa de Cronbach.

El Juez, Mag. Jorge Luis ESPINOZA VELA, que suscribe recomienda que el instrumentos es:

- Válido __X__,
- Válido, luego de corregir las observaciones indicadas_____,
- No es válido____ para su administración.



Mag. Jorge Luis ESPINOZA VELA
CÓDIGO ORCID 0009-0000-7037 -3118

PERÚ | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Registro y Reconocimiento de Grados y Títulos e Información Universitaria

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
FLORES MOZOMBITE, VICTOR MAHATMA **DNI 43371708**	BACHILLER EN CIENCIAS MILITARES CON MENCION EN INGENIERIA **Fecha de diploma: 10/03/20** Modalidad de estudios: PRESENCIAL Fecha matrícula: 01/04/2000 Fecha egreso: 01/01/2004	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
FLORES MOZOMBITE, VICTOR MAHATMA **DNI 43371708**	MAESTRO EN CIENCIAS MILITARES CON MENCIÓN EN PLANEAMIENTO ESTRATÉGICO Y TOMA DE DECISIONES **Fecha de diploma: 21/03/22** Modalidad de estudios: PRESENCIAL Fecha matrícula: 13/01/2019 Fecha egreso: 17/12/2020	ESCUELA SUPERIOR DE GUERRA DEL EJERCITO ***PERU***

PERÚ | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Registro y Reconocimiento de Grados y Títulos e Información Universitaria

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**LICENCIADO EN CIENCIAS MILITARES MENCION INGENIERIA ESPECIALIDAD COMUNICACIONES MENCION INGENIERIA ESPECIALIDAD COMUNICACIONES** **Fecha de diploma: 08/11/2008** Modalidad de estudios: -	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**BACHILLER EN INGENIERIA DE TELECOMUNICACIONES** **Fecha de diploma: 29/04/2011** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**INGENIERO DE TELECOMUNICACIONES** **Fecha de diploma: 16/07/2014** Modalidad de estudios: -	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**MAESTRO EN GESTIÓN Y EVALUACIÓN DE PROYECTOS DE INVERSIÓN** **Fecha de diploma: 30/12/16** Modalidad de estudios: PRESENCIAL Fecha matrícula: 14/01/2016 Fecha egreso: 09/12/2016	INSTITUTO CIENTÍFICO Y TECNOLÓGICO DEL EJÉRCITO ***PERU***
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**BACHILLER EN CIENCIAS MILITARES** **Fecha de diploma: 19/12/07** Modalidad de estudios: PRESENCIAL *TIPO:* • ***DUPLICADO*** Fecha matrícula: 01/04/2003 Fecha egreso: 14/12/2007	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
CACHO DE LA CRUZ, LIZET MILAGROS **DNI 43342014**	**MAESTRO EN CIENCIAS MILITARES CON MENCIÓN EN PLANEAMIENTO ESTRATÉGICO Y TOMA DE DECISIONES** **Fecha de diploma: 15/02/23** Modalidad de estudios: PRESENCIAL Fecha matrícula: 25/01/2021 Fecha egreso: 12/12/2022	ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO ***PERU***

PERÚ | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Registro y Reconocimiento de Grados y Títulos e Información Universitaria

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
ESPINOZA LUPUCHE, FELIX JUNIOR **DNI 42553498**	**BACHILLER EN CIENCIAS MILITARES** **Fecha de diploma: 19/12/07** Modalidad de estudios: PRESENCIAL Fecha matrícula: 01/04/2003 Fecha egreso: 10/12/2007	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
ESPINOZA LUPUCHE, FELIX JUNIOR **DNI 42553498**	**LICENCIADO EN CIENCIAS MILITARES CON MENCIÓN EN INGENIERÍA** **Fecha de diploma: 30/07/24** Modalidad de estudios: PRESENCIAL	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
ESPINOZA LUPUCHE, FELIX JUNIOR **DNI 42553498**	**MAESTRO EN CIENCIAS MILITARES CON MENCIÓN EN PLANEAMIENTO ESTRATÉGICO Y TOMA DE DECISIONES** **Fecha de diploma: 23/05/2025** Modalidad de estudios: PRESENCIAL Fecha matrícula: 17/01/2022 Fecha egreso: 13/12/2023	ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO ***PERU***

PERÚ | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Registro y Reconocimiento de Grados y Títulos e Información Universitaria

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
VIZARRETA PACHECO, DANIEL GERARDO **DNI 43309836**	**INGENIERO DE TELECOMUNICACIONES** **Fecha de diploma: 24/04/2012** Modalidad de estudios: -	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
VIZARRETA PACHECO, DANIEL GERARDO **DNI 43309836**	**BACHILLER EN INGENIERIA DE TELECOMUNICACIONES** **Fecha de diploma: 29/08/2007** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
VIZARRETA PACHECO, DANIEL GERARDO **DNI 43309836**	**MAESTRO EN ADMINISTRACIÓN MENCION: GESTION PUBLICA** **MENCION: GESTION PUBLICA** **Fecha de diploma: 09/11/16** Modalidad de estudios: PRESENCIAL Fecha matrícula: 17/08/2012 Fecha egreso: 19/10/2015	UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE ***PERU***

PERÚ | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Registro y Reconocimiento de Grados y Títulos e Información Universitaria

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
ESPINOZA VELA, JORGE LUIS **DNI 43388750**	**BACHILLER EN CIENCIAS MILITARES INGENIERIA INGENIERIA** **Fecha de diploma: 31/05/07** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ***PERU***
ESPINOZA VELA, JORGE LUIS **DNI 43388750**	**MAESTRO EN CIENCIAS MILITARES PLANEAMIENTO ESTRATÉGICO Y TOMA DE DECISIONES PLANEAMIENTO ESTRATÉGICO Y TOMA DE DECISIONES** **Fecha de diploma: 02/10/15** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO ***PERU***
ESPINOZA VELA, JORGE LUIS **DNI 43388750**	**DOCTOR EN CIENCIAS DE LA EDUCACIÓN** **Fecha de diploma: 18/10/22** Modalidad de estudios: PRESENCIAL Fecha matrícula: 18/03/2018 Fecha egreso: 05/02/2021	UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE ***PERU***
ESPINOZA VELA, JORGE LUIS **DNI 43388750**	**MAGISTER EN CIENCIAS DE LA EDUCACION CON MENCION EN DOCENCIA UNIVERSITARIA** **Fecha de diploma: 25/07/11** Modalidad de estudios: PRESENCIAL Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE ***PERU***

Anexo 5: Confiabilidad de Recolección de Datos

Resumen de procesamientos de pasos.

		N	%
Casos	Válido	57	100,0
	Excluido[a]	0	,0
	Total	57	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad.

Alfa de Cronbach	N de elementos
0,974	27

Anexo 6: Instrumento de Recolección de Datos.

Estimado(a) participante,

Como parte de un estudio académico, estamos desarrollando una tesis titulada: Centro de Ciberdefensa del Ejército y su aporte a las Operaciones de Información en el Ejército del Perú – 2024.

Su colaboración es fundamental para obtener un diagnóstico preciso y formular recomendaciones que contribuyan a la mejora de las acciones del centro de ciberdefensa del Ejército (CCE).

Sus respuestas serán completamente anónimas y confidenciales. Los datos recopilados serán utilizados exclusivamente con fines académicos. Agradecemos su tiempo y disposición para responder este cuestionario.

Instrucciones

Responda utilizando un bolígrafo de tinta negra (si el cuestionario es impreso).
Cada pregunta tiene cinco opciones de respuesta; seleccione solo una.
Marque con una x la opción que mejor refleje su opinión.
No seleccione más de una opción por pregunta.
Si tiene dudas, consulte con el investigador responsable.

ESCALA DE LIKERT

Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni desacuerdo	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

CUESTIONARIO

ENUNCIADOS	1	2	3	4	5
DIMENSIÓN: NIVEL DE ACTIVIDAD					
1. ¿Considera que la cantidad de instalaciones del CCE es suficiente para garantizar la cobertura en el territorio nacional?					
2. ¿Los hubs del CCE están ubicados estratégicamente para maximizar su operatividad en la ciberdefensa?					

3. ¿El equipamiento de los hubs del CCE es adecuado para responder a las amenazas cibernéticas actuales?					
DIMENSIÓN: CAPACITACIÓN Y ENTRENAMIENTO EN CIBERSEGURIDAD					
INCREMENTO EN LAS CAPACIDADES TÉCNICAS DEL CCE					
4. ¿Ha percibido mejoras en las capacidades técnicas del personal del CCE en los últimos tres años?					
5. ¿Considera que el personal del CCE está adecuadamente capacitado para enfrentar nuevas amenazas cibernéticas?					
6. ¿El CCE ofrece formación especializada para cada nivel jerárquico del personal militar?					
CANTIDAD DE PROGRAMAS DE CAPACITACIÓN OFRECIDOS					
7. ¿Considera que el número de programas de capacitación del CCE es suficiente para fortalecer la preparación del personal?					
8. ¿El CCE diversifica sus programas de capacitación en diferentes áreas de ciberseguridad?					
9. ¿Se ha incrementado la cantidad de cursos de capacitación en ciberseguridad en los últimos años?					
Dimensión: desarrollo y aplicación de estrategias de ciberseguridad					
OBJETIVOS ALCANZADOS POR EL CCE					
10. ¿Las estrategias implementadas por el CCE han permitido alcanzar los objetivos de ciberseguridad establecidos?					
11. ¿Se han logrado los objetivos estratégicos de ciberseguridad planteados en los últimos tres años?					
12. ¿Los resultados obtenidos por el CCE han mejorado la capacidad de defensa ante amenazas cibernéticas?					
FRECUENCIA DE ACTUALIZACIÓN DE ESTRATEGIAS DE CIBERSEGURIDAD					
13. ¿Las estrategias de ciberseguridad del CCE son revisadas y actualizadas con la frecuencia necesaria?					
14. ¿Las estrategias del CCE se actualizan de manera proactiva en función del análisis de riesgos y nuevas amenazas?					

15. ¿Existen mecanismos establecidos para evaluar y mejorar continuamente las estrategias de ciberseguridad del CCE?					
DIMENSIÓN: NIVEL DE EFICIENCIA					
PERCEPCIÓN POSITIVA DE LA POBLACIÓN					
16. ¿La comunidad militar percibe al CCE como una entidad eficaz en ciberdefensa?					
17. ¿La labor del CCE ha contribuido a mejorar la confianza en la seguridad digital del Ejército?					
18. ¿Las estrategias implementadas por el CCE han aumentado la percepción de seguridad en el personal militar?					
EMPLEO ADECUADO DE LOS RECURSOS ASIGNADOS					
19. ¿El CCE optimiza los recursos asignados para maximizar su efectividad en ciberseguridad?					
20. ¿Los recursos asignados al CCE son utilizados eficientemente en la ejecución de sus estrategias de ciberseguridad?					
21. ¿Existe un proceso de evaluación para mejorar continuamente la asignación de recursos en el CCE?					
DIMENSIÓN: NIVEL DE EFICACIA					
CANTIDAD DE OPERACIONES DE INFORMACIÓN REALIZADAS					
22. ¿Las operaciones de información del CCE han logrado los objetivos estratégicos definidos?					
23. ¿Las operaciones del CCE han tenido un impacto positivo en la seguridad digital del Ejército?					
24. ¿El CCE ha implementado mejoras operativas basadas en la evaluación de sus operaciones anteriores?					
CANTIDAD DE NORMAS Y DISPOSICIONES A NIVEL INSTITUCIONAL PROMULGADAS					
25. ¿Las acciones del CCE han generado cambios positivos en la normativa de ciberseguridad del Ejército?					

26. ¿El CCE ha participado en la elaboración de nuevas normativas para fortalecer la ciberseguridad?					
27. ¿Se han implementado mecanismos de control para garantizar el cumplimiento de las normativas generadas por el CCE?					

¡Gracias por su colaboración! ¡Sus respuestas contribuirán al desarrollo y fortalecimiento de la ciberdefensa en el Ejército del Perú!

Anexo 7: Autorización para la recolección de Datos.

PERÚ | Ministerio de Defensa | Ejército del Perú | COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 02 de Abril del 2025

Oficio N° 1034 - 2025/U-26.e/DGI/ESGE-EPG

Señor : GRAL BRIG COMANDANTE GENERAL DEL CITELE – **SAN BORJA.**

Asunto : Solicita brindar las facilidades para el levantamiento de datos e informaciones al personal que se indica.

Ref. : a. Reglamento para la obtención de grado académico de Maestro en Ciencia Militares AF - 2023.
b. Guía Metodológica para la elaboración de proyecto e informe final de tesis de grado 2024-2026.

Tengo el agrado de dirigirme a Ud., en relación a los documentos de la referencia a. y b., a fin de solicitar se digne brindar las facilidades necesarias para el levantamiento de datos e informaciones a los siguientes alumnos de la XIII Maestría en Ciencias Militares de esta casa de estudios: **MY COM MENDOZA BARRETO Maribel Jenny** y el **MY COM RUIZ HURTADO Marco Antonio**, quienes están realizando la investigación titulada: **"Centro de Ciberdefensa del Ejército y su aporte a las Operaciones de Información en el Ejército del Perú – 2024"**.

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

Dios guarde a Ud.

Carlos Garcia Rodrigues
503 EP
337028300
CECIBER
16-04-2025

O - 224724171 - A +
JUAN KENNETH VALVERDE VIRHUEZ
General Brigada
Director de la Escuela Superior de Guerra del Ejército
Escuela de Post - Grado

DISTRIBUCIÓN
CITELE.....01
ARCHIVO.....01/02

SERVICIO DE COMUNICACIONES DEL EJÉRCITO
OFICINA DE TRAMITE DOCUMENTARIO
RECEPCIÓN
FECHA 16 Abril 2025
HORA 1600 hrs.
FIRMA
C. Barrera E.
My Com.

Y. Espinoza C.
S017/COM
DEPER - COCIBER.
16.04.25. 16.11 hr.

Anexo 8. Consentimiento Informado

CONSENTIMIENTO INFORMADO

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO- ESCUELA DE POSGRADO

Investigadores:

BACH. Maribel Jenny MENDOZA BARRETO DE RUIZ

BACH. Marco Antonio RUIZ HURTADO

Título de Tesis:

Centro de Ciberdefensa del Ejército y su Aporte a las Operaciones de Información en el Ejército del Perú - 2024

Propósito del estudio:

Examinar el aporte del Centro de Ciberdefensa del Ejército (CCE) a las Operaciones de Información en el Ejército del Perú durante el año 2024

Procedimiento:

Si usted decide participar en este estudio, se realizará lo siguiente:

La encuesta puede demorar unos 45 minutos. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.

Riesgos:

La investigación no presentará riesgo alguno para su integridad física ni emocional.

Beneficios:

Considerar la relevancia social y/o institucional de la investigación.

Costos e incentivos:

Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.

Confidencialidad:

Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.

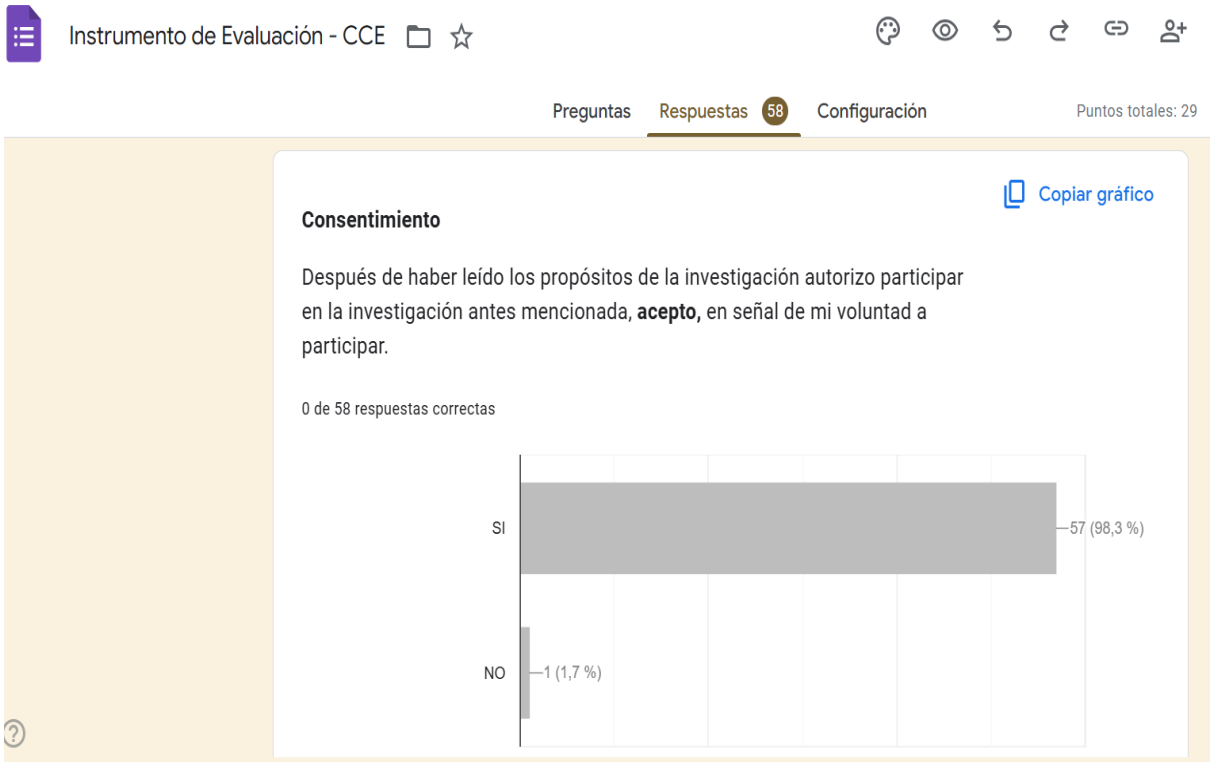
Si tiene alguna duda y necesita más información puede comunicarse con el Bach. Maribel Jenny Mendoza Barreto de Ruiz al teléfono: 947203539 o con el asesor: Dra. Yessenia SOLIER CASTRO, al teléfono: 990953005.

CONSENTIMIENTO:

Acepto voluntariamente participar en este estudio. Recibiré una copia de las respuestas a mi correo electrónico.

Figura 13

Estadística del personal que fue consultado sobre Consentimiento de Informado.



Nota. En la figura se muestra la población que indicó ser informada.

Anexo 9. Matriz de Objetivos, metas e Indicadores del Centro de Ciberdefensa del Ejército (CCE):

Elemento: Objetivo /Acción / Servicio	Indicador	Nombre del Indicador	Método de cálculo del indicador	Verificación de Características Deseables				
				Específico	Relevante	Medible	Realizable	Temporal
Objetivo 1 Meta 1.1 Capacitar al personal de Oficiales del CCE, en el empleo técnico y táctico de la ciberdefensa	IM 1.1.1	Porcentaje de Oficiales capacitados en ataque, respuesta y explotación cibernética.	**[**Número de Oficiales capacitados en ataque, respuesta y explotación cibernética **/** Total de Oficiales del CCE que no posee las competencias**]*** 100	Mejorar el nivel de capacitación en ciberdefensa del personal de Oficiales del CCE.	Mejora las competencias del personal y permite desarrollar Ciberdefensa por parte del CCE.	Medir la cantidad de personal de Oficiales del CCE capacitados en ataque, respuesta, explotación y análisis forense.	Alcanzar el 85 % de Oficiales Capacitados en ataque, respuesta y explotación.	Medición Semestral y Anual.
	IM 1.1.2	Porcentaje de Oficiales capacitados en análisis forense de redes informáticas.	**[**Número de Oficiales capacitados en análisis forense en redes informáticas **/** Total de Oficiales del CCE que no posee las competencias**]*100**				Alcanzar el 30% de Oficiales capacitados en análisis forense de redes.	
	IM 1.1.3	Porcentaje de Oficiales del CCE que alcanzan Nivel óptimo de capacitación en ciberdefensa.	**[**Número de Oficiales que alcanzaron nivel alto e intermedio en ciberdefensa / Total de Oficiales capacitados del CCE**] *100**			Medir los resultados de los cursos impartidos al personal de Oficiales en ataque, respuesta, explotación y análisis forense.	Alcanzar un 80% de nivel alto y medio del personal de oficiales capacitados.	
Objetivo 1 Meta 1.2 Capacitar al personal de Técnicos y Suboficiales del CCE, en el empleo técnico y táctico de la ciberdefensa .	IM 1.2.1	Porcentaje de Técnicos y Suboficiales capacitados en ataque, respuesta y explotación cibernética.	**[**Número de Tcos y SSOO capacitados en ataque, respuesta y explotación cibernética **/** Total de Oficiales del CCE que no posee las competencias**]*** 100	Mejorar el nivel de capacitación en ciberdefensa del personal de Técnicos y Suboficiales del CCE.	Mejora las competencias del personal y permite desarrollar Ciberdefensa por parte del CCE.	Medir la cantidad de personal de Técnicos y Suboficiales del CCE capacitados en ataque, respuesta, explotación y análisis forense.	Alcanzar el 70 % de Técnicos y Suboficiales Capacitados en ataque, respuesta y explotación.	Medición Semestral y Anual.
	IM 1.2.2	Porcentaje de Técnicos y Suboficiales capacitados en análisis forense de redes informáticas.	**[**Número de Tcos y SSOO capacitados en análisis forense en redes informáticas **/** Total de Oficiales del CCE que no posee las competencias**]*** 100				Alcanzar el 50% de Técnicos y Suboficiales capacitados en análisis forense de redes.	
	IM 1.2.3	Porcentaje de Técnicos y Suboficiales del CCE que alcanzan Nivel óptimo de capacitación en ciberdefensa.	**[**Número de Tcos y SSOO que alcanzaron nivel alto e intermedio en ciberdefensa **/** Total de Oficiales capacitados del CCE**] *** 100			Medir los resultados de los cursos impartidos al personal de Técnicos y Suboficiales en ataque, respuesta, explotación y análisis forense.	Alcanzar un 80% de Técnicos y Suboficiales nivel alto y medio del personal de oficiales capacitados.	
Objetivo 2 Meta 2.1 Reducir el tiempo de	IM 2.1.1	Porcentaje de optimización del tiempo de respuesta por parte de CCE, frente a	**[**Tiempo en horas trascurrido desde la detección de un incidente de seguridad informática hasta su restablecimiento **/** Horas	Optimizar el proceso de respuesta por parte del CCE	Mejorar la **eficiencia** de la producción del CCE,	Medir las horas que transcurren para restablecer los servicios que han sido	Reducir en 30 % el tiempo de respuesta actual frente a incidentes de seguridad	Medición Semestral y Anual.

respuesta ante incidentes por parte del CCE.		incidente de seguridad informática.	empleadas para restablecer el servicio actualmente por el CCE**]** ***100	frente a un incidente de seguridad informática.	optimizando el empleo de recursos y mejorando el proceso.	afectados	Informática.	
Objetivo 2 Meta 2.2 Incrementar la cobertura y aplicación de ciberdefensa del CCE en las redes del Ejército.	IM 2.2.1	Porcentaje de incremento de cobertura de ciberdefensa en redes informáticas del Ejército por parte del CCE.	**[**Número de redes informáticas coberturadas por el CCE**/** Total de redes informáticas de responsabilidad del CCE**]** ***100	Ampliar el área de cobertura de redes informáticas por el CCE que apoyen a la toma de decisiones del comando del Ejército.	Permite mejorar la **eficacia** Toma de decisiones por parte de los diferentes niveles de comando.	Medir el número de redes informáticas (hardware y software) coberturadas por el CCE.	Alcanzar el incremento de un 25 % de redes informáticas coberturadas por el CCE	Medición Semestral y Anual.
Objetivo 2 Meta 2.3 Incrementar las operaciones y acciones de ciberdefensa por parte el CCE.	IM 2.3.1	Porcentaje de incremento de las operaciones de ciberdefensa realizadas por el CCE.	**[**Número de operaciones o actividades cibernéticas realizadas por el CCE/ Número Total de operaciones o actividades realizadas durante los últimos doce meses] ***100	Asegurar las redes informáticas del Ejército mediante la ciberdefensa y apoyar las operaciones de información mediante la toma de decisiones.	Mejora la **eficacia** en la Toma de decisiones por parte de los diferentes niveles de comando.	Medir el número de reportes, informes y planes ejecutados por el CCE.	Alcanzar el incremento del 35 % de las operaciones y acciones de ciberdefensa por el CCE.	Medición Semestral y Anual.

Nota. Elaboración propia. Guía para la elaboración de indicadores 2024, (CEPLAN, 2024).

Anexo 10. Plan de implementación de indicadores en el CCE 3 / 6 / 12.

Objetivos por alcanzar	Metas por alcanzar	Indicadores	Línea de tiempo de la implementación				Resultado Esperado
			Línea Base	Acciones a los 90 días	Acciones a los 180 días	Acciones a los 365 días	
OBJ 1 Capacitar al personal del CCE, a fin de que cuenten con las competencias de ciberdefensa necesarias para desarrollar ataque, respuesta, explotación y análisis forense.	**Meta 1.1** Capacitar al personal de Oficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.	○ % OO capacitados en ataque, respuesta y explotación cibernética. ○ % OO capacitados en análisis forense de redes. ○ % OO del CCE que alcanzan Nivel óptimo de capacitación en ciberdefensa.	06 oficiales prestan servicio CCE de los cuales uno (01) cuenta con capacitación en ataque, explotación y respuesta.	○ Capacitar en conocimiento básico de Ciberdefensa al personal del CCE. ○ Capacitar en conocimiento básica en análisis forense de redes informática. ○ Incluir en las mallas curriculares de instrucción de EMCH, nociones básicas de Ciberdefensa. ○ Incluir nociones técnicas de empleo de redes y ciberdefensa en las mallas curriculares de la IESTPE. ○ Incluir talleres y módulos de ciberdefensa en todos los programas conducidos por la ECOME. ○ Incluir módulo de ciberdefensa y operaciones de información dentro de las Programas conducidos por la ESGE.	○ Realizar la medición de los programas académicos sobre Ciberdefensa. ○ Realizar la medición del CCE sobre personal capacitado en ciberdefensa. ○ Realizar talleres y ejercicios de ciberdefensa.	○ Realizar la evaluación del nivel de conocimiento de ciberdefensa por parte del personal del CCE. ○ Realizar la evaluación de la percepción del personal de las unidades de comunicaciones sobre la situación de ciberdefensa y el CCE.	Alcanzar una percepción positiva por parte del personal de las UU de COM.
	Objetivo 1 **Meta 1.2** Capacitar al personal de Técnicos y Suboficiales del CCE, en el empleo técnico y táctico de la ciberdefensa.	○ % Tcos y SSOO capacitados en ataque, respuesta y explotación cibernética. ○ % Tcos y SSOO capacitados en análisis forense de redes informáticas. ○ % Tcos y SSOO del CCE que alcanzan Nivel óptimo de capacitación en ciberdefensa.	10 Tcos y SSOO prestan servicio CCE de los cuales dos (02) cuentan con capacitación en básica de ataque, respuesta y explotación cibernética.				
OBJ 2 Realizar Operaciones de ciberdefensa que permitan el uso efectivo del ciberespacio.	**Objetivo 2** **Meta 2.1** Reducir el tiempo de respuesta ante incidentes por parte del CCE.	% de optimización del tiempo de respuesta por parte de CCE, frente a incidente de seguridad informática.	Actualmente no se atiende incidentes de seguridad con el personal de CCE.	○ Establecer y elaborar los procesos, procedimientos y protocolos sobre respuesta ante incidentes de seguridad de redes informática por parte del CCE. ○ Establecer tiempos de respuesta recomendado para los diferentes Niveles de incidentes (Crítico, alto, medio y bajo). ○ Mejorar el nivel de madurez del sistema CCE a un nivel [**Nivel 1 (Inicial)**; **Nivel 2 (Gestionado)**; Nivel 3	○ Realizar la medición de la implementación de procesos, procedimiento y protocolos sobre ciberdefensa en el CCE. ○ Establecer la reducción de 30 % del tiempo de atención ante incidentes de redes informáticas. ○ Medir y afianzar el nivel de madurez alcanzado con	○ Realizar la evaluación de la percepción del personal de las unidades de comunicaciones sobre la situación de ciberdefensa y el CCE. ○ Realizar la evaluación del desarrollo de competencias por parte del personal de CCE. ○ Realizar la evaluación del Nivel	

				(Definido); Nivel 4 (Gestionado cuantitativamente) y Nivel 5 (Optimizado)]	capacitaciones, talleres y ejercicios.	de madurez del CCE.	
	Objetivo 2 **Meta 2.2** Incrementar la cobertura y aplicación de ciberdefensa del CCE en las redes del Ejército.	% de incremento de cobertura de ciberdefensa en redes informáticas del Ejército por parte del CCE.	El CCE solo presta servicio de ciberseguridad al Data Center (HUB Principal).	○ Realizar el levantamiento de información sobre redes informáticas en el Ejército a nivel nacional y clasificar según la relevancia para la toma de decisiones. ○ Realizar el levantamiento de información de los sistemas informáticos que poseen los activos críticos y recursos claves. ○ Realizar el diagnóstico seguridad de las redes del Ejército y mapeo de todos protocolos de seguridad.	○Realizar la trazabilidad de la generación de reportes e informes por las unidades encargadas de ciberseguridad y ciberdefensa. ○Realizar la medición de los avances de levantamiento y diagnóstico de información de redes informáticas.		
	Objetivo 2 **Meta 2.3** Incrementar las operaciones y acciones de ciberdefensa por parte el CCE.	% de incremento de las operaciones de ciberdefensa realizadas por el CCE.	Actualmente no se registran las actividades realizadas por el CCE.	○ Realización de dos (02) Ejercicios mensuales en respuesta ante incidentes. ○ Realizar ejercicios virtuales de ciberseguridad, juego de guerra (res team vs blue team), ejercicios de mesa(discusión de simulación de escenarios de ataque); CTF (Capture The Flag) competencias prácticas para completar desafíos de ciberseguridad.	○Realizar la trazabilidad de la generación de reportes e informes por las unidades encargadas de ciberseguridad y ciberdefensa. ○Realizar la recopilación de información y realizar la medición de actividades desarrolladas por el CCE.		

Nota. Tabla relacionada a los objetivos con sus respectivas metas, planificados, desde los 90 días hasta los 365 días.