INSTITUTO CIENTÍFICO Y TECNOLÓGICO DEL EJÉRCITO

FACULTAD DE CIENCIAS Y HUMANIDADES

CARRERA DE INGENIERÍA DE TELECOMUNICACIONES

TRABAJO DE SUFICIENCIA PROFESIONAL

Optimización de la Gestión Operativa y Cibernética Mediante el Diseño del Cuadro de Organización y Equipo en el Centro de Ciberdefensa del Ejército del Perú, Lima, 2025.

PARA OPTAR EL TÍTULO PROFESIONAL DE:
Ingeniería en Telecomunicaciones

PRESENTADO POR:
Bach. Zully Melissa Poclin Guevara
(Código ORCID: https://orcid.org/0009-0006-3829-7577)

ASESOR:
Mg. Carlos Quinto Huamán
(Código ORCID: https://orcid.org/0000-0001-9995-3941)

LÍNEA DE INVESTIGACIÓN:
Ciencia de datos, Inteligencia Artificial, Ciberseguridad y Ciberdefensa

Lima, mayo del 2026

DEDICATORIA

A mi familia, a mi novio y mi bebe que viene en camino por su paciencia y respaldo constante. A mis instructores y superiores por su guía profesional.

AGRADECIMIENTOS

Al Centro de Ciberdefensa por facilitar el desarrollo de esta experiencia, a mi asesor por sus observaciones técnicas y a mis compañeros de trabajo por su compromiso en cada actividad.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS

RESUMEN EJECUTIVO

Durante el periodo comprendido del AF-2024 y del AF-2025 laboré en el Centro de Ciberdefensa del Ejército del Perú y tuve la responsabilidad de jefe del departamento de respuesta e integré en el comité de la formulación y el Diseño del Cuadro de Organización y Equipo del Centro de Ciberdefensa del Ejército del Perú, con sede en Lima - San Borja orientada a la optimización de la Gestión Operativa y Cibernética institucional dentro del Comando de Operaciones Cibernéticas. La experiencia se desarrolló en tres frentes complementarios.

El primero consistió en realizar un Informe de estudio de estado mayor que consistió en identificar el problema, suposiciones, hechos o factores que influyen en el problema, discusión, conclusiones y acción recomendada para la formulación del Cuadro de Organización y Equipo del Centro de Ciberdefensa y fue validada por la Dirección de Planeamiento del Ejército.

El segundo consistió en la Formulación de la Sección I (Generalidades) validado por la Dirección de Doctrina del Ejército, Sección II (Personal) validado por la Dirección de personal del Ejército, Sección III (Equipo) validado por el Comando logístico del Ejército, Sección IV (Personal y Equipo por capacidades) validado por la Dirección de Planeamiento del Ejército.

El tercero se centró en la formulación de la Hoja de Recomendación, cuyo objetivo fue sustentar y viabilizar la aprobación del Proyecto de Cuadro de Organización y Equipo del Centro de Ciberdefensa, incorporando los lineamientos técnicos, administrativos y operativos emitidos por las diferentes dependencias responsables de la implementación.

Las acciones implementadas fueron diseñadas con lineamientos a la realidad operativa de la unidad, la normativa vigente y las capacidades institucionales existentes, priorizando el uso eficiente de los recursos, el fortalecimiento de los procesos internos y la mejora progresiva de la gestión operativa y cibernética del Centro de Ciberdefensa

CAPÍTULO I. INTRODUCCIÓN

1.1 Datos generales de la institución

El Centro de Ciberdefensa forma parte orgánica del Comando de Operaciones Cibernéticas del Ejército del Perú, con sede en Lima – San Borja. Su estructura responde a la organización del arma de comunicaciones del Ejército, teniendo como función principal realizar operaciones militares con capacidades de defensa, explotación, respuesta e investigación digital para proteger el sector en el ciberespacio propio y asignado.

1.2 Razón social y canales de contacto

La institución pertenece al Ejército del Perú, con sede administrativa en el Cuartel General del Ejército. Los canales de contacto oficiales se desarrollan a través de las oficinas administrativas, la red de intranet institucional y los canales de comunicación establecidos en la normativa militar.

1.3 Actividad principal

La actividad central del Centro de Ciberdefensa es planificar y ejecutar operaciones militares para prevenir, detectar y responder a amenazas cibernéticas, protegiendo los sistemas de información, redes y activos críticos del Ejército, y garantizando la continuidad operativa y la seguridad nacional.

1.4 Breve reseña histórica

El Comando de Telemática del Ejército y una de sus unidades orgánicas el Centro de Ciberdefensa fue creada con Resolución de la comandancia General N°129, el 28 enero del 2019 de manera experimental, así mismo el 26 de agosto 2019 se aprueba la Ley N°30999 (Ley de Ciberdefensa),el 12 noviembre 2019 con Resolución de la Comandancia General N° 998, se crea la Ciberdefensa y Telemática del Ejército (CITELE) con una de sus unidades el Centro de Ciberdefensa (CECIBER) de manera experimental, en enero 2020 se crea el Comando Operacional de Ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas, el 13 febrero del 2024 aprueban el reglamento de la Ley de Ciberdefensa, el 04 setiembre del 2024 con el Decreto Legislativo N° 1640 que modifica el Decreto Legislativo Nº 1137, Ley del Ejército del Perú, se crea el

Comando de Operaciones Cibernéticas como un Órgano de Línea, ubicado en el "Cuartel General del Ejército" del distrito de San Borja – Lima, sin embargo no contaba con un Cuadro de Organización y Equipo (COEq) con personal especializado y tecnología avanzada para asegurar su eficacia operativa durante su empleo en operaciones militares, así mismo teniendo dentro de su organización la Unidad de Ciberdefensa.

Es por ello que se conformó un comité encargado de formular el Cuadro de Organización y Equipo (COEq) de las unidades del Comando de Operaciones Cibernéticas, que fue aprobada con Resolución de la Comandancia General del Ejército N°1019 – CGE/DIPLANE el 23 diciembre 2025.

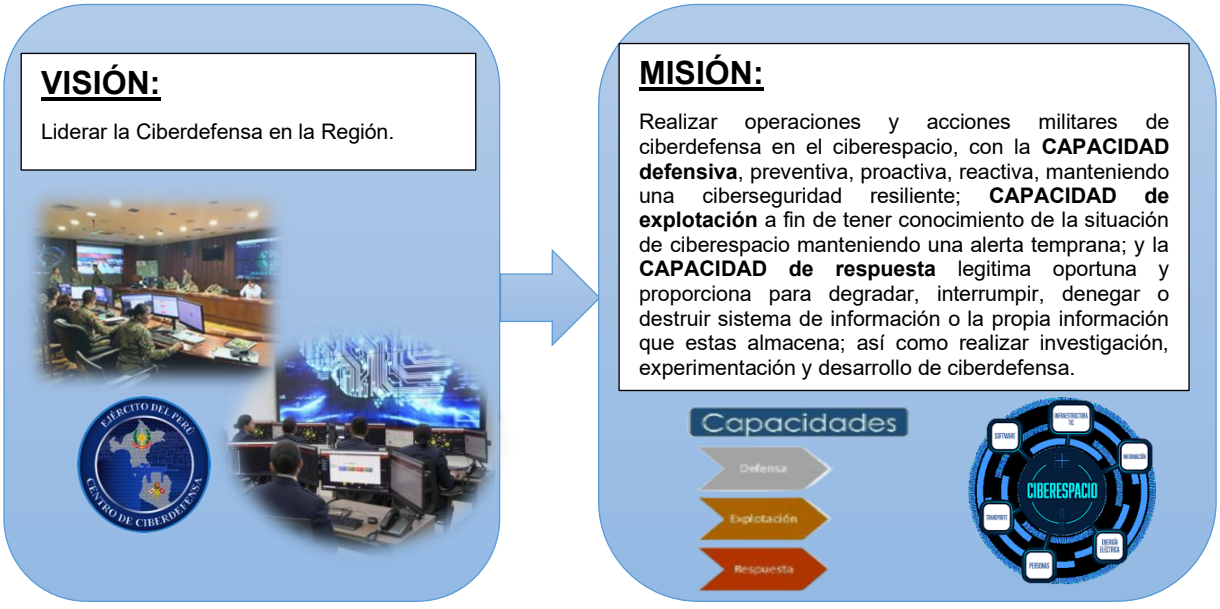
Para el año 2025, la unidad de Ciberdefensa proyectó ejecutar acciones articuladas al Plan Estratégico de Desarrollo Institucional (PTI 2034), orientadas al fortalecimiento de la capacidad operativa, doctrinaria del Centro de Ciberdefensa, Objetivo Estratégico OE 5 (Desarrollar la ciberdefensa en el Ejército).

1.5 Visión y misión institucional

En la Figura 1, detalla la visión y misión del Centro de Ciberdefensa relacionado a las operaciones militares en el ciberespacio con sus capacidades y como lideraría en un óptimo Centro de operaciones de Ciberdefensa en el Ejército del Perú (MOF, 2024 y la Directiva N° 003-2019-" Funcionamiento experimental").

Figura 1

Visión y misión del Centro de Ciberdefensa del Ejército del Perú hasta el AF-2025



1.6 Descripción de la posición laboral

Durante el periodo de la experiencia descrita, me desempeñé como Jefe del Departamento de Respuesta del Centro de Ciberdefensa, función desde la cual lideré, coordiné y supervisé al equipo técnico especializado. Estas actividades estuvieron orientadas a la prevención, detección, análisis, contención y respuesta ante incidentes y amenazas cibernéticas que pudieran afectar los sistemas de información, redes y activos críticos del Ejército, garantizando la continuidad operativa y la seguridad institucional.

Asimismo, tuve a mi cargo el departamento de respuesta, asegurando constantemente el funcionamiento en coordinación con el Comando de Operaciones Cibernéticas. Estas funciones incluyeron en todo momento una evaluación continua, elaboración de informes técnicos, gestiones y recomendaciones para mejorar las capacidades del Centro de Ciberdefensa.

De manera permanente, participé de forma activa y directa en el diseño y formulación del Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa, desarrollé un estudio de estado mayor orientados a definir la estructura orgánica, los perfiles del personal, los niveles de especialización, las capacidades operativas y los requerimientos de equipamiento tecnológico. Este proyecto se realizó en cumplimiento de la normativa vigente y en coordinación con las dependencias y direcciones competentes del Ejército.

1.7 Activos del Centro de Ciberdefensa

1.7.1 Activos de información

Los activos de información del Centro de Ciberdefensa comprenden todos los datos e información critica que permiten planificar, ejecutar y supervisar operaciones en el ciberespacio, incluyendo información operacional (planes de ciberoperaciones, reportes de incidentes e inteligencia sobre amenazas) e información técnica.

En la Figura 2, se puede observar el formato de reportes de alertas integradas de seguridad digital que realiza el Centro de Ciberdefensa y es reportada diariamente al Comando Operacional de Ciberdefensa (COCID – CCFFAA).

Figura 2

Alertas Integradas de Seguridad Digital emitida al COCID del CCFFAA

ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 287

Fecha: 14-10-2025

Página: 1 de 1

Componente que reporta	CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ
Nombre de la alerta	Ransomware BlackCat Activa
Tipo de Ataque	Ransomware
Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros
Código de familia	C
Código de Sub Familia	C01
Clasificación temática familia	Código Malicioso
Descripción	

1. **ANTECEDENTES:**
En octubre del 2025, el grupo de ransomware BlackCat (ALPHV) ha continuado sus actividades, afectando principalmente al sector salud en Estados Unidos Y otros paises de latinoamerica. Desde mediados de diciembre de 2023, ha incrementado la frecuencia de sus ataques, utilizando técnicas avanzadas de doble extorsión. En agosto de 2025, se descubrió que BlackCat podría haber cambiado su nombre a "Embargo", con demandas de rescate de hasta 1.3 millones de dólares. A pesar de esfuerzos de desmantelamiento por parte de las autoridades, el grupo sigue activo y representa una amenaza significativa para las organizaciones críticas.
2. **DETALLES:**
El ransomware se propaga principalmente a través de correos electrónicos de phishing que contienen enlaces o archivos adjuntos maliciosos, así como por la explotación de vulnerabilidades en servicios expuestos como RDP, SMB o VPN sin parchear. Una vez dentro del sistema, el malware cifra archivos tanto en dispositivos locales como en unidades de red conectadas para maximizar el impacto. Además, elimina o modifica copias de sombra y puntos de restauración para dificultar la recuperación de datos sin pagar el rescate. Antes de proceder al cifrado, el ransomware suele ejecutar movimientos laterales dentro de la red, utilizando herramientas de enumeración y robo de credenciales, como Mimikatz, para expandir su alcance. Este comportamiento permite afectar múltiples sistemas críticos, lo que puede dejar fuera de servicio aplicaciones empresariales y bases de datos compartidas. En algunas variantes, se ha reportado la exfiltración de datos sensibles previa al cifrado, con lo que se combina la doble extorsión: cifrado y amenaza de divulgar información confidencial. Los atacantes solicitan el pago del rescate en criptomonedas, y emplean tácticas de presión como la amenaza de publicar los datos robados para aumentar la probabilidad de pago. Esta modalidad convierte al ransomware en una amenaza compleja que afecta tanto la integridad como la confidencialidad de la información en las organizaciones.

3. **RECOMENDACIONES:**
- Desconectar inmediatamente los hosts sospechosos de la red (físico o a nivel de puerto/segmento). Deshabilitar RDP y accesos remotos hasta verificar.
- No apagar máquinas comprometidas (apagar puede destruir evidencias). Tomar imágenes forenses, capturar memoria RAM si es posible, recolectar logs (SIEM, firewall, EDR) y hashes de archivos cifrados. Activar el plan de respuesta a incidentes.
- Restaurar desde backups verificados en sistemas limpios. Antes de restaurar, asegurarse de que la amenaza esté erradicada (escaneo EDR/antivirus actualizado). Parchear inmediatamente vulnerabilidades publicadas relacionadas y rotar credenciales privilegiadas.
- Evaluar obligaciones regulatorias (notificación de brechas a autoridades y clientes según la jurisdicción). Considerar contactar a un equipo de respuesta forense especializado y, si procede, a la policía/cert nacional de ciberseguridad.

Fuente de Información	https://www.varonis.com/blog/blackcat-ransomware

1.7.2 Activos tecnológicos

Esto se refiere a recurso de hardware del Centro de Ciberdefensa que dispone de equipos de computación, servidores de tecnología desactualizada y limitada, instalados en un ambiente sin sistema de refrigeración y cableado estructurado tradicional. En cuanto al suministro de internet, el Centro de Ciberdefensa cuenta con un servicio restringido proporcionado por el Centro de Informaciones y estadística del Ejército - CINFE.

En las Figuras 3 y 4, se puede apreciar los equipos de cómputo, servidores y equipos de red (firewalls, switches, routers) instaladas en el área de operaciones del Centro de Ciberdefensa, en el cual se realiza las diversas funciones y capacitaciones de acuerdo a las capacidades de ciberdefensa a pesar de las limitaciones.

Figura 3

Tomas fotográficas de los equipos de cómputo del Centro de Ciberdefensa

Figura 4

Tomas fotográficas de los servidores y equipos de red del Centro de Ciberdefensa

1.7.3 Activos de software

Según el National Institute of Standards and Technology (NIST) y las normas ISO/IEC 2700 “Los activos de software en un centro de ciberdefensa se refieren a todos los programas, aplicaciones y sistemas informáticos que almacenan, procesan o transmiten datos críticos, como herramientas de monitoreo de amenazas, firewalls, sistemas de detección de intrusiones (IDS/IPS) y software de análisis de malware”. El Centro de Ciberdefensa utiliza software libre que permite analizar, detectar a ciberataques.

En la Figura 5, detalla algunas herramientas open source (software libre) que utiliza el Centro de Ciberdefensa como (Ubuntu server, Wazuh, Snort, Suricata, Ubuntu, Nessus, Tenable, Kali Linux, Metaexploit, etc.).

Figura 5

Herramientas de software libre que utiliza el Centro de Ciberdefensa

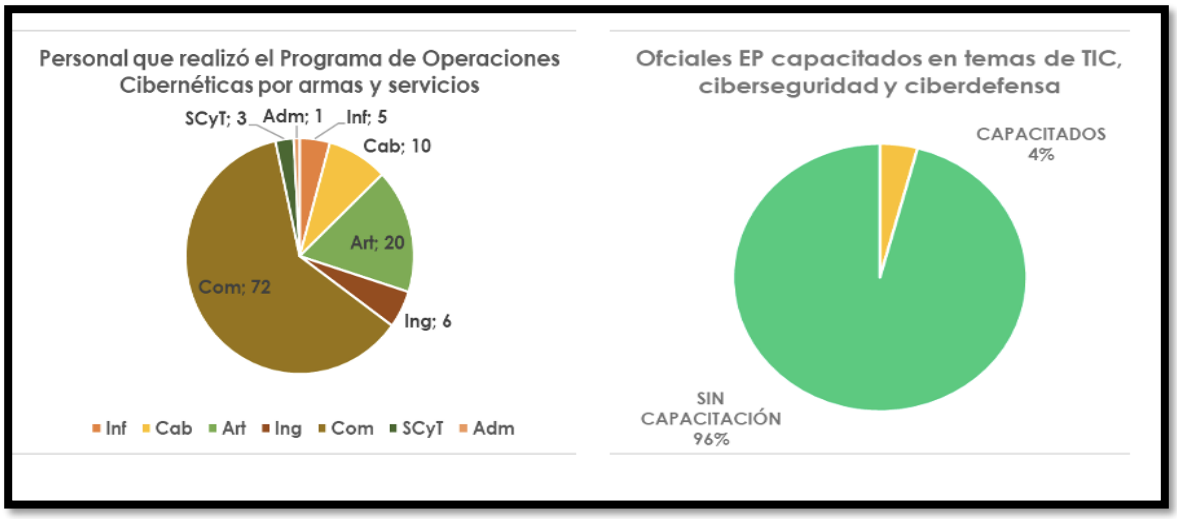
1.7.4 Activos humanos

Según la Guía de Ciberdefensa de la Junta interamericana de Defensa (2020), “El personal de ciberdefensa debe considerarse como crítico, operativo, permanente, de dedicación exclusiva y de larga amortización. Además, se debe prestar especial atención, por su gran potencial, a la reserva voluntaria en el campo de la ciberdefensa” (p. 48). En el Ejército del Perú existe personal de oficiales, técnicos y suboficiales que han sido capacitados y se puede evidenciar en los cuadros estadísticos.

En la Figura 6, detalla la estadística del personal que realizarón el Programa de Operaciones Cibernéticas por armas y servicios, teniendo un resultado del total de 117 oficiales, en las cuales el 70% es del arma de comunicaciones, así como también se puede apreciar que es reducido el personal que tiene a capacitación en temas de ciberdefensa.

Figura 6

Estadística de oficiales que realizaron curso y capacitación en Ciberdefensa



Nota. La figura que se observa es información del diagnóstico situacional del Centro de Ciberdefensa AF – 2024.

1.7.5 Activos de conocimientos y procedimientos

Es una de las capacidades fundamentales para la operatividad del Centro de Ciberdefensa; tiene la finalidad de distribuir el conocimiento entre las partes interesadas y facilitar su acceso de acuerdo a los criterios de necesidad y autorización.

El conocimiento es una capacidad basada en dos áreas, funcional y técnica; siendo el área funcional la parte fundamental y más compleja debido a que precisa de un planteamiento y procedimientos personalizados adaptados a las peculiaridades y necesidades de la unidad; mientras que la parte técnica se puede resolver mediante la utilización de herramientas y procedimientos comerciales de uso generalizado.

En la Figura 7, se observa la explicación de los procedimientos que se realiza en el Centro de ciberdefensa al personal de cadetes y alumnos que visitaron las instalaciones del centro.

Figura 7

Tomas fotográficas de procedimientos de Ciberdefensa

1.7.6 Activos de infraestructura

Los activos de infraestructura en un Centro de Ciberdefensa comprenden los recursos tecnológicos y estructurales que soportan el funcionamiento de los sistemas de información y de seguridad, tales como redes de comunicación, centros de datos y sistemas de soporte operativo (National Institute of Standards and Technology, 2023; International Organization for Standardization, 2022). Asimismo, la norma de seguridad de la información de la International Organization for Standardization establece que las instalaciones, redes y recursos de soporte tecnológico son activos que deben protegerse dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

En la Figura 8, se observa las instalaciones y el equipamiento tecnológico que cuenta del Centro de Ciberdefensa, encontrándose ubicada en el sótano del Cuartel General del Ejército, asimismo se puede apreciar que los espacios son reducidos para el funcionamiento de las capacidades de Ciberdefensa.

Figura 8

Tomas fotográficas de las instalaciones del Centro de Ciberdefensa

1.7.7 Activos normativos e intangibles

Marco legal y doctrinario, conocimiento especializado y reputación institucional. El Centro de Ciberdefensa del Ejército del Perú cuenta con la doctrina de Operaciones en el Ciberespacio (CCFFAA - 2018), la Ley de Ciberdefensa N°30999 y el reglamento de la ley y otros manuales que sirven como referencias para el planeamiento como la Guía de Ciberdefensa de la Junta Interamericana de Defensa, Manuales extranjeros, que tienen información de cómo se está desempeñando la ciberdefensa en el ciberespacio a nivel mundial, en el cual el Centro de Ciberdefensa se puede orientar ya que tiene un rol muy importante al realizar operaciones militares en el ciberespacio propio y asignado

1.8 Organigrama

1.8.1 Organización del Centro de Ciberdefensa del Ejército

En la Figura 9, se muestra el organigrama del Centro de Ciberdefensa con sus capacidades (Defensa, Explotación, Respuesta e Investigación Digital)

Figura 9

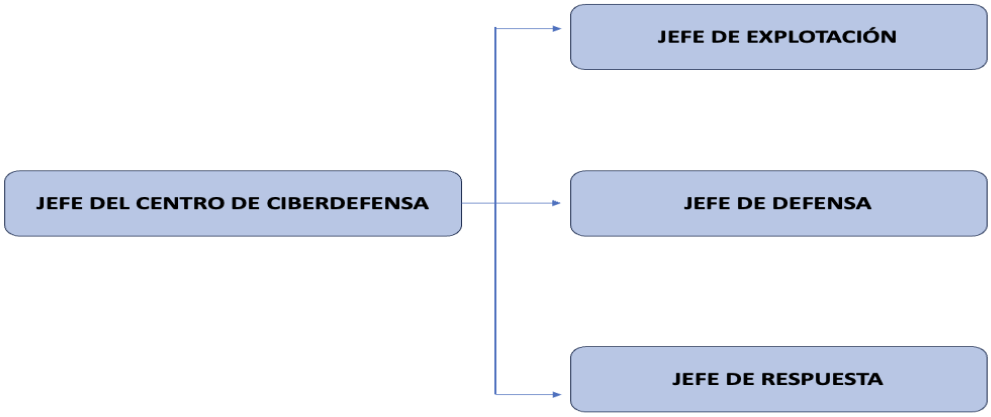
Organigrama del Centro de Ciberdefensa hasta el AF-2025

1.8.2 Organización de los puestos del Centro de Ciberdefensa

En la Figura 10, se observa los puestos de responsabilidad como el Jefe del Centro de Ciberdefensa y los puestos de acuerdo a las capacidades de Ciberdefensa y esta a su vez cuenta con puestos en cada una de ellas.

Figura 10

Organigrama de los puestos de responsabilidad del Centro de Ciberdefensa



CAPÍTULO II. MARCO TEÓRICO

2.1. Fundamentación conceptual

2.1.1 Gestión operativa

La gestión operativa representa el núcleo fundamental de la administración empresarial, un proceso complejo que trasciende la simple ejecución de tareas y se posiciona como un elemento estratégico para el éxito organizacional. La gestión operativa implica el desarrollo de funciones administrativas básicas: planear, organizar, dirigir y controlar (Itcons, 2025). En un Centro de Ciberdefensa, la gestión operativa se orienta a garantizar la continuidad de las operaciones en el ciberespacio, asegurando la detección, análisis y respuesta oportuna ante incidentes cibernéticos.

2.1.2 Gestión cibernética

La gestión cibernética comprende el conjunto de acciones orientadas a la administración, coordinación y control de las capacidades relacionadas con la seguridad y defensa en el ciberespacio (Organización de los Estados Americanos [OEA], 2022). Este tipo de gestión integra aspectos técnicos y organizacionales, considerando al ciberespacio como un dominio operacional dinámico y complejo. En el ámbito militar, la gestión cibernética busca proteger los sistemas de información críticos, garantizar la integridad, confidencialidad y disponibilidad de la información, así como mantener una adecuada conciencia situacional cibernética.

2.1.3 Ciberespacio

Se adopta la definición del diccionario Oxford, “El entorno conceptual en el que se produce la comunicación a través de redes informáticas.” El ciberespacio es un concepto, idea o noción; no es un espacio material, físico, visible ni tangible. Dado que el ciberespacio es una noción, ningún elemento físico o tangible es parte intrínseca de la infraestructura TIC, personas, tampoco los elementos no tangibles como la información, el software o la energía eléctrica (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

El concepto “ciberespacio” se materializa gracias a la interrelación de unos elementos específicos (la infraestructura de tecnologías de información y comunicaciones, el software, la información, los protocolos de transporte, la energía eléctrica y las personas) proporcionándole vitalidad.
El conjunto de los elementos, el ciberespacio y sus relaciones conforman el ecosistema ciberespacial. En la práctica, se utiliza el término ciberespacio incluyendo los elementos y sus relaciones, asimilándolo al término ecosistema ciberespacial (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

Se tiende a identificar al ciberespacio con la infraestructura de las tecnologías de la información y las telecomunicaciones (ordenadores, servidores, cableado, todo tipo de dispositivos y material hardware), de esta manera parece más entendible; pero esta identificación ciberespacio -TIC, conlleva el gran peligro de desviar la verdadera finalidad de la ciberdefensa (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

2.1.4 Ciberataques

Un ciberataque es el uso deliberado de una ciberarma, por una persona o de manera automática, para generar un daño o efecto perjudicial en las redes y sistemas de información de un adversario pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales. El comandante de una operación debe considerar todas las capacidades en su mano para conseguir los efectos deseados, para ello debe considerar ataques convencionales y ciberataques y efectos físicos y ciberefectos (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

En una operación conjunta se debe considerar todas las combinaciones posibles de ataques: ataques procedentes de un ámbito y con un objetivo en el mismo ámbito (Tierra-Tierra, Mar-Mar, Aire-Aire, Espacio-Espacio, Ciberespacio-Ciberespacio) y ataques procedentes de un ámbito y con un objetivo en otro ámbito (Tierra-Mar, Tierra-Aire, Tierra- Espacio, Tierra-Ciberespacio. Mar-Tierra, Mar-Aire, Mar-Espacio, Mar-Ciberespacio. Aire-Tierra, Aire- Mar, Aire-Espacio, Aire-Ciberespacio. Espacio-Tierra, Espacio-Mar, Espacio-Aire, Espacio-Ciberespacio.

Ciberespacio-Tierra, Ciberespacio-Mar, Ciberespacio- Aire, Ciberespacio-Ciberespacio) (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

2.1.5 Ciberdefensa

La ciberdefensa adopta un enfoque más estratégico y ofensivo (a menudo en el marco de la seguridad nacional). Interviene para defender infraestructuras críticas consideradas vitales frente a ataques coordinados a gran escala. En este sentido, se caracteriza por una reacción rápida y focalizada. (DataScientest, 2024).

Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia. (Guía de Ciberdefensa - Junta Interamericana de Defensa [JID], 2020).

2.1.6 Centro de Ciberdefensa

El Centro de Ciberdefensa es una unidad especializada encargada de planificar, conducir y ejecutar operaciones de defensa en el ciberespacio (Ministerio de Defensa del Perú [MINDEF], 2024). Su función principal es monitorear de manera permanente los sistemas de información institucionales, identificar amenazas y coordinar acciones de respuesta ante incidentes cibernéticos.

Desde una perspectiva organizacional, el Centro de Ciberdefensa debe contar con una estructura clara, roles definidos y procedimientos establecidos que permitan una actuación coordinada y eficiente. La correcta articulación entre sus áreas funcionales resulta fundamental para el cumplimiento de su misión (Ejército del Perú [EP], 2025).

2.1.7 Cuadro de Organización y Equipo

El Cuadro de Organización y Equipo (COEq) es un instrumento técnico-administrativo que define la estructura organizacional de una unidad militar, estableciendo los cargos, funciones, jerarquías y recursos asignados (Ejército del Perú, 2025). Su finalidad es garantizar que la organización cuente con el personal y los medios necesarios para cumplir eficazmente su misión.

En un Centro de Ciberdefensa, el Cuadro de organización y equipo adquiere especial relevancia debido a la necesidad de contar con personal altamente especializado y equipamiento tecnológico necesario. Un diseñado adecuado contribuye a mejorar la eficiencia operativa, optimizar la distribución de personal y fortalecer las capacidades de ciberdefensa ante amenazas cibernéticas.

2.1.8 Operaciones militares en el ciberespacio

Es el empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo con sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o ataques en y mediante el ciberespacio que atenten contra la seguridad nacional, la soberanía, los intereses nacionales y/o los ACN/RC. Entiéndase también como ciberoperaciones. (Ley de Ciberdefensa N°30999).

2.1.9 Efectivos

Se entiende por efectivos al número de hombres que forman una Unidad orgánica. Los efectivos, constituyen una de las principales indicaciones de la capacidad combativa de una Unidad; por consiguiente, para determinar el grado de efectividad de la Unidad es esencial que el Comandante y el EM disponga de las informaciones más precisas sobre los efectivos actuales o planeados. (Manual del Ejército 100 – 10 Estado Mayor – Personal).

2.2. Principios teóricos aplicados

El trabajo desarrollado se sustentó en los siguientes principios:

2.2.1 Principio de seguridad integral

La seguridad integral abarca la protección en todos los niveles de la organización. Esto incluye la seguridad física (instalaciones y personal), la ciberseguridad (sistemas y datos) y la seguridad operativa (procesos internos y acceso). A diferencia de la seguridad tradicional, que tiende a enfocarse en áreas individuales, la seguridad integral coordina cada aspecto de la protección en un sistema unificado, asegurando que todas las partes estén interconectadas para

ofrecer una defensa sólida y completa (CampusETIC, 2024). En el ámbito de la ciberdefensa, este principio reconoce que las amenazas cibernéticas afectan simultáneamente a los sistemas de información, a las personas que los operan y a los procesos que los regulan.

2.2.2 Principio de prevención

El principio de prevención es la necesidad de anticiparse a los riesgos antes de que estos se materialicen en incidentes cibernéticos. En ciberdefensa, este principio implica la identificación temprana de amenazas, el análisis permanente de vulnerabilidades y la implementación de controles de seguridad proactivos. La prevención permite reducir el impacto de los ataques, minimizar daños operativos y fortalecer la capacidad de respuesta institucional frente a amenazas emergentes en el ciberespacio (Instituto Nacional de Estándares y Tecnología [NIST], 2024).

2.2.3 Principio de defensa en profundidad

El principio de defensa en profundidad establece que una organización no debe depender de una sola línea de defensa para protegerse contra posibles amenazas. El problema con una sola línea de defensa es que, si falla, la organización es vulnerable a la defensa. Con la defensa en profundidad, la organización superpondrá múltiples líneas de defensa en toda la organización. De esta manera, existe una mayor probabilidad de que, si un atacante se desliza más allá de una línea de defensa, una posterior bloquee o detecte el ataque (Check Point, 2023).

2.2.4 Principio de disponibilidad operativa

La disponibilidad operativa se refiere a la capacidad de los sistemas, redes e información para mantenerse accesibles y funcionales cuando sean requeridos, especialmente en contextos de crisis o conflicto. En el ámbito militar, este principio es fundamental, ya que la indisponibilidad de los sistemas de información puede afectar directamente la conducción de operaciones y la toma de decisiones estratégicas (MINDEF, 2024).

2.2.5 Principio de confidencialidad, integridad y disponibilidad

El principio de confidencialidad, integridad y disponibilidad constituye la base teórica de la seguridad de la información. La confidencialidad asegura que la información sensible sea accesible únicamente para personal autorizado; la integridad garantiza que los datos no sean alterados de forma indebida; y la disponibilidad permite el acceso oportuno a la información cuando es necesaria. En la ciberdefensa, la aplicación de esta triada resulta esencial para la protección de la información estratégica, operativa y táctica del Estado (NIST, 2024).

2.2.6 Principio de jerarquía y unidad de mando

El principio de jerarquía y unidad de mando, propio de la doctrina militar, establece que toda organización debe contar con una estructura clara de autoridad y responsabilidad. En el ámbito de la ciberdefensa, este principio permite una toma de decisiones rápida, coordinada y eficaz durante la gestión de incidentes cibernéticos, evitando la duplicidad de funciones y los conflictos de mando dentro de la organización (JID, 2020).

2.2.7 Principio de especialización

El principio de especialización significa que las funciones se organizan de modo que cada puesto y cada equipo se dedica a un campo técnico específico, con competencias claras, diferenciadas, monitoreo 24/7, respuesta a incidentes, análisis forense, inteligencia de amenazas, administración de plataformas, etc. Este principio busca que las tareas críticas no recaigan en perfiles “generalistas” sino en personal altamente capacitado en cada área, para aumentar la eficacia operativa, la calidad del análisis técnico y la velocidad de respuesta frente a incidentes (Inter-American Development Bank, 2020).

2.2.8 Principio de adaptabilidad

El principio de adaptabilidad reconoce que el ciberespacio es un entorno dinámico y en constante evolución, caracterizado por la aparición permanente de nuevas amenazas y tecnologías. En este sentido, las organizaciones de ciberdefensa deben ser flexibles y capaces de ajustar sus estructuras,

procedimientos y capacidades operativas para responder eficazmente a escenarios cambiantes, fortaleciendo así su capacidad de resiliencia institucional (OEA, 2022).

2.2.9 Principio de coordinación interinstitucional

El principio de coordinación interinstitucional establece que la ciberdefensa no puede desarrollarse de manera aislada, sino que requiere la cooperación entre diversas entidades del Estado y, cuando corresponda, con organismos internacionales. Esta coordinación facilita el intercambio de información, la estandarización de procedimientos y la respuesta conjunta ante amenazas cibernéticas que superan las capacidades de una sola institución (OEA, 2022; OTAN, 2023).

2.3 Estándares de ciberdefensa más reconocidos

2.3.1 El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología también denominado en inglés National Institute of Standards and Technology and Cybersecurity Framework (NIST CSF) proporciona un enfoque más flexible que se estructura en seis funciones: identificar, proteger, detectar, responder, recuperar y gobernar. A diferencia de las normas certificables, es un marco voluntario que posibilita personalizar los controles según el perfil de riesgo y contexto de la organización. Su adaptabilidad lo hace especialmente útil en distintos sectores y tamaños de empresa (National Institute of Standards and Technology, 2024)

2.3.2 Las normas de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional 27001 y 27002

Las normas ISO/IEC 27001 y 27002 define los requisitos para implementar un SGSI (Sistema de Gestión de Seguridad de la Información). Establece procesos como planificación de riesgos, auditoría de controles, mejora continua y revisión directiva, con posibilidad de certificación externa, a fin de demostrar formalmente el

compromiso con las mejores prácticas de seguridad informática y con el compliance en ciberseguridad **(**ISO/IEC 27001:2022, 2022)

2.3.3. Política de Ciberdefensa de la Organización del Tratado del Atlántico Norte

La Organización del Tratado del Atlántico Norte reconoce el ciberespacio como un dominio operacional, integrándolo plenamente en la planificación estratégica y operativa militar. La Política de Ciberdefensa de la OTAN enfatiza la resiliencia, la defensa colectiva y el mando y control cibernético como elementos esenciales para la seguridad de los Estados (OTAN, 2023). Este enfoque doctrinario constituye una referencia clave para el diseño y funcionamiento de centros de ciberdefensa militares.

2.3.4. Marco de Ciberseguridad de la Agencia de la Unión Europea para la Ciberseguridad

El marco desarrollado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) se orienta a la protección de infraestructuras críticas y a la gestión coordinada de incidentes cibernéticos. Este estándar destaca la importancia de la cooperación interinstitucional, la preparación ante cibercrisis y la articulación de equipos de respuesta especializados (ENISA, 2023). Su aplicación resulta relevante para centros de ciberdefensa que operan en entornos complejos y altamente interconectados.

2.3.5. Los controles de seguridad críticos

Los Controles de Seguridad Críticos también denominado en inglés Critical Security Controls (CIS) consisten en un conjunto priorizado de controles diseñados para mitigar las amenazas cibernéticas más comunes. Su enfoque práctico y progresivo permite a las organizaciones implementar medidas de ciberdefensa de manera gradual, priorizando la gestión de activos, el control de accesos y el monitoreo continuo (Center for Internet Security, 2023). Este marco es especialmente útil en organizaciones con recursos limitados, al facilitar la optimización de capacidades operativas.

2.3.6 Marco de Ciberdefensa de la Organización de los Estados Americanos

La Organización de los Estados Americanos promueve el fortalecimiento de las capacidades de ciberdefensa de los estados miembros mediante lineamientos estratégicos y cooperación regional. Su marco enfatiza la protección de infraestructuras críticas, la gestión del riesgo cibernético y la respuesta coordinada ante amenazas transnacionales (OEA, 2022). Este enfoque resulta particularmente relevante para los países de América Latina y el Caribe.

2.3.7 Normativa y doctrina nacional de Ciberdefensa en el Perú

En el Perú, la ciberdefensa se rige por un conjunto de normas y políticas que establecen las responsabilidades del Estado en la protección del ciberespacio nacional. La Ley de Ciberdefensa y los lineamientos doctrinarios del Ministerio de Defensa permiten adaptar los estándares internacionales a la realidad operativa del Ejército del Perú, garantizando coherencia con los objetivos estratégicos de seguridad y defensa nacional (MINDEF, 2024).

2.4 Fundamentos reglamentarios y normativos

La experiencia se enmarcó en el cumplimiento de reglamentos y directivas institucionales, entre los que destacan:

2.4.1 Decreto Supremo N° 012-2017-DE Política de Seguridad y Defensa Nacional

Se difunde la política de Seguridad y Defensa Nacional 2017, aprobada por el Consejo de Seguridad y Defensa Nacional, es una política de Estado que permite orientar la selección, preparación y utilización de los medios del Estado para la obtención y mantenimiento de la Seguridad Nacional, tanto en el frente externo cómo en el frente interno. Está política Nacional tiene objetivos relacionados a la Ciberdefensa de acuerdo con el siguiente detalle:

Objetivo N° 1

“Garantizar la soberanía, la independencia, la integridad territorial y la protección de los intereses nacionales”.

Lineamiento N° 7

“Proteger los Activos Críticos Nacionales (ACN) contra todo tipo de amenazas, así como los sistemas de información de las amenazas que, desde el ciberespacio, atenten contra la Seguridad y Defensa Nacional”.

Objetivo N° 2

“Garantizar el orden interno contribuyendo al normal funcionamiento de la institucionalidad política y jurídica del Estado”.

Lineamiento N° 9

“Promover un proceso integral de reforma y adecuación de las normas vigentes del ordenamiento jurídico, referidas a las amenazas a la Seguridad Nacional, en particular el terrorismo, la ciberdelincuencia, el tráfico ilícito de drogas y delitos conexos, el tráfico ilícito de flora y fauna silvestre, la tala ilegal, la minería ilegal e informa, la trata de personas y el lavado de activos, entre otras.

2.4.2 Ley N° 30999, Ley de Ciberdefensa y el reglamento de la Ley de Ciberdefensa

Se establece el marco normativo para regular las operaciones militares de ciberdefensa en el ciberespacio, con el propósito de preservar la Seguridad Nacional. Indicando que, la ciberdefensa comprende al Comando Operacional de Ciberdefensa y a sus componentes de ciberdefensa que son: el componente de Ciberdefensa del Ejército del Perú, componente de Ciberdefensa de la Marina de Guerra del Perú y componente de Ciberdefensa de la Fuerza Aérea del Perú, los cuales ejecutan operaciones de ciberdefensa en y mediante el ciberespacio.

2.4.3 Decreto Legislativo N° 1640 que modifica el Decreto Legislativo Nº 1137, Ley del Ejército del Perú

Se amplió la competencia institucional en el aspecto de Ciberdefensa; asimismo, dentro de la estructura orgánica, se creó al Comando de Operaciones Cibernéticas como un Órgano de Línea que opera, defiende, responde, influye e informa en el dominio del ciberespacio, teniendo como misión proteger y defender la información y las comunicaciones, a través de la capacidad de ciberdefensa, asegurando el comando y control, frente a las amenazas que afecten la seguridad

nacional, los intereses nacionales, los activos críticos nacionales (ACN) y recursos claves (RC) para mantener las capacidades nacionales en el área de su responsabilidad.

2.4.4 Decreto Supremo N° 005-2025-DE que adecua al reglamento del Decreto Legislativo Nº 1137, Ley del Ejército del Perú del 05 Julio 2025.

En el **Artículo 66-A,** el Comando de Operaciones Cibernéticas opera, defiende, responde, influye e informa en el dominio del ciberespacio, en el ámbito de su competencia, para proteger y defender la información y las comunicaciones, a través de la capacidad de ciberdefensa, asegurando el comando y control, frente a las amenazas que afecten la seguridad nacional, los intereses nacionales, los activos críticos nacionales (ACN) y recursos claves (RC) para mantener las capacidades nacionales en el área de su responsabilidad.
El cargo de Comandante General del Comando de Operaciones Cibernéticas, será ejercido por un Oficial General del grado de General de Brigada es nombrado mediante Resolución Suprema.

En el **Artículo 66-B** Unidades Orgánicas del Comando de Operaciones Cibernéticas tiene a su cargo las unidades orgánicas siguientes:

66 B.1 Unidad de Ciberdefensa
66 B.2 Unidad de Comando y Control
66 B.3 Unidad administrativa

2.4.5 El Plan de transformación institucional al 2034

Contempla la capacidad en Ciberdefensa, para el cumplimiento del objetivo N° 5 (Desarrollar la Ciberdefensa en el Ejército del Perú) y en el mapa de procesos respectivo.

2.4.6 Directiva N° 001-2024/DIPLANE/H-3 sobre reestructuración y aprobación de cuadros de organización y equipo.

Establece que la Dirección de Planeamiento del Ejército (DIPLANE) fija los lineamientos para la formulación, reestructuración y aprobación de los cuadros de

organización y equipo (COEq) de las unidades y pequeñas unidades, de acuerdo con el Plan Estratégico de Magnitud de la Fuerza (PEMFza) al 2034.

En conjunto, estos documentos constituyen el marco político, jurídico, estratégico y técnico que sustenta la ciberdefensa en el Ejército del Perú, proporcionando legitimidad normativa, orientación estratégica y criterios organizacionales para el diseño del Cuadro de Organización y Equipo del Centro de Ciberdefensa. Su articulación permite optimizar la gestión operativa y cibernética, alineando la estructura organizacional con las nuevas amenazas del ciberespacio y los objetivos de la defensa nacional.

2.5 Limitaciones identificadas

Durante el desarrollo de la experiencia profesional**,** se identificaron diversas limitaciones que influyeron en el proceso de análisis, planificación y formulación de del Cuadro de Organización y Equipo del Centro de Ciberdefensa, teniendo las siguientes limitaciones.

2.5.1 Limitación presupuestal

Durante mi experiencia profesional se realizó diversas gestiones para adquirir el presupuesto para implementar las capacidades de ciberdefensa, sin embargo, hubo limitaciones presupuestales asignadas al Centro de Ciberdefensa. La disponibilidad limitada de recursos financieros dificultó la adquisición o actualización de herramientas tecnológicas en ciberdefensa.

2.5.2 Limitación en el acceso a información clasificada y sensible

Propia del ámbito militar y de la ciberdefensa. Esta restricción condicionó el nivel de detalle con el que se pudo analizar determinados procesos operativos, capacidades técnicas y estructuras internas del Centro de Ciberdefensa, obligando a trabajar con información autorizada, lineamientos generales y documentación normativa disponible.

2.5.3 Limitación relacionada con la actualización y disponibilidad de documentación institucional

Algunos manuales, directivas internas y documentos organizacionales se encontraban en proceso de actualización y adecuación a la normativa vigente en

materia de ciberdefensa y al proceso de transformación institucional, lo cual limitó la disponibilidad de información completamente actualizada durante el desarrollo del trabajo.

2.5.4 Limitación relacionada a la rotación y reasignación frecuente del personal

Lo cual generó que parte del personal asignado al Centro de Ciberdefensa no contara con formación especializada en ciberdefensa o ciberseguridad. Esta situación obligó a emplear personal con perfiles generales o provenientes de otras especialidades, quienes se encontraban en proceso de adaptación a funciones técnicas específicas.

2.5.5 *Limitación en las instalaciones y estructuración en el Centro de Ciberdefensa*

Se identificaron limitaciones en el Centro de Ciberdefensa que se encuentra temporalmente en el sótano del Cuartel General del Ejército, el ambiente es pequeño y no permite crecer en relación al personal y demás capacidades. Asimismo, no se cuenta con un ambiente de refrigeración para los servidores.

2.6 Aporte práctico del marco teórico

El sustento conceptual y normativo desarrollado permitió orientar el diseño del Cuadro de Organización y Equipo del Centro de Ciberdefensa del Ejército del Perú de acuerdo con su realidad operativa y misional. Más allá del enfoque teórico, los principios de gestión operativa y cibernética se materializaron en acciones concretas, como la definición de funciones especializadas, la reorganización de roles críticos y la priorización de capacidades esenciales para la detección y respuesta ante incidentes cibernéticos.

Asimismo, los conceptos de ciberdefensa, diseño organizacional y la optimización permiten establecer criterios técnicos para la asignación de roles especializados, la definición de perfiles profesionales y la estructuración jerárquica del Centro de Ciberdefensa.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA PROFESIONAL

3.1 Ingreso, circunstancias y conformación del equipo

Con Resolución N°001/COCIBER/DEPLANO/7.a de la Comandancia del Comando de Operaciones Cibernéticas del Ejército con fecha 28 marzo 2025 fui designada para conformar en el Comité encargado de elaborar la formulación y aprobación del Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa del Ejército del Perú, en el marco de los procesos de optimización de la gestión operativa y cibernética impulsados por la institución. Dicha designación respondió a la necesidad de fortalecer la estructura organizacional del Centro de Ciberdefensa, considerando el incremento de las amenazas cibernéticas y la creciente importancia del ciberespacio como dominio operacional.

La designación se realizó por lo conocimientos obtenidos durante la carrera profesional y el puesto que me desempeñaba dentro de la unidad de ciberdefensa en el Ejército del Perú. Es por ello al analizar la situación del Centro de Ciberdefensa se evidenció la necesidad de contar con un COEq actualizado que permitiera una distribución eficiente de funciones, roles y responsabilidades, así como una mejor articulación entre las áreas operativas, técnicas y de gestión del Centro de Ciberdefensa.

El equipo de trabajo estuvo conformado por personal militar con experiencia en ciberseguridad y Ciberdefensa, sistemas de información, planeamiento y gestión organizacional, quienes contribuyeron de manera coordinada al análisis de la estructura existente y a la formulación de la propuesta del COEq. La conformación del equipo permitió que el diseño del COEQ sea la más óptima, ya que la persona que trabajo en el proyecto facilitó criterios técnicos, operativos y normativos durante el desarrollo de la experiencia profesional.

3.2 Objetivos y alcance

- **Objetivo general**

  Optimizar la gestión operativa y la capacidad de ciberdefensa del Centro de Ciberdefensa del Ejército del Perú mediante el diseño y adecuación del Cuadro de Organización y Equipo.

- **Objetivos específicos:**

  a. Analizar la estructura orgánica y funcional actual del Centro de Ciberdefensa, identificando brechas en roles, funciones y capacidades cibernéticas.
  b. Determinar los requerimientos de personal, equipamiento y especialización técnica necesarios para el cumplimiento eficiente de las funciones de ciberdefensa.
  c. Diseñar un Cuadro de Organización y Equipo alineado con la normativa vigente y con los estándares nacionales e internacionales de ciberdefensa.
  d. Proponer lineamientos para la implementación progresiva del Cuadro de Organización y Equipo que permitan mejorar la respuesta ante incidentes cibernéticos y la resiliencia institucional.

- **Alcance**

  Comprende la identificación de brechas organizacionales y funcionales relacionadas con la ciberdefensa, la definición de perfiles de puestos y roles especializados, así como la propuesta de una estructura organizacional alineada con la normativa vigente, los lineamientos estratégicos institucionales y los estándares reconocidos de ciberdefensa. El trabajo no contempla la ejecución presupuestal, la adquisición de equipamiento tecnológico ni la implementación integral del Cuadro de Organización y Equipo propuesto, limitándose a la formulación técnica y conceptual del diseño organizacional como insumo para la toma de decisiones institucionales.

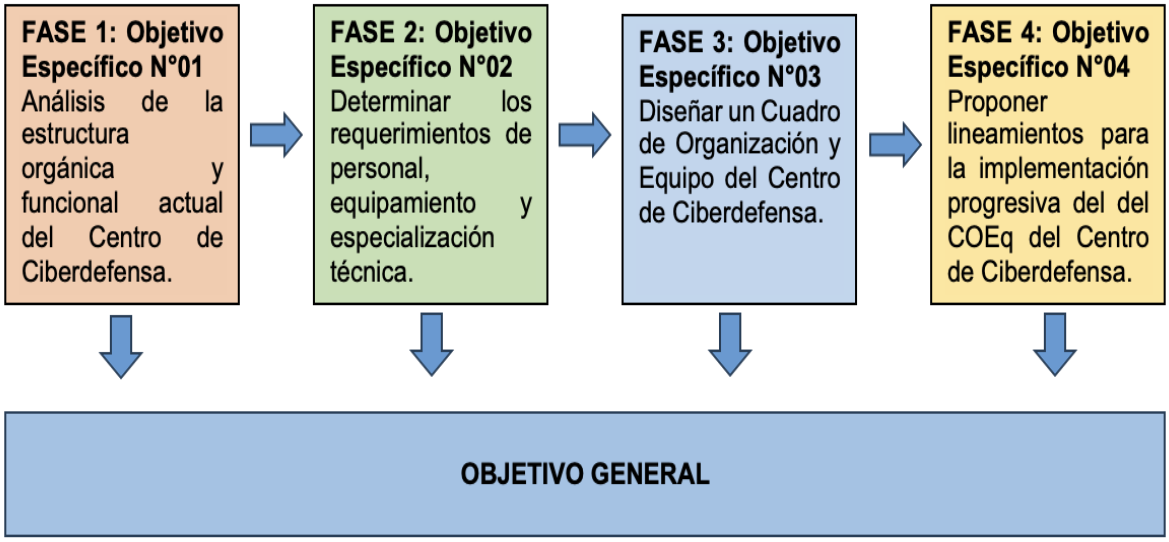
3.3 Estrategia desarrollada

La estrategia aplicada para el desarrollo de la presente experiencia profesional fue seguir 4 fases secuenciales que se alinea con los objetivos propuestos, Primero el análisis de la estructura orgánica y funcional actual del Centro de Ciberdefensa, Segundo en determinar los requerimientos de personal, equipamiento y especialización técnica necesarios para el cumplimiento eficiente de las funciones de ciberdefensa, Tercero el diseñar un Cuadro de Organización y Equipo alineado con la normativa vigente y con los estándares nacionales e internacionales de

ciberdefensa y el Cuarto proponer lineamientos para la implementación progresiva del Cuadro de Organización y Equipo que permitan mejorar la respuesta ante incidentes cibernéticos y la resiliencia institucional (Ver Figura 11).

Figura 11

Fases de los Objetivos Propuestos



3.3.1 FASE 1: Análisis de la estructura orgánica y funcional actual del Centro de Ciberdefensa

a. Revisión documental y normativa

Se realizó el análisis de la normativa legal, doctrinaria y técnica aplicable al centro de ciberdefensa, incluyendo leyes, decretos supremos, directivas institucionales, con el fin de establecer los lineamientos obligatorios para el diseño del COEq (Ver Tabla 1).

Tabla 1

Documentos doctrinarios y normativos aplicados al Centro de Ciberdefensa

001	DOCUMENTOS	DESCRIPCIÓN
D1	DFA-CD-03-28-CCFFAA, 2018 (Doctrina de operaciones del ciberespacio).	Establece los fundamentos teóricos doctrinarios de las Operaciones en el Ciberespacio (CO) en el nivel Estratégico Operacional para las operaciones y acciones militares.

D2	ME-11-225,2018 (Conocimientos básicos de las Operaciones Cibernéticas).	Establece los conocimiento básicos de las Operaciones Cibernéticas, a través de la Jefatura de Doctrina del Ejército – COEDE.
D3	Ley de Gobierno Digital N° 1412.	Tiene por objeto establecer el marco de gobernanza del gobierno digital.
D4	Ley N° 30999, Ley de Ciberdefensa publicada 09 de agosto del 2019.	Regula las operaciones militares en y mediante el ciberespacio, y define la Ciberdefensa.
D5	Con el Decreto Supremo N°005-2021-DE aprueba la "Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030"	Con el objetivo de garantizar la seguridad y defensa del país a través de un enfoque integral y coordinado entre diversas entidades del Estado
D6	El Plan de Transformación Institucional al 2034	Contemplan la capacidad de Ciberdefensa, para el cumplimiento del objetivo N° 5 (Desarrollar la Ciberdefensa Institucional) y en el mapa de procesos respectivo.
D7	Decreto Supremo N° 017-2024-PCM del 13 de febrero 2024	Aprueba el reglamento de la Ley de Ciberdefensa, se establece el marco normativo para regular las operaciones militares de ciberdefensa en el ciberespacio, con el propósito de preservar la Seguridad Nacional.
D8	Decreto Legislativo N° 1640 que modificó el Decreto Legislativo Nº 1137, Ley del Ejército del Perú del 04 Set 2024,	Se amplió la competencia institucional en el aspecto de Ciberdefensa; asimismo, dentro de la estructura orgánica, se creó al Comando de Operaciones Cibernéticas como un Órgano de Línea
D9	DS N° 005-2025-DE que adecua al reglamento del DL Nº 1137, Ley del Ejército del Perú del 05 Julio 2025.	En el Artículo 66-B Unidades Orgánicas del Comando de Operaciones Cibernéticas.
D10	Directiva N° 001 2024/DIPLANE/H-3 sobre reestructuración y aprobación de cuadros de organización y equipo.	Establece que la Dirección de Planeamiento del Ejército (DIPLANE) fija los lineamientos para la formulación, reestructuración y aprobación de los cuadros de organización y equipo (COEq).
D11	La guía de ciberdefensa de la junta interamericana de defensa JID edición 2020	ha lanzado el Programa de Ciberdefensa, el cual apoya a los 29 países miembros con actividades y ejercicios enfocados a la generación y desarrollo de capacidades individuales y colectivas de ciberdefensa.

b. Diagnóstico organizacional y funcional

Se evaluó la estructura orgánica existente del Centro de Ciberdefensa, identificando funciones, procesos, roles y niveles de responsabilidad, así como brechas entre la organización actual y las capacidades requeridas para una gestión eficaz de la ciberdefensa, se realizó un diagnóstico de cómo estaba organizado por departamentos y secciones y cuál era su función como Centro de Ciberdefensa hasta el AF-2025 (Ver Figura 12).

Figura 12

Organigrama del Centro de Ciberdefensa y su función General del AF-2025

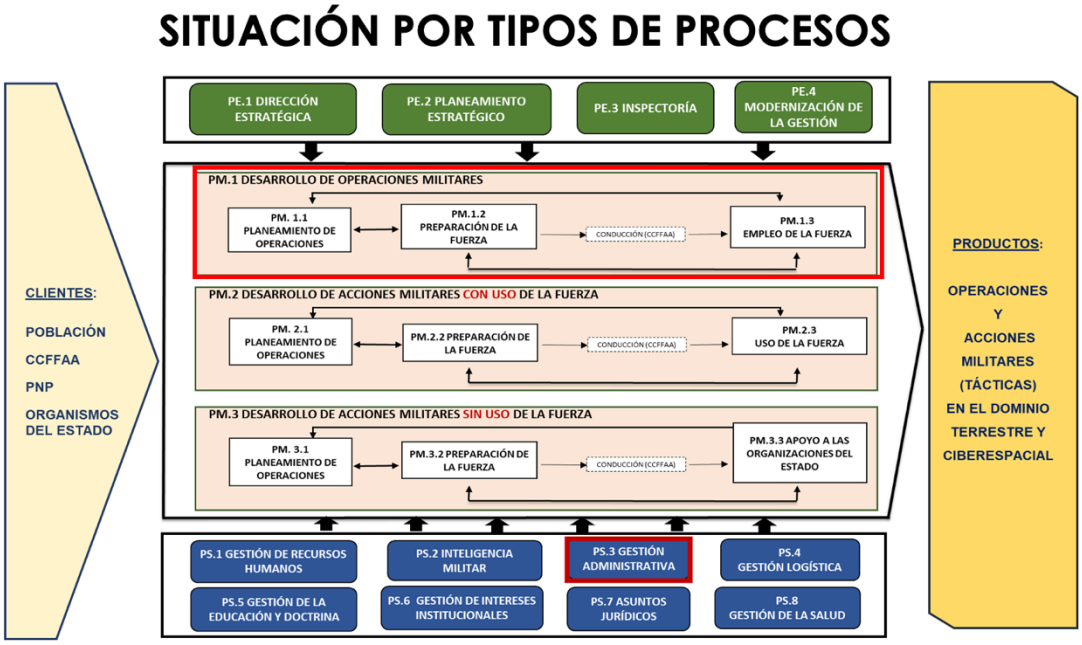
Nota. La figura se muestra el organigrama del Centro de Ciberdefensa del AF-2025 que esta subdividido por departamentos y secciones. Adaptado de la Directiva N°003 H-1.a.3/06.00 del Funcionamiento experimental de Ciberdefensa y Telemática del Ejército – CITELE (2019).

c. Identificación de procesos de Ciberdefensa

Se identificaron los procesos institucionales del Ejército del Perú en relación al ciberespacio y las capacidades de ciberdefensa como la defensa, explotación, respuesta y análisis forense ante incidentes cibernéticos, determinando que el Proceso Misional N°01 del Centro de Ciberdefensa es el desarrollo de operaciones militares en el ciberespacio propio y asignado (Ver Figura 13).

Figura 13

Procesos institucionales del Ejército del Perú



d. Detección y diagnóstico

La detección y el diagnóstico se realizaron mediante un proceso sistemático de análisis organizacional y funcional, orientado a identificar la situación real del Centro de Ciberdefensa en relación con su estructura, capacidades operativas y gestión cibernética.

En un principio, se realizó con la revisión de la estructura orgánica existente, documentos internos de la unidad, funciones asignadas y procedimientos operativos vigentes, lo que permitió identificar diversas funciones y una distribución óptima del personal y equipamiento tecnológico.

Posteriormente, se desarrolló un análisis comparativo entre la estructura actual y las necesidades operativas de ciberdefensa que permitió evidenciar la necesidad del personal y equipos tecnológicos adecuados para el cumplimiento de la misión.

Asimismo, se evaluó las funciones asignadas y la necesidad del personal, también se identificó la constante rotación de personal no beneficia a la operatividad del Centro de Ciberdefensa.

e. Capacitación y concientización

La capacitación y concientización del personal es fundamental dentro del proceso de implementación y fortalecimiento del Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa**,** debido a que la eficacia de las capacidades del Centro de Ciberdefensa no depende únicamente de la estructura organizacional o del equipamiento tecnológico, sino principalmente del factor humano**.**

En el contexto del Centro de Ciberdefensa, la capacitación siendo un factor muy importante se debe orientar a los conocimientos, habilidades y competencias del personal con los roles y funciones establecidos en el COEq. Por tal razón, se priorizó la formación en temas de ciberdefensa, ciberseguridad, gestión de incidentes cibernéticos, análisis de amenazas, normatividad vigente y uso adecuado de herramientas tecnológicas**,** de acuerdo con el nivel de responsabilidad y especialización de cada cargo.

La capacitación debe ser un proceso continuo y progresivo**,** considerando una dinámica y práctica continua. En ese sentido, se debe promover la actualización permanente de capacitación al personal mediante entrenamientos, talleres técnicos, simulaciones de incidentes cibernéticos y participación en programas de formación especializados.

3.3.2 FASE 2: *Determinación de los requerimientos de personal, equipamiento y especialización técnica necesarios para el cumplimiento eficiente de las funciones de ciberdefensa.*

a. Requerimiento de personal, perfil y especialidades

Se realizó un diagnóstico situacional de personal, cargos y especialidades, considerando competencias en ciberseguridad y ciberdefensa, gestión de incidentes, análisis de amenazas y soporte tecnológico del Centro de Ciberdefensa. La situación del CECIBER en cuanto a personal en el AF-2025, tenía un efectivo de cuatro (04) Oficiales y un efectivo de once (11) Técnicos y Suboficiales, descuentos cero (00) y un disponible de quince (15) (Ver Tabla 2 y Tabla 3).

Tabla 2

Efectivos del CECIBER

CECIBER	EFECTIVO	DESCUENTOS	DISPONIBLES
OFICIALES	04	00	04
TÉCNICOS Y SUBOFICIALES	11	00	11
TOTAL	**15**	**00**	**15**

Tabla 3

Oficiales, Técnicos y Suboficiales por armas/servicios y especialidad del CECIBER

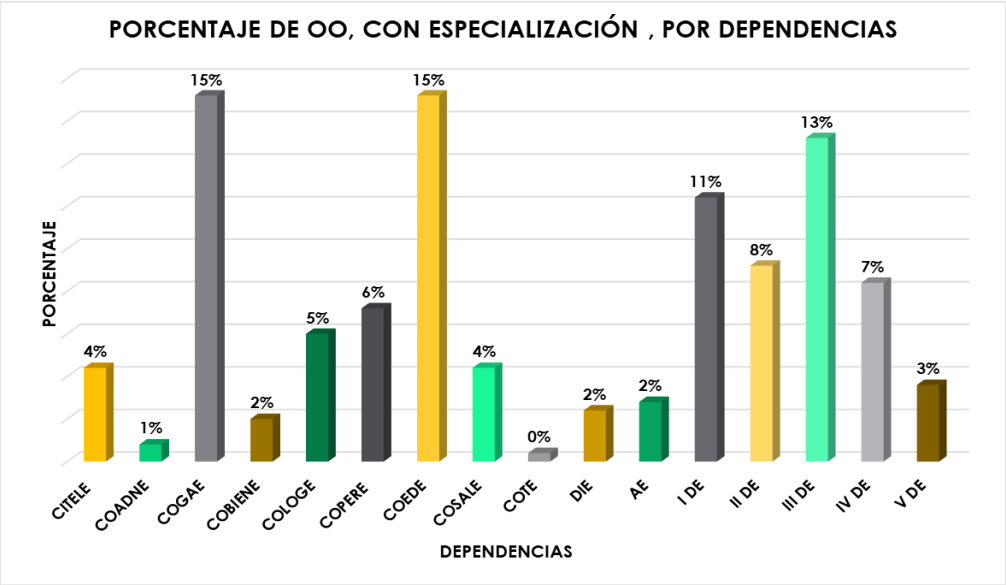
CECIBER	ARMA/SERVICIO	
OFICIALES	COM	SCYTE
	02	02

CECIBER	ESPECIALIDAD				
TCOS Y SSOO	T/COM	T/MCE	T/COMP INFO	T/ADM	T/INTG
	04	01	03	01	02

Se realizó una estadística del personal de oficiales que tiene alguna capacitación en tecnología de la información, ciberseguridad y ciberdefensa vienen laborando en diversas dependencias del Ejército del Perú (Ver Figura 14).

Figura 14

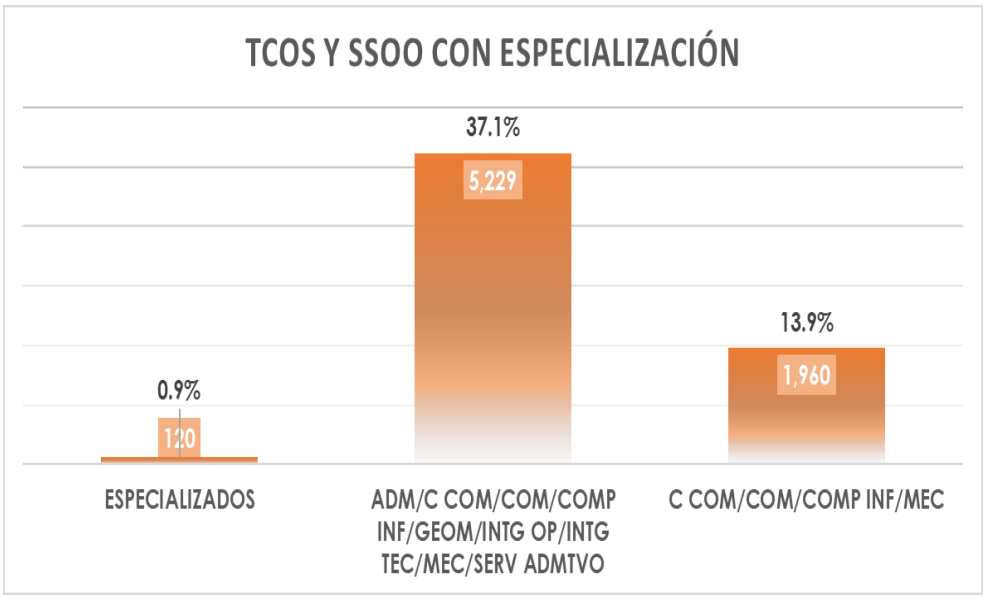
Porcentaje de Oficiales con especialización en las dependencias



Se realizó una estadística del personal de técnicos y suboficiales, de un total de 14,088, solo 120 han recibido capacitación en tecnologías de la información, ciberseguridad y ciberdefensa, lo que representa el 0.9% del total (Ver Figura 15).

Figura 15

Porcentaje de Técnicos y Suboficiales con especialización



b. Requerimiento de equipamiento

En cuanto a equipamiento de hardware, el Centro de Ciberdefensa (CECIBER) dispone de equipos de cómputo limitados, servidores de tecnología desactualizada y limitada, instalados en un ambiente sin sistema de refrigeración, cableado estructurado limitado. En cuanto a las herramientas informáticas, el CECIBER no dispone de herramientas licenciadas. Las herramientas que se vienen empleado son Open Source. En cuanto al suministro de internet, el CECIBER no cuenta con un servicio dedicado, el servicio de internet es proporcionado por el CINFE (Ver Tabla 4).

Tabla 4

Equipamiento tecnológico del Centro de Ciberdefensa

COMPONENTE	SITUACIÓN
HARDWARE	Se dispone de lo siguiente: • 12 computadoras clientes • 02 servidores • 01 laptop
SOFTWARE	• No se cuenta con personal para el desarrollo del software necesario. • Se emplea software libre (Ubuntu server, Wazuh, Snort, Suricata, Kali Linux, Metaexploit, etc.) • También se usan periodos de prueba de softwares con licencia privada.
INFRAESTRUCTURA	No se cuenta con un ambiente adecuado para realizar operaciones cibernéticas.
INTERNET	El Centro de Ciberdefensa no cuenta con una red independiente para realizar operaciones cibernéticas que le permitan cumplir con sus funciones asignadas.

3.3.3 FASE 3: Diseñar un Cuadro de Organización y Equipo del Centro de Ciberdefensa.

a. Planificación del diseño del Cuadro de Organización y Equipo

La planificación se realizó de manera estructurada, progresiva y alineada al marco normativo vigente**,** con el propósito de garantizar que el Diseño del Cuadro de Organización y Equipo del Centro de Ciberdefensa respondiera a las necesidades operativas, cibernéticas y estratégicas de la institución.

En primer lugar, se establecieron los objetivos del trabajo, definiéndose el alcance del diseño del COEQ en función a la misión del Centro de Ciberdefensa, las capacidades actuales y los lineamientos institucionales del Ejército del Perú.

Posteriormente, se elaboró un plan de trabajo, en el cual se definieron actividades, responsables y plazos, considerando las limitaciones de tiempo, disponibilidad de personal especializado y recursos existentes que permitió recopilar información de la unidad, análisis de la estructura orgánica, evaluación de funciones y conllevar a la formulación del proyecto del COEq.

Asimismo, la planificación contempló la articulación con el marco legal y doctrinario**,** asegurando la coherencia del diseño con los objetivos estratégicos y la normativa aplicable.

Finalmente, se establecieron criterios técnicos y operativos, tales como la especialización del personal, la jerarquización de funciones, la asignación eficiente de recursos y la sostenibilidad de la estructura propuesta. De esta manera, la planificación constituyó la base para un diseño ordenado, viable y orientado al fortalecimiento de las capacidades de ciberdefensa del Ejército del Perú.

b. Ejecución del diseño de un Cuadro de Organización y Equipo

El diseño de un Cuadro de Organización y Equipo (COEq) se ejecutó de acuerdo a la Directiva N° 001 2024/DIPLANE/H-3, sobre reestructuración y aprobación de cuadros de organización y equipo de las unidades y pequeñas unidades a implementar según el PEMFza 2034, en el cual indica que el COEq es un documento de Clasificación “SECRETO”, es por ello que se redactará de manera general del cómo se realizó el diseño del Coeq del Centro de Ciberdefensa. El Cuadro de organización y Equipo tiene la siguiente estructura:

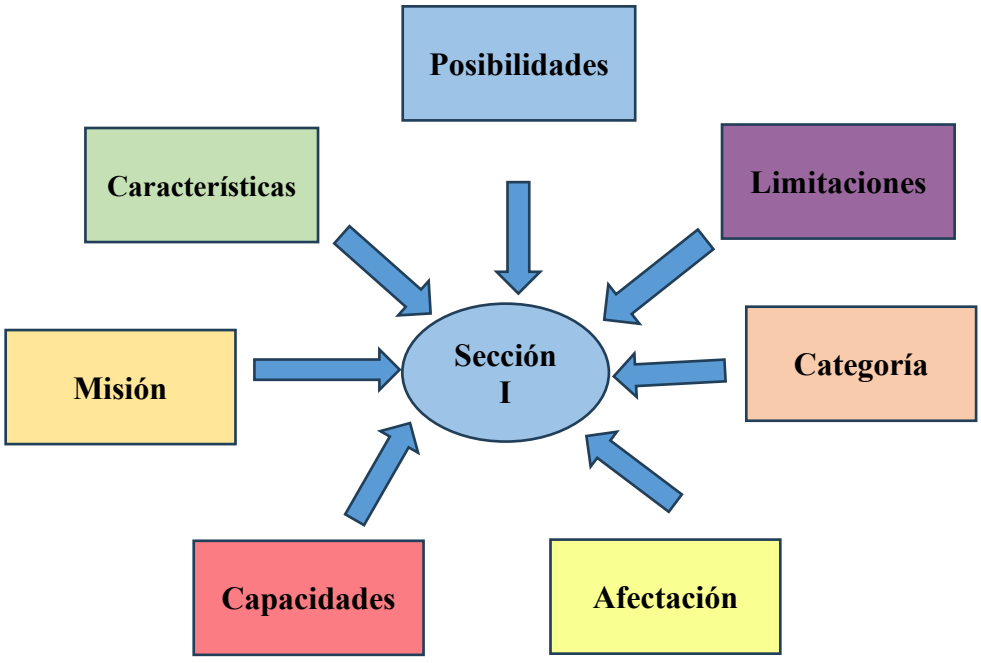
- **Sección I:** Generalidades
- **Sección II:** Personal
- **Sección III:** Equipo
- **Sección IV:** Personal y equipo por capacidades.

1. Sección I: Generalidades

Se inició con el desarrollo de las generalidades del Centro de Ciberdefensa, donde se estableció la denominación de la unidad, su organización y ámbito de acción dentro de la estructura del Ejército del Perú. Esta sección permitió definir el marco institucional y operativo en el cual sustenta al Centro de Ciberdefensa, teniendo una estructura como la misión que consiste en indicar de forma clara y concisa la misión que debe cumplir, en el marco de la unidad que pertenece, características que consiste en especificar aquellas particularidades de distinguen y diferencian a la unidad de otras unidades, posibilidades consiste en indicar las posibilidades de la unidad para cumplir la misión, limitaciones consiste en indicar los impedimentos o dificultades de la unidad, capacidades consiste en establecer la participación en las operaciones y acciones militares de acuerdo a los factores de las capacidades operacionales, afectación consiste en detallar las unidades que integran cada unidad y la categoría consiste en que las unidades se encuentran clasificada en categorías, desde el punto de vista del enfrentamiento con el enemigo (Ver Figura 16).

Figura 16

Estructura de la Sección I



2. Sección II: Personal

En esta sección se detalla el efectivo de personal requerido por las unidades para el cumplimiento de su misión y está constituido de las Sub Secciones siguientes:

- Distribución de personal según esquema de organización
- Resúmenes de efectivos totales del personal
- Observaciones referentes a las armas individuales, funciones adicionales, etc

Asimismo, se desarrolló esta sección considerando criterios de especialización, jerarquía, cantidad de efectivos y funciones, teniendo en cuenta las capacidades cibernéticas actuales y proyectadas, priorizando la asignación de especialistas en ciberdefensa, seguridad de la información, análisis de amenazas, respuesta a incidentes y gestión de redes, para el cumplimiento de la misión del Centro de Ciberdefensa.

3. Sección III: Equipo

En esta sección se prescribe el equipamiento autorizado para las Unidades organizada de la Fuerza Operativa, de conformidad con la distribución de personal autorizado, consta de las Sub Secciones siguientes:

- Distribución del equipo autorizado, por cada unidad orgánica de la organización.
- Resumen de los totales de equipo por servicios logísticos
- Observaciones, incluyendo notas explicativas necesarias, que aclaran el contenido de la sección III, tales como distribución de equipo para personal específico, identificación de artículos, etc.

Asimismo, se evaluó la disponibilidad actual de equipos y se determinó el requerimiento adicional necesario para fortalecer las capacidades operativas, se identificaron los medios tecnológicos, herramientas y recursos materiales indispensables para el funcionamiento del Centro de Ciberdefensa.

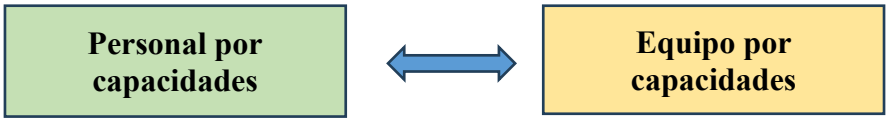
4. Sección IV: Personal y equipo por capacidades

Esta sección muestra en resumen la organización de las unidades de la Fuerza Operativa, agrupadas tanto de personal y equipo, teniendo en consideración las capacidades fundamentales y operaciones a las cuales responden, consta de Sub secciones.

Asimismo, para cada capacidad se asignó el personal especializado correspondiente, así como el equipamiento técnico necesario para su ejecución eficiente. Esto permitió asegurar que cada capacidad contara con los recursos humanos y materiales adecuados, evitando duplicidad de funciones y fortaleciendo la articulación operativa (Ver Figura 17).

Figura 17

Subsecciones de la Sección IV



c. Validación técnica

La propuesta del COEq fue validada con personal especialista, con el propósito de verificar su funcionalidad, pertinencia y aplicabilidad dentro del contexto operativo del Centro de Ciberdefensa. Asimismo, la propuesta fue sometida a revisión por parte de las dependencias competentes, tales como COPERE, COLOGE, DIGEDOCE, entre otras áreas directamente vinculadas con su implementación, las cuales evaluaron sus alcances operativos, logísticos y administrativos. Como resultado de este proceso de validación, las dependencias competentes otorgaron la viabilidad para la implementación del COEq**,** al considerar que la propuesta es factible y coherente con las capacidades y necesidades del de Centro de Ciberdefensa.

d. Pruebas, verificación y control

1. Pruebas

Durante el proceso de diseño del Cuadro de Organización y Equipo, las pruebas se orientaron a comprobar la funcionalidad operativa de la estructura propuesta.

Por tal motivo, se realizaron diversos estudios técnicos, en los cuales se evaluó si los cargos, funciones y niveles jerárquicos en el Centro de Ciberdefensa permiten una funcionalidad necesaria. Estas pruebas permitieron verificar la correcta asignación de personal y equipamiento tecnológico necesario para implementar las del Centro de Ciberdefensa.

2. Verificación

Consistió en validar que el diseño del COEq cumpliera con los requisitos normativos, doctrinarios y técnicos establecidos. Así mismo, se pudo comprobar la estructura propuesta con la normativa vigente, orientándose a la Ley de Ciberdefensa, la Ley del Ejército del Perú, el Plan de Transformación Institucional, directivas internas sobre cuadros de organización y equipo y otros manuales doctrinarios que fueron necesarios para la realización del COEq.

Además, se verificó el correcto misionamiento del Centro de Ciberdefensa, las funciones asignadas y los recursos humanos y equipos contemplados en el COEq. Este proceso permitió asegurar que el diseño no solo fuera técnicamente viable, sino también legalmente válido y alineado con los objetivos estratégicos institucionales.

3. Control

Se orientó a garantizar la sostenibilidad y mejora continua del COEq una vez diseñado. Por tal motivo, se establecieron mecanismos de seguimiento y evaluación, que permitieron supervisar el desempeño de la unidad, que permitieron detectar algunas limitaciones que carecía la unidad.

Asimismo, facilitó la identificación de oportunidades de mejora y la necesidad de reforzar determinadas funciones, ajustar perfiles de personal o actualizar el equipamiento, considerando la evolución constante de las amenazas en el ciberespacio. De esta manera, el control permitirá que el COEq se mantenga actualizado y acorde a las necesidades operativas del Centro de Ciberdefensa.

3.3.4 FASE 4: Proponer lineamientos para la implementación progresiva del Cuadro de Organización y Equipo

a. Consideraciones éticas y de seguridad

En el desarrollo del diseño del Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa, se incorporaron consideraciones éticas y de seguridad orientadas a garantizar un desempeño profesional, responsable y transparente. Protegiendo la información, aplicando los principios de confidencialidad, integridad y disponibilidad de sistemas y datos como base de toda la operación del centro siempre respetando los derechos y marcos legales.

b. Confidencialidad de la información

La confidencialidad implica los esfuerzos de una organización para garantizar que los datos se mantengan en secreto o privados. Para lograr esto, el acceso a la información debe controlarse para evitar el intercambio no autorizado de datos, ya sea intencional o accidental y asegurar la integridad de la información. Un componente clave para mantener la confidencialidad es asegurarse de que las personas sin la autorización adecuada no tengan acceso a activos importantes.

Constituye un aspecto fundamental en el proceso de elaboración del COEq**,** ya que la información utilizada para su formulación fue utilizada bajo criterios de seguridad y reserva institucional, garantizando que su acceso se limite únicamente al personal autorizado y especializado.

c. Respecto al marco legal y normativo

La elaboración del COEq se desarrolló con conocimiento del marco legal y normativo vigente que regula las actividades vinculadas a la seguridad, defensa y gestión de la información en el ámbito institucional. En este sentido, su formulación consideró las disposiciones establecidas en las normas, directivas y lineamientos aplicables al funcionamiento del Centro de Ciberdefensa y lo más importante de la normativa que se tomó en cuenta es el marco normativo que regula las operaciones militares en y mediante el ciberespacio.

d. Separación de funciones y control interno

La separación de funciones no solo refuerza la postura de seguridad de una organización, sino que también permite una mayor especialización y un enfoque más preciso en cada dominio. Un fenómeno similar se observa actualmente con la inteligencia artificial, donde algunas empresas comienzan a identificar la necesidad de establecer departamentos especializados, aunque estrechamente interconectados con otras áreas de la organización.

En La elaboración del COEq se desarrolló considerando el principio de separación de funciones y control interno, con el propósito de garantizar la transparencia, objetividad y confiabilidad durante su formulación.

Asimismo, se aplicaron mecanismos de control interno que permitieron supervisar el proceso de elaboración, verificar la coherencia de la información y asegurar que la propuesta cumpla con los procedimientos y lineamientos institucionales. De esta manera, se fortalece la integridad del proceso y se contribuye a una adecuada implementación del COEq dentro del Centro de Ciberdefensa.

e. Utilizar una metodología para la mejora de implementación progresiva.

Una metodología sería La Design Science Research (DSR) o Investigación en Ciencias del Diseño se puede utilizar para diseñar, desarrollar y validar una propuesta organizacional, como el Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa, a través de un proceso sistemático orientado a resolver un problema práctico.

La DSR se utiliza principalmente en disciplinas aplicadas como la ingeniería, la tecnología de la información, la educación y la gestión. Sus objetivos principales son:

- **Resolver problemas prácticos:** Crear soluciones que no existían o mejorar significativamente las actuales.
- **Generar conocimiento prescriptivo:** No solo soluciona un problema puntual, sino que establece guías o principios de diseño que otros pueden seguir para problemas similares.

- **Innovación:** Fomenta la creación de "artefactos sintéticos" (objetos creados por el hombre) que expanden los límites de las capacidades humanas o de las organizaciones.

f. Evaluación y mejora continua

La implementación del Cuadro de Organización y Equipo (COEq) debe estar permanente en una evaluación, orientado a verificar el cumplimiento de las funciones asignadas y el adecuado funcionamiento de la estructura organizacional del Centro de Ciberdefensa. Estas evaluaciones permitirán analizar el desempeño de las áreas establecidas, así como la eficiencia en la coordinación y desarrollo de las actividades relacionadas con la ciberdefensa.

Asimismo, los resultados obtenidos de dichas evaluaciones facilitarán la identificación de oportunidades de mejora, permitiendo realizar los ajustes necesarios en la organización, en la asignación de funciones y en la distribución de recursos. De esta manera, se promueve a la mejora continua que contribuya al fortalecimiento progresivo de las capacidades operativas y organizacionales del Centro de Ciberdefensa.

Finalmente, este proceso de evaluación continua permitirá adaptar la estructura del COEq a las nuevas necesidades institucionales, a los avances tecnológicos y a la evolución de las amenazas en el ciberespacio, garantizando que el Centro de Ciberdefensa mantenga un nivel adecuado de eficiencia, capacidad de respuesta y actualización permanente.

CAPÍTULO IV. RESULTADOS

4.1 Presentación de resultados alcanzados

4.1.1 Resultado de la Fase 1: Análisis de la estructura orgánica y funcional actual del Centro de Ciberdefensa

Como resultado del análisis de la estructura orgánica y funcional actual del Centro de Ciberdefensa, realizado mediante la revisión normativa, el diagnóstico organizacional y la identificación de procesos institucionales, se elaboró un Informe de Estudio de Estado Mayor (IEM) y una Hoja de Recomendación, documentos que permitieron sustentar técnicamente la necesidad de optimizar un diseño de Cuadro de Organización y Equipo del Centro de Ciberdefensa.

El Informe de Estudio de Estado Mayor permitió analizar la situación actual del Centro de Ciberdefensa, evaluando su estructura organizacional, la distribución de funciones, los procesos operativos y las capacidades existentes para el desarrollo de operaciones militares en el ciberespacio. A través de este análisis se identificaron diversas brechas organizacionales y funcionales, la ausencia de roles técnicos claramente definidos, limitaciones en la especialización del personal y una distribución no óptima de los recursos humanos y tecnológicos.

Asimismo, el estudio permitió evidenciar que, si bien el Centro de Ciberdefensa contaba con capacidades para realizar operaciones de defensa, explotación y respuesta en el ciberespacio, la estructura organizacional existente hasta el Año Fiscal 2025 no se encontraba plenamente alineada con las nuevas exigencias normativas, doctrinarias y operativas derivadas de la Ley de Ciberdefensa, su reglamento y la creación del Comando de Operaciones Cibernéticas**.**

Por lo tanto, se definió la organización del Centro de Ciberdefensa de acuerdo a los lineamientos de la Ley de Ciberdefensa N°30999 y a la organización aprobada del Comando de Operaciones Cibernéticas de acuerdo al Decreto Supremo N° 005 - 2025 - DE que adecua al reglamento del Decreto Legislativo Nº 1137 en la que se menciona la unidad de Ciberdefensa dentro de su organización, partiendo de ese punto se propuso la organización que se ve contemplada en el Cuadro de Organización y Equipo del Centro de Ciberdefensa, en la que se puede determinar su estructura de acuerdo a las capacidades que cuenta la Ciberdefensa:

- Capacidad de Defensa que esta subdividida por: Defensa pasiva, Defensa activa e Investigación Digital.
- Capacidad de Explotación que esta subdividida por: Explotación pasiva y Explotación activa.
- Capacidad de respuesta que esta subdividida por: Respuesta preventiva y Respuesta reactiva.

Finalmente, el Cuadro de Organización y Equipo (COEq) N° 11- 495 S, con fecha 01 de enero de 2026, de clasificación SECRETO, correspondiente al Centro de Ciberdefensa fue aprobada de acuerdo a la estructura orgánica del Comando de Operaciones Cibernéticas (Ver Figura 18 y 19).

Figura 18

Estructura Orgánica del Comando de Operaciones Cibernéticas

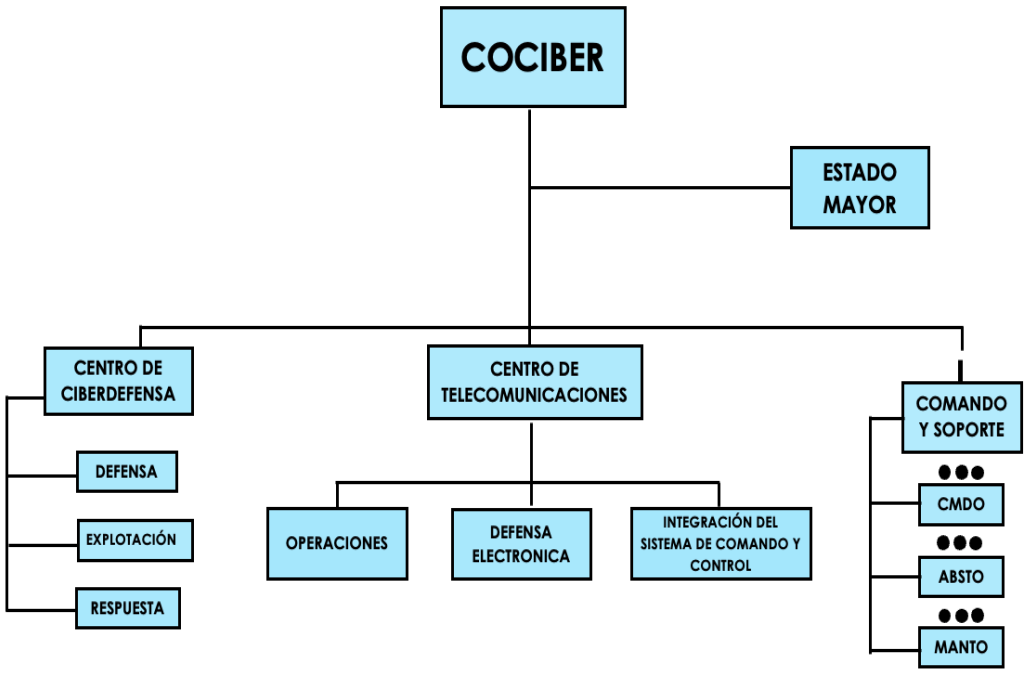
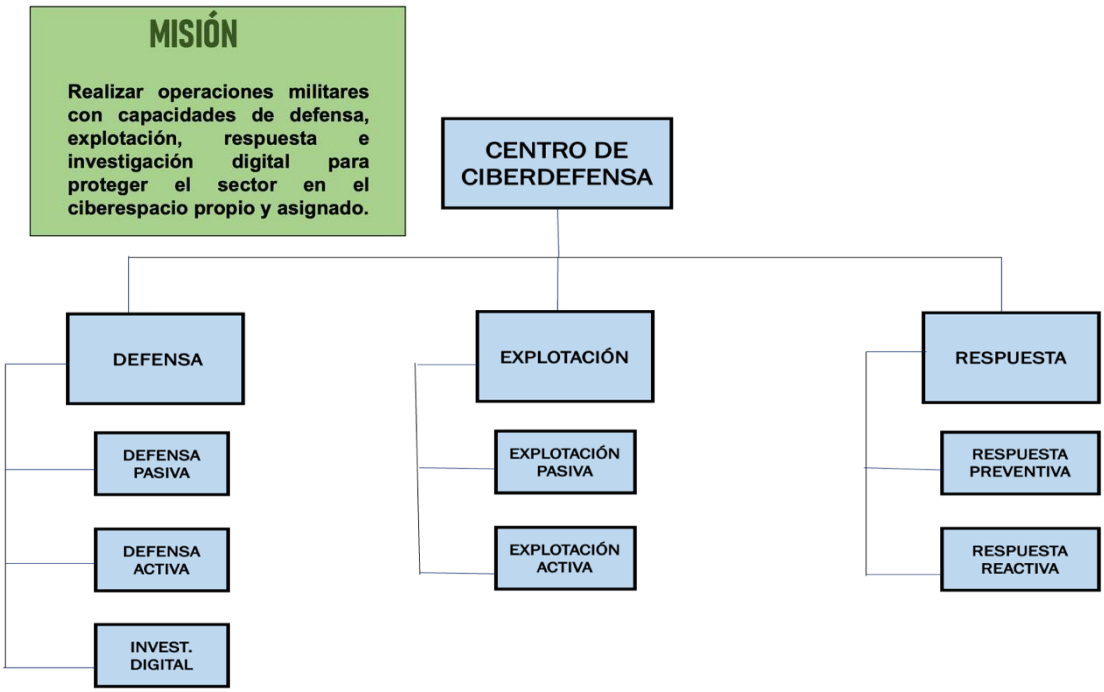


Figura 19

Organización y la misión del Centro de Ciberdefensa aprobado



Nota. Propuesta de acuerdo a la Ley de Ciberdefensa N°30999 y un informe de Estudio mayor del Centro de Ciberdefensa de acuerdo a la doctrina y normas legales antes mencionado en la Tabla 1.

4.1.2 Resultado de la Fase 2: *Determinación de los requerimientos de personal, equipamiento y especialización técnica necesarios para el cumplimiento eficiente de las funciones de ciberdefensa.*

Como resultado se determinaron los requerimientos de personal, equipamiento y especialización técnica necesarios para el adecuado funcionamiento del Centro de Ciberdefensa. Este análisis permitió establecer los perfiles profesionales requeridos, la cantidad de personal especializado y los recursos tecnológicos necesarios para fortalecer las capacidades de monitoreo, detección, análisis y respuesta ante incidentes en el ciberespacio. Estos resultados sirvieron como base para la formulación del Cuadro de Organización y Equipo (COEq), orientado a optimizar la estructura organizacional y mejorar la eficiencia operativa en el desarrollo de las funciones de ciberdefensa.

a. Resultados en la gestión del personal

En el ámbito del recurso humano, permitió identificar el perfil ideal del personal requerido, tanto especializado como de apoyo, considerando competencias técnicas en ciberseguridad, gestión de incidentes, análisis de amenazas y operaciones en el ciberespacio. Este resultado contribuyó a una gestión más eficiente del talento humano y a la mejora de la preparación operativa del Centro en lo que se pudo determinar la siguiente necesidad de personal de 35 Oficiales, 36 Técnicos y Suboficiales con un total de 71efectivos, Asimismo la necesidad por especialidades (Ver Tablas 5 y 6).

Tabla 5

Necesidad de personal para el Centro de Ciberdefensa

EFECT	OFICIALES					TCOS Y SSOO					
	CRL	TC	MY	CAP	TTE	TCO1	TCO2	TCO3	SO1	SO2	SO3
71	1	3	7	12	12	0	0	0	36	0	0
	35					36					

Tabla 6

Necesidad de personal por especialidades para el Centro de Ciberdefensa

Nº	GRADO	ARMA	PUESTO	CANTIDAD
1	CRL	COM	JEFE	01
CAPACIDAD DE EXPLOTACIÓN				
2	TTE CRL	COM	JEFE DE EXPLOTACIÓN	01
3	MY	SCYTE	JEFE EXPLOTACIÓN PASIVA	01
4	CAP	SCYTE	ESPECIALISTA DE CIBERINTELIGENCIA	02
5	TTE	SCYTE	ANALISTA PARA CIBERINTELIGENCIA	02
6	SO1	T/COMP INFO	OPERADOR PARA CIBERINTELIGENCIA	06
7	MY	SCYTE	JEFE EXPLOTACIÓN ACTIVA	01
8	CAP	SCYTE	ESPECIALISTA DE CIBERINTELIGENCIA	02
9	TTE	SCYTE	ANALISTA PARA CIBERINTELIGENCIA	02
10	SO1	T/COMP INFO	OPERADOR PARA CIBERINTELIGENCIA	06
CAPACIDAD DE DEFENSA				
11	TTE CRL	COM	JEFE DE DEFENSA	01
12	MY	SCYTE	JEFE DE DEFENSA PASIVA	01

13	CAP	SCYTE	ANALISTA DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
14	TTE	SCYTE	OPERADOR DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
15	SO1	T/COMP INFO	ASISTENTE DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	06
16	MY	SCYTE	JEFE DE DEFENSA ACTIVA	01
17	CAP	SCYTE	ANALISTA DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	01
18	TTE	SCYTE	OPERADOR DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	01
19	SO1	T/ COMP INFO	ASISTENTE DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	03
20	MY	SCYTE	JEFE DE INVESTIGACIÓN DIGITAL	01
21	CAP	SCYTE	ANALISTA DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	01
22	TTE	SCYTE	OPERADOR DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	01
23	SO1	T/ COMP INFO	ASISTENTE DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	03
CAPACIDAD DE RESPUESTA				
24	TTE CRL	COM	JEFE DE RESPUESTA	01
25	MY	SCYTE	JEFE DE RESPUESTA PREVENTIVA	01
26	CAP	SCYTE	ANALISTA DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
27	TTE	SCYTE	OPERADOR DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
28	SO1	SCYTE	ASISTENTE DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	06
29	MY	SCYTE	JEFE DE RESPUESTA REACTIVA	01
30	CAP	SCYTE	ANALISTA DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
31	TTE	SCYTE	OPERADOR DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	02
32	SO1	T/COMP INFO	ASISTENTE DE CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO	06
TOTAL				**71**

b. Resultados en la asignación de equipos y capacidades tecnológicas

Entre los equipos considerados se incluyeron sistemas de monitoreo y detección de intrusiones, plataformas de análisis de incidentes, infraestructura de redes seguras, servidores, estaciones de trabajo especializadas y herramientas de respaldo y continuidad operativa para el Centro de Ciberdefensa. La asignación del equipo se realizó bajo criterios de racionalidad, eficiencia y sostenibilidad, en concordancia con las consideraciones presupuestales existentes por lo que se pudo determinar la necesidad de equipamiento tecnológico más importante para el funcionamiento del Centro de Ciberdefensa (Ver Tabla 7).

Tabla 7

Necesidad de equipamiento tecnológico para el Centro de Ciberdefensa

N°	DESIGNACIÓN DEL ARTÍCULO	CANT
	SERVICIO DE COMUNICACIONES	
1	Cámaras de videovigilancia Diurno/Nocturno/Cámara de seguridad y vigilancia S/M	18
2	Computadora Core i7	71
3	Laptop (Notebook) 15.6 Intel Core i7	5
4	Pantalla Interactiva 86TR3DJ	4
5	Proyector multimedia 4000 lúmenes	4
6	Router (Eq. Est Remoto.Fija) – VSAT MP2800	8
7	Servidor Tipo Rack Poweredge R740	6
8	Servidor para plataforma virtual	2
9	Sistema de control asistencial computarizada con huella digital	7
10	Software S/M (paquete de oficina)	71
11	Software S/M (antivirus corporativo)	71
12	Software S/M (análisis de tráfico de red)	1
13	Software para Centro de operaciones de ciberseguridad -SOC	23
14	Switch 48 puertos DGS-1510-52X	8
15	Teléfono IP GXP-1100	1
16	Televisor Smart UHD 4K LED 55	1
17	Televisor LED 60 HD	12
18	Ups Smart SMT1500RMI2U-1.50 K	78

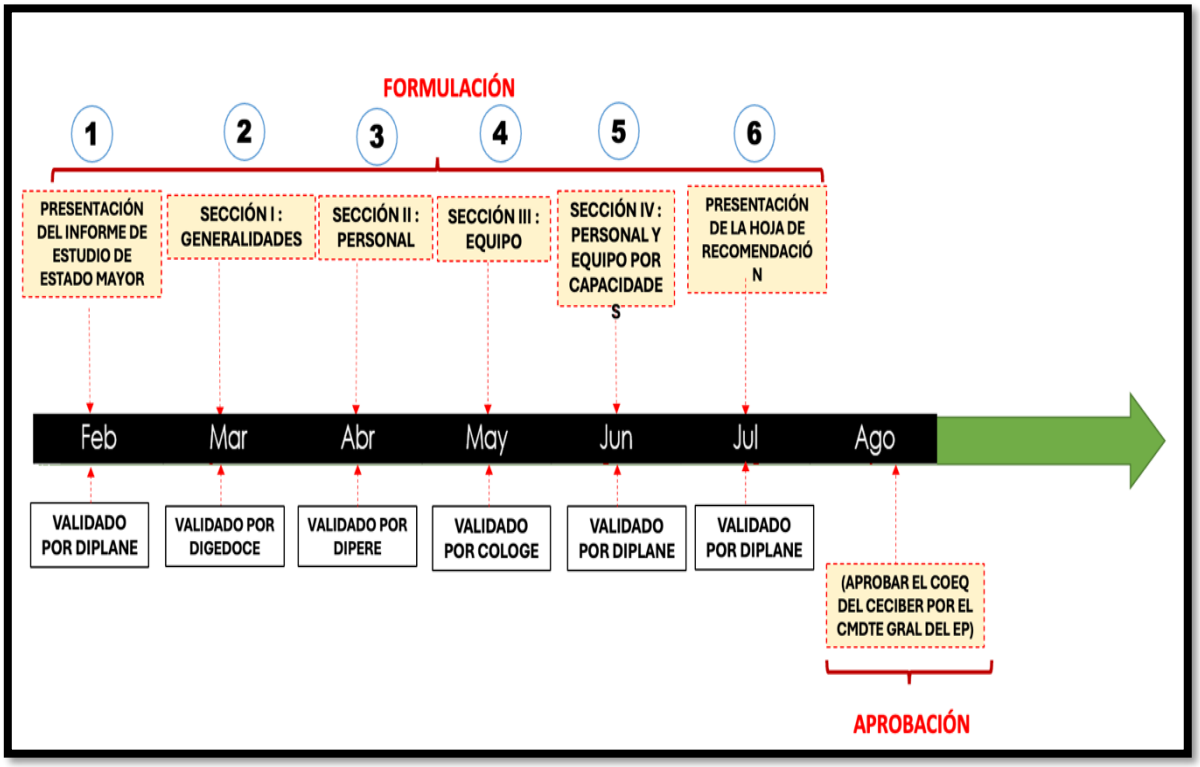
4.1.3 Resultado de la Fase 3: *Diseñar un Cuadro de Organización y Equipo del Centro de Ciberdefensa.*

El Cuadro de Organización y Equipo (COEq) del Centro de Ciberdefensa**,** el cual fue desarrollado siguiendo una línea de tiempo que comprendió las etapas de análisis, formulación, revisión técnica y validación institucional. Este documento establece la estructura organizacional, la distribución de cargos, los requerimientos de personal especializado y los medios tecnológicos necesarios para el cumplimiento eficiente de las funciones de ciberdefensa. El COEq fue presentado a las instancias correspondientes para su evaluación y, posteriormente, aprobado en el mes de diciembre. Debido a su carácter institucional y a la naturaleza sensible

de la información que contiene, el documento se mantiene con clasificación de SECRETO. En ese sentido, se adjunta el Anexo 1 con información genérica del COEq y el Anexo 2 con la Resolución de aprobación del COEq del Centro de Ciberdefensa (Ver Figura 20).

Figura 20

Línea de tiempo del COEq del Centro de Ciberdefensa



4.1.4 Resultado de la Fase 4: *Proponer lineamientos para la implementación progresiva del Cuadro de Organización y Equipo*

a. Lecciones aprendidas

- **El diseño organizacional es tan crítico como la tecnología**

Durante el desarrollo del Cuadro de organización y equipo (COEq) se evidenció que contar con herramientas avanzadas de ciberdefensa no garantiza una respuesta eficaz si la estructura organizacional no está claramente definida. La correcta asignación de funciones, jerarquías y responsabilidades permitió reducir duplicidades, vacíos operativos y errores en la toma de decisiones

durante incidentes. Esta lección demuestra que la ciberdefensa es, ante todo, una capacidad organizacional y no solo tecnológica.

- **La clara definición de roles fortalece la gestión de incidentes**

Se aprendió que la ambigüedad en los roles genera retrasos y conflictos durante la atención ante incidentes cibernéticos. Al establecer funciones específicas dentro del COEq (detección, análisis, respuesta, coordinación y supervisión), se mejorará la fluidez operativa y se reducirá el tiempo de respuesta. Esta experiencia confirmó que una estructura clara permite actuar con rapidez, control y responsabilidad.

- **La ética y la legalidad deben integrarse al trabajo técnico**

El acceso a información sensible y sistemas críticos exige que cada acción técnica esté respaldada por principios éticos y normas legales. Durante la experiencia, se comprendió que la ética y la legalidad deben integrarse de manera explícita al trabajo técnico y no verse como algo separado. La formación del personal de ciberdefensa debe incluir no solo herramientas y técnicas, sino también ética profesional y cumplimiento normativo, porque quien sabe vulnerar sistemas tiene una responsabilidad mayor al ejercer ese conocimiento.

- **La documentación y trazabilidad aseguran control y mejora continua**

La documentación permitió saber qué se hizo, cómo, cuándo y quién lo hizo, esto hizo posible auditar, detectar errores y demostrar cumplimiento; es decir sin una adecuada documentación, los errores se repiten y las buenas prácticas no se consolidan.

En cuanto a la trazabilidad permitió mantener una cadena de custodia de evidencias que registraron los procesos, decisiones y acciones técnicas que permitió evaluar el desempeño del COEq y corregir deficiencias detectadas.

- **La capacitación permanente sostiene la eficacia**

Se aprendió que el COEq no es un documento estático, sino una herramienta constante que requiere personal capacitado y consciente de sus responsabilidades. La actualización constante en procedimientos y normativas

fortaleció a la unidad. Esta lección confirma que el factor humano es decisivo en la ciberdefensa.

b. Indicadores de desempeño

A continuación, se presentan algunos indicadores clave obtenidos durante el periodo de ejecución como son el nivel de implementación del COEq, el grado de definición de roles y responsabilidades, la asignación de personal y equipo por capacidades y mejora de la gestión operativa y cibernética (Ver Tabla 8).

Tabla 8

Indicadores de desempeño

Indicador (%)	Meta establecida	Resultado alcanzado	Observación
Nivel de implementación del COEQ	100%	95 %	El COEQ fue diseñado casi en su totalidad; pendiente de validación presupuestal
Grado de definición de roles y responsabilidades	100 %	90 %	Roles clave definidos; ajustes en funciones altamente especializadas
Asignación de personal y equipos por capacidades	100 %	85 %	Limitaciones de personal especializado y equipamiento influyeron en el resultado
Mejora de la gestión operativa y cibernética	100 %	88 %	Optimización de procesos con necesidad de mejora continua

c. Propuesta de mejora futura

Si bien los objetivos planteados fueron alcanzados, se identificaron áreas de mejora:

- **Modernización organizacional (Eje de Gobernanza y Gestión):** Actualizar progresivamente el Cuadro de Organización y Equipo del Centro de Ciberdefensa, asegurando una estructura flexible, interoperable y orientada a capacidades, acorde con el proceso de transformación institucional.
- **Desarrollo del talento humano (Eje de Capital Humano):** Fortalecer la capacitación, especialización y certificación del personal en ciberdefensa, priorizando perfiles técnicos críticos y la profesionalización continua.

- **Innovación y tecnología (Eje de Transformación Digital):** Gestionar la incorporación gradual de tecnologías y herramientas especializadas para monitoreo, análisis y respuesta a incidentes, alineadas a estándares nacionales e internacionales.
- **Gestión por resultados y mejora continua (Eje de Eficiencia Operativa):** Implementar mecanismos permanentes de evaluación del COEQ mediante indicadores de desempeño y ejercicios operativos, garantizando la mejora sostenida de la capacidad de ciberdefensa.
- **Optimización del COEq mediante la integración de inteligencia artificial en la gestión operativa del Centro de Ciberdefensa:**

  La incorporación progresiva de herramientas de inteligencia artificial (IA) en el diseño y actualización del Cuadro de Organización y Equipo (COEQ), con el fin de optimizar la gestión operativa y cibernética del Centro de Ciberdefensa. La IA permitiría mejorar el análisis de datos organizacionales, identificar brechas de capacidades, prever necesidades de personal y recursos, así como apoyar la toma de decisiones basada en información en tiempo real. Asimismo, su implementación contribuiría a una distribución más eficiente del talento humano y a una planificación más precisa de los recursos tecnológicos y logísticos, fortaleciendo la flexibilidad, interoperabilidad y capacidad de respuesta institucional frente a amenazas cibernéticas emergentes. En ese sentido, **s**e adjunta el Anexo 3 un cuadro de optimización del coeq del centro de ciberdefensa mediante inteligencia artificial y tecnologías modernas.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. El análisis de la estructura orgánica y funcional del Centro de Ciberdefensa permitió sustentar técnicamente su reestructuración y como resultado se definió una organización basada en capacidades de defensa, explotación, respuesta e investigación digital, alineada a la normativa vigente y al Comando de Operaciones Cibernéticas, lo que permitió estructurar y formalizar el COEq del Centro de Ciberdefensa.

2. La determinación de los requerimientos de personal, equipamiento y especialización técnica permitió definir las capacidades necesarias para el funcionamiento eficiente del Centro de Ciberdefensa, estableciendo perfiles, cantidad de personal y recursos tecnológicos críticos. Asimismo, se evidenció la necesidad de fortalecer la especialización del talento humano y la dotación tecnológica, sirviendo como base fundamental para el diseño del COEq.

3. El diseño del COEq permitió consolidar una estructura organizacional definida, necesarios para la operatividad del Centro de Ciberdefensa. Su validación y aprobación institucional lo consolidan como un instrumento formal para la gestión y fortalecimiento de las capacidades de ciberdefensa, asegurando además su articulación con el Plan de Transformación Institucional al 2034 en el marco del Objetivo Estratégico OE 5 (Desarrollar la ciberdefensa en el Ejército).

4. Las propuestas de mejora planteadas orientan al COEq del Centro de Ciberdefensa hacia una estructura más flexible y eficiente. Asimismo, el fortalecimiento del talento humano, la incorporación de tecnologías emergentes, la gestión por resultados y el uso de inteligencia artificial permiten reducir las brechas identificadas durante su implementación. En ese sentido, la inteligencia artificial se consolida como un elemento estratégico que contribuye a una transformación institucional sostenible y alineada con las exigencias del entorno cibernético actual.

5.2 Recomendaciones

1. Mantener actualizada y alineada la estructura orgánica y funcional del Centro de Ciberdefensa, considerando la normativa vigente, la evolución del entorno cibernético y las necesidades operativas del Comando de Operaciones Cibernéticas, con el fin de asegurar una organización eficiente y coherente con sus capacidades.
2. Promover de manera progresiva la incorporación de personal especializado en ciberdefensa, así como la asignación de recursos presupuestales para la adquisición de equipamiento y herramientas tecnológicas especializadas, priorizando las capacidades de monitoreo, análisis y respuesta ante incidentes cibernéticos, con el fin de fortalecer el desempeño operativo del Centro de Ciberdefensa.
3. Asegurar que el Cuadro de Organización y Equipo del Centro de Ciberdefensa se mantenga articulado al Plan de Transformación Institucional al 2034 y al Objetivo Estratégico OE 5 (Desarrollar la ciberdefensa en el Ejército), promoviendo su actualización sistemática y su alineamiento con la gestión por capacidades, a fin de fortalecer la capacidad operativa y doctrinaria del Centro de Ciberdefensa.
4. Se sugiere desarrollar de manera gradual las acciones de mejora planteadas, priorizando la actualización del COEq, la capacitación del personal y la adopción de tecnologías emergentes como la inteligencia artificial, a fin de optimizar los procesos de gestión, reforzar la toma de decisiones y potenciar la capacidad operativa del Centro de Ciberdefensa.

REFERENCIAS

Arteaga, F. (2025). *El concepto de ciberdefensa activa. Real Instituto Elcano.* https://media.realinstitutoelcano.org/wp-content/uploads/2025/02/ari18-2025-arteaga-alonso-el-concepto-de-ciberdefensa-activa.pdf

CampusETIC. (2024). *Cómo implementar un enfoque de seguridad integral en una organización.* https://campusetic.com/enfoque-de-seguridad-integral-en-una-organizacion/

Check Point. (2023). ¿Qué es la Defensa en Profundidad? Recuperado de. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-defense-in-depth/

DataScientest. (2024, 5 de diciembre). *La ciberdefensa: ¿Qué es? ¿Por qué es importante?* https://datascientest.com/es/ciberdefensa-que-es

Decreto Legislativo N° 1640 *que modificó el Decreto Legislativo Nº 113, (2024).* https://busquedas.elperuano.pe/dispositivo/NL/2321390-2

Decreto Supremo N°005-2021-DE *aprueba la "Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030".* *https://www.gob.pe/institucion/mindef/normas-legales/2054885-005-2021-de*

Decreto Supremo N° 005-2025-DE *que adecua al reglamento del DL Nº 1137, Ley del Ejército del Perú del 05 Julio 2025.* https://www.gob.pe/institucion/mindef/normas-legales/7082941-05-2025-de

Decreto Supremo N° 017-2024-PCM del (2024). https://www.gob.pe/institucion/pcm/normas-legales/5192944-017-2024-pcm

Directiva N° 001 2024/DIPLANE/H-3 *sobre reestructuración y aprobación de cuadros de organización y equipo.*

Doctrina de operaciones en el Ciberespacio (DFA-CD-03-28 - 2018) *del Comando Conjunto de las Fuerzas Armadas.*

El Plan de Transformación Institucional al 2034 *https://es.scribd.com/document/706648142/ejercito-LIBRO-PEDI-FINAL-AL-02-DIC-23-1*

Estado Mayor Conjunto del Perú. (2020). *Doctrina de operaciones conjuntas. Ministerio de Defensa del Perú.* https://www.gob.pe/institucion/mindef

Ejército del Perú. (2025). *Manual de organización y funciones de las unidades especializadas*. Lima: EP, MINDEF.

Guía de Ciberdefensa – JID, *Manuales extranjeros (JP 3-12 Cyberspace Operations, FM 31-12 Cyberspace operations and electromagnetic warfare, etc)*

International Organization for Standardization. (2022). ISO/IEC 27001:2022. https://www.iso.org/standard/27001

Itcons. (2025). *¿Qué es la gestión operativa y por qué es clave para tu empresa?* https://itcons.app/que-es-la-gestion-operativa

Inter-American Development Bank. (2020). *Metodología de ciberdefensa para organizaciones: Versión 1.0.*

Ley de Gobierno Digital N° 1412. *Establecer el marco de gobernanza del gobierno digital. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412*

Lezama, C. R. Q. (2023). *Ciberdefensa y ciberseguridad en el Perú: Realidad y retos en torno a la capacidad de las FF. AA. Revista Científica de Investigación en Defensa, 1(1).* https://recide.caen.edu.pe/index.php/recide/article/view/99

López Villanueva D., Palau, R., & Santiago, R. (2025). *Analizando alternativas metodológicas para la investigación educativa: Design Science Resea rch(DSR).* UTE Teaching and Technology(Universitas Tarraconensis). https://revistes.urv.cat/index.php/ute/article/view/4062/4737#info

Manual del Ejército ME-11-225 (2018). *Conocimientos básicos de las Operaciones Cibernéticas.*

Manual de Organización y funciones del Centro de Ciberdefensa (2025).

Ministerio de Defensa del Perú. (2019). Ley N° 30999: Ley de Ciberdefensa. https://www.gob.pe/institucion/mindef/normas-legales

Ministerio de Defensa del Perú. (2024). *Lineamientos doctrinarios para la ciberdefensa en el Sector Defensa*. https://www.gob.pe/institucion/pcm/normas-legales/5192944-017-2024-pcm

National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. NIST. https://www.nist.gov/cyberframework

NATO. (2021). *Allied joint doctrine for cyberspace operations (AJP-3.17).* https://www.nato.int/nato_static_fl2014/assets/pdf/2022/5/pdf/220522-cyber-ops-doctrine.pdf

OTAN. (2023). *NATO Cyber Defence Policy*. NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Parlamento Europeo y Consejo. (2022). *Directiva (UE) 2022/2555 relativa a medidas para un nivel alto común de ciberseguridad.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

Silva, Autor. (2025). Los puestos de comando en ciberdefensa y su organización en el CECYBER Tesis. https://repositorio.escuelamilitar.edu.pe/bitstreams/ff20b69d-ad9f-4b46-98e3-1f7272576248/downloa

Slack, N., Brandon-Jones, A., & Johnston, R. (2016). *Operations management (8th ed.). Pearson.* https://www.pearson.com/uk/educational/operations-management-8e.html

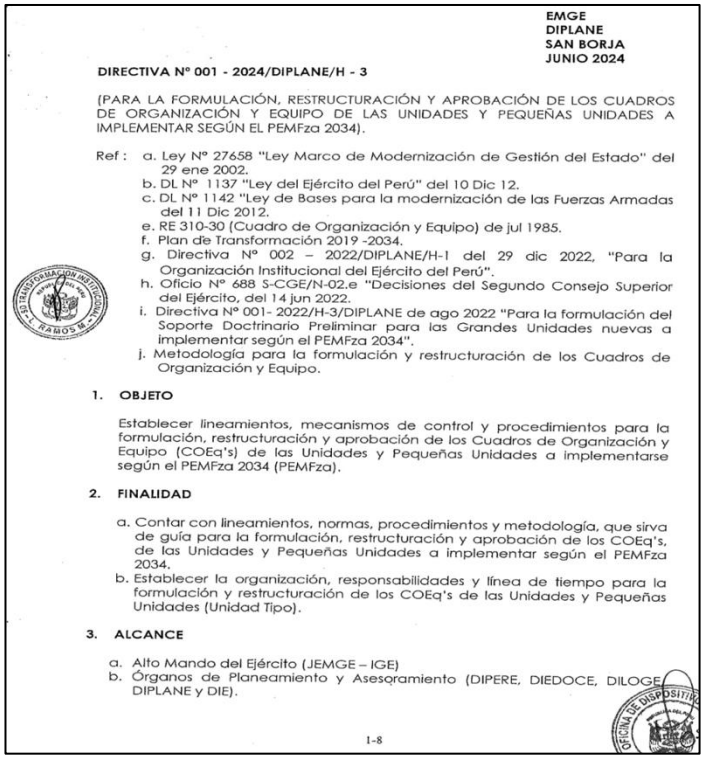
U.S. Joint Chiefs of Staff. (2020). *Joint publication 3-0: Joint operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

ANEXOS

1. El Proyecto del Cuadro de Organización y Equipo (COEq) N° 11- 495 S, con fecha 01 de enero de 2026, de clasificación SECRETO
2. Resolución de aprobación del COEq del Centro de Ciberdefensa.
3. Cuadro de optimización del coeq del centro de ciberdefensa mediante inteligencia artificial y tecnologías modernas.
4. Declaración jurada de autenticidad y no plagio.
5. Autorización para publicación de tesis en el Repositorio del ICTE.

Anexo 1

Información genérica del Proyecto del Cuadro de Organización y Equipo (COEq) N° 11- 495 S, con fecha 01 de enero de 2026, de clasificación SECRETO



EMGE
DIPLANE
SAN BORJA
JUNIO 2024

DIRECTIVA Nº 001 - 2024/DIPLANE/H - 3

(PARA LA FORMULACIÓN, RESTRUCTURACIÓN Y APROBACIÓN DE LOS CUADROS DE ORGANIZACIÓN Y EQUIPO DE LAS UNIDADES Y PEQUEÑAS UNIDADES A IMPLEMENTAR SEGÚN EL PEMFza 2034).

Ref : a. Ley Nº 27658 "Ley Marco de Modernización de Gestión del Estado" del 29 ene 2002.
b. DL Nº 1137 "Ley del Ejército del Perú" del 10 Dic 12.
c. DL Nº 1142 "Ley de Bases para la modernización de las Fuerzas Armadas del 11 Dic 2012.
e. RE 310-30 (Cuadro de Organización y Equipo) de jul 1985.
f. Plan de Transformación 2019 -2034.
g. Directiva Nº 002 – 2022/DIPLANE/H-1 del 29 dic 2022, "Para la Organización Institucional del Ejército del Perú".
h. Oficio Nº 688 S-CGE/N-02.e "Decisiones del Segundo Consejo Superior del Ejército, del 14 jun 2022.
i. Directiva Nº 001- 2022/H-3/DIPLANE de ago 2022 "Para la formulación del Soporte Doctrinario Preliminar para las Grandes Unidades nuevas a implementar según el PEMFza 2034".
j. Metodología para la formulación y restructuración de los Cuadros de Organización y Equipo.

1. **OBJETO**

Establecer lineamientos, mecanismos de control y procedimientos para la formulación, restructuración y aprobación de los Cuadros de Organización y Equipo (COEq's) de las Unidades y Pequeñas Unidades a implementarse según el PEMFza 2034 (PEMFza).

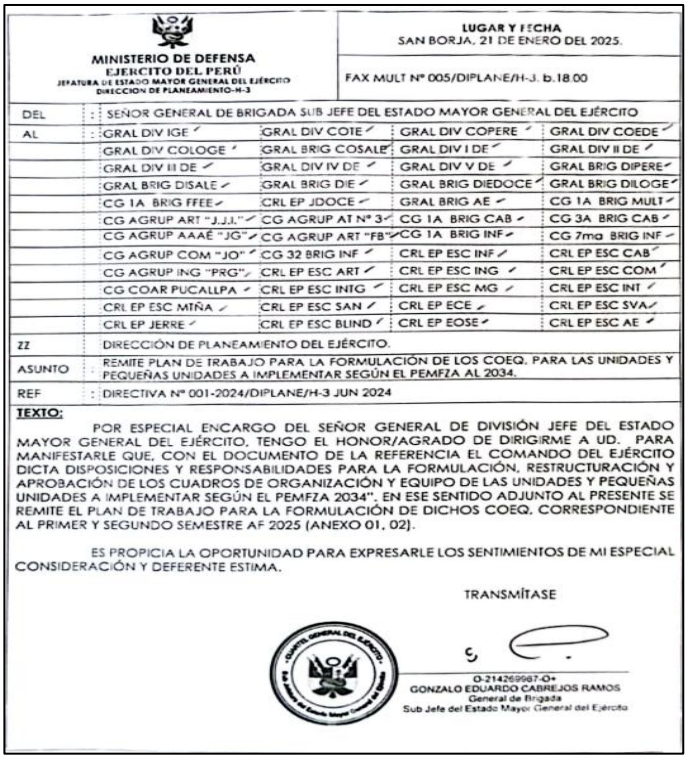
2. **FINALIDAD**

a. Contar con lineamientos, normas, procedimientos y metodología, que sirva de guía para la formulación, restructuración y aprobación de los COEq's, de las Unidades y Pequeñas Unidades a implementar según el PEMFza 2034.
b. Establecer la organización, responsabilidades y línea de tiempo para la formulación y restructuración de los COEq's de las Unidades y Pequeñas Unidades (Unidad Tipo).

3. **ALCANCE**

a. Alto Mando del Ejército (JEMGE – IGE)
b. Órganos de Planeamiento y Asesoramiento (DIPERE, DIEDOCE, DILOGE, DIPLANE y DIE).

1-8



MINISTERIO DE DEFENSA
EJERCITO DEL PERÚ
JEFATURA DE ESTADO MAYOR GENERAL DEL EJÉRCITO
DIRECCIÓN DE PLANEAMIENTO-H-3

LUGAR Y FECHA
SAN BORJA, 21 DE ENERO DEL 2025.

FAX MULT Nº 005/DIPLANE/H-3. h.18.00

DEL	SEÑOR GENERAL DE BRIGADA SUB JEFE DEL ESTADO MAYOR GENERAL DEL EJÉRCITO			
AL	GRAL DIV IGE	GRAL DIV COTE	GRAL DIV COPERE	GRAL DIV COEDE
	GRAL DIV COLOGE	GRAL BRIG COSALE	GRAL DIV I DE	GRAL DIV II DE
	GRAL DIV III DE	GRAL DIV IV DE	GRAL DIV V DE	GRAL BRIG DIPERE
	GRAL BRIG DISALE	GRAL BRIG DIE	GRAL BRIG DIEDOCE	GRAL BRIG DILOGE
	CG 1A BRIG FFEE	CRL EP JDOCE	GRAL BRIG AE	CG 1A BRIG MULT
	CG AGRUP ART "J.J.I."	CG AGRUP AT Nº 3	CG 1A BRIG CAB	CG 3A BRIG CAB
	CG AGRUP AAAÉ "JG"	CG AGRUP ART "FB"	CG 1A BRIG INF	CG 7ma BRIG INF
	CG AGRUP COM "JO"	CG 32 BRIG INF	CRL EP ESC INF	CRL EP ESC CAB
	CG AGRUP ING "PRG"	CRL EP ESC ART	CRL EP ESC ING	CRL EP ESC COM
	CG COAR PUCALLPA	CRL EP ESC INTG	CRL EP ESC MG	CRL EP ESC INT
	CRL EP ESC MIÑA	CRL EP ESC SAN	CRL EP ECE	CRL EP ESC SVA
	CRL EP JERRE	CRL EP ESC BLIND	CRL EP EOSE	CRL EP ESC AE
ZZ	DIRECCIÓN DE PLANEAMIENTO DEL EJÉRCITO.			
ASUNTO	REMITE PLAN DE TRABAJO PARA LA FORMULACIÓN DE LOS COEQ. PARA LAS UNIDADES Y PEQUEÑAS UNIDADES A IMPLEMENTAR SEGÚN EL PEMFZA AL 2034.			
REF	DIRECTIVA Nº 001-2024/DIPLANE/H-3 JUN 2024			

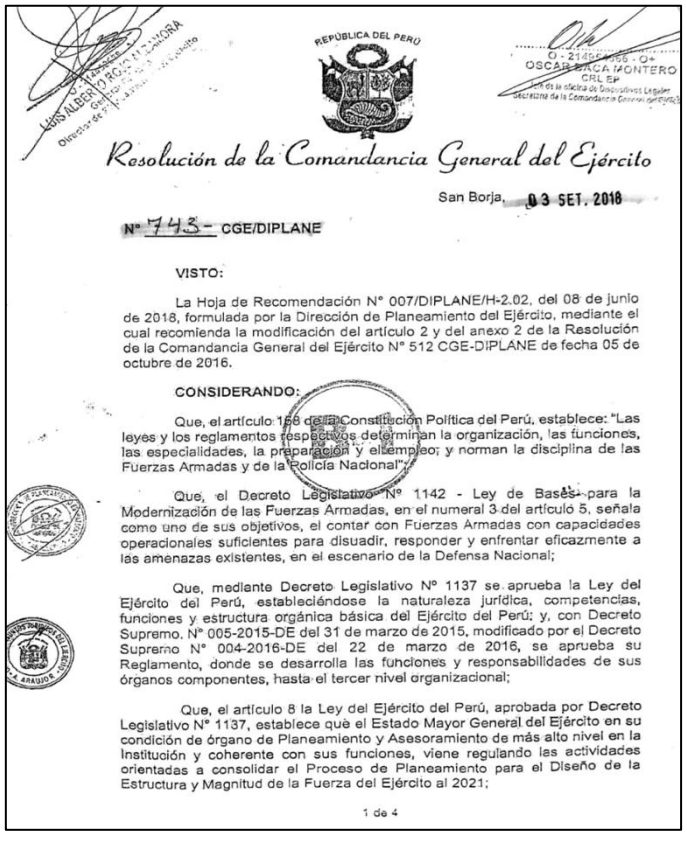
TEXTO:

POR ESPECIAL ENCARGO DEL SEÑOR GENERAL DE DIVISIÓN JEFE DEL ESTADO MAYOR GENERAL DEL EJÉRCITO, TENGO EL HONOR/AGRADO DE DIRIGIRME A UD. PARA MANIFESTARLE QUE, CON EL DOCUMENTO DE LA REFERENCIA EL COMANDO DEL EJÉRCITO DICTA DISPOSICIONES Y RESPONSABILIDADES PARA LA FORMULACIÓN, RESTRUCTURACIÓN Y APROBACIÓN DE LOS CUADROS DE ORGANIZACIÓN Y EQUIPO DE LAS UNIDADES Y PEQUEÑAS UNIDADES A IMPLEMENTAR SEGÚN EL PEMFZA 2034". EN ESE SENTIDO ADJUNTO AL PRESENTE SE REMITE EL PLAN DE TRABAJO PARA LA FORMULACIÓN DE DICHOS COEQ. CORRESPONDIENTE AL PRIMER Y SEGUNDO SEMESTRE AF 2025 (ANEXO 01, 02).

ES PROPICIA LA OPORTUNIDAD PARA EXPRESARLE LOS SENTIMIENTOS DE MI ESPECIAL CONSIDERACIÓN Y DEFERENTE ESTIMA.

TRANSMÍTASE

O-21426967-O+
GONZALO EDUARDO CABREJOS RAMOS
General de Brigada
Sub Jefe del Estado Mayor General del Ejército



REPÚBLICA DEL PERÚ

Resolución de la Comandancia General del Ejército

San Borja, 03 SET. 2018

Nº 743 - CGE/DIPLANE

VISTO:

La Hoja de Recomendación Nº 007/DIPLANE/H-2.02, del 08 de junio de 2018, formulada por la Dirección de Planeamiento del Ejército, mediante el cual recomienda la modificación del artículo 2 y del anexo 2 de la Resolución de la Comandancia General del Ejército Nº 512 CGE-DIPLANE de fecha 05 de octubre de 2016.

CONSIDERANDO:

Que, el artículo 166 de la Constitución Política del Perú, establece: "Las leyes y los reglamentos respectivos determinan la organización, las funciones, las especialidades, la preparación y el empleo; y norman la disciplina de las Fuerzas Armadas y de la Policía Nacional";

Que, el Decreto Legislativo Nº 1142 - Ley de Bases para la Modernización de las Fuerzas Armadas, en el numeral 3 del artículo 5, señala como uno de sus objetivos, el contar con Fuerzas Armadas con capacidades operacionales suficientes para disuadir, responder y enfrentar eficazmente a las amenazas existentes, en el escenario de la Defensa Nacional;

Que, mediante Decreto Legislativo Nº 1137 se aprueba la Ley del Ejército del Perú, estableciéndose la naturaleza jurídica, competencias, funciones y estructura orgánica básica del Ejército del Perú; y, con Decreto Supremo Nº 005-2015-DE del 31 de marzo de 2015, modificado por el Decreto Supremo Nº 004-2016-DE del 22 de marzo de 2016, se aprueba su Reglamento, donde se desarrolla las funciones y responsabilidades de sus órganos componentes, hasta el tercer nivel organizacional;

Que, el artículo 8 la Ley del Ejército del Perú, aprobada por Decreto Legislativo Nº 1137, establece que el Estado Mayor General del Ejército en su condición de órgano de Planeamiento y Asesoramiento de más alto nivel en la Institución y coherente con sus funciones, viene regulando las actividades orientadas a consolidar el Proceso de Planeamiento para el Diseño de la Estructura y Magnitud de la Fuerza del Ejército al 2021;

1 de 4

"Artículo 53.- Comando General de Apoyo del Ejército
*El Comando General de Apoyo del Ejército, es el órgano responsable de realizar los procesos y actividades para cumplir las funciones de seguimiento a las operaciones terrestres, **operaciones cibernéticas**, de apoyo al desarrollo nacional, de salud, de reemplazos y movilización y de brindar apoyo administrativo a la seguridad al Cuartel General del Ejército, de economía, de generación de recursos y otros inherentes a las funciones del Ejército.*

Tiene las funciones específicas siguientes:

(...)
*53.1 Efectuar el seguimiento a las operaciones que realiza el componente terrestre de los comandos operacionales y **a las operaciones cibernéticas, así como** supervisar el entrenamiento de la fuerza operativa.*
(...)"

"Artículo 55.- Comando de Operaciones Terrestres del Ejército
*El Comando de Operaciones Terrestres del Ejército es la unidad orgánica técnico administrativa responsable de efectuar el seguimiento a las operaciones que realiza el Ejército y supervisar el Entrenamiento de la Fuerza Operativa del Componente Terrestre **y del Componente de Ciberdefensa del Ejército del Perú.***

Tiene las funciones específicas siguientes:

(...)
*55.2 Organizar, programar y ejecutar la supervisión del entrenamiento de la Fuerza Operativa del Componente Terrestre y **del Componente de Ciberdefensa del Ejército del Perú**, a fin de lograr una preparación efectiva de las Fuerzas Operativas.*
(...)"

Artículo 3.- Incorporación de los numerales 2.14, 2.15 y 2.16 en el artículo 2, de los numerales 5.09.3, 5.09.3.1, 5.09.3.2 y 5.09.3.3 en el artículo 5, el artículo 66-A y el artículo 66-B, en el Reglamento del Decreto Legislativo N° 1137, Ley del Ejército del Perú, aprobado por Decreto Supremo N° 005-2015-DE

Incorporar los numerales 2.14, 2.15 y 2.16 en el artículo 2, los numerales 5.09.3, 5.09.3.1, 5.09.3.2 y 5.09.3.3 en el artículo 5, el artículo 66-A y el artículo 66-B, en el Reglamento del Decreto Legislativo N° 1137, Ley del Ejército del Perú, aprobado por Decreto Supremo N° 005-2015-DE, conforme al siguiente detalle:

"Artículo 2. De la Base Legal
(...)
2.14 Ley N° 30999, Ley de Ciberdefensa.
2.15 Decreto Legislativo N° 1640, Decreto Legislativo que modifica el Decreto Legislativo N° 1137, Ley del Ejercito del Perú.
2.16 Decreto Supremo 017-2024-PCM, aprueban el Reglamento de la Ley 30999, Ley de Ciberdefensa.
(...)"

"Artículo 5. Estructura Orgánica Básica
El Ejército del Perú está compuesto por los siguientes órganos y sus funciones y atribuciones específicas se establecerán en el reglamento de la presente norma:

(...)
***5.09.3** Comando de Operaciones Ciberméticas*
***5.09.3.1** Unidad de Ciberdefensa*
***5.09.3.2** Unidad de Comando y Control*
***5.09.3.3** Unidad administrativa*
(...)"

"Artículo 66-A- Comando de Operaciones Cibernéticas
El Comando de Operaciones Ciberméticas opera, defiende, responde, influye e informa en el dominio del ciberespacio, en el ámbito de su competencia, para proteger y defender la información y las comunicaciones, a través de la capacidad de ciberdefensa, asegurando el comando y control, frente a las amenazas que afecten la seguridad nacional, los intereses nacionales, los activos críticos nacionales (ACN) y recursos claves (RC) para mantener las capacidades nacionales en el área de su responsabilidad.
El cargo de Comandante General del Comando de Operaciones Ciberméticas, será ejercido por un Oficial General del grado de General de Brigada es nombrado mediante Resolución Suprema.
En su ausencia las funciones son asumidas por el Oficial que le sigue en antigüedad.

Tiene las funciones específicas siguientes:

***66-A.1.** Planear, organizar y conducir a su nivel las operaciones militares en y mediante el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa propias.*
***66-A.2.** Alistar integralmente a las unidades a su cargo, para el eficiente desempeño de sus funciones, desarrollando y manteniendo un óptimo nivel de sus capacidades de ciberdefensa.*
***66-A.3.** Realizar operaciones militares en y mediante el ciberespacio propio o asignado, para proteger y defender los Activos Críticos Nacionales (ACN) y Recursos Claves (RC) asignados, así como la información y las comunicaciones frente a amenazas que comprometan la Seguridad Nacional.*
***66-A.4.** Responder de manera eficaz ante amenazas y ataques en y mediante el ciberespacio propio y asignado, que comprometan la Seguridad Nacional.*
***66-A.5.** Influir en y mediante el ciberespacio para contribuir con las operaciones de información cuando sean requeridas.*
***66-A.6.** Informar de manera oportuna sobre amenazas en y mediante el ciberespacio a los Órganos de Línea y a otros cuando corresponda.*
***66-A.7.** Analizar la evidencia digital para determinar su funcionalidad, comportamiento, origen e impacto, así como su explotación futura.*
***66-A.8.** Operar y mantener el sistema de telecomunicaciones del Ejército para asegurar el comando y control de los Órganos de Línea del Ejército.*
***66-A.9.** Establecer los procedimientos operativos para la ejecución de operaciones de soporte, protección y ataque electrónico de los Órganos de Línea.*
***66.-A.10.** Otras, por designación expresa del Comandante General del Ejército o que le sean dadas por norma sustantiva."*

"Artículo 66-B Unidades Orgánicas del Comando de Operaciones Cibernéticas
El Comando de Operaciones Ciberméticas tiene a su cargo las unidades orgánicas siguientes:

66 B.1 Unidad de Ciberdefensa
66 B .2 Unidad de Comando y Control
66 B .3 Unidad administrativa"

Artículo 4.- Financiamiento
La implementación de las acciones involucradas en la presente norma se financia con cargo al presupuesto institucional del Pliego 026: M. de Defensa, Unidad Ejecutora 003: Ejército Peruano, sin demandar recursos adicionales al Tesoro Público.

Artículo 5.- Refrendo
El presente Decreto Supremo es refrendado por el Ministro de Defensa.

Dado en la Casa de Gobierno, en Lima, a los cuatro días del mes de julio del año dos mil veinticinco.

DINA ERCILIA BOLUARTE ZEGARRA
Presidenta de la República

WALTER ENRIQUE ASTUDILLO CHAVEZ
Ministro de Defensa

2416480-3

Copia N° ... de ... Copias
CGE
DIPLANE
SAN BORJA

DIRECCIÓN DE PLANEAMIENTO DEL EJÉRCITO

EFICIENCIA DESARROLLO VISIÓN

COEq Nº 11 - 49 S

CENTRO DE CIBERDEFENSA DEL COCIBER

CUADRO DE ORGANIZACIÓN
Y EQUIPO
Nº 11 - 49 S

EJEMPLAR Nº ... de ... copias
MINISTERIO DE DEFENSA
CUARTEL GENERAL DEL EJÉRCIT
LIMA, 01 DE ENERO DE 2026

CENTRO DE CIBERDEFENSA

Designación : Centro de Ciberdefensa del COCIBER

ÍNDICE PÁG

SECCIÓN I
GENERALIDADES

SECCIÓN II. ORGANIZACIÓN (Personal)

CENTRO DE CIBERDEFENSA — COEq N° 11 - 495 S 01 ENERO 2026

LINEA	DESIGNACIÓN	IDENT	ARMA O SERV	POME	EFECT	COD CAPAC	Oficiales						TCOS y SSOO						TSM			OBS
							CRL	TC	MY	CAP	TTE	STTE	TCO1	TCO2	TCO3	SO1	SO2	SO3	S1	S2	C	S
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
00	COMANDO																					
01	Jefe	O	COM		1	1.1	1															01
	TOTAL				1		1															
	RESUMEN																					
	-OFICIALES:	O	COM		1	1.1	1															
					1		1															
	TOTAL				1		1															
	OBSERVACIONES:																					
	-01: Personal dotado de pistola automática.																					

SECCIÓN – III EQUIPO

CENTRO DE CIBERDEFENSA — COEq Nº 11 - 495 S 01 ENERO 2026

Nº	COD ARTÍCULO	DESIGNACIÓN DEL ARTÍCULO	CANT	COD CAPACIDAD	OBS
		CENTRO DE CIBERDEFENSA			
		COMANDO			

SECCIÓN IV PERSONAL POR CAPACIDADES

CENTRO DE CIBERDEFENSA — COEq N° 11 - 495 S 01 ENERO 2026

CAP FUNDAMENTAL	CAPACIDAD OPERACIONAL	LÍNEA	DESIGNACIÓN	IDENT	ARMA O SERV	EFECT	GRADO	CÓDIGO CAPAC	OBS
1.COMANDO Y CONTROL	1.1 Mando y planificación	01	Jefe	O	COM	1	CRL	1.1	
	1.2 Cooperación cívico militar								
	1.3 Guerra psicológica								
	1.4 Acción psicológica								
	1.5 Participación multisectorial								
	1.6 Telemática								
	2.1 Colección								
	2.2 Procesamiento								

Anexo 2

Resolución de Aprobación del Cuadro de Organización y Equipo del Centro de Ciberdefensa

ES COPIA FIEL DEL ORIGINAL
23 DIC. 2025

O-40314957-1-O+
PERCY QUISPE SALAZAR
CRL EP

Resolución de la Comandancia General del Ejército

San Borja, 23 DIC. 2025

1019
Nº _____-CGE/DIPLANE

VISTOS:

La Hoja de Recomendación Nº 066/DIPLANE/H-1.c.1/06.00, de diciembre de 2025 que aprueba la adecuación del Comando de Operaciones Cibernéticas al Reglamento de la Ley del Ejército del Perú, y aprobación del Cuadro de Organización y Equipo de sus Unidades Orgánicas;

CONSIDERANDO:

Que, el artículo 168º de la Constitución Política del Perú, establece que las leyes y los reglamentos respectivos determinan la organización, las funciones, las especialidades, la preparación y el empleo; y, norman la disciplina de las Fuerzas Armadas en condiciones de operatividad y eficiencia;

Que, el Decreto Legislativo Nº 1142, Ley de Bases para la Modernización de las Fuerzas Armadas, en el artículo 4º, establece *"La modernización de las Fuerzas Armadas se inserta en el proceso de modernización del Estado Peruano y tiene como finalidad fundamental obtener mayores niveles de eficiencia y eficacia en la gestión institucional y operacional de las Fuerzas Armadas, en sus diferentes instancias y capacidades; de manera que su preparación, equipamiento y empleo sirva para garantizar la independencia, la soberanía y la integridad territorial de la República, así como en el desarrollo económico y social del país"*;

Que, mediante el Decreto Supremo Nº 054-2018-PCM, se aprobó los Lineamientos de organización del Estado, en el cual se prevé que las entidades deben contar con una estructura orgánica que se desarrolla en el Reglamento de Organización y Funciones, y cuenta con tres niveles organizacionales que reflejan la dependencia jerárquica;

Que, mediante Decreto Supremo Nº131-2018-PCM, se modificó el Decreto Supremo Nº 054-2018-PCM, incorporándose la Décimo Primera Disposición Complementaria Final, en la cual se ha establecido que *"En el caso de las Fuerzas Armadas, su estructura y funciones se regulan conforme lo dispuesto en su ley de creación y su reglamento, y se ciñe a los principios que*

1 de 3

SE RESUELVE:

Artículo 1.- Aprobar la adecuación del funcionamiento del Comando de Operaciones Cibernéticas al Reglamento de la Ley del Ejército del Perú, aprobado mediante Decreto Supremo Nº 005-2015-DE, modificado por el Decreto Supremo Nº 005-2015-DE, conforme al anexo único que forman parte integrante de la presente Resolución.

Artículo 2.- Aprobar los Cuadros de Organización y Equipo de las Unidades Orgánicas del Comando de Operaciones Cibenéticas: Centro de Ciberdefensa (COEq Nº 11-49 S), Centro de Telecomunicaciones (COEq Nº 11-485 S), y Compañía Comando y Soporte (COEq Nº 11-442 S), y entrarán en vigencia el 01 de enero de 2026.

Artículo 3.- Disponer que el COPERE, COLOGE, COTE, y OPRE, realicen las acciones administrativas de su competencia.

Regístrese, Comuníquese y Archívese, teniendo la clasificación de "SECRETO".

O-24115603-O+
CÉSAR AUGUSTO BRICEÑO VALDIVIA
General de Ejército
Comandante General del Ejército

Anexo 3

Cuadro de optimización del coeq del centro de ciberdefensa mediante inteligencia artificial y tecnologías modernas.

ELEMENTO DEL COEQ	COEQ ACTUAL (SITUACIÓN TRADICIONAL)	COEQ OPTIMIZADO CON IA Y TECNOLOGÍAS MODERNAS	MEJORA OBTENIDA
Capacidad de Defensa	Monitoreo manual y alertas básicas de seguridad	Detección automatizada con IA (SIEM, EDR, XDR inteligentes)	Mayor velocidad y precisión en la detección de amenazas
Capacidad de Explotación	Análisis manual de vulnerabilidades y OSINT	Análisis automatizado con IA y detección predictiva	Mejora en la anticipación de ataques
Capacidad de Respuesta	Respuesta manual ante incidentes	Automatización con SOAR e IA (bloqueo y contención automática)	Reducción del tiempo de respuesta (MTTR)
Investigación Digital	Forense manual de evidencias	Forense digital asistido por IA	Mayor eficiencia en análisis de evidencias
Gestión del personal	Asignación manual de funciones	Optimización con IA para distribución de carga	Mejor uso del recurso humano
Equipamiento tecnológico	Infraestructura convencional	SOC con IA y servidores de alto rendimiento	Mayor capacidad de procesamiento
Toma de decisiones	Reportes manuales	Dashboards inteligentes con predicción	Decisiones más rápidas y basadas en datos

Anexo 4

Declaración jurada de autenticidad y no plagio

Zully Melissa POCLIN GUEVARA

Declaro que, para optar el grado académico de **TÍTULO PROFESIONAL** en **INGENIERÍA DE TELECOMUNICACIONES**, a ser entregado en el ICTE, he elaborado íntegramente el trabajo de investigación titulado: **"Optimización de la Gestión Operativa y Cibernética mediante el Diseño del Cuadro de Organización y Equipo en el Centro de Ciberdefensa del Ejército del Perú, Lima, 2025"**

Confirmo que este trabajo de investigación es auténtico y de mi total autoría, no existiendo plagio o copia de otro trabajo de investigación o material existente cuya autoría corresponda a un tercero.

Dejo expresa constancia que la propiedad intelectual de otros autores ha sido debidamente citada o identificada. Así mismo asumo la responsabilidad de todo lo dicho en el trabajo de investigación, así como de cualquier error u omisión en la misma.

Finalmente reconozco y acepto que en caso se compruebe lo contrario a lo expresado en este documento, me someto a las medidas establecidas para tal hecho por el ICTE.

Me afirmo y ratifico en lo expresado anteriormente, en señal de lo cual firmo el presente documento.

Surco, 19 de mayo del 2026.

FIRMA: _____

POST FIRMA: _____Z.POCLIN.G_____

DNI: _____47051467_____

Anexo 5

Autorización para publicación de tesis en el Repositorio del ICTE

Título de la tesis:

"**Optimización de la Gestión Operativa y Cibernética mediante el Diseño del Cuadro de Organización y Equipo en el Centro de Ciberdefensa del Ejército del Perú, Lima, 2025**

Nombre: Zully Melissa Poclin Guevara

Nombre del asesor: Dr. Carlos Quinto Huamán

Año de sustentación 2026

Bajo los siguientes términos, autorizo la publicación de mi trabajo de investigación en el Repositorio Digital del **Instituto Científico y Tecnológico del Ejército - ICTE. Escuela de Pre y Posgrado.**

Con la autorización de publicación de mi Trabajo de Investigación, otorgo al ICTE una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público la tesis (incluido resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios provistos por el ICTE, creados o por crearse, tales como el Repositorio Digital de Tesis del ICTE, Portal de Tesis de la SUNEDU, entre otros, en el Perú y en el extranjero, por el tiempo y las veces que considera necesarias, y libre de remuneraciones.

En virtud de dicha licencia, el ICTE podrá reproducir mi trabajo de investigación en cualquier tipo de soporte y en más de un ejemplar; sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro asimismo que el trabajo de investigación es una creación de mi autoría y exclusiva titularidad, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha tesis no infringe derechos de autor de terceras personas.

El ICTE consignará el nombre del autor del trabajo de investigación, y no le hará ninguna modificación más que la permitida en la presente licencia.

Surco, 19 de mayo del 2026.

FIRMA : _____
POST FIRMA: Z.POCLIN.G
DNI : 47051467