ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

ANÁLISIS DE LA SEGURIDAD DE RED DE DATOS DEL CENTRO DE COMUNICACIONES 32ª BRIGADA DE INFANTERIA, 2022

AUTOR:

Bach. Felix Junior ESPINOZA LUPUCHE

000-0003-1426-634

Para optar al Grado Académico de

MAESTRO EN CIENCIAS MILITARES

Con mención en Planeamiento Estratégico y Toma de Decisiones

ASESOR:

Mg. Jorge Luis BONILLA FERREYRA

0000-0003-2704-8066

2025

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 005 – 2025/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veintidós (22) días del mes de abril del año dos mil veinticinco, siendo las ..10:00.. horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctor**	**IVAN RICARDO BARRETO BARDALES**	**Presidente**
❖	**Doctora**	**LILIANA RODRIGUEZ SAAVEDRA**	**Secretario**
❖	**Doctor**	**GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 005-2025/SIE/DGI/ESGE-EPG** del 04 de abril de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"ANALISIS DE LA SEGURIDAD DE RED DE DATOS DEL CENTRO DE COMUNICACIONES 32ª BRIGADA DE INFANTERIA, 2022"**, presentado por el Bachiller **FELIX JUNIOR ESPINOZA LUPUCHE**, para optar el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

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

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

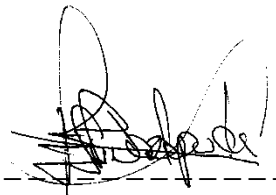
Firmado, en Chorrillos a los veintidós (22) días del mes de abril del año dos mil veinticinco.

DR. IVAN RICARDO BARRETO BARDALES	**DRA. LILIANA RODRIGUEZ SAAVEDRA**	**DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**
PRESIDENTE	**SECRETARIO**	**VOCAL**

Autorización para publicación y uso

Yo, Bach. Felix Junior ESPINOZA LUPUCHE a través del presente documento autorizo a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado la publicación del texto completo o parcial de la tesis de grado titulada: “Análisis de la seguridad de red de datos del Centro de Comunicaciones 32ª Brigada de Infantería, 2022” presentada para optar el grado académico de Maestro en Ciencias Militares, con mención en Planeamiento Estratégico y Toma de Decisiones, en el Repositorio Institucional y en el Repositorio Nacional de Tesis (Renati) de la Superintendencia Nacional de Educación Superior Universitaria (Sunedu), de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada, exhibida y usada también con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Chorrillos, 22 de abril de 2025



ESPINOZA LUPUCHE Felix Junior

D.N.I. Nº 42553498

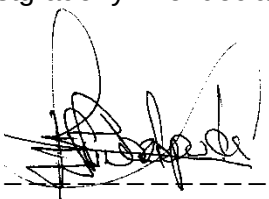
Declaración jurada de autoría

Mediante el presente documento, Yo, Bach. Felix Junior Espinoza, identificado con Documento Nacional de Identidad N° 42553498, con domicilio real en Jr. Huayna Cápac 181 Tahuantinsuyo del distrito de Independencia, provincia de Lima, departamento de Lima, estudiante de la XI Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG) declaro bajo juramento que:

Soy el autor de la investigación titulada: Análisis de la seguridad de red de datos del Centro de Comunicaciones 32ª Brigada de Infantería, 2022, que presento a los veintidós (22) días del mes de abril del año 2025, ante esta institución con fines de optar el grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones.

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

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



ESPINOZA LUPUCHE Felix Junior

D.N.I. N° 42553498

Dedicatoria

Gracias a ti amada abuela y a ti madre por tu cariño, comprensión y abrazos que siempre son reconfortantes. Además, gracias a mis queridos tíos que me han brindado afecto y respaldo en esta carrera militar, sobre todo mientras completaba esta tesis y obtenía mi Maestría en Ciencias Militares.

Índice

Contenido

Lista de tablas

Lista de figura

Resumen

Actualmente, todo lo relacionado con las operaciones cibernéticas está recibiendo mucha atención por parte del Ejercito del Perú, esta situación también está alineada con las políticas del estado en el tema de seguridad nacional para contrarrestar las amenazas emergentes, que ocupan un espacio dentro de la nueva dimensión de la actividad humana, el llamado "ciberespacio", que como parte de nuestra soberanía nacional está presente en el accionar de nuestras Fuerzas Armadas. Por tal motivo todos los ejércitos de todo el mundo deben combatir las amenazas informáticas a medida que aumentan las tecnologías de la información. En esta investigación de tipo teórico - empírico, basada en el enfoque cualitativo que tiene como limitación a la 32ª Brigada de Infantería, donde opera un Centro de Comunicaciones que maneja importante tráfico de información entre sus diferentes niveles de mando a través de redes informáticas, sin embargo, el Ejército del Perú, no dispone de información suficiente para el nivel de protección de la red de datos, especialmente en lo que respecta a los equipos informáticos. En tal sentido el objetivo principal de esta investigación es la de analizar cómo funciona la seguridad de la red de datos, teniendo como muestra para la aplicación de técnicas de recolección de datos al personal militar de la Compañía de Comunicaciones Nº 32, que pertenece a la 32ª Brigada de Infantería, dando la perspectiva de responsabilidad de los datos gestionados en el Centro de Comunicaciones de esta Gran Unidad de Combate, donde la seguridad de la información es vulnerable a amenazas informáticas.

***Palabras clave*:** operaciones cibernéticas, amenazas cibernéticas, centro de comunicaciones, ciberespacio.

Abstract

Currently, everything related to cyber operations is receiving a lot of attention from the Peruvian Army, this situation is also aligned with the state policies on the issue of national security to counteract emerging threats, which occupy a space within the new dimension of human activity, the so-called "cyberspace", which as part of our national sovereignty is present in the actions of our armed forces. For this reason, all armies around the world must be able to combat computer threats as information technologies increase. In this phenomenological research, based on the qualitative approach that is limited to the 32nd Infantry Brigade, where it operates a communications center that handles important information traffic between its different levels of command through computer networks, however, the Peruvian Army does not have sufficient information for the level of protection of the data network, especially with regard to computer equipment. In this sense, the main objective of this research is to analyze how data network security works, using as a sample the application of data collection techniques to the military personnel of the 32nd Communications Company, belonging to the 32nd Infantry Brigade, giving the perspective of responsibility for the data managed in the communications center of this large combat unit, where information security is vulnerable to computer threats.

Keywords: cyber operations, cyber threats, communications center, cyberspace.

Introducción

El adelanto de la tecnología a pasos agigantados, sumado a la creciente infraestructura del mundo digital, debido a los beneficios que nos brinda la internet, ha hecho que muchas instituciones, organizaciones, y centros de estudios estén conectados a diferentes tipos de sistemas el cual les permite facilitar su funcionamiento. Sin embargo, debido a la pandemia del COVID -19, tuvo repercusión en el aspecto informático, aumentando la importancia de la conectividad digital, convirtiéndose para muchas organizaciones como su fuente de subsistencia y desarrollo, la cual demanda una mayor integración a las Tecnologías de la Información y la Comunicación estas exigencias del mundo digital, involucra al ámbito militar para desarrollar, su desempeño tanto en la parte de operaciones como acciones militares.

Según Trama (2017) propuso que: “Los aspectos que influyen en la vida diaria con respecto al uso del espacio cibernético tienen amplia difusión. Todas las acciones que se desarrollen en este campo afectarán al componente armado del poder nacional desde varias perspectivas” (p.3). En el año 2017, en el Perú el Consejo de Seguridad y Defensa Nacional (COSEDENA) aprobó políticas que permiten proteger nuestros sistemas de información ante las emergentes amenazas informáticas, desde entornos ciberespaciales que puedan vulnerar la Seguridad y Defensa Nacional. El Ejército del Perú desde el año 2014, realiza diversas actividades, relacionadas con las operaciones cibernéticas las cuales han sido destinadas a generar conciencia en razón de estas nuevas amenazas informáticas emergentes, contando con el apoyo de diversas instituciones nacionales e internacionales, un ejemplo fue el caso del intercambio académico con el Ejército de Brasil, país con el cual, existen buenas relaciones, que contribuyen de manera activa con sus saberes cibernéticos al personal de oficiales quienes participarían durante la operación y funcionamiento de los variados sistemas de comunicaciones que utiliza el Ejército del Perú.

Actualmente, el Centro de Comunicaciones (CECOM) de la 32ª Brigada de Infantería tiene como responsable de manera doctrinaria y funcional a la Compañía Comunicaciones N° 32, sin embargo está carece de una adecuada protección lógica a su red de datos que no permite trabajar de manera segura frente a las amenazas cibernéticas existentes, todo el tráfico de información que se maneja tanto en lo correspondiente a las operaciones y acciones militares, viene efectuando en el interior de su campo de influencia que corresponde a la Sub Zona Nacional de Seguridad (SZNS-5) y al mismo tiempo el manejo administrativo de la Brigada. Finalmente, el estudio tiene como propósito, analizar cuál es el funcionamiento de la seguridad de red de datos que maneja el CECOM, el cual está a cargo de la Compañía Comunicaciones N° 32.

Capítulo I. El problema de investigación

1.1 Planteamiento del problema

Hablar acerca de la digitalización, es sinónimo de evolución de nuestro universo, evolucionando nuestra manera de existir, laborar, instruirse y distraernos. Las entidades en su totalidad, que pretenden proporcionar los productos y servicios que demandan los usuarios, deben salvaguardar sus datos de los probables ataques cibernéticos. La protección de la data, nos permite, mantener a buen recaudo la información clasificada de tipo confidencial. Finalmente, preserva el prestigio de la entidad. Según Cano (2022), “La ciberseguridad se ha convertido en el factor fundamental que articula los esfuerzos desde diferentes frentes estatales” (p.823). Por eso todos los países del orbe vienen realizando denodados esfuerzos en lograr la seguridad de sus redes de comunicaciones. En la actualidad todas las organizaciones a nivel mundial están más supeditadas a la internet de datos, esto debido a la vertiginosa aceleración, con la que se vienen desarrollando los avances de la tecnología, donde podemos concluir que este progreso ha influenciado marcadamente en la vida de las personas, con la disponibilidad de información necesaria, el valor de la interrelación e intercambio de información, se ha puesto de manifiesto más en estos tiempos, en los cuales, nuestras actividades vienen desarrollándose con restricciones debido a la pandemia de la COVID – 19, empero, el soporte que nos ha ofrecido la internet como elemento valioso de la globalidad en el orbe, nos ha permitido tener alternativas de solución, asimismo; nos ha permitido ver y creer, que una persona frente a una computadora en cualquier parte del mundo, puede acceder a nuestra información, sin necesidad de su presencia física, lo que, trae como una de sus consecuencias, la propagación de nuevas amenazas informáticas, en donde personas o grupos con malas intenciones puedan acceder a las bases de datos de manera ilícita.

En América Latina, análogo al resto del mundo, la información es considerada un capital apreciable, y, por tanto, requiere una defensa conveniente. La seguridad de la información la protege de diversas amenazas para garantizar el orden de las operaciones de las entidades, sean privadas o estatales de cada país y minimizar daños, y esto se logra imponiendo una totalidad apropiada de supervisiones, que pueden ser políticas, reglas, instrucciones, estructuras, herramientas para el tratamiento de la información digital, entre otros, concordante a lo expresado por los autores Agudelo et al (2020):

> Al normalizar y emplear los equipos de comunicaciones actuales, se han modificado, hoy en día las operaciones de adquisición, la disposición y de explotación de la información. De igual manera, las amenazas evolucionaron, por lo que la seguridad de las comunicaciones se ha trasformado igualmente. (p.14)

Por ende, es primordial que no se escatime las medidas y acciones destinadas a obtener el resguardo de las comunicaciones. En nuestro país, salvaguardar las comunicaciones, se ha vuelto un tema demandante en las organizaciones privadas y estatales, puesto que todos necesitan que las informaciones sean seguras en todo momento. Es necesario recalcar que la Del Perú, C. P. (1993) en su artículo 2 inciso 10. menciona, “Toda persona tiene derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados” (p.12). Así mismo el Ministerio de Transportes y Comunicaciones es encargado de garantizar este derecho, es por eso que el ciberespacio es considerado integrante de nuestra soberanía, dictando políticas y lineamientos que el consejo para la seguridad y defensa nacional ha considerado a las amenazas en el ciberespacio, distinguiendo medidas, que permitan proteger nuestros activos críticos nacionales. Es por eso, que las organizaciones de cualquier índole en nuestro país, se han esmerado en desarrollar las medidas y acciones, orientadas a lograr la seguridad de sus comunicaciones en todo momento. En nuestros tiempos, el Ejército del Perú, en su organización, dispone de la Primera División de Ejército (I DE) y como parte de sus componentes y dentro de su organización tiene a la 32ª Brigada de Infantería, emplazada en región de la Libertad. Dentro de la conformación de esta Gran Unidad de Combate (GUC), se encuentra la Compañía Comunicaciones N° 32, como parte de sus componentes de comando y control, la cual tiene como responsabilidad operar el CECOM de la GUC. Este CECOM, apoya en cuanto a comunicaciones con su personal, equipos, medios informáticos e instalaciones al Cuartel General de la GUC.

El CECOM, para su normal funcionamiento opera las redes institucionales a cargo de la GUC, como la fibra óptica, el sistema satelital VSAT, internet y el sistema de radio enlace. Sobre estas plataformas transita información particular, referente a las operaciones y aspectos administrativos, que involucran el empleo de esta GUC. En este particular, debido a la clasificación de la información, que se maneja en el CECOM, existe la posibilidad de exposición a las amenazas informáticas, obteniéndose información de manera indebida, que pueden ser empleados en múltiples oportunidades para cometer actos ilícitos, particularmente tareas contrarias que son asignadas a esta Brigada, motivo por el cual cobra trascendente importancia el resguardo de la estimable información, que transita en la red de datos del CECOM de la 32ª Brigada de Infantería, a su vez cuenta con una limitada protección informática, puesto que personas no acreditadas, puedan penetrar en ella, a través de operaciones cibernéticas, valiéndose de las limitaciones existentes; en ella, siendo necesario el presente estudio, dado que salvaguardar la red de datos, es de valiosa importancia para el accionar coordinado de la GUC en seguridad del empleo del espacio interconectado.

1.2 Justificación de la investigación

1.2.1 Justificación práctica

Es responsabilidad de la 32ª Brigada de Infantería salvaguardar la red de datos del CECOM de esta GUC, donde se realiza un tráfico de información clasificada que, siendo necesario disponer de medios y procedimientos, que permitan resguardar la red de datos de las amenazas informáticas, toda vez que el ciberespacio tiene la particularidad de no tener fronteras, debido a la proliferación del internet y el desconocimiento de las identidades de los operadores. Las operaciones cibernéticas, incluyen actividades de Ciberseguridad y Ciberdefensa, que debe garantizar la obtención, proceso, acopio y propagación de la información fehaciente a través de la red de datos de comunicaciones, que opera en el ciberespacio, configurando acciones eficaces para su empleo en protección cibernéticas para la consecución de su misión.

La 32ª Brigada de Infantería a futuro tendrá alcance para tener una mejor optimización del trabajo de la Compañía Comunicaciones N° 32 de esta GUC, durante la ejecución de las múltiples tareas castrenses que tenga que efectuar la Brigada en la observancia de su misión.

Desde la perspectiva práctica, esta investigación tuvo la finalidad de proporcionar datos a partir de la realidad observada acerca de salvaguardar las redes y la protección de la información que transita por el CECOM de la 32ª Brigada de Infantería, orientando al personal responsable de la instalación y operación, así como efectuar estrategias necesarias para el desarrollo de la seguridad de la redes, que van a resultar producto del presente estudio, ya que estos frutos pueden servir como sustento para otros investigadores que quieran ampliar el tema de estudio.

1.2.2 Justificación teórica

Este estudio es trascendental, ya que se consiguió brindar una contribución teórica beneficiosa para la argumentación de innovadores planeamientos con diseños renovadores que inciten el raciocinio, la discusión y la averiguación acerca de las comunicaciones militares, expresamente respecto al accionar de la Compañía Comunicaciones N° 32 en el AF- 2022, en la protección del CECOM que opera dicha unidad de Comunicaciones.

El estudio permitió analizar diversos conceptos relacionados a las operaciones cibernéticas y seguridad de redes, en este contexto de la información, permitió mejorar la cultura de seguridad informática la cual involucró dimensiones físicas, lógicas y humanas y las capacidades existentes de las organizaciones de comunicaciones responsables.

Mediante el vigente estudio se trató de encontrar evidencias que permitirá aportar con calidad y eficacia a la gestión de la red de datos del CECOM, a cargo de la Compañía Comunicaciones N° 32, en sus diversas plataformas de trabajo. Se intentó cubrir un vacío del

conocimiento en nuestra Institución por la inexistencia de una doctrina concreta que, valga como modelo al comando e integrantes de la Compañía Comunicaciones N° 32, durante el desarrollo de su gestión. Desde la perspectiva teórica, esta investigación creó gnoseología, sobre el conocimiento que se tiene en las comunicaciones militares, porque se realizó una comparativa con diversas teorías en las ciencias militares, fundamentalmente acerca del empleo de la Compañía Comunicaciones N° 32.

Este trabajo de investigación es importante, porque propuso una contribución teórica ventajosa, el cual permite entregar argumentos sólidos, sobre los procedimientos como alternativas de solución, para salvaguardar la red de datos que emplea el CECOM de la 32ª Brigada de Infantería. De esta manera, se dio la génesis en la investigación en la GUC, que permitió garantizar el uso del ciberespacio por los operadores de comunicaciones. Con el aporte que se logró, se espera poder proporcionar y contribuir a mejorar salvaguardar los datos que, se manejan en las redes que, opera el CECOM de la GUC y de la información reservada que recorre en ella.

1.2.3 Justificación metodológica

Desde la perspectiva metodológica, contribuyó con herramientas de recojo de datos previa validación y confiabilidad, en vista que, se administró un instrumento explícito, a cerca de la seguridad en la red de datos, que debería implementar esta GUC. Es útil para otros exploradores del norte, ya que brindó información y consejos sobre el problema encontrado.

El vigente estudio ayudó al esclarecimiento de la vinculación entre las categorías estudiadas, determinándose la relación que existe entre ellas, para mejorar las acciones propensas a lograr la seguridad de redes de datos de la 32ª Brigada de Infantería en defensa de la información que por ella transita en su CECOM. La presente investigación propone cómo estudiar adecuadamente la población definitiva en la 32ª Brigada de Infantería, en lo referente a la defensa de la red informática del CECOM para resguardar la información reservada que por ella viaja, mejorando la seguridad informática que debe existir.

1.3 Delimitación de la investigación

1.3.1 Delimitación espacial

La indagación de información abarcó el ambiente geográfico en la capital de La Libertad - instalaciones del Cuartel Ramón Zavala – Instalaciones de la Compañía Comunicaciones N° 32.

1.3.2 Delimitación temática

El concepto vertido en el vigente trabajo de investigación trató sobre la protección de la red de informaciones del CECOM que opera la Compañía Comunicaciones N° 32.

1.3.3 Delimitación temporal

El trabajo involucró el tiempo desde el 01 de setiembre de 2022 hasta el 01 de setiembre de 2023.

1.4 Limitaciones de la investigación

No hubo grandes impedimentos para llevarse a cabo este importante trabajo, toda vez que se aprobó las respectivas autorizaciones para obtener la información documentada como el acceso a la instalación militar, asimismo, se dispuso de los recursos financieros necesarios. No obstante, estas han tenido ciertas restricciones con respecto al tiempo, puesto que, al estar realizando simultaneas asignaturas en la Escuela Superior de Guerra, que pertenece al Comando de Educación y Doctrina del Ejército, ubicado en el distrito de Chorrillos, el tiempo disponible para efectuar el recojo de datos fue restringido, recurriéndose a algunas herramientas informáticas para poder hacer ciertas acciones en modo virtual y presencial empleando todos los medios disponibles con lo cual fue posible mitigar estas limitaciones logrando alcanzar todos los objetivos de la investigación, siendo considerado factible.

1.5 Formulación del problema

¿Cómo es el funcionamiento de la seguridad de red de datos en el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022?

¿Cuáles son los ataques informáticos que pueden afectar el funcionamiento de la seguridad de red de datos del Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022?

¿Cuáles son las políticas y controles de seguridad informática que posee el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022?

¿Cuáles son las capacidades de Ciberdefensa que debería poseer en cuanto a seguridad de red de datos el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022?

1.6 Objetivos de la investigación

Analizar el funcionamiento de la seguridad de red de datos en el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022.

Describir los ataques informáticos que puedan afectar el funcionamiento de la seguridad de red de datos del Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022.

Identificar las políticas y controles de seguridad informática que posee el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022.

Proponer las mejoras de las capacidades de Ciberdefensa que debería poseer en cuanto a seguridad de red datos el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022.

Capítulo II. Marco teórico

2.1 Antecedentes de la investigación

2.1.1 Antecedentes nacionales

Villarrubia (2021), presentó una investigación cuyo título fue *"*Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la región Lima, 2018", en el Centro de Altos Estudios Nacionales, para aspirar al grado académico de Maestro en Desarrollo y Defensa Nacional. El trabajo fue desarrollado con una perspectiva cualitativa, y el objetivo general buscó la defensa de la información de los centros de datos que se tiene en el Cuartel General del Ejército, y de los otros Institutos Armados, encuadrada en ciberseguridad intrínsecamente en la Política de Seguridad y Defensa Nacional. La población estuvo conformada por especialistas del Centro de Informática y Estadística del Ejército del Perú hizo uso de una entrevista semiestructurada gestionando con diez (10) personas conocedoras del tema. Su conclusión fue que:

> Preexiste una concreta salvaguardia de la información digital que transita por las redes de las instalaciones que, manejan los datos informáticos en nuestra institución como de otros institutos armados, la cual sería sensible ante las amenazas y los respectivos ciberataques por las debilidades en las medidas de ciberseguridad. (p.32)

La recomendación fue que "El Ejército del Perú opte por capacitar a personal especialista en lenguajes de programación y el desarrollo de un propio software de tal manera incrementar las capacidades de ciberseguridad". Se consideró este trabajo, como un antecedente porque realiza un estudio de la seguridad de las redes informáticas en los Institutos Armados.

Carrillo y Zapata (2020), presentaron una tesis titulada "La Ciberdefensa en el Sistema de Mando y Control de la 9ª Brigada Blindada" para conseguir ser Maestros en Ciencias Militares de la Escuela Superior de Guerra del Ejército – Escuela de Postgrado. El abordaje utilizado fue de enfoque cualitativo. Su objetivo general fue conceptualizar la Ciberdefensa en el ejercicio del comando y control de la 9ª Brigada Blindada, teniendo como referencia la implementación de la ley de Ciberdefensa, para protegerla de amenazas o ataques cibernéticos. Como conclusión principal se arribó que, "Es fundamental optimizar las capacidades militares de Ciberdefensa para proteger la información de los sistemas de mando y control de la 9ª Brigada Blindada, que va permitir hacer frente a los riesgos de seguridad cibernética" (p.15).

Se consideró el presente estudio, porque hace referencia a las capacidades de Ciberdefensa que debía alcanzar la 9ª Brigada Blindada para preservar su sistema de Comando y Control.

Saavedra (2020), formuló una tesis denominada “Defensa Nacional del Perú y el Análisis del Sistema de Seguridad, para la escuela de Postgrado en Ciencias Militares, utilizó una perspectiva cualitativa, siendo el propósito integral de este estudio, optimar y establecer la situación vigente del Sistema de Seguridad y Defensa Nacional en el desarrollo de sus funciones, a fin de exhibir una propuesta factible al Ministerio de Defensa que posibilite progresar la existente eficiente tarea del Sistema de Seguridad Nacional, con relación al logro total de sus funciones. La conclusión se orientó en la propuesta innovadora, a través de la confección de un Proyecto de Inversión Pública para optimar el Sistema de Seguridad y Defensa Nacional, ya que existe una perentoria exigencia de formar cuadros de expertos en la civilidad, en asuntos de Seguridad Nacional (p. 12).

Se tomó este trabajo como un antecedente, porque considera a la seguridad, como un factor preponderante en la Defensa Nacional y por ende en todas las actividades que lo conforman.

Ochoa (2019), confeccionó una tesis denominada “Diseño de una Red de Seguridad Informática para la Protección del Sistema Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO 27033”, ante la Universidad de Ciencias Aplicadas, Lima, Perú, para conseguir el título de Licenciado en Ingeniería de redes y Comunicaciones, la tesis se realizó con un enfoque cualitativo, dicho estudio, tuvo como objetivo fundamental el presentar un esbozo de una Red de Seguridad Digital que sirva para la salvaguardia del Sistema Web del Call Center, con el objeto de incrementar la capacidad del sistema. Asimismo, busca disminuir las debilidades tecnológicas de la entidad con relación a la protección de la red de datos y, finalmente, se orienta a aumentar significativamente la protección de la red de datos del Call Center. En última instancia, concluyó que: el primordial instrumento utilizado para materializar las medidas que permitan acrecentar la seguridad de la red de datos, con la norma ISO 27033, basada en manejo de riesgos, que pueden fortalecerse con otras medidas, y que el patrón puede ser usado por cualquier organización sea o no del mismo rubro (p.26).

Se tomó el vigente estudio como un antecedente, porque considera la seguridad como un elemento a tener en cuenta siempre en la seguridad de las redes informáticas, resultó fundamental para la realización del presente estudio.

Rivera (2019), formuló una tesis denominada “Riesgos de Ciberseguridad y sus Consecuencias en la Prevención de Fraudes en las Empresas Industriales del distrito de Yanacancha”, para adquirir el grado de Maestro, la investigación se realizó bajo una perspectiva cualitativa, siendo el propósito integral de este trabajo, proponer métodos de

> ciberseguridad para la prevención de amenazas informáticas que, puedan derivar en fraudes en el distrito de Yanacancha, en lo que refiere a las empresas existentes en esta latitud del país, que permiten la protección de las redes informáticas del sector privado asegurando su normal funcionamiento en seguridad. Su conclusión se orientó a la importancia de proteger los datos que, transitan en ciberespacio, así como, resguardar la información que manejamos en cada una de nuestras redes informáticas (p.12).

El presente estudio se consideró por tener temas como de ciberseguridad, elemento esencial para que las tareas cotidianas se desarrollen con normalidad en el distrito de Yanacancha.

2.1.2 Antecedentes internacionales

> Álvarez (2022), presentó una tesis llamada “Implementación de una arquitectura de red, como aporte a la gestión de seguridad informática del hotel "San Pablo" de la provincia de Santa Elena”, Guayaquil - Ecuador, graduándose como Licenciado en Sistemas de Información. Tuvo un enfoque cualitativo y su cardinal propósito fue el brindar a los usuarios una apreciable y eficiente conexión a internet. Como primordial conclusión se llegó a determinar que los resultados de las pruebas demostraron que el proyecto es viable, para el uso de redes privadas virtuales, por medio de las técnicas de preparar, planear, diseñar, implementar, operar y optimizar (p.28).

Se consideró este trabajo de investigación como un antecedente, porque toma en cuenta a la seguridad como un elemento a considerar permanentemente en el funcionamiento de las redes, que es uno de los aspectos a desarrollar que se ha tenido en consideración en el estudio.

> Pérez y Ramos, (2020) formularon la tesis denominada “Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas”, para ambos obtener el grado de Maestro en Estrategia Militar Terrestre en la Universidad de las Fuerzas Armadas de Ecuador, la perspectiva utilizada fue de enfoque cualitativo, siendo el propósito integral de este trabajo, el de proponer una política de seguridad digital para el manejo de las redes informáticas para el empleo de las Fuerzas Armadas Ecuatorianas, con los estándares internacionales de seguridad, acorde a las constantes apariciones de amenazas informáticas, y a la vez se realizó este trabajo de una manera articulada con las demás instituciones del estado (p.26).

Su conclusión se orientó a la importancia de desarrollar políticas de seguridad informática en un trabajo en conjunto con las demás instituciones que tiene el estado ecuatoriano pues la seguridad es integral y la información debe protegerse en todos los espacios donde transita, considerando al ciberespacio como una dimensión más del desarrollo de actividades humanas

como del campo de batalla. Se tomó este trabajo como un antecedente, porque consideró fomentar políticas de seguridad informática como parte de un engranaje del estado ecuatoriano para protegerse tanto de amenazas internas o externas que, pudieran darse en el ciberespacio en provecho del desarrollo de las Fuerzas Armadas Ecuatorianas.

> Albarracín (2019), formuló una tesis denominada “Inteligencia Nacional y Estrategia de Ciberseguridad Nacional”, para adquirir el grado de Maestro en Ciencias Jurídicas, la investigación se realizó bajo una perspectiva cualitativa, considerando como propósito principal la de iluminar y entender el progreso de la actividad criminal por redes cibernéticas en el país de Colombia, con la finalidad de identificar riesgos y amenazas para hacer frente a esta modalidad de actividad criminal (p.35).

Su conclusión se orientó a aprovechar las capacidades que, nos ofrece la inteligencia nacional en lo que se, refiere fundamentalmente a la explotación positiva de cada ciclo de la inteligencia, conjugando esfuerzos con las capacidades que, nos ofrece la ciberseguridad para de esta manera minimizar las actividades delincuenciales en el ciberespacio. Se tomó este trabajo como un antecedente, porque consideró la sinergia de capacidades de génesis militares para hacer frente a un problema nacional en relación a la ciberseguridad, como un factor que viene, afectando las actividades de los organismos gubernamentales, privados y personas naturales en Colombia.

> Rincón et al. (2022), elaboraron un artículo científico, denominado “Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos?” En la revista Criminalidad, de la República de Colombia. Fue una investigación descriptiva con un enfoque cualitativo respaldada por los métodos de revisión documental y triangulación de datos en relación a la ciberdelincuencia en dicho país. Tuvo como objetivo fundamental el analizar los factores que, afectan a los delincuentes informáticos a partir de la promulgación de la Ley de Delitos Informáticos, para posteriormente determinar el comportamiento de dichos delincuentes (p. 36).

Finalmente se tuvo al final del estudio una conclusión que podemos ver lo importante que resulta proteger los sistemas informáticos siendo estos una parte esencial para la vida moderna en tareas cotidianas y económicas de una nación, ante esta situación se promulgó la Ley de delitos informáticos para mitigar el nivel de amenaza para la sociedad colombiana. Se tomó el presente artículo científico como un antecedente, porque toma en cuenta a la seguridad informática como un elemento a considerar permanentemente en la seguridad de las redes, siendo este uno de los aspectos a desarrollar en el presente estudio.

> Svintsytskyi (2022) elaboró un artículo científico, denominado “El sistema de organismos de ciberseguridad en Ucrania” en la revista científica “General José María Córdova” Criminalidad, de la República de Colombia. Se hizo la vigente investigación descriptiva con un enfoque cualitativo respaldada por los métodos de revisión documental y entrevistas. Teniendo como objetivo fundamental: analizar los métodos utilizados para realizar la ciberseguridad de manera exitosa, teniendo como referencia los hechos suscitados en Ucrania (p.16).

Se obtuvo de este estudio algo muy claro que resultó en que el tema de la ciberseguridad debe ser holística e integral donde deben participar todos los niveles de gobiernos e incluso a nivel internacional entre estados, para poder tener una seguridad solida de un solo lenguaje que, asegure el funcionamiento en seguridad de nuestras redes informáticas. Se tomó el presente artículo científico como un antecedente, porque toma en cuenta a la ciberseguridad como principal componente para el funcionamiento de las redes informáticas en todos los niveles de gobierno en relación a la garantía de que la información es confidencial, integra y disponible, siendo este uno de los aspectos a desarrollar en este estudio en curso.

2.2 Bases teóricas

2.2.1 Teoría general de sistemas

Fue planteado por Gutiérrez (2013), esta teoría general de sistemas nos ayuda a entender y nos aproxima en una forma holística precisar el estudio de los sistemas y su aplicación en cualquier contexto de la vida. La teoría de sistemas, en forma general, consiste en el estudio desde la óptica de distintas disciplinas de los sistemas. Su propósito es aprender los principios adaptables a los sistemas en distintos rangos en cualquier campo de la investigación. Un sistema se puntualiza como una entidad que tiene fronteras y con elementos interconectados e interdependientes cuya adición es más a la unión de sus partes. La modificación de una parte del sistema influye en los demás componentes y consiguientemente al sistema total, forjando patrones predecibles de desempeño. El desarrollo efectivo y el ajuste de un sistema residen en cómo se adapta este a su ambiente. Además, casi siempre, coexisten para cumplir un objetivo usual, que también favorece al mantenimiento del sistema y a evitar sus deficiencias.

El propósito de esta teoría es el develamiento metódico de los procesos, limitaciones y condicionantes de un sistema, así como de fundamentos, propósitos, acciones, metodologías empleadas, instrumentos, etc., que puedan ser discutidos y llevados cabo en los procesos de los sistemas en cualquier rango y en cualquier área, con el fin de obtener una equivalencia y un objetivo optimado. Por ende, un sistema, como son las redes de comunicaciones se encuadra dentro de la teoría general de sistemas.

2.2.2 Teoría matemática de la comunicación

La ciberseguridad, desde la perspectiva de la teoría de las comunicaciones, de Shannon y Weaver (1948) puede definirse como:

> El conjunto de medidas y tecnologías diseñadas para asegurar la correcta transmisión de información a través de medios digitales, protegiendo la integridad, confidencialidad y disponibilidad de los datos frente a posibles interferencias, o “ruidos”, que incluyen amenazas cibernéticas como el malware, el phishing, y los ataques de intercepción. (p. 134)

Al igual que el "ruido" en el modelo clásico de comunicaciones distorsiona o destruye el mensaje, los ciberataques interrumpen o modifican la información digital, poniendo en peligro el flujo seguro de datos entre emisor y receptor. En este sentido, los principios de codificación (cifrado) y canales seguros juegan un papel crucial en la comunicación moderna, ayudando a mitigar el "ruido" generado por los atacantes y asegurando que la información llegue de manera confiable y segura al destino previsto.

El estudio de la ciberseguridad bajo el enfoque de la “teoría de las comunicaciones” permite comprender cómo los ataques cibernéticos representan formas modernas de ruido que alteran la comunicación digital. A través de herramientas como el cifrado, la autenticación y el uso de protocolos seguros, las organizaciones pueden mitigar estos riesgos y garantizar la protección de la información. En la medida en que la interconexión digital sigue creciendo, la aplicación de los principios de la teoría de las comunicaciones sigue siendo vital para el diseño de sistemas de seguridad robustos, orientados a preservar la integridad y confidencialidad de los datos. Por lo tanto, es fundamental que el desarrollo de la ciberseguridad no solo se enfoque en la tecnología, sino también en la correcta implementación de estos principios, asegurando que la comunicación digital continúe siendo segura y confiable en un entorno cada vez más amenazante. Diversos estudiosos, han tratado sobre el tema, en continua discusión sobre la identidad científica y los paradigmas de la investigación en comunicación, Donsbach (2008), merece ser recordado por manifestar que, “La extensión y ambición de sus objetivos sostienen un debate en curso sobre la identidad académica y los paradigmas de investigación en comunicación debido a sus ambiciosos objetivos” (p. 56).

2.2.3 Teoría de la información

La Teoría de la Información, desarrollada por Claude Shannon (1948), se centró en la cuantificación, almacenamiento y transmisión de información. Dentro del marco de esta teoría, la ciberseguridad puede entenderse como el proceso de garantizar que la información digital, medida en términos de entropía y redundancia, sea transmitida de manera segura, sin que su

integridad, confidencialidad o disponibilidad se vean comprometidas por la interferencia de agentes externos. En este contexto, el ruido en el canal de comunicación es una metáfora para los ataques cibernéticos, mientras que la redundancia en los sistemas de información es una estrategia clave para garantizar la recuperación y corrección de errores provocados por dichos ataques. El cifrado y los algoritmos de corrección de errores, inspirados en esta teoría, son fundamentales para asegurar que los datos mantengan su valor informativo a pesar de las amenazas.

El enfoque de la Teoría de la Información ofrece una base matemática sólida para entender cómo la ciberseguridad, se centra en la protección de los datos durante su transmisión y almacenamiento. Desde la perspectiva de Shannon, el objetivo principal de la seguridad digital es minimizar el "ruido" o las interferencias que los ciberataques pueden generar, garantizando que la información llegue al destinatario de manera precisa y sin pérdidas. Aplicar los conceptos de entropía y redundancia permite desarrollar estrategias efectivas de ciberseguridad, ya que buscan maximizar la cantidad de información útil transmitida y minimizar el impacto de las amenazas. Por lo tanto, el estudio de la ciberseguridad, basado en la Teoría de la Información, resalta la importancia de crear sistemas resilientes, capaces de mitigar ataques y recuperar la información de manera eficiente, protegiendo así el activo más valioso en la era digital: Los datos.

2.2.4 Teoría de la seguridad en las comunicaciones

Aguado (2004), planteó la teoría de seguridad de las comunicaciones como una parte notable de las comunicaciones actuales cómo son las redes y los sistemas de información. Nuestra casi total sumisión a las tecnologías de la información y las comunicaciones, resulta incuestionable, siendo evidente el progresivo avance de Internet en nuestra economía y su impacto en las redes sociales, inclusive superando las vinculaciones propias. Podemos expresar entonces, que el progreso tecnológico de las tecnologías de la información y las comunicaciones, está produciéndose una evolución rápida en las comunicaciones en las últimas décadas. Las enormes primacías y beneficios de las tecnologías de la información y las comunicaciones, están presentes en nuestras vidas.

En el momento que, nuestras vidas se están transmutando a magnitudes significativas de información, siendo uno de los mayores desafíos para la tecnología, el resguardo de las mismas. Esta noción simboliza la salvaguarda de los capitales preciosos propios de una entidad: sean instalaciones, personas, hardware, software, mobiliario, datos, etc. Aunque, como anotamos, se trata de un propósito formidable y, en consecuencia, de no fácil realización y obtención, por tanto, debe ser convenientemente atendido por todos los encargados, con la finalidad de asegurar la forzosa confianza en la sociedad de la tecnología. La prelación del asunto se hace notoria a

través de varias acciones que, se han realizado en los últimos años por diversas organizaciones en todo el mundo. Con la dinámica que, comprenderse la situación actual, cuyo propósito es formar a expertos en el sector tecnologías de la información y las comunicaciones, en la ciberseguridad. Así, en este ámbito formativo comienza a ser reconocido como de preocupación en las diversas entidades.

2.2.5 Teoría de red de datos

> Se fundamenta en el conjunto de dispositivos interconectados físicamente, vía cableado o vía inalámbrica, que emplean los pulsos eléctricos, transmisiones electromagnéticas o cualquier otra tecnología para la transferencia de datos, a fin de usar mancomunadamente medios (hardware y software), información y servicios. Que se interconectan entre sí a través de normas (protocolos) de comunicación (Galloway, 2007, p. 67).

2.2.6 Teoría de la comunicación de riesgo

Iglesia (2012), mediante la teoría de la comunicación de riesgo especificó que la injerencia comunicativa entre varias sociedades de comunicación. La comunicación de riesgo se considera como el espacio donde el riesgo obtiene un sentido mediante la disputa sobre la probable amenaza o sus consecuencias asociadas (p. 65). Por tanto, la exposición del riesgo de la comunicación se convierte forzosamente en la explicación de los procedimientos de comunicación de riesgo, entendidos como las distintas intervenciones notables entre las sociedades de comunicación. En consecuencia, los procesos de comunicación de riesgo involucran, entre otros, las campañas corporativas de información, la propaganda institucional o las tácticas informales de la percepción del riesgo.

Por consiguiente, la mundialización del riesgo se transforma paralelamente en el globalismo de su comunicación a través de los instrumentos digitales. Las diversas sociedades de comunicación de riesgo perseveran para hacer perceptibles sus tesis, evolucionando el ambiente comunicativo y, por consiguiente, el total de los procesos de comunicación. Los estudios realizados acerca de los recursos habituales y su impacto se sitúan en una visión mucho más amplia y complicada de interrelaciones.

2.2.7 Teoría de la seguridad de la comunicación

Según Serrano (2009) la Teoría de la Comunicación, nos entregó estrategias de defensa de los datos que, realizan las entidades para el resguardo de sus datos, siendo pieza clave en esta estratagema el factor humano como principal ente de seguridad para la información de las redes o sistemas de comunicaciones (pp. 67- 68).

Los distintos papeles que realizan los individuos, tendrán un impacto y resultado distinto para cada caso. Se ha determinado, que las teorías más evidentes, que los investigadores emplean en sus estudios, respecto a la obediencia de las políticas de seguridad, están destinadas a entender la conducta de los sujetos, mediante de teorías anímicas o sociales, lo cual conlleva a poseer una perspectiva de diversas disciplinas, que permitan una visión integral, y no solo tecnológica. Es una manera más ordenada de educarse acerca de los procesos de protección de información que adoptan los Estados, destinado al sector político-militar en un determinado ámbito, teniendo en cuenta una cierta autonomía del sistema integral, ya que la interacción en cada región de los Estados es palpablemente más extensa entre ellos.

2.2.8 Principios para la organización de una red de comunicaciones

De acorde con el Manual de Doctrina Operacional de Comunicaciones y Procedimiento de las Fuerzas Armadas (1989) sugiere los siguientes conceptos.

2.2.8.1 Confiabilidad. Es la situación de seguridad que brinda un sistema para asegurar y sostener las comunicaciones en forma permanente. La mejora de dicho sistema debe tener en cuenta las demandas operativas y administrativas en todos los escalones del Instituto. Los equipos principales y secundarios de comunicaciones deben operar en toda circunstancia climatológica que se presente dado en el tiempo, espacio y lugar, inclusive en ambiente electromagnético hostil, es decir de Guerra Electrónica (p. 45).

2.2.8.2 Simplicidad. Circunstancia de entendimiento fácil que, permita obtener el mayor beneficio al Sistema de Comunicaciones, el cual debe diseñarse de manera inteligente para su conducción y sostenimiento. Debe ser un Sistema que permita empeñar menor cantidad de personal y medios, haciéndolo más adaptable a las exigencias operativas. Se debe disponer de personal entrenado, capacitado, manuales y herramientas adecuadas (p. 67).

2.2.8.3 Seguridad. Debe asegurarse el resguardo de los equipos de comunicaciones, contra las diversas amenazas existentes en el espectro electromagnético, por parte de personal ajeno al sistema (p.71).

2.2.8.4 Rapidez y oportunidad. El tráfico de información deberá hacerse en tiempo real, concordante a la situación táctica, a fin de garantizar el éxito pronosticado. La corriente de la información debe garantizarse y realizarse con calidad en el momento pertinente en provecho de decisiones acertadas y la progresión de acciones que demanda las operaciones y acciones castrenses, que coadyuven a la consecución exitosa de una misión (p.81).

2.2.8.5 Flexibilidad. Es adaptarse rápidamente a los cambios de situación. Para poder desenvolverse eficientemente es necesario emplear la tecnología, para lograr una estructura de comunicaciones eficiente. Los equipos principales y secundarios de comunicaciones deben tener la autonomía suficiente de trasladar las subestructuras correspondientes, así como de un despliegue rápido de sus medios, la flexibilidad se logra por medio de una adecuada gestión de acuerdo con la situación que se presente (p. 98).

2.2.8.6 Interoperabilidad. Deben poseer la aptitud de vincularse entre redes de comunicaciones de las Instituciones Armadas, en los diferentes escalones, sean subordinados o no, en todos los niveles. Igualmente, con las entidades e Instituciones que sean precisas. La estandarización e integración de los medios de comunicaciones de los Institutos Armados, permitirá conducir la operaciones y acciones castrenses que, se desarrollen a partir de un sistema de comunicaciones integrado con todos los actores del ambiente operacional (p. 99).

2.2.8.7 Seguridad de las redes de comunicaciones. El vocablo seguridad señala una circunstancia o un estado que se intenta alcanzar con la inexistencia de amenazas para un contexto determinado. La seguridad es un concepto divulgado en las relaciones universales y ha sido una inalterable aspiración de los pueblos el llegar a conseguirla. Tiene varias concepciones y significados, su significado obedece a la conducta del representante con respecto a cómo siente las amenazas, sean existentes o ficticias. Diversas posturas filosóficas y académicas redelinean permanentemente la definición de seguridad, con respecto a los sucesos históricos y puesta en ejecución de los actores, sean nacionales e internacionales, por ello se certifica que la principal peculiaridad de la seguridad, es su constante evolución. A los riesgos y amenazas que se conocía tradicionalmente se han adicionado nuevos de naturaleza transnacional que, unidos a los potenciadores, impactan en la seguridad estatal. Las amenazas son sucesos que representan un riesgo potencial a la entereza física o mental de un sujeto, grupo de personas o de una nación, así como estructuras críticas. También es una manera de agresión, declarada que viola la seguridad, sea en cualquier sentido que se dirija (p. 101).

Las amenazas a las comunicaciones, constituyen diligencias o acciones que son determinadas como una circunstancia de riesgo, en que un elemento puede impactar negativamente en nuestra seguridad, las amenazas se determinan el respectivo Plan de Comunicaciones y son el ingrediente básico para formular las Políticas de Comunicaciones.

El efecto de la globalización que va junto a la tecnología, está acarreando grandes provechos a las entidades de cualquier índole, pero igualmente están originando enormes

dificultades de seguridad y de salvaguardar datos, las que deben ser superadas por las diversas entidades. La ciberseguridad es un evento de gran impacto en este escenario en el mundo, la productividad científica es escasa; lo que dificulta realizar indagaciones profundas de la situación en el escenario castrense; sin embargo, al ser, la ciberseguridad, un aspecto que atañe a todo tipo de entidad, pueden llevarse las posibles amenazas al ámbito militar.

2.3 Categorías y sub categorías apriorísticas

Las categorías y sub categorías apriorísticas que se han presentado en el estudio por las cuales se determinó del análisis inductivo, realizado preliminarmente, que son las que se enuncian a continuación, de acuerdo a la Tabla 1.

Tabla 1

Categorías y sub categorías apriorísticas

Categoría	Definición	Sub Categorías	Definición	Patrones
Seguridad de la red de datos.	Medidas y acciones de seguridad tendientes a dar protección a la red de telecomunicación	Políticas y controles.	Grupo de normas que se rigen a las actividades de protección de los sistemas y medios de comunicaciones de una determinada organización.	Equipos satelitales Equipos de microondas Equipos de radios Equipos de telefonía IP
		Vulnerabilidades	Son los intentos que pueden llevar a cabo los hackers para obtener acceso sin autorización a nuestros datos.	
			Consisten en debilidades o mal funcionamiento de los sistemas informáticos que pueden ser explotados y aprovechados por actores malintencionados, comprometiendo así la protección de la información.	Sistema de Comando y Control Puesto de Comando
Centro de Comunicaciones de la 32a Brigada de Infantería.	Establecimiento de comunicaciones administradora de la recepción, intercambio y entrega de los mensajes.	Amenazas	Son las acciones que son probables que realicen personas ajenas a nuestra red de datos, para obtener información privilegiada.	Empleo de radios. Empleo de telefonía IP. Empleo de microondas. Empleo de equipos satelitales.
		Operaciones ofensivas	Es un acto militar ofensivo realizada para cumplir una misión de carácter táctico o administrativo.	Acción defensiva de las Comunicaciones
		Operaciones defensivas.	Es un acto militar defensivo que, mantiene una actitud determinada en una situación táctica para generar condiciones favorables para la realización de una acción ofensiva.	Acción ofensiva de las comunicaciones

2.4 Definición de términos

2.4.1 Red de comunicaciones.

Consiste en la unión de dos o más infraestructuras de comunicaciones, terminales o repetidoras que viabilizan el enlace y mantenimiento de las comunicaciones entre los equipos de las unidades, desde el punto de emisión de la señal. Las redes de comunicaciones se emplazan y operan utilizando varios medios de comunicaciones. (CCFFAA, 1989, p. 4)

2.4.2 Seguridad de la red del centro de comunicaciones

Es cualquier gestión específica destinada a proteger la entrada y el empleo de la red de comunicaciones. Envuelve 1) Tecnologías de comunicaciones (hardware y software), 2) Se encamina a afrontar el total de amenazas, 3) Busca impedir que las amenazas ingresen o se irradien por la red y 4) Busca una seguridad de red poderosa que gestione el acceso a la red. (CCFFAA, 1989, p. 44)

2.4.3 Centro de comunicaciones

Infraestructura que gestiona y controla la transferencia de datos. Normalmente consta de un centro de mensajes, elementos criptográficos, infraestructura de transmisión y recepción. La estación transmisora, la estación receptora y la estación repetidora no están necesariamente ubicadas en el centro de comunicaciones, pero son monitoreadas por este. (CCFFAA, 1989, p. 23)

2.4.4 Centro de mensajes

Es parte integral del CECOM y es responsable de recibir, distribuir y gestionar la data enviada o recibida a través de las plataformas de comunicación a cargo del Centro de Comunicaciones. (CCFFAA, 1989, p. 44)

2.4.5 Comando, control, comunicaciones, computadoras e inteligencia (C4I)

Sumatoria de componentes y cuestiones doctrinarias establecen la unificación, modos estrategias, infraestructura, equipamiento, comunicaciones, tecnología informática y aspectos de inteligencia. También, incluye sistemas de defensa y aviso de misiles, los cuales utilizan sensores conectados a objetos terrestres. C4I proporciona datos fácticos oportunos a varios comandos en varios niveles para garantizar una eficiente sinergia en cada proceso y actividades que consisten de cientos de tareas ejecutadas. Es el medio por el cual los líderes militares responsables de las operaciones comunican sus intenciones, ejercen el mando y control sobre las fuerzas militares subordinadas y difunden información relevante dentro de su zona de acción. (CCFFAA, 1989, p. 35).

2.4.6 Comando, control y comunicaciones (C3)

Definido como el ejercicio del mando militar con total comprensión de los subordinados, así como, el control, considera un grupo de normas y acciones encaminadas a controlar y dirigir las medidas emitidas por el comandante, donde la comunicación se refiere a la capacidad de establecer y mantener las comunicaciones necesarias entre las unidades subordinadas. (CCFFAA, 1989, p. 26)

2.5 Hipótesis

Se dejó de lado el diseño de una hipótesis durante esta investigación de corte cualitativo, toda vez que, se investigó desde la óptica subjetiva, sin plantear limitados precedentes, fundamentándose en la perspectiva y elucidación de los sujetos que han dado origen a la investigación y, en consecuencia, no hay mediciones posibles. Como dijeron Hernández y Mendoza (2018), “En el caso de estudios cualitativos, regularmente no se formulan hipótesis antes de recolectar datos. Su naturaleza es más bien inducir las hipótesis por medio de la recolección y el análisis de los datos” (p.124). Además, sí puede usarse como una orientación general para robustecer la orientación que tiene que perseguir el estudio, pero no es un compromiso metodológico emplearla (Monge, 2011).

Capítulo III. Método

3.1 Enfoque de investigación

El trabajo de investigación se desarrolló con un enfoque cualitativo teniendo en cuenta lo explicado por Hernández y Mendoza (2018), estos autores enfatizaron que “Para estudiar un fenómeno de manera sistemática, da lugar a una teoría y luego se debe “enfocar” esta. "En el mundo empírico para confirmar si esto está respaldado por datos y resultados" (p. 7). Colección de diversos materiales empíricos, estudios de casos; experiencia personal; introspección; historia de vida; entrevista; artefacto; texto de observación; histórico; interactiva y visual, que representa momentos y significados rutinarios y problemáticos en la vida individual, esta investigación se desarrolló a través de un enfoque cualitativo, que necesita ser analizado, comprendido y generalizado, considerando el entorno y procedimientos involucrados desarrollados, conociendo más específicamente, desde la percepción de la realidad del personal que integra la sección de comunicaciones y tiene experiencia y conocimiento, respecto de la seguridad de la red que debe tener en el CECOM de la 32 Brigada de Infantería, en cuanto a estándares, tácticas, técnicas y procedimientos de seguridad, lo que le permitirá brindar un apoyo eficiente y eficaz durante las operaciones y acciones militares.

La postura elegida posibilitó fijar las estrategias de manera flexible, dinámica, continua y permanente, de acuerdo a una variedad de actividades recíprocamente vinculadas, siendo necesario resaltar que un punto muy importante sobre estas estrategias es que no representó categorías estrictas; y no se tuvo que elegir entre ellas porque de ninguna manera fueron mutuamente excluyentes.

3.2 Tipo de investigación

El estudio es de tipo teórico – empírico por lo que la investigación militar cualitativa se realizó por su naturaleza con distintas disciplinas holísticas y el papel que cumplió el investigador, como de los sujetos participantes, buscó la imparcialidad, exponiendo e interpretando las interrelaciones, dado que se indagó un desarrollo de producto determinado, mostrándose que, con motivo de las preguntas de investigación, objeto de estudio y el contexto del problema.

Jiménez (2008) planteó que, “Los métodos cualitativos parten del supuesto básico, de que la sociedad está erigida por significados y símbolos. La subjetividad es un elemento crucial de la investigación cualitativa y punto de inicio para absorber intencionadamente los significados sociales” (p.1). La realidad social así interpretada, está conformada por significados afines de manera subjetiva. Desde el punto de vista subjetivo, lo objetivo es lo que se atribuye a la acción.

3.3 Método de investigación

El método hermenéutico-interpretativo es consecuente con el tipo de investigación teórico - empírico, toda vez que, se orientó a enfatizar en preguntas sobre nuevas generalizaciones ambientales, sociales y militares, basadas en la experiencia del investigador y observaciones fácticas y de las opiniones de los participantes. Vélez (2001) afirmó:

> El camino para alcanzar una meta, sistema de principios (identidad, contradicción, exclusión) y normas (inducción) de razonamiento para establecer conclusiones en forma objetiva, la postura que, edificará este trabajo de investigación, el proceso cualitativo se cimentó metodológicamente en lo inductivo, para obtener teorías o fundamentos generales comunes a los hechos estudiados (p.124).

Como tal, la investigación lejos de manipular o controlar las categorías en estudio, se orientó hacia la definición de conceptos y argumentos vinculados, macizos sin contradicciones, que puedan afectar su creencia, tomando como base la literatura en consulta.

El Manual de Trabajos de Grado de Especialización y Maestrías y Tesis Doctorales (UPEL, 2005) lo definió como: “El estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos” (p.53). Lo que permitió disponer de un marco interpretativo adecuado. Con relación a los objetivos, el proceso cualitativo que se realizó, buscó entender y exponer las medidas de protección de red que debe poseer el CECOM de la 32ª Brigada de Infantería, durante las operaciones y acciones castrenses.

3.4 Objeto de estudio

Vargas (2011) dijo que: “La identificación del objeto de estudio dentro de este ámbito o circunstancia por el cual nos interesamos. Este puede ser empírico (edificios concretos, espacios, objetos, etc.), y/o teórico (un concepto, una idea teórica, etc.)” (p. 21). El trabajo de investigación, tiene como objeto de estudio, el análisis referido a salvaguardar la red informática, enfocada en la Compañía Comunicaciones N° 32, orgánica de la 32ª Brigada de Infantería– provincia de Trujillo. Siendo este el escenario de estudio, cuyos elementos son el personal militar del arma de comunicaciones que prestan servicio en esta compañía.

3.5 Muestra de estudio

La muestra del estudio estuvo conformada por la población de tres (03) Oficiales, cuyos puestos de trabajo fueron el de jefe de unidad, oficial ejecutivo y oficial de instrucción y entrenamiento (S-3) de la Compañía de Comunicaciones, además un (01) técnico quien se desempeñó como jefe del CECOM, y una (01) sub oficial como operadora de comunicaciones del CECOM, haciendo un total de cinco (05).

Para determinar la cantidad de la muestra se empleó la estrategia del muestreo por conveniencia, selección intencional y al respecto se puede decir que, en esta estrategia, determinados contextos, personas o actividades se eligieron intencionadamente para suministrar información que fueron específicamente aplicable a las preguntas para determinar la nominación de los sujetos a entrevistar, se consideró como perspectiva de inclusión y la pertinencia de la formación del experto; sus conocimientos y capacidades, referidos a la protección de redes de comunicaciones del CECOM de esta GUC.

3.6 Técnicas e instrumentos de recolección de datos

3.6.1 Técnicas

> Las técnicas de acopio de datos aluden a los métodos empleados para recoger diferentes datos. Las técnicas habituales de recojo de datos incluyen el examen de documentos relacionados con un tema en estudio, así como la realización de entrevistas y observaciones (Vargas, 2007, p. 35).

Considerando la situación planteada tras el estudio del tema, el trabajo de campo se permitió tener en cuenta el punto de vista del investigador, su experiencia, incentivos profesionales y su competitividad; lo que permitió formular en la práctica generalizaciones, perspectivas, problemas informáticos relacionados con el tema en estudio, así como establecer los significados de los problemas encontrados, teniendo en cuenta la percepción subjetiva de cómo los sujetos participantes distinguen la realidad presentada. Las técnicas que se emplearon en el estudio fueron: la observación no participante, la entrevista y el análisis documental.

3.6.1.1 Observación no participante. Este procedimiento permitió acopiar información referente al tema de nuestro estudio, como un veedor pasivo, limitando a registrar la información que apareció ante nuestros ojos, sin interacción, ni implicación alguna. Sin embargo, fue necesario buscar contactar a las personas más expertas de la unidad de comunicaciones visitada, para explicar las incertidumbres sobre los fenómenos observados y tomar notas en forma ordenada (Baena, 2017, p. 38).

En cuanto a la observación no participante se utilizaron hojas preparadas, realizando notas descriptivas sobre los resultados de la observación registrando conceptos interpretativos adecuados. Finalmente se llegó a estandarizar los tipos de anotaciones por ser de suma trascendencia.

3.6.1.2 Entrevista. Bajo esta técnica se realizaron cinco (05) entrevistas mediante las cuales se pudieron obtener percepciones y puntos de vista de los diversos expertos que se entrevistaron acerca del tema en estudio, en base a una guía de entrevista con preguntas abiertas, para que en base a sus experiencias y conocimientos profesionales emitan sus respectivas opiniones, además pudieron explayarse sobre los tópicos considerados en la entrevista (Baena, 2017, pp. 38-41).

3.6.1.3 Análisis documental. Nos posibilitó disponer de información documental con cierto nivel de lógica sobre la seguridad de red del CECOM de la 32ª Brigada de Infantería, y como es la actuación durante las operaciones y acciones militares, ayudaron a comprender el fenómeno en estudio, también permitió al investigador comprender el contexto de estudio, así como las experiencias o situaciones que ocurrieron en el entorno, sus actividades cotidianas y planificadas, así como los antecedentes para la elaboración de una doctrina operativa para el arma de comunicaciones (Baena, 2017, pp. 78-80).

3.6.2 Instrumentos

Son las herramientas que sirven para recolectar los datos. Los instrumentos de recolección de datos que se emplearon en la investigación, fueron los siguientes: Guía de observación, ficha de análisis documental y guía de entrevista semiestructurado, con preguntas abiertas en la cual los expertos entrevistados pudieron expresar libremente su opinión sobre los temas que se les planteo, con relación a la seguridad de red de datos del CECOM de la 32ª Brigada de Infantería (Hernández et al., 2018).

Respecto al análisis documental, se realizó un examen de contenido de los documentos incluidos en el marco teórico, con la finalidad de descubrir e interpretar el significado de los mensajes taxativos, a fin de ordenarlos y/o codificarlos en categorías y sub categorías.

3.7 Rigor científico

Hernández y Mendoza (2018) señalaron que:

> Lo que se busca en un estudio cualitativo es conseguir datos, que posteriormente se evolucionen en información sobre sujetos, otros seres vivos, colectividades, circunstancias o procesos, en las propias expresiones de cada unidad de muestreo. Al tratarse de individuos del género humano, los datos que nos atañen son perspectivas, percepciones, creencias, interrelaciones, experiencias, vivencias y roles revelados en la voz de los partícipes, ya sea de manera individual o grupal. Se recogen datos a fin de estudiarlos y entenderlos, y así dar respuesta, a las preguntas de investigación y producir sapiencias. Normalmente, estos datos están señalados en narraciones de distintos tipos: escritas, verbales, visuales, auditivas, audiovisuales. Este tipo de datos es muy

provechoso para comprender los impulsos profundos, las significaciones, las razones de la conducta humana (p. 443).

Los estudios cualitativos, por ser netamente de naturaleza interpretativa, se orientan a identificar, valorar y comprender los efectos y probables sesgos, durante el desarrollo del estudio, con el propósito de determinar las incongruencias dentro del ámbito de acción, respetando el fundamento básico de la coherencia interna, el que influye en el modo de establecer la arquitectura del estudio, vinculado con todos y cada uno de las cuestiones que la integran, basado en una eficiente interconexión con calidad, con el objetivo de entender la complejidad y extensión del proceso.

Para alcanzar su propósito, el investigador necesitó observar los resultados y hallazgos encontrados en retrospección, de forma tal de entender el estado del rigor científico, con que se confeccionó la investigación. Guba (1981) planteó que para lograr un adecuado rigor científico en la investigación existen por lo menos cuatros criterios fundamentales para lograrlo (p. 98).

3.7.1 Credibilidad

Consistió en la evaluación de las circunstancias, por medio de las que una investigación obtiene legitimidad como ser convincente, en base a una fundamentación factible que pudo ser comprobada en los productos de la investigación, acordes con su proceso de confección. En la vigente investigación, la credibilidad se amparará en los siguientes aspectos:

En la veracidad de los eventos que sucedan en la investigación, mediante las cuales se observará, examinará, valorará y dilucidará, la percepción de los Oficiales, Técnicos y Sub Oficiales en actividad de comunicaciones, respecto a sus conocimientos y experiencia profesional, acerca de salvaguardar las redes de datos del CECOM de la 32ª Brigada de Infantería, durante las operaciones y acciones militares, en cuanto a su normatividad, tácticas, técnicas y procesos, que le posibiliten suministrar un apoyo de calidad durante las operaciones. La valoración y ratificación del instrumento de acopio de datos de la investigación, por expertos militares y en el campo de la metodología.

Apreciación valorativa de los datos y/o información lograda por medio de los instrumentos de recojo de datos ejecutados, mediante los conocimientos profesionales y experiencias del entrevistador y entrevistados, particularmente en lo que concierne a la seguridad de red de datos del CECOM de la 32ª Brigada de Infantería, tema de nuestra investigación. La experiencia profesional a considerar, se estima sea entre los 02 y 05 años de tiempo de servicios de los sujetos de investigación considerados para ser entrevistados. El empleo adecuado de la triangulación de datos, como un procedimiento de comparación de técnicas, instrumentos e información obtenidos sobre el tema en estudio. Este proceso, en base al empleo de diversos

instrumentos de investigación, nos permitirá construir una gama de vínculos entre los hallazgos manifiestos y que serán debidamente ordenados, bajo esta perspectiva, la triangulación se realizó mediante:

3.7.1.1 Triangulación integral de instrumentos. Este proceso consistió en el contraste de la información obtenida por los instrumentos cualitativos elegidos. En el esquema, se tuvo en cuenta, el aporte de los instrumentos de acopio de datos escogidos, posibilitando la comparación necesaria de los datos conseguidos, con las técnicas, instrumentos y procesos de investigación del fenómeno en estudio, es decir de las entrevistas, de la observación no participante y del análisis documental.

3.7.1.2 Triangulación de sujetos. Se realizó con la finalidad de lograr solidez en los datos a conseguir en el progreso de la investigación, a partir de la óptica de los sujetos claramente implicados en el fenómeno en estudio, es decir los Oficiales, Técnicos y Sub Oficiales en actividad del arma de comunicaciones que prestan servicio en la Compañía Comunicaciones N° 32 de la guarnición de Trujillo, seleccionados para ser entrevistados, quienes con sus declaraciones posibilitó la obtención de distintas perspectivas interpretativas sobre el fenómeno estudiado, convirtiéndose en los pilares para lograr una aproximación de la realidad subjetiva.

3.7.1.3 Transferibilidad o aplicabilidad. Los productos que se obtuvieron en este estudio, no son transferibles ni aplicables a otros contextos y/o ámbitos de acción, dada la complejidad y la naturaleza de índole social del fenómeno en estudio son concretos. No obstante, puede ser considerado como un referente para generar instrumentos y fases, en otra investigación con una situación y/o contexto análogo, dependiendo de la proximidad, en cuanto a similitud del proceso desarrollado, de quien investiga y que desea producir con esa transferencia. Asimismo; se puede explicar que: La investigación interpretativa se preocupa más por la validez que por la fiabilidad, en cuanto a la estabilidad de los datos y su réplica.

Lo importante de la investigación es la capacidad de reflejar lo sucedido y percibido por los sujetos de esa situación particular y al mismo tiempo, apreciado como válido para la comprensión de su mundo y de ellos, como criterio de rigor científico en la actual investigación de abordaje cualitativo, la generalización, es el producto obtenido de una investigación, por medio de diversas técnicas de recojo de datos previamente seleccionadas, que posibilitó la interpretación de los resultados, vinculados con las propias necesidades y exigencias del estudio, dada la diversidad de dimensiones concurrentes y la flexibilidad de los conceptos y temas metodológicos inmersos en el estudio. En la presente investigación para indagar sobre su carácter científico, y en concordancia con el enfoque cualitativo se utiliza la metodología de validación científica sugerida por Guba (1981), que considera los criterios siguientes:

3.7.1.3.1 Descripciones detalladas. Emergen de las mismas transcripciones de los datos logrados en el análisis documental, entrevista y de los registros de observación, en otras palabras, con el propósito de producir información relevante lo más cercana a la realidad, se procuró de forma descriptiva y fidedigna, detallar la información relativa a los involucrados en el fenómeno en estudio, las circunstancias y a sus escenarios de actuación.

3.7.1.3.2 Amplio monitoreo de datos e información*:* En base a las entrevistas y los registros de la observación, efectuados a los Oficiales, Técnicos y Sub Oficiales en actividad de comunicaciones que sirven en la compañía comunicaciones N° 32, en el cuartel Ramón Zavala - Trujillo, año 2022, se obtuvo una gran cantidad de datos que permitió realizar la aproximación y compresión del tema en estudio.

3.7.1.3.3 Dependencia. Envuelve el grado de solidez de los resultados y descubrimientos obtenidos en el estudio. Siguiendo este criterio, el tema principal que guío la investigación fue el empleo de la compañía comunicaciones N° 32 orgánica de una Gran Unidad de Combate desde la óptica de los Oficiales, Técnicos y Sub Oficiales pertenecientes al arma de comunicaciones que sirven en esta unidad en la guarnición de Trujillo, año 2022, teniendo como criterio de inclusión sus conocimientos profesionales y experiencia personal. Los resultados que se encontró proporcionó una aproximación más cercana a la real situación de la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, año, 2022.

3.7.1.3.3 Confirmabilidad. El nivel de involucramiento del investigador, se constituyó como garantía idónea en el progreso de la investigación, toda vez que los datos obtenidos como producto de los instrumentos de acopio de datos a aplicar, no fueron expuestos a manipulación personal ni a ningún tipo de sesgo. La validez de esta aseveración, se confirmó en base a los textos documentales que se utilizó en el análisis y compilación de resultados, en los diversos puntos de vista de los entrevistados y lo que se registró en la observación. Asimismo, durante el progreso de la investigación, se efectuó siempre un procedimiento de raciocinio sobre el tema en estudio, con los sujetos inmersos en el estudio, lo que se incrementó en base a la peculiaridad reconstructiva y analítica de los instrumentos utilizados (entrevista y observación no participante), concretando la posición metodológica adoptada con relación al tema en estudio. Los datos se obtuvieron a través de la aplicación de los instrumentos seleccionados a los Oficiales, Técnicos y Sub Oficiales en actividad de comunicaciones que sirven en esta unidad en la guarnición de Trujillo, año 2022, lo cual fue revisado y aprobado en su totalidad por los sujetos inmersos en la investigación.

3.8 Técnica de procesamiento y análisis de datos

Partiendo del antecedente que el método de análisis y la síntesis se erigen en dos métodos complementarios, se recurrió a esta metodología, dado que se posibilitó aislar y estudiar individualmente las partes (categorías de investigación) de un todo (análisis) y también, luego de reunir los datos dispersos en forma metódica y razonadamente, estudiarlos en su conjunto (síntesis). Para desarrollar dichos procedimientos se empleó técnicas que guio el procedimiento de raciocinio a través de una guía de entrevista con preguntas abiertas, registro de datos de observación y fichas de textos, etc.

A pesar de la posibilidad latente de alejarse del enfoque global del estudio y que se generen inconvenientes para separar y mantener la información útil de la que no lo es, la propensión hacia el análisis, nos permitió considerar que fue posible lograr un alto nivel de penetración en el estudio. Asimismo, la síntesis nos proporcionó amplitud en la reflexión y pericia para fijar ideas, a pesar de que permanecer en ese punto podría involucrar una insuficiente penetración en el estudio. Consecuentemente, desde nuestra perspectiva, en el desarrollo del estudio, fue fundamental incluir metodologías de análisis-síntesis en forma reiterada, de modo tal, que los productos logrados fueron idóneos y coherentes con los objetivos de nuestro estudio. Para el desarrollo del análisis, así como de la síntesis, fue fundamental establecer los criterios a seguir, para evitar el desconcierto y la impresión de inconformidad sobre determinados aspectos, cuando en realidad lo que sucede es que los criterios empleados son distintos.

Por otra parte, la metodología que se empleó nos posibilitó arribar a una conclusión, como producto del análisis de los datos conseguidos, estudiados y planteando un esclarecimiento fiable del fenómeno por estudiar. Por otra parte, el análisis que se efectuó en el estribo de las categorías, se constituyó en un procedimiento flexible, ordenado y armónico, conciliando diversas perspectivas, conceptualizando, diseñando, probando, analizando y categorizando datos, para tratar de encontrar significancias mediante la definición o análisis de los datos logrados, para posteriormente a través de la síntesis, se emitió resultados en forma de: Descripciones, temas y patrones. El investigador se constituyó en el fundamental y exclusivo elemento del recojo de datos, utilizando la fenomenología y la teoría fundamentada, como métodos apropiados en la investigación con abordaje cualitativo del problema, de naturaleza inductiva, empleándose como técnicas de recojo de datos: La observación no participante, el análisis de contenido documental y la entrevista semiestructurada, basados en los temas/patrones apriorísticos.

Tomando en consideración, que existe un vínculo cercano entre la estructura de la muestra, la elaboración y la puesta en práctica del instrumento de acopio de datos, de responsabilidad total del investigador y su respectivo análisis, y que el recojo de datos se efectuó

en instalaciones y situaciones reales filados en el actual estudio, se señaló que los instrumentos elegidos aseguró un idóneo acopio de datos cualitativos ,los cuales fueron: la observación de contextos y circunstancias concretas, una entrevista a expertos previamente elegidos y el análisis documental de estudios relacionados a las categorías en estudio en la actual investigación. El análisis cualitativo consistió en organizar los datos recogidos, transformando y registrando en texto para luego codificarlos. Inicialmente con la codificación se buscó generar unidades de significado y categorías, y posteriormente surgió temas y vinculaciones entre ideas y conceptos, para finalmente generar hipótesis basadas en los datos obtenidos.

Respecto a la observación de escenarios y situaciones específicas se recurrió a la observación no participante, empero, en algunos casos se pudo acudir a los sujetos más experimentados sobre la materia de nuestro estudio, para aclarar ciertas dudas como resultado de la observación. En este proceso, los propósitos esenciales que se desarrolló fueron los siguientes: observación de contextos y situaciones concretas, entrevistas a expertos con sapiencias relacionadas al tema en estudio, análisis documental de estudios referentes al tema a investigar e identificación de problemas.

Para la inmersión inicial de la observación, se empleó solamente hojas acondicionadas previamente, de tal forma que una cara se anoten asuntos descriptivos producto de la observación, mientras que en la otra cara se registren aspectos interpretativos realizados por el investigador normalizándose los tipos de anotaciones por tener relevancia significativa. Con relación al rol del observador, es necesario resaltar su papel de intervención activa y completa. Se efectuó de esta manera a fin reducir la existencia de ribetes personales, así como para obtener diversos puntos de vista, apreciando directamente y personalmente en el ambiente y las situaciones donde se produce el fenómeno. En la observación cualitativa que se realizó, no se circunscribió solamente a establecer patrones y categorías apriorísticas, sino que consistió en un proceso iterativo, creando un diseño propio en el cual surjan nuevas categorías, temas/patrones, como producto de la aplicación de los instrumentos de acopio de datos. Según Vargas (2011), La validez científica de esta técnica se amparó en las reglas siguientes:

> a) El qué y el para qué se observó con respecto con el objetivo de la investigación, b) Definición y delimitación de la población y muestra cualitativa, inmersos en el área de estudio. c) Planeamiento de la participación y la capacitación del observador, que a la vez será el investigador. d) Identificación de las categorías por observar y el modo como se efectuó el registro de la información, elaborando una guía de observación adaptable para dicho efecto. e) Inclusión de los equipos y materiales en la recolección de datos: libreta de anotaciones, hojas para registros descriptivos y registros interpretativos, grabadora y

> cámara fotográfica. f) La totalidad de los registros de informaciones que se obtuvo fueron explotados de forma inmediata, con objetividad y responsabilidad (p. 87).

También, el empleo de la entrevista como otra técnica de acopio de datos, la misma, nos proporcionó la posibilidad de analizar, sintetizar, categorizar y entender las diferentes percepciones de los entrevistados y la manera como describen las categorías en estudio, así como el nivel de significancia que le asignan los sujetos inmersos en el fenómeno. Según Vargas (2011), se emplearon los siguientes criterios para elaborar el contenido de la guía de entrevista:

> a) Rango: Incluyó una gama de temas que faciliten la obtención de los datos deseados, así como otros adicionales. b) Especificidad: Los datos fueron concretos. c) Profundidad: Los datos recogidos son referentes a la seguridad de la red del CECOM de una GUC. Por tanto, las percepciones, opiniones, conocimientos y experiencia de los entrevistados sobre el tópico en estudio son de suma importancia. d) Entorno personal: Para la obtención de los datos, se tuvo en cuenta los conocimientos y experiencia profesional de utilidad en el área considerada del fenómeno en estudio. (p. 76)

La entrevista se inició en base a los temas/patrones de análisis considerados en la muestra, motivo por el cual la conversación con los entrevistados fue totalmente abierta, recabando sus opiniones, sus conocimientos y experiencias en forma amigable. Para desarrollar la entrevista se formuló una guía de entrevista semiestructurada en base a temas establecidos, sin embargo, las preguntas contenidas en dicho documento fueron totalmente abiertas y con dos propósitos: 1) Salvaguardar los aspectos prácticos, obteniendo y manteniendo la atención de los entrevistados, haciendo que se sientan cómodos durante la entrevista y 2) Resguardar los aspectos teóricos, por medio del logro de la información requerida y útil para comprender profundamente y a cabalidad el fenómeno estudiado. La información obtenida en base a los testimonios, así como las conclusiones que se generó, fueron registrados en el cuaderno de anotaciones. Para Vargas (2011) los criterios para desarrollar esta técnica fueron:

> a) Como técnica cualitativa, la entrevista congregó a un entrevistador-moderador con el informante y su exclusivo propósito fue conseguir respuestas que coadyuven a evidenciar el fenómeno estudiado. El investigador se erigió en entrevistador. b) La entrevista cualitativa a elaborar fue de naturaleza organizada, respetando modelos concretos en su preparación, su ejecución e interpretación de los datos. Se efectuó a través de una conversación personal con cada entrevistado de manera virtual previo acuerdo con el entrevistado. c) Los equipos y materiales empleados fueron: una guía de entrevista, una laptop con grabadora y el diario del entrevistador. El investigador se erigió en relator. d)

> El desarrollo de la entrevista fue concebida y dispuesta para antes, durante y después de su aplicación a los entrevistados. (p. 71)

El análisis documental de estudios preliminar relacionado al tema en estudio, fue la tercera técnica de recolección de datos utilizado. Por medio de esta técnica se pudo tener acceso a documentación con cierto nivel de clasificación, dada la fuente encargada de su confección, lo que coadyuvó a pre-determinar las categorías de la investigación. Por otra parte, es menester mencionar que fue necesario solicitar las correspondientes autorizaciones formales para la obtención de los datos respetando un determinado cuerpo normativo referente a la seguridad en su uso, acceso y privacidad.

Capítulo IV. Análisis y síntesis

4.1 Recolección de datos

La actividad referida a la recolección de datos se realizó durante los años 2022 y 2023. Para la realización de la investigación se tuvo en cuenta en todo momento, nuestro enfoque cualitativo, para obtener la información en el campo a partir de las experiencias del personal militar de comunicaciones que, tienen vínculo con la labor que, se realiza en el CECOM de la 32ª Brigada de Infantería, para de esta manera arribar a vínculos sistemáticos a partir de la determinación de las unidades de análisis. Hernández y Mendoza (2018), refirieron que:

> La recolección de datos resulta de vital importancia en la realización de la investigación, soló que su propósito no es medir variables para llegar a un análisis estadístico. El estudio cualitativo obtiene datos, los que más adelante se convertirán en información a partir de personas, otros seres vivos, comunidades, situaciones o procesos en profundidad; en sus propias maneras de expresión (p. 443).

La adquisición de información para el desarrollo de la investigación, fue de fuentes humanas y documentales, existentes en la compañía comunicaciones N° 32, de la 32ª Brigada de Infantería del Ejército del Perú. Las técnicas empleadas para la obtención de datos fue el análisis documental, la observación no participante y la entrevista. Se tuvo en consideración que, para el desarrollo de esta investigación cualitativa se trató de obtener información relevante de los participantes, que posteriormente, dicha información fue sometido a un análisis, síntesis y codificación, para convertirse en información de importancia a partir de la percepción y formas de expresión de la realidad de los participantes, en un contexto determinado. En este sentido el procedimiento para poder generar un nuevo conocimiento a partir de la información obtenida por nuestros instrumentos aplicados al personal militar de comunicaciones en la guarnición de Trujillo, se tuvo que, trabajar un proceso, el cual inició con la recolección de datos, la clasificación, determinación de las unidades de análisis, la síntesis y codificación correspondiente. Los instrumentos aplicados fueron los que, se indican a continuación:

4.1.1 La entrevista

Se empleó el instrumento de la guía de entrevista semiestructurada en base a preguntas abiertas, permitiendo al investigador explorar en razón al entendimiento de la realidad de los entrevistados en razón de nuestro fenómeno de estudio. En este caso en particular, se tuvo en consideración la existencia de amenazas cibernéticas emergentes, nos centramos en los motivos que sustentan, la salvaguarda de la red de datos del CECOM de la Compañía Comunicaciones N° 32**,** orgánica de la 32ª Brigada de Infantería, para incrementar su capacidad de protección a la información que, se maneja en dicho CECOM.

Tabla 2

Característica de los entrevistados participantes

Nº del entrevistado	Grado Militar	Experiencia laboral	Fecha de entrevista	Lugar de entrevista
Entrevistado 1	Mayor	2 años	05 de mayo de 2023	Sala Virtual
Entrevistado 2	Mayor	2 años	09 de junio de 2023	Sala Virtual
Entrevistado 3	Teniente	2 años	12 de mayo de 2023	Sala Virtual
Entrevistado 4	Técnico	4 años	24 de mayo de 2023	Sala Virtual
Entrevistado 5	Sub Oficial	4 años	27 de mayo de 2023	Sala Virtual

4.1.2 Guía de observación

El segundo instrumento fue la guía de observación, el cual tuvo relación con la técnica de observación no participante, se empleó para poder recabar información sobre nuestro fenómeno de estudio, para de esta manera como investigador, se pudo arribar a reflexiones y opiniones informadas. Cabe mencionar que, se pudo atisbar la manera como se maneja el tráfico de información en el CECOM de la compañía comunicaciones N° 32, tanto con sus unidades subordinadas, unidades vecinas y escalón superior.

En lo que, refiere a la guía de observación, se determinó la realización en función de los objetivos de la investigación. De acuerdo con las actividades cotidianas que, se realizan en el CECOM, así como, las facilidades otorgadas por el comando de la GUC, para tener acceso a dicha instalación de responsabilidad de la compañía comunicaciones N° 32, resultando una fuente importante para la obtención de información cualitativa, el cual nos ayudó a comprender nuestro fenómeno de estudio. Dicha guía de observación fue útil para estudiar el método de seguridad informático que posee el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería.

4.1.3 Análisis documental

Referente al instrumento de análisis documental, podemos inferir que, este instrumento nos ha permitido tener acceso a documentación pertinente referido a la seguridad de la red de datos del CECOM de la compañía comunicaciones N° 32, coadyuvando de esta manera a poder entender nuestro fenómeno de estudio. Asimismo, permitió al investigador conocer documentación que, se emplea en dicha instalación militar, así como, experiencias del personal de operadores de comunicaciones que, se generan producto del trabajo diario realizado en la

transmisión y recepción de información que, se maneja, las medidas de seguridad informática que, se emplea en dicha instalación, ante la evolución de amenazas informáticas emergentes.

Tabla 3

Indagación documental

Nº	Documentos/Reglamentos	Año
1	Directiva de Funcionamiento del Centro de Comunicaciones de la 32ª Brigada de Infantería	2022
2	Manual de Procedimientos del Centro de Comunicaciones de la 32ª Brigada de Infantería	2022
3	IOC del Centro de Comunicaciones de la 32ª Brigada de Infantería	2022
4	Empleo de la Compañía de Comunicaciones	2022
5	Conocimientos básicos de Operaciones Cibernéticas	2018
6	Directiva Única de Funcionamiento del Sistema de Telemática	2020

4.2 Organización de datos

La organización de datos se realizó coherentemente teniendo como principal referencia el planteamiento de realización de la metodología para el desarrollo de nuestra investigación, el cual, se estableció en el capítulo anterior, consecuente con el método de investigación hermenéutico-interpretativo. En este sentido, para el desarrollo de la investigación fue necesario obtener información del objeto de estudio e interpretado hermenéuticamente. “Bajo este paradigma el conocimiento resulta de la construcción subjetiva y continua de aquello que le da sentido a la realidad investigada como un todo”. (Vargas, 2011, p.16)

Para visualizar de una manera general de la situación, posterior a la aplicación de los instrumentos, se realizó una revisión cuidadosa de la información recabada, lo que nos permitió identificar nuevos conceptos, relaciones entre el objeto de estudio y posibles definiciones respecto a nuestro tema de investigación, revisando las entrevistas, los documentos que, fueron analizados y la realidad encontrada a partir de la guía de observación.

Tabla 4

Organización de datos

Instrumento/ Técnica	La entrevista	Observación no participante	Análisis documental
GUIA DE ENTREVISTA SEMIESTRUCTURADA	Entrevista N° 1 Entrevista N° 2 Entrevista N° 3 Entrevista N° 4 Entrevista N° 5		
GUIA DE OBSERVACIÓN		Registro de lo observado en el Centro de Comunicaciones de la 32ª Brigada de Infantería	
FICHA DE ANÁLISIS DOCUMENTAL			Análisis documental de los siguientes textos: - Directiva de Funcionamiento del Centro de Comunicaciones. - Manual de Procedimientos del Centro de Comunicaciones. - IOC del Centro de Comunicaciones de la 32ª Brigada de Infantería. - Manual de Empleo de la Compañía de Comunicaciones. - Manual de Conocimientos básicos de Operaciones Cibernéticas. - Directiva Única de Funcionamiento del Sistema de Telemática.

4.3 Definición de categorías

A la luz de nuestro problema que se abordó en la investigación y posterior obtención de datos en el campo, se continuó con el procesamiento de la información obtenida en lo referente a la codificación a partir de las unidades de análisis, en donde según las experiencias del personal militar de comunicaciones de la Compañía Comunicaciones N°32, los extractos de los

textos considerados en el análisis documental y la observación del investigador en el campo, se logró definir las categorías de la presente investigación, los cuales fueron considerados en este acápite; De acuerdo con Hernández y Mendoza (2018):

> La creación de categorías a partir del análisis de unidades es una muestra de por qué el enfoque cualitativo es inductivo. Los nombres de las categorías y las reglas de clasificación deben ser claras para evitar reprocesos excesivos en la codificación. (p.468)

Donde las categorías obtenidas coinciden con las apriorísticas; sin embargo, emergieron nuevas sub categorías, las cuales se observa en la tabla que a continuación se indica:

Tabla 5

Codificación selectiva, axial-elaboración de categorías y subcategorías

Codificación selectiva	**Codificación axial**	**Patrones**	**Frecuencia de mención**
Categorías	**Subcategorías**		
Seguridad de la Red de Datos (SRD)	Ataques Cibernéticos (Atq Ci)	• Obtención de Información. • Operaciones Ofensivas en la red • La PCM a través de la Secretaría de Gobierno y Transformación Digital es la responsable de la seguridad digital • Centro Nacional de Seguridad Digital • Desactualización de los Software. • Acceso al Internet Público • Inoperatividad del Sistema VSAT • Necesidad de Internet Dedicado • Cursos de Ciberdefensa	3 entrevistas Análisis Documental
	Políticas y Controles (PyC)		3 entrevistas
	Vulnerabilidad de la Red (VdR)		4 entrevistas
	Ciberdefensa (Ciberdef)		
	Parque Informático Moderno (PIM)	Avance de la tecnología Se cuenta con equipos de más de 20 años. Los equipos no cuentan con tecnología de última generación.	4 entrevistas
Centro de Comunicaciones (CDC)	Personal Capacitado en Operaciones Cibernéticas. (PCEOC)	Personal instruido donde las comunicaciones son más vulnerables.	3 entrevistas

	No se cuenta con personal capacitado en Operaciones Cibernéticas. Conocimiento de Manejo de Redes Manejo de herramientas actualizadas de informática.

4.4 Soporte de categorías

Tabla 6

Codificación axial de las categorías de la guía documental

Categorías	Sub categorías	Codificación axial
C1: Seguridad de la red de datos	SC1: Ataques Cibernéticos SC2: Políticas y Controles SC4: Ciberdefensa	Atq Ci PyC Ciberdef
C2: Centro de Comunicaciones	SC6: Personal capacitado en Operaciones Cibernéticas	PCEOC

Tabla 7

Codificación axial de las categorías de la guía de entrevistas

Categorías	Sub categorías	Codificación axial
C1: Seguridad de la red de datos	SC1: Ataques Cibernéticos SC2: Políticas y Controles SC3: Vulnerabilidad de la Red SC4: Ciberdefensa	Atq Ci PyC VdR Ciberdef
C2: Centro de Comunicaciones	SC5: Parque Informático Moderno SC6: Personal capacitado en Operaciones Cibernéticas	PIM PCEOC

Tabla 8

Codificación axial de las categorías de la guía de observación

Categorías	Sub categorías	Codificación axial
C1: Seguridad de la red de datos	SC2: Políticas y Controles SC3: Vulnerabilidad de la Red	PyC VdR
C2: Centro de Comunicaciones	SC5: Parque Informático Moderno SC6: Personal capacitado en Operaciones Cibernéticas	PIM PECEOC

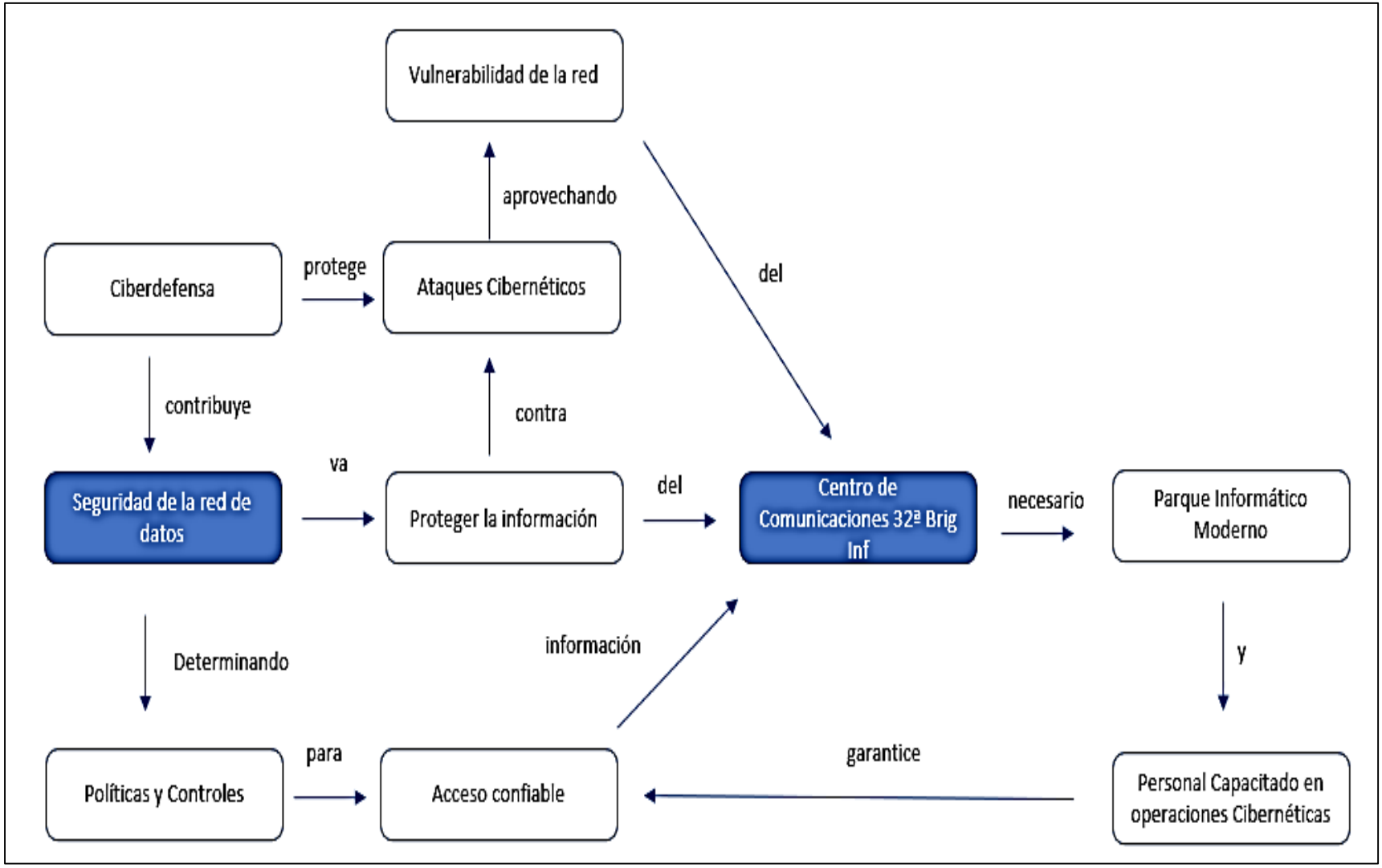
Tabla 9

Soporte de la técnica de las categorías, subcategorías y observables

Tema	Categoría	Descripción	Patrón	Descripción
Análisis de la seguridad de red de datos del Centro de Comunicaciones 32ª Brigada de Infantería, 2022	Seguridad de la Red de Datos (SRD)	La Seguridad de la Red de Datos son todas las actividades que, se realizan para proteger la información que, transita en nuestra red informática de la organización a la cual pertenecemos con la finalidad impedir el acceso a la misma a personas ajenas a nuestra organización a través de un ataque cibernético.	Ataques Cibernéticos	Son los intentos por acceder a una red informática ajena, para perjudicarla, ya sea mediante el robo de información y/o modificación del funcionamiento de sus sistemas,
			Políticas y Controles	Normas y disposiciones existentes en diferentes textos desde leyes a reglamentos emanadas por organismos gubernamentales para la protección de las diferentes plataformas digitales.
			Vulnerabilidad de la red	Debilidades existentes en una red de datos, la cual lo coloca en una situación de fragilidad ante un posible ataque cibernético
			Ciberdefensa	Acciones que realiza un estado para la protección de redes digitales ante determinadas amenazas cibernéticas
	Centro de Comunicaciones (CDC)	Instalación que, alberga un conjunto de personal y medios de comunicaciones, que permiten al comandante ejercer el comando y control sobre sus unidades subordinadas, así como el enlace con unidades vecinas y su escalón superior	Parque Informático Moderno	Es el conjunto de equipos de cómputo que, poseen hardware y software de última tecnología.
			Personal capacitado en Operaciones Cibernéticas	Personal instruido en el dominio de operaciones ofensivas y defensivas en redes de datos informáticas en provecho de la 32ª Brigada de Infantería

4.5 Red semántica

Figura 1: *Red semántica del análisis de las entrevistas, guía de observación y análisis documental.*



4.6 Triangulación

Tabla 10

Matriz de triangulación de las categorías en función de los hallazgos

Categorías	Síntesis conclusivo resumen de las entrevistas	Síntesis conclusivo resumen de la guía de observación	Síntesis conclusiva resumen del análisis documental	Resultados
Seguridad de la red de datos (SRD)	(SC1: Atq Ci y C1: SRD) Estas premisas poseen una relación condicional, toda vez que, la concepción de la seguridad de la red de datos tiene su génesis a partir de la existencia de las amenazas cibernéticas, las cuales, materializan principalmente sus actos en las redes a través de los ataques cibernéticos. Donde la red de datos del centro de comunicaciones de la 32a Brigada de Infantería, estaría expuesta a dichas amenazas por carecer de un sistema de protección de datos. (SC2: PyC y C1: SRD) Según las informaciones recabadas por nuestras guías de entrevistas, la seguridad de la red de datos y las políticas y controles están relacionados bicondicionalmente entre sí, lo cual tienen una influencia mutua,	(SC2: PyC y C1: SRD) Estas premisas están relacionadas de manera bicondicional, en razón que, uno de los pilares fundamentales para el funcionamiento del centro de comunicaciones es la existencia de políticas y controles para la seguridad de la red de datos, los cuales vienen siendo aplicados por el personal militar de comunicaciones, según las disposiciones emanadas de su comando y las determinadas por la compañía comunicaciones N° 32. SC3: (VdR y C1: SRD) Los equipos con los cuales trabaja el centro de comunicaciones de la compañía comunicaciones N° 32, tienen una antigüedad	(SC2: PyC y C1: SRD) Estas premisas están relacionadas de manera bicondicional, en razón de la existencia de documentos que, determinan las normas de seguridad en el centro de comunicaciones, como lo son: El manual de procedimientos, la directiva de funcionamiento del centro de comunicaciones y la directiva única de funcionamiento de telemática, los cuales rigen el norte de las medidas a adoptar por parte del personal militar que, realiza su servicio en dicho centro, en función de la disponibilidad de sus medios materiales y humanos. (SC4: PyC y C1: SRD)	Los equipos de cómputo con los que trabaja el Centro de Comunicaciones de la Compañía Comunicaciones N° 32 Nº 32, son de hardware y software que, poseen una antigüedad superior a los 10 años, en el pasado se contó con una red propia de internet institucional la cual tuvo estándares de seguridad; en la actualidad se trabaja con internet comercial, el cual hace vulnerable la información que, se maneja en dicha red de datos, vulnerando de igual manera todos los conceptos referidos a la Ciberdefensa que, no se pueden aplicar, estando las disposiciones de seguridad en cuanto al manejo de la información, limitada a lo plasmado en sus documentos normativos.

Categorías	Síntesis conclusivo resumen de las entrevistas	Síntesis conclusivo resumen de la guía de observación	Síntesis conclusiva resumen del análisis documental	Resultados
	donde podríamos inferir que, el punto de partida para concebir medidas de seguridad en la red, se dará a partir de la determinación de políticas y controles, los cuales se adaptan a la realidad de cada organización militar, considerando nuestro tema de estudio. SC3: (VdR y C1: SRD) Estas premisas poseen una relación condicional, toda vez que, la concepción de la seguridad de la red de datos se tiene que determinar a partir del conocimiento de las vulnerabilidades de la red, de acuerdo a los hallazgos encontrados, determinamos que, el personal militar de comunicaciones que, realiza sus servicios en el Centro de Comunicaciones de la 32a Brigada de Infantería, tiene conciencia de la existencia de vulnerabilidades en la red, principalmente debido a la inexistencias de dispositivos digitales de protección, como los son los Firewall.	que, supera los diez (10) años, esto implica que, el sistema operativo con el cual trabaja es Windows 8, el cual lo hace totalmente vulnerable a las amenazas cibernéticas en la actualidad.	Estas premisas poseen una relación bicondicional, toda vez que, la concepción de la seguridad de la red de datos se determina en el concepto más amplio de la ciberdefensa, para lo cual se tiene como principal referencia lo establecido en el Manual ME 11-225 Conocimientos Básicos de Operaciones Cibernéticas (2018). En la actualidad desde el punto de vista militar se conceptualiza el ciberespacio como una dimensión más en el campo batalla, en ese sentido emerge la Ciberdefensa, para tomar medidas y controles necesarios para proteger nuestras redes informáticas, dichos conceptos no son aplicados en el Centro de Comunicaciones de la compañía comunicaciones N° 32, el cual se limita a dar sus disposiciones de	

Categorías	Síntesis conclusivo resumen de las entrevistas	Síntesis conclusivo resumen de la guía de observación	Síntesis conclusiva resumen del análisis documental	Resultados
	En este sentido, de acuerdo a la información recabada por nuestro instrumento de recolección de datos, se pudo inferir que, el nivel de protección de la información que, se maneja en la red del centro de comunicaciones es bajo, en vista que no se cuenta con software de protección de información, la línea de internet con la cual trabajan en la instalación pertenece a una línea comercial, sin estándares definidos de seguridad, se tiene una red institucional determinada por el sistema VSAT, sin embargo esta línea tiene problemas con su funcionamiento debido a su tiempo de vida útil. De ahí que, muchos de los entrevistados están de acuerdo con obtener una línea de internet dedicado empleado por la Gran Unidad de Combate.		seguridad a través de sus documentos normativos.	
Centro de Comunicaciones de la 32ª Brigada de Infantería (CDC)	SC5: (PIM y C2: CDC) Estas premisas establecen relaciones de interdependencia entre sí, toda vez que, los equipos de cómputos son en la actualidad parte vital para el funcionamiento del centro de comunicaciones, es decir que, ambas premisas están	SC5: (PIM y C2: CDC) Estas premisas establecen relaciones de interdependencia entre sí, toda vez que, los equipos de cómputos, son piezas angulares en la estructura del funcionamiento del centro	SC6: (PCEOC y C2: CDC) Estas premisas tienen una relación condicional con una serie de conceptos donde la variable SC6: PCEOC se relaciona con el concepto de centro de comunicaciones en el	El componente más importante dentro de una organización son los recursos humanos siendo su potencial incalculable, cuando se cuenta con personal con conocimientos producto de la capacitación, siendo necesario la capacitación permanente en

Categorías	Síntesis conclusivo resumen de las entrevistas	Síntesis conclusivo resumen de la guía de observación	Síntesis conclusiva resumen del análisis documental	Resultados
	relacionadas entre sí, tanto en la parte doctrinaria, donde se determina que, un centro de comunicaciones lo conforma personas y medios, donde dentro de los medios están los equipos de cómputo y en la parte funcional de acuerdo a la información recabada en las entrevistas, se aprecia que las computadoras, los cuales ya poseen varios años de uso, representando el medio principal para el enlace entre los diferentes niveles de comando. SC6: (PCEOC y C2: CDC) De acuerdo a los hallazgos, determinamos que, en la 32a Brigada de Infantería el personal militar de comunicaciones no se encuentra capacitado en conocimientos básicos de Operaciones Cibernéticas, lo cual aumentaría el nivel de vulnerabilidad del empleo de la red de datos, considerando que, el principal elemento dentro de un sistema de seguridad es el hombre. Debido a la antigüedad que, posee los equipos de cómputo, se	de comunicaciones, pudiendo apreciar que, el material trabaja con tecnologías desfasadas, a las tecnologías de vanguardia existentes en el mundo informático, careciendo de características técnicas inherentes que, permita resguardar la información que, se maneja en las redes del Centro de Comunicaciones de la 32a Brigada de Infantería. Orientándonos en los medios materiales y humanos que, se posee como institución, apreciamos que, la falta de funcionamiento del sistema satelital VSAT y falta de capacitación del personal de Operadores de Comunicaciones que, hacen diariamente el servicio de Centro de Comunicaciones, hace de que, las vulnerabilidades al acceso de nuestras redes incremente cada día, por la rotación del personal a los cuales se apela a su	aspecto de la estructura de personal, teniendo en consideración su definición Instalación de comunicaciones integradas por personal y medios que controla la transmisión y recepción de mensajes. Normalmente consta de un centro de mensajes, elementos criptográficos, infraestructura de transmisión y recepción. Las disposiciones de seguridad en cuanto al manejo de las redes de datos, están plasmadas en los documentos normativos, los cuales son motivo de relevo entre el personal que entra de servicio, el manual de empleo de la compañía comunicaciones, determina que, el funcionamiento de los Centros de Comunicaciones que, apoyan a un determinado escalón del Cuartel General, son de responsabilidad de la	lo referente a conocimientos básicos de Operaciones Cibernéticas al personal de operadores de Comunicaciones, el cual debería ser administrado por la Compañía comunicaciones N° 32, como responsable del funcionamiento de los Centros de Comunicaciones; asimismo, se hace necesario renovar el parque informático en cuanto a hardware y software los cuales deben ser de una tecnología acorde a nuestros tiempos, complementando con elementos informáticos que nos permita garantizar la accesibilidad y manejo de información que, se realiza en esta red de datos.

Categorías	Síntesis conclusivo resumen de las entrevistas	Síntesis conclusivo resumen de la guía de observación	Síntesis conclusiva resumen del análisis documental	Resultados
	hace necesario realizar las gestiones necesarias para renovar el parque informático, esta renovación debería incluir la implementación de un servidor o cortafuegos que, proteja la información que, se maneja en el Centro de Comunicaciones de la compañía comunicaciones Nº 32, asimismo, el personal que labora en dicha instalación no cuenta con ninguna capacitación en Operaciones Cibernéticas, teniendo en consideración que todos los principios de seguridad tienen su génesis en el hombre, en este sentido esta responsabilidad recae en los Operadores de Comunicaciones. La mayoría del personal militar entrevistado incide en que, se debería contar con equipos de cómputo que estén a la par con la tecnología existente.	conciencia de seguridad para realizar el trabajo diario.	compañía antes mencionada, en ese sentido se determina que las responsabilidades en seguridad de comunicaciones, involucra a la misma compañia. Siendo necesario la capacitación del personal en conocimientos básicos de Operaciones Cibernéticas según lo determinado en el Manual ME 11-225 (2018).	

Capítulo V. Diálogo teórico-empírico

Vargas (2011), refirió que en el desarrollo de este capítulo de la investigación de enfoque cualitativo se “Responde a las preguntas de investigación, las cuales están relacionados con los objetivos de la misma, empleando como sustento la realidad encontrada en el campo, después de haber realizado el proceso del análisis y síntesis en la investigación” (p.70). Según el desarrollo de nuestro análisis interpretativo, se reunió en nuestro marco teórico, diferentes conceptos, principios, políticas, teorías, procedimientos, términos y estrategias, las cuales están contenidas en la protección de la información que, transita en una red informática, en la cual se determinó relación con nuestra doctrina del arma de comunicaciones, según él ME 11- 225 Conocimientos Básicos de Operaciones Cibernéticas (2018), aplicable en nuestro estudio sobre el Análisis de la seguridad de red de datos del CECOM de la 32ª Brigada de Infantería, 2022. Para responder a nuestras preguntas y objetivos de nuestra investigación se realizó teniendo en cuenta la contrastación de lo desarrollado en nuestro capítulo II, marco teórico, desarrollándolo de la siguiente manera:

5.1 En relación al objetivo 1

De acuerdo al objetivo 1: Analizar el funcionamiento de la seguridad de red de datos en el CECOM a cargo de la Compañía Comunicaciones de la 32ª Brigada de Infantería, 2022, la teoría de la seguridad de las comunicaciones determina que, nuestras vidas se están transmutando a magnitudes significativas de información, siendo el mayor desafío para la tecnología, el resguardo de ellos. Esta noción simboliza la salvaguarda de los capitales preciosos propios de una entidad: Sean instalaciones, personas, hardware, software, mobiliario, datos, etc. (…) por tanto, debe ser convenientemente atendido por todos los encargados, con la finalidad de asegurar la forzosa confianza en la sociedad de la tecnología.

Al respecto, se determinó que, de acuerdo a los hallazgos que se realizó en el campo, el CECOM de la 32ª Brigada de Infantería, el funcionamiento de la seguridad de red de datos es limitada, en relación al tránsito de la información que, se emplea en dicha instalación y en sus redes informáticas, limitándose solo a las medidas de seguridad referidas al control de accesos por medio de empleo de contraseñas en los equipos de cómputo y sistemas propios del Ejército Perú, careciendo de dispositivos digitales para la seguridad de datos como : Firewall y sistema de detección y prevención de intrusos (IDPS) que, permita negar el acceso a nuestra red de datos y detectar la intromisión de agentes ajenos a nuestras redes, los cuales podrían tener la intención de obtener información clasificada de manera ilícita, manipular información o impedir el normal funcionamiento del CECOM afectando sus capacidades informáticas, lo cual se contrapone a lo referido en la teoría de la seguridad de las comunicaciones.

5.2 En relación al objetivo 2

De acuerdo al objetivo 2: Describir los ataques informáticos que pueden afectar el funcionamiento de la seguridad de red de datos del CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, según lo expresado en el manual de procedimientos de comunicaciones de las FFAA MFA-06-03 (1989), advierte los principios de organización para una red de comunicaciones, siendo uno de ellos la seguridad de las redes de comunicaciones, el cual señala que, el efecto de la globalización que va junto a la tecnología, está acarreando grandes provechos a las entidades de cualquier índole, pero igualmente están originando enormes dificultades de seguridad y de salvaguarda de datos, las que deben ser superadas por las diversas entidades.

Con respecto a lo mencionado anteriormente, Villarrubia (2021) sostuvo que, se debe salvaguardar la información digital que transita por las redes informáticas de las respectivas organizaciones militares, dada las circunstancias que manejan los datos informáticos que son de importancia para nuestra institución armada, toda vez que, proliferan las amenazas y los respectivos ciberataques debido a las vulnerabilidades de nuestras medidas de ciberseguridad.

En este sentido, el CECOM de la 32ª Brigada de Infantería está expuesto a amenazas cibernéticas, debido a que, como se mencionó anteriormente, es limitada la protección de la información existente es sus redes de datos, lo cual lo hace vulnerable a ataques cibernéticos como: a. Malware: El cual se determina como un software maligno el cual tiene la finalidad de infiltrarse en una determinada red o sistema informático para causarle daños a su funcionamiento. b. Virus: Infecta archivos magnéticos mediante códigos malignos, para dañar la información que se maneja en una determinada red informática, pudiendo afectar el funcionamiento de todo el sistema al lograr diseminarse por el mismo. c. Gusanos: Es un software maligno que, al lograr infiltrase en la red, realiza copias de la información difundiéndolas a redes ajenas, siendo difícil su detección, en vista que, a diferencia de los virus, estos no afectan el funcionamiento del sistema. d. Troyanos: Tiene por finalidad abrir un portal digital para que, de esta manera puedan ingresar a la red programas malignos que puedan afectar a la información que se maneja en una determinada red. e. Phishing: Es una técnica que, busca suplantar una identidad para obtener información, no refiere un software, siendo el medio más empleado el envío de correos electrónicos, en este sentido, en relación a nuestro tema de estudio, consideramos que, este ataque cibernético sería el cual, estaría más expuesto el CECOM, toda vez que, la circulación de información que se realiza en la misma es a través de correos electrónicos.

5.3 En relación al objetivo 3

De acuerdo al objetivo 3: Identificar las políticas y controles de seguridad informática que posee el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, la teoría de red de datos, encuentra su fundamento en el conjunto de dispositivos interconectados físicamente, sea vía cableado o vía inalámbrica, que emplean los pulsos eléctricos, transmisiones electromagnéticas o cualquier otra tecnología para la transferencia de datos, a fin de usar mancomunadamente medios (hardware y software), para lo cual se emplean diversas normas que, aseguren la comunicación. (Galloway, 2007, p.26).

Asimismo, tenemos que, según el principio de la seguridad de las redes de comunicaciones expresado en el manual de procedimientos de comunicaciones de las FFAA MFA 06-03 (1989), se determinó que, las amenazas a las comunicaciones, constituyen diligencias o acciones que son determinadas como una circunstancia de riesgo, en que un elemento puede impactar negativamente en nuestra seguridad, las amenazas (…) son el ingrediente básico para formular las Políticas de Comunicaciones.

Tras haber acopiado información en base a la observación no participante, en relación a la aplicación de las normas y políticas de seguridad de redes de datos en el CECOM de la 32ª Brigada de Infantería, se determinó que, los operadores de comunicaciones que, realizan el servicio de CECOM, cumplan con las normas y políticas establecidas en sus documentos normativos para el funcionamiento del mismo, en cuanto a la seguridad del tráfico de mensajes que, circulan en los diferentes escalones de comando, permitiendo que, todo el personal militar de comunicaciones, logre incrementar los niveles de seguridad de los datos e informaciones que se gestionan en las redes de datos informáticas. Sin embargo, se ha podido apreciar que, el personal de operadores de comunicaciones falta ser capacitado en conocimientos básicos de operaciones cibernéticas, para de esta manera incrementar la conciencia de seguridad entre todo el personal militar, considerando que la base de la seguridad recae en los operadores de comunicaciones, en este sentido cabe mencionar que, en nuestra institución existe el Comando de Ciberdefensa y Telemática del Ejército, como un ente rector de la ciberseguridad en el Ciberespacio en provecho de nuestra institución.

5.4 En relación al objetivo 4

De acuerdo al objetivo 4: Proponer las mejoras de las capacidades que debería poseer en cuanto a seguridad de red de datos el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, tenemos la definición de Comando, Control, Comunicaciones, Computadoras e Inteligencia (C4I) la cual sostiene que, es una sumatoria de

componentes que permiten la unificación de cuestiones doctrinarias, modos, estrategias, infraestructura, equipamiento, comunicaciones, tecnología informática y aspectos de inteligencia.

> Rivera (2019), advirtió la importancia de proteger los datos que, transitan en el ciberespacio, así como, resguardar la información que manejamos en cada una de nuestras redes informáticas, es decir que nuestras redes informáticas en la actualidad deben tener capacidades que nos permita proteger la información que circula dentro de ella, teniendo en consideración que, el ciberespacio es una dimensión de actividades humanas y del campo de batalla desde el punto de vista militar (p. 45).

Como se ha hecho referencia en las entrevistas, por parte del personal militar, el CECOM debería tener capacidades de Ciberdefensa, para hacer frente a las diferentes amenazas cibernéticas, disponiendo de las siguientes capacidades principales: a. Dispositivos digitales con protección de redes informáticas. b. Funcionamiento del sistema VSAT, explotando sus protocolos de seguridad de encriptación de información. c. Parque informático con tecnología de última generación. d. Personal capacitado en operaciones cibernéticas.

Capítulo VI. Conclusiones y recomendaciones

6.1 Conclusiones

Para el primer objetivo de analizar el funcionamiento de la seguridad de red de datos en el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, esta investigación ha encontrado que el funcionamiento de la seguridad del centro de comunicaciones de la 32ª Brigada de Infantería, ofrece limitaciones en cuanto a la seguridad de información que, se maneja en la red de datos, en vista de que, carece de recursos tecnológicos que, permitan salvaguardarla de amenazas cibernéticas, es decir que, se apreció que, la inexistencia de un Firewall como recurso básico de protección de información, el cual tiene por finalidad evitar que agentes ajenos a la red de una organización puedan acceder a la misma de una manera ilícita para sustraer y/o manipular información o perjudicar el normal funcionamiento de los sistemas informáticos de una organización, este nuestro caso de estudio seria los propios de la 32ª Brigada de Infantería a partir de las informaciones que, transita en las redes de datos de su CECOM. Evidenciando en el estudio de campo que, la principal medida de seguridad informática refiere al “control de acceso” en lo que, respecta al uso de contraseñas que, permita el empleo de los diferentes sistemas de comunicaciones e informática que, posee la institución, donde dichos sistemas son empleados por el personal militar de comunicaciones que, realiza su servicio en dicho CECOM, para gestionar la información que proviene de los diferentes niveles de comando.

Para el segundo objetivo describir los ataques informáticos que pueden afectar el funcionamiento de la seguridad de red de datos del CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, al determinar producto de los hallazgos que, el CECOM posee una limitada protección en la dimensión del ciberespacio, dado que, la protección existente se basa en la dimensión humana, en efecto esta realidad encontrada evidencia que, las redes de datos del CECOM están vulnerables a las diferentes amenazas informáticas que, existen en el ciberespacio, los cuales se pueden traducir a una variada gama de ataques cibernéticos, los cuales cada vez se van haciendo más sofisticados con el paso del tiempo con el avance vertiginoso de la tecnología, siendo imperativo que, una organización como la 32ª Brigada de Infantería, este prevenida y preparada ante cualquier tipo de ataque cibernético, toda vez que, en sus redes se maneja información clasificada entre sus diferentes niveles de comando en relación a función administrativa, así como la determinada en su rol principal de garantizar la independencia, soberanía e integridad territorial, el cual se desarrolla diferentes acciones y operaciones militares en su ámbito de responsabilidad. Ante los diferentes cambios de tendencias informáticas y las características del trabajo que, se ha podido

evidenciar que, se realiza en el CECOM de la GUC, las redes de datos se hacen vulnerable principalmente a los siguientes ataques informáticos: Malware, Virus, Gusanos, Troyanos y Phishing.

Para el tercer objetivo identificar las políticas y controles de seguridad informática que posee el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, Nuestra institución, se rige en las normas del derecho internacional, como miembro activo en las Organización de las Naciones Unidas (ONU), ante la existencia de amenazas cibernéticas, surge un concepto llamado arma cibernética el cual se podría definir como un malware que, solo tiene la intención de causar un daño, lo cual constituiría su prohibición en el marco internacional según la carta de las Naciones Unidas, al constituirse el uso de armas cibernéticas como una acción armada de una fuerza en perjuicio de un estado, entendemos en este sentido el marco legal internacional y de la creación del CITELE, el cual está destinada en realizar acciones que permita garantizar los medios informáticos en nuestra institución como parte del sistema de comando y control; sin embargo, esta organización no realiza actividades de ciberataque.

De acuerdo a lo recabado, en el campo de investigación se valida que, en el CECOM de la 32ª Brigada de Infantería, existen políticas y normas para garantizar la seguridad de sus redes de datos, las cuales están plasmadas en sus documentos normativos e Instrucciones Operativas de Comunicaciones (IOC), los cuales son de conocimiento del personal militar de comunicaciones que, realiza servicio en el CECOM para de esta manera dentro de las limitaciones existentes hacer frente a las amenazas informáticas y de esta manera mitigar las vulnerabilidades de la red de datos, partiendo de la premisa que, la seguridad tendrá su génesis en los operadores de comunicaciones, los cuales a la luz de la observación y las entrevistas, se determina que, este personal no está capacitado, según lo expresado en el ME 11-225 Conocimiento Básico de Operaciones Cibernéticas (2018).

Para el cuarto objetivo proponer las mejoras de las capacidades que debería poseer en cuanto a seguridad de red de datos el CECOM a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022, teniendo en consideración que, un CECOM es una instalación que reúne personal especialista y medios de comunicaciones que, aseguren el ejercicio del mando a un comandante, en el desarrollo de este ejercicio esta instalación debe poseer capacidades de Comando, Control, Comunicaciones, Computación e Informática (C4I) acorde a los avances de la tecnología. Debiendo contar el CECOM con un parque informático moderno en software y hardware, complementado con dispositivos digitales para la protección de la red de datos.

El análisis de la seguridad de red de datos en el CECOM de la 32 Brigada de Infantería, es un proceso crucial para garantizar la protección de la información sensible y las operaciones críticas. Al respecto se tiene una conclusión general basada en la seguridad de red en un entorno militar requiere un enfoque integral que considere las amenazas internas y externas, los posibles ataques cibernéticos, el manejo de incidentes, y la implementación de medidas preventivas y de mitigación. En general, el CECOM de la 32 Brigada de Infantería, realiza el análisis de la seguridad de red de datos con la finalidad de la identificación de amenazas y vulnerabilidades para detectar posibles debilidades en la infraestructura de red y prever ataques cibernéticos que puedan comprometer la integridad, confidencialidad o disponibilidad de los datos. Es vital para el fortalecimiento de los protocolos de seguridad que incluyan la implementación de medidas como firewalls avanzados, encriptación de datos, autenticación de múltiples factores, y redes segmentadas que dificulten el acceso no autorizado, además de realizar un monitoreo continuo y respuesta a incidentes por ello se debe contar con sistemas de monitoreo en tiempo real para detectar cualquier actividad sospechosa y responder de manera eficaz a incidentes de seguridad, combinando la avanzada tecnología, políticas de seguridad estrictas y capacitación continua del personal para enfrentar eficazmente los desafíos dinámicos del entorno cibernético.

6.2 Recomendaciones

Para cumplir con el primer objetivo es necesario que las medidas de seguridad informática sean actualizadas, analizadas y realizar auditorías de seguridad de forma periódica, como revisión a la red de datos para identificar vulnerabilidades en los servidores y dispositivos de la red (routers, switches, firewalls), y demás componentes de la infraestructura con un escaneo de vulnerabilidades utilizando herramientas tecnológicas para detectar vulnerabilidades en los sistemas y evaluar la postura de seguridad frente a las amenazas cibernéticas, así mismo se deberá de implementar una Arquitectura de Seguridad en Capas para una defensa en profundidad, para lo cual debe de aplicar y combinar varias soluciones como firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), encriptando y realizando una división de la red en zonas segmentadas para limitar el acceso a áreas sensibles y permitir el acceso solo a usuarios autorizados y minimizar el impacto de posibles ataques. Estas recomendaciones ayudarán a establecer una seguridad sólida en la red de datos del CECOM y proteger las comunicaciones críticas que maneja la 32ª Brigada de Infantería frente a los riesgos cibernéticos, garantizando su operatividad en todo momento.

La recomendación para el segundo objetivo el personal militar de comunicaciones que, labora en la 32ª Brigada de Infantería debe de establecer alianzas estratégicas con empresas privadas especialistas en manejo de redes informáticas partiendo del entendimiento situacional

del escenario regional y mundial en seguridad cibernética y por parte de la institución de tal manera que se conozca las amenazas cibernéticas que, pueden realizar ciberataques a la red de datos del Centro Comunicaciones, haciendo énfasis a las amenazas de : Malware, Virus, Troyanos y Phishing, en este sentido para mitigar estos riesgos se hace de vital importancia contar con antivirus originales en las computadoras del CECOM, las cuales deben ser renovadas periódicamente, de acuerdo a su vigencia de caducidad de esta forma al describir los ataques informáticos que pueden afectar el funcionamiento del CECOM de la Compañía de Comunicaciones N° 32, es esencial abordar una amplia gama de amenazas que abarcan desde ataques directos a la infraestructura crítica hasta tácticas de espionaje y ciberataques de alta tecnología estas recomendaciones presentadas ayudarán a identificar, prevenir y mitigar estos ataques, garantizando que las comunicaciones militares puedan continuar funcionando de manera segura y eficiente frente a las amenazas cibernéticas.

La recomendación para cumplir con el tercer objetivo, el CECOM de la Compañía de Comunicaciones N° 32, debe desestimar el empleo del servicio de internet comercial sobre el cual, se apoya el funcionamiento de las redes de datos del CECOM debido a que vulnera la seguridad de la información clasificada que, se gestiona entre los diferentes niveles de comando, dicha red debe ser reemplazada por una red de internet dedicado, el cual asegure el empleo solo por el personal militar de comunicaciones de la 32ª Brigada de Infantería. En coordinación con la Sección Telemática e Inteligencia de la 32ª Brigada de Infantería, implementar un sistema de políticas y normas enfocadas al empleo de las redes informáticas, de tal manera que, incida en la protección de la información que, transita en el CECOM teniendo en consideración las amenazas cibernéticas existente, teniendo como principal referencia el ME 11-225 Conocimiento Básico de Operaciones Cibernética, al Identificar las políticas y controles de seguridad informática el CECOM de la Compañía de Comunicaciones N° 32, debe enfatizar la implicancia de revisar múltiples áreas críticas, desde políticas de acceso y cifrado de datos hasta sistemas de monitoreo y respuesta a incidente por ello es vital que se realicen auditorías regulares, se mantengan actualizadas las políticas de seguridad y se realicen pruebas de los planes de respuesta a incidentes y recuperación ante caídas de sistemas. Además, la formación constante del personal y el cumplimiento de las normativas de ciberseguridad las cuales son esenciales para mantener un entorno seguro.

Finalmente para el cuarto objetivo se debe de coordinar con el CITELE para que, de manera progresiva amplié sus capacidades, el cual le permitirá generar un canal técnico y elevar el nivel de Ciberdefensa para su aplicación posterior en un eventual campo de batalla, implementando un Centro de Ciberdefensa a nivel GUC estableciéndose en el CECOM de la 32ª

Brigada de Infantería , en este sentido es recomendable aprovechar las buenas relaciones con el hermano país de Brasil, para tomar los modelos de Ciberdefensa implementados en sus fuerzas armadas, y de esta manera poder replicarlos y mejorarlos en nuestra GUC. Asimismo, el CITELE, realice la capacitación y entrenamiento en Operaciones Cibernéticas a todo el personal militar de comunicaciones. Es menester proteger la red de datos del CECOM para restringir el tráfico de información tanto entrante como saliente de nuestras redes, evitando que personal ajeno tenga acceso a la misma para manipular u obtener información y no puedan afectar el normal funcionamiento de la 32ª Brigada de Infantería con hardware Fortinet o Cisco y un servidor proxy el cual administre solicitudes destinados a otros servidores los cuales no tengan compatibilidad para realizar una conexión directa, de esta manera se aumentaría notablemente los niveles de seguridad informática, al proponer mejoras en las capacidades de seguridad del CECOM, esto implicaría la implementación de soluciones tecnológicas avanzadas, políticas de seguridad actualizadas y una constante preparación del personal para el fortalecimiento de los controles de acceso, la detección y respuesta ante amenazas, la resiliencia ante incidentes, y la concienciación sobre ciberseguridad son clave para proteger las infraestructuras críticas militares. Estas recomendaciones apuntan a aumentar la capacidad de seguridad informática del CECOM de la 32ª Brigada de Infantería, para enfrentar las amenazas actuales y futuras de manera efectiva.

Referencias

Aguado Terrón, J. M. (2004). *Introducción a las teorías de la información y la comunicación.* http://coralito.umar.mx:8383/jspui/bitstream/123456789/1363/1/Introducci%C3%B3n%20a%20las%20Teor%C3%ADas%20de%20la%20Informaci%C3%B3n%20y%20la%20Comunicaci%C3%B3n.pdf

Agudelo, M., Chomali, E., Suniaga, J., Nuñez, G., Jordán, V., & Rojas, F. (2020). *Las oportunidades de la digitalización en América Latina frente al Covid-19*. CEPAL. https://scioteca.caf.com/handle/123456789/1541

Albarracín Keticoglu, A. A. (2019). *Inteligencia nacional y estrategia de ciberseguridad nacional* [Tesis de Maestría, Universidad Nacional de la Plata]. http://sedici.unlp.edu.ar/bitstream/handle/10915/87062/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Álvarez Pinto, J. E. (2019). *Implementación de una arquitectura de red, como aporte a la gestión de seguridad informática del Hotel San Pablo de la provincia de Santa Elena* [Tesis de Licenciatura, Universidad de Guayaquil, Ecuador]. http://repositorio.ug.edu.ec/handle/redug/59969

Baena Paz, G. (2017). *Metodología de la investigación* (3.a ed.). [Recuperado de ProQuest Ebook Central]. http://ebookcentral.proquest.com

Barreto, J. (2017). *La Defensa Nacional y la Estrategia Militar de Seguridad Cibernética*. Argentina. https://cefadigital.edu.ar/bitstream/1847939/1061/1/TFM%2004-2018%20BARETTO.pdf

Cano Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova, 20*(40), 815–832. https://dx.doi.org/10.21830/19006586.866

Carrillo Sáenz, C. & Zapata Díaz, E. (2020). *La Ciberdefensa en el sistema de Comando y Control en la 9ª Brigada Blindada* [Tesis de Maestría, Escuela de Guerra del Ejército de Perú]. http://repositorio.esge.edu.pe/handle/20.500.14141/327

Castro, C., & Filippi, L. (2010). Modelos matemáticos de información y comunicación, cibernética (Wiener, Shannon y Weaver): mejorar la comunicación es el desafío de nuestro destino cultural. *Re-Presentaciones: Periodismo, Comunicación y Sociedad, (6)*, 145–161.

Comando Conjunto de las Fuerzas Armadas. (1989). *MFA-06-03 Manual de Doctrina Operacional de Comunicaciones y Procedimientos de las Fuerzas Armadas (2da Edición)*.

Craig, R. T. (1999). Communication theory as a field. *Communication Theory, 9*(2), 119–161.

Del Perú, Congreso. (1993). *Constitución Política del Perú*. Lima, Perú.

De Moragas Spa, M. (1981). *Teorías de la comunicación*. Gustavo Gili.

De Vergara, E., & Trama, G. (2017). *Operaciones militares cibernéticas. Planeamiento y ejecución en el nivel operacional*. [s. l.]: [s. e.].

Donsbach, W. (2006). The identity of communication research. *Journal of Communication, 56*(3), 437–448.

Donsbach, W. (Ed.). (2008). *The international encyclopedia of communication*. Blackwell.

Ejército del Perú. (2017). *RE 1-53 Diccionario de Términos Militares*.

Ejército del Perú. (1994). *ME 11-5 Empleo de la Compañía de Comunicaciones*.

Galloway, A. (2007). *The Exploit: A Theory of Networks*. [Manuscrito en línea]. https://dss-edit.com/plu/Galloway-Thacker_The_Exploit_2007.pdf

Gómez, P. J. S. (2003). Un modelo pragmático de la comunicación escrita en el aula de ciencias. *Enseñanza de las ciencias: revista de investigación y experiencias didácticas*, 21(2), 307–318.

González, S. G., Canto, S. D., & Moreno, J. S. (2019). La teoría general de sistemas como herramienta de investigación y solución ante la ciberseguridad en sistemas de automatización industrial. *Revista internacional de sistemas, 23*(1), 16–25.

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Technology Research and Development, 29*, 75–91.

Gutiérrez Gómez, G. (2013). *Teoría general de sistemas*. [s. l.]: [s. e.].

Hartley, R. V. (1928). Transmission of information 1. *Bell System Technical Journal, 7*(3), 535–563.

Hernández, R., Fernández, C., & Baptista, P. (2003). *Metodología de la investigación* (3.a ed.). México D.F.: McGraw-Hill.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: McGraw-Hill Education.

Iglesia, G., & Luis, J. (2012). *Teoría de la comunicación de riesgo*. [s. l.]: [s. e.].

Jiménez-Domínguez, B. (2008). Investigación cualitativa y psicología social crítica. Contra la lógica binaria y la ilusión de la pureza. *Investigación cualitativa en Salud*. https://11363399309270719102.googlegroups.com/attach/9f8c3ae9fcaac317/http ww

w.cge.udg.mx_revistaudg_rug17_3investigacion.pdf?part=0.1&view=1&vt=ANaJVrFtLCBxKXUfeV_kgIeHQDbFws2Dy8aiQH_4iBGPvcVHMM3QnHh2CSWS7wY1uSn23AurQBJDb-rUmuog8hPSWXy-23Kg_3pSnsDqg9juduojFRsGnNc

Kuehl, D. (2009). Cyberspace & Cyber power. Defining the problem. En F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyber power & National Security* (pp. X–XX). National Defense University Press.

Ley N.° 1412. (2018). *Ley de Gobierno Digital*. Perú. *(Año de promulgación: 2018)*

Ley N.° 30999. (2019). *Ley de Ciberdefensa*. Perú.

Serrano, M.M. (2009). *La Teoría de la Comunicación, la vida y la sociedad*. [s. l.]: [s. e.]. https://revistas.intercom.org.br/index.php/revistaintercom/article/download/247/240

Martínez. (2020). *Sistema de Comando y Control y sus efectos en la capacidad de respuesta de la 7ª Brigada de Infantería, Lambayeque 2019* [Tesis de Maestría, Instituto Científico Tecnológico del Ejército].

Monje, C. (2011). *Metodología de la investigación cuantitativa y cualitativa: Guía didáctica*. Universidad Sur colombiana / Facultad de Ciencias Sociales y Humanas.

Ochoa Palomino, A. (2019). *Diseño de una Red de Seguridad Informática para la Protección del Sistema Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO 27033* [Tesis de Licenciatura, Universidad de Ciencias Aplicadas, Lima, Perú]. https://repositorioacademico.upc.edu.pe/handle/10757/625726

Pérez, M. W., & Ramos Pilco, M. (2020). *Propuesta de una Política de Ciberseguridad. Universidad de las Fuerzas Armadas de Ecuador* [Tesis de Maestría, Universidad de las Fuerzas Armadas de Ecuador]. http://repositorio.espe.edu.ec/handle/21000/23372

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad, 64*(3), 95–116. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/368

Ritchie, D. (1986). Shannon and Weaver: Unravelling the paradox of information. *Communication Research, 13*(2), 278–298.

Rivera, O. (2019). *Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco. Universidad Daniel Alcides Carrión 2019* [Tesis de Licenciatura]. http://repositorio.undac.edu.pe/handle/undac/1372

Saavedra Cerva, J. A. (2020). *Defensa nacional del Perú y el análisis del sistema de seguridad en la Escuela Militar de Chorrillos "Crl Francisco Bolognesi"*. https://repositorio.escuelamilitar.edu.pe/server/api/core/bitstreams/ec16a59d-5020-42ec-9526-5e21304db733/content

Shannon, C. E., & Weaver, W. (1949). Teoría matemática de la información. *The Bell System Technical Journal, 27*, 379–434.

Svintsytskyi, A. V. (2022). El sistema de organismos de ciberseguridad en Ucrania. *Revista Científica General José María Córdova, 20*(38), 287–305. https://revistacientificaesmic.com/index.php/esmic/article/view/903

Trama, G., & De Vergara, E. (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. https://cefadigital.edu.ar/handle/1847939/939

UPEL. (2005). *Manual de trabajos de grado de especialización y maestría y tesis doctorales*. Caracas: Universidad Pedagógica Experimental Libertador.

Vargas Beal, X. (2011). ¿Cómo hacer investigación cualitativa? *ETXETA*, [s. l.], 138.

Vélez S., C. (2001). *Apuntes de metodología de la investigación*. Departamento de Ciencias Básicas, Universidad EAFIT, Medellín – Antioquia.

Villarrubia Marcelo, G. A. (2021). *Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima, 2018* [Tesis de Maestría, Centro de Altos Estudios Nacionales]. [Repositorio Institucional: Centro de Altos Estudios Nacionales]

Zúñiga, J. (2017). *Ciberdefensa y su incidencia en la protección de la información del Ejército. Caso: COPERE, 2013-2014* [Tesis de Maestría, ICTE, Perú]. http://repositorio.icte.ejercito.mil.pe/handle/ICTE/32

Anexos

ANEXO 1

MATRIZ DE CONSISTENCIA

ANEXO 01. Matriz de consistencia cualitativa

Título: Análisis de la seguridad de red de datos del centro de comunicaciones de la 32ª Brigada de Infantería, 2022

Preguntas de investigación	Objetivos	Teorías	Categorías	Subcategorías	Metodología	Análisis de datos
¿Cómo es el funcionamiento de la seguridad de red de datos en el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022? ¿Cuáles son los ataques informáticos que pueden afectar el funcionamiento de la seguridad de red de datos del Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022? ¿Cuáles son las políticas y controles de seguridad informática que posee el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022? ¿Cuáles son las capacidades de Ciberdefensa que debería poseer en cuanto a seguridad de red de datos el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022?	Analizar el funcionamiento de la seguridad de red de datos en el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022. Describir los ataques informáticos que pueden afectar el funcionamiento de la seguridad de red de datos del Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022. Identificar las políticas y controles de seguridad informática que posee el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32º Brigada de Infantería, 2022. Proponer las mejoras de las capacidades de Ciberdefensa que debería poseer en cuanto a seguridad de red de datos el Centro de Comunicaciones a cargo de la Compañía Comunicaciones N° 32 orgánica de la 32ª Brigada de Infantería, 2022.	Teoría general de sistemas. Teoría de la comunicación. Teoría de la información. Teoría de red de datos.	Seguridad de la red de datos Centro de Comunicaciones de la 32ª Bridada de Infantería	Políticas y controles Ataques cibernéticos Vulnerabilidades de la red Ciberdefensa Personal capacitado Parque Informático Moderno	**Enfoque**: Cualitativo **Tipo**: Teórico- empírico **Método**: Hermenéutico-interpretativo **Informantes** Personal que labora en el CECOM de la 32ª Brigada de Infantería **Muestreo** Cinco (05) expertos que laboran en el CECOM de la 32ª Brigada de Infantería	**Técnicas**: -Análisis documental -Entrevista Observación no participante **Instrumentos**: -Ficha de análisis documental -Guía de entrevista -Guía de observación **Técnica de análisis de datos**: el análisis se realizó de forma artesanal, buscando entender y comprender en forma inductiva la realidad problemática del CECOM, de la 32ª Brigada de Infantería, sobe la base de los temas determinados en la investigación, sobre la base de la unidad de análisis, las cuales fueron sintetizadas a través de la codificación abierta, axial y selectiva.

ANEXO 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

ANEXO 02: Instrumento de recolección de datos

Guía de entrevista

Guía de entrevista sobre “ANÁLISIS DE LA SEGURIDAD DE RED DE DATOS DEL CENTRO DE COMUNICACIONES DE LA 32ª BRIGADA DE INFANTERIA, 2022”

a. Fecha: b. Lugar: c. Hora:

d. Lugar:

e. Entrevistadores: Entrevistador: Bach Félix ESPINOZA LUPUCHE
Moderador: Ídem
Filmador: Ídem

f. Entrevistado:

1. **Introducción:**

   En esta investigación se plantea desarrollar con sustento metodológico y académico un “Análisis de la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022”. La investigación se abordará desde el enfoque cualitativo, es decir será multimetódico, en el cual se estudió el fenómeno en su ambiente natural, pretendiendo darle sentido o interpretarlo, basado en los significados que las personas le otorgan. En tal sentido, el propósito principal del estudio, es presentar una propuesta viable y práctica, para realizar el “Análisis de la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022”, en base a un modelo, a fin de que pueda ser aplicado a las unidades análogas.

2. **Características de la entrevista**

   La entrevista que se aplicó se caracterizó por ser semiestructurada, abierta y planificada. Se consideró que la información obtenida fue válida y fidedigna, dado los amplios conocimientos y experiencia profesional en campo militar de los sujetos entrevistados, particularmente en los temas relacionados a las comunicaciones militares y a la organización de unidades militares, por tanto, se consideró este recojo de datos como “CONFIDENCIAL”. La duración de la aplicación de este instrumento de recolección de datos fue aproximadamente de cincuenta (50) minutos, en un horario previamente concordado con los entrevistados y se condujo conforme a los criterios considerados para elaboración del contenido de la presente guía de entrevista.

3. Preguntas

a. ¿Considera Ud. que la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022 cuenta con las políticas y controles apropiados para su instalación y operación? Explique.
b. ¿Considera Ud. que la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, ha apreciado los ataques cibernéticos posibles que pueden realizarse o debe apreciarse otros tipos de ataques en el desarrollo de las operaciones y acciones militares que realizara la GUC, ¿sean ofensivas o defensivas? Explique.
c. ¿Considera Ud. que la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería se ha considerado en la actualidad o debe apreciarse otras vulnerabilidades en la instalación y operación del equipo y material de comunicaciones satelitales, de radios de microondas, de radios tácticas y de telefonía IP, durante el desarrollo de las operaciones y acciones militares, sean ofensivas o defensivas? Explique.
d. ¿Considera Ud. que, en la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, se ha tenido en cuenta todas las amenazas posibles o debe considerarse otras más, en la instalación y operación del equipo y materiales de comunicaciones satelitales, de radios de microondas, de radios tácticas y de telefonía IP, durante el desarrollo de las operaciones y acciones militares, sean ofensivas o defensivas? Explique.
e. ¿Considera Ud. que la seguridad de la red datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones ofensivas se cumple de acuerdo a las necesidades del Instituto? Explique.
f. ¿Considera Ud. que la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones defensivas se cumple de acuerdo a las necesidades del Instituto en cuanto a Ciberdefensa? Explique.
g. ¿Conoce Ud., el nivel de seguridad que cuenta actualmente la red de datos del Centro de Comunicaciones de la 32ª Brigada de infantería, 2022?
h. ¿Ha identificado Ud., el efecto positivo o negativo que cuenta actualmente la red de datos del Centro de Comunicaciones de la 32ª Brigada de infantería ante posibles ataques cibernéticos?
i. ¿Tiene conocimiento Ud., cuales son las capacidades que debe poseer los operadores que laboran en el Centro de Comunicaciones de la 32ª Brigada de infantería, 2022?

j. ¿Considera Ud., que las capacidades que cuenta actualmente de red de datos del Centro de Comunicaciones en cuanto a seguridad son adecuadas ante un ataque cibernético?

Guía de observación

Indicaciones para el investigador – observador

1. Objetivo principal:

Observar en detalle el nivel de eficiencia y eficacia de la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022.

2. Descripción del instrumento:

La observación tiene como propósito identificar las áreas de mejora para un empleo eficiente y eficaz de la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, Se enfocó en hechos de la realidad para darles sentido y establecer enlaces entre situaciones y acciones. La técnica para la observación y detección de áreas de mejora en la seguridad de red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, es directa, sistemática y continua.

Por tanto, la observación es:

- ***Confiable.*** El investigador se aseguró de que el hecho observado no es resultado de algo fortuito, sino que es constante y verdadero. Es un aspecto de la conducta del elemento evaluado y también puede ser detectado por otra persona.
- **Válida**. La observación adquirió validez porque se aplicó a una situación en la que se apreció con claridad la conducta del elemento evaluado.
- **Precisa*.*** Enfocó exclusivamente el hecho que se deseó destacar y lo separó de todas las acciones que lo rodeó.
- **Objetiva*.*** Se registró y describió la conducta observada, sin calificarla de positiva o negativa.

3. Categorías de observación

Categoría 1: Seguridad de la red de datos*.*

a) Nivel de conocimientos y experiencia sobre la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, en la guerra convencional y la guerra no convencional.

b) Nivel de conocimientos y experiencia acerca de las políticas y controles a desarrollar para garantizar la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones y acciones militares.

c) Nivel de conocimientos y experiencia sobre los posibles ataques que atenten contra la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería,2022 durante las operaciones y acciones militares.

d) Nivel de conocimientos y experiencia sobre las vulnerabilidades que presenta la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones y acciones militares.

e) Nivel de conocimientos y experiencia acerca de las amenazas que atentan contra la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones y acciones militares.

Categoría 2: Centro de Comunicaciones de la 32º Brigada de Infantería.

a) Conocimientos sobre la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones ofensivas y acciones militares.

b) Conocimientos sobre la seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería, 2022, durante las operaciones defensivas y acciones militares.

.

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

ANEXO 03. Validación de instrumentos de recolección de datos

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN:"Analisis de la seguridad de red de datos del centro de comunicaciones 32ª Brigada de infanteria, 2022"

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : CHINCHAY CELADA EDGAR
b. Grado académico-profesión : MAESTRO
c. D.N.I. : 43337057
d. N° de teléfono : 982753451
e. Lugar y fecha : CHORRILLOS 09 JUN 2023
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor del instrumento :Bach Felix Junior ESPINOZA LUPUCHE
b. Institución a la que pertenece:ESGE-EPG
c. Método de investigación :Hermeneutica-Interpretativa
d. Tipo de entrevista :Semiestructurada

III. ASPECTOS DE EVALUACIÓN

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

IV. RESULTADO DE VALORACIÓN:

87%

V. OPINIÓN DE APLICACIÓN

INSTRUMENTO APLICABLE

Aspectos para la valoración

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

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN:"Analisis de la seguridad de red de datos del centro de comunicaciones 32ª Brigada de infanteria, 2022"

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : Flores Mosquito Victor
b. Grado académico-profesión : MAGISTER
c. D.N.I. : 43374708
d. N° de teléfono : 996139417
e. Lugar y fecha : BAGUA 13.10.23
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor del instrumento :Bach Felix Junior ESPINOZA LUPUCHE
b. Institución a la que pertenece:ESGE-EPG
c. Método de investigación :Hermeneutica-Interpretativa
d. Tipo de entrevista :Semiestructurada

III. ASPECTOS DE EVALUACIÓN

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

IV. RESULTADO DE VALORACIÓN:

86 %

V. OPINIÓN DE APLICACIÓN

Instrumento Aplicable

Aspectos para la valoración

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

TÍTULO DE LA INVESTIGACIÓN:"Analisis de la seguridad de red de datos del centro de comunicaciones de la 32ª Brigada de infanteria, 2022"

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : Talavera Prado Gamaliel
b. Grado académico-profesión : Dr en educacion
c. D.N.I. : 09771027
d. N° de teléfono : 996132950
e. Lugar y fecha : Chorrillos 20 feb - 2023
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor del instrumento :Bach Felix ESPINOZA LUPUCHE
b. Institución a la que pertenece:ESGE-EPG
c. Método de investigación :Hermeneutica-Interpretativa
d. Tipo de entrevista :Semiestructurada

III. ASPECTOS DE EVALUACIÓN

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

IV. RESULTADO DE VALORACIÓN:

89 %

Aspectos para la valoración

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

V. OPINIÓN DE APLICACIÓN

Instrumento aplicable

ANEXO 4

AUTORIZACIÓN DE RECOLECCIÓN DE DATOS

ANEXO 04. Autorización de recolección de datos

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

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

Chorrillos, 04 de abril del 2023

Oficio Nº 044 - 2023/ ESGE-EPG/U-26.e.a

Señor : General de Brigada
Comandante General de la 32° Brigada de Infantería
Trujillo.

Asunto : Solicita brindar facilidades al personal que se indica.

Ref. : a. Reglamento para la obtención del grado académico de Maestro en Ciencias Militares AF-2023.
b. Reglamento General de Investigación de la ESGE-EPG

Tengo el honor/agrado de dirigirme a Ud., en relación a los documentos de la referencia, se solicita se digne brindar las facilidades para el levantamiento de datos e informaciones al **My EP ESPINOZA LUPUCHE Félix Junior**, estudiante de la XI Maestría en Ciencias Militares de esta casa de estudios y que realiza la investigación titulada: **"ANALISIS DE LA SEGURIDAD DE RED DE DATOS DEL CENTRO DE COMUNICACIONES 32ª BRIGADA DE INFANTERIA, 2022"**.

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

Dios guarde a Ud.

EJÉRCITO DEL PERÚ - ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

O -2144740731- O +
EMILIO JESUS CAM ALBUJAR
Coronel de Artillería
Sub Director de la Escuela Superior de Guerra
Escuela de Post - Grado

Distribución:
Solicitante.....01
Archivo.....01/02

COMANDO DE EDUCACIÓN Y DOCTRINA DEL EJÉRCITO
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POST - GRADO
SECCIÓN TRAMITE DOCUMENTARIO
MESA DE PARTES
RECIBIDO
Fecha Hora: 27/04/23
Firma

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO – ESCUELA DE POSTGRADO

AUTORIZACIÓN PARA REALIZAR LA INVESTIGACIÓN

DECLARACIÓN DEL RESPONSABLE DEL ÁREA O DEPENDENCIA DONDE SE REALIZARÁ LA INVESTIGACIÓN

Dejo Constancia que el área o dependencia que dirijo, ha tomado conocimiento del proyecto de tesis titulado:

Análisis de la seguridad de la red de datos del Centro de Comunicaciones de la 32° Brigada de Infantería, 2022

El mismo que es realizado por el Señor Bachiller

ESPINOZA LUPUCHE Félix Junior

, en condición de estudiante – investigador del Programa:

Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército - Escuela de Postgrado.

Así mismo señalamos, que según nuestra normativa interna procederemos con el apoyo al desarrollo de la investigación, dando las facilidades del caso para la aplicación de los instrumentos de recolección de datos.

En razón de lo expresado, doy mi consentimiento para el uso de la información y/o la aplicación de los Instrumentos de recolección de datos:

Nombre de la Entidad:	Autorización para el uso del nombre de la Entidad en el Informe Final	SI
Ejército del Perú. - 32ª Brig Inf		NO

Apellidos y Nombres del jefe/Responsable del área	Cargo del jefe/Responsable del área
..... **O - 225360870 – O (+)** **VICTOR SANCHEZ MORALES** **CRL INF**	**Jefe de Estado Mayor Operativo de la 32ª Brigada de Infantería**

ANEXO 5

COMPROMISO ÉTICO

ANEXO 05. Compromiso ético

Declaración de compromiso ético

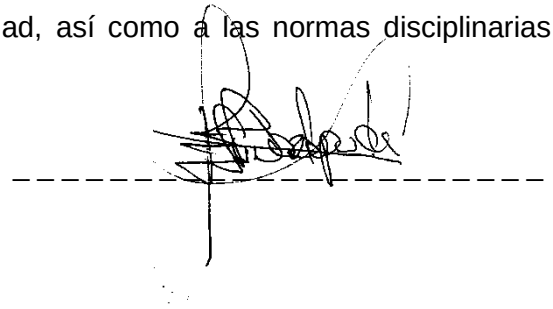
El presente trabajo de investigación titulado: **Análisis de la Seguridad de Red de Datos del Centro de Comunicaciones 32ª Brigada de infantería 2022.**

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

En vista de lo anterior:

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

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



ANEXO 6

HOJA DE DATOS PERSONALES

ANEXO 06. Hoja de datos personales

GRADO: MY COM

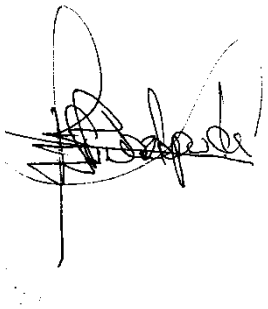
NOMBRES APELLIDOS: Félix Junior ESPINOZA LUPUCHE

EMAIL: FESPINOZAL@ESGE.EDU.PE

DIRECCIÓN: JR HUAYNA CAPAC 181 TAHUANTINSUYO - INDPENDENCIA

CELULAR: 995422131

FIRMA



ANEXO 7

APORTE DE INVESTIGACIÓN

ANEXO 07. Aporte de Investigación

7.1 Título del aporte de investigación

Implementación de un Sistema de Seguridad Informática en el Centro de Comunicaciones de la 32ª Brigada de Infantería con sede en el Distrito Trujillo.

7.2 Objetivos del aporte de investigación

Los Objetivos de la implementación de un Sistema de Seguridad Informática en el Centro de Comunicaciones de la 32ª Brigada de Infantería, son los siguientes:

1. Fortalecer el nivel de seguridad de la red de datos del Centro de Comunicaciones de la 32ª Brigada de Infantería.
2. Renovar el parque informático del Centro de Comunicaciones de la 32ª Brigada de Infantería, con hardware y software de última generación.
3. Capacitar y especializar al personal militar de Comunicaciones de la 32ª Brigada de Infantería en Operaciones Cibernéticas.
4. Realizar una alianza estratégica con el Comando de Telemática y Ciberdefensa del Ejército, para la implementación de un centro piloto de Ciberdefensa en el Centro de Comunicaciones de la 32ª Brigada de Infantería.

7.3 Justificación del aporte de investigación

a. **Justificación de la Implementación de un sistema de seguridad informático al Centro de Comunicaciones de la 32ª Brigada de Infantería.**

1. Frente a las diversas amenazas cibernéticas existentes en el ciberespacio, es necesario proteger la red de datos del Centro de Comunicaciones, debido que, en los hallazgos realizados en la investigación, esta instalación no cuenta con sistemas de protección en lo referente a dispositivos digitales y/o físicos que permitan proteger la información que transita en las redes del Centro de Comunicaciones entre los diferentes niveles de comando.
2. La tecnología y la seguridad son elementos que, van asociados, en la informática, en este sentido se hace necesario contar con equipos de cómputo que, posean dentro de sus características técnicas, protocolos de seguridad para su empleo en una determinada red de datos.
3. La parte principal dentro de la estructura de una organización militar es su personal, en este sentido se hace necesario que, el personal militar comunicaciones que, labora en el Centro de Comunicaciones, tenga los conocimientos necesarios en el tema de las Operaciones Cibernéticas, partiendo de la premisa que la piedra angular dentro de un sistema de seguridad en el hombre.

4. Es importante la realización de alianzas estratégicas con el Comando de Telemática y Ciberdefensa del Ejército, para incrementar la capacidad operativa en la dimensión del ciberespacio en provecho de la 32ª Brigada de Infantería, siendo importante tener la génesis de un centro piloto de Ciberdefensa, tomando como modelo lo desarrollado por el hermano país de Brasil.

b. **Desarrollo de la propuesta**

Primer paso: Se debe establecer un equipo de trabajo, presidido por el Comandante de la compañía comunicaciones N° 32 N° 32, con participación del Jefe de la Sección Telemática, Jefe de la Sección Inteligencia y Contra Inteligencia y el Jefe del centro de comunicaciones de la 32ª Brigada de Infantería, para realizar un estudio de estado mayor donde se analice la conveniencia de implementar un Sistema de Seguridad Informática en la referida unidad de Comunicaciones, a fin de optimizar las medidas de seguridad informática para el manejo de información que, se maneja en la redes con los diferentes niveles de comando de la GUC, asimismo, determinar los elementos sobre los cuales se debe basar dicho sistema de protección de redes.

Segundo paso: Determinada la conveniencia de su implementación, realizar la obtención del citado Sistema de Seguridad Informático el cual deberá requerir de la renovación del parque informático, obtención de un Firewall con su respectivo software y hardware, sistema de detección y prevención de intrusiones y un servidor proxy, lo cual necesariamente requerirá la formulación de un expediente técnico para la adquisición de dichos componentes, por aproximadamente la suma de (S/. 47,000.00), que incluya también una capacitación por parte de las empresas privadas dirigido al personal militar del arma de Comunicaciones de la 32ª Brigada de Infantería sobre el empleo de los diferentes sub sistemas, Kits de repuestos y el mantenimiento de los equipos que conformarían el Sistema de Seguridad Informática. Donde toda esta referida adquisición, debe estar acompañada de una garantía a cargo del proveedor de los diferentes sub sistemas.

Tercer paso: Revisión de la doctrina operativa del Arma de Comunicaciones, principalmente en los conocimientos básicos de las Operaciones Cibernéticas y el empleo de la compañía comunicaciones N° 32 Nº 32 de la 32ª Brigada de Infantería, respecto al empleo de redes informáticas de comunicaciones para el enlace con los diferentes niveles de Comando, a la luz de las necesidades externas y/o internas de comunicación que, se requiera de acuerdo a la situación existente.

c. Coordinaciones

Realizar coordinaciones con el CITELE para realizar una supervisión técnica para la implementación del sistema de seguridad informático, para establecer de manera adecuada las características técnicas de cada material propuesto como componente de dicho sistema. Asimismo, la 32ª Brigada de Infantería, gestione ante el escalón superior la inclusión de la adquisición de este sistema en su respectivo presupuesto, en cuanto a los equipos que se requieran para materializar y mantener la seguridad de la red informática en el Centro de Comunicaciones.

d. Instrucción y capacitación

Desarrollo de un Plan de Capacitación propuesto a cargo de las empresas proveedoras.

Desarrollo de programa de capacitación presencial y virtual a cargo del CITELE sobre el conocimiento de las Operaciones Cibernéticas, la importancia de preservar el ciberespacio como parte de nuestra soberanía y conocimiento de las diferentes amenazas cibernéticas existentes, orientado a los Oficiales, Técnicos y Sub-Oficiales de Comunicaciones de la 32ª Brigada de Infantería, en coordinación con las empresa proveedoras de los equipos que conformaran el Sistema de Seguridad Informática del Centro de Comunicaciones.

Desarrollo de un Plan de Instrucción en Operaciones Cibernéticas por parte de Oficiales del hermano país de Brasil, para adquirir experiencias sobre su empleo del centro de Ciberdefensa.

ANEXO 8

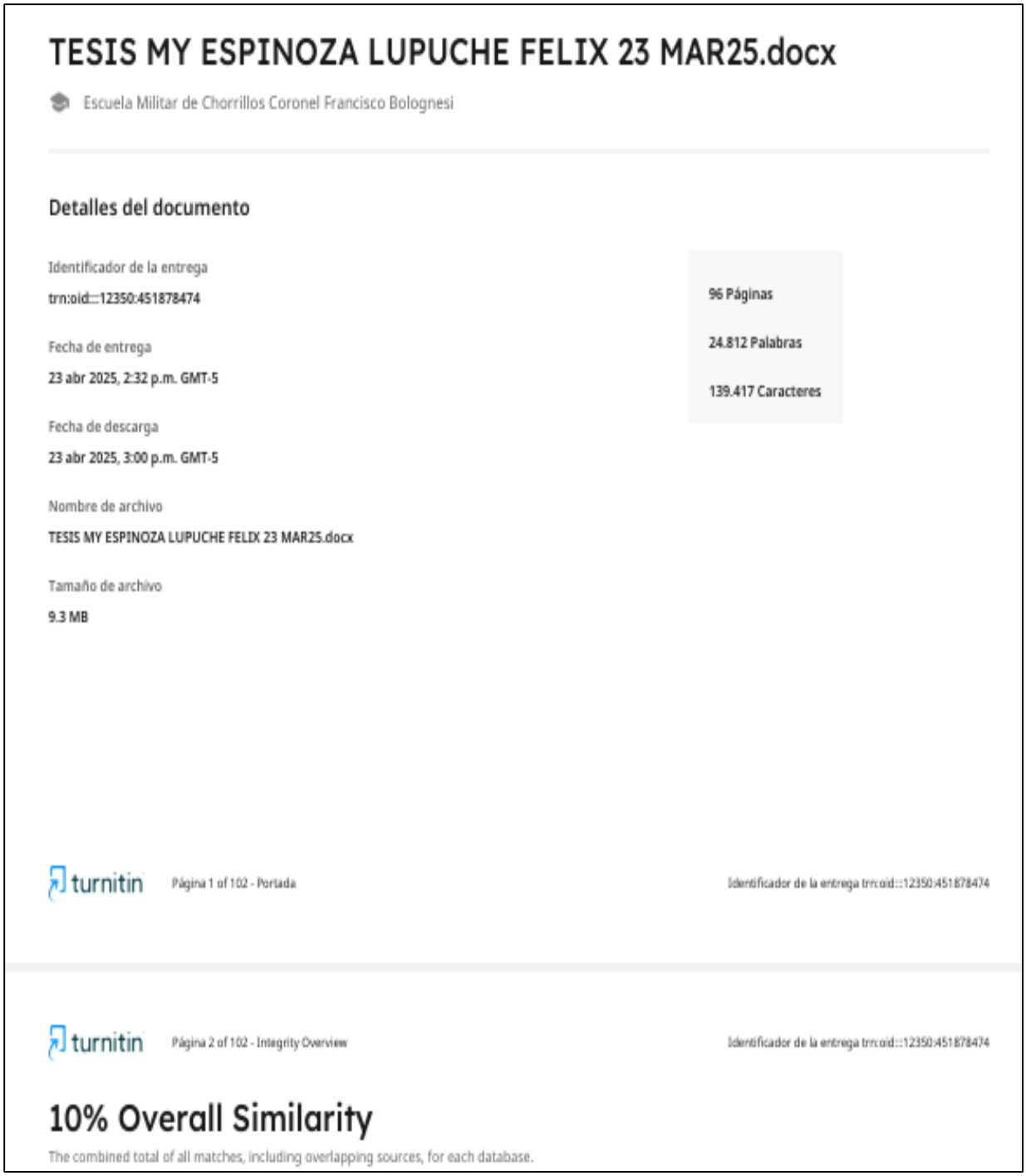
CD CONTENIENDO LA TESIS EN PDF

ANEXO 08. CD contenido de tesis en PDF

ANEXO 9

REPORTE DE SIMILITUD DE TURNITIN

ANEXO 09. Reporte de similitud de turnitin



TESIS MY ESPINOZA LUPUCHE FELIX 23 MAR25.docx

Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:451878474

Fecha de entrega
23 abr 2025, 2:32 p.m. GMT-5

Fecha de descarga
23 abr 2025, 3:00 p.m. GMT-5

Nombre de archivo
TESIS MY ESPINOZA LUPUCHE FELIX 23 MAR25.docx

Tamaño de archivo
9.3 MB

96 Páginas

24.812 Palabras

139.417 Caracteres

turnitin Página 1 of 102 - Portada Identificador de la entrega trn:oid:::12350:451878474

turnitin Página 2 of 102 - Integrity Overview Identificador de la entrega trn:oid:::12350:451878474

10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.