ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POST GRADO

TESIS

ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022

AUTOR

Bach. Anibal Willibrord Mercado Cortez
0000-0003-1615-9510

Para optar al Grado Académico de

MAESTRO EN CIENCIAS MILITARES

Con mención en Planeamiento Estratégico y Toma de Decisiones

ASESOR

Mg Roberto Joaquín VIVANCO BURGOS

0000-0002-4360-8396

2023

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 039 – 2023/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veinticuatro días del mes de octubre del año dos mil veintitrés, siendo las ...1230... horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctora**	**BERTHA MILAGROS VILLALOBOS MENESES**	**Presidente**
❖	**Doctor**	**GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**	**Vocal**
❖	**Maestro**	**EMILIO JESUS CAM ALBUJAR**	**Secretario**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 039-2023/SIE/DGI/ESGE-EPG** del 10 de octubre del 2023, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**, presentado por el Bachiller **MERCADO CORTEZ ANIBAL WILLIBRORD,** 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 ...Aprobar por Unanimidad (16)...

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.

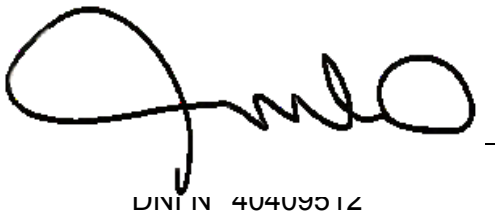
Firmado, en Chorrillos a los veinticuatro días del mes de octubre del 2023.

DRA BERTHA MILAGROS VILLALOBOS MENESES	**DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**	**MG. EMILIO JESUS CAM ALBUJAR**
PRESIDENTE	**VOCAL**	**SECRETARIO**

Autorización de Publicación y Uso

Yo, Bach. Mercado Cortez Anibal Willibrord 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 Ciberseguridad como Prioridad Institucional en el Comando Logístico del Ejército, 2022** presentada para optar al grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones en el Repositorio Institucional y en el Repositorio Nacional de Tesis (Renati) de la Superintendencia Nacional de Educación Superior Universitaria (Sunedu), de conformidad al marco legal y normativo vigente. La tesis se 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, 20 de agosto de 2022



DNI N° 40409512

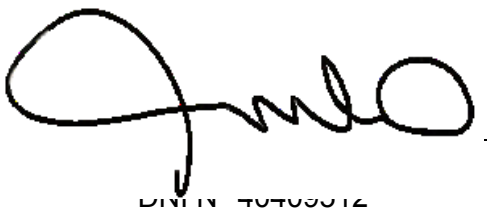
Declaración jurada de autoría

Mediante el presente documento, Yo, Bach. Mercado Cortez Anibal Willibrord, identificado con Documento Nacional de Identidad N° 40409512, con domicilio real en calle Coronel Ayllón N° 169, del distrito de Chorrillos, provincia de Lima, departamento de Lima, estudiante / egresado de la V Maestría en Ciencias Militares con Mención en Planeamiento estratégico y Toma de Decisiones 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 CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022** que presento a los 12 días de diciembre del año 2022, ante esta institución con fines de optar al 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 y otros que corresponden 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 como el único responsable.



DNI N° 40409512

Dedicatoria

A mi esposa e hijas, soporte de esta difícil carrera y en memoria de las personas que desde el cielo guían mi camino.

ÍNDICE

Lista de tablas

Página

Lista de figuras

Página

Resumen

La presente investigación presentó como objetivos: Describir la importancia institucional de la ciberseguridad según el marco normativo vigente, analizar la situación actual de ciberseguridad y describir el riesgo que está expuesto el Comando Logístico del Ejército (Cologe) respecto a la ciberseguridad de la información que maneja, que permitió analizar el contexto actual de la ciberseguridad en el Comando Logístico del Ejército, para ello se utilizó el enfoque cualitativo, el tipo de investigación fue aplicada con una muestra de seis (06) participantes que fueron seleccionados al azar de cada sección de estado mayor de la división.

El Comando Logístico del Ejército (Cologe) constituye la dependencia encargada de llevar a cabo el proceso logístico institucional tanto para operaciones como acciones militares, este se articula con otras dependencias en la institución que en su conjunto llevan el flujo de la corriente logística a nivel nacional y a todas sus dependencias, en tal sentido la información que maneja es álgida pues constituyen aspectos de cargos, operatividad, año de fabricación etc., que llevan a proporcionar particular atención en la ciberseguridad que debe tener para proteger el cúmulo de datos que maneja.

En ese sentido, después de haber realizado el análisis correspondiente se llegó a las siguientes conclusiones: La situación actual de ciberseguridad por parte del Cologe es deficiente o nula, el personal desconoce lo que es ciberseguridad, procedimientos mínimos de seguridad como son las contraseñas que deben ser cambiadas cada cierto tiempo, la seguridad externa e interna mediante firewalls que protejan la información que manejan diariamente y comparten con otras dependencias, además de emplear el aplicativo de WhatsApp para intercambiar información a nivel nacional, contraviniendo lo descrito por la Directiva Única de Funcionamiento del Sistema Telemática del Ejército (Dufsitele) respecto a la trasmisión de información en la institución.

Palabras clave: ciberseguridad, ataque cibernético, hackers.

Abstract

The present investigation presented as objectives: Describe the institutional importance of cybersecurity according to the current regulatory framework, analyze the current cybersecurity situation and describe the risk that the Army Logistics Command (Cologe) is exposed to regarding the cybersecurity of the information it manages, which allowed analyzing the current context of cybersecurity in the Army Logistics Command, for this the qualitative approach was used, the type of research was applied with a sample of six (06) participants who were randomly selected from each state section major of the division.

The Army Logistics Command (Cologe) constitutes the unit in charge of carrying out the institutional logistics process for both operations and military actions, this is articulated with other units in the institution that as a whole carry the flow of the logistics current at the national level. and to all its dependencies, in this sense the information it handles is critical since it constitutes aspects of charges, operation, year of manufacture, etc., which lead to providing particular attention to cybersecurity that it must have to protect the amount of data it handles. In this sense, after having carried out the corresponding analysis, the following conclusions were reached: The current cybersecurity situation by Cologe is deficient or non-existent, the staff does not know what cybersecurity is, minimum security procedures such as the passwords that must be changed for some time, external and internal security through firewalls that protect the information they handle daily and share it with other agencies, in addition to using the WhatsApp application to exchange information at the national level, in contravention of what is described by the Dufsitele regarding the transmission information in the institution.

Keywords: cybersecurity, cyber-attack, hackers

Introducción

La ciberseguridad hoy en día es una preocupación latente en el Ejército del Perú, la práctica de proteger los sistemas más importantes y la información confidencial ante ataques cibernéticos también conocida como seguridad de la Tecnología de la Información (TI), cobra vital importancia con los sucesos ocurridos en México, en los cuales el grupo activista de hackers Guacamaya logró hackear 400,000 correos electrónicos del Estado Mayor Conjunto de las Fuerzas Armadas mexicanas, lo cual nos permite interiorizar la débil y deficiente barrera de protección que se dispone.

El desarrollo de la investigación aborda al Comando Logístico del Ejército (Cologe) como dependencia encargada de llevar a cabo todo el procedimiento logístico y satisfacer las necesidades de la fuerza para operaciones y acciones militares, para ello desarrolla sus actividades con el personal, equipo y medios que permitan el cumplimiento de su misión.

Actualmente se aprecia que los hackers informáticos cada día están ampliando su radio de acción, es común ver en los medios sobre ataques a organizaciones, empresas, instituciones militares con suma facilidad, que nos llevan a pensar que tan vulnerables somos y como se encuentra el aspecto de la ciberseguridad de la información que se maneja al interior de las instituciones militares, en ese sentido, la investigación se centró en analizar cuál es la situación actual de la ciberseguridad en el Comando Logístico del Ejército y por qué debe ser de prioridad institucional el cuidado y custodia de la información, para ello a través del enfoque cualitativo se dio respuesta a la pregunta de investigación planteada que permitió realizar las conclusiones y recomendaciones adecuadas que permitan mejorar la ciberseguridad en el Cologe.

Para ello la presente investigación se desarrolló en cinco capítulos que se detallan a continuación:

En el primer capítulo, se trató sobre el planteamiento del problema de investigación, en el que se describe la realidad actual del Cologe respecto a la ciberseguridad de la

información que maneja, desprendiéndose alineadamente las preguntas y objetivos de la investigación, así como, la justificación e implicaciones prácticas de la investigación realizada.

En el segundo capítulo, se enfocó el estado del conocimiento de la investigación desarrollada como sustento para la elaboración del presente trabajo, permitió revisar investigaciones hechas sobre el tema de estudio, desde el punto de vista de su actualidad y valor teórico, las teorías o soporte teórico que se pudieron debatir, ampliar, conceptualizar y concluir, así como el marco conceptual, siendo entre ellas teoría de la ciberamenaza, teoría del ciberespacio y la ciberseguridad en el ámbito militar, que describen las características y procedimientos para el manejo de la información actualmente.

En el tercer capítulo de acuerdo al tipo de problema se definió el diseño metodológico más idóneo para la investigación, todo ello centrado en un trabajo de campo adecuado que permitió levantar la información correspondiente con los instrumentos más adecuados y con la debida riqueza interpretativa para su posterior análisis, se plantearon dos instrumentos de investigación los mismos que fueron triangulados adecuadamente para contrastar los resultados y así poder dar el rigor científico correspondiente.

En el cuarto capítulo se realizó el análisis y síntesis de la investigación, para ello se analizó de acuerdo al libro de Hernández Sampieri (Metodología de la Investigación, la ruta de la investigación cualitativa, cuantitativa y mixta, edición 2018) donde se desarrolló inicialmente una codificación abierta de las unidades de análisis, posteriormente una codificación axial y después la selectiva que permitió enfrentar el problema desde una perspectiva holística y dar respuesta a las preguntas de investigación planteadas.

En el quinto capítulo se realizó el diálogo teórico empírico, donde se confrontó la teoría con los hallazgos empíricos, en el sexto capítulo se establecieron las conclusiones y recomendaciones donde se refleja lo que se quiso comunicar como resultado de las experiencias de los participantes, respecto a la importancia de la ciberseguridad y la prioridad institucional que debe darse al Cologe.

Capítulo I: Planteamiento del Problema

1.1 Planteamiento del problema

El siglo XXI es el siglo de la expansión de la digitalización, que se caracteriza por la constante e imparable evolución tecnológica, y de la mano de la inteligencia artificial o el big data, traen consigo vastos beneficios que simplifican la vida de los seres humanos, sin embargo, traen también numerosos riesgos. Un mundo totalmente digitalizado es vulnerable a los ataques cibernéticos, los mismos que están cada vez más a la orden del día, pudiendo no solo vulnerar información delicada, sino que también pueden acceder, modificar o dañar un sistema de redes tanto de empresas particulares como de entidades gubernamentales.

En el Perú, la pandemia de la COVID 19 fue una de las causales para que diferentes entidades empiezan a incrementar de manera exponencial el uso de plataformas virtuales, ya sea para realizar ventas online o para la prestación de servicios, asimismo, las instituciones públicas o privadas, constituyeron la modalidad del trabajo remoto para dar continuidad a los servicios que prestan, en ese entorno:

> Los hackers informáticos también aumentaron, ataques a empresas e incluso a redes de ejércitos como es el caso del Ejército de Colombia el año 2021 atribuida a Anonymous, y la que ha sufrido recientemente el Ejército del Perú, considerada como el mayor hackeo de su historia, que puso al descubierto planes convencionales con el vecino país del sur. (Quintana, 2021, p. 19).

1.1.1 ¿Cómo se vulnera la seguridad de la información?

Pereda (2019), sostuvo:

> A los ataques malintencionados perpetrados a través de cauces electrónicos contra las bases de datos se les denomina guerra de la información o ciberguerra*,* dependiendo de sus fines, se habla de delincuencia o terrorismo cibernético, un intruso informático puede acceder y emplear información privada referida a determinado grupo al que no pertenece. De este modo, destruye la confidencialidad y, al mismo tiempo, la confianza en la seguridad que ofrecen las nuevas tecnologías, requisito básico para el correcto funcionamiento de la sociedad de la información. (p.37).

Asimismo, un intruso puede acceder a la información a través de distintos medios, los más comunes son a través de la manipulación de los archivos mediante la alteración de la base de datos con la finalidad que respondan al propósito de hurtar la información, otra

modalidad es mediante la creación de comandos no válidos y poder llegar a destruir el sistema mediante la degradación de sus medios.

Otra de las modalidades más usadas por los hackers informáticos que actualmente es muy común en empresas de servicios es:

> Mediante el envío masivo de información, se puede bloquear un servidor temporalmente o hacer que quede por completo inservible, para ello, el malhechor puede ordenar el envío simultáneo de programas no autorizados y autoinstalables a gran cantidad de ordenadores que no cuentan con la suficiente protección, dichos programas, controlados remotamente, enviarán a su vez de forma masiva paquetes de datos que bloquearán e inutilizarán las redes al saturar su capacidad de procesamiento de información. (Armero y Calderon, 2018, p. 45).

Una bomba lógica, constituye para un hacker una modalidad de extraer información clasificada a través de un ordenador, al respecto:

> Para ello, los virus informáticos se pueden inocular en el sistema como portadores de un material nocivo que se transmitirá de archivo en archivo o, a mayor escala, irá infectando otros sistemas conectados a la misma red. Al pirata le es posible limitar la capacidad del ordenador que ataca, o bien alterar la lógica interna del sistema de manera que éste produzca respuestas absurdas cuando no nocivas. (Clarke y Knake, 2018, p. 126).

Quintana (2021) sostuvo:

> En Latinoamérica, los países más afectados por el aumento de ciberataques ha sido México, con 60,8 mil millones; Brasil, con 16,2 mil millones; Perú, en el tercer lugar con 4,7 mil millones y Colombia, con 3,7 mil millones, según un estudio de la firma de ciberseguridad Fortinet**,** Perú ha sufrido más de 4,700 millones de intentos de ciberataques solo durante el primer semestre del 2021, esto representa casi 300 ataques por segundo en el país, cifra preocupante por la cantidad de amenazas. (p.34).

El incremento es preocupante no solo por el alto volumen de amenazas, sino también por el aumento de personas que cada vez destruyen sistemas operativos y roban la información:

> Una de las consecuencias que se puede tener es la proliferación de delitos informáticos, delitos sofisticados como el virus informático ransomware, que destacan

> tanto por la pérdida económica como por el daño a la imagen que causan a las empresas y la información personal que acceden los hackers informáticos. (Machin y Gazapo, 2017, p.35).

> En Estados Unidos la seguridad en el ciberespacio, así como la ciberseguridad está a cargo de una empresa de seguridad denominada «Homeland Security», habiendo nombrado desde el gobierno de OBAMA, un coordinador de ciberseguridad en la Casa Blanca, responsable de supervisar una estrategia nacional para garantizar los intereses de los americanos en el ciberespacio. En el ámbito militar americano, ya desde hace unos años, se han llevado a cabo trabajos para la obtención de una capacidad de Operaciones en el Ciberespacio en cada uno de los ejércitos protegiendo de esta manera la información que se trasmite diariamente. (Del rio, 2011, p. 45).

Otro virus muy nocivo que se inocula a través de un tercero bajo la modalidad de protección es:

> Mediante descarga desde la red, se puede introducir en el sistema un virus del tipo Caballo de Troya que actuará sobre él una vez transcurrido el tiempo determinado por el programador. Igualmente, el pirata puede ocultar su identidad o falsificarla modificando, por ejemplo, el remitente desde el que envía los paquetes de datos, de forma que la autenticidad de determinados archivos quede destruida, o bien emplear un ordenador al que ha accedido como estación intermedia desde la que emprender nuevos ataques a terceros sistemas. (Machin y Gazapo, 2017, p. 56).

Sin embargo, una de las causales que más afecta la ciberseguridad en todos los campos de la actividad es el desconocimiento de conceptos básicos y medidas de seguridad que deben ser usadas por los usuarios de las PC, debido que, no se establecen medidas de seguridad adecuadas para proteger la información.

En el Perú, el Reglamento del DL Nº 1412 (2019), Ley de Gobierno Digital en su Artículo 103 sostuvo:

> Adopción de estándares y buenas prácticas, establece que las entidades de la Administración Pública pueden adoptar normas técnicas peruanas o normas y/o estándares técnicos internacionales ampliamente reconocidos en materia de gestión de riesgos, gestión de incidentes, seguridad digital, ciberseguridad y seguridad de la información en ausencia de normas o especificaciones técnicas nacionales vigentes. (p.17).

En este contexto, la ciberseguridad del Comando Logístico del Ejército (Cologe), dependencia encargada de manejar información sensible respecto a los medios que dispone la institución, así como de las actividades que anualmente se realizan para aumentar la capacidad operativa, no cuenta con un buen manejo de la ciberseguridad. Después de haber conversado con algunos oficiales, técnicos, personal civil, si tienen alguna noción sobre ciberseguridad, muchos de ellos carecen del concepto de ciberseguridad, siendo este aspecto en la actualidad con la utilización de las redes informáticas, del trabajo remoto prioritario debiendo ser internalizado por cada uno de los integrantes con la finalidad de evitar ataques informáticos, se maneja información por WhatsApp, correos personales para trasmitir y recibir información como oficios, directivas, etc., vulnerando las normas que se deben seguir para poder contar con medidas de seguridad adecuadas que permitan contar con controles necesarios y garantizar la seguridad de su infraestructura, evitando que se afecte la confidencialidad que posee toda información, de manera que, pueda de ser utilizado por el personal adecuado, sin embargo, aún parece utópico alcanzar tal grado de protección de la información.

1.2 Justificación de la investigación

La presente investigación contribuirá al vacío del conocimiento de un tema muy actual pero poco fomentado en el Comando Logístico del Ejército (Cologe) respecto a la ciberseguridad, los resultados se pueden generalizar a otras dependencias, la información que se obtenga de los resultados puede servir para crear protocolos de control de la información, sugiriendo ideas, que permitan que el personal se concientice con el riesgo y manejo de la información que maneja la institución y lo que pudiera suceder si fuera hackeada, con respecto a las implicaciones prácticas, ayudaría a resolver el problema de la ciberseguridad en el Cologe.

1.3 Delimitación de la investigación

La investigación se situará en el contexto de la seguridad que se utiliza para el flujo de información por el personal que labora en el Comando Logístico del Ejército, ubicado en la ciudad de Lima (Cuartel General del Ejército), la delimitación temporal es el año 2022.

1.4 Limitaciones de la investigación

La investigación tiene como limitaciones el tiempo para el levantamiento de la información, se va a superar con la coordinación de las entrevistas sean estas aprovechando los medios digitales como Zoom.

1.5 Formulación del problema

¿Cuál es la situación actual de ciberseguridad en el Comando Logístico del Ejército (Cologe)?

¿Cuál es el riesgo que genera el uso no adecuado de la información en el Comando logístico del Ejercito (Cologe)?

¿Cuál es el protocolo de ciberseguridad obligatorio para el personal que labora en el Comando logístico del Ejercito (Cologe)?

1.6 Objetivos de la investigación

Describir la situación actual de ciberseguridad en el Comando Logístico del Ejército (Cologe).

Describir el riesgo que genera el uso no adecuado de la información en el Comando logístico del Ejercito (Cologe).

Implementar protocolo de ciberseguridad obligatorio para el personal que labora en el Comando logístico del Ejercito (Cologe).

Capítulo II: Marco Teórico

2.1 Antecedentes de la investigación

Hernández-Sampieri et al. (2010) sostuvieron:

> Esta etapa de la investigación permite ahondar y contextualizar el problema de investigación, se debe conocer estudios, investigaciones y trabajos anteriores, ver qué cosa se ha investigado con respecto al tema que se está abordando, especialmente si uno no es experto en tal tema, conocer lo que se ha hecho con respecto a un tema ayuda a no investigar sobre algún tema que ya se haya estudiado a fondo, esto implica que una buena investigación debe ser novedosa, lo cual puede lograrse al tratar un tema no estudiado, profundizar en uno poco o medianamente conocido, o al darle una visión diferente o innovadora a un problema aunque ya se haya examinado repetidamente (p. 28).

Coincidiendo con esto Granada (1984) sostuvo:

> Todo hecho anterior a la formulación del problema que sirve para a aclarar, juzgar e interpretar el problema planteado, constituye los antecedentes del problema, establecer los antecedentes del problema, de ninguna manera es hacer un recuento histórico del mismo, sino se trata de hacer una síntesis conceptual de las investigaciones y trabajos realizados sobre el problema formulado. (p.76).

2.1.1 Antecedentes nacionales

Ormachea (2019) en su tesis titulada: *Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional*, para obtener el Grado de Doctor en el Centro de Altos Estudios Nacionales, con el objetivo de:

> Proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, así como, Identificar las limitaciones referentes al desarrollo de la ciberseguridad en el Perú, mediante un enfoque sistémico que abarca el ámbito nacional a través de encontrar estrategias que permitan desarrollar mecanismos que permitan implementar la ciberseguridad en el ámbito nacional, mediante la aplicación del marco normativo vigente protegiendo de esta manera el valor de la información estratégica y crítica del Estado, y el de las que son publicadas por los peruanos en la red. (Ormachea, 2019, p. 64), concluyó que:

> El desarrollo de una cultura de ciberseguridad constituye un punto crítico importante para la obtención del desarrollo socioeconómico de un área, sector empresa, institución, en ese sentido, se deben establecer estrategias que deben ser

> implementadas según el análisis situacional de cada país, asimismo, estas deben ser plasmadas en normas, reglamentos que desarrolle una cultura de ciberseguridad, a su vez el seguimiento y monitoreo permanente del personal. (Ormachea, 2019, p. 45).

La tesis se relaciona con la investigación, por cuanto establece el análisis integral de la ciberseguridad de acuerdo con la utilización de la información y el tipo de seguridad que se debe aplicar, en ese sentido, la investigación enfocará el área del Comando Logístico del Ejército, a través de la información sensible que maneja respecto a la logística institucional.

Huamán (2020) en su tesis de maestría: *Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército*, tuvo como objetivos:

> Describir las capacidades de Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército para brindar soporte y apoyo, así como, explicar de qué manera sus capacidades protegen la integridad y confiabilidad de la información que maneja la Dirección de Telemática y Estadística del Ejército. (Huaman, 2020, p. 34).

Asimismo, respecto a la seguridad que debe tener el manejo de la información sostuvo:

> La seguridad inicial o primaria es la que es dada por el usuario inicial, previa a ello se debe tener conocimiento de la situación así como los riesgos que puede ocasionar la vulneración de la información, sumado al actual ambiente de pandemia del COVID 19, donde los ataques cibernéticos cobraron más vigor, para ello es imperante establecer mecanismos que permitan incrementar la capacidad de ciberseguridad y ciberdefensa, para ello se diferencian dos aspecto bien definidos, el primero la ciberseguridad en un primer nivel, asegurando este a través de la ciberseguridad se puede establecer el segundo nivel de la ciberdefensa, es decir estos términos se asocian con una sola finalidad. (Huaman, 2020, p. 37).

La defensa de la información sea este por medios electrónicos o por el espacio electromagnético, utilizando la metodología cualitativa concluye que; existe un proceso de formación e implementación con respecto al apoyo que debe proporcionar a través de sus capacidades el Centro de ciberdefensa y telemática del Ejército, además este proceso deba ser bien apoyado por la Jeduce y el Coede.

Taípe (2020) en su tesis titulada: *La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú, año 2017*, en la Universidad Nacional de Piura, tuvo como objetivo:

> Determinar de qué manera se relaciona las Políticas de Ciberseguridad con respecto a la Ciberseguridad, así como, la relación de la Ciberseguridad con respecto a los Riesgos de la información digital del Sector Público, siendo uno de sus sustentos de la problemática identificada la existencia de personas malintencionadas que pueden causar daño a la información digital que manejan. (Taipe, 2020, p. 27).

Asimismo, se puede acceder a los lugares de almacenamiento, a través del empleo de hackers para romper las contraseñas y apoderarse de archivos que pueden ser usados en contra de las personas o de la organización, utilizando para ello un enfoque cuantitativo, concluyó que:

> Es muy poco el conocimiento del personal que labora en las áreas de informática, sin embargo, debe ser necesario conocer los riesgos a los que se está expuesto cuando se maneja información sensible relacionada a procesos y actividades cotidianas de la organización poseen bajos niveles de conocimiento con respecto al concepto de ciberseguridad, siendo este un riesgo que podría ser aprovechado por hackers para el acceso a la información de manera ilícita. (Taipe, 2020, p. 29).

Asimismo, también se puede encontrar que existen otras formas como es el escaneo, claves de acceso, aplicaciones, borrado de huellas, etc. son realizados por personal técnico y adiestrado para tal fin, asimismo, muchas veces un gobierno puede estar vinculado a un tema de ciberseguridad con otro a través de empleo de diferentes medios para obtener la información, la ciberseguridad es un problema generalizado hasta el nivel de Estado. Esta tesis se relaciona con la investigación, en el sentido que aporta una deficiencia y riesgo de la información a través del usuario inicial quien por desconocimiento de medidas de protección de la información pone en riesgo a esta.

Mallma y Flores (2019) en su tesis titulada: *Implementación de la asignatura de ciberseguridad y la formación profesional de los cadetes del arma de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi – 2019*, para optar el grado académico de Licenciado en Ciencias Militares, en la Escuela Militar de Chorrillos, Perú, donde tuvieron como objetivo:

> Describir la relación existente entre la ciberseguridad y la asignatura correspondiente a esta materia impartida a los cadetes de inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, asi como, como el adquirir conocimientos sobre esta materia contribuye a la formacion profesional de los cadetes de Inteligencia, con la finalidad que puedan ser aplicados proactivamente en beneficio institucional. (Malma y Flores, 2019, p,35).

Para ello emplearon el enfoque cuantitativo donde a partir de cuestionarios abordaron las siguientes conclusiones:

> La formación académica que recibe el cadete es muy insipiente, no existe una buena formación profesional sobre este concepto que debe ser de conocimiento común por todo el personal, para que cuando salgan a sus unidades sean entes multiplicador de buenas prácticas a desarrollarse por el personal militar de todas las dependencias, asi como, que la no existencia de la doctrina de ciberdefensa y ciberseguridad, por ende, un bajo nivel de conocimiento en esta materia, no pudiendo durante los primeros años de oficial asesorar y recomendar la implementación de mecanismos que conlleven a la ciberseguridad empezando por ellos mismos, con la finalidad de recomendar aspectos basicos que permita tener un nivel de ciberseguridad adecuado, asimismo, se debe stablecer seminarios sobre sensibiliacion que permitan tomar conciencia del gran riesgo que existe sin no se hace un adecuado tratamiento de la información. (Malma y Flores, 2019, p675).

Esta tesis se relaciona con la investigación, pues desarrolla el aspecto de falta de conocimientos a partir del personal de cadetes de inteligencia en ese sentido, si embargo, actualmente se puede apreciar que existe un total desconocimiento de aspectos comunes que llevan a desarrollar una cultura de ciberseguridad en la Escula Miitar de Chorrillos.

2.1.2 Antecedentes Internacionales

Las investigaciones que después del proceso de búsqueda permitieron enmarcar el problema de investigación en el campo del conocimiento y guardaron relación con nuestro objeto de estudio; fueron las siguientes:

Guerrero y Proaño (2020) en su tesis: *El manejo de la ciberseguridad en Fuerzas Armadas,* para obtener el Grado de Magister en Estrategia Militar Terrestre, en la Universidad de las Fuerzas Armadas de Ecuador tuvieron como objetivo:

> Establecer la necesidad de la protección de la información estratégica que manejan las Fuerzas Armadas vital para el Estado en materia de Defensa, pare ello implementar y desarrollar proteger la infraestructura por donde fluye la información, las redes estratégicas y la información electrónica; el desarrollo de las capacidades de ciberdefensa; y, el fortalecimiento de los mecanismos interinstitucionales para hacer frente a las amenazas cibernéticas. (Guerrero y Proaño, 2020, p. 61).

Asimismo, a través de un estudio integral del riesgo inicial que permita un diagnóstico del nivel de ciberseguridad:

> Determinar un mecanismo articulador entre la doctrina y las capacidades que podrían minimizar las posibles amenazas y riesgos existentes en el manejo de la Ciberseguridad en las Fuerzas Armadas, a fin de establecer los lineamientos doctrinarios ante la necesidad de la protección de la información estratégica del Estado en materia de Defensa y Seguridad. (Guerrero Proaño, 2020, p. 34).

Los autores después de evaluar de manera holística la problemática de la ciberdefensa concluyeron que:

> El disponer de una capacidad adecuada para vigilar las redes y así detectar de manera oportuna los ataques de red, reduce considerablemente el tiempo de respuesta y la capacidad para recuperar los servicios afectados, por lo tanto, es fundamental disponer de la correspondiente plataforma de supervisión de la seguridad, entendida ésta como una plataforma especializada que se centra en la gestión de la seguridad de los sistemas de información y de las redes bajo la responsabilidad de una determinada organización. (Guerrero y Proaño, 2020, p. 45).

La tesis aporta a la investigación, en el sentido que prioriza la necesidad de la protección de la información, particularmente en las fuerzas armadas, además establece un ente encargado de realizar el control, dirección de la ciberseguridad mediante un monitoreo permanente, a nivel nacional.

Baretto (2017) en su tesis titulada: *La Defensa Nacional y la estrategia militar de seguridad cibernética*, para optar el grado académico de Magíster en Estrategia y Conducción Superior, en la Escuela Superior de Guerra Conjunta, Argentina, tuvo como objetivo:

> Analizar de qué manera los delitos cibernéticos en los últimos años se han convertido en los actos delictivos cuyo crecimiento fue exponencial con el empleo masivo de las redes informáticas y los teléfonos, razón por ello más personas se suman a estos ilícitos con la finalidad de ingresar a los sistemas de computadoras para robar datos que pueden ser usados para otros ilícitos consecuentes. (Baretto, 2017, p. 54)

Asimismo, establece que de manera general las organizaciones asignan escasos recursos en contra de estas actividades, lo que ocasiona que se genere una vulnerabilidad, sumado esto a la falta de personal especializado, utilizando la metodología cualitativa concluye que:

> Una amenaza o ataque cibernético no solo es exclusividad del área militar, también son las organizaciones, empresas blancos de agresiones a través de redes informáticas, por lo que combatirla requiere de estrategia conjunta con un marco normativo que genere sinergia y desarrollar capacidades para proteger la información

> crítica, además, se comprobó y verificó que se han dictado disposiciones para lograr que el personal se concientice de la problemática a la que está expuesta y adopte medidas pasivas en ciberseguridad, sin embargo, la vulnerabilidad parte desde el usuario, quien por no aplicar procedimientos para proteger la información permiten que los hacker informáticos ingresen y obtengan información. (Baretto, 2017, p. 67).

La tesis se relaciona con la investigación desde el punto de vista de acciones para combatir el riesgo a la ciberseguridad, que debe ser de manera integral a través de un marco normativo para desarrollar un nivel de ciberseguridad adecuado.

Dorneles (2018), en su tesis titulada: *Capacitación de las Fuerzas Armadas en ciberseguridad para la seguridad, defensa y desarrollo del Estado Plurinacional de Bolivia*, para optar el grado de Magíster en Seguridad, Defensa y Desarrollo, en la Universidad Militar "Mariscal Bernardino Bilbao Rioja", Bolivia, tuvo como objetivo:

A través de las lecciones aprendidas y tomando como modelo otros países la creación de un centro de capacitación en ciberseguridad para el personal militar de las Fuerzas Armadas de Bolivia, con la finalidad de contar con personal calificado y entrenado en seguridad y defensa del ciberespacio, proponiendo para ello el análisis de acciones y ataques cibernéticos en otros países afectaron a estos, así como las acciones que estos países desarrollaron con la finalidad de desarrollar una ciberseguridad aceptable y por último la infraestructura desarrollada que permita prevenir, proteger y cuál es la más efectiva y aplicada por más países que han obtenido buenos beneficios en su aplicación. (Domeles, 2018, p. 43).

Para ello utilizo el método cuantitativo, donde después de evaluar las variables correspondientes, concluyó que:

> Muchos países han creado estructuras para la realización de sus acciones cibernéticas a través de la capacitación del personal en escuelas de ciberseguridad, donde se desarrolle el conocimiento completo de los ataques cibernéticos, modalidades y la vulnerabilidad de los sistemas informáticos de las Fuerzas Armadas, que posteriormente sean entes supervisores de ciberseguridad institucional. (Domeles, 2018, p. 34).

Esta investigación aporta el interés que tienen otros países por lograr un ambiente de ciberseguridad adecuado, para ello, sostuvo que se debe de empezar por el personal que labora en esta área, podría bien aplicarse al Perú, siendo este el tercer país en Sudamérica con más ataques cibernéticos en el último año 2021.

2.2 Bases teóricas

Constituyen el soporte teorico de la investigacion, diversos conceptos y enfoques respecto a este concepto, sin embargo, Granada (1984) sostuvo:

> La teoria son enunciados que se van a verificar con los hallazgos, constituyen punto de partida en donde la actividad predominante es la de carácter empírico, búsqueda de datos, para ello combina el proceso inductivo con el deductivo, donde el investigador hace un análisis del papel que juega la teoría en la investigación científica entendida como proceso de generación y construcción de conocimientos. (p. 78).

A cotinuacion se plantean las teorias siguientes:

2.2.1 La teoría de ciber amenaza

La ciberseguridad es un concepto amplísimo, sin embargo, Del Rio (2011) sostuvo:

> El término Computer Network Operations (CON) que se utiliza en el ámbito militar, delimita la ciberseguridad a cinco Operaciones de Información en el espectro electromagnetico: NEC (Networking Enable Capability), Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC) y Electronic Warfare (EW) (p. 227).

Estas cinco Operaciones de Información trabajan con el concepto de amenaza cibernética, en este sentido:

> Una amenaza a la seguridad de las TIC puede ser definida como «cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio sistema. (Ministerio de la Defensa, 2014, p. 36).

El objetivo de los ataques cibernéticos es recopilar información o destruir las redes de comunicación con la finalidad de vulnerar la confidencialidad de datos que se maneja, hoy en día se ha sofisticado el uso de virus que atacan e ingresan por distintos canales de la red, esta amenaza se percibe cada vez más como un problema tanto en el contexto de Seguridad Nacional como en el internacional, al respecto:

> Las evaluaciones de cuán real es la amenaza, dónde radica el peligro, quién es el más adecuado para responder a ella y qué tipo de medidas y estrategias son apropiadas para proteger a las sociedades de la información contra los actores malintencionados más cuál debiese ser la mejor forma de salvaguardar la estabilidad a largo plazo varían ampliamente. (Del Rio, 2011, p. 44).

Es importante conocer que es la ciberdefensa y también se debe entender qué es el ciberespacio en todo su contexto, en ese sentido:

> Para abordar la Ciberseguridad y Ciberdefensa debemos señalar el concepto de ciberespacio, entendiéndose por este el espacio artificial creado por el conjunto de 28 sistemas de la información y telecomunicaciones que utilizan las TIC, es decir de redes de ordenadores, mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás, ha sido. (Del Río, 2011, p.217).

La teoría incluye conceptos de defensa que deben ser implementados para alcanzar un grado de ciberseguridad:

> A partir de lo mencionado, la defensa activa es una estrategia determinada en adquirir una capacidad de defensa del ciberespacio, combinando la protección interior de los sistemas, la vigilancia permanente de redes sensibles y la respuesta rápida en caso de ataque, contrarrestando las amenazas ciberespaciales y garantizando acceso al ciberespacio y la defensa pasiva es la estrategia para la protección de los activos relacionados con los sistemas de información a través de controles detectores, correctivos, disuasivos que contrarresten las posibles amenazas (Machin y Gazapo, 2017, p. 40).

Debido a las amenazas y los ataques que podrían ocurrir, es importante adoptar diversos mecanismos de seguridad a través del ciberespacio, ello permitirá que sucedido un ataque se bloqueen los sistemas desde donde procede el ataque, para ello adquirir capacidades y medios es importante, al respecto:

> En ese sentido, dotar al personal de capacidades que hagan frente a las nuevas tecnologías para anular cualquier posible ciberataque, además, debido al bajo costo de los equipos informáticos, lo más probable es que, en el futuro las guerras se desarrollen en el ciberespacio; el resto del dinero se podría invertir en fabricar armamento sofisticado o en desarrollar capacidades en los militares. (Machin y Gazapo, 2017, p. 34).

2.2.2 Protección de los activos digitales

Constituye un entorno donde todo el personal que labora en una organización tiene el conocimiento y producto de ello asume la responsabilidad de adoptar mecanismos necesarios para contrarrestar las amenazas que vienen del ciberespacio o a raves de la red, esta seguridad que se proporciona debe ser adoptada más aun con los clientes externos, pues

estos también por desconocimiento pueden portar hackers que vulneren la información que se protege, la información sobre procesos no puede ser compartida con otros, debe mantener su compartimentaje. Esta distribución de responsabilidades debe ser llevada por personal especialista en ciberseguridad a través de mecanismos que permitan una protección adecuada del volumen de datos que maneja la empresa, dependencia. etc.

2.2.3 Teoría del ciberespacio y la ciberseguridad en el ámbito militar

Delgado (2017) sostuvo:

> Las tecnologías usadas en el ámbito militar se han ido desarrollando de manera exponencial como un medio estratégico, los ataques cibernéticos ante cualquier sistema informático están más allá de las motivaciones intelectuales o económicas, sino que también cuentan con un ámbito político, pues pueden ser usadas para medir sus fuerzas en el ciberespacio. (p. 44)

Además, esta teoría considera que el ciberespacio y la ciberseguridad tienen un común denominador en lo que respecta a amenazas, para ello se debe invertir en medidas preventivas que permitan controlar tales amenazas, algunos países con alta tecnología invierten en materia de ciberseguridad, al respecto:

> El concepto de ciberespacio comparable a la concepción de espacio vital, es decir, el espacio en el que se puede desarrollar un país y que está más allá de los límites físicos que se puedan establecer. En el ciberespacio puede haber ataques informáticos de los terroristas, pero también pueden ser de otros grupos u organizaciones criminales de diferentes ideologías. Pereda (Pereda, 2019, p. 34).

En el ámbito militar, el uso del ciberespacio constituye un dominio global y dinámico donde es importante mantener el control, al respecto:

> En el ámbito militar, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes, realizados en el ciberespacio. (Pereda, 2019, p. 23).

2.2.4 Ley de Protección de Datos Personales

Garantiza la protección de datos a través de un marco normativo de respeto hacia la información personal, al respecto:

> Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que

no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización. (Ley 29733, 2013, p.3).

2.2.5 Ley de Delitos Informáticos Nº 30096:

Guerrero y Proaño (2020) afirmaron:

Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información y la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, cubre de cierta forma el vacío normativo que existía sobre algunos de los ataques más comunes: la vulneración de sistemas informáticos, entre otros. (Guerrero y Proaño, 2020, p. 33).

2.2.6 Ley de Ciberdefensa:

La ley 30999 (2019), Ley de Ciberdefensa estableció que:

La normativa en el ámbito de la protección de los sistemas cibernéticos del Estado peruano comprende la regulación de las operaciones militares adelantadas por las dependencias adscritas al Ministerio de Defensa. Define la ciberdefensa como una capacidad militar de contención y respuesta frente a amenazas en el ciberespacio, delegando en las Fuerzas Armadas las tareas de ejecución de la ciberdefensa. (p. 46).

2.2.7 Comando Logístico del Ejército

El Comando Logístico del Ejército (Cologe) cuenta con un Estado Mayor, el cual desarrolla las actividades administrativas en apoyo a sus funciones propias como comando logístico, órgano director de la logística en el Ejército, de la misma manera, cuenta con una División de Operaciones Logísticas, encargada del asesoramiento en la ejecución de todas las funciones logísticas en coordinación con los Servicios Logísticos del Cologe. Así mismo cuenta con una inspectoría que realiza el control de todas las actividades logísticas realizadas en esta dependencia importante del Ejército. (Ditele, 2019, p. 56).

2.3 Categorías y subcategorías apriorísticas

Tabla 1

Matriz de Categorías y subcategorías apriorísticas

Categorías	Subcategorías
Situación actual de ciberseguridad	Conocimiento de ciberseguridad
	Seguridad de los dispositivos
	Empleo de sistemas de protección
Riesgo que genera el uso no adecuado de la información	Manejo de otros medios para envió de información
	Tipo de información que se maneja
	Vulneración del marco normativo vigente
Factores que inciden en el nivel de ciberseguridad	Personal
	Dispositivos informáticos
	Protección contra ataques electrónicos
	Planes de recuperación de información

Situación actual de ciberseguridad

Conocimiento de ciberseguridad

La ciberseguridad abarca un conjunto de acciones y estrategias diseñadas para salvaguardar de manera efectiva los sistemas, redes, programas, datos y dispositivos de accesos no autorizados. Su objetivo es prevenir posibles ciberataques deliberados y otras amenazas maliciosas en entornos digitales dentro de una entidad. (Safety Culture, 2023, párr. 1)

Seguridad de los dispositivos

Los sistemas estructurales de red están conformados por diversos componentes que posibilitan la transmisión de información entre distintos sistemas. Estos componentes se dividen en dispositivos pasivos y activos. Los dispositivos pasivos no requieren el empleo de energía externa para funcionar; sin embargo, pueden almacenar energía en forma de voltaje o corriente. Estos pueden incluir elementos como resistencias eléctricas, condensadores eléctricos, fibra óptica, cables, filtros, entre otros.

Por otro lado, los dispositivos activos son hardware que operan directamente con señales en una red informática, ya sea para amplificar, modificar, evaluar, entre otras funciones. Estos dispositivos inyectan energía al circuito y pueden ser ejemplos tales como Access Points, routers, hubs, bridges, gateways, switches, módems, o brouters. (Conzultek, 2023, párrs 1-3)

Empleo de sistemas de protección

Con el aumento en el uso de las tecnologías de la comunicación para una amplia gama de propósitos, el incremento de los ciberataques se ha vuelto evidente, a menudo debido a la falta de protección por parte de las entidades frente a estas amenazas. Para abordar este fenómeno, existen tres modalidades principales de ciberseguridad: la seguridad de red, la seguridad en la nube y la seguridad física. Estas se perfilan como enfoques clave para contrarrestar esta creciente amenaza. (Docusign, 2022)

Riesgo que genera el uso no adecuado de la información

Manejo de otros medios para envió de información

La seguridad informática engloba un conjunto de tecnologías, procesos y prácticas elaboradas para salvaguardar redes, dispositivos, programas y datos en caso de ciberataques, hackeos, daños o accesos no autorizados. Este campo dispone de una serie de mecanismos de protección, incluyendo la seguridad de datos, seguridad de aplicaciones y seguridad de la identidad. Estos elementos se diseñan para prevenir y mitigar los riesgos

inherentes a la era digital, protegiendo la integridad y confidencialidad de la información. (Coppola, 2023).

Tipo de información que se maneja

La información puede clasificarse de maneras muy distintas, conforme a numerosos criterios. Uno de los más comunes tiene que ver con la relación establecida entre los emisores de la información y sus eventuales o posibles receptores, de la siguiente manera:

Información confidencial o clasificada. Aquella a la que sólo puede acceder un pequeño conjunto de personas, dada la naturaleza secreta, peligrosa, delicada o privada de los datos contenidos en ella.

Información externa. Aquella que emana de un organismo, institución o empresa, y cuyos destinatarios son instancias o personas externas a la misma.

Información interna. Aquella, por el contrario, que emana de un organismo, institución o empresa, con el fin de ser consumida de manera interna, sin salir de la organización. (Etecé, 2020)

Vulneración del marco normativo vigente

El progreso de los ciberataques, la ciberdelincuencia, el ciberterrorismo y otras amenazas tanto para la seguridad pública como privada se ha convertido en un problema sumamente complejo. Estas amenazas han vulnerado el marco normativo vigente a través de prácticas como el fraude informático, la estafa agravada, y la suplantación, dirigidas específicamente hacia entornos digitales, incluyendo redes sociales y diversos dispositivos. Estas acciones han ocasionado daños irreparables en los sistemas de información, en las entidades y en la sociedad en su conjunto.

Factores que influyen en la ciberseguridad

Personal

El factor humano es fundamental en la ciberseguridad, ya que la preparación y conocimiento del personal son determinantes para la protección de la información contra una variedad de ciberataques. Este personal puede ser interno, directamente involucrado con la información de la entidad, o externo, con una relación menos directa con las funciones de la entidad. Sin embargo, el mal uso de los datos por parte de cualquier individuo, interno o externo puede resultar en un ciberataque.

Dispositivos informáticos

En el ámbito de la información, se utilizan diversos dispositivos que van desde ordenadores o computadoras, pasando por dispositivos móviles (teléfonos), hasta llegar a las memorias externas. Estos mecanismos digitales, si no se manejan adecuadamente en términos de seguridad frente a los ciberataques, pueden representar amenazas serias para la entidad.

Protección contra ciberataques

Para protegerse contra ciberataques, se emplean diversos métodos de seguridad informática, tales como la inteligencia artificial, software antivirus, firewalls o cortafuegos, planes de seguridad informática, infraestructura de clave pública y pruebas de penetración, pentesting. (Docusign, 2022)

Planes de recuperación de información

Un plan de recuperación de datos engloba todas las medidas de protección de la privacidad digital que se aplican con el objetivo de recuperar la información, evitar el acceso no autorizado a los datos o su pérdida. Estos sucesos pueden tener lugar en ordenadores, bases de datos o sitios web. (Bernabe, 2021)

2.4 Definición de términos

Ciberdefensa:

Conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas, para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otros actores en oposición,

Rivera (2018) sostuvo:

> Otra definición de ciberdefensa que es interesante es la que describo en el siguiente párrafo; como el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y tele informáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos. (p.34).

Ciberterrorismo:

Delgado (2017) sostuvo:

> Acción terrorista en el ciberespacio o la definición que expresa que el ciberterrorismo o terrorismo electrónico es el uso de medios y tecnologías de información,

> comunicación, informática o similares con el propósito de generar terror o miedo generalizado en una población o gobierno, causando con ello una violación a la libre voluntad de las personas. (p.21).

Cibercrimen:

Flores (2017) sostuvo:

> Acción criminal en el ciberespacio, o también conocido como delitos cibernéticos, en otras palabras, los delitos cometidos por medio de ordenadores a través de internet, consisten en el uso ilícito de equipos para promover o realizar prácticas ilegales como la pornografía infantil, el robo de información personal o violación de las leyes de asociación, difamaciones, etcétera. (p. 6).

Ciber inteligencia:

Constituyen actividades que tienen por finalidad vigilar los diferentes procesos que se desarrolla en la ciberseguridad, Gómez (2021) sostuvo:

> La ciber inteligencia, es una prestación de vigilancia en el ámbito digital, un servicio que ayuda, y permite comprender conceptos. Es decir, es el proceso de recopilar conocimientos y evidencias respecto amenazas que pueden afectar a la información de una empresa, además, de tener información proporciona inteligencia, por lo tanto, conseguirla es la clave para conocer un terreno y, en efecto, tener poder sobre él, lo que permite anticiparse a los hechos, tomar mejores decisiones y en relación a ello, actuar. (p.33).

Ciberseguridad:

Gómez (2021) definió la ciberseguridad como la actividad que permite la protección de los datos que se manejan en una organización, además, sostuvo:

> Se define la Ciberseguridad como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados, además, define el Activo de la Información como los conocimientos o datos que tienen valor para una organización, mientras que, en la misma norma, los Sistemas de Información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.(p.45).

Por tanto, es fácil deducir que la ciberseguridad, tiene como foco la protección de la información digital que *vive* en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

La ciberseguridad ofrece un foco de protección para la información digital que se encuentra entre *sistemas* interconectados. Como consecuencia, se encuentra en la seguridad de la información.

Figura 1

El Ransomware

Nota. Como actúa el Ransomware y se propaga

Seguridad de la Información:

Pereda (2019) sostuvo:

> Para poder establecer la diferencia con la seguridad de la información, debemos revisar varios conceptos más que nos permiten tener el contexto general. Según la Real Academia Española (RAE), la seguridad se puede definir como: *Libre o exento de todo peligro, daño o riesgos*. Sin embargo, es una condición ideal, ya que en la realidad no es posible tener la certeza de que se puedan evitar todos los peligros. (p. 44)

La finalidad de la seguridad es proporcionar una seguridad en los diferentes aspectos que comprende la confidencialidad que debe tener el personal con los equipos informáticos

para proteger este activo y evitar que la información caiga en manos de hackers que pueden actuar de manera anónima aprovechando la vulnerabilidad que parte del personal.

Del Rio (2011) afirmó:

> La información se puede encontrar en diferentes formatos, por ejemplo, en formato digital (utilizando los diferentes medios electrónicos que existen hoy en día), de forma física (bien sea escrita o impresa), además de manera no representada, esto pueden ser ideas o conocimiento de personas que pertenecen a la organización. Los activos de información se pueden encontrar en diferentes formatos. (p. 29).

En un Sistema que permita un control adecuado de la seguridad en una organización se pueden encontrar diversas maneras de seguridad tales como:

- ✓ Formato electrónico que se traduce en antivirus.
- ✓ De manera verbal a través de disposiciones
- ✓ Enviando mensajes escritos
- ✓ Impresiones

Huaman (2020) sostuvo:

> Esto quiere decir que será posible encontrarlos en diferentes formatos, No importa la forma o el estado, la información requiere que se cumpla una serie de medidas de protección que sean adecuadas según la importancia y la criticidad de la información, esto es especialmente importante en el ámbito de la seguridad de la información. (p. 56)

En ese sentido estableció pautas que orientan a la seguridad en los diversos campos que se desarrollan:

> Debemos recordar que la seguridad en cómputo se limita a la protección de los sistemas y equipos que permiten procesar toda la información, mientras que la seguridad informática se involucra en todos los métodos, procesos o técnicas para tratar de forma automática la información que se encuentra en formato digital, teniendo un mayor alcance, ya que se incluye la protección de las redes e infraestructuras tecnológicas. (Machin y Gazapo, 2017, p. 56)

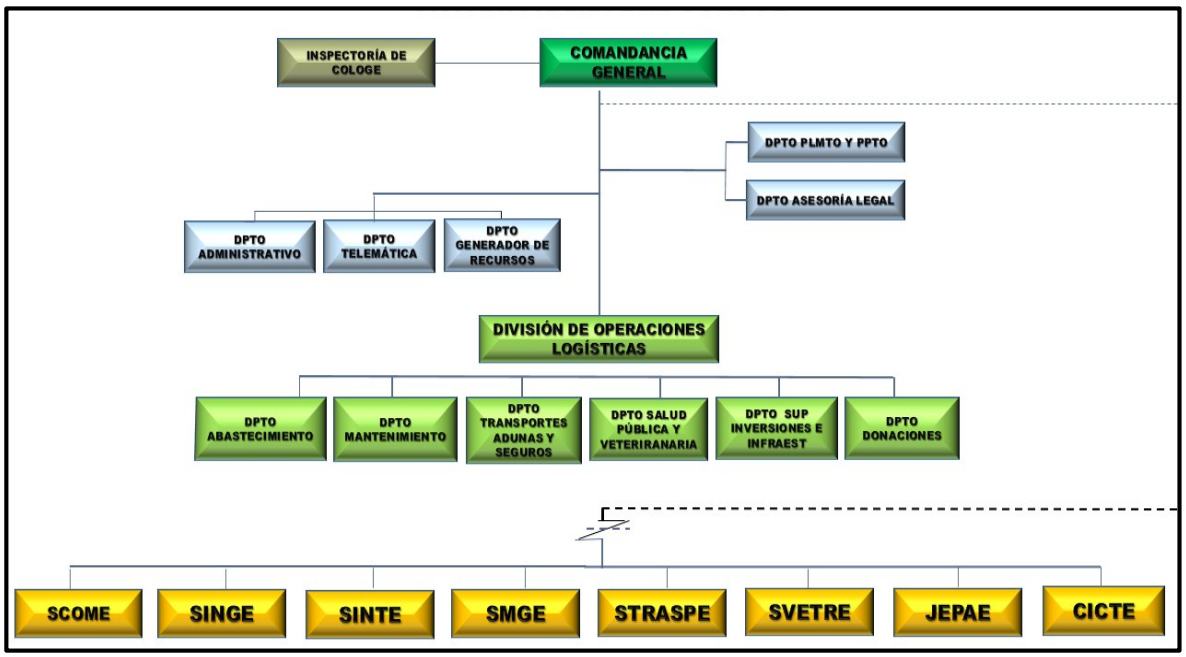
Comando Logístico del Ejército (Cologe)

Es el órgano responsable de realizar procesos y actividades de carácter técnico y normativo del sistema logístico y del control patrimonial de la institución, tiene como funciones:

Planificar, coordinar, dirigir, controlar y supervisar la ejecución del apoyo logístico del Ejército, realizar los procesos y actividades de las funciones logísticas de abastecimiento, mantenimiento, transporte, construcciones, evacuación y hospitalización de veterinaria y diversos, planificar, coordinar y ejecutar las actividades relacionadas a los seguros de los bienes del Ejército. (Rojas, 2018, p.34).

Figura 2

Organización del Cologe



Seguridad informática:

El concepto de la seguridad comienza desde nuestra PC, la seguridad a nivel local es lo primero que debemos cuidar. Es conveniente cambiar las contraseñas cada 15 días, o por lo menos una vez al mes, existen sistemas de fuerza bruta, *John the zipper* que consiste en un ataque a las contraseñas por medio de un programa que prueba palabras que están en un diccionario hasta que las descubre (normalmente un archivo de texto). Es decir, exploran combinaciones con el fin de hallar la contraseña. Pero en estos diccionarios no están todas las posibles claves, por lo tanto, lo adecuado es poner cosas que no estén en los diccionarios, por ejemplo, una contraseña que no signifique nada, sin sentido, con caracteres, así como ^y ~, y lo suficientemente larga.

Tabla 2

Niveles de amenazas cibernéticas

Nota: se describe el perfil del atacante y los posibles daños que causaría.

NIVEL	Descripción	Perfil del atacante	Daños potenciales
I	Profesionales que hacen uso de exploits conocidos	Profesionales con una cualificación de nivel medio	Interrupción temporal de servicios TIC
II	Profesionales con gran experiencia y capacidad para desarrollar sus propias herramientas a partir de vulnerabilidades conocidas	Profesionales con una cualificación de nivel alto	Interrupción temporal de servicios TIC
III	Profesionales que se centran en el descubrimiento y el uso de códigos maliciosos desconocidos	Profesionales con una cualificación de nivel alto	Interrupción prolongada de servicios TIC
IV	Actores estatales o grupo criminales bien organizados y financiados con el objetivo de descubrir nuevas vulnerabilidades y desarrollar exploits	Actores estatales y grupos criminales	Sustracción de información clasificada y ataques a infraestructuras criticas
V	Actores estatales con la capacidad de crear vulnerabilidades a partir de la infiltración en la cadena de producción de productos y servicios comerciales con el objetivo de explotar redes y sistemas de interés	Actores estatales	Sustracción de información clasificada y ataques a infraestructuras criticas
VI	Actores estatales con la capacidad de ejecutar ataques de espectro completo, mediante el uso de capacidades cibernéticas y cinéticas, con el objeto de lograr un resultado especifico en los ámbitos político, militar, económico y/o social a gran escala	Actores estatales	Ataques a infraestructuras críticas y cambios geopolíticos

Hay tres tipos de contraseñas que conviene no olvidar de poner en un PC si queremos que tenga una mínima seguridad. La primera, la de la Bios. Esta es para que en el arranque no se pueda acceder a arrancar el SO (Sistema Operativo). Es muy conveniente hacerlo ya que hay muchas intrusiones a nivel *local* es el primer sitio que debemos cuidar. Si quitamos la pila de la Bios eliminaríamos la contraseña, esto implica un mayor trabajo en caso de un ataque.

Después es importante poner también una contraseña de acceso al sistema (nos centramos en Windows). Dicha contraseña debe constar de, al menos, 8 caracteres para que sea algo segura. Procuraremos mezclar números, letras y también símbolos tipo la @ (pensad que, en un ataque por fuerza bruta, una contraseña de menos de 15 caracteres es *rompible*, pero tardaría tiempo).

A continuación, hay otra contraseña para tener en cuenta, el del salvapantallas de Windows. No lo descuidéis, en el trabajo hay verdaderos problemas con este tema, un descuido y podemos sufrir ataques rápidos fortuitos desde casa o el trabajo. Lo del

salvapantallas no es una tontería, te vas al baño y el PC abierto, entonces te pueden colar un troyano, ver tus archivos, etc. Lo mejor es activar el salvapantallas con la opción de introducir contraseña para volver a tener acceso al PC.

La seguridad informática de aquello que está abierto

> Uno de los problemas que está afectando a la seguridad de la información en nuestros PC es la falta de cuidado que los usuarios tenemos, con más frecuencia de la debida, respecto a dónde ponemos los datos y las informaciones que más nos interesan y cómo disponemos de las mismas en el momento de borrarlas o eliminarlas de un fichero o archivo. (Gomez, 2021, p. 34).

Curiosamente, todos somos conscientes de cómo funciona el sistema operativo de los PC cuando se borra un fichero, pero la inconsciencia surge cuando esto se nos olvida, existen dos aspectos que afectan al quehacer diario de todos nosotros.

Los datos y las informaciones normalmente los tenemos almacenados en el disco duro del PC que usamos a diario, y al cual, en principio, no tenemos acceso más que nosotros, tanto si se trata de un PC puramente personal, como si se trata de un PC corporativo de la organización para la que trabajamos. Claro que la situación es diferente si el PC es personal y lo tenemos en casa, o si es de la organización y lo tenemos en su sede conectado a una red. Veamos cuáles son las diferencias y las similitudes. Atención, parto de la base de que se dispone de un PC tipo fijo o portátil, (es lo mismo) con los últimos avances como Wifi, puerto infrarrojo, puerto bluetooth, puertos USB y conexión a Internet vía red interna o vía módem, en ese sentido, el primer problema es el de analizar si los datos y las informaciones que tenemos en nuestro disco duro son importantes y por tanto deberíamos cifrarlas para impedir a cualquier intruso tener acceso a su contenido. Hoy en día hay sistemas de cifrado de variada complejidad, pero incluso el sistema de cifrado Pretty Good Privacy es lo suficientemente robusto para tener una protección adecuada en la mayoría de los casos.

Espectro de amenazas de la seguridad de la información

Respecto a los ataques que atentan contra la seguridad de la información, se pueden distinguir dos ámbitos: En primer lugar, los perpetrados contra las redes de comunicación del sector económico. Precisamente, este sector está empleando cada vez más las redes de acceso público para interconectar sus sistemas informáticos.

Aparte de las posibilidades de integración que aporta la actual tecnología (Intranet), las empresas tienden hoy a conectarse entre ellas. Todo eso constituye un valor económico capital, tanto más urgente será garantizar su seguridad y fomentar la confianza en este tipo

de procesos entre empresas, los ataques informáticos pueden facilitar el acceso a información reservada o, más grave aún, posibilitar la falsificación de datos (espionaje industrial, violaciones del copyright, piratería; véase el espectacular robo de datos personales y de grandes empresas en el Foro Económico Mundial en Davos el año 2021, amenazan algunos de los principios básicos de la competencia. En segundo lugar, la política de defensa de la información respecto a los ataques perpetrados contra infraestructuras clave dentro de cualquier sociedad.

2.5 Hipótesis

Hernández et al. (2010) sostuvieron:

Los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos.

> Con frecuencia, estas actividades sirven, primero, para descubrir cuáles son las preguntas de investigación más importantes, y después, para refinarlas y responderlas, la acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien “circular” y no siempre la secuencia es la misma. (p. 44).

Es en este sentido, que es lo que guía la investigación y conlleva al alineamiento metodológico y epistemológico en la investigación, lo que permite plantear la siguiente hipótesis:

La situación actual de Ciberseguridad es deficiente en el Comando Logístico del Ejército.

Capítulo III: Método

3.1 Enfoque de la investigación

La investigación se desarrolló bajo el enfoque cualitativo, las técnicas e instrumentos se basaron en la situación actual de ciberseguridad en el Comando Logístico del Ejército, en este sentido se observó la realidad con respecto a la ciberseguridad que se adopta en el Comando Logístico del Ejército, las deficiencias y los aspectos que inciden en el desarrollo de esta y su aplicación por cada uno de los integrantes de esta dependen. Porto y Ruiz (2014) sostuvieron:

> Al respecto la metodología cualitativa podría identificarse como *una especie de cajón de sastre* que engloba todos aquellos aspectos que no se ajustan a lo puramente cuantitativo, de tal modo que lo cualitativo se podría considerar como *un espacio en negativo*, al que se le otorga una función principal: la búsqueda del significado de los fenómenos, la obtención de la palabra de los sujetos de la acción social, el lugar primordial del lenguaje. (p. 254)

El planteamiento del enfoque cualitativo es más abierto y flexible, vivencial en cuanto a lo que actualmente se suscita con respecto a la ciberseguridad en el Comando Logístico del Ejército. En tal sentido, Mendizábal (2014) refiere:

> El concepto de flexibilidad alude a la posibilidad de advertir durante el proceso de investigación situaciones nuevas e inesperadas vinculadas con el tema de estudio que puedan implicar cambios en las preguntas de investigación y en los propósitos (…) por lo tanto la idea de flexibilidad abarca tanto al diseño en la propuesta escrita como al diseño del proceso de investigación. (p. 67).

3.2 Tipo de investigación

El tipo de investigación llevado a cabo es de tipo aplicada por cuanto va a resolver un problema concreto, tomando como unidad de análisis de la investigación el personal que labora en el Comando Logístico del Ejército (Cologe). Valerino et al. (2015) señalaron: “La investigación aplicada aparte de su propósito de generar conocimiento, también busca solución práctica al fenómeno en estudio que es parte de la realidad” (p. 68).

3.3 Método de investigación

El método de la investigación fue Hermenéutico interpretativo, que corresponde al mismo paradigma, según Vargas (2011). La aplicación de este método se sustenta en cuanto al haber laborado en el Comando Logístico del Ejército.

Al respecto, Castro (2001) señaló:

> La hermenéutica consiste en la interpretación de lo expresado por la conducta humana, a partir de lo expresado con respecto al entendimiento de un fenómeno, por lo tanto, busca comprender y descubrir la lógica de los significados que se configuran por lo expresado por los participantes. (p. 169)

3.4 Objeto de estudio

El objeto de estudio de la investigación fue la ciberseguridad en el Comando Logístico del Ejército. Al respecto Sáenz y Rodríguez (2014) afirmaron que:

> El investigador debe tener conocimiento profundo de la disciplina concerniente a su objeto de estudio, comprendiendo las teorías relevantes que le permitan la elaboración de mapas mentales en donde pueda mostrar las relaciones teóricas de las principales corrientes de pensamiento, esto habilita el manejo correcto de los teóricos, investigadores y teorías relevantes para el análisis teórico y sustentación de la investigación. (p. 89)

Por su parte, Sáenz y Rodríguez (2014) refieren que:

> Para ello es importante la delimitación correcta del objeto de estudio antes de empezar con el proceso indagativo, para así revisar la literatura apropiada y adecuada sobre el tema, esto permitirá un acercamiento en toda la investigación a este, el mismo que será en todo momento el centro de la observación que nos orientará y guiará el trabajo. (p. 35).

3.5 Muestra de estudio

En la investigación cualitativa el diseño de la investigación tiende a evolucionar en el desarrollo del mismo, por eso se dice que es emergente, lo mismo ocurre en la muestra, conforme se desarrolla la investigación se va decidiendo de quien obtener los datos, pues lo que se pretende es reflejar la realidad y los puntos de vista de los participantes. Hernández y Mendoza (2018) sostuvieron: “En estudios cualitativos el tamaño de muestra no es importante desde una perspectiva probabilística, pues el interés del investigador no es generalizar los resultados de su estudio a una población más amplia, sino profundizar en el entendimiento de un fenómeno” (p. 424).

En ese sentido, la muestra correspondió a cinco militares que laboraron más de un año de servicio en el puesto en las dependencias del Comando Logístico del Ejército el 2022, de acuerdo al siguiente detalle:

- Oficial del Estado Mayor del Cologe
- Jefe de la Jefatura de Patrimonio del Ejército

- Oficial del Servicio de Comunicaciones
- Oficial del Servicio de Ingeniería
- Oficial del Servicio de Material de Guerra

Para ello se tomaron en cuenta los siguientes criterios de selección:

- Entendimiento del fenómeno por parte del personal de entrevistados
- Naturaleza del fenómeno bajo análisis, la realidad que se vive día a día y la situación de la ciberseguridad
- Saturación de la información a la hora de realizar las entrevistas

3.6 Técnicas e Instrumentos de recolección de datos

Las técnicas utilizadas fueron la entrevista semi estructurada, el análisis documental y la observación. Con respecto a la entrevista semi estructurada Gayou (2009) afirmó:

> En la investigación cualitativa se realizan entrevistas semiestructuradas que tienen una secuencia de temas y algunas preguntas sugeridas, estas presentan una apertura en cuanto al cambio de tal secuencia y forma de las preguntas, de acuerdo con la situación de los entrevistados. (p. 111)

Con respecto a la segunda técnica, es decir, el analisis documental se estableció una exhaustiva revisión documental que permitió extraer la información relevante en torno a nuestro objeto de estudio y responder la pregunta de investigación.

Los instrumentos aplicados fueron la guía de la entrevista, la indagación documental y la ficha de observación, estos permitieron hacer emerger todos los posibles flecos, ramificaciones y bifurcaciones del objeto de estudio examinado. Es decir, permitieron recabar información pertinente que nos permitió responder a nuestra pregunta de investigación.

3.7 Rigor científico

Constituye la forma como la investigación alcanza un grado de calidad y aceptación en el marco científico, desde el planteamiento del problema hasta los resultados obtenidos por la aplicación de los instrumentos, en la investigación el rigor científico estará dado, por lo manifestado por Izcara (2014), “los elementos básicos definitorios del rigor metodológico de la investigación cualitativa son dos: La rigurosidad del diseño metodológico y el rigor en la aplicación de las técnicas cualitativas de acopio de información” (p. 129).

Con respecto a la rigurosidad del diseño metodológico, este estuvo dado por tres elementos: el diseño metodológico que guardó correspondencia con los objetivos perseguidos, el proceso de selección de la muestra estuvo suficientemente justificado y ofreció una saturación durante la recopilación de los datos.

Además, acerca del rigor en la aplicación de las técnicas cualitativas, la rigurosidad hizo referencia a los siguientes elementos: la justificación de la técnica o combinación de técnicas cualitativas seleccionadas, la eliminación de todo tipo de relaciones no comunicables que provoquen una represión del discurso enunciado por los actores sociales investigados, la indagación adecuada de las áreas temáticas convergentes con los objetivos de la investigación, la destreza para mantener la motivación del entrevistado durante la interacción conversacional y la grabación y trascripción de todas las situaciones discursivas, para su posterior análisis.

3.8 Técnica de procesamiento y análisis de datos

El método de análisis de la información de la investigación se realizó de manera manual, no se utilizó ningún programa informático, de acuerdo con los modelos de Xavier Vargas Beal (2011) y Hernández-Sampieri y Mendoza (2018).

Izcara (2014) sostuvo: “El análisis de datos cualitativos es un proceso artesanal, singular y creativo que en gran parte depende de las habilidades y destrezas del investigador que se agilizan y perfeccionan con la experiencia” (p. 53).

Capítulo IV: Análisis

4.1 Recolección de los datos

Después de haber seleccionado la muestra correspondiente para el levantamiento de la información de campo correspondiente que permitió entender el problema de investigación y el fenómeno planteado respecto a la importancia de la ciberseguridad y a la prioridad institucional que se debe tener respecto a la ciberseguridad en el Comando Logístico del Ejército, se procedió a realizar la recolección de los datos cualitativos. Hernández y Mendoza (2018) afirmaron que:

> La recolección de datos resulta fundamental, solamente que su propósito no es medir variables para llevar a cabo inferencias y análisis estadístico, lo que se busca en un estudio cualitativo es obtener datos de personas, otros seres vivos, comunidades, situaciones o procesos en profundidad; en las propias "formas de expresión" de cada unidad de muestreo (p. 443).

Para ello durante la recolección de datos se utilizaron fuentes humanas, documentarias y la observación por parte del propio investigador que constituyó el principal instrumento de recolección de datos, basado en la experiencia de haber llevado un curso de ciberseguridad en el año 2021, así como, dar a conocer la importancia que se debe tener actualmente en el Comando Logístico del Ejército (Cologe) por la información sensible que se maneja, para ello se consideraron cinco (05) militares que laboraron en esta dependencia, los mismos que respondieron a las preguntas planteadas sobre la base de las categorías apriorísticas para finalmente establecer las categorías emergentes que permitieron el entendimiento del fenómeno de una manera holística e integral.

Tabla 3

Relación de personal entrevistado

Nº	Grado	Seu	Edad	Instrumento	Fecha	Lugar	Genero
1	Tte Crl	Lob	45	Entrevista	15/03/2023	Lima	Masculino
2	Tte Crl	Run	44	Entrevista	14/03/2023	Lima	Masculino
3	Mayor	Mac	45	Entrevista	22/03/2023	Lima	Masculino
4	Técnico	Sap	46	Entrevista	17/03/2023	Lima	Masculino
5	Técnico	Oma	43	Entrevista	10/03/2023	Lima	Masculino

Con respecto a las fuentes documentarias que permitieron complementar esta etapa de análisis, se utilizaron datos de fuentes abiertas y documentos institucionales del Cologe, Dirección de Telemática y Estadística del Ejército (Ditele), etc.

Tabla 4

Relación de documentos analizados

N°	Documento
1	Ley N° 303999 “Ley de ciberdefensa” (2019)
2	DL 1412 que aprueba la Ley del Gobierno Digital (2018)
3	Decreto Supremo N° 029 -2021 Reglamento de la Ley de Gobierno Digital (2021)
4	Decreto de Urgencia N° 006-2020 Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital (2020)
5	Texto Especial sobre el Funcionamiento del Sistema de Telemática del Ejercito (2019)
6	El Gran libro de la Seguridad Digital (2017)
7	La Guerra Cibernética (2018)
8	DL 1412 que aprueba la Ley del Gobierno Digital (2018)
9	Decreto Supremo N° 029 -2021 Reglamento de la Ley de Gobierno Digital (2021)
10	Decreto de Urgencia N° 006-2020 Decreto que crea el Sistema Nacional de Transformación Digital (2021)
11	Texto Especial sobre el Funcionamiento del Sistema de Telemática del Ejercito (2019)

4.2 Organización de los datos

La información disponible fue revisada, seleccionada, clasificada y organizada de una manera dinámica y sistemática con el único propósito de poder obtener información clave, en relación con la realidad de la problemática, con el fin de dar respuestas a las preguntas de investigación planteadas. Hernández y Mendoza (2018), sostuvo “se debe diseñar e implementar una base de datos sistema en el cual se organizan los datos cualitativos recolectados, utilizando uno o más criterios pertinentes” (p. 469).

Posterior al llenado de la guía de entrevista y la ficha documental, se procedió a la transcripción de la información a una base de datos en una computadora, para organizar la información y la data obtenida por familia de documentos, memorandos, párrafos e ideas

fuerza y, se clasificó por tipo de datos: (entrevistas, observaciones, documentos, fotografías). El fin fue tener, en todo momento, información disponible para poder relacionarla (según convino) en beneficio de la investigación, teniendo siempre presente el principio de confidencialidad.

4.3 Definición de categorías

Para la definición de categorías se siguió con el procedimiento como lo describe Hernández y Mendoza (2018), inicialmente se definieron las unidades de análisis que posteriormente se codificaron según las categorías.

Hernández y Mendoza (2018) sostuvo:

> En los estudios cualitativos se codifican los datos para tener una descripción más completa de estos, pero ¿qué se codifica? Las unidades de análisis. Entonces, lo primero es definir, identificar o determinar cuál va a ser la unidad de análisis. (pág. 471).

Asimismo, se definieron lo que correspondió a unidades de análisis de los instrumentos de recolección de datos según el criterio siguiente:

Tabla 5
Definición de las unidades de análisis

Instrumentos	Unidad de análisis: Citas
Guía de Entrevista	Palabras o conceptos incluyendo adjetivos Líneas y oraciones Frases y párrafos
Ficha documental	Líneas y oraciones Frases y párrafos Páginas
Guía de cuestionario	Párrafos de descripción

En ese sentido se realizó la codificación abierta, posteriormente una comparación constante de las unidades de análisis que permitió generar las siguientes categorías:

Tabla 6
Codificación abierta de las entrevistas

Participante	Unidades de análisis	Código	Categoría
1	- La ciberseguridad es la seguridad hacia los equipos informáticos.	A1	- Poco conocimiento de ciberseguridad
	- Que debemos tener a la hora que trabajamos con ellos, por ejemplo, una computadora, un celular.	A2	- Seguridad en todo momento
	- Si es importante porque te van a robar tus datos, claves de tarjetas de crédito.	A3	- Hurto de información personal
	- Además, debemos saber que actualmente se está viendo los hackers que han surgido del Ejército del Perú.	A4	- Han crecido los hackers
	- Donde publican información que tiene que ver con la seguridad nacional, en el Cologe la información que se maneja es sensible.	A5	- Manejo de información sensible
	- Toda la parte logística institucional que de ser obtenida puede ser perjudicial como institución, hay aspectos que solo militares debemos tener.	A6	- Información de importancia institucional
	- Ciberataque es atacar a las computadoras, a través de virus.	A7	- Poco conocimiento de ciberataque
	- Sí exactamente, sí sé que existe personal que se dedica exclusivamente a obtener claves de correos, tarjetas con la finalidad de obtener beneficio económico.	A8	- Existencia de hackers
	- La clave personal, que dispone, bueno creo que con eso nadie puede ingresar.	A9	- Confianza en la clave de seguridad
	- Aparte la seguridad de mi oficina, la llave la tengo yo nada más.	A10	- Creer que es suficiente la seguridad
	- En el teléfono, bueno mi última clave la tengo desde hace 1 año.	A11	- Cambio de contraseña no se hace periódicamente
	- De mi computadora, me releve con esa clave, no soy de los que están cambiando de clave cada rato.	A12	- Falta de conciencia de seguridad
	- Es más, mi celular antes no tenía clave, el tema es por mis menores hijos para que no	A13	- Falta de normas de seguridad

Partic ipante	Unidades de análisis	Código	Categoría
	accedan se le puso clave.		
	- En el Cologe que sepa nadie nos dice que se debe cambiar la clave de la computadora del Ejército.	A14	- No existe normas de seguridad contra ciberataques
	- Lo hace por medida de seguridad personal que se toma, pero no creo que alguien cambie de clave permanentemente.	A15	- Poca conciencia de seguridad
	- Claro, ya nos hackearon, no sé cómo obtuvieron esa información.	A16	- Vulnerables a los hackers
	- Alguien se las dio o tal vez a un alumno de la escuela de guerra le robaron los datos de su laptop como siempre ocurre cuando se la mandan a arreglar.	A17	- Falta de protección a información personal
	- Haber, normalmente casi toda la información se comparte por WhatsApp, porque es más rápido y creo que por lo menos es seguro.	A18	- Uso de medios no adecuados
	- Bueno, como virus sí, pero el conocimiento que tengo es que ponen lento las computadoras, hay que resetearlos e instalar antivirus.	A19	- Desconocimiento de cómo actúan los antivirus
	- Muy pocas veces, más aún que lo han deshabilitado y restringe el acceso de la computadora personal.	A20	- Desconocimiento del daño de los antivirus
	- Charla en el Cologe, no nos han dicho nada respecto a ciberseguridad.	A21	- Falta de instrucción sobre ciberseguridad
	- Sí habláramos de importancia, por supuesto el comando de la institución debe promover esta cultura de ciberseguridad.	A22	- Poca importancia a la ciberseguridad
	- No, que será eso, se guarda en USB en caso de que la computadora se malogre.	A23	- Falta de normas de recuperación de información
	- Bueno, La ciberseguridad es la manera o la forma como se protege los datos.	B1	- La ciberseguridad
	- Para que no puedan ser obtenidos por otras personas ajenas al trabajo y que no tienen	B2	- Seguridad de la información

Participante	Unidades de análisis	Código	Categoría
	relación con la información que manejan.		
	- Respecto a la información y la importancia en el Cologe, bueno aquí se maneja información a cargo de todos los servicios logísticos a nivel institucional.	B3	- Información de importancia institucional
	- Un ciberataque, es atacar a las computadoras, celulares o cualquier otro medio electrónico.	B4	- Poco conocimiento de ciberataque
	- Que contenga datos para ser usados maliciosamente, sé que hay gente que se dedica exclusivamente a ese propósito.	B5	- Hackers informáticos
	- Pero desconozco como lo hacen, se aprecia mucho por los medios de información que extraen información de diferentes instituciones.	B6	- Desconocimiento de procedimiento de hackers
	- Suficiente, creo que con la clave ya hay una seguridad, lo único que no está actualizado es el antivirus.	B7	- Falta de seguridad
	- Allí, sí que te digo, la computadora que se trabaja en la oficina tiene clave, me releve con esa y solamente una vez la cambie, hace 2 años.	B8	- Falta de contraseñas dinámicas
	- En el teléfono, bueno no acostumbro a colocar clave.	B9	- Seguridad personal con dispositivos
	- Bueno, no creo, es más a veces se acostumbra a dejar la clave en el escritorio anotado.	B10	- Falta de seguridad
	- Porque a veces uno necesita ingresar a la maquina cuando alguien está de permiso, comisión etc.	B11	- Falta de protección de equipos
	- Quedaríamos mal como institución, para ello debería haber una buena cultura de manejo de la información.	B13	Imagen institucional
	- Evitando que caiga en manos de los hackers.	B14	- Ciberseguridad institucional

Participante	Unidades de análisis	Código	Categoría
	- Normalmente hasta cuando se manda arreglar la laptop allí sacan la información.	B15	- Falta de seguridad en disposición
	- Casi diario, información de todo tipo, excepto planes, pero las directivas, disposiciones oficios, radiogramas.	B16	- Falta de planes de recuperación
	- Se hacen utilizando este medio, en el caso del Cologe tenemos un grupo de control patrimonial donde están todos a nivel nacional.	B17	- Riesgo asociado a WhatsApp
	- Conocimiento, haber, a las maquinas hay que instalarlos antivirus, para evitar que ingresen y se apaguen constantemente,	B18	- Falta de antivirus
	- Los nombres, recién los escucho, la verdad no he indagado respecto a este tema.	B19	- Falta de planes de recuperación
	- Que actualmente es muy importante por todo lo que se realiza actualmente, todo por computadoras.	B20	- Importancia de la ciberseguridad.
	- Sinceramente, casi nada, excepto cuando envías información al Ministerio de Defensa, es allí donde normalmente usas el correo institucional.	B21	- No uso de correos institucionales
	- Ellos si te envían al correo institucional, jamás al personal, ni mucho menos por WhatsApp	B22	- Empleo adecuado de correo institucional
	- Bueno las coordinaciones que hago con la dirección de control patrimonial son así, correo institucional.	B23	- MINDEF se envía por correo institucional
	- Pero internamente, no, hasta por WhatsApp se envía oficios y otro tipo de documentos.	B24	- Uso de WhatsApp para enviar información
	- Que existe una ley de ciberseguridad y ciberdefensa, pero sinceramente, desconozco el alcance.	B25	- Desconocimiento de marco normativo
	- Este es mi tercer año aquí en el Cologe, nunca nadie nos dio una charla respecto a ese tema.	B26	- Falta de charlas de ciberseguridad

Partic ipante	Unidades de análisis	Código	Categoría
	- Planes, no, solo guardo mis archivos en mi memoria externa que es de mi propiedad.	B27	- No existe planes de recuperación de información
	- Para que en un momento cuando se malogre la maquina tenga archivado y no tener que buscar mi información que realice.	B28	- Archivos guardados en USB
	- La ciberseguridad consiste en la seguridad que debemos dar a las informaciones para evitar que intrusos informáticos se apoderen de ella.	C1	- Conocimiento limitado de ciberseguridad
	- Para ello es importante disponer de elementos que constantemente estén concientizando al personal a realizar esta tarea.	C2	- Falta de instrucción de ciberseguridad
	- Mira con respecto al Cologe, tiene a su cargo los servicios logísticos y la Jepae, ellos se conectan con todo el Perú a través del Siscobam.	C3	- Información de importancia institucional
	- En realidad, hay mucha información que debería estar con ciertos parámetros de seguridad debido que representa clasificada.	C4	- Información clasificada
	- Por ello la ciberseguridad en el Cologe es muy importante, así como en cualquier dependencia del Ejército.	C5	- Ciberseguridad institucional
	- Es aquel que se realiza con la finalidad de hurtar la información o dañar los sistemas informáticos.	C6	- Hackers informáticos
	- Claro, es fácil darse cuenta a través de los medios televisivos, el internet de los ciberataques.	C7	- Aumento de ciberataques
	- Asimismo, como ingresan a páginas de reconocidas empresas o de bancos para robar información.	C8	- Zona de acción de ciberataques
	- Que posteriormente puede ser usada en la contra de las personas, de igual forma del	C9	- Información extraída

Participante	Unidades de análisis	Código	Categoría
	celular, te pueden sacar los datos.		
	- Haber, la computadora que uso en el trabajo es propia, en la oficina se dispone de solamente una computadora.	C10	- Falta de equipos de computo
	- Ese PC tiene su clave de seguridad, bueno por lo menos tiene clave.	C11	- Solamente una clave de acceso
	- Además de antivirus que se encuentra desactualizada, eso sí se pondría a pensar que a través de él pueda acceder a robar tu información.	C12	- Antivirus desactualizado
	- Lo común es que las computadoras del Cologe cada relevo que ingresa y se le asigna la computadora.	C13	- Falta de control con los equipos
	- Haga el cambio de contraseña, con respecto a mi maquina portátil, solo una vez cambie de clave, pero es mía, solo yo la uso.	C14	- Difícilmente se cambia contraseñas
	- Eso es lo único que podría corroborar con respecto a procedimientos, plazos para cambiar contraseñas.	C15	- Falta de seguridad con contraseñas
	- Haber, en mi departamento la información a mi parecer no es tan sensible pues solo ve el tema de personal, efectivos y procedimientos de personal.	C16	- Información logística
	- Solo una pequeña base de datos sonde se coloca información de los oficiales y Tcos y Suboficiales.	C17	- Información de personal
	- Sin embargo, por ejemplo, en contrataciones, allí si hay mucha responsabilidad, la parte logística creo que es la más sensible.	C18	- Información sensible
	- A través de los servicios logísticos, lo de hurtar la información claro, existe el espionaje, que consiste en llevar información de un país a otro.	C19	- Conceptos de hackers
	- Para ser honesto, casi todo el tiempo, es común que se imparta información por ese	C20	- Compartir información por WhatsApp

Participante	Unidades de análisis	Código	Categoría
	medio.		
	- Incluso existen diferentes grupos en las dependencias que lo hace con la finalidad de intercambiar información.	C21	- Falta de seguridad con las informaciones
	- Porque es más fácil de enviar, sin embargo, no se debería, por medida de seguridad.	C22	- No empleo de medios autorizados
	- Se que son virus, actúan bloqueando la computadora, lo hace más lenta para dificultar el trabajo y en algunos casos malogra de inmediato el disco duro.	C23	- Conocimiento de virus
	- Correo institucional Chasqui, muy poco, la información institucional como por ejemplo cuadros básicos allí si se utiliza bastante este medio.	C24	- Poco uso de medios autorizados
	- Pero en el trabajo, muy poco se usa este correo, como ya te dije anteriormente parece ser que el WhatsApp ha desplazado a correos personales, institucionales.	C25	- Uso de WhatsApp para trasmitir información
	- Desconozco el marco normativo respecto a ciberseguridad.	C26	- Desconocimiento de marco normativo
	- Charlas con respecto a ciberseguridad, ninguno, sin embargo, se debería dar porque es un tema nuevo.	C27	- Falta de conocimiento de ciberseguridad
	- Que ya todos debemos manejar para proteger la información que se dispone.	C28	- Termino que se debe conocer
	- Planes como tal, los guardo en USB de mi propiedad.	D1	- Desconocimiento de planes de recuperación
	- La ciberseguridad son los procedimientos, las maneras de cómo vamos a través de medidas de seguridad en las computadoras.	D2	- Conocimiento limitado de ciberseguridad
	- Cuidar la información que allí se encuentra, ahora que es común los hackers.	D3	- Medidas de seguridad
	- Se puede apreciar en distintos medios de comunicación acerca de cómo ingresan a las	D4	- Difusión de hackeos a instituciones

Participante	Unidades de análisis	Código	Categoría
	páginas institucionales.		
	- Bloqueándolas y hurtando la información para después difundirla, se debe tener un especial cuidado con la información que maneja el Cologe.	D5	- Manejo de información clasificada
	- Debido que abarca procesos que se articulan con la Oficina Económica del Ejercito, y a nivel nacional.	D6	- Proceso logístico
	- Por lo tanto, se debe tener particular cuidado con esta dependencia, el Cologe.	D7	- Protección al Cologe
	- Claro, tienen dedicación exclusiva a realizar este tipo de actividades ilícitas, ciberataques.	D8	- Presencia de hackers
	- El ciberataque puede provenir desde distintas partes, uno nunca sabe de donde proviene.	D9	- Propensos a ciberataques
	- Pero para ello hay que adoptarlas medidas de seguridad adecuadas para contrarrestarlos y minimizar riesgos.	D10	- Adoptar medidas de seguridad
	- En ese sentido, entra a tallar el conocimiento del personal que labora en la dependencia primero para que generar conciencia	D11	- Conciencia de seguridad
	- Respecto a este tipo de procedimientos que podría poner en riesgo la información que se maneja.	D12	- Evitar ataques a las redes
	- Tipo de seguridad, bueno contraseña, la mía tiene antivirus original, pero la del Cologe tiene el antivirus vencido.	D13	- Medidas de seguridad
	- Actualmente casi segundo semestre no creo que compren, tiene sus contraseñas, pero es la misma desde hace 8 meses.	D14	- Cambio de contraseña
	- Llegue a labora y han rotado casi 3 personas en el puesto, sencillamente no tenemos una buena cultura de seguridad con las informaciones.	D15	- No se adoptan medidas de seguridad
	- La de mi PC personal, cada 8 meses o cuando veo que quizás alguien puede	D16	- Seguridad personal con contraseñas

Partic ipante	Unidades de análisis	Código	Categoría
	tener la clave.		
	- Lo de mi celular, cada 5 meses o cuando cambio de equipo.	D17	- Seguridad de quipos
	- Ordenaron que las claves de las computadoras sean dejadas al costado del escritorio, por si alguien tiene que sacar una información y se necesita.	D18	- Control de ingreso a los equipos
	- Para mí eso está mal, quizás porque uno es responsable de la PC que maneja y la información que en ella se encuentra, pero bueno ordenes son órdenes.	D19	- Ausencia de conciencia de seguridad
	- Que puede pasar, primero puede salir publicada en diarios de comunicación, así como sucedió con las exposiciones los planes que fueron filtradas.	D20	- Exposición mediática a la prensa
	- Además, es mediático, que al Ejército del Perú le hackeen y salga información no solo institucional, si no también personal de los Oficiales y Tcos SSOO.	D21	- Vulneración de información personal
	- Yo lo uso diario, es común ver este tipo de enlace para trasmitir y recibir información.	D22	- Uso de medios no autorizados
	- Bueno, bloquean las computadoras, lo inactivan, en algunos casos dañan el sistema operativo.	D23	- Conocimiento de virus
	- Con poca frecuencia, a veces enviamos el correo Olaya para envío de fax, pero el resto de información muy poco.	D24	- Poco uso de correo institucional
	- Se que existe una ley de ciberseguridad pero que muy poco se conoce en las dependencias	D25	- Desconocimiento de marco normativo de ciberseguridad
	- Mucho menos en el ejército, es algo que muy poca importancia le estamos dando institucionalmente.	D26	- Poca importancia
	- En el presente año, ninguna, ya dije antes, la institución muy poca importancia le da a este	D27	- Ausencia de charlas

Participante	Unidades de análisis	Código	Categoría
	tema.		
	- Algo que debemos promover actualmente, la ciberseguridad es un aspecto que debe ser manejado como prioridad institucional.	D28	- Ciberseguridad prioridad institucional
	- Todos los países actualmente están invirtiendo bastante en este tema, esperemos que el ejército del Perú comience a ver esto como un tema álgido.	D29	- Poca inversión en ciberseguridad
	- No se dispone de planes de recuperación que permita disponer de la información perdida	D30	- Falta de planes de recuperación
	- La ciberseguridad consiste en el cuidado de la información por parte de las personas para evitar que sea obtenida por otras con fines nocivos.	E1	- Poco conocimiento de ciberseguridad
	- Como robo de información personal, chantaje, retiro de dinero etc., todo aquello a través de la internet.	E2	- Ciberataques
	- Eso es lo que entiendo de este concepto nuevo y muy poco difundido en las dependencias institucionales la ciberseguridad.	E3	- Poca difusión de ciberseguridad
	- Respecto a la información del Cologe, como dependencia maneja la parte logística institucional, se interconecta a través del módulo Siscobam.	E4	- Manejo de información sensible
	- A nivel nacional, allí se ven actividades de todo tipo, aspectos económicos, cargos, es por ello que tiene mucha importancia la información.	E5	- Procesos logísticos
	- El manejo de información logística en coordinación con otras dependencias, por ello es muy importante.	E6	- Importancia institucional
	- Un ciberataque, es aquel que es realizado para causar daño en las redes informáticas, sé que existen los llamados piratas	E7	- Conocimiento de ciberataque

Participante	Unidades de análisis	Código	Categoría
	informáticos.		
	- Que constantemente están queriendo sacar información de las cuentas de bancos, tarjetas de crédito, asimismo, el hackeo a las páginas institucionales.	E8	- Presencia de hackers
	- Recientemente podemos apreciar como el denominado Guacamaya hackeo información del ejército, sobre todo conversaciones del planeamiento de la operación patriota en el VRAEM.	E9	- Hackeo a paginas institucionales
	- Cuenta con contraseña, por lo menos nadie puede ingresar si no la tiene, ah y antivirus si se encuentra desactualizado.	E10	- Limitadas medidas de seguridad
	- En ese aspecto si no incido mucho, mi laptop tiene 1 año, desde allí siempre ha tenido la misma contraseña.	E11	- Seguridad con contraseñas
	- Pero solamente el uso yo, por algo es personal, las del Cologe, por ejemplo, en el departamento administrativo todas tienen contraseña.	E12	- Gestión de contraseñas
	- Lo del cambio constante sino tengo mucha idea cada que tiempo se hace eso por parte del usuario.	E13	- Seguridad de hardware
	- Claro, puede salir hasta por parte de nosotros, quien controla si alguien se puede llevar en su USB información y después usarla en contra.	E14	- Riesgos de personal
	- Deberíamos tener un control de acceso a la información, para poder saber si la información no sale de uno de nosotros.	E15	- Control de la información
	- Además, si alguien quisiera obtener la información del Cologe, de que les puede servir, sin embargo, a otros países quizás si les pueda interesar esos datos.	E16	- Información sensible
	- Casi a diario, se ha convertido en el principal	E17	

Partic ipante	Unidades de análisis	Código	Categoría
	medio de comunicación que yo sepa para enviar información de todo tipo.		- WhatsApp para enviar información
	- Puedes apreciar los denominados grupos donde se esa enviando información como directivas, fax, etc., en el Cologe.	E18	- Exceso uso de aplicativos
	- Existe el grupo de WhatsApp llamado control patrimonial, que si bien es cierto deben ser espacios de intercambiar información e ideas, pero por acá se envía de todo.	E19	- Vulnera las medidas de seguridad
	- Bueno, no al detalle, pero malogran los equipos sean estas computadoras, tables, celulares etc.	E20	- Definición de virus
	- Muy poco lo utilizo, solamente cuando alguna dependencia lo solicita que se envíe por correo institucional.	E21	- Poco uso de correo institucional
	- Charlas con respecto a ciberseguridad, ninguno, sin embargo, se debería dar porque es un tema nuevo.	E22	- Falta de instrucción de ciberseguridad
	- Planes como tal, no solamente en mi caso guardo la información y mi disco externo.	E23	- Ausencia de planes de recuperación de información

Definición de temas (codificación axial) de las entrevistas

Habiendo realizado la codificación abierta y haber descubierto las categorías emergentes, se procedió a realizar la codificación axial, para generar temas que agrupen ciertas categorías que guardan relación entre sí.

Hernández y Mendoza (2018) sostuvieron “La codificación axial implica descubrir las categorías más importantes en términos de frecuencia (las más mencionadas) o relevancia para el planteamiento del problema y agrupar las categorías similares en temas (categorías más generales)” (p.489).

Tabla 7
Codificación axial del cuestionario

Categoría producida de la codificación abierta	Subcategoría central	Categoría
- Seguridad en todo momento. - Poco conocimiento de ciberseguridad. - Poca difusión de ciberseguridad - Conocimiento limitado de ciberseguridad. - Falta de conocimiento de ciberseguridad. - Falta de charlas de ciberseguridad. - Falta de instrucción de ciberseguridad. Riesgos de personal. - Hurto de información personal. - Ha crecido los hackers. - Existencia de hackers. - Hackers informáticos. - Desconocimiento de procedimiento de hackers. - Aumento de ciberataques. - Presencia de hackers. - Definición de virus. - Conceptos de hackers. - Termino que se debe conocer. - Presencia de hackers. - Limitadas medidas de seguridad. - Seguridad con contraseñas. - Gestión de contraseñas. - Difícilmente se cambia contraseñas. - Falta de seguridad con contraseñas. - Falta de antivirus. - Medidas de seguridad. - Cambio de contraseña. - No se adoptan medidas de seguridad. - Seguridad de hardware. - Vulneración de información personal. - Seguridad personal con contraseñas. - Seguridad de quipos. - Control de ingreso a los equipos.	Conocimiento de ciberseguridad Seguridad de los dispositivos Empleo de sistemas de protección	Situación actual de ciberseguridad

- Adoptar medidas de seguridad. - Evitar ataques a las redes. - Solamente una clave de acceso. - Imagen institucional. - Ciberseguridad institucional - Difusión de hackeos a instituciones. - Conocimiento de ciberataque. - Ciberataques. - Hackeo a paginas institucionales. - Exposición mediática a la prensa. - Confianza en la clave de seguridad. - Creer que es suficiente la seguridad. - Cambio de contraseña no se hace periódicamente - Falta de conciencia de seguridad. - Poca conciencia de seguridad. - Riesgo asociado a WhatsApp - Poco conocimiento de ciberataque. - Uso de WhatsApp para enviar información. - No uso de correos institucionales. - Empleo adecuado de correo institucional. - Mindef se envía por correo institucional. - Poco uso de medios autorizados. - Poco uso de correo institucional. - WhatsApp para enviar información. - Exceso uso de aplicativos - Vulnera las medidas de seguridad. - Uso de medios no autorizados.	Manejo de otros medios para envío de información Tipo de información que se maneja Vulneración del marco normativo vigente	Riesgo que genera el uso no adecuado de la información

- Información logística. - Información de personal. - Manejo de información sensible. - Información de importancia institucional. - Manejo de información clasificada. - Información de importancia institucional. - Información clasificada. - Manejo de información sensible. - Procesos logísticos. - Control de la información. - Información sensible. - Proceso logístico. - Protección al Cologe. - Importancia institucional. - Desconocimiento de marco normativo. - Desconocimiento de marco normativo de ciberseguridad. - Poca importancia. - Ausencia de conciencia de seguridad. - Falta de normas de seguridad. - No existe normas de seguridad contra ciberataques. - Antivirus desactualizado. - Falta de control con los equipos. - Vulnerables a los hackers - Falta de equipos de cómputo. - Falta de seguridad con las informaciones. - Seguridad de la información - Falta de seguridad. - Poca inversión en ciberseguridad. - Conocimiento de virus. - Archivos guardados en USB. - Ciberseguridad institucional - Falta de protección a información personal. - Falta de contraseñas dinámicas.	Personal Dispositivos Protección contra ciberataques	Factores que influyen en la ciberseguridad

- Seguridad personal con dispositivos. - Falta de seguridad. - Falta de protección de equipos. - Desconocimiento de cómo actúan los antivirus. - Desconocimiento del daño de los antivirus. - Poco conocimiento de ciberataque. - Zona de acción de ciberataques. - Ausencia de planes de recuperación de información. - de información - Desconocimiento de planes de recuperación. Falta de seguridad en la disposición. - Falta de instrucción de ciberseguridad. - Falta de instrucción sobre ciberseguridad. - Poca importancia a la ciberseguridad. - Falta de normas de recuperación de información. - ausencia de charlas. - Ciberseguridad prioridad institucional. - La ciberseguridad.	Planes de recuperación de información	

Matriz de análisis de los documentos

Tabla 8
Matriz de análisis de documentos

Documento	País	Referencia	Tema
Política Nacional de Ciberseguridad	Perú	Gobierno del Perú	**Conocimiento de ciberseguridad** Tiene como objetivo generar y fortalecer las capacidades existentes en materia de ciberseguridad, con el propósito de afrontar las amenazas, para ello es importante la capacitación del personal de funcionarios y servidores de las diferentes instituciones del estado.
Directiva de Funcionamiento del Sistema de Telemática y Estadística del Ejército (Dufsitele)		Ditele	**Planes de recuperación de información** Las Unidades y Dependencias del Ejército, deberán prever un ARCHIVO DIGITAL DE RESPALDO (BACKUP) de la documentación e información importante en todos los campos de estado mayor, y de forma especial la que tenga relación al uso de fondos presupuestarios, proporcionando la seguridad correspondiente en un lugar externo al centro informático. El acceso de personas a estas áreas será restringido y controlado
Directiva de Funcionamiento del Sistema de Telemática y Estadística del Ejército (DUFSITELE)		Ditele	**Personal** Las DDEE, GGUUC, UU y PPUU deberán difundir mediante publicaciones, cartillas e instructivos trimestralmente información técnica, con la finalidad de mantener actualizado al personal técnico de las últimas adquisiciones de material de telemática, así como las instrucciones de mantenimiento de los respectivos equipos. A fin de mantener al personal a la vanguardia de la modernidad y la eficiencia tecnológica, las DDEE y Dependencias del Ejército

			deberán en lo posible realizar por intermedio de las Instituciones Públicas – Privadas convenios interinstitucionales y/o de capacitación; realizando charlas, seminarios u otras modalidades de capacitación.
Directiva de Funcionamiento del Sistema de Telemática y Estadística del Ejército (Dufsitele)	Perú	Ditele	**Empleo de otros medios para envió de información** La prioridad en el empleo de los medios de telemática para la trasmisión de la información, teniendo con criterio principal la SEGURIDAD DE LAS COMUNICACIONES son los siguientes: **Para la trasmisión de información escrita:** (a) Correo Electrónico Institucional. (OLAYA) (b) Correo Electrónico Individual. (CHASQUI) (c) Fax institucional.
Ley Ejercito del Perú-Comando Logístico del ejercito		Ejército del Perú	**Tipo de información que se maneja** El Comando Logístico del Ejército es el órgano responsable de realizar procesos y actividades de carácter técnico y normativo del sistema logístico y del control patrimonial de la institución, tiene como funciones: Planeficaz, coordinar, dirigir, controlar y supervisar la ejecución del apoyo logístico del ejército, realizar los procesos y actividades de las funciones logísticas de abastecimiento, mantenimiento, transporte, construcciones, evacuación y hospitalización de veterinaria y diversos. planificar, coordinar y ejecutar las actividades relacionadas a los seguros de los bienes del ejército. etc.
Decreto Supremo N° 029 -2021 Reglamento de la Ley de Gobierno Digital	Perú	Gobierno del Perú	**Empleo de sistemas de protección** componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura

			tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.
Directiva de Funcionamiento del Sistema de Telemática y Estadística del Ejército (Dufsitele)	Perú	Ditele	**Dispositivos** Los usuarios del Sistema de Telemática exigen informaciones confiables, rápidas y seguras, por consiguiente, los encargados de diseñar el Sistema de Telemática tendrán en cuenta las siguientes consideraciones: (1) Con capacidades de Guerra Electrónica (Defensa Electrónica) y Ciberdefensa, que permita la protección de la información y enlace entre usuarios, a través del empleo de dispositivos y técnicas de seguridad. (2) Los equipos deben responder a los requerimientos operativos de la Fuerza Operativa (FO) y Otros Medios de Apoyo (OMA) y estandarizados por la Dirección de Telemática y Estadística del Ejército, articulado para el cumplimiento de los planes de operaciones y conducción de las operaciones y acciones militares.
Libro digital de Ciberseguridad	Perú	https://ciberseguridadenlinea	**Seguridad de los dispositivos** Es una declaración general producida por la alta dirección o un comité que habla del rol y el papel que juega la seguridad en la organización. Una política de seguridad puede ser generada de manera general a nivel organizacional o particular a nivel de un tema específico como un sistema.
La Guerra Cibernética (texto)	Perú	Reyes (2018)	**Protección contra ataques cibernéticos** Los virus informáticos se pueden inocular en el sistema como portadores de un material nocivo que se transmitirá de archivo en archivo o, a mayor escala, irá infectando otros sistemas

			conectados a la misma red. Al pirata le es posible limitar la capacidad del ordenador que ataca, o bien alterar la lógica interna del sistema de manera que éste produzca respuestas absurdas cuando no nocivas (bombas lógicas). La estrategia más efectiva en las empresas para mitigar y minimizar los efectos de un ataque informático es construir una base sólida de tecnología de seguridad. Las estrategias cubren una multitud de tecnologías, dispositivos, proceso y reglas que se deben seguir para proteger la integridad, confidencialidad y accesibilidad de las redes. Ten presente que el correo electrónico se considera el vector de amenaza número uno para una violación de seguridad. Pero, una aplicación adecuada de seguridad es capaz de bloquear los ataques entrantes y controlar los mensajes salientes para evitar la pérdida de datos confidenciales
La Guerra Cibernética (texto)	Perú	Reyes (2018)	**Los hackers** En el otro extremo, también crece la frecuencia de los accesos no autorizados por parte de individuos que se sirven de los canales mencionados para infligir daños a los sistemas de información y cuya importancia y significado no parece percibir la opinión pública, por más que las espectaculares hazañas de los hackers (intrusos informáticos) menudeen últimamente en los titulares de prensa. Las amenazas que para la comunidad internacional supone la vulnerabilidad informática de las sociedades civiles y sus infraestructuras de seguridad El hacker es una persona que tiene unos conocimientos avanzados en el área de informática y es capaz de acceder ilegalmente a sistemas informáticos ajenos para manipularlos.

			Ciberataque
La Guerra Cibernética (texto)	Perú	Reyes (2018)	Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o, incluso, utilizada para extorsionar.

Nota. Se elaboró con los documentos planteados para el análisis documental

4.4 Soporte de categorías

Tabla 9
Soporte de categorías

Categorías	Subcategorías	Patrones	Explicación Subcategoría
Situación actual de ciberseguridad	Conocimiento de ciberseguridad	Ciberseguridad	Entendimiento y aplicación de prácticas para proteger sistemas informáticos contra accesos no autorizados y amenazas digitales, garantizando la seguridad de la información en entornos digitales
		Ciberataques	
	Seguridad de los dispositivos	Dispositivos pasivos	Implica tomar medidas para proteger la información en aparatos electrónicos, como computadoras y teléfonos móviles
		Dispositivos activos	
	Empleo de sistemas de protección	Seguridad de la red	Utilización y configuración de herramientas y medidas específicas diseñadas para resguardar sistemas informáticos contra amenazas cibernéticas, garantizando la seguridad y la integridad de la información digital almacenada y procesada
		Seguridad de la nube	
		Seguridad física	
Riesgo que genera el uso no adecuado de la información	Manejo de otros medios para envió de información	Seguridad de datos	La utilización de diversos canales y métodos para transmitir datos electrónicos de manera segura y eficiente, asegurando la integridad y confidencialidad durante la transferencia de información digital
		Seguridad de aplicaciones	
		Seguridad de la identidad	
	Tipo de información que se maneja	Información confidencial o clasificada	La categorización y naturaleza de los datos electrónicos que se gestionan, abarcando desde información pública hasta datos altamente confidenciales, en función de su contenido y grado de sensibilidad
		Información externa	
		Información interna	

Nota. Se elaboró con las categorías apriorísticas y las emergentes

	Vulneración del marco normativo vigente	Fraude informático	Incumplimiento de las normas y regulaciones establecidas en el ámbito de la ciberseguridad, comprometiendo la integridad y legalidad de las prácticas digitales actuales
		Estafa agravada	
		Suplantación	
Factores que inciden en el nivel de ciberseguridad	Personal	Personal interno	Responsables de gestionar y procesar datos, asegurando la integridad, confidencialidad y disponibilidad de la información digital en su posesión o responsabilidad
		Personal externo	
	Dispositivos informáticos	Computadoras	Herramientas electrónicas como computadoras, tablets y smartphones utilizados para procesar, almacenar y acceder a información en entornos digitales
		Móviles	
		Memorias externas	
	Protección contra ataques electrónicos	Software antivirus	Implementación de medidas y estrategias para resguardar sistemas y datos frente a amenazas digitales, evitando accesos no autorizados y minimizando el impacto de posibles ciberataques
		Firewall perimetral de red	
		Servidor proxy	
		Cifrado de punto final	
	Planes de recuperación de información	Medidas de protección privacidad digital	Procedimientos detallados que establecen las acciones y pasos a seguir para restaurar datos y sistemas después de un incidente, asegurando la continuidad operativa y la recuperación eficiente de información
		Recuperar la información	
		Evitar acceso no autorizado a los datos o su perdida	

Descripción narrativa del soporte de categorías

Categoría 1: Situación actual de ciberseguridad

- **Sub categoría:** Conocimiento de ciberseguridad

Durante la investigación de campo se observó respecto a esta categoría que, no existe un buen concepto respecto a ciberseguridad en el Comando Logístico del Ejército, los entrevistados tienen definiciones generales, sin embargo, la finalidad, el campo de acción, desconocen cómo actúa la ciberseguridad siendo esto una falencia en el propósito de tener una buena cultura de ciberseguridad que actualmente se debe tener para proteger la información que maneja la institución y en especial el Cologe, se puede afirmar que saben un poco del que cosa es, pero no saben nada de cómo enfrentarlo.

- *La ciberseguridad es la seguridad hacia los equipos informáticos.*
- *Que debemos tener a la hora que trabajamos con ellos, por ejemplo, una computadora, un celular.*
- *Para que no puedan ser obtenidos por otras personas ajenas al trabajo y que no tienen relación con la información que manejan.*

Según el análisis de documentos, la Política Nacional de Ciberseguridad, tiene como objetivo generar y fortalecer las capacidades existentes en materia de ciberseguridad, con el propósito de afrontar las amenazas, para ello es importante la capacitación del personal de funcionarios y servidores de las diferentes instituciones del Estado.

- **Sub categoría**: Los hackers

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan definiciones que se acercan a la adecuada definición de estas personas que se dedican a hurtar la información a través de mecanismos como virus que inoculan el sistema mediante diversas modalidades, sin embargo el personal del Cologe solamente conoce que existe, pero no saben el procedimiento de ingreso a los sistemas, allí se aborda el problema del desconocimiento y conlleva a no tomar las medidas de seguridad respectivas para la protección de los datos que maneja la dependencia.

- *Pero desconozco como lo hacen, se aprecia mucho por los medios de información que extraen información de diferentes instituciones.*
- *Que constantemente están queriendo sacar información de las cuentas de bancos, tarjetas de crédito, asimismo, el hackeo a las páginas institucionales.*

Según el análisis de documentos: La Guerra Cibernética (texto), define el hacker, es una persona que tiene conocimientos avanzados en el área de informática y es capaz de acceder ilegalmente a sistemas informáticos ajenos para manipularlos, el intruso puede manipular archivos introduciendo datos propios o alterando los existentes.

Puede, también, reprogramar sistemas de información que controlan importantes procesos mediante la introducción de comandos falsos y destruir la integridad del sistema, o bien comprometer la disponibilidad de determinados datos suprimiéndolos o modificando los servicios que proporcionan, de modo que sistemas enteros dejen de funcionar.

- **Sub categoría** Protección contra ataques informáticos

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que no disponen de antivirus en su mayoría, se encuentran desactualizados, desconocen si existen otros sistemas de protección contra ataques cibernéticos, no han recibido la instrucción correspondiente respecto a medidas de seguridad contra ciberataques por parte de las dependencias encargadas, no existe una estrategia adecuada de ciberseguridad.

- *Asimismo, como ingresan a páginas de reconocidas empresas o de bancos para robar información.*
- *Que posteriormente puede ser usada en la contra de las personas, de igual forma del celular, te pueden sacar los datos.*
- *Según el análisis de documentos: La Guerra Cibernética (texto), La estrategia más efectiva en las empresas para mitigar y minimizar los efectos de un ataque informático es construir una base sólida de tecnología de seguridad.*

Las estrategias cubren una multitud de tecnologías, dispositivos, proceso y reglas que se deben seguir para proteger la integridad, confidencialidad y accesibilidad de las redes.

- **Sub categoría** Ciberataque

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que tiene algún conocimiento de cómo se produce este tipo de acciones por parte de los hackers, definen donde actúan los hackers en un ciberataque, pero no tienen la manera como lo hacen, la mayoría lo lleva a los celulares, hurto de información, cuando se sabe que un ciberataque al Cologe tiene otro propósito más amplio.

- *Que constantemente están queriendo sacar información de las cuentas de bancos, tarjetas de crédito, asimismo, el hackeo a las páginas institucionales*

- *Recientemente podemos apreciar como el denominado Guacamaya hackeo información del ejército, sobre todo conversaciones del planeamiento de la operación patriota en el VRAEM.*
- *Un ciberataque, es aquel que es realizado para causar daño en las redes informáticas, sé que existen los llamados piratas informáticos.*
- *Según el análisis de documentos: La Guerra Cibernética (texto), Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas.*

Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o, incluso, utilizada para extorsionar.

Categoría 2: Riesgo que genera el uso no adecuado de la información

- **Sub categoría:** Seguridad de los dispositivos

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que no tienen una costumbre de seguridad con los dispositivos que emplean en el Cologe, las claves de las computadoras no son cambiadas periódicamente, empleo de USB a cada momento, sumado al punto que los antivirus se encuentran desactualizados.

- *Actualmente casi segundo semestre no creo que compren, tiene sus contraseñas, pero es la misma desde hace 8 meses.*
- *Llegue a labora y han rotado casi 3 personas en el puesto, sencillamente no tenemos una buena cultura de seguridad con las informaciones.*
- *Haber, normalmente casi toda la información se comparte por WhatsApp, porque es más rápido y creo que por lo menos es seguro.*
- *Según el análisis de documentos: La Guerra Cibernética (texto), la seguridad de los dispositivos que pertenecen a una organización, empresa, etc. es una declaración general producida por la alta dirección o un comité que habla del rol y el papel que juega la seguridad en la organización.*

Una política de seguridad puede ser generada de manera general a nivel organizacional o particular a nivel de un tema específico como un sistema.

- **Sub categoría:** Empleo de otros medios para envió de información

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan no usar con mucha frecuencia correos institucionales autorizados que permitan tener cierta seguridad a la hora de trasmitir la información, es común ver el envío de información clasificada vía aplicativos como WhatsApp, vulnerando la seguridad correspondiente, incluso a través de grupos se comparte distinto tipo de información:

- *Sinceramente, casi nada, excepto cuando envías información al Ministerio de Defensores allí donde normalmente usas el correo institucional.*
- *Para ser honesto, casi todo el tiempo, es común que se imparta información por ese medio.*
- *Incluso existen diferentes grupos en las dependencias que lo hace con la finalidad de intercambiar información.*

Según la Directiva de Funcionamiento del Sistema de Telemática y Estadística del Ejército (Dufsitele) La prioridad en el empleo de los medios de telemática para la trasmisión de la información, teniendo con criterio principal los siguientes:

Para la Trasmisión de información escrita:

- *Correo Electrónico Institucional. (Olaya)*
- *Correo Electrónico Individual. (Chasqui)*
- *Fax institucional.*

- **Sub categoría:** Tipo de información que se maneja

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que el Cologe maneja bastante información desde el punto de vista logístico a nivel institución, además esta se intercambia con otras dependencias como parte del proceso logístico y también por medio del Siscobam.

- *Respecto a la información del Cologe, como dependencia maneja la parte logística institucional, se interconecta a través del módulo Siscobam E4*
- *A nivel nacional, allí se ven actividades de todo tipo, aspectos económicos, cargos, es por ello que tiene mucha importancia la información E5*
- *El manejo de información logística en coordinación con otras dependencias, por ello es muy importante E6*

La Ley Ejército del Perú, dice: El Comando Logístico del Ejército es el órgano responsable de realizar procesos y actividades de carácter técnico y normativo del sistema logístico y del control patrimonial de la institución, tiene como funciones: Planificar, coordinar, dirigir, controlar y supervisar la ejecución del apoyo logístico del Ejército, realizar los procesos

y actividades de las funciones logísticas de abastecimiento, mantenimiento, transporte, construcciones, evacuación y hospitalización de veterinaria y diversos. Planificar, coordinar y ejecutar las actividades relacionadas a los seguros de los bienes del Ejército, etc.

Categoría 3: factores que influyen en la ciberseguridad

- **Sub categoría:** Marco normativo vigente

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan conocer de la mayoría, la ley de Ciberseguridad, además de su reglamentación y todas las que conciernen, sin embargo, solo conocimiento, mas no saben el alcance, la finalidad etc. Que permita crear conciencia para tomar medidas que reduzcan *la vulnerabilidad existente respecto a la ciberseguridad.*

- *Se que existe una ley de ciberseguridad y ciberdefensa, pero sinceramente, desconozco el alcance.*
- *Se que existe una ley de ciberseguridad pero que muy poco se conoce en las dependencias.*
- *Mucho menos en el ejército, es algo que muy poca importancia le estamos dando institucionalmente.*

La Ley de Ciberdefensa N° 30999 – 2019, tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado del Perú, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

- **Sub categoría:** Sistema de protección

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que no existe en el Cologe un adecuado sistema de protección contra ataques cibernéticos, desconocen cuáles son los procedimientos para generar una seguridad a las informaciones que maneja el Cologe institucionalmente.

- Algo *que debemos promover actualmente, la ciberseguridad es un aspecto que debe ser manejado como prioridad institucional.*
- *Los países actualmente están invirtiendo bastante en este tema, esperemos que el ejército del Perú comience a ver esto como un tema álgido. Según el Decreto Supremo N° 029 - 2021 Reglamento de la Ley de Gobierno Digital un sistema de protección lo constituyen componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera*

que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

- **Sub categoría:** Planes de recuperación de información

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan desconocer respecto a los planes de recuperación de datos que debe haber en toda dependencia, desconocimiento total de los procedimientos que afectan la seguridad de la información sensible que maneja el Cologe.

- *Planes como tal, no solamente en mi caso guardo la información de mi disco externo" F20.*

Según la DITELE (2019) especifico que:

> Las Unidades y Dependencias del Ejército, deberán prever un archivo digital de respaldo (BACKUP) de la documentación e información importante en todos los campos de estado mayor, y de forma especial la que tenga relación al uso de fondos presupuestarios, proporcionando la seguridad correspondiente en un lugar externo al centro informático, por lo tanto, el acceso de personas a estas áreas será restringido y controlado. (p. 65)

- **Sub categoría:** Personal y dispositivos

Durante la investigación de campo se observó respecto a esta categoría que los entrevistados manifiestan que el comando de la institución no le da la importancia al nuevo concepto de ciberseguridad, asimismo, en los dispositivos como hardware no se realizan las debidas acciones para cambiarlos o actualizarlos con antivirus adecuados, esto parte desde el comando institucional, estamos viviendo la era digital y debemos partir primeramente por los riesgos que estamos expuestos al hacer uso de la internet y los medios digitales.

Según la Ditele (2019) estableció que:

Los usuarios del Sistema de Telemática exigen informaciones confiables, rápidas y seguras, que permita articular el Sistema de Telemática del Ejercito, estos deben ser tomados en cuenta por todo el personal que labora en todas las dependencias de la institución (p.34).

Además, el mismo texto abordo otros aspectos que comprende la parte operativa del Sistema de Telemática del Ejército:

> Con capacidades de Guerra Electrónica (Defensa Electrónica) y Ciberdefensa, que permitan la protección de la información y enlace entre usuarios, a través del empleo de dispositivos y técnicas de seguridad, los equipos deben responder a los requerimientos operativos de la Fuerza Operativa (FO) y Otros Medios de Apoyo

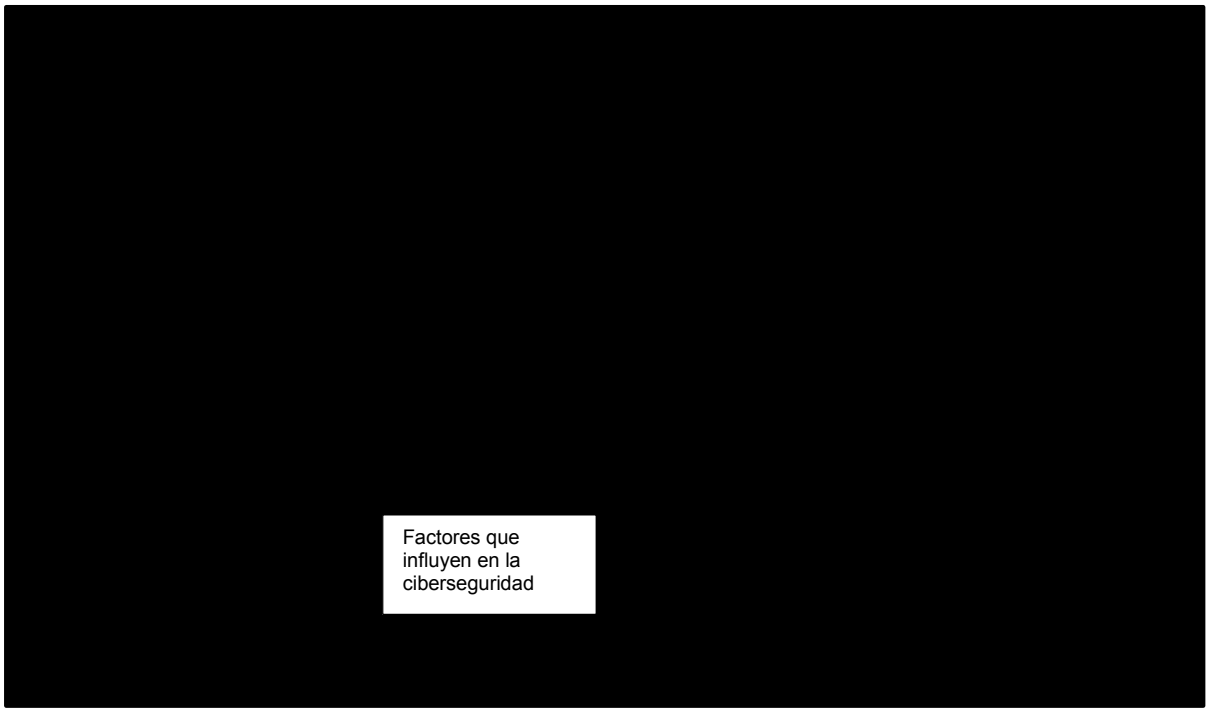
(OMA) y estandarizados por la Dirección de Telemática y Estadística del Ejército, articulado para el cumplimiento de los planes de operaciones y conducción de las operaciones y acciones militares.(p.76)

4.5 Red semántica

Respecto a la situación actual de ciberseguridad en el Comando Logístico del Ejército, existe un total desconocimiento del término por parte del personal que labora en esta dependencia, esto trae consigo que no exista una protección contra los ataques informáticos por intermedio de hackers que pueden vulnerar la información que se dispone.

El desconocimiento del marco normativo vigente actualmente en el Perú respecto a la ciberseguridad es uno de los factores que inciden en el nivel de seguridad correspondiente, no se puede cuidar lo que no se sabe que es importante, esto ocasiona la confianza por parte del personal, por ejemplo el empleo de medios o aplicativos para enviar información clasificada, asimismo, no existe un adecuado plan de recuperación de datos que debería haber así como lo establece el marco normativo para la institución.

Figura 3
Red semántica



Nota. Se elaboró de acuerdo a las categorías y sub categorías de las entrevistas

La información que maneja el Comando Logístico del ejército de todo el proceso logístico institucional, hace que el comando de la institución considere de prioridad la ciberseguridad que se debe tener por el tipo de información sensible que se dispone, asimismo, la concientización a través de las dependencias encargadas de llevar a cabo la promoción de la ciberseguridad en cada uno de los integrantes considerando que vivimos en la era digital y el manejo y empleo de redes implica la seguridad correspondiente.

4.6 Triangulación

En las investigaciones uno de los procedimientos para el rigor científico lo constituye la triangulación, sean estas de datos, de investigadores, teóricas etc. Ruiz (2003) sostuvo: “La triangulación es una especie de control de calidad total que debería ser aplicado en todas las investigaciones cualitativas, ya que la limitación a una única fuente de información pone en riesgo su confiabilidad” (p,123), en ese sentido en la investigación se realizó la triangulación de técnicas cualitativas (entrevistas y análisis documental) que permitió cruzar información relevante que se plasmó en la síntesis integrativa.

Tabla 10

Tabla de triangulación de técnicas cualitativas

Categorías	Entrevista	Análisis documental	Síntesis integrativa
Situación actual de ciberseguridad	La Situación actual de la ciberseguridad en el Comando Logístico del ejercito constituye una preocupación por parte de la institución, el personal militar desconoce la importancia de llevar a cabo procedimientos que conlleven a una cultura de ciberseguridad que pueda garantizar el flujo de la información que se maneja, esto trae consigo vulnerabilidades que pueden ser aprovechadas por los hackers para hurtar la información de todo el proceso logístico, se desconoce cómo actúan los hackers, por ende , se desconoce cómo protegerse,	Según la Política Nacional de Ciberseguridad: esta “Tiene como objetivo generar y fortalecer las capacidades existentes en materia de ciberseguridad, con el propósito de afrontar las amenazas, para ello es importante la capacitación del personal de funcionarios y servidores de las diferentes instituciones del estado” en tal sentido se debe llevar a cabo una campaña de concientización e instrucción respecto a la ciberseguridad en la institución, que promueva buenas prácticas así como el conocimiento de los términos como hackers, ataque informático y sobre	La situación actual de la ciberseguridad en el Comando Logístico del Ejercito, de acuerdo al marco normativo vigente desde leyes, Políticas Nacionales, que ya tienen desde ya varios años, parece que no tiene cabida en la institución, a pesar que constituye un elemento importante dentro de la estructura organizacional debido que lleva a cabo todo el proceso logístico, en tal sentido se debe desarrollar acciones para revertir esta situación en beneficio institucional que implica el

	mediante el empleo de medidas de seguridad que parten del usuario, de la persona como eje de la ciberseguridad en la institución.	todo como se realizan para la precaución necesaria del personal militar que labora en el Cologe.	manejo y cuidado de la información.
Riesgo que genera el uso no adecuado de la información	La información que maneja el Comando Logístico del Ejercito es muy sensible, a través de los Servicios Logísticos y mediante el módulo Siscobam desarrollan el proceso logístico a nivel nacional, en este proceso se intercambia con otras dependencias, es decir la información que diariamente se comparte es de importancia institucional, sin embargo no existe un adecuado sistema de protección de la información, se guarda información en USB no existiendo planes de recuperación correspondientes que permita asegurar la información en caso de incidentes.	El Comando Logístico del Ejército es el órgano responsable de realizar procesos y actividades de carácter técnico y normativo del sistema logístico y del control patrimonial de la institución, tiene como funciones: Planeficaz, coordinar, dirigir, controlar y supervisar la ejecución del apoyo logístico del ejército, realizar los procesos y actividades de las funciones logísticas de abastecimiento, mantenimiento, transporte, construcciones, evacuación y hospitalización de veterinaria y diversos. planificar, coordinar y ejecutar las actividades relacionadas a los seguros de los bienes del ejército. etc.	El riesgo que genera el uso no adecuado de la información por parte del personal militar que labora en el Comando Logístico del ejército, es alto, debido que se está tomando como una rutina diaria no disponer de medidas de protección como antivirus actualizados, conocimiento del personal que se convierte en el factor más vulnerable de la ciberseguridad, pues se está guardando información en USB, las claves de las computadoras no son cambiadas periódicamente y un total desconocimiento de cómo actúan los piratas informáticos que permita por lo menos cuidar la información que maneja.
Factores que influyen en la ciberseguridad	El desconocimiento del marco normativo vigente respecto a la ciberseguridad y de manera general a la seguridad de toda la información que se maneja, el no utilizar	La ciberseguridad lo constituye componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas de	Uno de los factores que incide en dar en el nivel de bajo respecto a la ciberseguridad en el Comando Logístico del Ejercito es el desconocer que estamos en la

	adecuados sistemas de protección, no disponer de equipos adecuados, antivirus desactualizados, sumado al desconocimiento del personal inciden que, de acuerdo a lo manifestado por los entrevistados, que el nivel de seguridad en el Cologe es bajo respecto a la ciberseguridad.	información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.	era digital y que existe un marco normativo respecto a la ciberseguridad que debe adoptar de manera obligatoria las instituciones públicas entre ella el ejército, asimismo esto implica que se lleven a cabo acciones que al parecer no saben que es atentar contra las medidas de seguridad adecuadas que permitan cuidar la información que diariamente se maneja.

Nota. Se realizó la triangulación de datos para dar el rigor científico correspondiente.

Capítulo V: Diálogo teórico empírico

En este capítulo se procedió a realizar el dialogo teórico empírico que permita articular la teoría con los hallazgos, al respecto Vargas (2011) sostuvo:

> Al llegar a esta etapa si la investigación fue teórica empírica Una de las etapas correspondientes en la investigación es el dialogo teórico empírico, es decir empezar a contrastar los hallazgos de la realidad develada con la teoría propuesta, sean estos datos de normas, leyes, que permita opinar respecto a si los hallazgos afirman la parte teórica o la refutan (p.34).

Tabla 11
Dialogo teórico empírico

Cita teórica	Hallazgo	Dialogo teórico empírico
La DUFSITELE 2020 dice: Las DDEE, GGUUC, UU y PPUU deberán difundir mediante publicaciones, cartillas e instructivos trimestralmente información técnica, con la finalidad de mantener actualizado al personal técnico de las últimas adquisiciones de material de telemática, así como las instrucciones de mantenimiento de los respectivos equipos.	El Comando Logístico del Ejercito no cuenta con una cultura adecuada de ciberseguridad, no se dictan charlas al personal respecto a ciberseguridad y las medidas de seguridad que se debe tener para evitar ataques cibernéticos que pongan en riesgo la información sensible que se maneja sobre el procedimiento logístico.	El investigador refuta lo descrito en la DUFSITELE, respecto a los instructivos, cartillas de ciberseguridad que debe dictarse al personal, pues el hallazgo indica que no existe interés por educar e incentivar respecto a ciberseguridad en el Cologe, no se han desarrollada charlas que promuevan el interés institucional en esta dependencia.
La Dufsitele 2020 sostiene: La prioridad en el empleo de los medios de telemática para la trasmisión de la información, teniendo con criterio principal la *Seguridad De Las*	Se ha encontrado que se ha convertido en una rutina la difusión de información clasificada utilizando aplicativos webs, siendo el más usado el WhatsApp, esto contraviene las medidas de seguridad	El investigador refuta lo descrito en la Dufsitele, respecto a la trasmisión de datos que debe realizarse por fuentes autorizada que garanticen la seguridad y la confiabilidad, pues los hallazgos indican que esto no

Comunicaciones son los siguientes: Para la Trasmisión de información escrita: (a) Correo Electrónico Institucional. (Olaya) (b) Correo Electrónico Individual. (Chasqui) (c) Fax institucional.	establecidas en la Musítele, respecto a la trasmisión de la información, considerando lo sensible de la información que maneja el Cologe como parte del sistema logístico con otras dependencias.	viene realizándose, esto ocasiona que la información este expuesta a los hackers o a personas que podrían brindar esa información a medios de prensa con la finalidad de desprestigiar respecto a la ciberseguridad institucional.

Capítulo VI: Conclusiones y recomendaciones

6.1 Conclusiones

Después de haber realizado el proceso de análisis correspondiente y de haber comprendido el problema de manera holística, se ha llegado a las conclusiones siguientes:

Respecto al objetivo N° 1: *Describir la situación actual de ciberseguridad en el Comando logístico del Ejército (Cologe).*

La situación actual de ciberseguridad por parte del Cologe es deficiente o nula, el personal que labora en esta dependencia en su mayoría desconoce lo que es ciberseguridad, tiene un conocimiento vago de cuál es el procedimiento de cómo actúan los hackers y cuáles son las medidas de protección que debe darse a la información.

Se desconocen procedimientos mínimos de seguridad como son las contraseñas que deben ser cambiadas cada cierto tiempo, la seguridad externa e interna mediante firewalls que protejan la información que manejan diariamente y la comparten con otras dependencias.

Se emplea el aplicativo de WhatsApp para intercambiar información a nivel nacional, se han creado grupos donde diariamente se realiza este procedimiento, contraviniendo lo descrito por la Dufsitele respecto a la trasmisión de información en la institución.

La Ditele encargada de promover la ciberseguridad en la institución no ha emitido boletines, folletos, charlas que concienticen al personal del Cologe respecto a la seguridad de las informaciones.

Respecto al objetivo N° 2: *Describir el riesgo que genera el uso no adecuado de la información en el Comando logístico del Ejercito (Cologe).*

El desconocimiento de medidas de seguridad mínimas que parte desde el usuario, el desconocimiento de las normas y procedimientos de la Dufsitele que regula el empleo de los equipos informáticos, esto genera que el Comando Logístico del Ejército este expuesto al hurto de la información que maneja respecto a los cargos de armamento, vehículos, tipo de munición que se dispone, sean filtradas a través de personas ajenas a la institución y sean llevadas a medios de comunicación, u obtenidas por otros países para cualquier tipo de uso.

No se dispone de un buen sistema de ciberseguridad, esto puede ser aprovechado por hackers que logren obtener información del personal (contraseñas de cuentas, bienes, direcciones) a través del Phishing, que consiste en engañar a las personas para que

compartan información confidencial como contraseñas y números de tarjetas de crédito, para luego ser chantajeadas.

Respecto al objetivo N° 3: *Implementar protocolo de ciberseguridad obligatorio para el personal que labora en el Comando logístico del Ejercito (Cologe).*

En el aporte doctrinario se ha propuesto mediante afiches, lemas, que el personal militar que labora en el Cologe tome conciencia de la ciberseguridad en esta época, además de establecer un protocolo simple de uso práctico para el personal antes de empezar las labores con sus equipos informáticos diariamente.

6.2 Recomendaciones

De acuerdo a las conclusiones se plantean las siguientes recomendaciones que deben transformarse en acciones para poder disponer de una adecuada ciberseguridad en el Comando Logístico del Ejercito y salvaguardar la información que maneja sobre el proceso logístico a nivel nacional y la importancia que debe darse a esta dependencia, para ello se proponen las recomendaciones siguientes:

Respecto al objetivo N° 1:

El Comando Logístico del Ejército, debe coordinar con la Ditele y el Oficial de Seguridad y Confianza Digital de la institución charlas correspondientes al personal que labora en esta dependencia y los servicios Logísticos para concientizar respecto a los riesgos que se está expuesto si no se cuenta con un adecuado nivel de ciberseguridad, se debe entender que el principal riesgo a la ciberseguridad es el ser humano.

El Cologe en coordinación con la Dirección de Telemática del Ejército, debe evaluar los diferentes riesgos de ciberseguridad en lo que respecta a hardware y software que permita tomar acciones de control y respuesta.

Se debe fomentar el masivo empleo de los correos institucionales, se debe instalar antispam que no permita que en las computadoras de la institución exista el ingreso a aplicativo WhatsApp y otras páginas desconocidas que pongan en peligro la información.

Respecto al objetivo N° 2:

Se debe implementar constantemente antivirus, filtros que permita contrarrestar a los hackers.

El Comando Logístico del Ejército debe solicitar a la Ditele personal especialista para realizar un análisis de riesgos informáticos, que lleve a cabo una evaluación de los distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza a la dependencia, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas, salvaguardando la información que se maneja.

Respecto al objetivo N° 3:

En coordinación con la Ditele, emitir boletines, folletos, charlas que concienticen al personal del Cologe respecto a la seguridad de las informaciones.

En el aporte doctrinario se ha propuesto mediante afiches, lemas, que el personal militar que labora en el Cologe tome conciencia de la ciberseguridad en esta época, además de establecer un protocolo simple de uso práctico para el personal antes de empezar las labores con sus equipos informáticos diariamente.

Elaboración de un vademécum con indicaciones sencillas y fáciles de ser llevadas a cabo por el personal para un buen empleo de los medios informáticos y contribuir a la ciberseguridad en el Cologe.

Referencia bibliográfica

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación.* México: Editorial Mexicana.

Granada, H. (1984). *La Teoría, su estructura e importancia en la investigación científica. Revista de Psicología.* Obtenido de http://revistas.pucp.edu.pe/index.php/psicologia/article/view/4494

Vargas, X. (2011). *Como Hacer Investigación Cualitativa.* Jalisco: Exteta.SAC.

Palomino, Peña, Zevallos, & Orizano. (2015). *Metodología de la Investigación.* Lima: San Marcos.

Hernández, J., & Ibarra, S. (2013). La teoría de los Recursos y Capacidades. Un Enfoque actual en la estrategia empresarial. *Visión Universitaria*, 23-24.

Porto, L., & Ruiz, J. (2014). Los Grupos de Discusión. En Sáenz, Tamez, & (Cord), *Métodos y Técnicas Cualitativas y Cuantitativas Aplicables a la Investigacion en Ciencias Sociales* (págs. 254-271). Monterrey: Tirant Humanidades.

Mendizábal, N. (2014). Los Componentes en el Diseño Flexible en la Investigación Cualitativa. En G. (. Vasilachis, *Estrategias de Investigación Cualitativa* (págs. 65-105). Madrid: Lucerna.

Trujillo, A., Naranjo, M., Lomas, K., & Merlo, M. (2019). *Investigación Cualitativa, Epistemología, Consentimiento Informado, Entrevistas en Profundidad.* Ibarra: Universidad Técnica del Norte.

Sáenz, K., & Rodríguez, K. (2014). Habilidades Investigativas. En K. Sáenz, & G. (. Tamez, *Métodos y Técnicas Cualitativas y Cuantitativas Aplicables a la Investigación en Ciencias Sociales* (págs. 86-95). Monterrey: Tirant Humanidades.

Gayou, J. L. (2009). *Como hacer investigación cualitativa. Fundamentos y Metodología.* México: Paidos mexicana SA.

Vargas, Z. (2009). La Investigación Aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación de la Universidad de Coata Rica*, 155-165.

MONTSERRAT, D. (2017). *Desminando la confianza en América del Sur: el rol del desminado humanitario en la construcción de confianza entre Ecuador y Perú (1998-2016).* UNIVERSIDAD TORCUATO DI TELLA, Caba, Argentina.

Cisterna, F. (2005). CATEGORIZACIÓN Y TRIANGULACIÓN COMO PROCESOS DE VALIDACIÓN DEL CONOCIMIENTO EN INVESTIGACIÓN CUALITATIVA. *Departamento de Ciencias de la Educación, Facultad de Educación y Humanidades. Universidad del Biobío, Chillán, 14*, 63.

Izcara, S. (2014). *Manual de Investigación Cualitativa.* Colonia del Carmen, México: Fontamara.

Hernández, R., & Mendoza, C. (2018). *Metodología de la Investigación, Las rutas cuantitativa, cualitativa y mixta* (Vol. 8va edición). Celaya, México: McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.

Ormachea, J. (2019). *Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional.* Centro de Altos Estudios Nacionales, Lima.

Guerrero, R., & Proaño, C. (2020). *El manejo de la ciberseguridad en Fuerzas Armadas.* Universidad de las Fuerzas Armadas, Quito.

Huamán, J. (2020). *Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejercito, Lima 2020.* Escuela Superior de Guerra del Ejercito, Lima, Perú.

Baretto, J. (2017). *La Defensa Nacional y la Estrategia militar de Seguridad Cibernética.* Escuela Superior de Guerra Conjunta de Argentina, Buenos Aires, Argentina.

Taype, M. (2020). *La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú, año 2017.* Universidad Nacional de Piura, Piura, Perú.

Castro, M. (2001). Cuestiones de Metodología Cualitativa. *Revista de la Universidad Nacional de Educación a Distancia*, 169.

Quintana, M. (2021). Los Ciberataques en America Latina y sus consecuencias. *Revista Científica de la Universidad de Medellin*, 21.

Legislativo, P. (2019). Ley de Gobierno Digital. Lima, Perú: Diario Oficial El Peruano.

Armero, J., & Calderón, V. (2018). *UTILIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y LA INSTRUCCIÓN DE MORTEROS DE LOS CADETES DE INFANTERÍA DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019.* Escuela Militar de Chorrillos, Lima.

Fernández, A. (2020). Revista Anahuac-Uni CELAYA. *Revista Científica de la UNI Celaya*, 37-78.

Del rio, R. (2011). La Ciberamenaza y como combatirla en siglo XX1. *Revista de la Universidad de Murcia*, 23.

Machin, N., & Gazapo, M. (2017). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA. *Revista UNISCI / UNISC*, 45-55.

Pereda, L. (s.f.). El Ciberespacio, retos y desafíos. *Revista científica de l Universidad del Nprt*.

Pereda, C. (2019). El ciberespacio, nuevos retos y desafíos para fortalecer la Seguridad Nacional. *Revista Científica de la Universidad del Norte*, 34.

P Ejecutivo, P. (mayo de 2013). Ley de Protección de Datos Personales . Lima, Peru.

Rivera, M. (2018). Ciberdefensa y Seguridad Hemisférica. *Revista académica de WHINSEC*, 23.

Delgado, m. (2017). El Ciberterrorismo y sus implicancias en América latina. *Revista Científica de la Universidad Ricardo Palma*, 23.

Flores, J. (2017). Delitos en la Internet y como combatirlos. *Revista Científica de la ESP EPG*, 21.

Gómez, G. (2021). Ciberseguridad y Ciberinteligencia: ¿Por qué son importantes? *Revista de la escuela Superior de Guerra del Ejercito*, 17.

Valerino, E., Yaber, G., & Cenborain, M. (2015). *Metodología de la Investigación Paso a Paso.* México: Trillas.

Republica, C. d. (2019). *Ley de Ciberdefensa.* Lima, Peru: El Peruano.

Ejecutivo, P. (2018). *Decreto Legislativo N° 1412 que aprueba la Ley del Gobierno Digital.* Lima: El Peruano.

ejecutivo, P. (2021). *Reglamento de la Ley de Gobierno Digital .* Lima: El Peruano.

Ejecutivo, P. (2020). *Decreto de Urgencia tiene por objeto crear el Sistema Nacional de Transformación Digital.* Lima: El Peruano.

DITELE. (2019). *Texto Especial sobre el Funcionamiento del Sistema de Telemática del Ejercito .* Lima: DITELE.

Forman, D. (2017). *El Gran libro de la Seguridad Digital.* Madrid, España: Rama Editorial.

Clarke, R., & Knake, R. (2018). *La Guerra Cibernética.* Madrid, España: Giraldo.

Ejecutivo. (2018). *DL 1412 que aprueba la Ley del Gobierno Digital.* Lima: El Peruano.

Ejecutivo. (2021). *Reglamento de la Ley de Gobierno Digital.* Lima: El Peruano.

Ejecutivo. (2021). *DECRETO DE URGENCIA QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL.* Lima: El Peruano.

Dómeles, J. (2018). *Capacitación de las Fuerzas Armadas en ciberseguridad para la seguridad, defensa y desarrollo del Estado Plurinacional de Bolivia.* Universidad del Altiplano, La Paz.

Ejecutivo. (2019). *Ley de Ciberdefensa.* Poder Ejecutivo, Lima.

Safety Culture. (19 de Mayo de 2023). *La ciberseguridad explicada: Una guía sencilla*. Obtenido de Safety Culture: https://safetyculture.com/es/temas/ciberseguridad/#:~:text=Los%20tres%20tipos%20principales%20de,acceso%20inal%C3%A1mbricos%2C%20hosts%20y%20servidores.

Conzultek. (2023). *8 tipos de dispositivos de red y sus características*. Obtenido de Conzultek: https://blog.conzultek.com/dispositivos-de-red-caracteristicas

Docusign. (2022 de Diciembre de 2022). *Conoce los 7 mejores métodos de seguridad informática para tu empresa*. Obtenido de Docusign: https://www.docusign.com/es-mx/blog/seguridad-informatica

Bernabé, R. (12 de Noviembre de 2021). *¿Aún no conoces nuestro Plan de Recuperación de Datos?* Obtenido de R2 Tecnio: https://www.r2tecnio.com/blog/plan-de-recuperacion-de-datos/#:~:text=Un%20plan%20de%20recuperaci%C3%B3n%20de%20datos%20engloba%20todas%20las%20medidas,de%20datos%20o%20sitios%20web.

Etecé. (27 de Agosto de 2020). *Información*. Obtenido de Concepto 1: https://concepto.de/informacion/

Coppola, M. (8 de Mayo de 2023). *Seguridad informática: qué es, tipos y características*. Obtenido de Hub Spot: https://blog.hubspot.es/website/que-es-seguridad-informatica

ANEXOS

ANEXO N° 1

MATRIZ DE CONSISTENCIA

Título: ANALISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGISTICO DEL EJERCITO, 2022

Preguntas de investigación	Objetivos	Teorías	Categorías	Sub categorías	Metodología	Plan de análisis de datos
¿Cuál es la situación actual de ciberseguridad en el Comando Logístico del Ejército (Cologe)? ¿Cuál es el riesgo que genera el uso no adecuado de la información en el Comando logístico del Ejercito (Cologe)? ¿Cuál es el protocolo de ciberseguridad obligatorio para el personal que labora en el Comando logístico del Ejercito (Cologe)?	Describir la situación actual de ciberseguridad en el Comando Logístico del Ejercito (Cologe). Describir el riesgo que genera el uso no adecuado de la información en el Comando logístico del Ejercito (Cologe). Implementar protocolo de ciberseguridad obligatorio para el personal que labora en el Comando logístico del Ejercito (Cologe).	Teoría de la ciber amenaza. Teoría del ciberespacio y la ciberseguridad en el ámbito militar.	Situación actual de ciberseguridad Riesgo que genera el uso no adecuado de la información Factores que influyen en la ciberseguridad	Conocimiento de ciberseguridad. Seguridad de los dispositivos Empleo de sistemas de protección Manejo de otros medios para envió de información Tipo de información que se maneja Vulneración del marco normativo vigente Personal Dispositivos Protección contra ciberataques Planes de recuperación de información	- **Enfoque**: Cualitativo - **Tipo de investigación**: Aplicada - **Método:** Hermeneútico **Informantes:** Personal que labora en Jepae, Singe, Straspe, Sinte, Svetre, etc M**uestra**: 05 personal militar que laboran en el Cologe	**Tecnicas:** Entrevista semi estructurada, Analisis de documentos **Instrumentos** Guia de entrevista, indagacion documental. **Metodo de analisis** Metodo manual/Artesanal, estableciendo elementos con sentido, categorias, macrocategorias y patrones.

ANEXO N° 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Guía de entrevista (1)

Buenos días, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar la presente entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la investigación que lleva por título: "**ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**

Entrevistado:	Emmanuel Julián Cienfuegos Malpartida
Grado Académico:	Magister en Ciencias Militares
DNI:	25846727
Lugar fecha:	15 de marzo de 2023

Categoría 1: Situación actual de ciberseguridad

1. **¿Qué es la ciberseguridad para usted, considera que es importante para el manejo de la información en el Cologe?**

   Bueno, la ciberseguridad es la seguridad hacia los equipos informáticos que debemos tener a la hora que trabajamos con ellos, por ejemplo, una computadora, un celular.
   Si es importante porque te van a robar tus datos, claves de tarjetas de crédito, además debemos saber que actualmente se está viendo los hackers que han surgido del ejército del Perú, donde publican información que tiene que ver con la seguridad nacional, en el Cologe la información que se maneja es sensible, toda la parte logística institucional que de ser obtenida puede ser perjudicial como institución, hay aspectos que solo militares debemos tener.

2. **¿Qué es un ciberataque, conoce que existe personal que diariamente extrae o hurta información sensible de las redes informáticas?**

   Ciberataque es atacar a las computadoras, a través de virus, si exactamente, sí sé que existe personal que se dedica exclusivamente a obtener claves de correos, tarjetas con la finalidad de obtener beneficio económico.

3. **¿Cuál es el tipo de seguridad con que cuenta su PC que utiliza? Considera que es suficiente**

   La clave personal, que dispone, bueno creo que con eso nadie puede ingresar, aparte la seguridad de mi oficina, la llave la tengo yo nada más.

4. **¿Cada que tiempo cambia sus contraseñas de su PC, teléfono móvil, sabe si las computadoras del Cologe son cambiadas de clave permanentemente?**

   En el teléfono, bueno mi última clave la tengo desde hace 1 año, de mi computadora, me releve con esa clave, no soy de los que están cambiando de clave cada rato, es más mi celular antes no tenía clave, el tema es por mis menores hijos para que no accedan se le puso clave, en el Cologe que sepa nadie nos dice que se debe cambiar la clave de la computadora del ejército, uno lo hace por medida de seguridad personal que se toma, pero no creo que alguien cambie de clave permanentemente.

Categoría 2: Riesgo que genera el uso no adecuado de la información

5. **¿Según la información que maneja e intercambia, que cree usted que puede pasar si es hurtada por elementos ajenos a la institución**?

   Claro, ya nos hackearon, no sé cómo obtuvieron esa información, alguien se las dio o talvez a un alumno de la escuela de guerra le robaron los datos de su laptop como siempre ocurre cuando se la mandan a arreglar.

6. **¿Con que frecuencia hace uso del WhatsApp para envío de información a otras dependencias, por qué?**

   Haber, normalmente casi toda la información se comparte por WhatsApp, porque es más rápido y creo que por lo menos es seguro.

7. **¿Tiene conocimiento como actúan los virus informáticos, Troyano, spyware?**

   Bueno, como virus sí, pero el conocimiento que tengo es que ponen lento las computadoras, hay que resetearlos e instalar antivirus

8. **¿Con que frecuencia hace uso del correo institucional para envío de información a otras dependencias?**

   Muy pocas veces, más aún que lo han deshabilitado y restringe el acceso de la computadora personal, creo que es por el tema del hackeo a la institución

9. **¿Conoce el marco normativo vigente respecto a la ciberseguridad, Centro Nacional de Seguridad Digital?**

   Desconozco

Categoría 3: Factores que influyen en la ciberseguridad

10. **¿Ha recibido alguna charla en el presente año, años anteriores con respecto a ciberseguridad, considera que es importante?**

Charla en el Cologe, haber, no nos han dicho nada, y si habláramos de importancia, por supuesto el comando de la institución debe promover esta cultura de ciberseguridad.

11. **¿Dispone de planes de recuperación de información?**

No, que será eso, se guarda en USB en caso de que la computadora se malogre.

Agradecemos su colaboración

Guía de entrevista (2)

Buenos días, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar la presente entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la investigación que lleva por título: "**ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**

Entrevistado: Edwin Gamboa Medina
Grado Académico: Magister en Ciencias Militares
DNI: 40030643
Lugar fecha: 14 de marzo de 2023

Categoría 1: Situación actual de ciberseguridad

1. **¿Qué es la ciberseguridad para usted, considera que es importante para el manejo de la información en el Cologe?**

   Bueno, La **ciberseguridad** es la manera o la forma como se protege los datos para que no puedan ser obtenidos por otras personas ajenas al trabajo y que no tienen relación con la información que manejan, respecto a la información y la importancia en el Cologe, bueno aquí se maneja información a cargo de todos los servicios logísticos a nivel institucional muy importante, respecto a armamento, equipos con lo que se cuenta.

2. **¿Qué es un ciberataque, conoce que existe personal que diariamente extrae o hurta información sensible de las redes informáticas?**

   Un ciberataque, es atacar a las computadoras, celulares o cualquier otro medio electrónico que contenga datos para ser usados maliciosamente, sé que hay gente que se dedica exclusivamente a ese propósito, pero desconozco como lo hacen, se aprecia mucho por los medios de información que extraen información de diferentes instituciones, bancos, lo sacan de WhatsApp, es común ahora ver eso.

3. **¿Cuál es el tipo de seguridad con que cuenta su PC que utiliza? ¿Considera que es suficiente?**

   Suficiente, creo que con la clave ya hay una seguridad, lo único que no está actualizado es el antivirus.

4. **¿Cada que tiempo cambia sus contraseñas de su PC, teléfono móvil, sabe si las computadoras del Cologe son cambiadas de clave permanentemente?**

Ahí, sí que te digo, la computadora que se trabaja en la oficina tiene clave, me releve con esa y solamente una vez la cambie, hace 2 años, en el teléfono, bueno no acostumbro a colocar clave, bueno, no creo, es más a veces se acostumbra a dejar la clave en el escritorio anotado, porque a veces uno necesita ingresar a la maquina cuando alguien está de de permiso, comisión etc.

Categoría 2: riesgo que genera el uso no adecuado de la información

5. **¿Según la información que maneja e intercambia, que cree usted que puede pasar si es hurtada por elementos ajenos a la institución**?

   Claro, ya nos hackearon, no sé cómo obtuvieron esa información, alguien se las dio o talvez a un alumno de la escuela de guerra le robaron los datos de su laptop como siempre ocurre cuando se la mandan a arreglar.

6. **¿Con que frecuencia hace uso del WhatsApp para envío de información a otras dependencias, por qué?**

   Casi diario, información de todo tipo, excepto planes, pero las directivas, disposiciones oficios, radiogramas, se hacen utilizando este medio, en el caso del Cologe tenemos un grupo de control patrimonial donde están todos a nivel nacional.

7. **¿Tiene conocimiento como actúan los virus informáticos, Troyano, spyware?**

   Conocimiento, haber, a las maquinas hay que instalarlos antivirus, para evitar que ingresen y se apaguen constantemente, los nombres, recién los escucho, la verdad no he indagado respecto a este tema, que actualmente es muy importante por todo lo que se realiza actualmente, todo por computadoras.

8. **¿Con que frecuencia hace uso del correo institucional para envío de información a otras dependencias?**

   Sinceramente, casi nada, excepto cuando envías información al Ministerio de Defensa, ellos si te envían al correo institucional, jamás al personal, ni mucho menos por WhatsApp, bueno las coordinaciones que hago con la dirección de control patrimonial es así, correo institucional, pero internamente, no, hasta por WhatsApp se envía oficios y otro tipo de documentos.

9. **¿Conoce el marco normativo vigente respecto a la ciberseguridad, Centro Nacional de Seguridad Digital?**

   Se que existe una ley de ciberseguridad y ciberdefensa, pero sinceramente, desconozco el alcance.

Categoría 3: Factores que influyen en la ciberseguridad

10. ¿Ha recibido alguna charla en el presente año, años anteriores con respecto a ciberseguridad por parte de algún oficial en el Cologe?

Este es mi tercer año aquí en el Cologe, nunca nadie nos dio una charla respecto a ese tema.

11. ¿Dispone de planes de recuperación de información?

Planes, no, solo guardo mis archivos en mi memoria externa que es de mi propiedad para que en un momento cuando se malogre la maquina tenga archivado y no tener que buscar mi información que realice.

Guía de entrevista (3)

Buenos días, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar la presente entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la investigación que lleva por título: "**ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**

Entrevistado: Dany Hernán Maquera Vizcarra
Grado Académico: Magister en Ciencias Militares
DNI: 40071362
Lugar fecha: 22 de marzo de 2023

Categoría 1: situación actual de ciberseguridad

1. **¿Qué es la ciberseguridad para usted, considera que es importante para el manejo de la información en el Cologe?**

   La ciberseguridad consiste en la seguridad que debemos dar a las informaciones para evitar que intrusos informáticos se apoderen de ella, para ello es importante disponer de elementos que constantemente estén concientizando al personal a realizar esta tarea, mira con respecto al Cologe, tiene a su cargo los servicios logísticos y la Jepae, ellos se conectan con todo el Perú a través del Siscobam, en realidad hay mucha información que debería estar con ciertos parámetros de seguridad debido que representa clasificada, por ello la ciberseguridad en el Cologe es muy importante así como en cualquier dependencia del ejército.

2. **¿Qué es un ciberataque, conoce que existe personal que diariamente extrae o hurta información sensible de las redes informáticas?**

   Es aquel que se realiza con la finalidad de hurtar la información o dañar los sistemas informáticos, claro, es fácil darse cuenta a través de los medios televisivos, el internet de como ingresan a páginas de reconocidas empresas o de bancos para robar información que posteriormente puede ser usada en la contra de las personas, de igual forma del celular, te pueden sacar los datos.

3. **¿Cuál es el tipo de seguridad con que cuenta su PC que utiliza? ¿Considera que es suficiente?**

   Haber, la computadora que uso en el trabajo es propia, en la oficina se dispone de solamente una computadora, esa PC tiene su clave de seguridad, bueno por lo menos

tiene clave, además de antivirus que se encuentra desactualizada, eso sí se pondría a pensar que a través de él puedan acceder a robar tu información.

4. **¿Cada que tiempo cambia sus contraseñas de su PC, teléfono móvil, sabe si las computadoras del Cologe son cambiadas de clave permanentemente?**

   Lo común es que las computadoras del Cologe cada relevo que ingresa y se le asigna la computadora, haga el cambio de contraseña, con respecto a mi maquina portátil, solo una vez cambie de clave, pero es mía, solo yo la uso, eso es lo único que podría corroborar con respecto a procedimientos, plazos para cambiar contraseñas.

Categoría 2: riesgo que genera el uso no adecuado de la información

5. **¿Según la información que maneja e intercambia, que cree usted que puede pasar si es hurtada por elementos ajenos a la institución**?

   Haber, en mi departamento la información a mi parecer no es tan sensible pues solo ve el tema de personal, efectivos y procedimientos de personal, solo una pequeña base de datos sonde se coloca información de los oficiales y Tcos y Suboficiales, sin embargo, por ejemplo en contrataciones, allí si hay mucha responsabilidad, la parte logística creo que es la más sensible a través d los servicios logísticos, lo de hurtar la información claro, existe el espionaje, que consiste en llevar información de un país a otro.

6. **¿Con que frecuencia hace uso del WhatsApp para envío de información a otras dependencias, por qué?**

   Para ser honesto, casi todo el tiempo, es común que se imparta información por ese medio, incluso existen diferentes grupos en las dependencias que lo hace con la finalidad de intercambiar información, porque es más fácil de enviar, sin embargo, no se debería, por medida de seguridad.

7. **¿Tiene conocimiento como actúan los virus informáticos, Troyano, spyware?**

   Se que son virus, actúan bloqueando la computadora, lo hace más lenta para dificultar el trabajo y en algunos casos malogra de inmediato el disco duro.

8. **¿Con que frecuencia hace uso del correo institucional para envío de información a otras dependencias?**

   Correo institucional Chaqui, muy poco, la información institucional como por ejemplo cuadros básicos allí si se utiliza bastante este medio, pero en el trabajo, muy poco se usa este correo, como ya te dije anteriormente parece ser que el WhatsApp ha desplazado a correos personales, institucionales.

9. **¿Conoce el marco normativo vigente respecto a la ciberseguridad, Centro Nacional de Seguridad Digital?**

   Desconozco.

Categoría 3: Factores que influyen en la ciberseguridad

10. **¿Ha recibido alguna charla en el presente año, años anteriores con respecto a ciberseguridad por parte de algún oficial en el Cologe, cree que es importante?**

    Charlas con respecto a ciberseguridad, ninguno, sin embargo, se debería dar porque es un tema nuevo que ya todos debemos manejar para proteger la información que se dispone.

11. **¿Dispone de planes de recuperación de información?**

    Planes como tal, los guardo en USB de mi propiedad.

Guía de entrevista (4)

Buenos días, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar la presente entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la investigación que lleva por título: "**ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**

Entrevistado:	Luis Pedro Sotelo Figueroa
Grado Académico:	Magister en Ciencias Militares
DNI:	43337350
Lugar fecha:	17 de marzo de 2023

Categoría 1: situación actual de ciberseguridad

1. **¿Qué es la ciberseguridad para usted, considera que es importante para el manejo de la información en el Cologe?**

   La ciberseguridad son los procedimientos, las maneras de cómo vamos a través de medidas de seguridad en las computadoras cuidar la información que allí se encuentra, ahora que es común los hackers que se puede apreciar en distintos medios de comunicación acerca de cómo ingresan a las páginas institucionales, bloqueándolas y hurtando la información para después difundirla, se debe tener un especial cuidado con la información que maneja el Cologe, debido que abarca procesos que se articulan con la Oficina Económica del Ejercito, y a nivel nacional, por lo tanto se debe tener particular cuidado con esta dependencia.

2. **¿Qué es un ciberataque, conoce que existe personal que diariamente extrae o hurta información sensible de las redes informáticas?**

   Claro, tienen dedicación exclusiva a realizar este tipo de actividades ilícitas, el ciberataque puede provenir desde distintas partes, pero para ello hay que adoptarlas medidas de seguridad adecuadas para contrarrestarlos, en ese sentido, entra a tallar el conocimiento del personal que labora en la dependencia primero para que generar conciencia respecto a este tipo de procedimientos que podría poner en riesgo la información que se maneja.

3. **¿Cuál es el tipo de seguridad con que cuenta su PC que utiliza? ¿Considera que es suficiente?**

   Tipo de seguridad, bueno contraseña, la mía tiene antivirus original, pero la del Cologe tiene el antivirus vencido y actualmente casi segundo semestre no creo que compren,

tiene sus contraseñas, pero es la misa desde hace 8 meses que llegue a labora y han rotado casi 3 personas en el puesto, sencillamente no tenemos una buena cultura de seguridad con las informaciones.

4. **¿Cada que tiempo cambia sus contraseñas de su PC, teléfono móvil, sabe si las computadoras del Cologe son cambiadas de clave permanentemente?**

   La de mi PC personal, cada 8 meses o cuando veo que quizás alguien puede tener la clave, lo de mi celular, cada 5 meses o cuando cambio de equipo, el caso del Cologe la verdad hace mucho tiempo paso una situación, un técnico que trabaja como auxiliar de contrataciones lo llamaban para que saquen una información, se lo estaban pidiendo al jefe del departamento, su computadora estaba con clave, se terminó el día y el Tco no respondió, todos amargos con respecto a la información que estaba pidiendo el escalón superior y no se dio respuesta, a partir de allí, ordenaron que las claves de las computadoras sean dejadas al costado del escritorio, por si alguien tiene que sacar una información y se necesita, para mí eso está mal, quizás porque uno es responsable de la PC que maneja y la información que en ella se encuentra, pero bueno ordenes son órdenes.

Categoría 2: riesgo que genera el uso no adecuado de la información

5. **¿Según la información que maneja e intercambia, que cree usted que puede pasar si es hurtada por elementos ajenos a la institución**?

   Que puede pasar, primero puede salir publicada en diarios de comunicación, así como sucedió con las exposiciones los planes que fueron filtradas hace poco respecto Al VRAEM, además es mediático, que al Ejército del Perú le hackeen y salga información no solo institucional, si no también personal de los Oficiales y Tcos SSOO.

6. **¿Con que frecuencia hace uso del WhatsApp para envío de información a otras dependencias, por qué?**

   Yo lo uso diario, es común ver este tipo de enlace para trasmitir y recibir información.

7. **¿Tiene conocimiento como actúan los virus informáticos, Troyano, spyware?**

   Bueno, bloquean las computadoras, lo inactivan, en algunos casos dañan el sistema operativo.

8. **¿Con que frecuencia hace uso del correo institucional para envío de información a otras dependencias?**

   Con poca frecuencia, a veces enviamos el correo Olaya para envío de fax, pero el resto

de información muy poco.

9. **¿Conoce el marco normativo vigente respecto a la ciberseguridad, Centro Nacional de Seguridad Digital?**

   Se que existe una ley de ciberseguridad pero que muy poco se conoce en las dependencias, mucho menos en el ejército, es algo que muy poca importancia le estamos dando institucionalmente.

Categoría 3: Factores que influyen en la ciberseguridad

10. **¿Ha recibido alguna charla en el presente año, años anteriores con respecto a ciberseguridad por parte de algún oficial en el Cologe, cree que es importante?**

    En el presente año, ninguna, ya dije antes, la institución muy poca importancia le da a este tema, es algo que debemos promover actualmente, la ciberseguridad es un aspecto que debe ser manejado como prioridad institucional, todos los países actualmente están invirtiendo bastante en este tema, esperemos que el ejército del Perú comience a ver esto como un tema álgido.

11. **¿Dispone de planes de recuperación de información?**

    No se dispone.

Guía de entrevista (5)

Buenos días, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar la presente entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la investigación que lleva por título: "**ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022"**

Entrevistado: Omar Lozada Santillán
Grado Académico: Magister en Ciencias Militares
DNI: 43451123
Lugar fecha: 10 de marzo de 2023

Categoría 1: situación actual de ciberseguridad

1. **¿Qué es la ciberseguridad para usted, considera que es importante para el manejo de la información en el Cologe?**
   La ciberseguridad consiste en el cuidado de la información por parte de las personas para evitar que sea obtenida por otras con fines nocivos, como robo de información personal, chantaje, retiro de dinero etc., eso es lo que entiendo de este concepto nuevo y muy poco difundido en las dependencias institucionales, respecto a la información del Cologe, como dependencia maneja la parte logística institucional, se interconecta a través del módulo Siscobam a nivel nacional, allí se ven actividades de todo tipo, aspectos económicos, cargos, es por ello que tiene mucha importancia la información que esta maneja en coordinación con otras dependencias.
   Cologe es muy importante, así como en cualquier dependencia del Ejército.

2. **¿Qué es un ciberataque, conoce que existe personal que diariamente extrae o hurta información sensible de las redes informáticas?**
   Un ciberataque, es aquel que es realizado para causar daño en las redes informáticas, sé que existen los llamados piratas informáticos, que constantemente están queriendo sacar información de las cuentas de bancos, tarjetas de crédito, asimismo, el hackeo a las páginas institucionales, recientemente podemos apreciar como el denominado Guacamaya hackeo información del ejército, sobre todo conversaciones del planeamiento de la operación patriota en el VRAEM.

3. **¿Cuál es el tipo de seguridad con que cuenta su PC que utiliza? ¿Considera que es suficiente?**

   Cuenta con contraseña, por lo menos nadie puede ingresar si no la tiene, ah y antivirus si se encuentra desactualizado.

4. **¿Cada que tiempo cambia sus contraseñas de su PC, teléfono móvil, sabe si las computadoras del Cologe son cambiadas de clave permanentemente?**

   En ese aspecto si no incido mucho, mi laptop tiene 1 año, desde allí siempre ha tenido la misma contraseña, pero solamente el uso yo, por algo es personal, las del Cologe, por ejemplo, en el departamento administrativo todas tienen contraseña, lo del cambio constante sino tengo mucha idea cada que tiempo se hace eso por parte del usuario.

Categoría 2: riesgo que genera el uso no adecuado de la información

5. **¿Según la información que maneja e intercambia, que cree usted que puede pasar si es hurtada por elementos ajenos a la institución**?

   Claro, puede salir hasta por parte de nosotros, quien controla si alguien se puede llevar en su USB a información y después usarla en contra, tendríamos que tener un control de acceso a la información, para poder saber si la información no sale de uno de nosotros, además si alguien quisiera obtener la información del Cologe, de que les puede servir, sin embargo, a otros países quizás si les pueda interesar esos datos.

6. **¿Con que frecuencia hace uso del WhatsApp para envío de información a otras dependencias, por qué?**

   Casi a diario, se ha convertido en el principal medio de comunicación que yo sepa para enviar información de todo tipo, puedes apreciar los denominados grupos donde se esa enviando información como directivas, fax, etc., en el Cologe existe el grupo de WhatsApp llamado control patrimonial, que si bien es cierto deben ser espacios de intercambiar información e ideas, pero por acá se envía de todo.

7. **¿Tiene conocimiento como actúan los virus informáticos, Troyano, spyware?**

   Bueno, no al detalle, pero malogran los equipos sean estas computadoras, tables, celulares etc.

8. **¿Con que frecuencia hace uso del correo institucional para envío de información a otras dependencias?**

Muy poco lo utilizo, solamente cuando alguna dependencia lo solicita que se envié por correo institucional.

9. **¿Conoce el marco normativo vigente respecto a la ciberseguridad, Centro Nacional de Seguridad Digital?**
   Desconozco.

Categoría 3: Factores que influyen en la ciberseguridad

10. **¿Ha recibido alguna charla en el presente año, años anteriores con respecto a ciberseguridad por parte de algún oficial en el Cologe, cree que es importante?**
    Charlas con respecto a ciberseguridad, ninguno, sin embargo, se debería dar porque es un tema nuevo que ya todos debemos manejar para proteger la información que se dispone.

11. **¿Dispone de planes de recuperación de información?**
    Planes como tal, no solamente en mi caso guardo la información y mi disco externo.

Documentos para análisis documental

N°	Documento	Observación
1	Ley N° 303999 “Ley de ciberdefensa”	
2	DL 1412 que aprueba la Ley del Gobierno Digital	
3	Decreto Supremo N° 029 -2021 Reglamento de la Ley de Gobierno Digital	
4	Decreto de Urgencia N° 006-2020 Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital	
5	Texto Especial sobre el Funcionamiento del Sistema de Telemática del Ejercito	
6	El Gran libro de la Seguridad Digital	
7	La Guerra Cibernética (texto)	
8	Centro de Conocimiento Digital implementado por la Secretaría de Gobierno y Transformación Digital	
9	Documentos de la La Secretaría de Gobierno Digital (SEGDI)	
10	Otros	

ANEXO N° 3

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Experto Informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
Henry Valentín Mendoza Lopez	Ejército del Perú	ENTREVISTA	Aníbal Mercado Cortez

Título de la Investigación: "Análisis de la ciberseguridad como Prioridad Institucional en el Comando Logístico del Ejército, 2022"

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%	REGULAR 21-40%	BUENO 41-60%	MUY BUENO 61-80%	EXCELENTE 81-100%	
1. CLARIDAD	Esta formulado con lenguaje apropiado						92
2. OBJETIVO	Está expresado en Capacidades observables						94
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de los observables de investigación						93
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento						94
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a los observables de investigación						93
6. INTENCIONALIDAD	Adecuado para valorar aspectos de los observables de investigación						92
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento						94
8. COHERENCIA	Existe coherencia entre las categorías y sub categorías planteadas.						93
9. METODOLOGÍA	La estrategia responde al propósito de la investigación						92
10. PERTINENCIA	La investigación es aplicable						91

II. OPINIÓN DE APLICACIÓN:

.....

III. PROMEDIO DE VALORACIÓN: 92.80

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELÉFONO
Tacna, 25/04/23	10031381		981687461

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Experto Informante	Cargo o Institución donde labora	Nombre del Instrumento	Autor del Instrumento
Alex Kike Bautista Mostacero	Ejército del Perú	ENTREVISTA	Aníbal Mercado Cortez

Título de la Investigación: "Análisis de la Ciberseguridad como prioridad Institucional en el Comando Logístico del Ejército 2022"

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%	REGULAR 21-40%	BUENO 41-60%	MUY BUENO 61-80%	EXCELENTE 81-100%
1. CLARIDAD	Esta formulado con lenguaje apropiado					94
2. OBJETIVO	Está expresado en Capacidades observables					93
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de los observables de investigación					94
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento					93
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a los observables de investigación					94
6. INTENCIONALIDAD	Adecuado para valorar aspectos de los observables de investigación					94
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento					93
8. COHERENCIA	Existe coherencia entre las categorías y sub categorías planteadas.					93
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					94
10. PERTINENCIA	La investigación es aplicable					93

II. OPINIÓN DE APLICACIÓN:

.....

III. PROMEDIO DE VALORACIÓN: 93.50

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELÉFONO
Pto Maldonado 01/04/23	43676725		968417 22

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Experto Informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
Richard Trebejo Rondinel	Ejército Perú	ENTREVISTA	Aníbal Mercado Cortez

Título de la Investigación: Análisis de la Ciberseguridad como prioridad Institucional en el Comando Logístico del Ejército, 2022

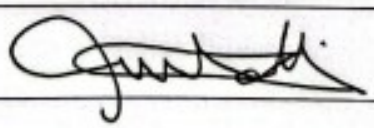
I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE 00-20%	REGULAR 21-40%	BUENO 41-60%	MUY BUENO 61-80%	EXCELENTE 81-100%
1. CLARIDAD	Esta formulado con lenguaje apropiado					94
2. OBJETIVO	Está expresado en Capacidades observables					95
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de los observables de investigación					95
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento					95
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a los observables de investigación					94
6. INTENCIONALIDAD	Adecuado para valorar aspectos de los observables de investigación					93
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento					94
8. COHERENCIA	Existe coherencia entre las categorías y sub categorías planteadas.					95
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					94
10. PERTINENCIA	La investigación es aplicable					93

II. OPINIÓN DE APLICACIÓN:

.....

III. PROMEDIO DE VALORACIÓN: 94.20

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELÉFONO
Lima, 19-04-23	10671195		936458303

ANEXO N° 4

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

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

"Año del Fortalecimiento de la Soberanía Nacional"

Chorrillos, 05 de junio de 2022

Oficio N° 726 /U-8.g.l/27.00

Señor **Gral de División Comandante General del Cologe – San Borja**

Asunto: Solicita brindar facilidades a personal que se indica

Ref. : a. Reglamento para la obtención del grado académico de Maestro en Ciencias Militares

b. Reglamento de Investigaciones de la ESGE -EPG

Tengo el honor de dirigirme a usted., en relación a los documentos de la referencia para solicitarle se digne brindar las facilidades para el levantamiento de datos e información al Sr. Teniente Coronel, estudiante de esta casa de estudios integrante de la V Maestría en Ciencias Militares, que realizará la investigación titulada "**Análisis de la Ciberseguridad como Prioridad Institucional en el Comando Logístico del Ejercito, 2022**"

La investigación está siendo realizada por:

- TTE CRL ING MERCADO CORTEZ ANIBAL WILLIBRORD

Es propicia la oportunidad para expresarle los sentimientos de mi especial consideración y estima personal.

Dios guarde a Ud.

DISTRIBUCIÓN.

- Cologe……..……...01
- Archivo ……..…01 /02

ESCUELA SUPERIOR DE GUERRA DEL EJERCITO
ESCUELA DE POST GRADO
DIRECCION

L
Direc

ANEXO 5

COMPROMISO ÉTICO

DECLARACIÓN DE COMPROMISO ÉTICO

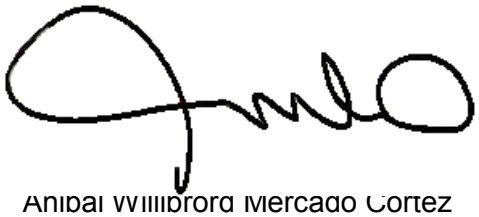
El presente trabajo de investigacion titulado: "**Análisis de la Ciberseguridad como Prioridad Institucional en el Comando Logístico del Ejercito, 2022"**

Se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para la investigación en Ciencias Militares promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra-Escuela de Posgrado.

En vista de lo anterior:

Yo, Bach Anibal Willibrord Mercado Cortez, estudiante egresado de la V Maestría en Ciencias Militares con mencion en Planeamiento estrategico y Toma de decisiones de la Escuela Superior de Guerra del Ejercito – Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado la investigacion siguiendo las instrucciones brindadas por el Departamento de Gestion de la Investigacion desde la elaboracion del marco referencial y recoleccion de la informacion, hasta el analisis de datos y elaboracion del informe final.

En tal sentido la informacioncontenida en el presente documento es producto de mio rabajo personal, apegandome a la legislacion sobre propiedad intelectual, sin haber incurrido en falsificacion de la informacion o cualquier tipo de fraude, por lo cual me someto al marco legal y normativo vigente relacionado a dicha responsabilidad, asi como a las medidas disciplinarias establecidas en la ESGE-EPG.



Anibal Willibrord Mercado Cortez

DNI: 40409512

ANEXO 6

HOJA DE DATOS PERSONALES

GRADO	:	**Teniente Coronel de Ingeniería**
NOMBRES	:	**Anibal Willibrord**
APELLIDOS	:	**Mercado Cortez**
EMAIL	:	**anibalmercadoc@gmail.com**
DIRECCIÓN	:	**Calle coronel Ayllón 169, Villa Militar Oeste, Chorrillos**
CELULAR	:	**988031847**
FIRMA		

ANEXO 7

APORTE A LA INVESTIGACIÓN

PRESENTACIÓN

El presente aporte doctrinario tiene como finalidad establecer procedimientos que se debe seguir desde el nivel usuario que constituye la base para un buen sistema de ciberseguridad que debe desarrollarse en el Comando Logístico del Ejército, el mismo que tiene la responsabilidad de desarrollar articulado con otras dependencias los procedimientos logísticos institucionales.

El Comando Logístico del Ejército (Cologe) constituye la dependencia encargada de llevar a cabo el proceso logístico institucional tanto para operaciones como acciones militares, este se articula con otras dependencias en la institución que en su conjunto llevan el flujo de la corriente logística a nivel nacional y a todas sus dependencias, en tal sentido la información que maneja es álgida pues constituyen aspectos de cargos, operatividad, año de fabricación etc., que llevan a proporcionar particular atención en la ciberseguridad que debe tener para proteger el cúmulo de datos que maneja.

En ese sentido, después de haber realizado el análisis correspondiente se llegó a las siguientes conclusiones: La situación actual de ciberseguridad por parte del Cologe es deficiente o nula, el personal desconoce lo que es ciberseguridad, procedimientos mínimos de seguridad como son las contraseñas que deben ser cambiadas cada cierto tiempo, la seguridad externa e interna mediante firewalls que protejan la información que manejan diariamente y comparten con otras dependencias, además de emplear el aplicativo de WhatsApp para intercambiar información a nivel nacional, contraviniendo lo descrito por la Directiva Única de Funcionamiento y Sistema Telemática del Ejército (Dufsitele) respecto a la trasmisión de información en la institución.

Capítulo 1:
Aspectos referentes a la tesis

1.1 Título de la tesis

Análisis de la ciberseguridad como prioridad institucional en el Comando Logístico del Ejército, 2022

1.2 Objetivos de la tesis

- Describir la situación actual del nivel de ciberseguridad en el Comando Logístico del Ejército (Cologe).

- Describir los factores que inciden en el nivel de ciberseguridad en el Cologe con respecto a la información que maneja.

- Implementar un protocolo de ciberseguridad de aplicación obligatoria por todo el personal que labora en el Cologe.

1.3 Conclusiones de la tesis

Respecto al objetivo N° 1: Describir la situación actual de ciberseguridad en el Cologe.

- La situación actual de ciberseguridad por parte del Cologe es deficiente o nula, el personal que labora en esta dependencia en su mayoría desconoce lo que es ciberseguridad, tiene un conocimiento vago de cuál es el procedimiento de cómo actúan los hackers y cuáles son las medidas de protección que debe darse a la información.

- Se desconocen procedimientos mínimos de seguridad como son las contraseñas que deben ser cambiadas cada cierto tiempo, la seguridad externa e interna mediante firewalls que protejan la información que manejan diariamente y la comparten con otras dependencias.

- Se emplea el aplicativo de WhatsApp ara intercambiar información a nivel nacional, se han creado grupos donde diariamente se realiza este procedimiento, contraviniendo lo descrito por la Dufsitele respecto a la trasmisión de información en la institución.

- La Ditele encargada de promover la ciberseguridad en la institución no ha emitido boletines, folletos, charlas que concienticen al personal del Cologe respecto a la seguridad de las informaciones.

Respecto al objetivo N° 2: Describir los factores que inciden en el nivel de ciberseguridad en el Cologe con respecto a la información que maneja.

- El desconocimiento de medidas de seguridad mínimas que parte desde el usuario, el desconocimiento de las normas y procedimientos de la Dufsitele que regula el empleo de los equipos informáticos, esto genera que el Cologe este expuesto al hurto de la información que maneja respecto a los cargos de armamento, vehículos, tipo de munición que se dispone, sean filtradas a través de personas ajenas a la institución y sean llevadas a medios de comunicación, u obtenidas por otros países para cualquier tipo de uso.

- No se dispone de un buen sistema de ciberseguridad, esto puede ser aprovechado por hackers y logren obtener información del personal (contraseñas de cuentas, bienes, direcciones) a través del Phishing, que consiste en engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito, para luego ser chantajeadas.

Respecto al objetivo N° 3: Implementar y describir un protocolo de ciberseguridad de aplicación obligatoria por todo el personal que labora en el Cologe.

- En el aporte doctrinario se ha propuesto mediante afiches, lemas, que el personal militar que labora en el Cologe tome conciencia de la ciberseguridad en esta época, además de establecer un protocolo simple de uso práctico para el personal antes de empezar las labores con sus equipos informáticos diariamente.

Capítulo 2:
Aspectos referentes al aporte doctrinario

2.1 Aporte doctrinario

Guía de Procedimientos para desarrollar una cultura de ciberseguridad en el Cologe.

a. Objetivo

Reducir los riesgos generales de ciberseguridad mediante el fortalecimiento de los eslabones más débiles de la organización y su recurso más preciado: la gente.

b. Finalidad

Disminuir riesgos y detectar posibles problemas y amenazas de seguridad de las informaciones, a fin de garantizar el uso adecuado de los recursos y sistemas del Cologe.

c. Metas

1) El personal que labora en el Cologe sean conscientes del impacto de un incidente de ciberseguridad y conozcan las medidas simples para evitarlos.

2) Sea un punto de partida de un proceso continuo que debe seguir el Cologe con la finalidad de desarrollar estrategias e implementación de medidas de seguridad de la información.

3) Aprobación y difusión de las medidas básicas de seguridad a través de afiches y aplicativos.

d. Justificación

Aplicación de medidas básicas de seguridad a la información a través de la concientización a los usuarios, además, los resultados se pueden generalizar a otras dependencias, permitirá además que el personal se concientice con el riesgo y manejo de la información que maneja la institución y lo que pudiera suceder si fuera hackeada.

2.2 Lugar

Comando Logístico del Ejército (Cologe).

2.3 Tiempo

Desde su elaboración, hasta la impresión y difusión, aproximadamente 15 días.

2.4 Población objetivo

Aproximadamente 500 personas militares y civiles.

2.5 Identificación de necesidades

Tabla 1

Identificación de necesidades

Situación por mejorar	Causas que motivan el mejoramiento	Acciones	Priorización de las acciones para el año 2023
Cultura de ciberseguridad	La necesidad de proteger la información que se maneja	Elaboración de guía práctica de ciberseguridad.	Confeccionar los afiches correspondientes.

2.6 Programa de actividades

Tabla 2

Programa de actividades

Actividades	Participantes	Recursos y materiales
Confección de la Guía de medidas básicas de seguridad de la información.	Oficiales graduados del curso superior de Tecnología de la Información y comunicación.	Papel A3 plastificado

Capítulo 3:
Guía de buenas prácticas en seguridad de la información

3.1 Seguridad de la información en la PC

El concepto de la seguridad informática comienza desde nuestro PC y se enfoca en la protección de su infraestructura computacional, especialmente la información contenida en una computadora o a través de redes de computador.

La seguridad a nivel local es lo primero que debemos cuidar. Un 90% de los ataques se dan por el empleo de contraseñas poco seguras, o el uso repetido de estas. Es conveniente cambiarlas cada 15 días, o por lo menos una vez al mes. Además, se garantiza la seguridad de nuestra PC manteniendo actualizado el antivirus, así como el empleo de una red wifi segura.

3.2 Hackeo de contraseñas

Existen diferentes sistemas para recuperar contraseñas, "John the Ripper", es una de las herramientas que más se utilizan para este fin, consiste en un ataque a las contraseñas por medio de un programa que combina palabras que están en un diccionario hasta que las descubre (normalmente un archivo de texto). Es decir, exploran combinaciones con el fin de hallar la contraseña. Pero en estos diccionarios no están todas las posibles claves, por lo tanto, lo adecuado es colocar palabras que no estén en los diccionarios, por ejemplo, una contraseña que no signifique nada, sin sentido, con caracteres, así como ^ y ~, y lo suficientemente larga.

Sin embargo, hay otras estrategias que suelen usar los hackers informáticos y que conviene tener presente a fin de evitar en todo momento que puedan romper nuestra clave y poder acceder a nuestra información:

a. Phishing

Es uno de los métodos más comunes que se utilizan para acceder a nuestra información. Básicamente se trata de un cebo que envía el atacante por intermed0io de un SMS o correo electrónico, básicamente, con el objetivo de que caigamos en una trampa. Por ejemplo, puede aparecer un enlace para solucionar un problema en el servicio que usamos o que descarguemos algo.

El problema es que realmente estaremos enviando datos a un servidor controlado por los atacantes. Se trata de un **enlace falso** que nos dirige a una página web que es una copia del original. Este método es un clásico para el robo de claves de todo tipo, como pueden ser redes sociales, cuentas bancarias, etc.

b. Keylogger

Los hackers también pueden utilizar un tipo de malware (programa maligno) que se conoce como keylogger. Lo que hace es registrar todas las **pulsaciones de teclas** que hacemos en el ordenador o móvil. De esta forma pueden registrar también todas las contraseñas que ponemos y de esta forma robarla junto al nombre de usuario y otra información que pongamos.

Normalmente este tipo de software malicioso llega a través de un archivo adjunto que envían por correo, en la descarga de una página web fraudulenta o cualquier aplicación que instalamos y resulta ser una amenaza. Los ciberdelincuentes tienen múltiples opciones en este sentido para robar las claves con un keylogger.

c. Vulnerabilidad en el servicio

Existe el riesgo de que haya alguna **vulnerabilidad** en el servicio que utilicemos. Por ejemplo, en una red social como Facebook o Twitter, podría haber un problema de seguridad que permita a los atacantes explotarlo y llegar a las contraseñas almacenadas.

Esto no va a depender del usuario, sino del servicio. No es habitual, por suerte, existen ataques a gran escala en los que se ha filtrado información importante y esto incluye también las contraseñas. Por eso siempre que haya alguna filtración de este tipo conviene cambiar la clave lo antes posible. Es recomendable cambiarlas de cada cierto periodo y así aumentar la seguridad.

Dependiendo de todo lo anterior mencionado, el tiempo que demora un hacker en descubrir una contraseña estará en función de la cantidad de caracteres que contenga y de la combinación de letras (minúsculas y mayúsculas), números y símbolos. (Figura 1).

3.3 Servicios vulnerables a ser atacados

Los servicios en línea son constantemente blanco de ataques cibernéticos destinados a robar contraseñas y acceder a cuentas de usuarios. Estos ataques se dirigen a plataformas populares y servicios ampliamente utilizados, donde los piratas informáticos esperan obtener información valiosa.

a. **Correo electrónico:** Los servicios de correo electrónico son objetivos frecuentes para los hackers, ya que permiten acceder a una gran cantidad de información personal y cuentas vinculadas.

b. **Redes sociales:** Las plataformas de redes sociales son muy populares y almacenan una gran cantidad de información personal. Los hackers a menudo buscan acceder a estas cuentas para difundir malware, robar información confidencial y aprovecharse de la identidad de la víctima.

c. **Banca en línea:** Los servicios bancarios en línea son atractivos para los piratas informáticos debido a la cantidad de información financiera confidencial que pueden obtener.

d. **Plataformas de comercio electrónico:** Los sitios web de comercio electrónico son otro objetivo para robar contraseñas, ya que implican transacciones financieras y almacenan datos de tarjetas de crédito.

e. **Servicios de almacenamiento en la nube:** Los servicios de almacenamiento en la nube son populares para almacenar y compartir archivos, lo que los convierte en objetivos atractivos para los piratas informáticos.

f. **Plataformas de juegos en línea:** Los servicios de juegos en línea son cada vez más populares y atraen a una gran cantidad de usuarios. Los piratas informáticos pueden apuntar a estas cuentas para robar credenciales de inicio de sesión, robar artículos virtuales valiosos o utilizar cuentas comprometidas para actividades maliciosas en el juego.

Figura 1

Tiempo que tarda un hacker en descifrar tu contraseña.

Número de caracteres	Solo números	Minúsculas	Mayúsculas y minúsculas	Números, mayúsculas y minúsculas	Números, mayúsculas, minúsculas y símbolos
4	instantáneamente	instantáneamente	instantáneamente	instantáneamente	instantáneamente
6	instantáneamente	instantáneamente	instantáneamente	1 segundo	5 segundos
8	instantáneamente	5 segundos	22 minutos	1 hora	8 horas
10	instantáneamente	58 minutos	1 mes	7 meses	5 años
12	25 segundos	3 semanas	300 años	2,000 años	34,000 años
14	41 minutos	51 años	800,000 años	9,000,000 años	200M años
16	2 días	34,00 años	2MM años	37MM años	1 Billon de años
18	9 meses	23,000,000 años	6 Billones de años	100 Billones de años	7 Trillones de años

3.4 Empleo de contraseñas simples y repetidas

"Las contraseñas que utilizamos en internet suelen ser breves, simples y fáciles de descifrar. No por falta de esfuerzo al pensarlas, al menos no en todos los casos, sino porque tendemos a usar palabras, números y combinaciones de ambos con símbolos que siguen patrones comunes al razonamiento de buena parte de los seres humanos."

Esta investigación, para la que se ha utilizado una muestra de 10 millones de contraseñas ideadas por personas, revela que la combinación más común para proteger cuentas de cualquier plataforma de internet es "123456", la segunda la palabra inglesa "password" (o "contraseña" en el caso de Hispanoamérica), la tercera "12345678", la cuarta "qwerty", y así hasta 50 composiciones.

Figura 2

Las 50 contraseñas más usadas.

Aunque resulte difícil de creer, el “123456” o el “111111” se siguen empleando como parte de las contraseñas que usamos en el Ejército, lo que permite descifrarlas casi instantáneamente. Se debe elegir algo complejo y evitar utilizar información personal, como su nombre, edad, fecha de nacimiento, nombres de hijos, nombres de mascotas, color o canción favorita, ya que estos datos son más fáciles de adivinar y/o hackear.

Además, hoy en día, deberíamos tener pleno conocimiento que las contraseñas jamás deberían repetirse, en especial para cuentas de correo electrónico, banca electrónica, redes sociales, y sobre todo para aquellos usuarios que manejan información sensible en sus PC, ya que esto podría significar el robo de identidad. Sin embargo, más de un 80 % aún lo continuamos haciendo.

Ejemplo: Existen personas cuya contraseña para el desbloqueo de su PC, es la misma que utilizan para su correo, APP de banca móvil, Facebook, Instagram, Netflix, etc.

3.5 Preguntas de seguridad para recuperar contraseñas

Cuando una persona no recuerda la contraseña que empleó, normalmente hace clic en “Olvidé mi contraseña”, usualmente se suele solicitar que responda una o más preguntas. Se debe evitar las respuestas que usen nombres de familiares, mascotas o algo relacionado a usted, además, otras que puedan encontrarse en su perfil de redes sociales. Recuerde que las respuestas no deben ser necesariamente verdaderas: el único requisito es recordarlas. Elija respuestas al azar y eso ayudará a despistar a los hackers.

3.6 Recomendaciones al crear una contraseña

Tener una contraseña con buena extensión y dificultad es fundamental para que su crackeo sea difícil o casi imposible. Además, la combinación con letras, números y símbolos aumentan su grado de complejidad. El empleo de una buena contraseña que utilice palabras combinadas con números y símbolos, la extensión recomendada estaría establecida en 12 caracteres como mínimo.

Para que te hagas una idea, una buena contraseña sería del tipo: “4dO/&-28enW=s?q”. A continuación, te damos unas recomendaciones que deberás tener en cuenta al momento de crear una contraseña para una PC:

g. Use un administrador de contraseñas que pueda crear contraseña fuertes y complejas, y recordarlas por usted. Si elige un software de seguridad robusto, este podría incluir un administrador de contraseñas.

h. Si lo consideras necesario, puedes acudir a servicios en internet para proceder a crear una contraseña. Nos podemos encontrar multitud de ellos que podemos utilizar. Su funcionamiento es simple, tendremos que acceder al portal donde está la herramienta, seleccionar algunos parámetros que nos indica la página y sobre los que creará la contraseña, y este generará una clave.

i. Si no usa un administrador de contraseñas o no consideras necesario acceder a servicios de internet para la creación de una, aprenda cómo crear contraseñas que sean más largas y complejas que una contraseña tradicional, pero a su vez, fáciles de recordar, empleando frases al azar.

Ejemplo 1: si a usted le gusta la lectura y quiere citar un libro que haya leído, la frase sería: “El caballero Carmelo fue escrita por Abraham Valdelomar y tiene más de 40 páginas” podría convertirse en la siguiente contraseña: “EcC*fexAV+40p”.

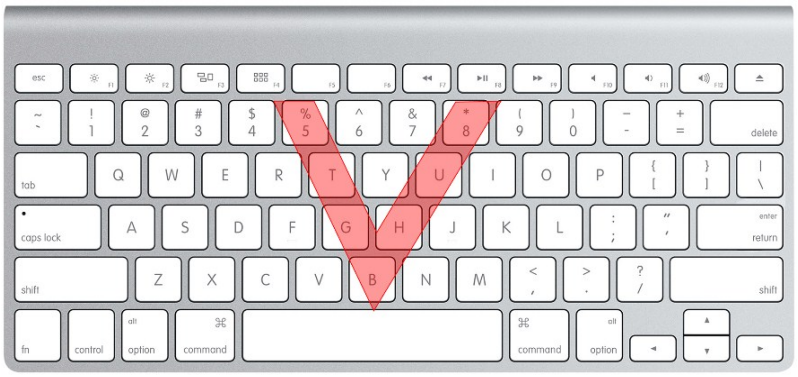
Ejemplo 2: si le fascina jugar el futbol su frase podría ser: “Me gusta jugar Futbol, uso la camiseta 9, juego de Puntero Izquierdo, anoto más de 2 goles por partido”, su contraseña podría ser “mgjF/uc9jPI@+2g*p”.

j. También puede usar combinaciones de teclas que creen una forma o letra particular en el teclado. Por ejemplo, observe la secuencia: 5tgbHU8 que en el teclado forma una V (Figura 3). se usó en minúsculas las letras que descendían y en mayúscula las letras que ascendían, además, podrían agregarse símbolos para dificultar su descifrado: “%5-tgb~HU/8*”. Podría crear la letra V, o cualquier otra letra y empezando desde cualquiera de las teclas.

Para cambiar la contraseña asiduamente podría empezar por otra tecla. Los más osados suelen usar también una W.

Figura 3

Ejemplo de uso de contraseña en V (elaboración propia)



k. Es importante crear una contraseña de acceso al sistema (nos centramos en Windows) que conste por lo menos de 12 caracteres para que sea segura. Además, deberemos mezclar números, letras, además de símbolos tipo la @, %, ^, *, ~, etc. Tener presente que, en un ataque por fuerza bruta, una contraseña de 12 a 18 caracteres y siguiendo lo antes mencionado es "rompible", pero tardaría demasiado tiempo.

l. Se debe tener en cuenta la protección del salvapantallas de Windows, es un aspecto de seguridad que muchos dejan de lado. En el trabajo hay verdaderos problemas con este tema, un descuido y podemos sufrir ataques rápidos y fortuitos desde casa o la oficina. El salvapantallas de Windows es un aspecto que no se debe dejar de lado, al salir al baño o a la cafetería dejando el PC abierto, puedes ser víctima de hurto de información, que te coloquen un troyano, que vean tus archivos, etc. Lo mejor es activar el salvapantallas con la opción de introducir contraseña para volver a tener acceso al PC.

3.7 Protocolos de seguridad Wifi

Los algoritmos de seguridad Wifi han ido evolucionando y mejorando desde la década de los 90 con el propósito de buscar un servicio más eficaz, pero a la vez darle mayor seguridad. Se desarrollaron diferentes tipos de protocolos de seguridad inalámbricos para la protección de redes inalámbricas. Los protocolos de seguridad inalámbrica son WEP, WPA, WPA2 y WPA3, que cumplen el mismo propósito pero que son diferentes al mismo tiempo.

Los protocolos de seguridad inalámbrica no sólo evitan que ajenos se conecten a su red inalámbrica, sino que también encriptan sus datos privados enviados a través de las ondas de radio.

No importa lo protegido y cifrado, las redes inalámbricas no pueden mantenerse en seguridad con redes cableadas. Estos últimos, en su nivel más básico, transmiten datos entre dos puntos, A y B, conectados por un cable de red. Para enviar datos de A hacia B, las redes inalámbricas lo transmiten dentro de su alcance en todas las direcciones a cada dispositivo conectado que esté escuchando.

Si contamos con un router Wifi en la oficina o en la casa, querrás protegerlo de elementos exógenos y evitar que accedan a la red. Para ello, debes poner una contraseña que refuerce la seguridad. Sin embargo, como lo hemos visto anteriormente, no es suficiente con poner una contraseña básica, pues son vulnerables a ataques con software maliciosos y sistemas operativos para irrumpir en tu red. Todo depende del tipo de Protocolo de Seguridad Wifi que hayas elegido.

a. Tipos de Protocolos de Seguridad Wifi

Hay varios tipos de Protocolos de Seguridad Wifi a la cual puedes acceder, a continuación, te las detallamos:

- **WEP:** Incluido en 1997 para proteger las primeras contraseñas Wifi. Las primeras versiones llevaban 64 bits de cifrado y las últimas 128. Se quedó rápidamente obsoleto, ya que se puede hackear muy fácilmente en cuestión de minutos. Aun así, todavía hay dependencias que lo utilizan.

- **WPA:** Se planteó en 2003 como una mejora para la seguridad de las redes Wifi. El protocolo es similar que el de WEP, pero mejorado con el protocolo TKIP. En 2012 se declaró obsoleto, ya que se podía hackear con ataques de diccionario.

- **WPA2:** Este sistema de seguridad salió en 2004 y es uno de los más utilizados. Fue el primero en introducir el sistema de cifrado AES, mucho más seguro que TKIP. Eso sí, todavía era compatible con este último por temas de compatibilidad. Este sistema poseía una vulnerabilidad en el protocolo WPS que permitía hackear muchas redes en cuestión de segundos, aunque ha sido parcheado en algunos modelos de dispositivos en la actualidad.

- **WPA3:** Es el tipo de cifrado Wifi más reciente, ya que se implementó en 2018. En este caso, solamente es compatible con el sistema AES. Además, ha cambiado el protocolo WPS por DDP, que permite dar acceso por un código QR.

b. Tipos de Protocolo Wifi WPA: TKIP o AES

Dentro de los protocolos Wifi tenemos a el WPA, que posee dos tipos de cifrados:

- **TKIP:** Se inventó para corregir la vulnerabilidad que existía en WEP, siendo también compatible con WPA2. Viene de las siglas Temporal Key Integrity Protocol (Protocolo de integridad de clave temporal). Se quedó rápidamente obsoleto por ser vulnerable a ataques de diccionario y por hacer que la red vaya más lenta.

- **AES:** Viene de las siglas Advanced Encryption Standard (Estándar de cifrado avanzado) y fue introducido en WPA2, siendo el único estándar disponible para WPA3. Es más seguro que el sistema anterior y es muy difícil de descifrar.

3.8 Riesgos al conectarse a una red Wifi abierta o gratuita

"Por lo general, la gente tiene la percepción equivocada de que utilizar una red Wifi abierta no tiene ningún tipo de peligro para su seguridad de los datos almacenados en el dispositivo que esté conectado, por lo que no toman las medidas necesarias para garantizar la protección de su información".

La emergencia sanitaria provocada por la pandemia de la COVID 19, ocasionó que el mundo incremente la modalidad laboral de presencial a remota, la tecnología jugó un papel importante no solo para los trabajadores, sino también para aquellos que necesitaban sujetarse a una red para realizar diversas actividades; estudios, reuniones de trabajo, hablar con un familiar, etc. La habitual y sedentaria forma de trabajo en oficina alternó drásticamente a la modalidad de trabajo remoto, teletrabajo o trabajo desde casa, particularmente en las entidades del estado.

En la actualidad, el trabajo remoto en el Ejército sigue reconfigurándose en la medida que el Perú y el mundo se ajuste a una nueva normalidad. En tal sentido, la seguridad de las informaciones puede ser vulnerables cuando realicemos trabajo remoto, trabajar un fin de semana en el hogar o inclusive hacerlo estando de vacaciones, y esto se agrava cuando nos conectamos a una red Wifi de procedencia dudosa.

Las redes Wifi abiertas o gratuitas se han convertido, especialmente fuera de la oficina o de la casa, en uno de los recursos fundamentales para conectarse a internet, como un

restaurante, aeropuerto, estando de viaje, entre otras. Permitiéndonos un acceso rápido y cómodo, pero quedamos expuestos a un ataque de un pirata cibernético.

Los riesgos al conectarse a una red Wifi abierta o gratuita como la falta de privacidad, suplantación de identidad, Infección de dispositivos, robo de información sensible, etc. son algunos de los peligros que los usuarios corren ante esta práctica. Por lo cual es menester evitar conectarse a este tipo de redes si lo que quieres es no correr el riesgo de que se atente contra la seguridad de tus informaciones.

3.9 Recomendaciones al usar un antivirus

a. Podemos usar dos antivirus teniendo en cuenta que sean compatibles entre sí. Por ejemplo, el KAV sólo para rastreos y el NOD como residente siempre activo, en el antivirus, el módulo activo controla todo lo que entra al PC y escanea constantemente en busca de virus.

b. Además de los virus, están los troyanos: programas de código "malicioso" que se dedican a hacer de puente entre el PC de un atacante y nuestro ordenador. Los antivirus suelen fallar con los troyanos en muchos casos.

c. El Bitdefender, Total AV, el McAfee y el Norton 360 son considerados como unos de los mejores antivirus, cuentan con una excelente capacidad de detección de virus, eliminando fácilmente troyanos, adware, spyware, ransomware y otros elementos; además, no detectan falsos positivos. Si tenemos un troyano dentro y nos lo detectan, las entradas pueden ser interminables; por lo que el uso de un firewall (muro virtual entre el ordenador y la red) se hace imprescindible, además de para otras muchas cosas. El firewall vigilará cualquier conexión entrante y saliente entre Internet y el PC.

ANEXO 8

CD CONTENIENDO LA TESIS

TESIS

ANALISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGISTICO DEL EJERCITO, 2022

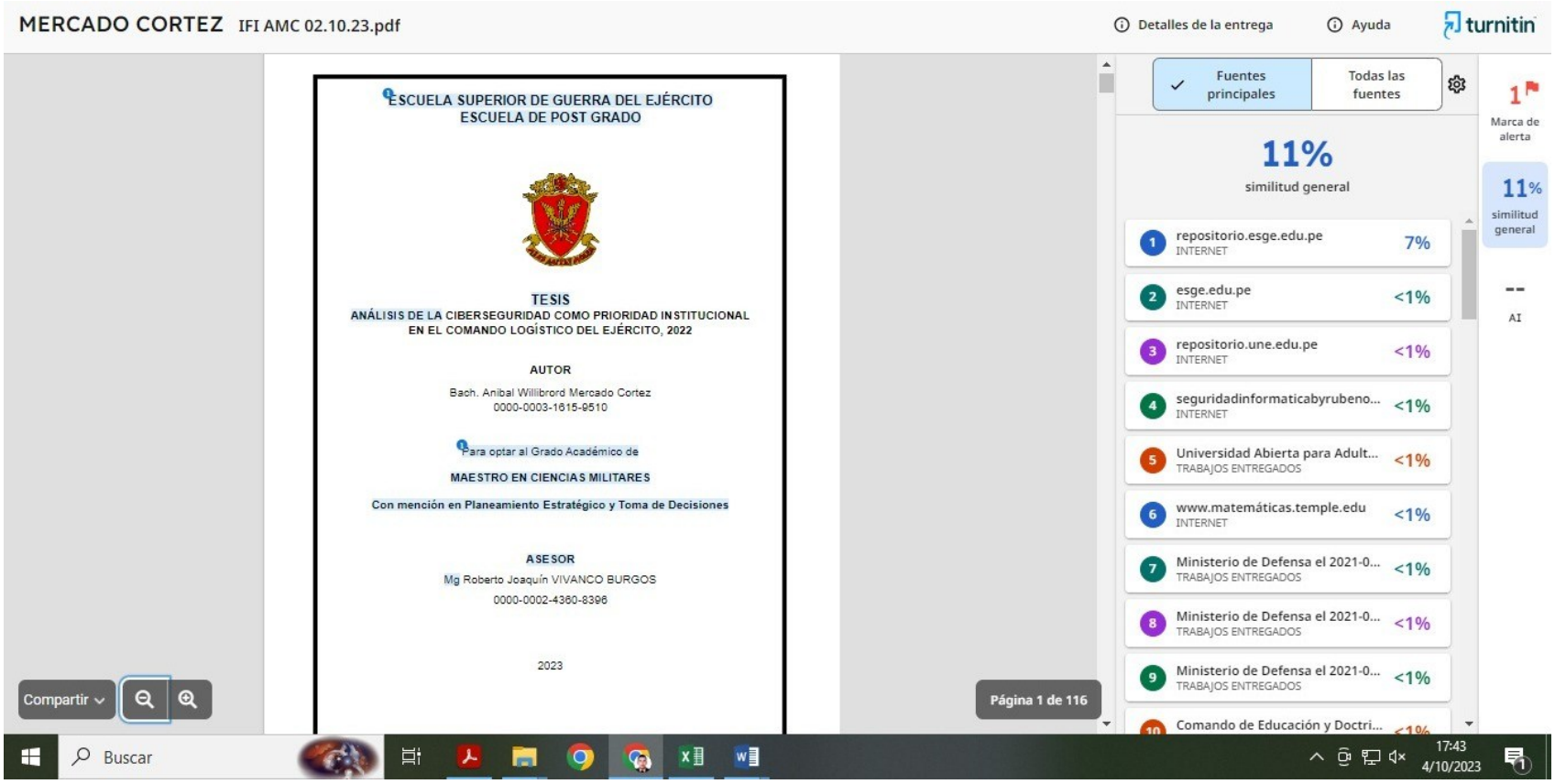
AUTOR

Bach. Anibal Willibrord Mercado Cortez

2023

ANEXO 9

REPORTE DE SIMILITUD DE TURNITIN


MERCADO CORTEZ IFI AMC 02.10.23.pdf
Detalles de la entrega
Ayuda
turnitin
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POST GRADO
TESIS
ANÁLISIS DE LA CIBERSEGURIDAD COMO PRIORIDAD INSTITUCIONAL EN EL COMANDO LOGÍSTICO DEL EJÉRCITO, 2022
AUTOR
Bach. Aníbal Willibrord Mercado Cortez
0000-0003-1615-9510
Para optar al Grado Académico de
MAESTRO EN CIENCIAS MILITARES
Con mención en Planeamiento Estratégico y Toma de Decisiones
ASESOR
Mg Roberto Joaquín VIVANCO BURGOS
0000-0002-4360-8396
2023
Fuentes principales
Todas las fuentes
11%
similitud general
1 repositorio.esge.edu.pe INTERNET 7%
2 esge.edu.pe INTERNET <1%
3 repositorio.une.edu.pe INTERNET <1%
4 seguridadinformaticabyrubeno... INTERNET <1%
5 Universidad Abierta para Adult... TRABAJOS ENTREGADOS <1%
6 www.matemáticas.temple.edu INTERNET <1%
7 Ministerio de Defensa el 2021-0... TRABAJOS ENTREGADOS <1%
8 Ministerio de Defensa el 2021-0... TRABAJOS ENTREGADOS <1%
9 Ministerio de Defensa el 2021-0... TRABAJOS ENTREGADOS <1%
10 Comando de Educación y Doctri... <1%
1 Marca de alerta
11% similitud general
-- AI
Compartir
Página 1 de 116
Buscar
17:43
4/10/2023