ESCUELA MILITAR DE CHORRILLOS

"CORONEL FRANCISCO BOLOGNESI"

"LOS PUESTOS DE COMANDO EN CIBERDEFENSA Y CIBERSEGURIDAD EN EL CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ"

Trabajo de suficiencia profesional para optar el título profesional de Licenciado en Ciencias Militares con mención en Ingeniería

Autor:

CARLOS ISRAEL NESTARES ENCINAS

0000-0002-0018-7587

Lima - Perú

2023

NOMBRE DEL TRABAJO

NESTARES ENCINAS.docx

RECUENTO DE PALABRAS

10709 Words

RECUENTO DE CARACTERES

60575 Characters

RECUENTO DE PÁGINAS

47 Pages

TAMAÑO DEL ARCHIVO

139.5KB

FECHA DE ENTREGA

Apr 11, 2024 3:28 PM GMT-5

FECHA DEL INFORME

Apr 11, 2024 3:29 PM GMT-5

21% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 19% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 9% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 15 palabras)
- Fuentes excluidas manualmente

Dedicatoria

Dedico esta investigación a mi amorosa familia, quienes son mi motivación para superar todas las dificultades que se me presentan día a día.

Agradecimiento

Un agradecimiento especial para mi asesora, por darse un tiempo y apoyarme a realizar este gran trabajo.

INDICE

RESUMEN III

INTRODUCCIÓN V

CAPÍTULO I: INFORMACIÓN GENERAL 1

1.2 Dependencia 1

1.3 Tipo de Actividad 1

1.4 Lugar y Fecha 1

1.5 Visión del Centro de Ciberdefensa del Ejército (CECYBER) 1

1.6 Misión del Centro de Ciberdefensa del Ejército (CECYBER) 1

1.7 Funciones y actividades del Puesto que Ocupó 2

CAPÍTULO II: MARCO TEÓRICO 3

2.1. 3

2.1.1 Antecedentes Internacionales 3

2.1.2 Antecedentes Nacionales 5

2.2 8

2.2.1 Creación de un Cibercomando en las Fuerzas Armadas 8

2.2.1.1. Ciberataques al estado y a activos críticos 8

2.2.1.2. 9

2.2.1.3. 10

2.2.1.4. 11

2.2.2 Ciberseguridad 11

2.2.2.1. 12

2.2.2.2 Traslación del conflicto a la dimensión virtual. 13

2.2.2.3. 14

2.3 17

2.3.1. Riesgo. 17

2.3.2. Ciberseguridad 18

2.3.3. Amenazas. 18

2.3.4 Traslación 18

2.3.5. Ciberataque 19

2.3.6. Ciberespionaje 19

CAPÍTULO III: DESARROLLO DEL TEMA 20

3.1. 21

3.2. 21

3.3. 22

3.4 23

CONCLUSIONES 27

RECOMENDACIONES 29

REFERENCIAS BIBLIOGRÁFICAS 30

ANEXOS 33

RESUMEN

El presente trabajo surgió de la experiencia adquirida por el autor, al laborar en el Centro de Ciberdefensa del Ejército (CECYBER), dependencia que es liderada por Ciberdefensa y Telemática del Ejército (CITELE). Unidad en la que aprendió sobre las capacidades que debe de dominar el personal del arma de Comunicaciones del Ejército y el desempeño que debe tener en la Defensa Cibernética de las comunicaciones del Ejército. La dependencia del CECYBER se encuentra ubicada en el Cuartel General del Ejército (CGE) – San Borja. Esta investigación tiene por objetivo analizar y describir la problemática que presenta el Ejército del Perú en lo referente a Ciberdefensa y Ciberseguridad y además promover a partir de la propuesta de mejora presentada en este trabajo, la creación de puestos de comandos en ciberdefensa y ciberseguridad para el entrenamiento y preparación del personal militar ante las nuevas amenazas tecnológicas.

El *problema de estudio* hace referencia a la falta de implementación o pocos Puestos de Comando en Ciberdefensa y Ciberseguridad que dispone el país para la protección de las cyber comunicaciones debido quizás, a los altos costos de los equipos, softwares y a la falta de conocimientos que dispone el personal en los avances tecnológicos actuales, en ciberataques y ciberdefensa, lo que nos coloca en una posición de desventaja ante los demás países frente a estos ataques tecnológicos. Esta situación generó al autor la siguiente interrogante *¿en qué medida*

la creación de nuevos puestos de comando mejoraría nuestra capacidad en ciberdefensa y ciberseguridad?

En este trabajo, se analiza la situación actual, llegando a la *conclusión* de formar puestos de comando que protegerán la información secreta del país y obtendrán la capacidad de defensa contra ciberataques. Definimos como equipos de detección y respuesta a ataques cibernéticos y se recomienda que los sistemas adquiridos permanezcan actualizados y no se vean afectados por los cambios tecnológicos. Asimismo, la propuesta sobre la "C*reación de puestos de comando en ciberdefensa y ciberseguridad en el Ejército del Perú",* para el entrenamiento y preparación del personal militar ante las nuevas amenazas tecnológicas y la implementación de una política de ciberseguridad que ayudaría a mantener la seguridad física de la información.

Palabras clave: ciberdefensa en Perú, ciberdefensa, ciberseguridad, ciber, cyber, seguridad, redes.

INTRODUCCIÓN

El autor del presente trabajo al laborar en el Centro de Ciberdefensa del Ejército (CECYBER), dependencia que es liderada por Ciberdefensa y Telemática del Ejército (CITELE), desempeñándose como Jefe de la Defensa Cibernética de las comunicaciones del Ejército, las principales dificultades que tuvo en ese periodo laboral fueron la falta de presupuesto asignado, el desconocimiento de la importancia de la labor en la protección cibernética de toda la información institucional y la falta de equipamiento del Puesto de Ciberdefensa a comparación de otras realidades que se resumen en los párrafos siguientes.

A nivel continental, el Observatorio de Ciberseguridad de América Latina y el Caribe, patrocinado por la Organización de Estados Americanos y el Banco Interamericano de Desarrollo, basado en el modelo de Madurez de Capacidades Ciberseguridad (MMCC). Su dimensión "Política y estrategia de seguridad cibernética" incluye un campo "Organización" para examinar la existencia de entidades coordinadores nacionales y proporcionar un presupuesto integral y supervisión.

El Modelo de Madurez de Capacidades Ciberseguridad divide los resultados de madurez en cinco etapas: etapa inicial, etapa formativa, etapa de consolidación, etapa estratégica y etapa dinámica. (Organización de los Estados Americanos y Banco Interamericano de Desarrollo 2020).

El sector público de ciberseguridad de América Latina está en construcción. A pesar de los avances en la dirección correcta desde finales del siglo XX y desarrollar una política de ciberseguridad eficaz, sigue siendo un proceso paso a paso que sigue en etapa inicial o formación. Esta situación motiva a poner el acento analítico en su organización y funcionamiento, aspecto preliminar de su proceso evolutivo dada la centralidad del diseño institucional como condición de contexto necesaria para concebir estrategias sectoriales y políticas contribuyentes. (Unión Internacional de

Telecomunicaciones, 2021).

El tipo de medición que realiza la OEA y el BID nos permite mirar dentro de la región y desde un prisma intertemporal. Según el informe de 2020, América Latina ha mejorado las capacidades de ciberseguridad de los estados desde 2016. Sin embargo, funcionarios de dichas organizaciones describen este progreso como "Tímido" porque la madurez promedio de las capacidades específicas del sector varía solo entre las etapas inicial y de capacitación, debido al carácter ad - hoc de las iniciativas y a la falta de intervención llevado a cabo entre los principales actores. (OEA y BID 2020).

El Perú no ha sabido desarrollar el sector de ciberdefensa. Actualmente, el país no cuenta con una inversión destinada a promover los sistemas de seguridad y la defensa cibernética. Si bien la región Latinoamericana tiene poca incidencia en conflictos cibernéticos a gran escala, es importante destacar que la seguridad nacional podría verse vulnerada de no nivelarse a las exigencias actuales. (J Quevedo L. C, 2023).

El presente trabajo consta de cuatro (04) capítulos, los cuales se han estructurado de la siguiente manera: *El capítulo I,* contiene la *información general*, cómo es la dependencia dónde se inspiró el trabajo, el *tipo de actividad o actividades realizadas*, lugar y *fecha, misión, visión* de la unidad o dependencia y *funciones del puesto* que se desempeñó. El c*apítulo II*, comprende los *antecedentes* internacionales y nacionales que enmarcan el trabajo, y narran la realidad desde otras perspectivas de los puestos de comando de ciberdefensa y ciberseguridad y la *descripción teórica*, que es el fundamento científico y tecnológico que da sustento a las variables de estudio y algunos términos teóricos básicos referentes a la ciber tecnología, la evolución de los ataques en el ciberespacio y la creación de una nueva dimensión de conflicto bélico. En el c*apítulo III*, se desarrolla el tema donde se explica la propuesta de mejora hecha por el autor, los campos y tipos de aplicación de la misma, el diagnóstico de la realidad observada durante la experiencia del autor hasta la actualidad, los objetivos y descripción de la propuesta, y los elementos para su desarrollo. En el capítulo IV, se establecen las conclusiones y recomendaciones. Y finalmente van las referencias bibliográficas y anexos.

CAPÍTULO I: INFORMACIÓN GENERAL

1.2 Dependencia

El presente trabajo de Suficiencia Profesional se desarrolló en el Centro de Ciberdefensa del Ejército (CECYBER) – Ciberdefensa y Telemática del Ejército (CITELE) que se encuentra en el Cuartel General del Ejército ubicado en San Borja, Departamento de Lima, Perú.

1.3 Tipo de Actividad

La actividad principal que desarrolló el autor mientras estuvo laborando en el departamento de defensa cibernética fue detectar en tiempo real y anular los ataques cibernéticos que se realizaban con la intención del robo de información con el apoyo del departamento de Explotación Cibernética,

1.4 Lugar y Fecha

Centro de Ciberdefensa del Ejército (CECYBER), ubicado en San Borja, Departamento de Lima, Perú. El autor desempeñó funciones en esta unidad en el año 2021.

1.5 Visión del Centro de Ciberdefensa del Ejército (CECYBER)

"Liderar la Ciberdefensa en la Región".

1.6 Misión del Centro de Ciberdefensa del Ejército (CECYBER)

"Realizar operaciones defensivas, de explotación y ofensivas en el ciberespacio; investigando, experimentando, desarrollando e innovando en ciberdefensa".

1.7 Funciones y actividades del Puesto que Ocupó

a. Realizar operaciones y acciones defensivas, proactivas en el ciberespacio como el análisis de vulnerabilidades web y de infraestructura.

b. Realizar operaciones y acciones defensivas, preventivas en el ciberespacio como monitoreo de eventos e incidentes.

c. Realizar operaciones y acciones defensivas reactivas en el ciberespacio como análisis forense informáticos.

d. Priorizar y determinar los límites de funcionamiento eficiente y establecer las medidas necesarias que garanticen la continuidad de sus funciones mediante un Plan de continuidad destinados a mitigar el impacto provocado por algún incidente.

e. Desarrollar los métodos y medios de la capacidad de defensa en el ciberespacio a fin de salvaguardar los activos institucionales y otros que el Comando designe

f. Detallar y consolidar los reportes de vulnerabilidades que pudiesen afectar los activos institucionales, realizando actividades preventivas, monitoreo de redes en los activos de información del Ejército

g. Garantizar la adecuada cadena de custodia a fin de mantener la información forense recabada en condiciones de ser empleada legalmente, solo en casos de haber sufrido un ataque cibernético o delito informático.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

Para el presente estudio se encontraron diferentes trabajos de investigación realizados en otras realidades internacionales y nacionales afines o similares al tema desarrollado en este trabajo de suficiencia profesional, los que sirvieron al autor como una base teórica y metodológica importante, aportándole significativamente durante la elaboración de cada parte del proceso de esta investigación, permitiéndole analizar y comparar los estudios ya realizados y ayudándole en la elaboración de la propuesta de mejora

2.1.1 Antecedentes Internacionales

Villalba (2015) desarrolló una investigación titulada "*La ciberseguridad en España, 2011-2015. Una propuesta de modelo de organización",* tesis para optar el grado académico de Doctor en Ciencias Políticas. El *objetivo* de este estudio fue proponer un modelo de gobernanza en el ámbito de la ciberseguridad en España. El *diseño de investigación* fue no experimental, de enfoque *cualitativo*, analítico y propositivo. Tomando en consideración que la ciberseguridad corresponde a un conjunto superior de la seguridad, asociada a los desarrollos comunicacionales. En el campo de la ciencia política, esta investigación, por su carácter prescriptivo, propone soluciones a problemas complejos de organización de modelos de seguridad en el ámbito de la utilización del ciberespacio. La investigación *aportó al presente estudio* proponiendo políticas estructuradas en materia de ciberseguridad y recomendando la creación al más alto nivel de organizaciones para enfrentar las nuevas amenazas; asimismo, se ha identificado como carácter primordial el fomentar el gobierno electrónico y a la vez estructurar a nivel nacional redes que permitan brindar seguridad cibernética y garantizar el libre uso de los recursos reales y virtuales. Estas redes tienen como base la concientización de la población en lo referente a seguridad de la información y su capacitación para utilizar de la mejor forma los servicios.

Rubio (2016). En su investigación titulada: "*Un Marco para el Análisis de Riesgos en*

Ciberseguridad", tesis para optar el grado académico de Doctor en Ciencias de la Computación, Universidad Rey Juan Carlos, Madrid, España, tuvo como *objetivo*, realizar un análisis de los riesgos y establecer un mapa de riesgos. Diseño de estudio *no experimental* y de *enfoque cuantitativo*, empleando un método fundamentalmente *hermenéutico*, empleando como instrumento la *ficha de análisis* de documental, llegando a las siguientes conclusiones. Primero, las redes de computadoras o el llamado ciberespacio se ha convertido en la cuarta dimensión donde se pueden desarrollar operaciones militares, una de las primeras acciones ha sido la implementación de la ciberdefensa como capacidad militar para poder hacer frente al exponencial crecimiento de ciberataques a las redes de computadoras de las infraestructuras críticas e instituciones de valor estratégico. Segundo, se hace mención que uno de los ataques más comunes dirigidos hacia las instituciones de valor estratégico son los ataques de negación de servicio distribuida (DDoS), y otros tipos de ciberarmas y métodos, tomando en consideración los peligros y retos que presenta la realidad tecnológica actual. Esta investigación aportó mostrando como la cuarta dimensión de las operaciones militares es una realidad, en consecuencia, los Estados están en la obligación de priorizar las creaciones de las instituciones y la implementación de las capacidades necesarias para salvaguardar el ciberespacio de cada uno de ellos. y por último un marco legal claro que defina responsabilidades y funciones que permita legalmente el empleo de las capacidades necesarias para proteger el ciberespacio.

E. Vergara T; G Adolfo T. (2017), en su trabajo de investigación "*Operaciones Militares* Cibernéticas" - Buenos Aires. para optar el grado Doctor en desarrollo y seguridad estratégica, el *objetivo* fue dar a conocer que los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. El *diseño* de investigación fue *no experimental*, correlacional y descriptiva. La técnica de recolección de datos fue la *encuesta*. En resumen, la demanda de Internet y de conectividad digital exige una integración cada vez mayor de las Tecnologías de la Información y la Comunicación (TIC). A medida que fue aumentando la dependencia respecto de ellas, en el plano mundial también se incrementó la vulnerabilidad a los ataques contra las infraestructuras críticas a través

del espacio cibernético, entendiendo por este al dominio virtual, global y dinámico, creado por el hombre, compuesto por las infraestructuras de tecnología de la información, las redes y los sistemas de información y de telecomunicaciones, incluidas las de las Fuerzas Armadas. Aportando al presente trabajo en la influencia de la cibernética en las operaciones militares convencionales y, específicamente, en los aspectos que deben tenerse en cuenta en el nivel operacional de guerra, cuando llega el momento de implementar la dirección estratégica. Por esta razón, un comandante de un Teatro de Operaciones debe saber cómo incorporarlo al método de planeamiento y qué requerir de él en la ejecución de operaciones militares bajo su responsabilidad.

Albarracín (2019), en su tesis titulada *"Inteligencia Nacional y estrategia de ciberseguridad nacional"* para optar el grado académico de Magíster en Inteligencia Estratégica Nacional, en la Universidad Nacional de la Plata, Argentina, manifestó que *su objetivo* fue "iluminar sobre los factores que diluyen la definición de una Estrategia Nacional de Ciberseguridad en Argentina" , utilizando el método de investigación cualitativa, llegando a las siguientes conclusiones: Primero, la expansión de las TICs y la "difusión tecnológica trajo aparejada la necesidad de establecer medidas de ciberseguridad y ciberdefensa con el objeto de mitigar y proteger al país de las vulnerabilidades provenientes del ecosistema que compone el ciberespacio". Segundo, existen "diversas normativas destinadas a proteger la seguridad de la información y cooperar internacionalmente en el ámbito procesal", sin embargo, una distinción entre "ciberseguridad, ciberdefensa y cibercrimen, con diferente dinámicas y desarrollos". Esta investigación muestra al autor del presente trabajo, la necesidad de unificar los esfuerzos institucionales en materia de ciberdefensa. Del mismo modo, el gran requerimiento de inversión en equipo humano y tecnológico.

2.1.2 Antecedentes Nacionales

Ormachea (2019). "*Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional",* tesis para optar el grado académico de Doctor en Desarrollo y Seguridad Estratégica, en el Centro de Altos Estudios Nacionales, (CAEN) Lima, Perú, tuvo como *objetivo,* proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, 2019. La investigación fue en base al *diseño no experimental* y de *enfoque cualitativo*, empleando un método fundamentalmente *hermenéutico*, con instrumento empleando ficha de registro y ficha de análisis. Indicó que, para proteger íntegramente los activos críticos e instituciones de valor estratégico en nuestro país, es fundamental la implementación de estrategias de ciberseguridad de acuerdo a la categorización específica, las cuales deben ser enmarcadas dentro de normas y leyes las que deben estar especificadas en reglamentos, además menciona que, en la actualidad el Perú en el tema de ciberseguridad se encuentra en un nivel de capacidad de respuesta media baja, así mismo la Constitución Política del Perú no protege a la población vulnerable al acceso de material gráfico nocivo y que en el Plan Bicentenario existe brechas de diseño de políticas e implementación de ciberseguridad, por lo que se evidencia la necesidad urgente y obligatoria de la creación e implementación de la capacidad militar de ciberdefensa para poder fortalecer la ciberseguridad en nuestro país, por último, menciona que en el Perú aún no existe una estrategia integrada para la protección de ciberataques a los medios tecnológicos de los activos críticos, infraestructura esencial, información clasificada e instituciones de valor estratégico ya sea públicas o privadas. Resumiendo, es de urgencia la implementación y fortalecimiento de la capacidad de ciberdefensa, para que ésta fortalezca la ciberseguridad en nuestro país y así se logre alcanzar una adecuada protección de los medios tecnológicos de los activos críticos, infraestructura esencial, información clasificada e instituciones de valor estratégico, así mismo el empleo de dicha capacidad militar debe estar enmarcada dentro de leyes y normativas claras las que deben ser aprobadas y reglamentadas por la más altas autoridades políticas y militares, además que los activos críticos nacionales y las instituciones de valor estratégico no solo pueden ser públicas sino que también existen activos e instituciones de valor

estratégico que son privadas, por lo tanto para que se llegue a la protecciones de estas también se debe proponer estrategias que involucren al sector privado. ¿Y cuál es el aporte de esta investigación a la suya?

G Rossi L, (2021), realizó una investigación en la seguridad y defensa en la era de la cuarta revolución industrial: estos son elementos para una propuesta de estrategia de política exterior para país, el trabajo se denominó "*el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas desde finales del siglo XX",* el mundo se ha vuelto cada vez más interconectado e interdependiente a medida que avanza la Cuarta Revolución Industrial, caracterizada por la convergencia disruptiva de tecnologías digitales, físicas y biológicas. Estos avances traen consigo nuevas amenazas a la seguridad y defensa de las naciones, ya manifestadas en guerras y ciberataques por parte de actores estatales y no estatales que han logrado neutralizar sus capacidades defensivas, digitales y financieras. Por lo que concluye que, la ciberseguridad y la ciberdefensa son esenciales ya que protegen y responden de los ciberataques a infraestructuras, redes y sistemas informáticos y digitales críticos de actores gubernamentales, militares y del sector privado, garantizando así la seguridad y protección dentro de sus capacidades.

El General en retiro *A. Herrera L. (2017),* en su investigación "*La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador*", este autor quien se ha convertido en la primera y más importante parte del ciclo inteligente, procedimiento científico, desarrollado posteriormente por el historiador estadounidense Sherman Kent durante la Segunda Guerra Mundial. Hoy en día, los manuales militares actuales describen y llaman al trabajo de oficiales de infantería (observadores), como un servicio de inteligencia que proporciona a los comandantes sus necesidades de inteligencia Combate, hizo un artículo sobre inteligencia de combate en la Primera Guerra Mundial. Revista de la Escuela Conjunta de las Fuerzas Armadas de Lima Chorrillos Los observadores de infantería en la guerra de trincheras.

En resumen, aporto en que se convirtió en la primera parte y como un importante circuito de inteligencia, el procedimiento científico se desarrolló posteriormente. El historiador estadounidense Sherman Kent investigó en el periodo durante la Segunda

Guerra Mundial. Hoy Los manuales militares actuales describen y nombran al trabajo de oficiales de infantería (observadores), como un servicio de inteligencia que proporciona a los comandantes sus necesidades de inteligencia Combate.

Vasquez 2022, Capacidad Militar de ciberdefensa en el Ejército del Perú año 2021, tesis para optar el grado académico de Magister en Ciencias militares, tuvo como objetivos el analizar en qué situación se encontraba en el 2021 la ciberdefensa y, además, estudiar el tipo de ciberoperaciones que estaba en condiciones de realizar la ciberdefensa del Ejército del Perú. La presente investigación tiene un *enfoque cualitativo del tipo teórica-empírica*, con el método fenomenológico a razón de que las actividades en el ciberespacio son un fenómeno social que ha ido acrecentándose y tornándose en un ambiente cada vez más peligroso e impredecible.

Esta investigación muestra como aún en el Ejército del Perú se cuenta con la capacidad militar de ciberdefensa en situación de desarrollo e implementación. De la misma manera, de los tres tipos de ciberoperaciones que debería estar en condiciones de realizar ciberdefensa del Ejército del Perú, solamente está en la capacidad de realizar dos defensivas y de explotación, pero de manera muy limitada, respecto a ciberoperaciones ofensivas, aún no se cuenta con la capacidad y la legalidad para poder realizarlas.

2.2 Descripción teórica

2.2.1 Creación de un Cibercomando en las Fuerzas Armadas

El Estado debe tener la Capacidad de Ciberdefensa, ante posibles ciberataques a la nación y sus activos críticos, para estar en la capacidad de neutralizar dichas amenazas, a fin para proteger sus intereses nacionales. El Comando Conjunto tiene como una de sus funciones, garantizar a través de las Fuerzas Arma-das, la soberanía e integridad territorial. Siendo el ciberespacio, el nuevo escenario en el cual se desarrollan los ciberataques a un Estado. *(Smith, J. 2019)*.

Se entiende por ciberdefensa el conjunto de operaciones activas o pasivas utilizadas por el Estado para garantizar la seguridad y el uso adecuado del ámbito digital de un país, a la vez que lo protege de amenazas como las descritas

previamente. Sin embargo, la ciberdefensa se puede confundir con la ciberseguridad, puesto que a priori ambas parecen aludir a la protección de un espacio virtual o cibernético.

2.2.1.1. Ciberataques al estado y a activos críticos

Actualmente los ciberataques suceden todos los días, la mayoría están orientados al robo de información que se puede convertir en dinero, no interesa de donde se obtenga o el efecto que cause, el objetivo es uno solo: dinero. El ataque puede ser a una Instalación Militar para robar información confidencial que le pueda servir a otro país y eso es dinero, como lo sucedido a EEUU, en que china roba los planos del Avión de caza F-35 y El Director de la Inteligencia Nacional de Estados Unidos, James Clapper, lo toma como un ciberataque a los activos críticos militares y advierte de un ataque cibernético "a gran escala" podría "debilitar toda la infraestructura del país norteamericano; "En mis más de 50 años en el negocio de la inteligencia, no recuerdo un momento en el que hemos estado acosados por una mayor variedad de desafíos y riesgos de todo el mundo, tanto a nivel regional como funcionalmente", afirmó Clapper ante el Comité de Inteligencia de la Cámara de Representantes *(Taipe y Dominguez, 2017)*.

Se va a entender por un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

2.2.1.2. Espacio cibernético

Uno de los primeros obstáculos al abordar este tema es la variedad de definiciones. "No es un camión. "Es una serie de tuberías". Así es como el difunto senador de Alaska Ted Stevens explicó el ciberespacio durante una audiencia en el Congreso en 2006. Si bien es fácil burlarse de la idea del viejo senador de enviar correos electrónicos a través de tuberías, la realidad es que el ciberespacio puede definir ideas y los términos pueden ser difíciles. Las "tuberías" de Stevens son en realidad una forma de expresar la idea de "canales", una analogía utilizada por los expertos de la industria para describir las conexiones de datos. Respecto a este concepto de ciberespacio, el

Reglamento 2645/2014 dice: Otro aspecto relacionado con el nuevo paradigma tecnológico y de las tecnologías de la información es la importancia adquirida del ciberespacio para el desarrollo de operaciones militares. La dimensión del ciberespacio, al carecer de una localización física específica, provoca un replanteamiento de las categorías tradicionales de "guerra real" y exige una rápida adaptación de los sistemas de defensa según sus componentes debido a la dinámica de la innovación tecnológica. En las últimas décadas, muchos países han dirigido sus esfuerzos y recursos a proteger no sólo los espacios tradicionales (tierra, mar y aviación) sino también el ciberespacio. No se trata de un "espacio en sí mismo", sino de una dimensión que trasciende dichos espacios físicos con sus propias herramientas y reglas. Es un nuevo campo o dimensión para la guerra, que es muy influyente para los demás campos o dimensiones, ya que permite anticipar la acción del enemigo al obtener información de los planes de manera anticipada e incluso tiene la capacidad de neutralizar los ataques, dañando los equipos tecnológicos mediante ataques cibernéticos o en el espacio cibernético. (Arias A, 2019)

El espacio cibernético es, sin duda, uno de los fenómenos más impactantes y transformadores de la era contemporánea. Su esencia trasciende las barreras físicas y redefine la manera en que vivimos, nos comunicamos y gestionamos nuestras sociedades.

En resumen, el espacio cibernético es un doble filo: una fuente inagotable de innovación y oportunidades, pero también un campo de juego donde la seguridad y la ética deben ser prioridades. Navegar por este espacio requiere una comprensión profunda de sus dinámicas y la adopción de enfoques equilibrados que fomenten el progreso sin comprometer valores fundamentales

2.2.1.3. La virtualización de la inteligencia y la constitución del sujeto

Habiendo explorado previamente las funciones de virtualización, ahora destaco su objeto, o más específicamente, su aspecto de objeto, como una implementación de la virtualización. Aquí se entrelazan cuatro temas: la parte colectiva de la cognición, la afectividad personal, la cuestión del "pensamiento colectivo" como tal, y la

inteligencia colectiva como utopía tecno política. La complejidad del objeto y del sujeto de la inteligencia colectiva sólo puede justificarse en la segunda discusión. Los humanos nunca pensamos solos o sin herramientas. Cuando el colectivo piensa en nosotros: ¿Podemos pretender que existe un pensamiento actual y efectivo sobre los grupos humanos? ¿Podemos hablar de inteligencia sin conciencia unitaria o de pensamiento sin subjetividad? ¿Hasta qué punto es necesario redefinir los conceptos de pensamiento y psiquis para que sean compatibles con las sociedades? Se dice que nos convertimos en las neuronas de la hipercorteza planetaria. Por lo tanto, es necesario aclarar estas cuestiones y resaltar las diferencias entre las formas de inteligencia colectiva, especialmente aquellas que separan a las sociedades humanas de los hormigueros y las colmenas.

En este sentido, se establecen varios objetivos de defensa nacional, basados en el análisis del entorno interno y externo utilizando métodos del futuro.

2.2.1.4. Ciber espionaje estratégico para su economía y Defensa Militar.

El ciberespacio, es uno de los campos donde se ha permitido el avance de los diferentes factores sociales, culturales, militares, económicos, tecnológicos y educativos, evolucionando el mundo actual a grandes velocidades, creando una nueva era, la era del internet de las cosas "Internet of Things", donde esa gran era ha permitido la conexión y comunicación a nivel mundial, generando que la información y los sistemas informáticos tanto como hardware y software sean uno de los activos estratégicos más importantes dentro de una organización o estado, apareciendo el cibercrimen hacia las organizaciones estatales o gubernamentales y privadas, donde los cibercriminales pueden obtener este gran activo estratégico para obtener beneficios. La modernidad tecnológica nos agiliza en el funcionamiento de las actividades; sin embargo, nos genera un mayor riesgo para los ataques cibernéticos. Es una espada de doble filo. *(C. Sanabria C ,2018).*

El ciberespionaje estratégico representa un desafío contemporáneo que trasciende las fronteras físicas y se infiltra en los cimientos mismos de la seguridad nacional y la economía de un país. plantea desafíos multifacéticos que requieren

respuestas coordinadas a nivel nacional e internacional. La protección de la información económica y de defensa es esencial para preservar la soberanía y la estabilidad en un mundo cada vez más interconectado.

2.2.2 Ciberseguridad

2.2.2.1. Ciberataque.

Realmente es complicado dar una definición exacta porque depende de muchas variables, y sobre todo si la definición se pretende crear para la aceptación en la comunidad internacional, ya que entre las naciones tienen conceptos diferentes en la mayoría de los sentidos, (*Singer & Friedman, 2014)*. El término ciberataque se ha aplicado a todo tipo de actividades "extrañas" dentro de los confines del Internet, desde protestas en línea hasta operaciones militares reales en campos de batalla reales. Los propios expertos también deben dar una definición más que correcta al concepto debido a la poca importancia de los conceptos. Cualquier actividad maliciosa que implique el uso de Internet generalmente se denomina ciberataque. Para intentar definirlo bien, debemos empezar a distinguirlo de un ataque "normal" (físico), *(Singer y Friedman, 2014)*. La primera diferencia que encontramos es la fuerza utilizada en los ataques, mientras que en un ataque tradicional utilizamos fuerzas cinéticas como usar una bomba o una espada y por lo tanto está relacionado con la física y el terreno donde se encuentran. Mientras que en un ciberataque se usa cualquier tipo de acción informática de cualquier fuerza, y no tiene fronteras y es apolítico, queriendo decir que no proviene de una sola ideología, esto quiere decir que puede estar en múltiples lugares a la misma vez y propagarse en cuestión de segundos. *(Singer & Friedman, 2014)*. En la era digital, como lo refiere Singer, los ciberataques se han erigido como una amenaza omnipresente, desafiando la seguridad de sistemas informáticos a nivel global. Estos ataques, perpetrados por actores variados, van desde intrusiones a redes corporativas hasta la propagación de malware. El impacto va más allá de lo tecnológico, afectando la seguridad nacional, la privacidad individual y la estabilidad económica. La evolución constante de las tácticas cibernéticas demanda respuestas ágiles y estrategias de defensa robustas para proteger la integridad de la información digital y salvaguardar la infraestructura crítica. La colaboración

internacional y la concienciación pública son esenciales para hacer frente a este desafío en constante evolución.

Hay muchas maneras para llevar a cabo un ciberataque, ya sea por ejemplo infectando los ordenadores o las redes con virus y gusanos que controlen, ralenticen o dañen los ordenadores; o bien mediante la explotación de los programas espía para encontrar posibles puntos débiles dentro del sistema, o robar la información; enviando ataques de denegación de servicio (DDoS), con o sin la ayuda de Botnets, para saturar tanto páginas web como redes e infraestructuras críticas. Los ciberataques no provocan daños físicos a los ordenadores, como ocurriría si usáramos otro tipo de armas, como destruirlos con pistolas o explosivos. Por lo tanto, los ciberataques siempre se llevan a cabo en el ciberespacio. El ciberespacio incluye Internet, infraestructura de telecomunicaciones y sistemas informáticos.

Por otro lado, está el hacktivismo, entendido como el uso ilegal o jurídicamente ambiguo de recursos y herramientas digitales, normalmente con fines políticos. Las herramientas más comunes en este tipo de prácticas son: la desfiguración de páginas web, ataques de denegación de servicio, el robo de información o la paralización de páginas web. (Hacktivismo, s.f.).

Se entiene como una forma de protesta digital donde individuos o grupos utilizan habilidades informáticas para promover causas sociales, políticas o medioambientales. Los hacktivistas, a menudo operando bajo el manto del anonimato, emplean técnicas de ciberseguridad para desafiar sistemas y plataformas en línea en busca de visibilidad y cambio. Aunque algunas acciones hacktivistas buscan revelar información sensible para exponer la corrupción o injusticias, otras levantan cuestionamientos éticos sobre la legalidad y los límites de la protesta digital. Este fenómeno destaca la intersección compleja entre la tecnología, la libre expresión y la responsabilidad social en el ciberespacio.

2.2.2.2 Traslación del conflicto a la dimensión virtual.

El ciberespacio debe entenderse como un conjunto de dispositivos de Internet donde se almacena y se utiliza información electrónica y como un espacio donde se llevan a cabo diversas actividades de comunicación. Otro enfoque que debemos darle a la definición de ciberespacio es comprender su naturaleza y finalidad, la última de las cuales es el procesamiento, manipulación y uso de la información que facilita y mejora la comunicación entre las personas e interacción entre personas y la información. De ahí se desprende la idea de que tanto la información como las personas son elementos fundamentales en la composición del ciberespacio, por tanto, individuos e información son susceptibles de sufrir amenazas o presentar vulnerabilidades (Martin R, Stytz.; Sheila B. Bank 2014).

Según lo leído La traslación del conflicto a la dimensión virtual ha emergido como un fenómeno intrincado en la era digital, donde los enfrentamientos tradicionales encuentran una extensión en el ciberespacio. Este proceso implica la utilización estratégica de herramientas y tácticas digitales para perpetrar acciones hostiles, ya sea en forma de ciberataques, guerra de información o desestabilización de infraestructuras críticas. La naturaleza anónima y la capacidad de operar a escala global confieren a esta traslación un carácter complejo, desafiando las convenciones tradicionales de la guerra y planteando interrogantes sobre la seguridad nacional en un mundo cada vez más interconectado. Este fenómeno resalta la necesidad urgente de marcos normativos y estrategias de ciberseguridad que aborden eficazmente las dimensiones virtuales de los conflictos contemporáneos.

2.2.2.3. Riesgos o amenazas de la ciberseguridad.

Los ataques cibernéticos utilizan vulnerabilidades de las tecnologías de la información para copiar, eliminar o sobrescribir los datos de la víctima y explotar las vulnerabilidades en la mayoría de las estructuras cibernéticas, como las redes sociales. En el siglo XXI, los bits y los bytes pueden ser tan peligrosos como las balas y las bombas11. El número y la variedad de los ciberataques pueden crecer enormemente debido al continuo desarrollo y metamorfosis de las herramientas informáticas, que son cada vez más complejas. (Sanger, etc., 2015).

Los riesgos y amenazas en ciberseguridad constituyen una preocupación crucial en la era digital, donde la interconexión global ofrece oportunidades tanto para la innovación como para la vulnerabilidad. Desde ataques de malware y phishing hasta intrusiones más sofisticadas, los ciberdelincuentes explotan brechas de seguridad con consecuencias que van desde la pérdida de datos hasta la interrupción de servicios críticos. La amenaza constante de ciberataques contra sistemas gubernamentales, empresas y usuarios individuales subraya la necesidad de estrategias de defensa robustas, la implementación de prácticas de ciberseguridad sólidas y la colaboración internacional para mitigar eficazmente estos riesgos en evolución constante.

- Código malicioso: Esta es la amenaza más común en el ciberespacio. También conocido como código malicioso o malware, su objetivo principal es alterar el correcto funcionamiento de cualquier hardware informático, ya sea deshabilitando el sistema operativo o controlando la memoria.

- Gusano: Son códigos maliciosos que se clasifican como independientes porque están diseñados para copiarse a sí mismos, es decir. hacer copias de sí mismo y enviarlas a todas las computadoras conectadas a través de una red.

- Virus: Consiste en un programa que está diseñado para copiarse a sí mismo con el fin de infectar otros programas o archivos.

- Troyano: Este es un software que generalmente parece inofensivo o realiza tareas necesarias para el usuario, pero en realidad su propósito es robar o destruir datos almacenados en el dispositivo.

- Botnet: Es un conjunto de software que permite realizar ataques de denegación de servicio, fraude, robo de datos, desactivar sistemas antivirus o de detección de intrusos o interrumpir el comercio electrónico.

- Bomba Lógica: Son ciberataques que no están diseñados para propagarse ni operar de forma continua, sino para actuar en un momento predeterminado por el atacante. Así, su duración está limitada en el tiempo, desempeñando sus funciones nocivas sólo cuando se alcanza un tiempo o número de visitas previamente acordado. Los atacantes pueden clasificarse en diferentes categorías, como por perpetrador o instigador.

- Los atacantes se pueden clasificar según diferentes categorías como autoría o motivación. Pero es precisamente en base a la identidad de los autores que podemos clasificar a los posibles atacantes de una manera más robusta y procesable, permitiéndonos interpretar este nuevo escenario de conflicto: (Torrecuadrada, Soledad; 2013). Se considera a los atacantes como Hackers de sombrero negro o blanco, según sus intenciones; siendo los blancos los q buscan ayudar a las mejoras tecnológicas y los del sombrero negro, los que desean básicamente lucrar o dañar equipos tecnológicos de relevancia para el Estado por demostrar sus capacidades.

- Estados: Si bien puede parecer alarmante, el hecho de que los Estados puedan ser la fuente de tantas amenazas cibernéticas resulta en un aumento significativo en la complejidad de las situaciones en el ciberespacio. Esta situación demuestra que muchos países, como China, Rusia, Estados Unidos o Israel, Ya son conscientes de las ventajas comparativas que puede aportarles el desarrollo de armas cibernéticas, por lo que podemos predecir que el crecimiento exponencial de la sofisticación de los ataques cibernéticos se verá aún más exacerbado por las inversiones de los países.

- Terrorismo: Los conflictos tradicionales y sus actores se han trasladado al ciberespacio como un nuevo escenario de encuentro. Permite a las organizaciones terroristas y a las organizaciones extremistas religiosas buscar en el ciberespacio escenarios de ataque, promover, reclutar o adoctrinar a terroristas potenciales.

- Empresas: No hay que olvidar a estos actores económicos como una de las principales fuentes de ciberataques: el espionaje industrial y el espionaje comercial.

- Crimen organizado: La desmaterialización de las transacciones en el ciberespacio, la gran cantidad de recursos en la nube, el fracaso de los sistemas de negocios electrónicos y de los mercados financieros y la falta de un marco legal armonioso entre los países permiten enfrentar las amenazas provenientes del ciberespacio. Por otro lado, llama a las redes criminales organizadas a considerar el ciberespacio como un entorno favorable para el desarrollo de sus actividades. Un ejemplo es la banda Carbanak, que logró robar 876 millones de euros de 100 bancos e instituciones financieras en 30 países13.

- Hacktivismo: Este fenómeno, también conocido como piratería informática, puede explicarse por el uso de herramientas informáticas para la acción política no violenta, es decir utilizar los medios y herramientas que ofrece el ciberespacio para llevar a cabo protestas políticas, económicas o sociales de alto nivel. La naturaleza de sus herramientas va desde la manipulación hasta el robo de datos y el sabotaje virtual. Esta situación demuestra que muchos países, como China, Rusia, Estados Unidos o Israel, se han dado cuenta de las ventajas comparativas que les puede aportar el desarrollo de ciberarmas, por lo que podemos predecir que la sofisticación de los ciberataques seguirá creciendo exponencialmente, reforzado aún más por inversiones de varios países.

2.3 Definición de términos

2.3.1. Riesgo.

Es la medida de probabilidad en la que un suceso de peligro inminente pueda tomar

efecto en algún lugar determinado y llegar a perjudicar a uno o más individuos; esto quiere decir, que mide qué tan vulnerable es el entorno y los individuos en el mismo, de resultar afectados. Esto considera el alcance de daños que dicho suceso de riesgo pudiese ocasionar.

Es importante diferenciar ciertos conceptos que están relacionados y en ocasiones tienden a generar confusión respecto al término "riesgo", ya que éste se refiere a la medida de daños probable; pero, por ejemplo, vulnerabilidad se refiere a la probabilidad de daños que la situación de peligro ocasione; y peligrosidad se refiere a la probabilidad de que la situación de peligro ocurra.

Existen distintos tipos de riesgos en la cotidianidad, y un ejemplo de riesgo son los riesgos de las redes sociales; un nuevo tipo que se ha incrementado en los últimos años con la presencia de la tecnología en el día a día. (Martínez, 2023).

2.3.2. Ciberseguridad

La ciberseguridad es un conjunto de medidas y prácticas diseñadas para proteger los sistemas informáticos, redes y dispositivos electrónicos contra amenazas cibernéticas. Estas amenazas pueden ser ataques maliciosos, virus o malware que intentan acceder a información confidencial, robar información personal o corromper archivos importantes. En resumen, la ciberseguridad se centra en mantener la privacidad y seguridad de su información digital. Esto incluye todo lo relacionado con tu identidad digital: contraseñas, correos electrónicos, perfiles de redes sociales e información financiera. La ciberseguridad es importante para mantenernos seguros mientras navegamos por Internet y utilizamos dispositivos electrónicos en nuestra vida diaria. Por eso los profesionales especializados en ciberseguridad tienen una gran demanda. (Escrivá Gascó, G., 2013).

2.3.3. Amenazas.

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información, las amenazas surgen a partir de la existencia de

vulnerabilidades; es decir, que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. (DoD. 2018).

Diversas situaciones, como el incremento y mejora de las técnicas de ingeniería social, la falta de formación de los usuarios y de sensibilización en el uso de la tecnología, y especialmente el aumento de la rentabilidad de los ataques, han provocado un aumento de las amenazas intencionadas en los últimos años.

2.3.4 Traslación

Acción de trasladar o trasladarse de lugar. "Los gastos para la entrega de la cosa vendida serán de cuenta del vendedor, y los de su transporte o traslación, de cargo del comprador, salvo el caso de estipulación especial". (Real academia española,2023). Capacidad de realizar una acción en el espacio cibernético desde un punto o ubicación, pero hacer aparentar que se realiza esta o varias acciones similares desde otro lugar o varios lugares o ubicaciones diferentes. (Sutton, D., 2017).

2.3.5. Ciberataque

En un contexto cada vez más digitalizado y con nuevas iniciativas de tecnologías de la información, está surgiendo una economía digital que conecta a diversos actores sociales, cuyo objetivo es crear nuevos ecosistemas de negocios donde sea posible realizar oportunidades, ganancias y experiencias sin precedentes para diversos intereses o grupos. En este sentido, la inseguridad digital que representan los ciberataques se configura como un impuesto progresivo que grava la confianza digital de los consumidores y crea áreas de incertidumbre que afectan la dinámica comercial y el bienestar económico de los países. Por ello, este artículo desarrolla una reflexión conceptual sobre este nuevo impuesto progresivo y las ideas para evitarlo en un entorno cada vez más digital y tecnológicamente cambiante. (Roa Buendía, J. F., 2013)

2.3.6. Ciberespionaje

Hasta ahora, "la amenaza parece tener poco que ver con el ciberespionaje" - Nada más lejos de la verdad - El espionaje puro es sólo la punta del iceberg, la implementación de las medidas específicas para cada amenaza descritas en el capítulo anterior requiere la recopilación de información previa. En tiempos de paz, los adversarios pueden sondear los sistemas de información de gobiernos, universidades y empresas privadas, identificar objetivos clave, buscar vulnerabilidades y utilizar "puertas traseras" para utilizarlas en una crisis o confrontación. Como se puede concluir, estas actividades son actos de espionaje.

Un ejemplo sorprendente de este enfoque sobre las intrusiones antes mencionadas son las realizadas en sitios web oficiales de la India. Un posible resultado podría ser la identificación de vulnerabilidades y objetivos futuros, eliminando posibles fugas de datos. Este potencial ya es suficiente para crear desconfianza y hacerme sentir amenazado. Según los expertos en ciberseguridad y seguridad nacional de la India, el espionaje industrial se considera una prioridad para el ciberespionaje chino. La razón es que reduciría gastos y tiempo en el esfuerzo chino para construir un ejército e industria militar modernos. (Brodie, 2008).

CAPÍTULO III: DESARROLLO DEL TEMA

"***Creación de puestos de comando en Ciberdefensa y Ciberseguridad a nivel Ejército del Perú"***

3.1. Campos de Aplicación

Los campos donde se asigna la investigación son en la IV DE - CVRAEM – Pichari – Cuzco, en la II DE – Agrupamiento de Comunicaciones "José Olaya" - Arequipa - Tiabaya y Cuartel General del Ejército - Lima, estas dos Divisiones y una Unidad del Ejército son zonas estratégicas para crear puestos de comando de ciberdefensa y ciberseguridad en nuestro país; así mismo, el autor laboró en estas unidades y evaluó las necesidades y las zonas estratégicas de la creación de puestos de comandos estratégicos.

La Línea de Investigación es "El empleo de la Ciberdefensa y Ciberseguridad en el Ejército del Perú"

3.2. Tipos de aplicación

El autor de este estudio se basa en su propia experiencia en la II DE – Agrupamiento de Comunicaciones "José Olaya" – Arequipa – Tiabaya; trabajó como Jefe de Pequeña Unidad en la Compañía de Comunicaciones N° 8, perteneciente al Agrupamiento de Comunicaciones "José Olaya", donde pudo observar la necesidad de implementar al menos un (01) Puesto de Comando de Ciberdefensa y Ciberseguridad con unidades, equipamiento y personal capacitado en la ciberseguridad y ciberdefensa de nuestra nación a través del Ejército del Perú. Actualmente la tecnología está avanzando de manera muy acelerada a nivel mundial, en diversos Ejércitos los ataques cibernéticos en diferentes países es un denominador muy común. El Ejército del Perú en la actualidad no cuenta con alguna unidad implementada para hacer frente a un ciberataque. Por temas presupuestales, no existe una implementación adecuada; además, no hay personal capacitado que

pueda estar al frente de estas compañías a diferencia de otros países, que ya han implementado sus puestos o se están preparando para ello. Estos son factores que limitan el desarrollo de la capacidad funcional de los puestos de comando en ciberdefensa y ciberseguridad que existen actualmente; sin embargo, se puede superar estos factores a través de la implementación de estos puestos de comando y adicionar la capacitación del personal en las tres regiones propuestas.

El tipo de aplicación a ejecutarse con esta propuesta será en lo *administrativo y logístico* en lo que refiere a implementación y se desarrollará en el campo de trabajo *táctico y operacional*, según el escalón al que se le asigne la misión.

3.3. Diagnóstico

El diagnóstico desde el cual partió este proyecto de estudio se refiere a la falta de implementación en ciberdefensa y ciberseguridad, a su vez a la lucha constante contra la permanente evolución tecnológica. Los altos costos de los equipos, software y la falta de conocimiento del personal en los avances tecnológicos actuales, en ciberataques y ciberdefensa, nos coloca en una posición de desventaja ante los demás países frente a estos ataques tecnológicos, principalmente por no darle la importancia que merece al campo de la ciber tecnología.

Durante el periodo en el que el autor estuvo presente en el Centro de Ciberdefensa, se identificaron importantes carencias en las instalaciones, como la división del espacio en cuatro ambientes de triplay y la presencia de computadoras obsoletas sin el software necesario para realizar las funciones del centro. Además, se carecía de documentación que respaldara las operaciones del centro. Durante el transcurso del año, se llevaron a cabo mejoras significativas, que incluyeron el amoblamiento de las oficinas, la mejora de la capacidad de las computadoras y la adquisición de presupuesto para la compra de licencias que permitieran el escaneo de la red y el monitoreo de amenazas cibernéticas. A pesar de estos avances, el Centro de Ciberdefensa del Ejército del Perú, actualmente ubicado en el Cuartel General del

Ejército, en el pentagonito de Av. Paseo del Bosque Nº 740, en el Distrito de San Borja, Provincia de Lima, enfrenta desafíos continuos, como la desactualización del personal, la falta de software y la carencia de equipos sofisticados, siendo actualmente la única instalación de defensa cibernética con la que cuenta el Ejército del Perú.

En los últimos años el Ejército del Perú sufrió diversos ataques cibernéticos donde se filtró información clasificada; así mismo, instituciones del estado como la ONPE en el año 2018 que fue víctima de hackers donde filtraron los nombres, apellidos, fecha de nacimiento, sexo y edad de todos los peruanos mayores de edad estos datos fueron accesibles y descargables a través de la página web de la ONPE, otro programa hacker fue Pishinhg de Ingeniería social. El Phishing es el ciberataque que más aumento en el Perú a raíz de la pandemia. Hackean web del Bono Universal, Hackean web del Bono Familiar Universal y roban cerca de un millón de soles a personas en situación vulnerable, otro ataque hacker de datos clasificados es Anonymous quien se atribuye el hackeo al Congreso Peruano, Anonymous se atribuyó un hackeo al portal web del Congreso y amenazó a Manuel Merino con filtrar sus conversaciones, contratos y negociaciones. Estos son los ataques de hacker más resaltantes en estos últimos años.

3.4 Propuesta de Mejora

Con base en la experiencia profesional del autor, la situación problemática observada, los antecedentes encontrados en investigaciones similares, las bases teóricas correspondientes a las variables de estudio expuestas en el marco teórico, se presenta una propuesta de mejora con *alternativas de solución* para el problema investigado titulada: "*Creación de puestos de comando en ciberdefensa y ciberseguridad en el ejército del Perú*".

3.4.1. Objetivo general de la propuesta

El objetivo es diseñar e implementar eficientemente puestos de comando en ciberdefensa y ciberseguridad en el Ejército del Perú, para proteger en tiempo real la

información de la nación evitando riesgo de pérdidas o sabotaje de estructuras de alto valor que dispone el Estado.

3.4.2. Objetivos específicos

Los objetivos trazados en la siguiente propuesta son:

- Crear puestos de comando en ciberdefensa y ciberseguridad; para mantener la información de la nación segura y sin riesgo de pérdidas.

- Mejorar la capacidad en ciberdefensa, para detectar y anular las diversas amenazas virtuales y guerras cibernéticas.

- Mantener la seguridad de información, reducir o anular el robo de información o incluso la eliminación de la información mediante ataques cibernéticos.

- Impulsar la capacidad de ciberataque, que permita rechazar o iniciar una anulación cibernética contra un enemigo identificado.

- Avanzar a la par de la tecnología, permitiendo que el país se encuentre a la vanguardia con otros países que en la actualidad tienen una capacidad tecnológica mayor que el nuestro.

- Defender nuestras capacidades tecnológicas.

3.4.3. Descripción y presentación de la propuesta

La creación de puestos de comando en ciberdefensa y ciberseguridad en el Ejército del Perú; evita que nos expongamos a riesgos cibernéticos y por ende a robo de información, una implementación en ciberdefensa y ciberseguridad nos permite mejorar las capacidades operativas, incluso ante ciertas restricciones coyunturales.

Actualmente el ejército del Perú cuenta con un sistema de Software que nos permite dar cierta protección a nuestra información, como son: NESSUS, BURPSUITE y UP TIME ROBOT; estos son los tres programas que se utilizan, pero a la fecha están *desactualizadas por falta de licencia*. Esta es una situación que sucede con frecuencia, no se cuenta con programas de ciberataque y el porcentaje de ataques que se sufre es alto y consecutivo, como se describe líneas arriba los ataques van dirigidos a diversas instituciones del estado como, ONPE y los pagos a bono familiar universal; así mismo, también se realizan ataques a diversos bancos del país y robos de información confidencial como conversaciones personales de diversos congresistas.

Estos ataques se vienen dando por grupos de delincuentes de hacker que venden la información a grupos de interés o la usan para beneficios propios. En este sentido se recomienda *tres áreas principales de la ciberseguridad*: La *seguridad de la red*, la seguridad *de la nube* y la *seguridad física*. Los sistemas operativos y la arquitectura de red dan forma a la seguridad de su red. existen servidores como el CLOUD, éste es un programa para dar seguridad en la nube; COFENSE TRIAGE es un software de seguridad especializado en protección contra phishing o robo de identidad. Como sugiere el nombre, utiliza un método llamado triaje, un sistema de cribado o protocolo de intervención utilizado en muchos campos, especialmente el sanitario, para crear y clasificar listas de pacientes. En este caso, el programa funciona como un dispositivo virtual que puede conectarse al correo electrónico en busca de ataques de phishing; Kali Linux, software de seguridad Linux con varias herramientas de análisis para proteger su computadora o red informática. Gracias a este programa es posible detectar ataques y amenazas e incluso seguir el rastro dejado por el hacker.

En seguridad de los equipos también se verificará el filtro de información por acceso de personal, también conocido como sistema biométrico, que permite identificar de manera más minuciosa la identidad del personal que intenta ingresar a la instalación o manipular algún equipo, anulando el acceso a la información si no fuera la persona autorizada.

En ciberataques, Los países tienen programas de ciberataques que lo usan en casos de búsqueda de información ilegal vulnerando de esa manera información confidencial de países colindantes o instituciones nacionales y extranjeros, *ante esto se está proponiendo* la adquisición del programa para evitar los robos de información.

Los spywarees son un tipo de malware que se esconde en su dispositivo, rastrea sus actividades y roba información confidencial como información financiera, información de cuentas, contraseñas y más; El software espía puede propagarse aprovechando las vulnerabilidades del software o junto con programas legítimos o troyanos. Para estos programas se recomienda la adquisición de dos programas malware:

a) Cool Web Search: Este programa utilizó agujeros de seguridad en Internet Explorer para secuestrar el navegador, cambiar su configuración y enviar datos de navegación a su creador.

b) Gator: Generalmente viene con un software de transferencia de archivos como Kazaa. Este programa monitorea los hábitos de navegación de la víctima y utiliza los datos obtenidos para mostrarle anuncios específicos.

- Una vez adquirido estos programas, se captará personal capacitado para estas labores y se capacitará con la misma empresa que venda los programas.

- Seguido a esto se armará el primer Batallón de Ciberdefensa y Ciberataque del Ejército del Perú.

- Una vez captado y capacitado al personal que se encargará de manipular estos datos, se propone descentralizar en dos regiones del Perú en la IV DE- Cvraem – Pichari – Cuzco y en la II DE – Agrupamiento de comunicaciones "José Olaya" – Arequipa – Tiabaya, teniendo así tres (03) sedes con unidades de ciberataque y ciberdefensa.

3.4.4. Elementos para el desarrollo de la propuesta

Para realizar esta propuesta se requiere de cinco (05) elementos: software, equipos modernos, personal, capacitadores e infraestructura.

Tabla 1.

Elementos para el desarrollo de la propuesta

Elementos	Descripción
SOFTWARE	Seguridad de la red: COFENSE TRIAGE es un software de seguridad. Seguridad de la nube: CLOUD este es un programa que protege la información en la nube. Seguridad física: LINUX Este es un programa que brinda seguridad al software. CoolWebSearch: Este programa aprovechó los agujeros de seguridad en Internet Explorer. Gato: Generalmente viene con un software de transferencia de archivos como Kazaa.
EQUIPOS	Lenovo ThinkStation P620, accesorios de control, memorias extensibles, traductores digitales, redes de conexión, accesorios de escritorio, accesorios cibernéticos.
PERSONAL	El personal que se requiere es, personal capacitado en manejo e instalación de los programas, personal militar con perfil para conformar los puestos de comando.
CAPACITADORES	Personal militar capacitado en manejo e instalación de los programas que capaciten a empleados que trabajan en unidades de ciberdefensa y ciberataque; asimismo, el personal de capacitadores se encontrará en constante capacitación.
INFRAESTRUCTURA	Proteger el servicio del cliente y la infraestructura de red de Internet utilizando una plataforma de seguridad implementada para el perímetro de la red, infraestructura de los puestos de comando impermeable contra redes y contaminación de sonido del medio ambiente.

Nota. Elaboración propia, (2023)

CONCLUSIONES

1. En este trabajo, una vez analizada la situación actual, se podrá crear hasta tres puestos de comando que protegerán la información secreta del país y lo defenderán contra ciberataques. Se define equipos de detección y respuesta a ataques cibernéticos implementando los sistemas adquiridos los cuales deberán mantenerse siempre actualizados y evitar que sean afectados por los cambios tecnológicos. Asimismo, se generará una política de ciberseguridad que ayudará a mantener la seguridad física de la información.

2. En el mundo actual casi no hay ámbito social donde no exista este fenómeno, los sistemas de información ya existen y este uso parece continuar y aumentar por lo que habrá más en el futuro. Estas tecnologías ya desempeñan un papel importante e irremplazable en muchas organizaciones, incluida la infraestructura crítica del país. Por tanto, La red de estas infraestructuras es considerada una de las más vulnerables hoy en día, y al mismo tiempo, el ciberespacio se está convirtiendo en uno de los ámbitos de seguridad y defensa más exigentes y avanzados en la actualidad. En las nuevas directivas de protección, las ciberamenazas ya se consideran un riesgo nacional.

3. De este trabajo también podemos concluir que la tecnología avanza a pasos agigantados; por lo tanto, los líderes o altos mandos deben prestar atención a estos cambios para seguir el ritmo de las herramientas de defensa y seguridad de la red. Actualmente, los ciberataques y las violaciones de la información de seguridad son muy comunes. Es fácil para la seguridad civil, los ciberdelincuentes o los piratas informáticos violar la información de diversa

4. Como se mencionó anteriormente, las fuentes de ataques no son uniformes. Estos pueden ser actos de terroristas, criminales o estados, por lo que es necesario un esfuerzo multidisciplinario. Por eso existen diferentes unidades para combatir amenazas de diversas fuentes. En este contexto, no cabe duda del papel que pueden desempeñar las Fuerzas Armadas en defensa del ciberespacio

o su uso como vector de ataque. En cualquier caso, las Fuerzas Armadas son una parte importante de la ciberdefensa, porque su infraestructura es una de las denominadas infraestructuras críticas, que a su vez depende de otras infraestructuras críticas, además de una amplia utilización de la tecnología de la información.

RECOMENDACIONES

1. La ciberseguridad de una organización depende de muchos factores tecnológicos, humanos y de los estándares que la regulan, diseñar una política de ciberseguridad para el área de servicios de seguridad es muy importante para asegurar el compromiso de toda la organización. gestión de cada empleado.

2. Crear estrategias para una capacitación continua en ciberseguridad que sea obligatoria para todos los empleados que conozcan las prácticas centrales en este tema, ya que son un filtro importante de la ciber información corporativa que debe ser protegida y asegurada por las instituciones.

3. Organizar un monitoreo constante del uso de claves protegidas, lo suficientemente prolongado y robusto como parte de la política de protección, donde los usuarios tengan acceso a entornos protegidos, bloqueen páginas de navegación, listas negras y también implementen copias de seguridad programadas del sistema en caso de un ataque de Ransomware porque le permite eliminar la máquina infectada y actualizarla con la última copia de seguridad. Previene: los traumas, las crisis y sobre todo los ciberdelitos no se alimentan.

4. Crear tres (03) puestos de comando para la protección de la información nacional en el ciberespacio. Actualmente cuando una entidad del estado recibe un ciber ataque, solo se opta por apagar los equipos y pagar el monto que exige el hacker para la reactivación del sistema anulado. Implementando los puestos de comando, capacitando al personal, adquiriendo los equipos necesarios y generando las normativas requeridas se podrá poner fin a esta gran vulnerabilidad nacional que se tiene.

REFERENCIAS BIBLIOGRÁFICAS

1. OEA y BID (2020), "Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe", Reporte Ciberseguridad 2020, p. 11.

2. Unión Internacional de Telecomunicaciones (2021), "Índice Mundial de Ciberseguridad", p. 9.

3. J Quevedo L. C, 2023; Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional - Revista de Ciencia e Investigación en Defensa – CAEN - 10.58211/recide.v4i1.99 VL - 4.

4. R Vargas B, L Recal H, R Reyes Ch;2017; Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa Ecuador.

5. A Herrera L, 2017. LA INTELIGENCIA DE COMBATE EN LA I GUERRA MUNDIAL Revista de la Escuela Conjunta de las Fuerzas Armadas. Edición: Año 5 Núm. 3 - IAKOB Comunicadores & Editores S.A.C. Jr. Ica –LIMA.

6. Gómez, Ángel (2012): "El ciberespacio como escenario de conflicto. Identificación de las amenazas", en El ciberespacio. Nuevo escenario de confrontación, Madrid, Ed. Ministerio de Defensa, pp. 167-204.

7. Torrecuadrada, Soledad (2013): "Internet y el uso de la fuerza", en Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio, Granada, Ed. Universidad de Granada, pp. 91-118. 13.

8. Sanger, David and Perloroth, Nicole: "Bank Hackers Steal Millions via

Malware", New York Times, 14 February 2015, en http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-viamalware.html?_r=1.

9. Martin R, Stytz.; Sheila B. Bank (2014): "Cyber Warfare Simulation to Prepare to Control Cyber Space". National Cybersecurity Institute Journal, vol 1, Nº2. P. 9.

10. César Augusto Sanabria Casanova Universidad Nacional Abierta y a Distancia Publicado 2018-12-21 Número Vol. 10 Núm. 19 (2018) Sección Tecnología y desarrollo Revista Científica Perspectivas en Inteligencia.

11. Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" Carrera 8 A No. 101 – 33 Bogotá D.C., Colombia.

12. Stanković, N. (2019). "The conceptual analysis of identities and interests in the thought of Alexander Wendt". Politeia. 9 (18), 37-154.

13. DoD. (2018). National Cyber USA, (September) Universidad Nacional de Lujan Departamento de Seguridad Informática EN: Web: www.seguridadinformatica.unlu.edu.ar.

14. Real academia española: diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. <https://dle.rae.es> [14/08/2023].

15. Jeimy J. Cano M DOI 2020-11-26 economía digital, transformación digita, Ciberataque Asociación Colombiana de Ingenieros de Sistemas. EN: https://doi.org/10.29236/sistemas.n157a6.

16. Brodie, 2008) The Importance of Security Awareness Training, SANS Institute Infosec Reading Room, 30 de junio de 2008, consultado el 28 de enero de 2009, en:

http://www.sans.org/reading_room/whitepapers/awareness/rss/the_importance_of_security_awareness_training_33013).

17. Jeimy J. Cano M DOI, 2020 – 11 – 26; economía digital, transformación digital, Ciberataque - Asociación Colombiana de Ingenieros de Sistemas. En: https://doi.org/10.29236/sistemas.n157a6).

18. DoD. 2018, National Cyber USA, (September) Universidad Nacional de Lujan Departamento de Seguridad Informática en Web: www.seguridadinformatica.unlu.edu.ar.

19. (Martínez, 2023) Aurora. (Última edición: 14 de junio de 2023 a las 4:41 pm). Definición de Riesgo. Recuperado de: https://conceptodefinicion.de/riesgo/. Consultado el 14 de agosto de 2023).

20. (Stanković, 2019). "The conceptual analysis of identities and interests in the thought of Alexander Wendt". Politeia. 9 (18), 37-154.

21. Brodie, Cindy: The Importance of Security Awareness Training, SANS Institute Infosec Reading Room, 2008, consultado el 28 de enero del 2009, en: http://www.sans.org/reading_room/whitepapers/awareness/rss/the_importance_of_security_awareness_training_33013.

ANEXOS

ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI

"Alma Mater del Ejército del Perú"

ANEXO 01: INFORME PROFESIONAL PARA OPTAR

EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES

1. DATOS PERSONALES:

1.01	Apellidos y Nombres	NESTARES ENCINAS CARLOS ISRAEL
1.02	Grado y Arma / Servicio	MAYOR DE COMUNICACIONES
1.03	Situación Militar	ACTIVIDAD
1.04	CIP	123419600
1.05	DNI	44177124
1.06	Celular y/o RPM	920056317
1.07	Correo Electrónico	cine87@hotmail.com

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	01 enero 2006
2.02	Fecha_ egreso EMCH	01 enero 2010
2.03	Fecha de alta como Oficial	03 enero 2010
2.04	Años_ experiencia de Oficial	14 años
2.05	Idiomas	Español

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

Nº	Año	Lugar	Unidad / Dependencia	Puesto Desempeñad
3.01	2010	AREQUIPA	BCOM Nº 113	CMDTE SECCIÓN
3.02	2013	SANTA ROSA	BCOM Nº 501	CMDTE SECCIÓN
3.03	2015	AYACUCHO	CIA COM Nº 2	CMDTE SECCIÓN
3.04	2016	PICHARI	CIA COM Nº 2	CMDTE SECCIÓN
3.05	2018	LIMA	BCOM A/M Nº 511	CMDTE COMPAÑÍA
3.06	2019	LIMA	EMCH "CFB"	CMDTE COMPAÑÍA
3.07	2020	LIMA	BCOM Nº 112	CMDTE COMPAÑÍA
3.08	2021	LIMA	CECYBER	JEFE DEPARTAMENTO DEFENSA CIBERNÉTIC
3.09	2022	AREQUIPA	CIA COM Nº 8	JEFE DE PEQUEÑA UNIDAD
3.10	2023	LIMA	EMCH "CFB"	JEFE DE SECCIÓN

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Periodo	Denominación	Diploma / Certificación
4.01	2010	Escuela de Paracaidismo	Curso Básico	Certificado
4.02	2011	Escuela de Paracaidismo	Maestro de Salto	Certificado
4.03	2012	Escuela de Paracaidismo	Caída Libre	Certificado
4.04	2014	Escuela de Comunicaciones	Guerra Electrónica	Certificado
4.05	2015	Escuela de Comunicaciones	Curso Básico	Certificado
4.06	2020	Escuela de Comunicaciones	Curso Avanzado	Certificado

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Periodo	Bachiller / Licenciado
5.01			
5.02			

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Periodo	Grado Académico (Maestro – Doctor)
6.01			
6.02			

7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Periodo	Diploma o Certificado
7.01	2022	THE CENTER FOR CYBERCRIME INVESTIGATION AND CYBERSECURITY - CENTER FOR CIC	DIPLOMADO EN PERITO CIBERJUDICIAL

8. ESTUDIOS EN EL EXTRANJERO

Nº	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01				
8.02				

FIRMA

POSTFIRMA