ESCUELA MILITAR DE CHORRILLOS

“CORONEL FRANCISCO BOLOGNESI”

IMPLEMENTACION Y SOSTENIMIENTO DE LA CAPACIDAD MILITAR DE CIBERDEFENSA EN EL CENTRO DE CIBERDEFENSA DEL EJERCITO DEL PERU

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

Autor:

EDWIN ESPINOZA FERNÁNDEZ

ORCID: 0009-0003-2708-7943

Lima - Perú

2025

16% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

16% Fuentes de Internet
1% Publicaciones
5% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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

Dedicatoria

A mi familia, quienes son la fortaleza en mi camino para superar todas mis adversidades que se presenten en el transcurrir de la vida.

Agradecimiento

A mi Escuela Militar de Chorrillos que me enseño los valores y virtudes que hoy profeso.

INDICE

Índice

Pág.

Índice de tablas

RESUMEN

El presente trabajo de suficiencia profesional surgió de la experiencia adquirida por el autor, al laborar en el Comando de Operaciones Cibernéticas del Ejército (COCIBER), como Jefe de Estado Mayor de Operaciones Cibernéticas. Unidad en la que aprendí sobre las capacidades que debe de dominar el personal del arma de Comunicaciones y del servicio de Ciencia y Tecnología del Ejército y el desempeño que debe tener en la Defensa Cibernética "Ciberdefensa" para la protección de las plataformas informáticas del Ejército del Perú, la labor que tiene que ejecutar para "preparar a la fuerza", a fin de sostener una capacidad disuasiva necesaria para la defensa de la soberanía e integridad de la nación para la protección de infraestructura critica nacional y preparar una respuesta militar, para que con orden se degrade o neutralice una amenaza en el dominio del ciberespacio. Esta investigación tiene por objetivo diseñar, implementar y sostener en el tiempo eficientemente la capacidad militar de ciberdefensa 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.

Palabras clave: Ciberdefensa, ciberespacio, infraestructura critica, capacidades de ciberdefensa, operaciones militares en el ciberespacio.

INTRODUCCIÓN

El Centro de Ciberdefensa del Ejército (Cecyber), entidad perteneciente a Ciberdefensa y Telemática del Ejército (Cítele), dependencia en la cual desempeñe el cargo de Jefe de la Defensa Cibernética de las comunicaciones del Ejército, donde pude apreciar dificultades tales como la insuficiente asignación de presupuesto, la falta de conciencia en la protección cibernética institucional y deficiencia de infraestructura y equipamiento en capacidad militar de ciberdefensa en comparación al desarrollo de este ámbito a nivel mundial.

En lo que respecta al ámbito regional, el Observatorio de Ciberseguridad de América Latina y el Caribe, es una iniciativa de la Organización de Estados Americanos y el Banco Interamericano de Desarrollo, creado con la intensión de analizar, monitorear y fortalecer las capacidades de ciberseguridad en los países de todo América. Su objetivo es generar información confrontada y actualizada que facilite evaluar el nivel de preparación de los Estados en lo relacionado a políticas nacionales de ciberseguridad, infraestructura crítica, legislación, formación de talento humano, gestión de incidentes y cooperación internacional.

En tal sentido, su fortaleza está basada en el modelo de Madurez de Capacidades de Ciberseguridad (MMCC). Su dimensión Política y estrategia de seguridad cibernética involucra su organización a fin de examinar la existencia de entidades coordinadoras nacionales y proporcionar un presupuesto integral, así como la supervisión adecuada.

El Modelo de Madurez de Capacidades Ciberseguridad es una base conceptual que facilita evaluar el nivel de desarrollo, capacidad o sofisticación de una organización, proceso o sistema mediante etapas progresivas. Es así como, cada etapa o nivel de madurez, describe un grado específico de estructuración, estandarización y mejora continua. En ese sentido, se subdivide en cinco etapas: inicial, formativa, de consolidación, estratégica y dinámica. (Organización de los Estados Americanos y Banco Interamericano de Desarrollo 2020).

El sector público de ciberseguridad de Latinoamérica Latina está en construcción. Aun cuando los avances en la dirección correcta desde finales del siglo XX, así como desarrollar una política de ciberseguridad eficaz, sigue siendo un proceso

paso a paso que continua 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 desarrolla la OEA y el BID permitió mirar dentro de la región y desde un prisma intertemporal. De acuerdo con el informe de 2020, Latinoamérica ha reformado las capacidades de ciberseguridad de los estados desde 2016. No obstante, funcionarios de las mencionadas organizaciones describen este progreso como tímido debido a que la madurez promedio de las específicas del sector varía solo entre las etapas inicial y de capacitación, ya que 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 desarrollado adecuadamente la implementación de la capacidad militar de ciberdefensa. En la actualidad, el país no cuenta con una inversión consignada a desarrollar los sistemas de seguridad y de defensa cibernética, dirigida a la defensa nacional. Aunque la región Latinoamericana tiene escasa incidencia en conflictos cibernéticos a gran escala, es esencial resaltar que la seguridad nacional podría verse vulnerada de no alinearse de acuerdo con las necesidades actuales. (Quevedo, 2023).

Para un mejor entendimiento el trabajo de insuficiencia profesional ha sido distribuido en cuatro capítulos, los cuales se han estructurado de acuerdo con el siguiente detalle:

El capítulo I, contiene la información general, cómo la dependencia dónde se desarrolló el trabajo de suficiencia profesional, 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 capítulo II, comprende los antecedentes internacionales y nacionales que enmarcan el trabajo de suficiencia profesional, que describen la realidad desde otras perspectivas del desarrollo de la capacidad militar de ciberdefensa y ciberseguridad y la concepción 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 capítulo III, se desarrolló el tema donde se explica la propuesta de mejora realizada por el autor, a esto se suma 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.

Finalmente, se establecieron las conclusiones y recomendaciones. A esto se suman las referencias bibliográficas y anexos.

CAPÍTULO I: INFORMACIÓN GENERAL

1.1 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.

1.2 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,

1.3 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.

1.4 Visión del Centro de Ciberdefensa del Ejército (CECYBER)

"Liderar la Ciberdefensa en la Región".

1.5 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".

1.6 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 trabajo de suficiencia profesional se encontraron estudios investigativos desarrollados en diversas contextos internacionales y nacionales relacionados al tema que se realizó, los cuales sirvieron para sostener la base teórica y metodológica esencial, aportando esencialmente durante la ejecución de cada paso del proceso, lo que permitió el análisis y comparación de estudios ya realizados y apoyando en la preparación de la propuesta de mejora.

2.1.1 Antecedentes Internacionales

Rubio (2016), en su investigación titulada: "*Un Marco para el Análisis de Riesgos en Ciberseguridad*", tesis desarrollada a fin de conseguir el grado 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. La metodología empleó el enfoque cuantitativo, el diseño no experimental y, se utilizó un método fundamentalmente hermenéutico, a esto se sumó el uso como instrumento la ficha de análisis de documental. Los resultados revelaron que las redes de computadoras o el conocido ciberespacio se han transformado en la cuarta dimensión entorno en el cual se pueden ejecutar operaciones militares, con ello sus primeras acciones han sido dadas en la implementación de la ciberdefensa como capacidad militar a fin de poder enfrentar al vertiginoso crecimiento de ciberataques a las redes de computadoras de las infraestructuras críticas e instituciones de valor estratégico. Se concluyó que uno de los ataques más frecuentes conducidas a instituciones de valor estratégico son los ataques de negación de servicio distribuida (DDoS), a esto se suma otras ciberarmas y métodos, teniendo en cuenta los peligros y desafíos que muestran la realidad de la tecnología en la actualidad. La investigación contribuyó que la importancia de la cuarta dimensión de las operaciones militares es una realidad, por consecuente, los Estados están obligados a priorizar las necesidades de las instituciones y la implementación de capacidades requeridas a fin de resguardar el ciberespacio de cada uno de

ellos. Finalmente, la normativa legal adecuada que consolide responsabilidades y funciones que facilite el uso legal de las capacidades requeridas a fin de proteger el ciberespacio.

Vergara y Adolfo (2017), en su trabajo investigo "Operaciones Militares Cibernéticas" - Buenos Aires, a fin de obtener el grado de Doctor en desarrollo y seguridad estratégica, el objetivo fue conocer los avances tecnológicos y el incremento de infraestructura digital que han logrado que poblaciones enteras dependan de sistemas entrelazados y complejos. El diseño de investigación desarrollado fue no experimental, correlacional y descriptivo. La técnica de acopio de data fue la encuesta. El resultado mostró que el requerimiento de Internet y de conectividad digital demandan una mayor integración de las Tecnologías de la Información y la Comunicación (TIC), a consecuencia del incremento de la dependencia a ellas. Lo cual condujo al aumentó de la vulnerabilidad frente a los ataques a infraestructuras críticas mediante el espacio cibernético, comprendiendo la situación real del dominio virtual, global y dinámico, compuesto por el hombre, integrado por las infraestructuras de tecnología de la información, las redes y los sistemas de información y de telecomunicaciones, comprendidas las de las Fuerzas Armadas. Se concluyó que el aporte a la cibernética en las operaciones militares tradicionales y, esencialmente, en lo que respecta al nivel operacional de guerra, cuando corresponde implementar la dirección estratégica. Por ello, es importante que un comandante de un Teatro de Operaciones debe saber cómo integrarlo al planeamiento y el requerimiento de este 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 TIC 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. En conclusión, la existencia de varias normativas que pretenden resguardar la seguridad de la información y cooperar internacionalmente en el entorno procesal, no obstante, una diferenciación entre ciberseguridad, ciberdefensa y cibercrimen, con tendencias y desarrollos. Esta investigación muestra el requerimiento de integrar los esfuerzos institucionales en lo que respecta a ciberdefensa. Al mismo tiempo, la gran necesidad de invertir en talento humano y medios tecnológicos.

Olech y Strucl (2025), en su libro "La Evolución de las Fuerzas Cibernéticas en los países de la OTAN", para el Centro de Excelencia de Ciberdefensa de la OTAN, El surgimiento del ciberespacio como ámbito de competencia estratégica ha transformado radicalmente el entorno de seguridad global, obligando a la OTAN y a sus Estados miembros a reevaluar continuamente los marcos, las doctrinas y las capacidades necesarias para una defensa eficaz. A medida que las ciberamenazas aumentan en frecuencia, complejidad y gravedad *(*desde el sabotaje de infraestructuras críticas hasta las campañas híbridas de desinformación), los aliados de la OTAN están acelerando el establecimiento de unidades cibernéticas especializadas dentro de sus fuerzas armadas nacionales. Estos avances abordan las necesidades de seguridad nacional y mejoran significativamente la resiliencia colectiva de la Alianza.

Este estudio ofrece un análisis exhaustivo del desarrollo de las fuerzas cibernéticas en los 32 estados miembros de la OTAN, destacando sus distintas metodologías para establecer, organizar e integrar unidades cibernéticas en sus respectivas estructuras militares y de defensa. Cada nación se evalúa en función de su entorno de ciberseguridad, el desarrollo histórico de sus unidades cibernéticas y la organización y las competencias actuales de sus fuerzas cibernéticas. La investigación indica una tendencia sólida y creciente: si bien los estados pueden desarrollar inicialmente capacidades cibernéticas para

sus intereses nacionales, el impacto conjunto de estos esfuerzos simultáneos refuerza sustancialmente el marco de seguridad colectiva de la OTAN en el ciberespacio

2.1.2 Antecedentes Nacionales

Ormachea (2019). En su trabajo de investigación "Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional", a fin de alcanzar el grado de Doctor en Desarrollo y Seguridad Estratégica, en el Centro de Altos Estudios Nacionales, (CAEN) Lima, Perú, desarrolló como objetivo proponer estrategias integradas de ciberseguridad requeridas para fortalecer la seguridad nacional del Perú, 2019. La investigación se desarrolló en base al enfoque cualitativo y el diseño no experimental, así como el empleó de un método fundamentalmente hermenéutico, como instrumentos empleados fueron la ficha de registro y la ficha de análisis. El resultado refleja que para proteger íntegramente los activos críticos e instituciones de valor estratégico en el Perú, es esencial la implementación de estrategias de ciberseguridad según categorización determinada, las que deben ser constituida entre normas y leyes que deben estar detalladas en reglamentos, asimismo, en la actualidad el Perú en lo relacionado con ciberseguridad se encuentra en un nivel de capacidad de respuesta media baja, por su parte, la Constitución Política del Perú no resguarda a la población vulnerable al acceso frente a ciberamenazas, En ese sentido, en el Plan Bicentenario existe vacíos en lo que respecta a la elaboración de políticas e implementación de ciberseguridad, por tal motivo, se requiere con carácter de urgencia y obligatoriedad capacidades militares de ciberdefensa a fin de fortalecer la ciberseguridad en el Perú. Finalmente, en este escenario aún no se observa una estrategia integrada para la seguridad frente a ciberataques, así como de los medios tecnológicos de los activos críticos, infraestructura prioritaria, información clasificada e instituciones de valor estratégico sean públicas o privadas. Por ello, es de urgencia la implementación y fortalecimiento de la capacidad de ciberdefensa, a fin de prevalecer la ciberseguridad en el Perú y así se consiga alcanzar una apropiada

protección de los medios tecnológicos de los activos críticos, infraestructura principal, información clasificada e instituciones de valor estratégico, además, el uso de dicha capacidad militar debe estar enfocada dentro de leyes y normativas precisas las que deben ser adecuadas y reglamentadas por el más alto nivel de autoridades políticas y militares. Asimismo, que los activos críticos nacionales y las instituciones de valor estratégico no solo pueden ser públicas además, se puede apreciar en instituciones privadas, por tanto para que se llegue a la protecciones de estas también se debe plantear estrategias que incluyan al sector privado.

Rossi (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 se 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.

Vásquez (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.

Freitas (2025), *Anteproyecto de Política de Ciberseguridad para el Perú y su implicancia en la Defensa Nacional,* trabajo presentado para sustentar el programa de desarrollo de políticas cibernéticas y aplicaciones de la Inteligencia artificial para la defensa, realizado en la Universidad Nacional para la Defensa (Centro Perry), se presenta un proyecto de solución para el sostenimiento de una política de seguridad digital nacional, así como la presentación de una estrategia en base a ejes que planean cubrir la parte de la seguridad tecnológica permanente, la defensa nacional y el desarrollo sostenido de la seguridad digital.

2.2 Descripción teórica

2.2.1 Creación del Comando Operacional de Ciberdefensa, 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 EE.UU., 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 (Taípe y Domínguez, 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. (Sanabria, 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 Ciberdefensa

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 y 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 y 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 entiende 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 et al. 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 et al., 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 programa maligno 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 países.
- 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

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.

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. (DoD, 2018)

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, 2013)

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).

Ciberresiliencia

Capacidad de una organización para prevenir, detectar, dar respuesta y recuperarse rápidamente de las interrupciones de TI. Estas pueden ser incidentes de seguridad tales como ciberataques, así como el corte del suministro eléctrico, desastres naturales, fallos en el equipo, errores humanos y otras crisis y desafíos conocidos y desconocidos. (Akamai, s.f., párr. 1)

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. (Gascó, 2013).

Flexibilidad tecnológica

La *flexibilidad tecnológica* es la capacidad de un sistema de TI para adaptarse rápida y eficazmente a cambios en el entorno empresarial o tecnológico, permitiendo la reconfiguración de infraestructura, procesos y aplicaciones sin comprometer la estabilidad ni la eficiencia operativa. Esta flexibilidad se fundamenta en atributos clave como *modularidad,*

conectividad y compatibilidad, que permiten al sistema absorber variaciones externas o internas con bajo costo y alta resiliencia. (Hamidani y Ali, 2025)

Gestión de ciberdefensa

La ciberdefensa debe ser entendida como una metodología ordenada y metódica que articula la organización, la planificación, la dirección y el control de los recursos y las iniciativas destinadas a blindar los recursos digitales y la infraestructura crítica de la nación frente a las agresiones y las amenazas cibernéticas. Tal metodología abarca dimensiones estratégicas, tácticas y operativas, poniendo un acento particular en la armonización entre distintas instituciones y en el fortalecimiento simultáneo de capacidades de carácter tanto técnico como político. (Sánchez, 2021)

Información

La información de una empresa es un activo valioso que puede adoptar diferentes formas, entre otras, la impresión, la escritura, el almacenamiento electrónico y la transmisión. Es un recurso crucial para el negocio, por lo que debe ser salvaguardado y mantenido en buen estado. (NTP-ISO/IEC 17799, 2007, p. 1)

Interoperabilidad

La interoperabilidad, en el marco de la arquitectura digital, es la capacidad de sistemas, organizaciones y aplicaciones para intercambiar información de modo transparente, preservando su significado y operatividad sin conocimiento previo de las características internas de cada entidad. Esto incluye niveles técnicos, sintácticos, semánticos y organizacionales, garantizando cooperación eficaz y funcional dentro del ecosistema digital. (Soldatos, 2022)

Prevención de infraestructuras criticas

La *prevención de infraestructuras críticas* es el conjunto de medidas proactivas orientadas a anticipar y neutralizar amenazas cibernéticas sobre sistemas esenciales, como redes eléctricas, transporte, agua o

comunicaciones. Incluye el uso de controles técnicos (como segmentación de redes, firewalls, y detección de intrusiones), evaluación continua de vulnerabilidades y gestión de riesgos, con el fin de asegurar la disponibilidad y resiliencia de los servicios vitales (Fortinet, 2024, párr. 1).

Resiliencia cibernética

La resiliencia cibernética es la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse eficazmente frente a incidentes de ciberseguridad que puedan afectar la continuidad de sus operaciones críticas. Este concepto integra no solo medidas preventivas, sino también planes de respuesta y recuperación que permiten mantener la funcionalidad de los servicios esenciales ante ataques o fallas en los sistemas (Linkov et al., 2022, p. 48).

Repuestas ante incidentes cibernéticos

La respuesta a incidentes es el proceso estructurado de identificar, gestionar y mitigar los efectos de los incidentes de ciberseguridad para minimizar los daños, recuperar las operaciones y prevenir futuros incidentes. Es un componente fundamental de la estrategia de ciberseguridad de una organización, permitiendo una respuesta rápida y eficiente ante brechas de seguridad, ataques de malware, robo de datos y otras amenazas. La respuesta a incidentes implica la coordinación de esfuerzos de equipos especializados y el uso de marcos, herramientas y procesos diseñados para abordar eficazmente los eventos de seguridad. (SANS, 2024)

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).

Seguridad de la Información

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. (NTP-ISO/IEC 17799, 2007, p. 1)

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).

.

Capítulo III:
Desarrollo Del Tema

3.1. Campos de Aplicación

Los campos donde se asigna la investigación son a nivel nacional, ya que la "red informática del Ejército del Perú", se encuentra desplegada en todo el territorio nacional. Además de presentarse una acción de apoyo para proteger y/o restablecer la operación de un activo critico nacional (infraestructura critica), que se encuentre ubicado en cualquier punto del país obligaría a que la respuesta de una acción que haga resiliencia en una plataforma informática privada o pública demandaría a que elementos de ciberdefensa estén en condiciones de asistir a dicha eventualidad, y por ultimo de aperturarse un Teatro de Operaciones, tendríamos que estar en condiciones de cumplir el misionamiento encomendado por el Comando Conjunto de las Fuerzas Armadas, en apoyo a la maniobra del Comando Operacional que tenga el liderazgo de dicho teatro.

La Línea de Investigación es "La implementación y el sostenimiento de la capacidad militar de Ciberdefensa en el Ejército del Perú"

3.2. Tipos de aplicación

El autor de este estudio se basa en su propia experiencia en Ciberdefensa y Telemática del Ejército, hoy llamado Comando de Operaciones Cibernéticas del Ejército, órgano de línea del Ejército, donde pudo observar la necesidad de implementar y sostener la Capacidad Militar de Ciberdefensa, a través de los recursos existentes y a la vez mantener el esfuerzo de sostenimiento de estas plataformas pese al avance vertiginoso de la tecnología y la implicancia del efecto de las tecnologías disruptivas o emergentes, como la Inteligencia Artificial, Big Data y en un futuro cercano la computación cuántica. 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 una unidad de ciberdefensa (dentro del Comando de Operaciones cibernéticas del ejército), pero tiene muy pocos recursos tanto presupuestales y humanos con el que solo puede hacer operaciones de IVR en el ciberespacio, de manera mínima, lo cual solo cubre una de las

cuatro (04) capacidades de ciberdefensa que debe de tener esta fuerza, las cuales según el reglamento de ley de ciberdefensa deben ser protección, explotación, ataque y análisis digital. Por temas presupuestales y de planeamiento, no existe una implementación adecuada; además, no el personal existente no está laborando en esta unidad, ya que los mismos se encuentran laborando el otras dependencias, haciendo mal empleo del potencial que tiene la institución, además no existe un planeamiento adecuado para el empleo y capacitación de tropa especialista en este dominio, pese a existir un Instituto Nacional de las Fuerzas Armadas (órgano educativo del sector defensa) que no está siendo empleado para complementar los cuadros que requiere esta unidad militar, y los oficiales y técnicos y suboficiales del arma de comunicaciones y del servicio de Ciencia y Tecnología del Ejercito están siendo empleados en otros organismos que no tienen que ver con el desarrollo de la seguridad digital ni con loa defensa cibernética; sin embargo, se puede superar estos factores a través de la implementación y sostenimiento de esta capacidad a través de un ordenamiento adecuado de los recursos existentes y de la elaboración de una ruta estratégica que permita integrar los medios existentes para el desarrollo de esta unidad en el tiempo.

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 de la capacidad militar de ciberdefensa, 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, esta situación nos coloca en una posición de desventaja ante los demás países frente a estos ataques cibernéticos, y como tal afecta al nivel de disuasión que debemos

alcanzar y sostener ante la evolución de las amenazas en el ciberespacio.

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, 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. Asimismo otras entidades como la banca (Banco Interbank), en el año 2024, se vio afectada en sus operaciones ocasionando una parálisis de tres días y mucha incomodidad en sus clientes, esto

asegura en un corto tiempo el crecimiento de los ataques cibernéticos debido a la propia necesidad de los sectores a contar con plataformas interconectadas y que tengan procesos automatizados para darle una mejor calidad no solo a sus clientes sino también al ciudadano de a pie generando "Valor Público" y un crecimiento es el estado de confianza que debe de generar el estado para con el mismo.

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: "*Implementación y sostenimiento de la capacidad militar de ciberdefensa en el ejército del Perú*".

3.4.1. Objetivo general de la propuesta

El objetivo es diseñar, implementar y sostener en el tiempo eficientemente la capacidad militar de ciberdefensa 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:

- Implementar y sostener de manera adecuada la Unidad de ciberdefensa; 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 implementación y sostenimiento de la capacidad militar de ciberdefensa en el Ejército del Perú; evita que nos expongamos a riesgos cibernéticos y por ende a robo de información, una implementación efectiva 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:

- 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.
- 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: a través de un software de seguridad. Seguridad de la nube: CLOUD este es un programa que protege la información en la nube. Seguridad física: LINUX, ya que este sistema operativo es el mejor para administrar bases de datos. Una licencia a fin de explotar las vulnerabilidades de seguridad en Internet Explorer. Licencia de software de transferencia de archivos.
EQUIPOS	Estaciones de trabajo que tengan las siguientes características: procesador de hasta 64 núcleos, ofreciendo un rendimiento excepcional en multihilo, amplias opciones de memoria (hasta 1 TB DDR4 ECC) y almacenamiento, y soporte para múltiples tarjetas gráficas profesionales, accesorios de control, memorias extensibles, traductores digitales, redes de conexión, accesorios de escritorio, accesorios cibernéticos.

PERSONAL	El personal que se requiere es, programadores en Payton, ingenieros en sistemas y software, personal militar con perfil para conformar los puestos de comando.
CAPACITADORES	Personal experto y con experiencia en operación de programas que se instalaran en las plataformas de las unidades, empleados que trabajan en unidades de ciberdefensa y ciberataque; asimismo, el personal de capacitadores se encontrará en constante capacitación.
INFRAESTRUCTURA	Implementada para proteger entornos propios u otros que se nos encarguen administrar, a través de un sistema de seguridad perimetral, además de monitorear otras infraestructuras a pedido.

Nota: Elaboración propia

CONCLUSIONES

1. En este trabajo, una vez analizada la situación actual, se podrá crear hasta tres unidades de ciberdefensa interconectadas 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. La situación global actual describe una hiperconectividad global, en donde todos los ámbitos están expuestos a este tipo de amenazas, y en el devenir de los próximos años la demanda de seguridad para cubrir estas amenazas va a aumentar. El avance tecnológico y la aparición y evolución de nuevas tecnologías (disruptivas) ya tienen un papel importante en la gestión de las plataformas de administración de los sectores tantos públicos como privados, incluida la infraestructura crítica del país. Por tanto, la seguridad de estas infraestructuras es considerada un punto vital para la correcta gestión del desarrollo del estado, es importante considerar que el ciberespacio, si bien es cierto no tiene fronteras, los estados deben de tener una infraestructura que le permita conectarse a este de manera segura, con la finalidad de asegurar la continuidad de sus procesos, para su propio desarrollo.

3. El impacto de este avance tecnológico debe de ser considerado también por los líderes, así como los altos mandos, ya que ellos son los que de manera consensuada priorizan la destinación de los recursos nacionales a fin de fortalecer las capacidades propias

4. Los autores de estos ataques, se alimentan constantemente de los avances tecnológicos a fin de mejorar sus técnicas, tácticas y procedimientos, las mismos que no siguen un mismo patrón sino que buscan ocultarse del monitoreo que siguen los organismos de seguridad de los estados a fin de pasar desapercibidos, por eso se requiere de este tipo de unidades para que

de manera permanente estén observando estos comportamientos y tener una información que nos permita tener una visión preventiva en nuestros procedimientos de respuestas ante estas amenazas.

RECOMENDACIONES

1. El apoyo que la ciberdefensa debe darle a la seguridad digital (ciberseguridad) debe ser permanente y este radica en que tan bien estén preparados los cuadros con que cuenta la fuerza, el entrenamiento que tienen estos cuadros es básico y se deben de tener los recursos suficientes los mismos

2. La capacitación debe de ser continua ya que estos cuadros necesitan conocer lo nuevo de entorno que evoluciona rápidamente.

3. Los proyectos que visen la implementación y sostenimiento de este tipo de unidades deben de tener los recursos necesarios a fin de que su accionar sea sostenido en el tiempo.

4. La formación, actualización, y perfeccionamiento de nuestros cuadros deben de ver el impacto que tiene la ciberdefensa en cada uno de sus campos ya que estas amenazas discurren a través de las organizaciones por el eslabón más débil, quiere decir por el que menos conoce, es así donde entra el tema de la concientización que deben de tener todos los integrantes de la organización con el fin de prevenir este tipo de ataques .

Referencias bibliográficas

Akamai. (s.f.). *¿Qué es la Ciberresilencia?* Obtenido de https://www.akamai.com/es/glossary/what-is-cyber-resilence

Brodie, C., (2008); The Importance of Security Awareness Training, SANS Institute Infosec Reading Room, 30 de Junio de 2008, http://www.sans.org/reading_room/whitepapers/awareness/rss/the_importance_of_security_awareness_training_33013).

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

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

Fortinet. (2025). Obtenido de ¿Qué es la protección de infraestructura crítica (CIP)?: https://www.fortinet.com/resources/cyberglossary/critical-infrastructure-protection?utm_source=chatgpt.com

Gómez, Á., (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.

Hamidani, J., y Ali, H. (2025). Enterprise Architecture for Sustainable SME Resilience: Exploring Change Triggers, Adaptive Capabilities, and Financial Performance in Developing Economies. *Sustainabillity*, file:///C:/Users/guill/Downloads/sustainability-17-06688-v2.pdf.

Herrera, A., 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.

Jeimy, J., y Cano, M., (2020); Economía digital, transformación digita, Ciberataque Asociación Colombiana de Ingenieros de Sistemas. https://doi.org/10.29236/sistemas.n157a6.

Martin, R., Stytz, S. y Bank (2014): "Cyber Warfare Simulation to Prepare to Control Cyber Space". National Cybersecurity Institute Journal, vol 1, N°2. p. 9.

Martínez, (2023) Definición de Riesgo. Última edición: 14 de junio de 2023; https://conceptodefinicion.de/riesgo/.

NTP-ISO/IEC 17799. (2007). Tecnologia de la información. Codigo de buenas prácticas para la gestión de seguridad de la información. *Norma Técnica Peruana*. Lima, Perú: https://spij.minjus.gob.pe/Graficos/Peru/2007/agosto/25/RM-246-2007-PCM_25-08-07.pdf.

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

Quevedo, J., (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.

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

Sanabria, C., (2018); Tecnología y desarrollo; Universidad Nacional Abierta y a Distancia Publicado 2018-12-21 Número Vol. 10 Núm. 19 Revista Científica Perspectivas en Inteligencia.

Sánchez, M. (2021). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En Gestión de Riesgos en Seguridad Digital Escuela Super. En M. Critica, *Gestiión de Riesgos en seguridad Digital* (págs. 1-20). Bogotá: https://esdeglibros.edu.co/index.php/editorial/catalog/download/85/118/1163?inline=1.

Sanger, D., y Perloroth, N., (2015); "Bank Hackers Steal Millions via Malware",New York Times. http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-viamalware.html?_r=1.

SANS. (2024). *Incident Response. En Glossary of Terms. SANS Institute*. Obtenido de SANS Instituto: https://www.sans.org/security-resources/glossary-of-terms/incident-response

Soldatos, J. (2022). *Big Data and Artificial Intelligence in Digital Finance*. file:///C:/Users/guill/Downloads/978-3-030-94590-9.pdf.

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

Torrecuadrada, S., (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.

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

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

Anexos

Anexos A. Informe profesional

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	Espinoza Fernández Edwin
1.02	Grado y Arma / Servicio	Crl Com.
1.03	Situación Militar	Retiro
1.04	CIP	115456700
1.05	DNI	43239967
1.06	Celular y/o RPM	943658455
1.07	Correo Electrónico	

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	1986
2.02	Fecha_ egreso EMCH	1989
2.04	Fecha de alta como Oficial	01 de ago de 1989
2.05	Años de experiencia de Oficial	32 años
2.06	Idiomas	Español

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

N.º	Año	Lugar	Unidad / Dependencia	Puesto Desempeñado
3.01	1989	CHORRILLOS	ESC COM	ALUMNOC
3.02	1990	EL MILAGRO	CIA COM N°5	CMDTE DE SECC
3.03	1990	EL MILAGRO	CIA COM N°5	CMDTE DE SECC
3.04	1990	TTE PINGLO	BIS N° 25	CMDTE DE SECC
3.05	1991	TTE PINGLO	BIS N° 25	CMDTE DE SECC
3.06	1992	TUMBES	BTN SERV N° 1	CMDTE DE CIA
3.07	1993	ALTO SAUCE	CID 5	CMDTE DE CIA
3.08	1994	RIMAC	B COM A/M N°511	CMDTE DE SECC
3.09	1995	CALLAO	CIA COM N° 800	EJECUTIVO MANDO TROPA
3.10	1996	CALLAO	CIA COM N° 800	CMDTE DE SECC
3.11	1997	ABANCAY	BCS N° 63	CMDTE DE CIA
3.12	1998	CUSCO	BTN SERV N° 9	CMDTE CIA
3.13	1999	CUSCO	CIA COM N°9	EJECUTIVO/S-3
3.14	1999	CHORRILLOS	ESC COM	ALUMNO
3.15	2000	SAN BORJA	CCEE	JEFE DPTO ADM
3.16	2001	SAN BORJA	CCEE	JEFE DPTO ADM
3.17	2002	RIMAC	BTN SERV N°241	CMDTE CIA
3.18	2003	RIMAC	CIA COM N°18	EJECUTIVO/S-3
3.19	2004	RIMAC	BTN COM N° 112	CMDTE CIA

3.20	2005	AYACUCHO	CIA COM N°2	CMDTE PEQ UNIDAD
3.21	2006	AYACUCHO	CIA COM N°2	CMDTE PEQ UNIDAD
3.22	2007	SAN BORJA	DITELE	JEFE DE DEPARTAMENTO
3.23	2008	CHORRILLOS	ESGE	ALUMNO
3.24	2009	LIMA CERCADO	ESC CCFFAA	ALUMNO
3.25	2010	SAN BORJA	DITELE	SUB-DIRECTOR
3.26	2010	SAN BORJA	DITELE	SUB-DIRECTOR
3.27	2011	SAN BORJA	DITELE	JEFE DE DPTO
3.28	2011	MONTERRICO	ICTE	ALUMNO
3.29	2012	LIMA CERCADO	CCFFAA	JEFE DEPARTAMENTO
3.30	2012	RIMAC	B SER N° 112	CMDTE UNIDAD
3.31	2013	RIMAC	B SER N° 112	CMDTE UNIDAD
3.32	2014	TARAPOTO	COL MIL MAAC	DIRECTOR
3.33	2015	TARAPOTO	COL MIL MAAC	DIRECTOR
3.34	2016	SAN BORJA	DIEDOCE	OFICIAL EM
3.25	2017	SAN BORJA	DIPERE	COORDINADOR
3.26	2018	LIMA CERCADO	J DPTO GELECT	LIMA CERCADO
3.27	2019	LIMA CERCADO	JEFE DPTO	LIMA CERCADO
3.28	2020	LIMA CERCADO	JEFE DPTO	LIMA CERCADO
3.29	2021	SAN BORJA	JEM OPERATIVO	SAN BORJA

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Período	Denominación	Diploma / Certificación
4.01	1989	ESC COM - 06 MESES	CURSO COMPLEMENTARIO	CERTIFICADO
4.02	1999	ESC COM 06 MESES	CURSO AVANZADO	CERTIFICADO
4.03	2008	ESCUELA SUPERIOS DE GUERRA	CURSO DE ESTADO MAYOR	CERTIFICADO
4.04	2009	ESCUELA CONJUNTA FUERZAS ARMADAS	CURSO DE ESTADO MAYOR CONJUNTO	CERTIFICADO

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Período	Bachiller - Licenciado
5.01	1986 - 1989	ESCUELA MILITAR DE CHORRILLOS	BACHILLER EN CIENCIAS MILITARES CON MENCIÓN EN ADMINISTRACIÓN
5.02	01/10/2012	UNIVERSIDAD SAN PEDRO PERÚ	BACHILLER EN EDUCACIÓN
5.03	26/12/2012	UNIVERSIDAD SAN PEDRO PERÚ	LICENCIADO EN EDUCACION SECUNDARIA EN LA ESPECIALIDAD DE MATEMATICA, FISICA Y COMPUTACION

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
6.01			NO DISPONGO

7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Período	Diploma o Certificado
7.01			

8. ESTUDIOS EN EL EXTRANJERO

N°	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01				

FIRMA……

POST FIRMA: Espinoza Fernández Edwin