ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

INSTRUCCIÓN DE CIBERDEFENSA Y EL PERFIL DE EGRESO DEL CADETE DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI – 2022

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

Autores:

Kevin Sebastian Morote Cabrera

0000-000-2621-6689

Nataly Cristina Caballón Zabala

0000-0002-4260-5054

Asesores:

Dr. Oscar Noguera Bedoya

0000-0002-1171-8929

Dra. Teresa Haro Lizano

0000-0003-3412-1428

Lima – Perú

2022

NOMBRE DEL TRABAJO
2022_CABALLON - MOROTE.pdf

AUTOR
APROBADO

RECUENTO DE PALABRAS
21802 Words

RECUENTO DE CARACTERES
117012 Characters

RECUENTO DE PÁGINAS
96 Pages

TAMAÑO DEL ARCHIVO
2.1MB

FECHA DE ENTREGA
Mar 17, 2023 1:27 PM GMT-5

FECHA DEL INFORME
Mar 17, 2023 1:29 PM GMT-5

23% de similitud general

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

- 21% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 10% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

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

Jurado Evaluador

Los abajo firmantes, miembros del jurado evaluador de la sustentación de tesis titulada: "Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022".

Dan conformidad de la aprobación de la defensa de tesis a cargo de los cadetes del Cuarto Año:

Cad IV Com Morote Cabrera Kevin Sebastián

Cad IV Com Caballón Zavala Nataly Cristina

Surgiéndoles que continúen con el desarrollo histórico de la línea de investigación y tema, emprendidos, en las futuras investigaciones que efectúen en el desempeño y perfeccionamiento de la carrera en ciencias militares.

_ _

Presidente (a)

_ _

Secretario (a)

_ _

Vocal

AGRADECIMIENTO

A nuestra querida Alma Mater, que por medio de su formación integral nos permite optimizar nuestra formación profesional que coadyuvará en nuestra carrera militar como buen oficial del Ejército del Perú.

DEDICATORIA

Queremos dedicar este trabajo de investigación al creador por darnos la vida y acompañarnos en nuestro camino diario. A nuestros padres y hermanos a quienes amamos y han sido nuestro soporte y compañía durante todo este periodo de estudios. A nuestros instructores por habernos guiado en nuestra formación.

DECLARACIÓN JURADA DE AUTORÍA

Mediante el presente documento, Yo, Nataly Cristina CABALLÓN ZAVALA, identificado con Documento Nacional de Identidad N° 74834907, con domicilio real en Jr Sicuani 243 Tahuantinsuyo, en el distrito de Independencia, provincia de Lima , departamento de Lima, estudiante / egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"; y, Yo, Kevin Sebastián MOROTE CABRERA, identificado con Documento Nacional de Identidad N° 61335170, con domicilio real en Calle Inclán 177, en el distrito de San Miguel, provincia de Lima , departamento de Lima, estudiante / egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"; declaro bajo juramento que: Soy el autor de la investigación titulada "Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022" que presento a los 19 días de diciembre del año 2022, ante esta institución con fines de optar el grado académico de Licenciado en Ciencias Militares con mención en Administración. En dicha investigación se ha desarrollado respetando los principios éticos propios, no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponde al suscrito u a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad. (El delito de plagio se encuentra tipificado en el artículo 219 del Código penal). Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Militar de Chorrillos y me declaro el único responsable.

……	……..……..
Nataly Cristina Caballón Zavala	Kevin Sebastián Morote Cabrera
DNI 74834907	DNI 61335170

AUTORIZACIÓN DE PUBLICACIÓN

A través del presente documento autorizamos a las Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” la publicación del texto completo o parcial de la tesis de grado titulada: “Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022”, presentada para optar el grado académico de Licenciado en Ciencias Militares en el Repositorio Nacional de Tesis (Renati) de la SUNEDU, de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio en beneficio de la comunidad académica y de la sociedad. En tal sentido autorizamos gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser copiada, distribuida y exhibida con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Chorrillos, ….. de diciembre del 2022

……	……..
Nataly Cristina Caballón Zavala	Kevin Sebastián Morote Cabrera
DNI 74834907	DNI 61335170

ÍNDICE

Pag.

Jurado evaluador ii
Agradecimiento iii
Dedicatoria iv
Declaración jurada de autoría v
Autorización de publicación vi
Índice vii
Índice de tablas x
Índice de figuras xi
Resumen xii
Abstract xiii
Introducción xiv

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción problemática 15
1.2 Delimitación de la investigación 16
1.3 Formulación del Problema 17
1.3.1 Problema general 17
1.3.2 Problemas especificos 17
1.4 Objetivos de la investigación 17
1.4.1 Objetivo General 17
1.4.2 Objetivos Específicos 18
1.5 Justificación e Importancia de la Investigación 18
1.6 Limitaciones de la investigación 18

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación 20
2.1.1 Antecedentes internacionales 20
2.1.2 Antecedentes nacionales 22
2.2 Bases teóricas 26

2.2.1 Instrucción de Ciberdefensa 26
2.2.2 Perfil de Egreso del Cadete de Comunicaciones 41
2.3 Marco Conceptual 51
2.4 Operacionalización de las variables 56
2.5 Formulación de hipótesis 57
2.5.1 Hipótesis general 57
2.5.2 Hipótesis específicas 57

CAPÍTULO III. MARCO METODOLÓGICO

3.1 Enfoque de investigación 58
3.2 Tipo de Investigación 58
3.3 Método de Investigación 58
3.4 Alcance de investigación 58
3.5 Diseño de la Investigación 59
3.6 Población, muestra, unidad de estudio 59
3.6.1 Población de estudio 59
3.6.2 Muestra 59
3.6.3 Unidad de estudio 60
3.7 Técnica e Instrumento para la recolección de datos 60
3.7.1 Técnica de recolección de datos 60
3.7.2 Instrumento de recolección de datos 61
3.7.3 Validez y confiabilidad de los instrumentos de medición 61
3.8 Procesamiento y método de análisis de datos 62
3.8.1 Técnica para el procesamiento de datos 62
3.8.2 Método de análisis de datos 63
- Análisis descriptivo 63
- Análisis Inferencial 63
3.9 Aspectos éticos 63

CAPÍTULO IV: RESULTADOS

4.1 Análisis descriptivo 64
4.2 Análisis inferencial 68

CAPÍTULO V: DISCUSION DE RESULTADOS 73

CONCLUSIONES 76

RECOMENDACIONES 78

REFERENCIAS BIBLIOGRAFICAS 80

ANEXOS

Anexo 1: Matriz de consistencia 84

Anexo 2: Instrumento de recolección de datos 86

Anexo 3: Autorización para la recolección de datos 91

Anexo 4: Base de datos (de prueba piloto) 92

Anexo 5: Base de datos (origen de resultados) 93

Anexo 6: Otros de acuerdo con el nivel y diseño de investigación 95

ÍNDICE DE TABLAS

Pág.

Tabla 1.	*Operacionalización de las variables*	*56*
Tabla 2.	*Instrucción de ciberdefensa y el Perfil del Cadete Egresado de Comunicaciones*	*64*
Tabla 3.	*Ciberdelito Convencional y el Perfil del Cadete Egresado de Comunicaciones*	*65*
Tabla 4.	*Ciberdelitos Complejos y el Perfil del Cadete Egresado de Comunicaciones*	*66*
Tabla 5.	*Amenazas Emergentes y el Perfil del Cadete Egresado de Comunicaciones*	*67*
Tabla 6.	*Correlación de la hipótesis general*	*68*
Tabla 7.	*Correlación hipótesis especifica 1*	*69*
Tabla 8.	*Correlación hipótesis especifica 2*	*71*
Tabla 9.	*Correlación hipótesis especifica 3*	*72*

ÍNDICE DE FIGURAS

Pág.

Figura 1. *Instrucción de ciberdefensa y el Perfil del Cadete Egresado de Comunicaciones* *64*

Figura 2. *Ciberdelito Convencional y el Perfil del Cadete Egresado de Comunicaciones* *65*

Figura 3. *Ciberdelitos Complejos y el Perfil del Cadete Egresado de Comunicaciones* *66*

Figura 4. *Amenazas Emergentes y el Perfil del Cadete Egresado de Comunicaciones* *67*

RESUMEN

La presente investigación titulada “Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022”; considera dentro de su objetivo principal, determinar de qué manera se relaciona la Instrucción de ciberdefensa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

El método de estudio tiene un enfoque cuantitativo, con un diseño no experimental transversal, con una población objetiva de 27 cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” involucrados en el tema, de la investigación; con la aplicación de un cuestionario para determinar los objetivos de la investigación.

Durante el desarrollo de la presente investigación se llegó a la conclusión general siguiente: De acuerdo con la Hipótesis General que a la letra dice que, la Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. El valor calculado para la Chi cuadrada $0.041 < 0.05$ para un nivel de confianza de 95%. Hemos podido concluir que dicha hipótesis es válida; ya que, la Instrucción de ciberdefensa la cual debe incluir el ciberdelito convencional, los ciberdelitos complejos y amenazas emergentes contribuye directamente con la estructuración y consecución del Perfil de egreso del cadete de comunicaciones de la Escuela Militar, en provecho de la profesionalización de los futuros oficiales del arma de Comunicaciones.

Como parte final del estudio se exponen las recomendaciones de acuerdo con las conclusiones, las cuales son propuestas factibles para potenciar la Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Palabras claves: Instrucción, ciberdefensa y perfil de egreso.

ABSTRACT

The present investigation entitled "Cyberdefense Instruction and the Graduate Profile of the Communications Cadet of the Military School of Chorrillos “Coronel Francisco Bolognesi”-2022"; considers within its main objective, to determine how the Cyber Defense Instruction is related to the Graduate Profile of the Communications Cadet of the Military School of Chorrillos “Coronel Francisco Bolognesi”-2022.

The study method has a quantitative approach, with a non-experimental cross-sectional design, with an objective population of 27 cadets of the 4th year of Communications of the "Coronel Francisco Bolognesi" Military School of Chorrillos involved in the subject of the investigation; with the application of a questionnaire to determine the objectives of the investigation.

During the development of this investigation, the following general conclusion was reached: According to the General Hypothesis that literally says that the Cyber Defense Instruction is significantly related to the Graduate Profile of the Communications Cadet of the Chorrillos Military School Colonel Francisco Bolognesi-2022. The value calculated for the Chi square $0.041 < 0.05$ for a confidence level of 95%. We have been able to conclude that this hypothesis is valid; since the Cyber Defense Instruction, which must include conventional cybercrime, complex cybercrime and emerging threats, contributes directly to the structuring and achievement of the Graduate Profile of the Communications cadet of the Military School, in benefit of the professionalization of future officers. of the communications weapon.

As a final part of the study, the recommendations are presented in accordance with the conclusions, which are feasible proposals to enhance the Cyber Defense Instruction and the Graduate Profile of the Communications Cadet of the Chorrillos Military School “Coronel Francisco Bolognesi”-2022.

Keywords: Instruction, cyber defense and graduation profile.

INTRODUCCIÓN

Al referirnos a la instrucción de ciberdefensa y el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, primero debemos referirnos a la instrucción de ciberdefensa, la cual brinda los conocimientos requeridos para complementar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, para que se desempeñen de forma eficiente como futuros oficiales del arma.

La estructura de nuestra investigación consta de cinco capítulos que se desarrollaron metodológicamente y nos llevaron a conclusiones y recomendaciones de suma importancia; siendo el 1er Capitulo denominado planteamiento del problema, donde se realiza la descripción problemática, la delimitación, la formulación del problema, los objetivos, la justificación e importancia y las limitaciones de la investigación.

En el Capítulo 2 denominada marco teórico, podemos encontrar los antecedentes, las bases teóricas, el marco conceptual, la operacionalización de las variables y la formulación de las hipótesis.

El Capítulo 3 denominado marco metodológico, incluye el enfoque, el tipo, el método, el alcance, el diseño, la población, la muestra, la unidad de estudio, la técnica e Instrumento para la recolección de datos, el procesamiento y método de análisis de datos y los aspectos éticos.

Con respecto a los resultados en el Capítulo 4 denominado resultados, se desarrollaron el análisis descriptivo y el análisis inferencial.

Posteriormente en el Capítulo 5 denominada discusión de resultados, en el cual desarrollamos la discusión propiamente dicha de los resultados obtenidos en el Capítulo 4.

Por último, llegaremos a las conclusiones y recomendaciones que permitirán cumplir los objetivos previstos y comprobar las hipótesis planteadas.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción problemática

La ciberdefensa es un grupo de medidas técnicas, políticas y organizativas orientadas a brindar protección a la información, comunicación y control de cualquier tipo de ciberataque. Desde una perspectiva militar, se centra en las medidas técnicas, políticas y organizativas para proteger los sistemas y redes militares de los ataques cibernéticos, incluidas las posibilidades de respuesta y ataque típicas de los conflictos armados (utilizando el ciberespacio).

Abarca la protección a los sistemas de información civiles para apoyar al cumplimiento de la misión; la defensa cibernética se basa principalmente en técnicas de seguridad cibernética extensamente probadas implementadas en el sector civil.

Sin embargo, por los avances tecnológicos, es necesario desarrollar nuevas tecnologías, así como reposicionar las tecnologías existentes.

La ciberdefensa persigue diferentes objetivos complementarios que en conjunto brindan suficientes garantías sobre el grado de prevención, resistencia y recuperación de un sistema de información ante un ciberataque: además, debe tener la capacidad de impedir que un potencial adversario ejecutar un ciberataque. Ataque (prevención), mediante la implementación de medidas que involucren: consecuencias penales, operaciones de respuesta militar en el ciberespacio, se debe prevenir que ocurran ciberataques, se deben eliminar oportunidades, se deben proteger los sistemas de información en caso de un ciberataque, prevención de esta situación es satisfactoria, debe detectar la ejecución en curso, incluso en una fase temprana; y, debe facilitar una respuesta rápida que permita volver a un estado estable ante un ciberataque, si ha tenido éxito, con un impacto mínimo en el negocio.

Al mismo tiempo, la dependencia tecnológica, la globalización y la facilidad de acceso a la tecnología significan que el potencial de un ataque informático o ciberataque es muy alto hoy en día, lo que facilitaría a nuestros rivales obtener inteligencia de gran nivel que podría desestabilizar nuestras fuerzas. Lógicamente, cuanto mayor sea la dependencia, mayor será el impacto de un ataque a los sistemas en los que se basa una nación u organización.

Los ciberataques ya no tienen solo una motivación intelectual o económica, así mismo una motivación política, por lo que los resultados están centrados solo en el daño económico, sino también en los enfrentamientos bélicos entre naciones que exhiban y comparen su poder, así como en tierra, mar, aire y el medio ambiente. dimensión del espacio, a través del ciberespacio.

Es por lo que como futuros oficiales del arma de comunicaciones es que debemos considerar como se relaciona el conocimiento de la Ciberdefensa con el perfil que debe tener todo oficial de comunicaciones, el mismo que debe estar acorde con los avances tecnológicos, las necesidades de la institución y el desarrollo del país.

1.2 Delimitación de la investigación

1.2.1 Delimitación Espacial

La investigación se realizó en el departamento de Lima, distrito de Chorrillos.

1.2.2 Delimitación temporal

El presente trabajo de investigación está enmarcado en un periodo de tiempo comprendido entre el año 2022 y se proyecta a eventos futuros.

1.2.3 Delimitación Teórica

La investigación se encuentra enmarcada por los conocimientos referentes a la Instrucción de Ciberdefensa; así mismo, referente al perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

1.3 Formulación del Problema

1.3.1 Problema Principal

¿De qué manera la Instrucción de ciberdefensa contribuye con el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?

1.3.2 Problemas Especificos

- ¿De qué manera la Instrucción de Ciberdelito convencional contribuye con el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?

- ¿De qué manera la Instrucción de Ciberdelitos complejos contribuye con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?

- ¿De qué manera la Instrucción de Amenazas emergentes contribuye con el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?

1.4 Objetivos de la investigación

1.4.1 Objetivo General

Determinar de qué manera la Instrucción de ciberdefensa contribuye con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

1.4.2 Objetivos Específicos

- Establecer de qué manera la Instrucción de Ciberdelito convencional contribuye con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

- Establecer de qué manera la Instrucción de Ciberdelitos complejos contribuye con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

- Establecer de qué manera la Instrucción de Amenazas emergentes contribuye con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

1.5 Justificación e Importancia de la Investigación

Las tecnologías emergentes son importantes porque las nuevas tecnologías pueden representar amenazas u oportunidades para la seguridad nacional, pero están rodeadas de dudas, particularmente en el ámbito militar, donde se entiende el cómo crecerán las tecnologías nuevas, pero como sus contrapartes en las operaciones civiles Incertidumbre sobre la estrategia, emergente tecnologías significa que no tienen forma de saber qué tecnologías emergentes están maduras y pueden tener un impacto de gran alcance, cuánto tiempo llevará madurar o qué trayectoria tecnológica tomarán. Luego, explicó que la mayoría de las tecnologías emergentes, como las amenazas cibernéticas, representan mejoras incrementales sobre lo que ha sucedido antes y mejoran las capacidades en áreas que tradicionalmente han sido valoradas.

1.6 Limitaciones de la investigación

Los esfuerzos de investigación actuales se centran en una mayor necesidad de tiempo y dedicación.

- Desde la parte económica, se considera como limitación ya que nos muestra que los investigadores en formación reciben propinas por las cuales sus padres y otros familiares brindan apoyo económico para pagar lo que generan costo. investigación. investigación actual.
- Insuficiencia de tiempo por las diversas y múltiples académicas y administrativas.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes internacionales

En el ámbito internacional, en los repositorios de las principales universidades de Ecuador se ha identificado investigaciones relacionadas a la variable 1. Pérez y Ramos (2020), señalan que:

> El uso obligatorio de las TIC genera una serie de riesgos que afectan los derechos de las personas, la infraestructura de información crítica y los intereses vitales de todos los usuarios de Internet, una amenaza que las Fuerzas Armadas del Ecuador no han olvidado, traduciéndose en una falta de ciberseguridad para mantener el licenciamiento y proteger los medios digitales. Las políticas de seguridad causan grandes problemas. Ante las amenazas cibernéticas y la ausencia de una política de seguridad cibernética, el trabajo de esta titulación se enfocará en el desarrollo de la política de seguridad digital analizando distintos estándares internacionales e incorporación del análisis jurídico a nivel nacional en distintas instituciones, facilitando así la integración de instituciones que gestionan riesgos en el ciberespacio coordinación entre. (p. 12)

Asimismo.en el ámbito internacional, en los repositorios de las principales universidades de Ecuador se ha identificado investigaciones relacionadas a la variable 1. Como la realizada por Chiza y Izurieta (2020) que afirman que:

> El siglo XXI ha traído muchos avances tecnológicos a la humanidad, por un lado ha facilitado el desarrollo de actividades, pero por otro lado ha presentado grandes desafíos en cuanto a la seguridad, utilizamos la tecnología en casi todos los campos de la trabajo, pero no sabemos cómo usarlo, los peligros que representa, esta realidad pronosticada a nivel nacional hace que como país enfrentemos muchos peligros por el uso de la tecnología, en este trabajo de investigación partimos con un diagnóstico de la actualidad situación del Ecuador en materia de ciberseguridad, Establecer áreas de acción que requieran de lineamientos nacionales que permitan la articulación y coordinación de los esfuerzos de los diferentes organismos nacionales, complementado con el apoyo de los organismos internacionales, todo lo cual se refleja en la propuesta que se presenta como estrategia nacional de ciberseguridad, en la que se presenta la estrategia que hemos considerado el curso de acción seguido y las metas a alcanzar a través de cada estrategia propuesta, por lo que este trabajo constituye un aporte desde una perspectiva puramente académica y consciente de las principales limitaciones económicas que se pueden implementar. a medio plazo. (p.10)

En el ámbito internacional, en los repositorios de las principales universidades de Argentina se ha identificado investigaciones relacionadas a la variable 1. Como la realizada por Albarracín (2019) en la que afirma que:

> El objetivo del autor es “arrojar luz sobre los elementos que minan la definición de la estrategia nacional de ciberseguridad de Argentina” (p. 98), usando métodos de investigativos de enfoque cualitativo para concluir que: Primero, la proliferación de las TIC y la “propaganda de la tecnología han propiciado el establecimiento de medidas de ciberseguridad y ciberdefensa para mitigar y proteger a las naciones de las vulnerabilidades creadas por los ecosistemas que componen el ciberespacio” (p. 98). En segundo lugar, existen “varias normas destinadas a proteger la cooperación internacional en

> materia de seguridad de la información y procedimientos", pero la distinción "ciberseguridad, ciberdefensa y ciberdelincuencia, tienen dinámicas y desarrollos diferentes". Este estudio demuestra la necesidad de unificar los esfuerzos de las agencias en defensa cibernética. Nuevamente, esto apunta a la necesidad de inversión en mano de obra y equipo técnico. (p.13)

También, en el ámbito internacional, en los repositorios de las principales universidades de Argentina se ha identificado investigaciones relacionadas a la variable 1. Como la de Baretto (2017), que nos indica que hay que identificar los métodos, formas y medios de uso como un 'sistema de armas cibernéticas'" (p. 3), concluyendo que primero:

> Es necesario para la respuesta a la agresión provenga de un solo organismo. En segundo lugar, la ausencia de una estrategia nacional de ciberseguridad no facilita la ejecución de estrategias militares aplicables a la defensa nacional". En tercer lugar, los desarrollos y facultades específicas están bajo el nivel de amenaza. Así, en este estudio, podemos apreciar la necesidad de tener un sistema de ciberseguridad optimo, y así contribuye a este estudio tanto a nivel teórico como de investigación pragmática, ya que los militares son los que más necesitan un rol protector y defensivo. (p.136)

2.1.2 Antecedentes nacionales

En el ámbito internacional, se ha identificado investigaciones relacionadas a la variable 2. Como la de Alarcón y Suárez (2020) que concluyen en la investigación que realizaron:

> De la investigación pudimos concluir que la hipótesis planteada es válida debido al proceso de formación integral de los cadetes de artillería, incluyendo los campos de ciencias y humanidades, la ciencia militar, así como las áreas relacionadas con la fuerza física general, proporcionarán la base para el perfil de oficial necesario para que los oficiales de artillería se desempeñen de manera óptima

> en las unidades que deseen. Como parte final del estudio, se recomiendan elaborado con base en conclusiones que mejoran la comprensión de las recomendaciones accionables para la concientización de la formación integral de los cadetes de artillería y los documentos requeridos para los oficiales egresados de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". (p.59)

En el ámbito internacional, en los repositorios de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" se ha identificado investigaciones relacionadas a la variable 2. Aliaga y Bazán (2020), que señalan:

> Que, el entrenamiento en todas las áreas de la actividad militar (entrenamiento integrado) es fundamental para la realización de Los aspectos personales, académicos y profesionales de la imagen profesional de los oficiales de caballería egresados de la escuela militar "Coronel Francisco Bolognesi" son cruciales. (p. 25)

Otra investigación recurrida relacionada a la variable 2, es la de Vera (2018) que busco determinar si en su etapa de formación militar académica, un oficial del Ejército cumple satisfactoriamente los roles asignados, por ejemplo: táctico, instructor militar, administrador, investigador científico. Dichos roles se convirtieron en la esencia de este trabajo de investigación.

Y la última investigación tenida en cuenta en el presente trabajo de investigación y relacionada a la variable 2, es la desarrollada por Taipe; Huacasi y Liu (2017) que tuvo como finalidad determinar la relación que existe entre la formación académica de los cadetes y los perfiles de instructores de los cadetes de 4to año de Armas de Artillería de la Escuela Militar Chorrillos "CFB" 2016", con el propósito de seleccionar un Licenciado en Ciencias Militares. grado, basado en interés de nuestro ejército y del país. (p.122)

2.2 Bases teóricas

2.2.1 Instrucción de ciberdefensa

1. Ciberdelito convencional

a. Acceso Ilegal (Craqueo)

Al igual que los hackers, los crackers son unos apasionados del mundo informático. La principal diferencia es que el propósito de descifrar programas es dañar sistemas y computadoras. Como su nombre lo indica, cracker significa "rompedor" en inglés, y su propósito es destruir y causar el mayor daño posible. (Palau, 2013)

Para los hackers, los crackers no merecen ningún respeto porque no ayudan ni mejoran el programa y no contribuyen a ningún progreso en este sentido. (Palau, 2013)

Las cookies también se conocen como sombreros negros. Acceden maliciosamente a las cuentas de las personas y pueden hacer un mal uso de la información protegida en la web. Pueden robar información de tarjetas de crédito, pueden destruir documentos importantes, filtrar datos e información críticos o datos personales y venderlos para beneficio personal. Sus propósitos pueden variar desde pequeños intereses personales hasta intereses criminales más grandes. Pueden conducir a la divulgación de información altamente segura por parte de los empleados de la empresa. Violan la seguridad informática. Una vez que obtienen el control del sistema, pueden hacer cualquier cosa, como robar datos, destruir datos, usar datos para su propio beneficio, etc. (Palau, 2013)

Tipos de crackers

Estos son los diferentes tipos de crackers existentes.

- **De sistemas**

  Son personas que utilizan mecanismos de protección anticopia exclusivamente en el software. Tenga en cuenta que los crackers de software no involucran la explotación de la web, sino software protegido por derechos de autor. Puedes hackear el programa y cambiar el contenido del software. (Palau, 2013)

- **Ciberpunks**

  Los ciberpunks son piratas informáticos que se especializan en modificar páginas web o sistemas informáticos. (Palau, 2013)

- **De criptografía**

  Este tipo de cracker es experto en descifrar textos o documentos encriptados. (Palau, 2013)

- **Piratas**

  Sus actividades incluyen la copia ilegal de programas, socavando sus sistemas de protección y licencias. A continuación, el producto se distribuye a través de Internet, CD, etc. (Palau, 2013)

- **Phreakers**

  Sus actividades incluyen la copia ilegal de programas, socavando sus sistemas de protección y licencias. A continuación, el producto se distribuye a través de Internet, CD, etc. (Palau, 2013)

- **Insiders**

  Son saboteadores de la "empresa", empleados de la empresa que los atacan desde adentro, a menudo con motivos de venganza. (Palau, 2013)

b. Interceptación De Datos

El que intencional e ilícitamente intercepte datos informáticos que no sean públicamente transmitidos, dirigidos, originados o ejecutados en un sistema informático, incluyendo las radiaciones electromagnéticas de un sistema informático que transmita dichos datos informáticos, incurrirá en sanción de privación de libertad por tres años o no menos de seis años. De acuerdo con la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, si el delito es de información clasificada, reservada o clasificada, la pena de prisión no es menor de 5 u 8 años. Los delitos de atentar contra la defensa, la seguridad o la soberanía nacionales se sancionan con prisión no menor de ocho años ni mayor de diez años. Si un policía o militar delinque como miembro de una organización criminal, la sanción penal se incrementará hasta en un tercio sobre la pena máxima legal establecida en los casos anteriores." (Javier, 1998)

c. Pornografía Infantil

Artículo 5.- Quien proponga matrimonio a un niño o joven por medios científicos y tecnológicos se ponga en contacto con un menor de catorce años para obtener material pornográfico o realizar actividades sexuales a través de las tecnologías de la información o la comunicación, deberá serán reprimidos conforme al artículo 36 del Código Penal. Los números 1, 2 y 4 son reprimidos con pena privativa de libertad no menor de 4 años ni mayor de 8 años e inhabilitación. Si la víctima tiene de 14 a 18 años y medio engañada, será reprimida no menos de tres años y no menos de seis años, y será inhabilitada conforme a los números 1, 2 y 4 del artículo 36 de la Ley Penal. (*) (*) Artículo reformado por el Artículo 1 de la Ley N° 30171 de 10 de marzo de 2014, cuyo texto dice: "Artículo 5.- Asesoramiento a niños, niñas y adolescentes por medios técnicos con fines sexuales. solicita materiales pornográficos o participa en actos sexuales con menores de catorce años poniéndose en contacto con menores de catorce años a través de Internet u otros medios similares

será condenado a una pena de prisión de no menos de cuatro años, pero no más de ocho años, y será inhabilitada. Numerales 1, 2 y 4 del Artículo 36. Si la víctima tiene de 14 a 18 años y la mitad de la víctima es engañada, será reprimido con pena no menor de tres años y no menor de seis años, y será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36 de la Ley Penal." (Javier, 1998)

d. Spam

El spam, el correo no deseado abarrotado en nuestras bandejas de entrada, es un desafío para los usuarios de Internet, las empresas y los legisladores por igual. Las estimaciones varían, pero algunos creen que se envían más de 100 mil millones de mensajes de spam todos los días, lo que representa el 85 % del tráfico de correo electrónico diario del mundo. (Javier, 1998)

El término spam generalmente se refiere a comunicaciones electrónicas no solicitadas (generalmente correo electrónico) o, en algunos casos, comunicaciones comerciales no solicitadas que se envían de manera indiscriminada. Algunas personas llaman a este tipo de mensajes spam. Si bien las campañas de spam se presentan principalmente en forma de correo electrónico, el spam es una amenaza en evolución que se ha extendido a casi todas las formas de comunicación electrónica, incluidos mensajes de texto, publicaciones en redes sociales, sistemas de mensajería instantánea y más. (Javier, 1998)

Además de los inconvenientes y la pérdida de tiempo de los mensajes no deseados, el correo no deseado también puede causar daños significativos al contaminar las PC de los usuarios con malware con capacidad de interrumpir los sistemas y sustraer información personal. También puede tragarse recursos de red. (Javier, 1998)

Algunos de los tipos más comunes de spam dañino actualmente son correos electrónicos de estafas financieras, correos electrónicos que contienen software de phishing, malware de botnet y/o ransomware. Los spammers son muy ingeniosos e imperecibles. Continúan creando señuelos cada vez mejores para atraer a los usuarios y convencerlos de que abran mensajes que contengan malware. Constantemente buscan nuevas listas de direcciones de correo electrónico y nuevos medios de comunicación para atacar. (Javier, 1998)

Desafíos

En su conjunto, el spam es un desafío técnico, económico y de seguridad en constante evolución para muchos países. Por lo tanto, se requiere de múltiples caras para abordar los desafíos que trae consigo. Específicamente, el problema del spam presenta los siguientes desafíos:

- El spam es un problema caro tanto para las instalaciones para el Internet como para los consumidores del producto. Grandes masas de spam pueden acabar con valiosos recursos de red, especialmente en países con acceso a Internet y ancho de banda con límites. Los que brindan el servicio de Internet (ISP) hacen lo posible para controlar este tráfico, y los usuarios finales deben estar atentos para evitar abrir spam que contenga malware o estafas. Para los usuarios de datos móviles y aquellos suscritos a servicios medidos, recibir o enviar grandes cantidades de spam sin saberlo puede ser costoso. Además, la reparación de sistemas infectados y/o atacados por malware enviado por spam genera costos, así como costos asociados con el robo de datos de los usuarios. (Javier, 1998)
- En términos generales, la economía del spam beneficia en gran medida a los spammers. El costo de enviar un mensaje no solicitado es bajo; de hecho, la mayor parte del costo corre a cargo del destinatario del mensaje, el ISP, el usuario infectado o el operador de la red. (Javier, 1998)

- La naturaleza del spam ha cambiado con la introducción de nuevas aplicaciones y el intercambio de información en Internet. Los spammers están mejorando su capacidad de usar estas plataformas para entregar mensajes más intrusivos y maliciosos para robar información personal, interrumpir redes e infectar sistemas. (Javier, 1998)
- El spam afecta a muchos usuarios de Internet. Ninguna organización por sí sola puede resolver la amenaza que representa el spam, pero se necesita una comunidad global de múltiples partes interesadas para abordar el problema. (Javier, 1998)
- Además de causar daños inmediatos a los usuarios y sobrecargar los recursos de la red, el spam también crea sutilmente una falta de confianza entre los usuarios y algunos lo ven como una barrera para el uso de Internet y el comercio electrónico. Considere también el posible impacto negativo en la reputación de los usuarios cuyas identidades son robadas por los spammers y utilizadas para enviar spam. (Javier, 1998)
- Las comunidades involucradas en los esfuerzos antispam pueden estar sujetas a represalias (por ejemplo, víctimas de denegación de servicio distribuido (DDoS), ataques de piratas informáticos), por lo que los miembros de la comunidad antispam global no solo ofrecen ayuda para combatir el spam, pero también se ofrece apoyo técnico y de otro tipo para evitar posibles represalias. (Javier, 1998)

e. Incitación Al Odio

Los delitos de odio implican actos delictivos mediante los cuales los agresores expresan mensajes de odio o discriminatorios contra un grupo social. Una particularidad de este tipo de delitos es que el agraviado es elegido por el perpetrador tomando en cuenta los vínculos sociales que lo relacionan a un determinado grupo. Es esta facultad de su origen nacional o étnico u otras circunstancias relacionadas con su identidad, como el género, la orientación sexual o la ideología, lo que convierte a

las víctimas en objetivos atractivos para los perpetradores. Asimismo, a juicio del autor, el grupo social al que se vincula la víctima directa es receptor de la información discriminatoria y víctima indirecta de la conducta. (Pérez, 2015)

La investigación criminológica señala que inherente a esta experiencia de victimización está el mensaje de intimidación en el que las particularidades de la víctima no son importantes frente a la significación social que conllevan. Los ataques de odio no se dirigen a las propias víctimas, sino a lo que representan (Chakraborti y Garland, 2012). Según algunos enfoques, la idea de jerarquía y dominación es inherente al odio a la victimización, ya que la violencia es expresión de una actitud social hegemónica que perpetúa la subordinación de determinados grupos, un "castigo que sirve de recordatorio a los miembros"" La violencia sexual en estos grupos corresponde a su lugar en la sociedad (Perry, 2009). Este punto de vista es controvertido debido a que no se aplica a la violencia y el abuso contra las personas con discapacidad, los ancianos o las personas sin hogar, porque en este caso su selección como blanco está relacionada con el hecho de que fueron atacados. Están más en línea con la imagen social de la "víctima ideal" (Chakraborti y Garland, 2012).

f. Fraude Bancario

El phishing es un fraude que se produce desde un ordenador conectado a Internet. Los delincuentes recurren a herramientas tecnológicas para acceder o violar cualquier contraseña y sistema de seguridad. (Julinsky, 1999)

Los ciberdelincuentes ofrecen ofertas atractivas a través de pagos iniciales separados, requieren transferencias bancarias a cuentas personales vendiendo los artículos más caros, invitan a acceder a servicios bancarios en línea a través de mensajería instantánea, requieren la descarga e instalación de aplicaciones o mediante nombres de usuario

web falsos y página de contraseña. Otra técnica que utilizan estos estafadores es persuadir a sus consumidores para que continúen negociando para comprar productos fuera de las plataformas digitales. (Julinsky, 1999)

Hay cuatro tipos principales de fraude en línea:

- Compra de artículos online
- Pharming / Sitios con Virus
- Phishing / Suplantación de Identidad
- Carding / Robo de Tarjetas Bancarias

La suplantación de identidad a través del correo electrónico y los robos de datos se encuentran entre los delitos más denunciados en la región durante la pandemia de coronavirus, pero representan un alto riesgo no solo para los clientes de comercio electrónico sino también para los clientes de comercio electrónico las finanzas de las entidades y empresas. (Julinsky, 1999)

Los tipos más comunes de fraude electrónico durante emergencias sanitarias son:

- Hacerse pasar por agencias para brindar información, desviar segundas dosis y vender vacunas contra el COVID-19: según los expertos, se ha triplicado el número de anuncios y las vacunas con seguridad cuestionable tienen un precio de $500; un aumento desde enero de este año del 300 %
- Sitios que cometen fraude al vender productos como geles desinfectantes para manos, máscaras u otros productos solicitados
- Hacerse pasar por una entidad gubernamental para solicitar donaciones
- Ofertas fraudulentas de bancos, casas de bolsa o inversiones diseñadas para robar información bancaria. (Jurinski, 1999)

g. Robo de Identidad

El robo en línea es uno de los tipos de ciberdelincuencia más frecuentes, ya que todos los que usamos Internet hoy en día solemos usar datos personales confidenciales, como cuentas bancarias, tarjetas de crédito, etc., si cae en manos de estos ciberdelincuentes, causando enormes pérdidas financieras. (Atienza, M. y Ruiz, J., 2006)

Una etapa avanzada del robo en línea es el robo de identidad, que ocurre cuando alguien roba datos de acceso (nombres de usuario y contraseñas) a nuestro correo electrónico, cuentas de redes sociales, etc. y actúa en nuestro nombre, dañando nuestra reputación en línea y causando potencialmente pérdidas económicas importantes. (Atienza, M. y Ruiz, J., 2006)

h. Infracciones de Derechos de Autor

El 2013 fue un año lleno de debates sobre la libertad en internet en Perú, desde las negociaciones del TPP hasta las leyes contra el ciberdelito, la aprobación de propuestas pendientes para filtrar la pornografía y nuevas propuestas de excepciones y limitaciones de derechos de autor. Sin embargo, quizás el caso que mejor ilustra la vulnerabilidad de nuestro sistema es la eliminación del nombre de dominio peruano de The Pirate Bay. (Atienza y Ruiz, 2006)

A principios de diciembre, The Pirate Bay comenzó a utilizar un dominio peruano (thepiratebay.pe) como dirección principal de su sitio web. Solo seis días después, el Comité de Derechos de Autor del Instituto Nacional para la Defensa de la Competencia y la Propiedad Intelectual (INDECOPI) emitió una medida cautelar extrajudicial de oficio ordenando al registrador peruano cancelar el nombre de dominio. La Comisión considera que en otros países basta con que los administradores de las páginas demanden por supuesta infracción de

derechos de autor. En ningún momento los dueños de los servicios afectados tuvieron la oportunidad de presentar su defensa, y ni siquiera se les informó sobre las precauciones. Tampoco se sabe que hayan iniciado procedimientos importantes por infracción de derechos de autor. (Atienza y Ruiz, 2006)

Lo peor de todo es que todo esto se hace dentro de los límites de la propia ley de derechos de autor. En el Perú, los organismos administrativos pueden tomar precauciones para ordenar la suspensión o cese de cualquier medio que se considere infractor de los derechos de autor. Esto significa que cualquier página web o expresión en línea puede ser suspendida sin un proceso en curso o sin respetar los derechos de defensa del afectado. ni siquiera necesitas a alguien pregunte, ya que pueden hacerlo en tu nombre. Esta es ciertamente una regla peligrosa cuando se aplica a Internet, y muestra cuán frágil es nuestra libertad de expresión en línea. (Atienza y Ruiz, 2006)

2. Ciberdelitos complejos

a. Ciberterrorismo

El ciberespacio es un medio incontrolable cuyo alcance puede superar las barreras, el idioma y las identidades para convertirse en un refugio para delincuentes y terroristas que encuentran la manera de ser accesibles y procesables. Los grupos terroristas no se han quedado atrás, y su constante y constante amenaza para la sociedad occidental subraya la necesidad de que nuestros gobiernos implementen medidas preventivas en todos los ámbitos posibles. La única forma de enfrentar esta forma de terrorismo es ser proactivos, para evitar comprometer infraestructuras críticas, cuyo ataque significaría una disrupción de dimensiones inimaginables en nuestra sociedad. (Kranenbarg, 2018)

b. Ciberguerra

La guerra cibernética puede entenderse como una agresión de un país dirigida a perturbar severamente la capacidad de otro país para imponer sus propios objetivos, o simplemente, robar información, cortar o interrumpir sus sistemas de comunicación, alterar sus bases de datos, como generalmente entendemos por guerra, pero en la diferencia es que los medios utilizados no son la violencia física, sino los ataques informáticos, que van desde: «la infiltración de los sistemas informáticos enemigos para obtener información, hasta el control informático de proyectiles, pasando por la planificación de batallas, la gestión de suministros, etc.» (Colle, 2000).

Sin embargo, para aquellos que piensan que la guerra cibernética y la guerra cibernética son lo mismo, se debe señalar que la guerra cibernética es el uso de todas las herramientas electrónicas e informáticas para destruir los sistemas electrónicos y de comunicación del enemigo y mantener el propio funcionamiento (Sánchez, 2008, p. 15).

c. Ataques Contra Infraestructura Crítica

La protección de la infraestructura crítica es un tema de preocupación para los países. Un alto nivel de desarrollo en la sociedad actual depende en gran medida de una gama de servicios básicos y esenciales, proporcionados principalmente por el sector privado. (Kranenbarg, 2018)

Las infraestructuras nunca han sido más importantes para el buen funcionamiento de los servicios y de los grandes sistemas productivos, como la administración, el agua, los sistemas financieros y fiscales, la energía, el espacio, la industria nuclear o el transporte. (Kranenbarg, 2018)

Instalaciones, redes, servicios y equipos cuya interrupción puede tener un impacto significativo en la salud, la seguridad o el bienestar económico de los ciudadanos es lo que entendemos por infraestructura crítica. (Kranenbarg, 2018)

Ante las nuevas amenazas, garantizar la seguridad del suministro de estos servicios esenciales no solo es responsabilidad de las administraciones públicas, sino también de los operadores privados a nivel nacional e internacional. (Kranenbarg, 2018)

d. Ciberespionaje y Hacktivismo

Technopedia describe el espionaje cibernético (ciberespionaje) como "una forma de delito cibernético en el que los piratas informáticos apuntan a redes informáticas en funcionamiento para obtener información clasificada o de otro tipo que puede o no ser beneficiosa para el pirata informático" (Kranenbarg, 2018).

Según el diccionario del Financial Times, el ciberespionaje "describe el robo de secretos almacenados en formato digital o en redes informáticas y de TI". (Kranenbarg, 2018)

Para Mark Russinovich (distinguiendo entre ciberespionaje, ciberataques y ciberguerra), ciberespionaje significa "recopilación de información o robo de propiedad intelectual", mientras que los ciberataques "socavan el funcionamiento de las redes informáticas" (p.13) y tienen "propósitos políticos o de seguridad nacional". Si bien la guerra cibernética involucra solo a actores estatales, también "interrumpe el funcionamiento de las redes informáticas", tiene "propósitos políticos o de seguridad nacional" y es "igual a un ataque armado o en el contexto de un conflicto armado". (Kranenbarg, 2018)

El hacktivismo se define de la siguiente manera: el uso de Internet y las nuevas tecnologías para atacar los sistemas de comunicación de empresas, gobiernos u otras entidades con el objetivo de criticar determinadas prácticas o reivindicar un estatus político o social. (Kranenbarg, 2018)

3. Amenazas emergentes

a. Tráfico de drogas y armas

Internet se utiliza para el tráfico ilícito de dos tipos de sustancias controladas:

1) Sustancias controladas ilegalmente (p. ej., heroína, cocaína, MDMA ("éxtasis"), marihuana);
2) Drogas controladas fabricadas legalmente (p. ej., oxicodona/oxicodona, hidrocodona y benzodiacepinas), sí
3) Adulteración de sustancias controladas en forma de productos farmacéuticos legales. (Astudillo, 2020)

Las sustancias alucinógenas no son legales desde la producción hasta el uso final. Es decir, se producen ilegalmente, generalmente en laboratorios clandestinos o se traen del extranjero ilegalmente y luego se distribuyen ilegalmente (tráfico).

La segunda categoría incluye sustancias que se producen legalmente en un entorno farmacéutico estrictamente regulado, pero que luego se venden a través de Internet de manera no controlada para justificar o incluso alentar el desvío hacia usos ilícitos. La tercera categoría incluye sustancias controladas falsificadas, que se clasifican como medicamentos legales porque se fabrican y venden intencionalmente como medicamentos legales. A los efectos de esta guía, los medicamentos pueden incluir las clases II y III. (Astudillo, 2020)

La venta de sustancias ilegales controladas en Internet es ilegal en primer lugar, es contrabando. Por otro lado, las drogas legales que se venden por Internet no son necesariamente ilegales. Pueden ser ofrecidos y vendidos en Internet para su consumo legítimo, en el supuesto de:

1) El consumidor, el prescriptor y la farmacia están ubicados en el mismo país; y (Astudillo, 2020)
2) Operan a través de protecciones que reflejan completamente las protecciones contra fraude y abuso que existen en las farmacias tradicionales. (Astudillo, 2020)

En los Estados Unidos, existen varias farmacias legales en Internet. Funcionan de manera similar a las farmacias minoristas tradicionales, que requieren recetas médicas reales, basadas en la relación médico-paciente, el diagnóstico, el tratamiento y las condiciones médicas reales. Sin embargo, la mayoría de los medicamentos que se venden en las farmacias de Internet no tienen protección contra el desvío. La venta de medicamentos en los sitios de Internet generalmente está permitida sin receta escrita o consejo médico. Si hay necesidad de una consulta, una simple "consulta en línea", generalmente un cuestionario que ya contiene respuestas predeterminadas para justificar la obtención del medicamento luego cierra y desconecta la sesión con la cooperación del médico. Si bien la distribución por Internet de ambas sustancias debería ser motivo de preocupación para las fuerzas del orden, esta guía se centra en la distribución de drogas. (Astudillo, 2020)

b. Extorsión en línea

Llamadas telefónicas o extorsión indirecta: Son llamadas realizadas por personas o grupos cuyas entidades son anónimas o modificadas deliberadamente. (Astudillo, 2020)

c. Difusión de una cultura de violencia

La exposición a contenidos violentos de los medios se menciona a menudo como un factor que contribuye a la violencia juvenil. Numerosos estudios han investigado esta relación utilizando varios métodos. Aunque los resultados no siempre son consistentes, en el campo de los estudios de medios se tiende a aceptar que la exposición a la violencia mediática es un factor de riesgo para promover la agresión interpersonal entre los menores. Los medios digitales han abierto nuevas vías a través de las cuales los jóvenes pueden acceder a contenidos violentos, de forma intencionada o no, y han ampliado el enfoque a nuevas formas de participar en agresiones sociales y relacionales en entornos online. Los medios digitales han abierto nuevas vías a través de las cuales los jóvenes pueden acceder a contenidos violentos, de forma intencionada o no, y han ampliado el enfoque a nuevas formas de participar en agresiones sociales y relacionales en entornos online. Este trabajo revisa las principales contribuciones, avances y novedades de la influencia mediática en el campo de la violencia juvenil y ofrece pautas recomendadas para los agentes sociales implicados en la prevención de la violencia. Finalmente, los autores ofrecen una visión optimista que enfatiza las oportunidades educativas y pro sociales para los mensajes de los medios y concluyen que se necesita más investigación en esta área. (Astudillo, 2020)

d. Lavado de dinero cibernético y evasión fiscal

El crecimiento y desarrollo de los mercados financieros globales ha facilitado la comunicación y el comercio entre países, y hace 80 años, no pensaban que pudiesen operar con divisas tan fácilmente como presionando un botón en una computadora. (Astudillo, 2020)

Esto ayuda a mejorar las relaciones y el marketing entre los diferentes países. Pero, así como las tecnologías legítimas pueden

> mejorar el comercio, también facilitan el llamado lavado de dinero. Los países con leyes para proteger la privacidad bancaria están directamente relacionados con los países con leyes para reportar transacciones bancarias. Estos dos intereses económicos, proteger la privacidad personal y reportar transacciones sospechosas a las agencias gubernamentales, hacen posible depositar dinero sucio en un país mal regulado y moverlo a cualquier otro país que sea más restrictivo. Se creó una red económica clandestina para apoyar y apoyar actividades delictivas y actos terroristas. (Astudillo, 2020)
>
> El lavado de dinero ocurre en casi todos los países del mundo. Un solo esquema de lavado de dinero puede involucrar transferencias a través de múltiples países para ocultar su origen. Cuanto más difícil sea rastrear sus orígenes, más difícil será condenar a las empresas criminales organizadas. (Astudillo, 2020)

2.2.2 Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos

Debe entenderse que, debido al progreso tecnológico y la globalización, la formación de un hombre que sirva dentro de las armas y las instituciones jurídicas, sin desconocer los principios y valores humanos, está sujeta a una serie de cambios estructurales y de la sociedad en que se vive. necesidades, no puede ser alienado de las dinámicas y momentos históricos, pero no puede salir de la formación de la esencia del soldado.

Tomemos como punto de partida las palabras de Sir Winston Churchill, "El entrenamiento debe ser tan fuerte que la guerra sea descanso", lo que claramente constituye el grado integral de requisitos que los reclutas deben obedecer al decidir aceptar la carrera armamentista. algunos criterios sencillos de tipo peruano: ser un joven con valores y principios estructurados, tener buenos y saludables hábitos; tener capacidad de decisión, recursiva y creativa para resolver problemas. Ser una persona segura a nivel personal y apegarse a sus metas; tener

la capacidad de reconocer sus fortalezas y debilidades; tener habilidades sociales y relaciones interpersonales adecuadas; debe estar interesado en la vida militar, disciplinado, dispuesto y comprometido para el servicio; la capacidad emprender cambios de vida y adaptarse al entorno militar, y el deseo de estar preparado en los campos del conocimiento militar, profesional, científico, investigativo y social.

1. Como profesional castrense

a. Cumple normas y reglamentos

Los deberes se entienden como una serie de obligaciones impuestas a un soldado por su situación en el ejército. Obediencia, obediencia, valentía, audacia, lealtad, desinterés, abnegación, etc., suele presentarse de diversas formas. El cumplimiento del deber es a menudo arduo y arduo, requiriendo muchas veces dolorosos sacrificios; pero es el único camino posible para un soldado que se da cuenta de su dignidad y de la importancia de la misión que su país le ha encomendado. Lograrlo con una fórmula tibia está en conflicto con el verdadero espíritu de la profesión. El ejército debe encontrar el estímulo necesario para cumplirlo en su propio nombre. (Reglamento General de Deberes Militares, 1937)

La disciplina es la norma a la que deben obedecer los militares, se basa en la obediencia y en un alto sentido del honor, la justicia y la moralidad, y tiene por objeto el cumplimiento fiel y exacto de los deberes prescritos por los reglamentos militares. (Reglamento General de Deberes Militares, 1937)

b. Posee porte y disciplina

El porte militar te permite proyectar una presencia digna y una imagen profesional de autoridad, para lo cual debes tener en cuenta lo siguiente:

1) El buen físico y los buenos modales ayudan a superar situaciones difíciles. (RE 1-54, 2014)
2) Siempre preocupándose por su buena apariencia porque sabe que representa autoridad y verse a sí mismo como un profesional lo hace competente, entiende que el amor propio comienza con verse muy bien porque siempre tiene que ser bueno. (RE 1-54, 2014)
3) Actuar siempre de manera profesional. (RE 1-54, 2014)
4) Llevar siempre un uniforme atrevido, elegante y de sentirse bien; transmitir siempre una imagen digna de profesionalismo, haciendo que su unidad, unidad y compañeros se vean muy bien frente a la sociedad. (RE 1-54, 2014)
5) Al manejar su imagen pública y exhibir la etiqueta militar, ayuda a enviar un mensaje claro de que siempre está orgulloso del uniforme que usa y sirve a su país. (RE 1-54, 2014)

c. Bachiller en Ciencias Militares

Los egresados del programa de Ciencias Militares están dotados de las habilidades para comandar sus divisiones o pelotones, destacados líderes, entrenadores y conductores, encargados de organizar, dirigir, coordinar, controlar y su empleo, así como ser responsables del manejo de personal, armamento , equipo, Desempeñar tareas por rango, como táctico, docente, administrador, técnico, investigador militar, etc., mostrando en todo momento profesionalismo y predicando con el ejemplo, debiendo demostrar un dominio completo de las normas para que sean cumplidas a cabalidad, y debe comprender los procedimientos para llevar a cabo este reglamento con fluidez, prontitud y eficacia; de esta manera, después de haber sido forjado durante su fase de preparación militar, será competente; por lo tanto, después de este período de prueba, podrá asumir las funciones requeridas para el cargo y estar física y mentalmente preparado para los diversos desafíos que enfrentó en su carrera militar.

d. Capacidad de liderazgo

La moral, los valores y las virtudes militares están integrados en su personalidad, y cultiva y proyecta a sus tropas y a la sociedad como un líder humano, cívico y de combate, mantiene y fortalece la moral militar, practica la autoconciencia y la ley de hierro, y respeta las normas institucionales. intereses. (RE 1-54, 2014)

Su bagaje axiológico se enmarca en los siguientes valores:

- Valores nacionales establecidos en la Constitución:
  - La defensa de la persona humana y el respeto de su dignidad
  - Vida
  - Igualdad
  - Libertad
  - Justicia
  - Identidad étnica y cultural
  - Paz. (RE 1-54, 2014)
- Valores establecidos en el Manual de Ética-Profesional Militar de las Fuerzas Armadas del Perú:
  - Honestidad
  - Veracidad
  - Laboriosidad
  - Disciplina. (RE 1-54, 2014)
- Valores Institucionales:

VALORES INSTITUCIONALES	ACTITUDES
COMPROMISO CON LA EXCELENCIA INSTITUCIONAL	• SER LIDER • SER COMPETENTE • MOSTRAR ESPIRITU DE SUPERACION • TENER INICIATIVA E INGENIO • TENER IDENTIDAD INSTITUCIONAL
INTEGRIDAD	• PROCEDER CON HONOR • SER LEAL • SER VERAZ • SER HONESTO • TENER DIGNIDAD • TENER AUTOESTIMA
DISCIPLINA	• SER RESPONSABLE • SER OBEDIENTE • SER JUSTO • SER PUNTUAL • SER RESPETUOSO
VOCACIÓN DE SERVICIO	• SER TOLERANTE • SER SOLIDARIO • SER PERSEVERANTE • TENER CORAJE • TENER DESPRENDIMIENTO Y ENTREGA • FORTALECER EL ESPIRITU DE CUERPO • TENER VALOR Y PATRIOTISMO

Esta formación académica de diez semestres desarrollará líderes completos, según un informe a la UNESCO (1996) de la "Comisión para la Educación Internacional en el Siglo XXI" presidida por Jacques Delors, que dijo Nuestra futura educación debe basarse en cuatro pilares:

- Aprender a conocer (Educación en la Ciencia Militar: EL SABER).
- Aprender a hacer (Técnica / Táctica en Combate: EL HACER).
- Aprender a ser (Líder de Carácter: EL SER).
- Aprender a vivir juntos (Integrado a la sociedad EL CONVIVIR).

Estos cuatro caminos o pilares educativos deben ser igualmente valorados para que el profesional se convierta en una experiencia integral que dure toda la vida, ya que determinan las bases que forman la capacidad actual de los futuros oficiales del Ejército para inspirar a los estudiantes (cadetes) en base a principios como promover la democracia Autonomía en el aprendizaje, apertura al diálogo participativo y

constructivo entre profesores (instructores militares) y cadetes, y previsión de la necesidad de formación a largo plazo de los oficiales, todo ello, recordando que vivimos en un mundo globalizado, que es cambiando rápida y continuamente, se deriva de la sociedad de la información y el conocimiento. (RE 1-54, 2014)

2. Como instructor militar

a. Estratega

Aplicar conocimientos tácticos y técnicos en la planificación, ejecución, ejecución, evaluación y control de las misiones/operaciones de combate de una división o pelotón; integrar principios de liderazgo, ética y liderazgo; demostrar que tiene visión de futuro, es proactivo y apropiado para las relaciones interpersonales para habilitar Es capaz de demostrar empatía y tomar decisiones rápidas y efectivas en el trabajo en equipo. (RE 1-54, 2014)

b. Educador

Planificar, desarrollar y evaluar el conocimiento teórico del aprendizaje, seleccionar y preparar el contenido de la asignatura, utilizar métodos, estrategias y técnicas de enseñanza apropiados e integrar las tecnologías de la información y la comunicación en las actividades docentes, integrar la responsabilidad, la integridad y el liderazgo en su Otro modelo a seguir y modelo a seguir para los subordinados y aquellos que trabajan en su entorno; demuestre apertura al cambio y la crítica, respétese mutuamente y concéntrese en desarrollar las habilidades de los subordinados. (RE 1-54, 2014)

c. Investigador

Aplicar metodología, investigación y conocimiento técnico militar para participar, formular, desarrollar, demostrar y apoyar proyectos de investigación en ciencia y tecnología militar para generar doctrina, desarrollar y actualizar tecnologías para sistemas de armas, equipos y materiales de guerra; integrar verdad, sinceridad, y responsabilidad; encarnan el Humanismo, una actitud proactiva y una visión sistémica de las tendencias innovadoras que buscan mejorar las capacidades militares. (RE 1-54, 2014)

d. Planificador

Aplicar los conocimientos teóricos para planificar, organizar, dirigir y controlar la gestión interna de los recursos humanos, logísticos y financieros, desarrollar la cultura organizacional de la unidad de manera integral, resolver y resolver los conflictos y problemas laborales emergentes y priorizar el bienestar. tus empleados; Honestidad, Lealtad, Responsabilidad y Disciplina en uno; Habilidad demostrada para ser estratégico, conciliar, integrar, innovar y motivar, capaz de adaptarse a las necesidades y demandas de una cultura organizacional para que pueda adaptarse rápidamente a los cambios en el ambiente y tomar el curso de acción más conveniente para resolver los problemas. (RE 1-54, 2014)

e. Líder

Desarrollar una cultura de respeto por la cultura militar, el liderazgo y la disciplina a través de la observancia y el cumplimiento de las reglas, reglamentos y normas relacionadas con la etiqueta militar, la actitud y la conducta militar, así como demostrando, exigiendo, respetando y haciendo cumplir la jerarquía militar, reglas y actividades que reforzarán la cultura organizacional; integra liderazgo, habilidades de liderazgo,

honestidad, lealtad, responsabilidad y disciplina; tiene la capacidad de mantener relaciones interpersonales y adecuadas, demostrar responsabilidad social, empatía y flexibilidad para adaptarse a cualquier entorno. (RE 1-54, 2014)

3. En el campo de la proyección social

a. Dominio del idioma

El conocimiento lingüístico es un aspecto del desempeño que indica qué tan bien el comunicador comprende las reglas del lenguaje. Si centramos nuestra atención en el nivel en el que los alumnos dominan las propiedades formales de los sistemas fonológico, léxico y gramatical, nos adentramos en el ámbito teórico. (Acosta, 2007)

El uso es el aspecto del desempeño demostrado por el comunicador al demostrar la capacidad de comunicarse de manera efectiva utilizando su conocimiento de las reglas del lenguaje. Si examinamos cómo los estudiantes adquieren y transmiten significado a través del proceso de comprensión y estructuración de la información en expresiones orales o escritas, examinamos el uso. Una forma de lograr esto es estudiando los aspectos pragmáticos del lenguaje, por ejemplo, a medida que los estudiantes aprenden a realizar actos de habla como argumentar, preguntar, persuadir, construir textos coherentes, armonizar textos con el contexto para el análisis crítico. (Acosta, 2007)

Uno de los objetivos de gran parte de la investigación lingüística aplicada es caracterizar el verdadero conocimiento de la lengua de los estudiantes, es decir, describir e interpretar su competencia comunicativa como un verdadero estado de desarrollo, tanto antes (diagnóstico preliminar) como después. Uso de instrumentos en la práctica docente de resolución de problemas de comunicación (diagnóstico final). La diferencia entre ambos estados refleja la transformación del objeto de

investigación, es decir, el desarrollo y perfeccionamiento del dominio de los sistemas del lenguaje y su aplicación en la comunicación. (Acosta, 2007)

Se trata de desarrollar y refinar los imperativos teóricos y prácticos de los estudiantes de idiomas que ya dominan, especialmente las habilidades de proceso y comunicación. Una pequeña parte del lenguaje que adquieren los estudiantes es el resultado de una construcción personal y social que no agota el potencial de desarrollo y debe acercarse continuamente a las normas, reglas y usos de todo el lenguaje como modos de comunicación. La investigación en el campo de los idiomas del mundo se centra en la investigación en el campo de la teoría de los sistemas del lenguaje, aunque actualmente se está prestando más atención al uso del lenguaje, porque es claro que incluso uno tiene que entender cómo aprenden los estudiantes ciertas cosas puramente. elementos formales (formación de palabras, correspondencia sujeto-verbo, predicados de sustantivo y verbo, etc.), es necesario confirmar que utilizan estos aspectos para expresar significado en determinadas situaciones comunicativas. (Acosta, 2007)

De esta manera, el análisis basado únicamente en la forma fue dando paso gradualmente al análisis correspondiente a forma-función-contexto y contexto-función-forma. De esta forma, se propugna una investigación que integre el aprendizaje de elementos formales con el uso funcional del lenguaje. (Acosta, 2007)

Por esta razón, discusiones recientes sobre pedagogía o metodología del lenguaje han enfatizado la importancia de brindar a los estudiantes oportunidades para comunicarse en el idioma que han aprendido a través de la interacción social, en línea con el pensamiento de Vygotsky y sus seguidores, que el aprendizaje ocurre en la interacción verbal. y la comunicación en sí misma es interacción social. También enfatiza la idea de que el lenguaje es forma, significado y función, lo que

requiere un análisis integral de los sistemas lingüísticos y su uso, así como las relaciones texto-contexto (semántico-pragmática), y responde a las necesidades comunicativas de las personas, alumno. (Acosta, 2007)

b. Responsabilidad social

La responsabilidad social es un compromiso con temas de interés público, tales como: el medio ambiente, la pobreza, la desigualdad de ingresos, la salud, el hambre, la desnutrición y el analfabetismo, es responsabilidad de todo tipo de organizaciones (empresas, estados, universidades) que asumen Acción social para el impacto positivo, aportando soluciones basadas en la transparencia, la diversidad, la sostenibilidad y la ética, con el objetivo del desarrollo sostenible de las personas y su entorno. (Bowen, 1953)

c. Diplomacia

La diplomacia es como la ciencia de las relaciones exteriores, el arte de negociar, el manejo de las relaciones exteriores, la ciencia de las relaciones que existen entre diversos países, la forma de cimentar una determinada política exterior. (Jara, 1989)

Cualquiera que sea la definición, la diplomacia significa establecer relaciones interestatales con la comunidad internacional, negociando y dirigiendo los intereses de sus gobiernos en la vida relacional. (Jara, E., 1989)

Por ello, la diplomacia no tiene otro propósito que unir a los pueblos, acercar a los gobernantes a sus políticas y aliviar las dificultades entre ellos. Por lo tanto, la actitud de los involucrados debe ser tan constructiva como los principios que guían el arte que crean. (Jara, 1989)

Así mismo, la diplomacia contiene un elemento de política interna, íntimamente relacionado con los fines que persigue el gobierno, y se convierte así en una forma de obtener apoyo internacional para una política a través de la acción organizada de expertos llamados diplomáticos. En este sentido, estamos hablando de la diplomacia de un país en algún momento de su historia. (Jara, 1989)

El objetivo principal de la diplomacia es conseguir la paz en la región y mundo. Un país representa a otro, sirve a sus intereses, negocia y debe unir todos los esfuerzos de la diplomacia mundial para lograr este gran objetivo. (Jara, 1989)

¿La diplomacia es una ciencia o un arte? De hecho, es tanto porque emplea reglas básicas como preceptos que están metódicamente organizados de cierta manera y que pueden aplicarse sistemáticamente. Sin embargo, dado que no existen reglas fijas universalmente y están muy influenciadas por las costumbres regionales y locales y las habilidades personales, el concepto de arte parece triunfar sobre el concepto de ciencia. Si la diplomacia es una ciencia, algunos autores que apoyan esta elección dicen que es una ciencia imprecisa de todos modos. Importantes consecuencias se derivan de este carácter, cualidad que deben poseer quienes pretenden serlo. (Jara, 1989)

2.3 Marco Conceptual

Actitudes: Frente a las diversas alternativas que ofrece el ambiente de trabajo, los sujetos tienden a aplicar estándares éticos, estéticos y de seguridad a las personas, instalaciones y equipos, y al medio ambiente de manera responsable y autónoma.

Aprendizaje: Es el proceso de adquisición de conocimientos, habilidades, actitudes o valores a través del aprendizaje, la experiencia o la enseñanza.

Área ocupacional: Un determinado perfil profesional puede cubrir un espacio de empleo potencial en función de sus habilidades profesionales desarrolladas.

Capacidades: Su definición operativa más común sugiere que quienes las poseen pueden encontrar información y técnicas adecuadas a partir de la experiencia previa para abordar de manera efectiva los desafíos de diferentes dificultades y entornos. Requiere la capacidad de analizar o comprender situaciones nuevas, usar conocimientos y métodos previos cuando corresponda, y discernir las relaciones apropiadas entre la experiencia previa y los problemas actuales.

Ciberataque: Esta es una táctica ofensiva llevada a cabo por individuos u organizaciones con el fin de destruir diferentes tipos de sistemas informáticos.

Cibercrimen: Este es un delito cometido a través de una red en línea o en red y busca afectar una computadora o cualquier dispositivo de red relacionado con la informática.

Ciberdelincuentes: Persona que realiza acciones delictivas mediante el medio de internet.

Ciberespacio: Es un espacio virtual creado por medios cibernéticos con el propósito de transmitir información a través de la red.

Competencia profesional: Por lo tanto, definimos el conjunto complejo e integral de competencias, habilidades, competencias y actitudes que las personas invierten para resolver los problemas que plantean en una variedad de entornos de trabajo del mundo real, con base en estándares de desempeño satisfactorios en cada área profesional.

Competencias laborales: Los adquiridos por quienes están fuera de la institución educativa en su desempeño profesional.

Competencias profesionales: Conocimientos y habilidades para permitir actividades profesionales de acuerdo con las necesidades de producción y empleo.

Datos: Son hechos que han sido registrados de manera cuantitativa o cualitativa.

Destrezas: Son habilidades prácticas relacionadas con el desarrollo preciso de determinadas habilidades motrices profesionales, la visión, el oído, el gusto, la fuerza física, el equilibrio, etc. (por ejemplo, adquirir habilidades motoras finas para un trabajo preciso o detallado, usar ciertas herramientas para lograr ciertos resultados con precisión, etc.). Analizar las habilidades como habilidades prácticas nos permite alejarnos de una visión puramente conductual de su educación.

Estándar: Es un patrón, un punto de referencia para medir el valor de las cosas, una organización de la misma especie.

Formación profesional: Así se denomina a un conjunto de ofertas formativas, expresadas de forma coherente y sistemática, con objetivos tanto de formación en el puesto de trabajo como en el puesto de trabajo, independientemente del nivel de cualificación (desde nivel inicial hasta técnicos superiores). Nos basamos en un concepto amplio e incluyente de la formación profesional, ya que facilita el proceso de inserción y/o especialización y/o reconversión de carrera en las materias, teniendo en cuenta su relevancia para el mercado laboral en términos de empleabilidad y empleabilidad, no olvidar el componente de formación cívica. Estas sociedades del conocimiento exigen a sus miembros el desarrollo de la profesionalidad en la formación continua o a lo largo de toda la vida.

Gestión de riesgos: El proceso de determinación de las medidas necesarias para proteger cualquier servicio.

Habilidades: El desarrollo de competencias corresponde a la adquisición de una serie de prácticas metodológicas y técnicas en una determinada ocupación, persona profesional o campo ocupacional. Habilidad se refiere a la capacidad práctica de un método para acortar un proceso intelectual o mental (por ejemplo, al trabajar con materias primas o al calcular una determinada aplicación financiera, al determinar la entrada de una proporción, disparo o kilogramo). Curiosamente, el tiempo transcurrido de capacidad en capacidad se convierte en un indicador del nivel de calificación de la capacidad.

Información: Son datos procesados que contienen mensajes que permiten a la persona o sistema que recibe el mensaje adquirir nuevos conocimientos.

Infraestructuras críticas: Un sistema físico o virtual que facilita funciones y servicios centrales para respaldar el sistema central.

Liderazgo: La sociedad reconoce las competencias y competencias que debe poseer un equipo directivo para conducir una organización hacia la excelencia. Los líderes deben demostrar claramente su compromiso con la mejora continua, desarrollar una misión y visión de la agencia, participar y actuar en sus procesos, servir como modelos a seguir para el resto de la organización y confiar en las agencias asociadas.

Organización: Es un ajuste sistemático entre personas que desean alcanzar algún propósito en común.

Orientación Profesional: Un proceso que vincula actividades de información, asesoramiento y aprendizaje sobre posibles desarrollos profesionales. Esta función contiene información sobre las necesidades actuales y potenciales del mercado laboral, el desarrollo de cualificaciones y los requisitos de formación de especialización en determinadas disciplinas. Requiere que las instituciones de educación vocacional tengan información sistemática y actualizada sobre el desarrollo de la industria en términos de empleo y sus

requisitos en términos de calificaciones requeridas, transferibilidad y educación formal.

Perfil Profesional: Es una descripción de las habilidades profesionales específicas requeridas para trabajar en un campo profesional específico. Expresa la lógica de producción cuyo propósito es proporcionar insumos relevantes para la formación de organizaciones. Es una referencia fundamental para el diseño curricular, ya que orienta el proceso de formación al especificar el desempeño que desarrollarán los temas, cómo evaluarlos de manera efectiva y los alcances y condiciones de la práctica profesional.

Seguridad: Es una característica de alguna persona o máquina que esta con ausencia de peligro.

Sistema: Es un conjunto de medidas o procedimientos que guían el correcto funcionamiento de un grupo.

Valores: Principios rectores que configuran el comportamiento del personal de la institución y determinan todas sus interrelaciones.

2.4 Operacionalización de las variables

Tabla 1. *Operacionalización de las variables*

VARIABLES	DIMENSIONES	INDICADORES	ITEMS	ESCALA
Variable Independiente **(X)** Instrucción de Ciberdefensa	**X_1** Ciberdelito convencional	• Acceso Ilegal (Craqueo) • Interceptación de Datos • Pornografía Infantil • Spam • Incitación al Odio • Fraude Bancario • Robo de Identidad • Infracciones de Derechos de Autor	1 2 3 4 5 6 7 8	NOMINAL
	X_2 Ciberdelitos complejos	• Ciberterrorismo • Ciberguerra • Ataques Contra Infraestructura Crítica • Ciberespionaje y Hacktivismo	9 10 11 12	
	X_3 Amenazas emergentes	• Tráfico de drogas y armas • Extorsión en línea • Difusión de una cultura de violencia • Lavado de dinero cibernético y evasión fisca	13 14 15 16	
Variable Dependiente **(Y)** Perfil del Oficial de Comunicaciones	**Y_1** Como profesional castrense	• Cumple normas y reglamentos • Posee porte y disciplina • Bachiller en ciencias militares • Capacidad de liderazgo	17 18 19 20	NOMINAL
	Y_2 Como instructor militar	• Estratega • Educador • Investigador • Planificador • Líder	21 22 23 24 25	
	Y_3 En el campo de la proyección social	• Dominio del idioma • Responsabilidad social • Diplomacia	26 27 28	

2.5 Hipótesis de la investigación

2.5.1 Hipótesis general

La Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

2.5.2 Hipótesis especificas

- La Instrucción de Ciberdelito convencional se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

- La Instrucción de Ciberdelitos complejos se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

- La Instrucción de Amenazas emergentes se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Enfoque de investigación

Rodríguez (2010), señaló que los métodos cuantitativos se centran en los acontecimientos u orígenes de los fenómenos sociales y se preocupan menos en el estado subjetivo del individuo (p. 32). El método utiliza cuestionarios, listas de verificación y análisis demográfico para generar cifras que se pueden usar para validar, aceptar o rechazar relaciones entre variables definidas por análisis estadístico y para presentar periódicamente los resultados de la investigación cuantitativa en tablas, tablas y gráficos estadísticos.

3.2 Tipo de Investigación

El tipo de investigación fue básica, ya que esta busca dar respuesta a cuestiones teóricas de cambio de modelo y se orienta "a describir y explicar", en cierta medida, "encaminarla a la investigación básica o pura" (Sánchez y Reyes, 2002, p. 18-19) validó la observación: "Toda investigación básica puede ser sustantiva, pero no toda investigación sustantiva" (p. 21).

3.3 Método de Investigación

En este trabajo de investigación utilizamos el método hipotético-deductivo porque partimos de suposiciones hechas a partir de principios o leyes, o sacamos inferencias de datos empíricos, aplicamos las reglas de deducción, y si las predicciones que hacemos son consistentes, entonces las predicciones que hacemos se validan empíricamente. Verificar su autenticidad con los hechos, esta no es la suposición original. Este tratamiento común por parte de los médicos ilustra claramente el enfoque general adoptado por la deducción hipotética. La esencia del método es utilizar la verdad o falsedad del enunciado subyacente (basado en su verificación empírica) para inferir la verdad o falsedad de la hipótesis que estamos probando. Toma los contraejemplos más

exigentes y determina si están satisfechos. Refutar estos contraejemplos significa probar la verdad de la hipótesis (Behar, 2008, p.147).

3.4 Alcance de investigación (nivel)

El nivel de este trabajo de investigación es descriptivo, que como su nombre lo indica, permite describir situaciones, fenómenos o eventos de nuestro interés, medirlos y comprobar sus características. La investigación descriptiva busca identificar cualidades, características y características de personas, grupos, comunidades, o cualquier otro fenómeno que requiera análisis. (Hernández, Fernández y Baptista, 2016).

3.5 Diseño de la Investigación

El diseño del estudio se clasificó como no experimental, pero también transversal-descriptivo, y se administró en un modelo de campo. En este sentido, Méndez (2009) sostiene que, en los estudios no experimentales, solo se observan condiciones preexistentes, es decir, se ha producido el desarrollo de una o más variables y el investigador no tiene control directo sobre ellas.

3.6 Población, muestra, unidad de estudio

3.6.1 Población de estudio

Por su parte, Hernández et al. (2016) plantean que una población constituye un conjunto de personas, objetos, instituciones u otros que comparten ciertas características, y proporciona la información contenida en ellos como objeto de investigación y extrae conclusiones. Acerca de los resultados.

La población a delimitar la investigación estuvo conformada por veintisiete (27) Cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

3.6.2 Muestra

Hernández S. citado en Castro (2003), afirmando que “si la población es menor de cincuenta (50) personas, la población es igual a la muestra " (p.69).

Por lo tanto, la muestra será determinada por la totalidad de la población, veintisiete (27) Cadetes de 4to año del arma de Comunicaciones, por no ser una cantidad significativa.

3.6.3 Unidad de estudio

La de estudio estará conformada por t veintisiete (27) Cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

3.7 Técnica e Instrumento para la recolección de datos

3.7.1 Técnica de recolección de datos

De acuerdo con Hernández et al (2016), recopilar datos significa crear un método de procedimiento detallado para recopilar datos para un propósito específico. Sabino (2008) Señale que una herramienta de recopilación de datos es cualquier recurso que los investigadores utilizan para procesar fenómenos y extraer datos directamente.

A partir de ahí, se puede concluir que las técnicas de recolección de datos son todos los métodos que se pueden utilizar para obtener información sobre un tema específico. Cabe señalar que existen varias herramientas diferentes de recopilación de datos, incluso a través de cuestionarios, uno de los cuales es el más común.

Al respecto, con el fin de optimizar el desarrollo de este estudio, el proceso de recolección de datos se llevó a cabo por medio de técnicas de encuesta, lo que

Sabino (2008) interpreta como la investigación del desarrollo de determinados fenómenos a través de interrogantes directas. Para Bavaresco (2013), una encuesta es un medio que detalla las interrogantes, variables, dimensiones e indicadores a encuestar para medir variables y obtener conclusiones numéricas (p. 32).

En el mismo sentido, se emplea una herramienta tipo cuestionario, que Hurtado (2000), define como una herramienta formada por una serie de preguntas estrechamente relacionadas con las variables de investigación. Por otro lado, para Hernández et al. (2016), el cuestionario consiste básicamente en un conjunto de preguntas sobre una o más variables a medir, considerando que deben estar claramente enunciadas y que no es conveniente dar respuestas.

3.7.2 Instrumento de recolección de datos

Un cuestionario es una herramienta que agrupa una serie de preguntas relacionadas con un evento, situación o tema específico sobre el cual el investigador desea obtener información (Hurtado, 2000). Asimismo, Ander-Egg (2003) afirma que consiste en un conjunto más o menos amplio de preguntas diseñadas para obtener respuestas con datos e información sobre un tema o pregunta específica. Es una herramienta estrictamente estandarizada para traducir y tratar ciertos temas que son objeto de investigación.

Los cuestionarios se pueden preparar de varias formas: utilizando ítems en forma de preguntas, enunciados o instrucciones, abiertas o cerradas, sobre los aspectos a recoger, en todo caso tiene ventajas y desventajas.

3.7.3 Validez y confiabilidad de los instrumentos de medición

Validez

Una vez desarrollado un instrumento, pasa por un proceso de validación, que Hernández et al. (2016) definen como el grado en que una prueba o pregunta mide lo que pretende medir. Méndez (2009) señaló que para que una herramienta sea

suficiente, debe registrar datos representativos de las variables en estudio. En este caso, para validar el instrumento se utilizó el juicio de 5 expertos, quienes son expertos en el campo de estudio propuesto, para evaluar y brindar asesoría para determinar el desempeño del instrumento.

Confiabilidad

Para todo estudio, el instrumento debe ser confiable, y según Hurtado (2000), la confiabilidad se describe como uno de los requisitos fundamentales de la investigación cuantitativa, a partir del grado de consistencia con el que el instrumento logra su propósito, que busca aplicar los mismos objetos repetidamente, esperando resultados similares.

En el mismo sentido, Hernández et al., (2016) afirmaron que, para medir la confiabilidad, se utilizó un coeficiente de 0 a 1, cuya interpretación se basó en que a medida que el coeficiente se aproximaba a 1 (1), el instrumento sería más confiable, de lo contrario, el instrumento sería menos confiable. En base a lo anterior se puede determinar la confiabilidad, se realizó una prueba piloto del instrumento aplicado, a una población de 28 unidades informantes pertenecientes a la escuela militar "Coronel Francisco Bolognesi" de Chorrillos, por otro lado, los resultados evaluaron esta prueba. Prueba usando la fórmula de Alpha Cronbach.

3.8 Procesamiento y método de análisis de datos

3.8.1 Técnica para el procesamiento de datos

Una vez recolectados los datos de la investigación a través de cuestionarios a las unidades proveedoras de información, se inicia el proceso de tabulación, clasificación y procesamiento de la información obtenida, lo que según Chávez (2007) sugiere que la tabulación de datos es utilizada por los investigadores y los métodos de tratamiento de la información recolectada organizará continuamente los datos relacionados con variables, indicadores y artículos (p.59)

Para Hurtado (2010), una vez obtenidos los resultados, se debe realizar el análisis de acuerdo con los objetivos establecidos al inicio de la encuesta, y se debe determinar qué análisis se utilizará, ya sea estadístico, analítico, de contenido o analítico. Simbolista. En cuanto a la aplicación de pruebas estadísticas, se realizaron cálculos de frecuencias absolutas y relativas para representar los datos obtenidos a través de tablas, permitiendo la visualización de resultados cuantitativos.

3.8.2 Método de análisis de datos

- **Análisis descriptivo**

  En el caso de las estadísticas de análisis descriptivo, este tipo de enfoque proporciona un medio para resumir la información proporcionada por los datos de la muestra. Es decir, su objetivo es sintetizar información para brindar datos precisos, simples, claros y ordenados.

- **Análisis Inferencial (Prueba de hipótesis)**

  El análisis estadístico inferencial proporciona herramientas que permiten una evaluación sistemática y eficiente de la muestra poblacional objeto de estudio.

3.9 Aspectos éticos

La investigación considera los siguientes criterios éticos:

- La investigación tiene un valor social y científico.
- La investigación tiene validez científico-pedagógica.
- Para realizar la investigación ha existido un consentimiento informado y un respeto a los participantes.

CAPITULO IV

Resultados

4.1 Análisis Descriptivo

Tabla 2.

Instrucción de ciberdefensa y el Perfil del Cadete Egresado de Comunicaciones

			Perfil del Cadete Egresado de Comunicaciones					Total
			Nunca	Casi Nunca	A veces	Casi Siempre	Siempre	
Instrucción de Ciberdefensa	Nunca	Recuento	1	0	0	0	0	1
		%	100,0%	0,0%	0,0%	0,0%	0,0%	100,0%
	Casi Nunca	Recuento	0	2	1	0	0	3
		%	0,0%	66,7%	33,3%	0,0%	0,0%	100,0%
	A veces	Recuento	0	0	1	3	0	4
		%	0,0%	0,0%	25,0%	75,0%	0,0%	100,0%
	Casi Siempre	Recuento	0	0	0	14	0	14
		%	0,0%	0,0%	0,0%	100,0%	0,0%	100,0%
	Siempre	Recuento	0	0	0	1	4	5
		%	0,0%	0,0%	0,0%	20,0%	80,0%	100,0%
Total		Recuento	1	2	2	18	4	27
		%	3,7%	7,4%	7,4%	66,7%	14,8%	100,0%

El 80% de los encuestados señalan que siempre la Instrucción de ciberdefensa guarda una relación directa y significativa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Figura 1

Instrucción de ciberdefensa y el Perfil del Cadete Egresado de Comunicaciones

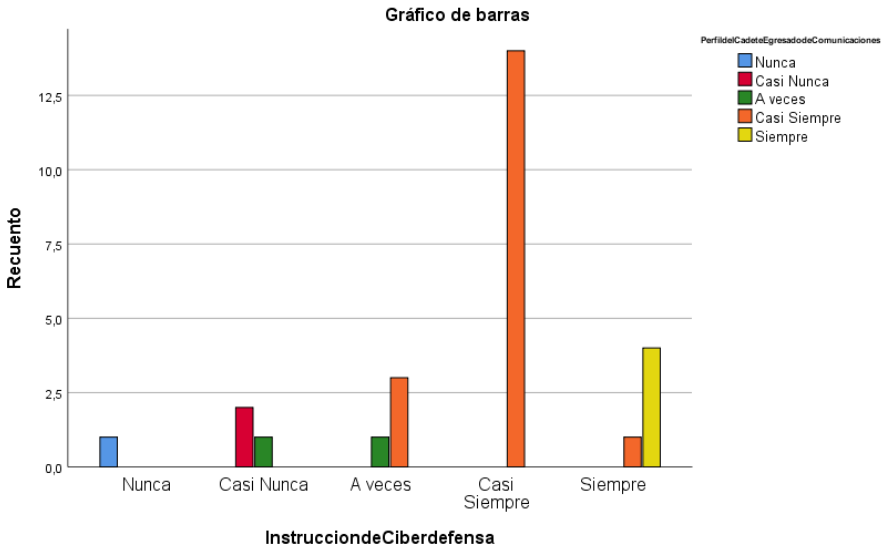


Tabla 3.

Ciberdelito Convencional y el Perfil del Cadete Egresado de Comunicaciones

			Perfil del Cadete Egresado de Comunicaciones					Total
			Nunca	Casi Nunca	A veces	Casi Siempre	Siempre	
Ciberdelito Convencional	Nunca	Recuento	1	0	1	0	0	2
		%	50,0%	0,0%	50,0%	0,0%	0,0%	100,0%
	Casi Nunca	Recuento	0	1	0	0	0	1
		%	0,0%	100,0%	0,0%	0,0%	0,0%	100,0%
	A veces	Recuento	0	1	1	4	0	6
		%	0,0%	16,7%	16,7%	66,7%	0,0%	100,0%
	Casi Siempre	Recuento	0	0	0	10	1	11
		%	0,0%	0,0%	0,0%	90,9%	9,1%	100,0%
	Siempre	Recuento	0	0	0	4	3	7
		%	0,0%	0,0%	0,0%	57,1%	42,9%	100,0%
Total		Recuento	1	2	2	18	4	27
		%	3,7%	7,4%	7,4%	66,7%	14,8%	100,0%

El 90,9% de los encuestados señalan que casi siempre la Instrucción de Ciberdelito convencional guarda relación significativa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Figura 2

Ciberdelito Convencional y el Perfil del Cadete Egresado de Comunicaciones

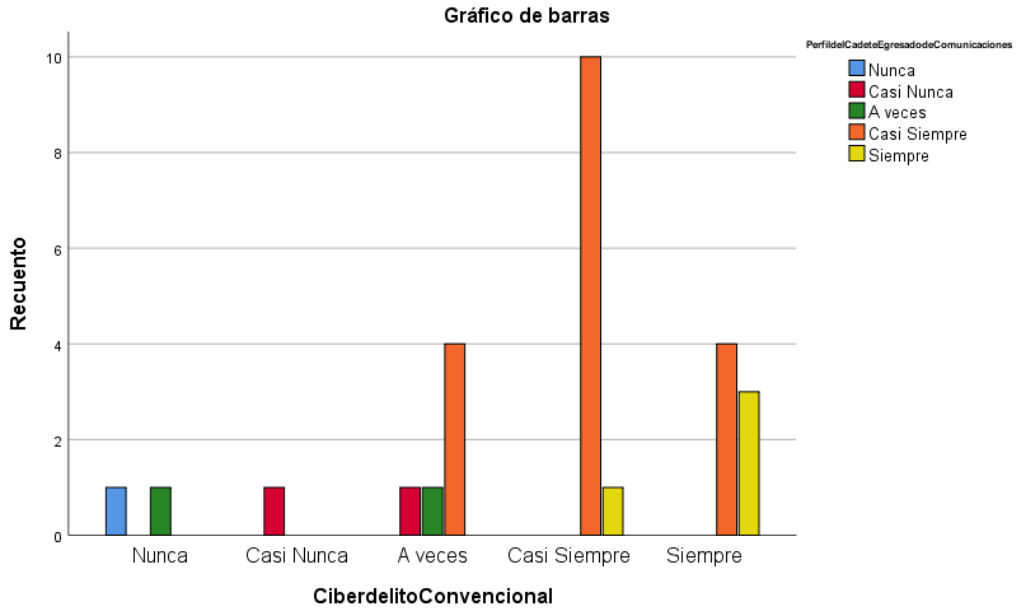


Tabla 4.

Ciberdelitos Complejos y el Perfil del Cadete Egresado de Comunicaciones

			Perfil del Cadete Egresado de Comunicaciones					Total
			Nunca	Casi Nunca	A veces	Casi Siempre	Siempre	
Ciberdelitos Complejos	Nunca	Recuento	1	1	0	0	0	2
		%	50,0%	50,0%	0,0%	0,0%	0,0%	100,0%
	Casi Nunca	Recuento	0	1	0	0	0	1
		%	0,0%	100,0%	0,0%	0,0%	0,0%	100,0%
	A veces	Recuento	0	0	2	2	0	4
		%	0,0%	0,0%	50,0%	50,0%	0,0%	100,0%
	Casi Siempre	Recuento	0	0	0	11	0	11
		%	0,0%	0,0%	0,0%	100,0%	0,0%	100,0%
	Siempre	Recuento	0	0	0	5	4	9
		%	0,0%	0,0%	0,0%	55,6%	44,4%	100,0%
Total		Recuento	1	2	2	18	4	27
		%	3,7%	7,4%	7,4%	66,7%	14,8%	100,0%

El 100% de los encuestados señalan que casi siempre la Instrucción de Ciberdelitos complejos guarda relación significativa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Figura 3.

Ciberdelitos Complejos y el Perfil del Cadete Egresado de Comunicaciones

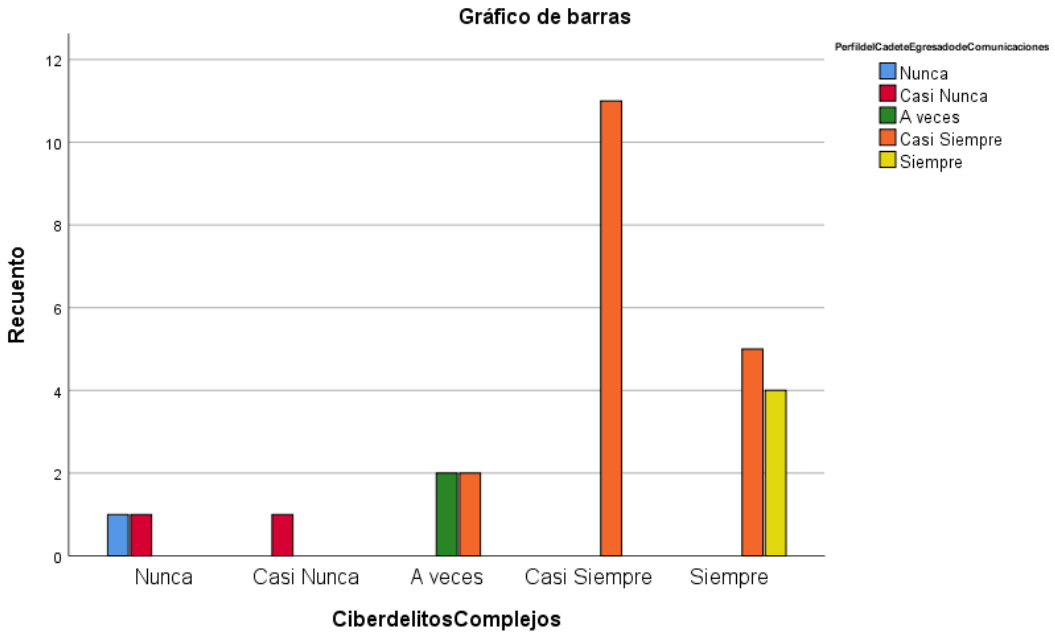


Tabla 5.

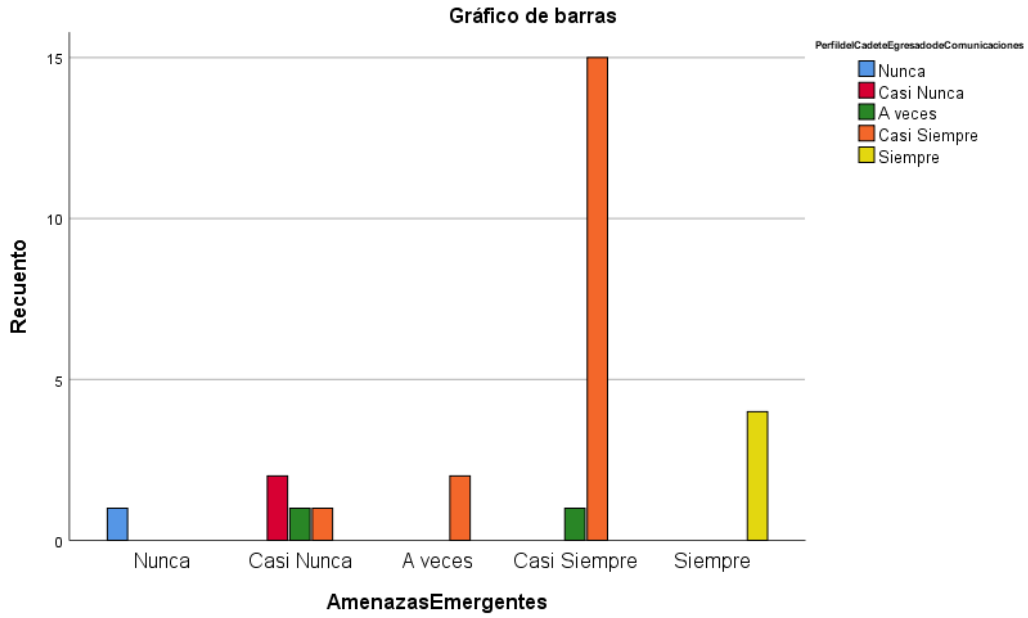
Amenazas Emergentes y el Perfil del Cadete Egresado de Comunicaciones

			Perfil del Cadete Egresado de Comunicaciones					Total
			Nunca	Casi Nunca	A veces	Casi Siempre	Siempre	
Amenazas Emergentes	Nunca	Recuento	1	0	0	0	0	1
		%	100,0%	0,0%	0,0%	0,0%	0,0%	100,0%
	Casi Nunca	Recuento	0	2	1	1	0	4
		%	0,0%	50,0%	25,0%	25,0%	0,0%	100,0%
	A veces	Recuento	0	0	0	2	0	2
		%	0,0%	0,0%	0,0%	100,0%	0,0%	100,0%
	Casi Siempre	Recuento	0	0	1	15	0	16
		%	0,0%	0,0%	6,3%	93,8%	0,0%	100,0%
	Siempre	Recuento	0	0	0	0	4	4
		%	0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
Total		Recuento	1	2	2	18	4	27
		%	3,7%	7,4%	7,4%	66,7%	14,8%	100,0%

El 100% de los encuestados señalan que siempre la Instrucción de Amenazas emergentes guara relación significativa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Figura 4

Amenazas Emergentes y el Perfil del Cadete Egresado de Comunicaciones



4.2 Análisis Inferencial (Prueba de hipótesis)

***Hipótesis general* (Paso 1)**

La Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022.

Hipótesis general nula

La Instrucción de ciberdefensa no se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022.

Paso 2

Nivel de significancia = 0.05

Paso 3

Cálculo del grado de relación

Tabla 6.

Correlación de la hipótesis general

			Instrucción de Ciberdefensa	Perfil del Cadete Egresado de Comunicaciones
Rho de Spearman	Instrucción de Ciberdefensa	Coeficiente de correlación	1,000	,877**
		Sig. (bilateral)	.	,000
		N	27	27
	Perfil del Cadete Egresado de Comunicaciones	Coeficiente de correlación	,877**	1,000
		Sig. (bilateral)	,000	.
		N	27	27

**. La correlación es significativa en el nivel 0,01 (bilateral).

Paso 4

Regla de decisión: Si p<0.05 rechazar Ho, caso contrario aceptar Ho

Paso 5

Decisión estadística: Dado que 0.000<0.05 se rechaza la Ho.

Paso 6

Conclusión: En la muestra, la Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", siendo el coeficiente de correlación Rho Spearman =877 así mismo p=0.000 < 0.05 señala que existe una relación significativa entre las variables de estudio.

Hipótesis específica 1 **(Paso 1)**

La Instrucción de Ciberdelito convencional se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022.

Hipótesis específica nula 1

La Instrucción de Ciberdelito convencional no se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022.

Paso 2

Nivel de significancia = 0.05

Paso 3

Cálculo del grado de relación

Tabla 7.

Correlación de la hipótesis especifica 1

			Ciberdelito Convencional	Perfil del Cadete Egresado de Comunicaciones
Rho de Spearman	Ciberdelito Convencional	Coeficiente de correlación	1,000	,714**
		Sig. (bilateral)	.	,000
		N	27	27
	Perfil del Cadete Egresado de Comunicaciones	Coeficiente de correlación	,714**	1,000
		Sig. (bilateral)	,000	.
		N	27	27

**. La correlación es significativa en el nivel 0,01 (bilateral).

Paso 4

Regla de decisión: Si p<0.05 rechazar Ho, caso contrario aceptar Ho

Paso 5

Decisión estadística: Dado que 0.000<0.05 se rechaza la Ho.

Paso 6

Conclusión: En la muestra, la Instrucción de Ciberdelito convencional se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, siendo el coeficiente de correlación Rho Spearman =0.714 así mismo p=0.000<0.05 señala que existe una relación entre la variable y dimensión de estudio.

Hipótesis específica 2 **(Paso 1)**

La Instrucción de Ciberdelitos complejos se relaciona significativamente con el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Hipótesis específica nula 2

La Instrucción de Ciberdelitos complejos no se relaciona significativamente con el perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Paso 2

Nivel de significancia = 0.05

Paso 3

Cálculo del grado de relación

Tabla 8.

Correlación de la hipótesis especifica 2

			Ciberdelitos Complejos	Perfil del Cadete Egresado de Comunicaciones
Rho de Spearman	Ciberdelitos Complejos	Coeficiente de correlación	1,000	,785**
		Sig. (bilateral)	.	,000
		N	27	27
	Perfil del Cadete Egresado de Comunicaciones	Coeficiente de correlación	,785**	1,000
		Sig. (bilateral)	,000	.
		N	27	27

**. La correlación es significativa en el nivel 0,01 (bilateral).

Paso 4

Regla de decisión: Si $p<0.05$ rechazar Ho, caso contrario aceptar Ho

Paso 5

Decisión estadística: Dado que $0.000<0.05$ se rechaza la Ho.

Paso 6

Conclusión: En la muestra, la Instrucción de Ciberdelitos complejos se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, siendo el coeficiente de correlación Rho Spearman =0.785 así mismo p=0.000<0.05 señala que existe una relación entre las variables de estudio.

Hipótesis específica 3 **(Paso 1)**

La Instrucción de Amenazas emergentes se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Hipótesis específica nula 3

La Instrucción de Amenazas emergentes no se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.

Paso 2

Nivel de significancia = 0.05

Paso 3

Cálculo del grado de relación

Tabla 9.

Correlación de la hipótesis especifica 3

			Amenazas Emergentes	Perfil del Cadete Egresado de Comunicaciones
Rho de Spearman	Amenazas Emergentes	Coeficiente de correlación	1,000	,842**
		Sig. (bilateral)	.	,000
		N	27	27
		Coeficiente de correlación	,842**	1,000
		Sig. (bilateral)	,000	.

	Perfil del Cadete Egresado de Comunicaciones	N	27	27

**. La correlación es significativa en el nivel 0,01 (bilateral).

Paso 4

Regla de decisión: Si p<0.05 rechazar Ho, caso contrario aceptar Ho

Paso 5

Decisión estadística: Dado que 0.000= <0.05 se rechaza la Ho.

Paso 6

Conclusión: En la muestra, la Instrucción de Amenazas emergentes se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", siendo el coeficiente de correlación Rho Spearman =0.842 así mismo p=0.000<0.05 señala que existe una relación entre las variables de estudio.

CAPÍTULO V

Discusión de Resultados

Considerando a la hipótesis general que la Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022, con un grado de correlación de Spearman de un Rho= 0.877, lo cual demostró que tienen una correlación alta y significativa: Una vez contrastado el resultado encontramos que tiene relación con la investigación de Pérez, W. y Ramos, M. (2020). El uso obligatorio de las TIC genera una serie de riesgos que afectan los derechos de las personas, la infraestructura de información crítica y los intereses vitales de todos los usuarios de Internet, una amenaza que las Fuerzas Armadas del Ecuador no han olvidado, traduciéndose en una falta de ciberseguridad para mantener el licenciamiento y proteger los medios digitales. Las políticas de seguridad causan grandes problemas. Ante las amenazas cibernéticas y la ausencia de una política de seguridad cibernética, el trabajo de esta

titulación se enfocará en el desarrollo de la política de seguridad digital analizando distintos estándares internacionales e incorporación del análisis jurídico a nivel nacional en distintas instituciones, facilitando así la integración de instituciones que gestionan riesgos en el ciberespacio coordinación entre. Por último, se propone una política de ciberseguridad para preservar la información digital de las FFAA, de acuerdo con la normativa y recomendaciones de los organismos del país encargados de la seguridad informática, como el Ministerio de Telecomunicaciones (MINTEL), que facilitara cumplir y actuar de acuerdo a nuestra agencia en el campo legal, tecnología Madurez de dominio, dominio organizacional para realizar actividades, buscar cooperación con diferentes agencias responsables de la seguridad de datos.

Considerando a la hipótesis especifica 1 que la Instrucción de Ciberdelito convencional se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022, con un grado de correlación de Spearman de un Rho= 0.714, lo cual demostró que tienen una correlación alta y significativa: Una vez contrastado el resultado encontramos que tiene relación con la investigación de Chiza, D. y Izurieta, H. (2020). El siglo XXI ha traído muchos avances tecnológicos a la humanidad, por un lado ha facilitado el desarrollo de actividades, pero por otro lado ha presentado grandes desafíos en cuanto a la seguridad, utilizamos la tecnología en casi todos los campos de la trabajo, pero no sabemos cómo usarlo, los peligros que representa, esta realidad pronosticada a nivel nacional hace que como país enfrentemos muchos peligros por el uso de la tecnología, en este trabajo de investigación partimos con un diagnóstico de la actualidad situación del Ecuador en materia de ciberseguridad, Establecer áreas de acción que requieran de lineamientos nacionales que permitan la articulación y coordinación de los esfuerzos de los diferentes organismos nacionales, complementado con el apoyo de los organismos internacionales, todo lo cual se refleja en la propuesta que se presenta como estrategia nacional de ciberseguridad, en la que se presenta la estrategia que hemos considerado el curso de acción seguido y las metas a alcanzar a través de cada estrategia propuesta, por lo que este trabajo constituye un aporte desde una perspectiva puramente académica y consciente de las principales limitaciones económicas que se pueden implementar. a medio plazo.

Considerando a la hipótesis específica 2 que la Instrucción de Ciberdelitos complejos se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones

de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022, con un grado de correlación de Spearman de un Rho= 0.785, lo cual demostró que tienen una correlación alta y significativa: Una vez contrastado el resultado encontramos que tiene relación con la tesis de 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. El objetivo del autor es “arrojar luz sobre los elementos que minan la definición de la estrategia nacional de ciberseguridad de Argentina” (p. 98), usando métodos de investigativos de enfoque cualitativo para concluir que: Primero, la proliferación de las TIC y la “propaganda de la tecnología han propiciado el establecimiento de medidas de ciberseguridad y ciberdefensa para mitigar y proteger a las naciones de las vulnerabilidades creadas por los ecosistemas que componen el ciberespacio” (p. 98). En segundo lugar, existen “varias normas destinadas a proteger la cooperación internacional en materia de seguridad de la información y procedimientos”, pero la distinción “ciberseguridad, ciberdefensa y ciberdelincuencia, tienen dinámicas y desarrollos diferentes”. Este estudio demuestra la necesidad de unificar los esfuerzos de las agencias en defensa cibernética. Nuevamente, esto apunta a la necesidad de inversión en mano de obra y equipo técnico.

Considerando a la hipótesis específica 3 que la Instrucción de Amenazas emergentes se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022, con un grado de correlación de Spearman de un Rho= 0.842, lo cual demostró que tienen una correlación alta y significativa: Una vez contrastado el resultado encontramos que tiene relación con la tesis de Baretto (2017) y cuyo objetivo del autor era “identificar los métodos, formas y medios de uso como un 'sistema de armas cibernéticas'” (p. 3), mediante el enfoque cualitativo del estudio, concluyendo que primero, “es necesario para la respuesta a la agresión provenga de un solo organismo” (p. 136). En segundo lugar, “la ausencia de una estrategia nacional de ciberseguridad no facilita la ejecución de estrategias militares aplicables a la defensa nacional” (p. 136). En tercer lugar, " los desarrollos y facultades específicas están bajo el nivel de amenaza ". Así, en este estudio, podemos apreciar la necesidad de tener un sistema de ciberseguridad optimo, y así contribuye a este estudio tanto a nivel teórico como de investigación pragmática, ya que los militares son los que más necesitan un rol protector y defensivo.

Conclusiones

1. De acuerdo con el Objetivo General que a la letra dice, determinar de qué manera la Instrucción de ciberdefensa se relaciona con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. El valor calculado para la Chi cuadrada 0.877 > 0.05 para un nivel de confianza de 95%. Hemos podido concluir que dicha hipótesis es válida; ya que, la Instrucción de ciberdefensa la cual debe incluir el ciberdelito convencional, los ciberdelitos complejos y amenazas emergentes contribuye directamente con la estructuración y consecución del Perfil de egreso del cadete de comunicaciones de la Escuela Militar, en provecho de la profesionalización de los futuros oficiales del arma de Comunicaciones.

2. De acuerdo con el Objetivo Especifico 1 que a la letra dice, establecer de qué manera la Instrucción de Ciberdelito convencional se relaciona con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. El valor calculado para la Chi cuadrada 0.714 > 0.05 para un nivel de confianza de 95%. Hemos podido concluir que dicha hipótesis es válida; ya que, la instrucción del ciberdelito convencional que a su vez incluye delitos de acceso ilegal, interceptación de datos, spam, incitación al odio, robo de identidad e infracciones de derechos de autor; contribuye directamente con los requerimientos para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar, apoyando a la profesionalización de los futuros oficiales del arma de Comunicaciones.

3. De acuerdo con el Objetivo Especifico 2 que a la letra dice, establecer de qué manera la Instrucción de Ciberdelitos complejos se relaciona con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. El valor calculado para la Chi cuadrada 0.785 > 0.05 para un nivel de confianza de 95%. Hemos podido concluir que dicha hipótesis es válida; ya que, la instrucción de los ciberdelitos complejos que a su vez incluye delitos de ciberterrorismo, ciberguerra, ataques contra infraestructura critica, Ciberespionaje y hacktivismo; contribuye directamente con los requerimientos para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar, proporcionando conocimientos especializados a los futuros oficiales del arma de Comunicaciones.

4. De acuerdo con el Objetivo Especifico 3 que a la letra dice, establecer de qué manera la Instrucción de Amenazas emergentes se relaciona con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. El valor calculado para la Chi cuadrada 0.842 > 0.05 para un nivel de confianza de 95%. Hemos podido concluir que dicha hipótesis es válida; ya que, la instrucción las amenazas emergentes que a su vez incluye es estudio del tráfico ilícito de drogas, extorsión en línea, difusión de la cultura de violencia, lavado de dinero cibernético y evasión fiscal; contribuye directamente para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar aportando los requisitos necesarios al proporcionar conocimientos especializados a los futuros oficiales del arma de Comunicaciones.

Recomendaciones

1. Teniendo en consideración que la Instrucción de ciberdefensa la cual debe incluir el ciberdelito convencional, los ciberdelitos complejos y amenazas emergentes contribuye directamente con la estructuración y consecución del Perfil de egreso del cadete de comunicaciones de la Escuela Militar, en provecho de la profesionalización de los futuros oficiales del arma de Comunicaciones; es recomendable que se implemente y/o complemente la instrucción referida a Ciberdefensa que se imparte a los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos a fin de que los mismos cuenten con mayores conocimientos sobre el tema y adquieran las capacidades que requiere el Perfil de egreso del cadete de Comunicaciones.

2. Teniendo en consideración que la instrucción del ciberdelito convencional que a su vez incluye delitos de acceso ilegal, interceptación de datos, spam, incitación al odio, robo de identidad e infracciones de derechos de autor; contribuye directamente con los requerimientos para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar, apoyando a la profesionalización de los futuros oficiales del arma de Comunicaciones; es recomendable que se implemente y/o complemente la instrucción referida al ciberdelito convencional que se imparte a los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos a fin de que dichos cadetes incremente sus conocimientos y puedan adquirir las capacidades que necesita el Perfil de egreso del cadete de Comunicaciones.

3. Teniendo en consideración que la instrucción de los ciberdelitos complejos que a su vez incluye delitos de ciberterrorismo, ciberguerra, ataques contra infraestructura critica, Ciberespionaje y hacktivismo; contribuye directamente con los requerimientos para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar, proporcionando conocimientos especializados a los futuros oficiales del arma de Comunicaciones; es recomendable que se implemente y/o complemente la instrucción referida a los ciberdelitos complejos que se imparte en la Escuela Militar de Chorrillos a los cadetes del arma de Comunicaciones con la finalidad los conocimientos impartidos tengan la importancia requerida para alcanzar el Perfil de egreso del cadete de Comunicaciones.

4. Teniendo en consideración que la instrucción las amenazas emergentes que a su vez incluye es estudio del tráfico ilícito de drogas, extorsión en línea, difusión de la cultura de violencia, lavado de dinero cibernético y evasión fiscal; contribuye directamente para alcanzar el Perfil de egreso del cadete de comunicaciones de la Escuela Militar aportando los requisitos necesarios al proporcionar conocimientos especializados a los futuros oficiales del arma de Comunicaciones; es recomendable que se implemente y/o complemente la instrucción referida a las amenazas emergentes que imparte la Escuela Militar de Chorrillos a los cadetes del arma de Comunicaciones, teniendo como objetivo alcanzar los requisitos que requiere el Perfil de egreso del cadete de Comunicaciones.

Referencias

Ander-Egg, e. (2003). Repensando la Investigación-Acción Participativa. *Colección política, servicios y trabajo social. https://abacoenred.com/wp-content/uploads/2017/05/Repensando-la-IAP-2003-Ed.4-Ander-Egg-Ezequiel.pdf.pd*

Gómez, Arnaldo, Acosta-Padrón, Rodolfo, & Hernández, José. (2016). Didáctica interactiva de lenguas extranjeras en Cuba. *Mendive. Revista de Educación, 14*(2), 142-149. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-76962016000200002&lng=es&tlng=es.

Alarcón y Suárez (2020). *Percepción de la formación integral de los cadetes de artillería y el perfil requerido para el oficial egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2020*. [Tesis de pregrado. Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH/567

Albarracín, A. (2019). *Inteligencia Nacional y estrategia de ciberseguridad nacional*. [Tesis de Maestría, Universidad Nacional de la Plata]. https://doi.org/10.35537/10915/87062

Aliaga y Bazán (2020). *Formación integral y el perfil profesional de los oficiales recién egresados del arma de caballería 2020*. [Tesis de pregrado. Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. https://repositorio.escuelamilitar.edu.pe/server/api/core/bitstreams/47417061-43d6-4764-a8bd-35fca2b472c1/content

Astudillo, C. (2020). *Un ensayo sobre la Seguridad y la Defensa en el Perú, Nuevas amenazas, nuevos roles*. Editorial NIU – SAC. https://cdn.www.gob.pe/uploads/document/file/2055508/Un%20ensayo%20sobre%20la%20Seguridad%20y%20la%20Defensa%20en%20el%20Per%C3%BA

%20Nuevas%20Amenazas%20Nuevos%20Roles%202da%20edici%C3%B3n%202020.pdf.pdf?v=1627933309

Atienza, M. y Ruiz, J. (2006). Ilícitos Atípicos. Editorial Trotta. https://www.trotta.es/libros/ilicitos-atipicos/9788481644180/

Baretto, J. (2017). *La Defensa Nacional y la estrategia militar de seguridad cibernética*". [Tesis de Maestría. Escuela Superior de Guerra Conjunta de Argentina]. http://cefadigital.edu.ar/handle/1847939/1061

Behar, (2008). Introducción a la metodología de la investigación.

Bowen, H. (1953). Social Responsibilities of the Businessman. Editorial Harper. https://books.google.com.pe/books?id=ALIPAwAAQBAJ&printsec=frontcover&hl=es&source=gbs_atb#v=onepage&q&f=false

Castro Márquez, F. (2003). *Proyecto de investigación y su esquema de elaboración*. Editorial Uyapar

Castro, M. (2003). El proyecto de investigación y su esquema de elaboración. (2ª.ed.). Editorial Uyapal. https://isbn.cloud/9789806629004/proyecto-de-investigacion-y-su-esquema-de-elaboracion/

Chakraborti, N. y Garland, J. (2012), 'Reconceptualising Hate Crime Victimisation Through the Lens of Vulnerability and 'Difference'', Theoretical Criminology, 16 (4): 499-514.

Chiza, D. y Izurieta, H. (2020). *Estrategia nacional de ciberseguridad. Maestría en Estrategia Militar Terrestre*. [Tesis de Maestría Universidad de las Fuerzas Armadas de Ecuador]. http://repositorio.espe.edu.ec/handle/21000/23141

Colle, R. (2000). «Internet: un cuerpo enfermo y un campo de batalla», Revista Latina de Comunicación Social, número 30, junio de 2000. http://www.ull.es/publicaciones/latina/aa2- 000qjn/91colle.htm

Decreto Legislativo 635 de 1991. Código Penal Peruano. 8 de abril de 1991.

Ejército del Perú. Reglamento de Liderazgo Militar RE 1-54. 2014

Hernández, R., Fernández, C. y Baptista, L. (2016). Metodología de la investigación. Editorial Mc Graw Hill. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Hurtado, J. (2000). Metodología de la Investigación Holística. Tercera Edición. Editorial Fundación Sypal.

Jara, E. (1989). La Función Diplomática. Proyecto de Cooperación con los Servicios Exteriores de América Latina. Santiago de Chile.

Javier, C. (1998). Seguridad de Sistema Silverio FALyB. Editorial Buenos Aires. https://es.scribd.com/presentation/420240759/Seguridad-de-Los-Sistemas-Informacion

Jurinski, J. (1999). Estafas Bancarias. Strategic Finance,

Kranenbarg, M. (2018). Cyber-offenders versus traditional offenders. An empirical comparison. https://www.cep-probation.org/wp-content/uploads/2020/11/complete-dissertation.pdf

Ley 27806 de 2002. Ley de Transparencia y Acceso a la Información Pública.

Méndez, C. (2009). *Metodología guía para elaborar diseños de investigación en ciencias económicas, contables y administrativas*. 2da. Edición, Editorial Mc Graw Hill interamericana. https://repository.urosario.edu.co/handle/10336/30059

Palau, M. (2013). Tipos de Crackers. http://mundoinformatich.blogspot.com/

Palmer, R. E. (1969*). Hermeneutics: Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer*. Evanston, IL: Northwestern University Press.

Pérez (2015). *Delitos de peligro abstracto y bienes jurídicos colectivos*, en Foro de la Fundación Internacional de Ciencias Penales, núm. 3, p. 137

Pérez, W. y Ramos, M. (2020). *Propuesta de una política de ciberseguridad para las Fuerzas Armadas"* [Tesis de Maestría, Universidad de las Fuerzas Armadas de Ecuador]. http://repositorio.espe.edu.ec/handle/21000/23372

Rodríguez, M. (2010). Métodos de investigación. 1ra. Edición, México. Ed. Universidad Autónoma de Sinaloa.

Sabino, C. (2008). *Cómo hacer una tesis (2a ed.)*. Caracas: Panapo

Sánchez, G. (2008). «Ciberterrorismo: la guerra del siglo XXI», El Viejo Topo, número 242, pp. 15-24

Sánchez, H. y Reyes, C. (2006) Metodología y diseño de la investigación científica. Lima: Editorial Visión Universitaria

Secretaría de Guerra y Marina de los Estados Unidos Mexicanos. (1937). http://www.ordenjuridico.gob.mx/Documentos/Federal/html/wo88720.html

Taipe, E, Huacasi, W. y Liu (2017). *La formación académica del cadete y el perfil del oficial instructor de los cadetes de cuarto año del arma de artillería de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2016*". [Tesis de pregrado. Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH/717

Vera R., (2018). *Mejoramiento de la evaluación del perfil profesional de los oficiales egresados de la Escuela Militar de Chorrillos "CFB" 2016-2017*". [Tesis de pregrado. Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH/159

ANEXOS

Anexo 1: Matriz de consistencia

Titulo: Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
Problema General ¿De qué manera se relaciona la Instrucción de ciberdefensa con Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022? **Problemas Específicos** ¿De qué manera se relaciona la Instrucción de Ciberdelito convencional con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022? ¿De qué manera se relaciona la Instrucción de Ciberdelitos complejos con el Perfil de egreso del cadete de comunicaciones de la Escuela	**Objetivo General** Determinar de qué manera se relaciona la Instrucción de ciberdefensa con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022. **Objetivos Específicos** Establecer de qué manera se relaciona la Instrucción de Ciberdelito convencional con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022. Establecer de qué manera se relaciona la Instrucción de Ciberdelitos complejos con el Perfil de egreso del cadete de comunicaciones de la Escuela	**Hipótesis General** La Instrucción de ciberdefensa se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022. **Hipótesis Específicas** La Instrucción de Ciberdelito convencional se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022. La Instrucción de Ciberdelitos complejos se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela	**Variable Independiente** **(X)** Instrucción de Ciberdefensa	**X_1** Ciberdelito convencional	• Acceso Ilegal (Craqueo) • Interceptación de Datos • Pornografía Infantil • Spam • Incitación al Odio • Fraude Bancario • Robo de Identidad • Infracciones de Derechos de Autor	**TIPO DE INVESTIGACIÓN** Básico-Descriptivo **DISEÑO** No Experimental-Transversal **ENFOQUE** Cuantitativo **POBLACIÓN** 27 cadetes de 4to año de Comunicaciones de la EMCH **MUESTRA** 27 cadetes de 4to año de Comunicaciones de la EMCH **TÉCNICA** Se ha aplicado: • Investigación documental **INSTRUMENTOS**
				X_2 Ciberdelitos complejos	• Ciberterrorismo • Ciberguerra • Ataques Contra Infraestructura Crítica • Ciberespionaje y Hacktivismo	
				X_3 Amenazas emergentes	• Tráfico de drogas y armas • Extorsión en línea • Difusión de una cultura de violencia • Lavado de dinero cibernético y evasión fisca	
			Variable Dependiente **(Y)**	**Y_1** Como profesional castrense	• Cumple normas y reglamentos • Posee porte y disciplina • Bachiller en ciencias militares • Capacidad de liderazgo	

Militar de Chorrillos “Coronel Francisco Bolognesi”-2022? ¿De qué manera se relaciona la Instrucción de Amenazas emergentes con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?	Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. Establecer de qué manera se relaciona la Instrucción de Amenazas emergentes con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.	Militar de Chorrillos “Coronel Francisco Bolognesi”-2022. La Instrucción de Amenazas emergentes se relaciona significativamente con el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022.	Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos	**Y_2** Como instructor militar	• Estratega • Educador • Investigador • Planificador • Líder	Se utilizó: • Cuestionarios **MÉTODOS DE ANÁLISIS DE DATOS** Estadística SPSS25
				Y_3 En el campo de la proyección social	• Dominio del idioma • Responsabilidad social • Diplomacia	

Anexo 2: Instrumento de recolección de datos

CUESTIONARIO

INSTRUCCIÓN DE CIBERDEFENSA Y EL PERFIL DE EGRESO DEL CADETE DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"-2022

INSTRUCCIONES:

A continuación, le presentamos 28 proposiciones, le solicitamos responda su apreciación personal, considere que no existe respuesta correcta e incorrecta. Marque con un (X) en la Hoja de Respuestas aquella que considere este de acuerdo con su punto de vista con el siguiente cuadro:

1 Nunca	2 Casi nunca	3 A veces	4 Casi siempre	5 Siempre

PARTE I: (Variable X, Instrucción de Ciberdefensa)

N°	ITEMS	Puntajes				
		1	2	3	4	5
	Ciberdelito convencional					
1	¿Cree Ud que el Acceso Ilegal (Craqueo) como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
2	¿Cree Ud que la Interceptación de Datos como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
3	¿Cree Ud que la Pornografía Infantil como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
4	¿Cree Ud que el Spam como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el					

	Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
5	¿Cree Ud que la Incitación al Odio como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
6	¿Cree Ud que el Fraude Bancario como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
7	¿Cree Ud que el Robo de Identidad como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
8	¿Cree Ud que las Infracciones de Derechos de Autor como un Ciberdelito Convencional y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
	Ciberdelitos complejos					
9	¿Cree Ud que el Ciberterrorismo como un Ciberdelito Complejo y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					
10	¿Cree Ud que la Ciberguerra como un Ciberdelito Complejo y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022?					

11	¿Cree Ud que los Ataques Contra Infraestructura Crítica como un Ciberdelito Complejo y parte de la Instrucción de ciberdefensa guardan relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
12	¿Cree Ud que el Ciberespionaje y Hacktivismo como un Ciberdelito Complejo y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
	Amenazas emergentes					
13	¿Cree Ud que el Tráfico de drogas y armas como una de las Amenazas Emergentes y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
14	¿Cree Ud que la Extorsión en línea como una de las Amenazas Emergentes y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
15	¿Cree Ud que la Difusión de una cultura de violencia como una de las Amenazas Emergentes y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					
16	¿Cree Ud que el Lavado de dinero cibernético y evasión fisca como una de las Amenazas Emergentes y parte de la Instrucción de ciberdefensa guarda relación con el Perfil del Oficial de Comunicaciones egresado de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022?					

PARTE II: (Variable Y, Perfil de egreso del cadete de comunicaciones de la Escuela Militar de Chorrillos)

N°	ITEMS	Puntajes				
		1	2	3	4	5
	Como profesional castrense					
17	¿Cree Ud que el Cumplir las Normas y Reglamentos como Profesional Castrense orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
18	¿Cree Ud que el Poseer Porte y Disciplina como Profesional Castrense orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
19	¿Cree Ud que el ser Bachiller en Ciencias Militares como Profesional Castrense orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
20	¿Cree Ud que el Tener Capacidad de Liderazgo como Profesional Castrense orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
	Como instructor militar					
21	¿Cree Ud que el ser Estratega como Instructor Militar orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
22	¿Cree Ud que el ser Educador como Instructor Militar orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
23	¿Cree Ud que el ser Investigador como Instructor Militar orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					

24	¿Cree Ud que el ser Planificador como Instructor Militar orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
25	¿Cree Ud que el ser Líder como Instructor Militar orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
	En el campo de la proyección social					
26	¿Cree Ud que el Dominio del Idioma en el campo de la proyección social orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
27	¿Cree Ud que la Responsabilidad Social en el campo de la proyección social orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					
28	¿Cree Ud que la Diplomacia en el campo de la proyección social orientado a cumplir con el Perfil del Oficial de Comunicaciones es influenciado por la Instrucción de Ciberdefensa?					

Anexo 3: Autorización para la recolección de datos

El Coronel EP Sub Director de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" que suscribe:

AUTORIZA

A los Bachilleres Morote Cabrera Kevin Sebastián y Caballón Zavala Nataly Cristina, para realizar actividades de recolección de datos en las instalaciones de este Centro Superior de Estudios para desarrollar la Tesis titulada:

Instrucción de ciberdefensa y el Perfil de egreso del cadete de comunicaciones de la Escuela Militar de "Chorrillos Coronel Francisco Bolognesi", 2022.

Sin que esta labor interfiera con las actividades programadas por Escuela Militar.

Chorrillos, diciembre del 2022

Firma del Crl Sub Director

……

Grado, Apellidos y Nombres

Anexo 4: Base de datos (Prueba Piloto)

Para la Variable X: Instrucción de Ciberdefensa				
Variable: Instrucción de Ciberdefensa	**PRETEST**		**POSTEST**	
¿Tiene ud conocimiento de cuáles con considerados como ciberdelitos convencionales?	7 (58,3%)	5 (41,7%)	12 (100%)	
¿Tiene ud conocimiento de cuáles con considerados como ciberdelitos complejos?	9 (75%)	3 (25%)	12 (100%)	
¿Conoce ud cuales son las amenazas emergentes para la ciberdefensa?	8 (66,7%)	4 (33,3%)	12 (100%)	
Para la Variable Y: Perfil de Egreso del Cadete de Comunicaciones				
Variable: Perfil de Egreso del Cadete de Comunicaciones	**PRETEST**		**POSTEST**	
¿Sabe ud cuales son los lineamientos del perfil como profesional castrense?	9 (75%)	3 (25%)	12 (100%)	
¿Sabe ud cuales son los lineamientos del perfil como instructor militar?	8 (66,7%)	4 (33,3%)	12 (100%)	
¿Sabe ud cuales son los lineamientos del perfil Enel campo de proyección social?	7 (58,3%)	5 (41,7%)	12 (100%)	

Anexo 5: Base de datos

Instrucción de Ciberdefensa																					Perfil de Egreso del Cadete de Comunicaciones																				
Ciberdelito convencional										Ciberdelitos complejos						Amenazas emergentes							Como profesional castrense					Como instructor militar							En el campo de la proyección social						
1	3	3	3	1	4	5	4	**3**		4	4	3	5	**4**		4	3	2	4	**3**	**3**		5	4	4	2	**4**		3	5	4	3	2	**3**		4	5	4	**4**	**4**
2	5	5	5	5	5	5	5	**5**		5	5	5	5	**5**		5	5	5	4	**5**	**5**		4	5	5	5	**5**		5	5	5	5	5	**5**		4	4	5	**4**	**5**
4	3	3	4	4	4	4	5	**4**		5	5	4	4	**5**		1	1	3	4	**2**	**4**		4	3	5	5	**4**		4	4	1	1	3	**3**		4	4	3	**4**	**4**
5	5	5	5	5	5	5	5	**5**		5	5	5	4	**5**		5	5	3	3	**4**	**5**		3	3	3	5	**4**		5	4	5	5	3	**4**		3	3	3	**3**	**4**
4	4	4	4	4	4	4	4	**4**		4	4	4	4	**4**		4	4	4	4	**4**	**4**		4	4	4	4	**4**		4	4	4	4	4	**4**		4	4	4	**4**	**4**
1	1	1	1	1	1	1	1	**1**		1	1	1	1	**1**		1	1	1	1	**1**	**1**		1	1	1	3	**2**		1	1	1	1	1	**1**		1	1	1	**1**	**1**
4	4	5	4	3	4	4	4	**4**		5	5	4	4	**5**		5	4	5	3	**4**	**4**		4	3	5	4	**4**		4	4	5	4	5	**4**		3	4	3	**3**	**4**
5	5	5	5	5	5	5	5	**5**		5	5	5	5	**5**		5	5	5	5	**5**	**5**		5	5	5	5	**5**		5	5	5	5	5	**5**		5	5	5	**5**	**5**
5	5	5	5	5	5	5	4	**5**		5	5	5	5	**5**		5	5	5	5	**5**	**5**		5	5	5	5	**5**		5	5	5	5	5	**5**		5	5	5	**5**	**5**
5	5	5	5	4	4	4	4	**5**		4	4	4	4	**4**		5	4	4	4	**4**	**4**		4	4	3	5	**4**		4	4	5	4	4	**4**		4	4	4	**4**	**4**
3	2	4	2	3	3	2	3	**3**		3	2	3	3	**3**		4	4	4	4	**4**	**3**		4	4	4	3	**4**		3	3	4	4	5	**4**		4	4	4	**4**	**4**
3	4	3	5	4	3	5	4	**4**		4	4	5	5	**5**		4	5	4	3	**4**	**4**		4	3	4	3	**4**		5	5	4	5	4	**5**		3	5	3	**4**	**4**
3	4	4	5	4	5	4	5	**4**		4	4	5	5	**5**		5	5	5	5	**5**	**5**		4	5	5	5	**5**		5	5	5	5	5	**5**		5	5	5	**5**	**5**
5	1	1	1	1	1	4	1	**2**		1	1	1	1	**1**		1	1	1	5	**2**	**2**		1	1	5	1	**2**		1	1	1	1	1	**1**		5	1	1	**2**	**2**
5	4	5	5	4	5	4	5	**5**		4	4	4	4	**4**		4	4	4	4	**4**	**4**		5	5	4	4	**5**		4	4	4	4	4	**4**		4	5	5	**5**	**4**
1	1	1	1	2	1	1	1	**1**		5	1	1	5	**3**		1	5	1	1	**2**	**2**		1	5	1	5	**3**		1	5	1	5	1	**3**		1	1	5	**2**	**3**
4	4	4	4	4	4	4	4	**4**		4	4	4	4	**4**		4	4	4	4	**4**	**4**		4	4	4	4	**4**		4	4	4	4	4	**4**		4	4	4	**4**	**4**
5	1	5	1	3	3	2	2	**3**		2	2	2	2	**2**		2	1	2	4	**2**	**2**		2	2	2	2	**2**		2	2	2	1	2	**2**		4	2	2	**3**	**2**
5	5	1	2	3	3	3	5	**3**		3	3	3	3	**3**		3	3	5	5	**4**	**3**		5	1	5	5	**4**		3	3	3	3	5	**3**		5	5	1	**4**	**4**
4	4	5	4	4	4	4	4	**4**		4	4	3	3	**4**		4	4	3	4	**4**	**4**		5	4	5	4	**5**		3	3	4	4	3	**3**		4	5	4	**4**	**4**
3	3	3	3	3	4	5	3	**3**		3	3	3	3	**3**		5	3	3	3	**4**	**3**		3	3	5	3	**4**		3	3	4	5	3	**4**		3	3	3	**3**	**3**

4	4	4	4	4	5	4	4	**4**	4	4	5	5	**5**	5	4	4	4	**4**	**4**	4	5	4	4	**4**	4	4	5	4	4	**4**	4	4	5	**4**	**4**
4	4	5	4	5	5	4	5	**5**	5	4	4	4	**4**	4	4	4	3	**4**	**4**	4	4	4	4	**4**	4	5	5	4	5	**5**	5	4	4	**4**	**4**
4	5	5	4	5	5	3	3	**4**	4	2	5	5	**4**	3	5	4	4	**4**	**4**	5	4	3	5	**4**	4	5	5	3	3	**4**	4	2	5	**4**	**4**
3	5	4	4	4	5	5	4	**4**	4	4	4	4	**4**	2	4	5	2	**3**	**4**	1	5	4	5	**4**	4	4	5	5	4	**4**	5	4	4	**4**	**4**
4	3	4	3	4	2	1	4	**3**	4	4	5	3	**4**	3	3	5	4	**4**	**4**	5	4	5	3	**4**	3	4	2	1	4	**3**	4	4	5	**4**	**4**
4	4	4	5	4	4	3	4	**4**	3	5	3	4	**4**	4	3	5	4	**4**	**4**	4	5	4	3	**4**	5	4	4	3	4	**4**	3	5	3	**4**	**4**

Anexo 6: Certificado de validez del instrumento por experto

FICHA DE VALIDACION DEL INSTRUMENTO

I. DATOS GENERALES

1.1 APELLIDOS Y NOBRES : Oscar Noguera Bedoya
1.2 GRADO ACADEMICO : Temático
1.3 INSTITUCION QUE LABORA : Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"
1.4 TITULO DE LA INVESTIGACION : Instrucción de ciberdefensa y el Perfil de Egreso del Cadete de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022
1.5 AUTOR DEL INSTRUMENTO : Morote Cabrera Kevin Sebastián
Caballón Zavala Nataly Cristina
1.8 NOMBRE DEL INSTRUMENTO : Encuesta
1.9 CRITERIO DE APLICABILIDAD

a) De 01 a 09: (No válido, reformular) b) De 10 a 12: (No válido, modificar)
c) De 12 a 15: (Válido, mejorar) d) De 15 a 18: (Válido, precisar)
e) De 18 a 20: (Válido, aplicar)

II. ASPECTOS POR EVALUAR:

INDICADORES DE EVALUACION DEL INSTRUMENTO	**CRITERIOS CUALITATIVOS CUANTITATIVOS**	**Deficiente (01-09) 01**	**Regular (10-12) 02**	**Bueno (12-15) 03**	**Muy Bueno (15-18) 04**	**Excelente (18-20) 05**
1.CLARIDAD	Esta formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Esta formulado con conductas observables					X
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología				X	
4.ORGANIZACION	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio					X
8.COHERENCIA	Entre las variables, dimensiones e indicadores					X
9.METODOLOGÍA	La estrategia responde al propósito del estudio				X	
10CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías				X	
SUB TOTAL					12	35
TOTAL						47

VALORACION CUANTITATIVA (total x 0.4): 18.8
VALORACION CUALITATIVA : Válido
OPINION DE APLICABILIDAD : Aplicar

Chorrillos ……. de diciembre del 2022

_____

…….
DNI: …….

FICHA DE VALIDACION DEL INSTRUMENTO

1. **DATOS GENERALES**
   - 1.1 APELLIDOS Y NOBRES : Teresa Haro Pizarro
   - 1.2 GRADO ACADEMICO : Doctor
   - 1.3 INSTITUCION QUE LABORA : Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"
   - 1.4 TITULO DE LA INVESTIGACION : Instrucción de ciberdefensa y el Perfil de Egreso del Cadete de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"-2022
   - 1.5 AUTOR DEL INSTRUMENTO : Morote Cabrera Kevin Sebastián
Caballón Zavala Nataly Cristina
   - 1.8 NOMBRE DEL INSTRUMENTO : Encuesta
   - 1.9 CRITERIO DE APLICABILIDAD

   a) De 01 a 09: (No válido, reformular) b) De 10 a 12: (No válido, modificar)
   c) De 12 a 15: (Válido, mejorar) d) De 15 a 18: (Válido, precisar)
   e) De 18 a 20: (Válido, aplicar)

2. **ASPECTOS POR EVALUAR:**

INDICADORES DE EVALUACION DEL INSTRUMENTO	**CRITERIOS CUALITATIVOS CUANTITATIVOS**	**Deficiente (01-09) 01**	**Regular (10-12) 02**	**Bueno (12-15) 03**	**Muy Bueno (15-18) 04**	**Excelente (18-20) 05**
1.CLARIDAD	Esta formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Esta formulado con conductas observables					X
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología				X	
4.ORGANIZACION	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio					X
8.COHERENCIA	Entre las variables, dimensiones e indicadores					X
9.METODOLOGÍA	La estrategia responde al propósito del estudio				X	
10CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías				X	
SUB TOTAL					12	35
TOTAL						47

VALORACION CUANTITATIVA (total x 0.4): 18.8
VALORACION CUALITATIVA : Válido
OPINION DE APLICABILIDAD : Aplicar

Chorrillos ……. de diciembre del 2022

_____

…….
DNI: …….

FICHA DE VALIDACION DEL INSTRUMENTO

3. **DATOS GENERALES**

1.1	APELLIDOS Y NOBRES	:	Janett Sanchez Pimentel
1.2	GRADO ACADEMICO	:	Metodólogo
1.3	INSTITUCION QUE LABORA	:	Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”
1.4	TITULO DE LA INVESTIGACION	:	Instrucción de ciberdefensa y el Perfil de Egreso del Cadete de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”-2022
1.5	AUTOR DEL INSTRUMENTO	:	Morote Cabrera Kevin Sebastián Caballón Zavala Nataly Cristina
1.8	NOMBRE DEL INSTRUMENTO	:	Encuesta
1.9	CRITERIO DE APLICABILIDAD		

a) De 01 a 09: (No válido, reformular) b) De 10 a 12: (No válido, modificar)
c) De 12 a 15: (Válido, mejorar) d) De 15 a 18: (Válido, precisar)
e) De 18 a 20: (Válido, aplicar)

4. **ASPECTOS POR EVALUAR:**

INDICADORES DE EVALUACION DEL INSTRUMENTO	**CRITERIOS CUALITATIVOS CUANTITATIVOS**	**Deficiente (01-09) 01**	**Regular (10-12) 02**	**Bueno (12-15) 03**	**Muy Bueno (15-18) 04**	**Excelente (18-20) 05**
1.CLARIDAD	Esta formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Esta formulado con conductas observables					X
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología				X	
4.ORGANIZACION	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio					X
8.COHERENCIA	Entre las variables, dimensiones e indicadores					X
9.METODOLOGÍA	La estrategia responde al propósito del estudio				X	
10CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías				X	
SUB TOTAL					12	35
TOTAL						47

VALORACION CUANTITATIVA (total x 0.4): 18.8
VALORACION CUALITATIVA : Válido
OPINION DE APLICABILIDAD : Aplicar

Chorrillos ……. de diciembre del 2022

_____

…….
DNI: …….