ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”

Implementación de la asignatura de ciberseguridad y la formación profesional de los cadetes del arma de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi - 2019.

TESIS PARA OPTAR EL TITULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES CON MENCION EN ADMINISTRACION

PRESENTADO POR LOS BACHILLERES:

Mallma Condor, Erik Alfredo

Flores Amasifuen, Gianfranco Paul

LIMA – PERÚ

2019

Asesor y miembros del jurado

ASESOR:

ASESOR METODOLOGICO: MAG. PEDRO VIGO SALIRROSAS

ASESOR TEMATICO: MAG. ANASTACIO PAUCAR LUNA

Dedicatoria

Dedicamos esta tesis de investigación a nuestros familiares, en especial a nuestros padres, que con esfuerzo y amor han encaminado nuestros pasos en esta etapa inicial de nuestra carrera profesional y también a la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi, alma mater de la estirpe inmortal que es la oficialidad líder de nuestra gran nación.

Agradecimiento

El agradecimiento sincero y especial a la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” por su gran trabajo y contribución en nuestra formación profesional como líderes militares y como hombres de la ciencia militar del Perú.

A las autoridades, docentes y personal administrativo de la Escuela militar de Chorrillos “Coronel Francisco Bolognesi”, que participaron en el proceso de nuestra formación profesional y en la elaboración de este trabajo, por su inestimable orientación, asesoramiento y apoyo.

PRESENTACIÓN

Sr. Presidente

Señores Miembros del Jurado.

En cumplimiento de las normas del Reglamento de elaboración y Sustentación de Tesis de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” se presenta a su consideración la presente investigación titulada “Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019”, para obtener el Título de Licenciado en Ciencias Militares.

Investigador metodológico: GIANFRANCO PAUL FLORES AMASIFUEN

Investigador temático: ERIK ALFREDO MALLMA CONDOR

La investigación tiene por finalidad describir la utilización de las tecnologías de información y comunicación en las actividades de Inteligencia, Contrainteligencia y seguridad, en el entorno de la web e internet, en el llamado Ciberespacio, en donde subyacen riesgos y amenazas y se configura en un campo de batalla del siglo XXI, por lo cual es necesario capacitar con una asignatura de Ciberseguridad como parte de la formación profesional de los cadetes de Inteligencia de la Escuela Militar, año 2018. Por lo expuesto, señores miembros del jurado, pongo a vuestra disposición esta investigación para ser evaluada esperando merecimiento de aprobación.

Los autores

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

RESUMEN

El presente trabajo, trata el tema relacionado a la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos ”Coronel Francisco Bolognesi”, con el objeto de determinar el nivel de conocimientos, destrezas y actitudes que adquieren los cadetes del Arma de Inteligencia, para una mejor influencia de conocimientos en los resultados de esta investigación, para la debida aplicación de una suficiencia profesional, como futuros Oficiales del Ejército el Perú. Se formuló la Hipótesis general que propone que existe relación entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. El objetivo principal de la investigación es determinar la relación que existe entre ambas variables. Aplicando como metodología que el enfoque es cuantitativo con diseño no experimental, teniendo como población a todo el arma de Inteligencia de 49 cadetes, con una muestra probabilística de tipo aleatorio de 44 cadetes, y así se pudo comprobar las Hipótesis general y específicas mediante el trabajo de campo con la técnica de la encuesta y con un instrumento de recolección de datos que es el cuestionario, concluyendo así que el valor calculado para la Chi cuadrada (11.936) es mayor que el valor que aparece en la tabla (9.488) para un nivel de confianza de 95% y un grado de libertad (4). Por lo que se adopta la decisión de rechazar la hipótesis general nula y se acepta la hipótesis general alterna.

Palabras Clave: Implementación de la Asignatura de Ciberseguridad, Unidad de Aprendizaje, Prácticas Especializadas, Herramientas de Estudio, Formación Profesional, Instrucción, Entrenamiento y Herramientas Académicas.

ABSTRACT

The present work, deals with the topic related to the Implementation of the Cybersecurity Subject and the Professional Training of the Cadets of the Weapon of Intelligence of the Military School of Chorrillos "Coronel Francisco Bolognesi", with the purpose of determining the level of knowledge, skills and attitudes that the cadets of the Intelligence Weapon acquire, for a better influence of knowledge in the results of this investigation, for the due application of a professional sufficiency, as future Officers of the Army of Peru. The General Hypothesis was formulated that proposes that there is a relationship between the Implementation of the Cybersecurity Subject and the Professional Training of the Intelligence Weapons cadets of the Chorrillos Military School "Colonel Francisco Bolognesi". The main objective of the investigation is to determine the relationship that exists between both variables. Applying as a methodology that the approach is quantitative with non-experimental design, having as a population the entire Intelligence weapon of 49 cadets, with a probabilistic sample of random type of 44 cadets, and thus it was possible to verify the general and specific Hypotheses through work field with the survey technique and with a data collection instrument that is the questionnaire, concluding that the value calculated for the Chi square (11,936) is greater than the value shown in the table (9,488) for a level 95% confidence and a degree of freedom (4). Therefore, the decision to reject the null general hypothesis is adopted and the alternate general hypothesis is accepted.

Keywords: Implementation of the Cybersecurity Subject, Learning Unit, Specialized Practices, Study Tools, Professional Training, Instruction, Training and Academic Tools.

INTRODUCCIÓN

El desarrollo del presente trabajo de Investigación, trató sobre un tema de importancia para el mejoramiento de la Instrucción militar y formación militar en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", con el objetivo de ver la relación que existe entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia.

El esquema de este trabajo de investigación abarca cuatro grandes capítulos, desarrollados metodológicamente de acuerdo al siguiente orden:

El Capítulo I, denominado Planteamiento del problema, trata sobre la problemática que existe en la implementación de la asignatura de ciberseguridad en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y como en otros ejércitos del mundo, con el propósito de mejorar la Formación Profesional, en este caso, en la mejora de la calidad de la instrucción de los cadetes del Arma de Inteligencia, considerando su formación militar durante 5 años, a fin de mejorar su nivel de desempeño como Oficial. Además de lo señalado, este capítulo también nos ha delimitado el ámbito de dicho estudio, complementado a la vez con la formulación de los problemas: general y específicos, los objetivos de la investigación, la justificación de la misma y las limitaciones de la investigación y la viabilidad de la misma.

El desarrollo del Capítulo II, se encontraron estudios relacionados con el tema que constituyen antecedentes para la investigación, primero los de carácter internacional y luego nacional. Con los aportes sobre ambas variables de la investigación. Además de lo señalado, en este capítulo se han establecido las bases teóricas que dan fundamento y consistencia al trabajo, igualmente las definiciones conceptuales, las hipótesis y las variables.

En el Capítulo III, conocido como Marco Metodológico, se estableció que el diseño de la presente Investigación será descriptivo correlacional. Además, se determinó el tamaño de la muestra, las técnicas de recolección y el procesamiento de datos, se realizó la Operacionalización de las variables y se consideró también los aspectos éticos.

El Capítulo IV Resultados, se ocupó de interpretar los resultados estadísticos de cada uno de los ítems considerados en los instrumentos, adjuntándose los cuadros y gráficos correspondientes. Se ha establecido al término de la investigación y con las pruebas de hipótesis, que existe significativa relación entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia. Se desarrolló la Discusión de los Resultados considerando trabajos similares cotejándolos con el presente trabajo de Investigación; este aspecto es de suma importancia para darle consistencia a este trabajo.

Luego se han establecido las Conclusiones y consecuentes con éstas, se presentan las Recomendaciones, teniendo en cuenta que el cadete necesita implementar la asignatura de ciberseguridad como parte de su formación profesional como cadete del Arma de Inteligencia.

CAPITULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del Problema

Con el desarrollo de la llamada Tercera Ola de Toffler las guerras y relaciones entre los países cambiaron su forma de desarrollo. Así, hubo un incremento en el desarrollo tecnológico de los medios de comunicación, lo que ha interconectado todo el mundo, de modo que nadie se queda más aislado. En ese contexto, el dominio de la información pasó a ser un bien intangible y extremamente poderoso, que puede hacer un desbalance en las relaciones entre los países. Esas informaciones se quedan en redes nacionales, corporativas o privadas y son objeto de codicia por parte de los interesados. Para obtener las informaciones o protegerlas surgió un nuevo actor: el "hacker". Los hackers son personas que poseen profundos conocimientos de los sistemas informatizados y que desarrollan sus conocimientos para invadir o proteger las diversas redes en todos los lugares del mundo.

Un ejemplo de la importancia y profundidad de las acciones de los hackers ocurrió en Estonia en 2007, donde hubo un ataque cibernético que en una semana bloqueó todas las páginas web gubernamentales y de los diferentes partidos políticos. Todos los medios de comunicación quedaron completamente desconectados, haciendo imposible que se le informara al mundo lo que estaba ocurriendo. Otros sistemas afectados fueron de los bancos, donde los hackers desconectaron todo el sistema bancario, bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar. Esos ataques duraron tres semanas y fueron conocidos como la primera ciberguerra. Estonia inmediatamente acusó

al gobierno de Rusia, sin embargo nada ha podido ser demostrado debido a la dificultad en ubicar los ataques.

De la misma forma que los hackers afectan a los servicios de un país, buscan informaciones privilegiadas para acuerdos comerciales o para desarrollo de armas de guerra. Recientemente, quedó conocido un caso de posible apropiación de conocimientos militares por parte de China contra los Estados Unidos. Éstos desarrollaron aviones de caza de quinta generación al mismo tiempo en que los chinos habían desarrollado aviones de caza de tercera generación. Para sorpresa de la gente en general, los chinos consiguieron producir un avión de quinta generación, como el producido por los Estados Unidos, sin desarrollar proyecto o producir un avión de cuarta generación, lo que es prácticamente imposible, pues son pasos necesarios a seguir para alcanzar un nuevo modelo tecnológicamente más moderno. Así China obtuvo una ventaja económica, tecnológica y de Seguridad y Defensa.

Con el incremento de las acciones en el ciberespacio, los países más desarrollados tecnológicamente han implementado medidas y acciones para proteger sus informaciones, de sus empresas, de sus servicios y de su población en general.

Con el desarrollo de las comunicaciones virtuales, nadie más está aislado y casi todo depende del control de sistemas cibernéticos para funcionamiento, como los servicios básicos y bancarios. Así, proteger las informaciones ha quedado como una acción primordial para las empresas que desarrollan productos tecnológicos de punta y para los Estados, de modo que puedan asegurar la Seguridad y Defensa de sus informaciones, de su patrimonio y de su pueblo en general.

En Suramérica, la Seguridad y Defensa Cibernética de los países está incipiente, con algunos países delante de otros en ese desarrollo. Hay países que han comenzado a

desarrollar su Seguridad y Defensa Cibernética con más intensidad después que se descubrió las acciones que países desarrollados hacían en el mundo (espionaje virtual). Los hechos que mostraron esas acciones fueron conocidos por medio de denuncias de Wikileaks.

Hoy en día tenemos muy en cuenta que los ciberataques dejaron de realizarse a nivel usuario o a nivel empresa, en la actualidad se habla de ciberataques a nivel de gobierno, de nación, de patria. Los grandes países del mundo se enfrascan por una preparación ante una ciberguerra mundial, imaginamos que podría ser una película de ciencia ficción todo esto más desafortunadamente los hechos descritos como premisa son reales, ocurrieron, ocurren y ocurrirán posiblemente con la mayor fuerza la que quizá ignoramos y no estamos emprendiendo proyecto alguno para estar preparados.

Hay que hacer una revisión propia como país para darnos cuenta en realidad en qué nivel de preparación estamos para afrontar una situación de tal magnitud. Eventos como "Cyber Security Goverment Perú 2012" muestran los retos, amenazas y avances en materia de seguridad informática para la protección de los gobiernos.

Especialistas que evalúan la ciberseguridad en las instituciones del gobierno resaltan la importancia de crear un cibercomando peruano, tenemos como premisa los ataques que llevaron a cabo miembros del grupo Anonymous y la seguridad que tienen las empresas del rubro bancario para realizar transacciones protegiéndose de posibles ciberataques.

En el ámbito militar enemigos cercanos de algún país que se preocupa no solo por el ataque de nuestro territorio, sino que también analizan otros espacios como infraestructuras críticas o tener acceso a información secreta, en manos equivocadas puede paralizarnos como país en solo cuestión de horas y por días. Tenemos también la

premisa del estado de Estonia, país que sufrió un ataque mayor que perjudicó a altas autoridades del gobierno, a raíz de este caso muchos países han implementado políticas, estrategias e inversiones en ciberdefensa y ciberseguridad. Tenemos el caso de Alemania que en el año 2011 lanzó su estrategia de ciberseguridad, Australia creo su centro de operaciones cibernéticas. Canadá también se preparada para enfrentar situaciones de la misma índole. EEUU. Invierte una gran cantidad de dinero para crear el centro de cibercomando unificado que depende de la Agencia de Seguridad Nacional.

En nuestro Perú no hay nada unificado, necesitamos tener estrategias definidas en temas de desarrollo y aplicación de ciberseguridad. Existen esfuerzos de ciberseguridad en el Perú pero están aislados, no fusionados. Falta unir a estos grupos para formar un cibercomando peruano de esta manera tendremos personal altamente capacitado para combatir cualquier amenaza con profesionales en seguridad de información.

El 57% de los expertos en seguridad global opinan que se está produciendo una verdadera "Carrera armamentista" en el ciberespacio un dato que se desprende del informe sobre Ciberdefensa efectuado por la compañía de software McAffe.

Finlandia, Israel y Suecia son los países mejor preparados en términos cibernéticos según los estudios de McAffe en colaboración con Agenda de Seguridad y Defensa.

Para capacitar al personal para la Seguridad y Defensa Cibernética, hay países que han hecho intercambios y cursos en diversos otros países del mundo con la finalidad de aprender lo que se está haciendo en Ciberseguridad por medio de convenios y participación en cursos y talleres.

En ese contexto, Perú, que posee destacados minerales energéticos y rica biodiversidad, debe buscar desarrollar su Seguridad y Defensa Cibernética para evitar que países más desarrollados se apropien de su conocimiento y de sus informaciones clasificadas y de sus riquezas.

De esa forma, por las misiones constitucionales que poseen de Seguridad y Defensa del Estado, además del mantenimiento de los intereses nacionales, los militares pueden ser los precursores de ese proceso, como ocurre en la mayoría de los países en el mundo.

El Perú se desarrolla industrial, cultural y tecnológicamente tanto en el sector público como el privado, también es cada vez más vulnerable a todo tipo de ciberataques; lo que implica la necesidad de contar con políticas definidas en este campo o en su defecto, articular sistemas de prevención confiables ante los delitos informáticos entre los expertos, académicos y sociedad civil; Por todo lo expuesto, la Escuela militar de Chorrillos debe considerar la incorporación como objetivo curricular, la incorporación de contenidos de la Teoría y la práctica de la Ciberseguridad, como disciplina de las Ciencias Informáticas, con la finalidad de optimizar la formación profesional especializada de los cadetes del arma de Inteligencia.

1.2. Formulación del problema

1.2.1. Problema general

¿Cuál es la relación que existe entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019?

1.2.2. Problemas específicos

Problema específico N°1: ¿Cuál es la relación que existe entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019?

Problema específico N°2: ¿Cuál es la relación que existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019?

Problema específico N° 3: ¿Cuál es la relación que existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar la relación que existe entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

1.3.2. Objetivos específicos

Objetivo específico N° 1: Determinar la relación que existe entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Objetivo específico N° 2: Determinar la relación que existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Objetivo específico N° 3: Determinar la relación que existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

1.4. Justificación

1.4.1. Justificación Teórica

El presente trabajo se establece en los fundamentos constitucionales, legales y doctrinarios relacionados con la Seguridad, Defensa y Desarrollo del Perú. La Constitución Política del Perú (1993) establece que el Estado es responsable por prestar la Defensa de la sociedad, del aparato industrial, de los servicios estatales, del material biológico y de los minerales estratégicos del País. Por lo tanto, el estudio de la Ciberseguridad para el incremento de la Defensa, Seguridad y Desarrollo del Estado está alineado con la ley máxima del País. Desarrollar una propuesta de diseño de la asignatura de Ciberseguridad permitirá profundizar el estudio del tema que es actual, novedoso y fundamental para Perú, contribuyendo a preservar su independencia, y desarrollo social y económico.

1.4.2. Justificación Metodológica

Esta investigación se justifica desde el punto de vista metodológico, pues se emplea el método cualitativo, no experimental, transversal, exploratorio y descriptivo para la investigación; así también porque hace un análisis utilizando la estrategia metodológica de Investigación documental en la Escuela militar de Chorrillos, en el ámbito de las actividades y operaciones del Ejército del Perú como parte integrante de las Fuerzas Armadas del Perú.

1.4.3. Justificación Práctica

La incorporación curricular de una asignatura de Ciberseguridad para la Seguridad, Defensa y Desarrollo para la formación profesional especializada para los cadetes del arma de Inteligencia permitirá capacitar con calidad a los futuros líderes militares de las Fuerzas Armadas para actuar con más capacidad e incrementar el nivel de Seguridad desarrollado en la defensa de los intereses del País. Además, posibilitará desarrollar doctrina, estandarizar procedimientos y fomentar el interés por la temática de Ciberseguridad, que es fundamental para el mantenimiento de los intereses y los recursos de un Estado. Asimismo, la Ciberseguridad es un aporte importante para la ejecución de la Política Externa de un país.

1.5. Limitaciones

En la presente investigación consideramos que no se presentaron mayores dificultades que pudieran afectar su desarrollo; por el contrario, todos estos pequeños inconvenientes serán superados.

En el desarrollo de la presente investigación, se ha previsto encontrar algunas de las siguientes limitaciones:

1.5.1. Limitaciones de tiempo

El factor tiempo, valor indispensable para el trabajo de investigación lo que constituye en una grave dificultad para realizar el estudio dentro de la EMCH y se convierte en una limitante; sin embargo, lograremos desarrollar un adecuado trabajo académico investigativo.

1.5.2. Limitaciones económicas

El aspecto económico también es una dificultad en el estudio investigativo, pues implica la inversión en diferentes rubros y esta será solventada íntegramente por los cadetes.

1.5.3. Limitaciones metodológicas

El desarrollo de todo trabajo de investigación, en sus diferentes niveles, obliga al empleo de una metodología para realizar el proceso investiga torio, que en este caso no es dominado profundamente por los integrantes del grupo, por la poca experiencia en el campo de la investigación científica, por tal motivo se convierte en un obstáculo más. Sin embargo, con las indicaciones de nuestro supervisor, compromiso categórico personal y profesional con el estudio, permitirán con mucho esfuerzo comprenderlo.

1.6. Viabilidad

Es viable la presente investigación porque se dispone de los recursos humanos y materiales suficientes para realizar el estudio en el tiempo disponible previsto. Es factible lograr la participación de los sujetos u objetos necesarios para la investigación. La metodología a seguir conduce a dar respuesta al problema.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes Internacionales

Aguirre (2017); Tesis de Maestría: "Ciberseguridad en Infraestructuras Críticas de Información". Universidad de Buenos Aires. Buenos Aires, Argentina.

El presente Trabajo Final de Maestría analiza la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades que se han desarrollado en este sentido de manera general en algunos países y el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su protección. En efecto, las tecnologías de la información se han esparcido rápidamente en todos los sectores de la sociedad y prácticamente no existen servicios críticos que no dependan de aplicaciones, bases de datos, servidores, redes de comunicaciones, centros de datos, etc. La falta de controles de ciberseguridad ha ocasionado que algunos servicios se vean afectados a nivel mundial, como lo demuestran los incidentes de ciberseguridad que se describen en el presente trabajo y que impactaron en el funcionamiento de diferentes servicios críticos de tres países. La mayoría de sectores que están utilizando tecnologías de información, proveen servicios importantes a la población. Sin embargo, debido a la falta de metodologías de clasificación de estos servicios, no se ha podido identificar cuáles son realmente críticos y que por lo tanto, cuáles requieren una protección acorde por parte de los operadores que

los proveen. Un aporte adicional del trabajo es el análisis del estado actual de la ciberseguridad en el Ecuador. En esta sección se analiza la situación de ese país, incluyendo las normativas y regulaciones que ha desarrollado para fortalecer la ciberseguridad en las empresas públicas y a nivel privado.

Anchundia (2017); Tesis de Doctorado: “Ciberseguridad en los sistemas de información de las universidades”. Universidad de Cuenca. Cuenca, Ecuador.

El impacto de la globalización que va acompañando la creciente implantación de las tecnologías, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad con los cuales las organizaciones tendrán que enfrentarse. El objetivo de esta investigación es revisar el estado actual del conocimiento en la ciberseguridad en los sistemas de información en el contexto universitario, con algunas implicaciones en el Ecuador. A partir de una revisión documental, usando como recursos plataformas como Sciencedirect® y Google Académico®, entre otros, se identificaron áreas de interés general, dada la escasa literatura de ciberseguridad en el contexto universitario. Aunque la ciberseguridad es un fenómeno de mucho impacto en este entorno globalizado, la productividad científica en este tema es escasa; lo que dificulta un análisis profundo de la situación en el contexto universitario; sin embargo, al ser, la ciberseguridad, un fenómeno global y generalizado a todo tipo de organización, pueden extrapolarse las amenazas al sector universitario. Así, la universidad está llamada a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de

ciberseguridad, apoyada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad.

2.1.2. Antecedentes Nacionales

Taipe (2018); Tesis de Maestría: “La Auditoría de Seguridad Informática y su Relación en la Ciberseguridad de la Fuerza Aérea del Perú Año 2017”. Escuela Superior de Guerra Aérea. Lima, Perú.

El desarrollo de la presente investigación tuvo como objetivo analizar cómo el realizar una Auditoria de Seguridad Informática tiene implicancia en la Ciberseguridad en la Fuerza Aérea del Perú; desde luego el estudio lo que pretende es generar aportes que contribuyan a la solución de la problemática que se presenta en este sector; En cuanto a la metodología utilizada, se puede señalar que ha sido de tipo descriptiva según Bernal y otros (2000), diseño no experimental descriptiva correlacional, según Hernández y otros (2014); para la recogida de datos se aplicó dos cuestionarios, uno sobre Auditoria de seguridad informática y el otro sobre la implicancia en la Ciberseguridad de la Fuerza Aérea del Perú año 2017., que fue desarrollado por el Personal Militar de la Fuerza Aérea del Perú. En lo que refiere a los resultados se puede señalar que los encuestados manifiestan que el realizar una Auditoria de seguridad informática no tiene implicancia en la Ciberseguridad de la Fuerza Aérea del Perú año 2017. Lo que demuestra que el nivel de conocimiento del personal de Informática, las normas y políticas no tiene un buen nivel de Ciberseguridad.

2.2. Bases teóricas

2.2.1. Variable 1: Implementación de la Asignatura de Ciberseguridad

En Latinoamérica, tres de cada cinco empresas sufren por lo menos un incidente de seguridad en la red, y una de cada cinco es víctima de 'secuestro' de información. Así lo reveló el estudio ESET Security Report 2018, que se realizó con 4.500 ejecutivos, técnicos y gerentes de 2.500 empresas de 15 países de la región. (CERO, 2019)

El análisis detalló que los países más afectados son Perú con el 25 por ciento, México con el 20 por ciento, seguido de Argentina con el 15 por ciento, Brasil con el 14 por ciento y Colombia con el 10 por ciento.

La amplia variedad de amenazas informáticas puede emplearse para robar información valiosa de las compañías, desde ataques externos hasta fraudes financieros, que incluye alteración de datos y el pago de sobornos al cibercrimen.

En la era digital, la información es un factor muy importante para las compañías, por ello, deben hacer un análisis de riesgo de la seguridad informática para determinar el nivel y el impacto, conocer las debilidades y fortalezas de la compañía, tener más control, hacer monitoreo y establecer estrategias para protegerse de los ciberataques.

En este informe especial conocerá lo que debe tener en cuenta una empresa para prevenir el cibercrimen.

A. ¿Qué es ciberseguridad?

En la era digital se habla de Ciberseguridad, que se asocia a las ciberamenazas, al cibercrimen, pero también a las buenas prácticas para proteger la información y prevenir o detectar los ataques cibernéticos. (CERO, 2019)

Las amenazas de la seguridad informática llegan a través de programas dañinos o maliciosos que se instalan en un dispositivo o se penetran por medio de la nube.

Information Systems Audit and Control Association (Isaca), un referente en la materia, define la ciberseguridad como "una capa de protección para los archivos de información. A partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo".

Instalar programas antivirus y sistemas de detección de intrusos, conocidos como anti-spyware, que puede detectar de manera temprana los programas espías o presencia de programas maliciosos, son algunas de las buenas prácticas para proteger la seguridad informática. (CERO, 2019)

La seguridad informática no sólo se refiere a tecnología para prevenir ataques sino también a estrategias de capacitación a empleados y usuarios para evitarlos.

B. Seguridad informática, entre los peores riesgos del 2018

Los ataques cibernéticos y el robo de datos están en la lista de los riesgos más altos del mundo, de acuerdo con el informe de 'The Global Risks Report 2018', del Foro Económico Mundial (WEF), que también incluyó en su ranking a la economía, la geopolítica y el medioambiente. (CERO, 2019)

Los ataques informáticos pasaron de ser extraordinarios a comunes y su impacto financiero está en aumento, lo cual afecta a personas y, sobretodo, a entidades financieras, según explica el informe del Foro Económico Mundial.

El ransomware, un software malicioso que pone en riesgo todos los datos y arrebata el control de la información almacenada, fue el peor ataque del año pasado, que representó el 64 por ciento de todos los correos electrónicos maliciosos. El ransomware puede implicar una pérdida masiva de datos, ya que los delincuentes secuestran la información con la intención de extorsionar a las empresas.

El ataque del ransomware más común en 2017 fue WannaCry, que afectó a 300.000 computadoras en 150 países, y NotPetya, que causó pérdidas trimestrales de 300 millones USD para las empresas afectadas. Otra tendencia fue el uso de ataques cibernéticos para perjudicar infraestructuras críticas y sectores industriales estratégicos. (CERO, 2019)

C. Lista de los ciberataques más comunes

Los ataques cibernéticos se basan principalmente en el ‘secuestro’ de datos. Hospitales, pequeñas y medianas empresas han sido las principales víctimas los últimos años. Sin embargo, ni las grandes compañías se salvan del cibercrimen.

Telefónica, el gigante de telecomunicaciones español fue víctima de ataques en su red corporativa, que obligó a los empleados a apagar todos los computadores de su sede central en Madrid en 2017. Se trató de un ataque masivo de ransmware no solo contra Telefónica sino también contra varias organizaciones.

Estos son los ciberataques más comunes que debe conocer su empresa para que no sea víctima. (CERO, 2019)

1. El ransomware:

El ransomware se caracteriza por restringir el acceso a un sistema informático pidiendo un rescate para eliminar el bloqueo. Puede llegar a ser fatal para una compañía, porque implicaría una pérdida masiva de datos, además de los perjuicios económicos. (CERO, 2019)

El virus WannaCry y el Petya, dos tipos de ransomware operan de la misma forma: durante el ataque, los datos del ordenador infectado se bloquean, ya sean documentos, fotos o videos. Para desencriptarlos, normalmente el programa exige el pago de una suma de dinero, generalmente de bitcoins. Si no se paga a tiempo, los datos son eliminados o bloqueados de forma permanente.

2. Ataque DDos

Con la transformación digital de los servicios bancarios, los riesgos financieros cambiaron y los fraudes o las fallas en las operaciones se incrementaron, así como el cibercrimen. Entre los ataques más comunes y peligrosos está el DDoS o de denegación del servicio, que consisten en provocar la caída de un servidor sobrecargando su ancho de banda. Estas acciones fuerzan la interrupción de un sitio web. (CERO, 2019)

En el caso del sistema financiero, los DDoS se utilizan para inundar con una gran cantidad de tráfico los servicios en línea de los bancos y de las plataformas de trading. De esa manera el servidor colapsa y deja de funcionar.

3. Troyanos bancarios

Los delincuentes cibernéticos persiguen la telefonía móvil mucho antes de que se incrementara el uso de smartphones para realizar transacciones bancarias, ahora

cada vez más están tras estos dispositivos para hacer sus fechorías. Precisamente, la mayor amenaza para los dispositivos móviles son los troyanos bancarios, otro software malicioso que en principio parece inofensivo, pero es muy peligroso y está tras los bancos. (CERO, 2019)

Los troyanos pueden instalarse en cualquier dispositivo por visitar un sitio web infectado, por descargar el anexo de un mail, o incluso, por bajar una aplicación. Una vez este virus se instale en el celular, detecta en qué momento se utilizan los servicios en línea de un banco y así capturar los datos personales y bancarios.

D. Claves para prevenir ataques informáticos

Los cibercriminales operan de forma encubierta y son difíciles de detectar, puede pasar mucho tiempo antes de que los problemas sean visibles para la organización. Para la prevención y detección temprana toma nota de las siguientes buenas prácticas. (CERO, 2019)

1. Evite amenazas a través de emails

Los correos electrónicos son uno de los puntos más débiles de una compañía, pues a través de estos, se pueden introducir de forma fácil amenazas de virus y robo de información. Sin embargo, muchas empresas creen que no son tan peligrosos e ignoran la actividad de los correos internos y pueden ser víctimas de ‘secuestro’ de datos.

No olvide monitorear la actividad de mensajes sospechosos, así como las descargas de archivos anexos; eduque al personal de su empresa sobre el buen uso de este medio para que sea empleado con fines laborales y para que alerte a la compañía en caso de ver un correo sospechoso. (CERO, 2019)

2. Detecte a tiempo códigos maliciosos

Es común que estos códigos se escondan en archivos PDF, HTML, GIF y Zip. Una buena práctica que no debe dejar de lado, es escoger un antivirus capaz de descubrir, decodificar y descifrar estos códigos ocultos y así evitar ser víctima de robo de información.

3. Reconozca las conexiones sospechosas

Los cibercriminales a menudo usan direcciones IP, sitios web, archivos y servidores de correo electrónico con un histórico de actividad maliciosa. Emplee herramientas capaces de examinar la reputación de fuentes no confiables ubicadas fuera de su organización. (CERO, 2019)

4. Monitorear las bases de datos

La modificación de la estructura en el banco de datos e intentos no autorizados de acceso a datos críticos pueden ser síntomas de alerta que indican que su red estaría amenazada. Use herramientas para monitorear bases de datos y registrar intentos de acceso no autorizado

5. Mantenga su sistema actualizado

La mejor manera de garantizar que los equipos de la empresa tengan buen funcionamiento, es haciendo un inventario de todo el hardware disponible. Después, escoja un plan para gerenciar sus equipos de la manera más efectiva.

Existen dos maneras de hacerlo: entrenar a sus empleados para que realicen las actualizaciones periódicamente o automatizar el proceso a través de una herramienta que actualice automáticamente el sistema. Esta última opción permitirá

que se descarguen las actualizaciones de una sola vez y luego se van distribuyendo dentro de la empresa. (CERO, 2019)

E. Ataque fraudes con tecnología

Los delincuentes no se detienen y todos los días están creando nuevas formas de hacer fraudes a través de internet, por ello, las organizaciones deben contar con sistemas apropiados que revelen oportunamente las actividades sospechosas.

Una estrategia de detección se compone de herramientas analíticas y de mecanismos que ayuden a reportar y escalar los eventos anormales. Precisamente, los reportes de excepciones, la minería de datos, el análisis de tendencias y la evaluación de riesgos en tiempo real son elementos claves de un sistema de detección.

Es importante incluir en la gestión de riesgos tanto los planes de prevención como los de detección. El fraude no solo es una posibilidad, sino una realidad, sin una estrategia efectiva, la amenaza es mayor. (CERO, 2019)

F. Faltan programas maduros y experiencia técnica

Para el Instituto Nacional de Patrones y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), no necesariamente todas las empresas con una infraestructura crítica cuentan con un programa maduro ni con la experiencia técnica suficiente para detectar, evaluar y evitar ataques cibernéticos.

Por ello, emitió la Orden Ejecutiva 13636, que establece que el Marco de seguridad cibernética "identificará áreas de mejora que deberían abordarse

mediante colaboración futura con sectores particulares y organizaciones de desarrollo de estándares". (CERO, 2019)

Para el Instituto Nacional de Patrones y Tecnología —que integra el Departamento de Comercio de los Estados Unidos— si bien existen herramientas, metodologías y estándares para reducir el riesgo, estos necesitan ser más maduros. Por ello, se enfocará en apoyar desarrollo de mejores soluciones de identidad y autenticación a través de los pilotos NTSC (National Television System Committee, en español Comisión Nacional de Sistemas de Televisión) y en realizar investigaciones de identidad y autenticación.

El análisis del Instituto muestra que en el mundo se necesita una fuerza laboral especializada en seguridad informática para satisfacer las necesidades únicas de la infraestructura crítica. “Existe una escasez bien documentada de expertos generales en ciberseguridad; sin embargo, hay una mayor escasez de expertos calificados en ciberseguridad que también comprenden los desafíos únicos que se plantean a partes específicas de la infraestructura crítica.” (CERO, 2019)

Igualmente, señala que a medida que evoluciona la amenaza de ciberseguridad y el entorno tecnológico, la fuerza de trabajo debe seguir adaptándose para diseñar, desarrollar, implementar, mantener y mejorar continuamente las prácticas de ciberseguridad necesarias en entornos de infraestructura críticos.

G. Automatizar los indicadores de información

En la hoja de ruta que propone el Instituto Nacional de Patrones y Tecnología, las organizaciones deben incluir el “intercambio automático de datos de indicadores porque puede proporcionar información oportuna y procesable para detectar y responder a eventos de ciberseguridad a medida que ocurren”.

Esto ayuda a mitigar y a prevenir ataques a medida que ocurren. “Recibir dichos indicadores permite a las tecnologías de automatización de seguridad una mejor oportunidad para detectar ataques pasados, mitigar y remediar vulnerabilidades conocidas, identificar sistemas comprometidos y apoyar la detección y mitigación de futuros ataques”. (CERO, 2019)

Asimismo, el instituto dice en su hoja de ruta que los grandes datos y las herramientas analíticas asociadas, junto con el surgimiento de la computación en la nube, móvil y social, ofrecen oportunidades para procesar y analizar datos estructurados y no estructurados relevantes para la ciberseguridad. Se pueden abordar cuestiones como la conciencia situacional de redes complejas e infraestructuras a gran escala. “El análisis de comportamientos complejos en estos sistemas a gran escala también puede abordar cuestiones de procedencia, atribución y discernimiento de patrones de ataque”. (CERO, 2019)

H. Las actividades futuras de NIST pueden incluir:

Evaluación comparativa y medición de algunos de los elementos científicos fundamentales del big data (algoritmos, aprendizaje automático, topología, teoría de grafos, etc.) a través de medios tales como investigación, evaluaciones comunitarias, conjuntos de datos y problemas de desafío.

Soporte y participación en actividades de estándares de big data tales como organismos de estándares internacionales y producción de arquitecturas de referencia y roadmaps comunitarios; y

Producción de Publicaciones Especiales del Instituto Nacional de Patrones y Tecnología sobre la aplicación segura de técnicas de análisis de big data en áreas

tales como control de acceso, monitoreo continuo, advertencia e indicadores de ataque y automatización de seguridad.

Los sistemas automáticos son buenas herramientas para defenderse de los ciberataques. Las compañías no deben ignorar esta realidad, por el contrario, deben esforzarse en incluir estrategias para minimizar los riesgos. (CERO, 2019)

I. La colaboración, clave para el éxito en ciberseguridad

En la actualidad las organizaciones se sienten ciberamenazadas frente a ciberatacantes que están encontrando cada vez maneras más sofisticadas de llevar a cabo estas actividades maliciosas. (García, 2017)

La tecnología de ciberseguridad puede ser crítica, pero solo es efectiva cuando hay procesos que la mantienen así. Los ataques de phishing, al WiFi o dirigidos a obtener contraseñas, entre otros, representan un nivel inferior pero hay un plano superior de amenazas que pueden afectar a las empresas y comprometer la información y los procesos corporativos. El tipo y el grado de amenazas están en constante evolución y las organizaciones deben revisar y probar sus sistemas regularmente.

El proceso de simular ataques y evaluar el desempeño de las herramientas de seguridad es necesario para determinar las fortalezas y debilidades de las organizaciones y tomar las medidas para que puedan estar preparadas frente a un incidente real. La preocupación por simular un escenario hipotético de “qué pasaría si…” y trabajar en cómo actuar frente a esa situación de manera efectiva es un aspecto importante de la ciberseguridad pero, frente a la escalada de amenazas, las corporaciones deben ir un paso más allá para hacerles frente, y la palabra clave es colaboración. (García, 2017)

Y me refiero a colaboración en la mayor extensión de la palabra, ya que los mayores beneficios de ese esfuerzo llegarán si el intercambio y cooperación son globales, sin censura y con una participación totalmente activa. Esto ha representado un problema en el pasado pero tras los últimos grandes ataques sufridos, como fue el caso de WannaCry, la balanza se inclina hacia este planteamiento.

Los malos han aprendido a moverse rápidamente para evitar los sistemas defensivos y, por ello, para frustrar los ataques, nuestros sistemas necesitan moverse con la misma o mayor rapidez. La colaboración en ciberseguridad puede mejorar nuestros tiempos de respuesta frente a ataques y hacer que la inteligencia contra amenazas esté disponible para un mayor número de corporaciones. A medida que progresan los procesos de intercambio, automatización y distribución de la información sobre amenazas se va reduciendo la fricción del intercambio de inteligencia en seguridad, lo que a su vez incrementa la cantidad y calidad de los datos compartidos, frente a lo que en la teoría de juegos se denomina juegos de "suma cero", para crear entornos en los que todos ganan en ciberseguridad. (García, 2017)

Israel y Japón, Singapur y Australia… ¿Una agencia europea de ciberseguridad?

Son varios los gobiernos que ya se han dado cuenta de los grandes beneficios de la colaboración en seguridad y, por ello, nos encontramos con colaboraciones que nunca habríamos pensado antes de esta disruptiva forma de trabajar.

Por ejemplo, Israel, que es una de las grandes potencias y referente en el ámbito de la ciberseguridad, ha firmado un acuerdo de colaboración en seguridad cibernética, que tiene como objetivo la preparación de cara a los Juegos Olímpicos

de Tokio 2020. Con el consentimiento del gobierno israelí y la respuesta positiva por parte de Japón, actualmente, varias empresas de ambos países trabajan con el fin de coordinar la cooperación en ciberseguridad. También sabemos que Singapur y Australia han firmado un acuerdo de dos años para cooperar estrechamente en materia de ciberseguridad, que incluirá intercambio de información, capacitación y ejercicios conjuntos centrados en las infraestructuras de información crítica. (García, 2017)

Éstos son algunos ejemplos de colaboración entre gobiernos, y el horizonte se amplía: recientemente Juncker proponía la creación de una agencia europea de ciberseguridad, ya que como él mismo indica: "se trata de un peligro que no conoce fronteras" y qué mejor forma de combatirlo que con la colaboración conjunta en ciberseguridad.

No hay duda de que las reglas del juego en ciberseguridad han cambiado y ya no va de silos estancos de información a modo de fortaleza, sino de cooperación internacional entre gobiernos y naciones y es que, entre todos, existe una opción mayor de dificultar los cada vez más complejos ataques de seguridad. La clave del éxito reside en la colaboración. (García, 2017)

2.2.1.1. Unidad de Aprendizaje

Debido a las numerosas innovaciones que se están sucediendo en el terreno de la ciberseguridad, un experto en este sector debe adquirir una gran variedad de conocimientos para poder estar actualizado y reconocer las posibles amenazas que van surgiendo. Por este motivo, lo primero que en aprender es a desarrollar diferentes capacidades para poder anticiparnos a los problemas que puedan aparecer en los sistemas informáticos. A medida que aprendamos

estaremos más preparados para dar la mayor protección a dicho sistema y responder de forma adecuada con los métodos o técnicas precisos para tener el control del mismo.

El temario de ciberseguridad es flexible y muy completo, comenzando con una base teórica donde aprenderemos conceptos y términos importantes dentro de este sector hasta la puesta en marcha de todos estos conocimientos adquiridos a través de talleres de práctica en los que podremos comprobar nuestras nuevas habilidades. En este sentido, también debemos destacar que aprenderemos a elaborar una estrategia para activar el protocolo necesario en el caso de que detectemos una posible amenaza dentro de nuestro sistema informático. (OBS, 2019)

Durante el proceso de aprendizaje en ciberseguridad se tiene que ser capaces de prevenir los problemas y de identificarlos cuando están dando sus primeros pasos. La prevención es un elemento crucial en el proceso de mantener los sistemas informáticos a salvo de posibles amenazas. Pero en el caso de que ya se esté comenzando a producir un incidente, al menos estos expertos que hayan cursado un máster podrán dar respuesta inmediata y encontrar una solución al instante para evitar males mayores.

Las principales funciones de un experto en ciberseguridad son la anticipación a las amenazas informáticas y la implantación de soluciones eficaces que den respuesta a situaciones críticas. Para lograr esto último los especialistas deben tener una buena formación que les permita gestionar con eficacia los sistemas de seguridad y las diferentes herramientas con las que trabajarán. En ocasiones los procedimientos a llevar a cabo se combinan unos

con otros o deben realizarse en un orden determinado, por lo que conviene tenerlo en cuenta. Por esto mismo las diferentes asignaturas también enseñan paso a paso a utilizar las principales herramientas de uso habitual en el sector, además de saber utilizar una metodología adecuada o el conocer cuáles son los mejores procesos que se pueden llevar a cabo para proteger los datos de las empresas. Y todo ello siempre teniendo en cuenta que los expertos en seguridad se deben mantener actualizados de forma constante para conocer las últimas novedades y cambios del sector. (OBS, 2019)

2.2.1.2. Prácticas Especializadas

Controlar el desarrollo seguro de producto, velar por el cumplimiento de todas las normativas tipo RGPD (Reglamento General de Protección de Datos), valorar el alcance de un intento de intrusión en la empresa, decidir qué incidente es más urgente y cuál más importante, descubrir fallos de seguridad (y solucionarlos), mejorar todos los sistemas, arquitectura, tecnologías y herramientas de una compañía, realizar un análisis forense cuando ha habido una intrusión…

Si el campo de la ciberseguridad es amplio, las labores que desarrollan los expertos en la materia no lo son menos. Por eso, lo más normal es que estos profesionales estén especializados en alguno o varios de estos cometidos y su quehacer diario sea, en cierto modo, muy diferente al de otros compañeros. Pero también está el rol del CISO (Chief Information Security Officer o director de seguridad de la información) que es la máxima "autoridad" en una organización para definir la estrategia, gestionar a los diferentes equipos y hablar con el comité de dirección. En muchas ocasiones, el CISO ha sido

cocinero antes que fraile y antes de llegar a esta posición ha pasado por roles técnicos.

Pero, como nos ha dicho -sonriendo- uno de nuestros interlocutores, vamos a intentar explicar en este artículo a qué se dedican los expertos en ciberseguridad, "aquello que nos ha costado más de 10 años que entiendan nuestros padres". Eso sí, dado que la seguridad es uno de los asuntos más críticos de las empresas, hay cosas que permanecen bajo secreto de sumario y ni siquiera estos profesionales pueden dar pistas de por dónde discurre su trabajo.

2.2.1.3. Herramientas de Estudio

Especialmente con la implementación de políticas de BYOD (big your own device) en las que, al usar el trabajador su propio dispositivo de trabajo, se genera una heterogeneidad en las plataformas laborales poniendo en riesgo la estandarización y elevando los costos de soporte para las organizaciones. Por lo anterior, las empresas deben contar con estrictas políticas de ciberseguridad para contrarrestar dichos riesgos.

A continuación, 5 consejos para implementar herramientas de ciberseguridad en las empresas de hoy:

- Las empresas deben contar con una política de seguridad informática que reconozca la presencia de los dispositivos y verificarlos antes de que cuenten con acceso a la red organizacional.

- La empresa debe contar con sistemas de IDS/ISP (Intrusion Detection / Prevention System) especialmente dedicados a las plataformas móviles.

- Implementación de sistemas y soluciones que integren la protección antivirus de los dispositivos con la encriptación de datos sensibles y medidas antirrobo basadas en la utilización de contraseña maestra y factores biométricos, como el reconocimiento facial y dactilar.

- Administrar el ciclo de vida de los dispositivos para asegurar que las actualizaciones de sistemas de ciberseguridad no se conviertan en obsoletas en determinado momento.

- Limitar el almacenamiento de información empresarial a los dispositivos y activos (físicos y virtuales) de la empresa y no permitir el acceso desde cuentas personales o ajenas a las corporativas. (Belluomo, 2017)

2.2.2. Variable 2: Formación Profesional

La Formación Profesional es el conjunto de acciones que tienen como propósito la formación socio-laboral para y en el trabajo, orientada tanto a la adquisición y mejora de las cualificaciones como a la recualificación de los trabajadores. La Formación Profesional permite compatibilizar la promoción social, profesional y personal con la productividad de la economía nacional, regional y local. También contempla la especialización y la actualización de conocimientos y capacidades, tanto de las distintas trayectorias de la ETP (Educación Técnico Profesional) como de los niveles superiores de la educación formal. (INET, 2018)

Asimismo, admite formas de ingreso y de desarrollo diferenciadas de los requisitos educativos propios de los niveles y ciclos de la educación formal.

El ámbito de la Formación Profesional se organiza en su interior según, el tipo de propósito formativo, y la forma de acceso, en: Capacitación laboral; Formación

profesional inicial organizada a su vez en tres niveles de certificación; y en la Formación Profesional Continua.

Sus objetivos específicos son: preparar, actualizar y desarrollar las capacidades de las personas para el trabajo, cualquiera sea su situación educativa inicial, a través de procesos que aseguren la adquisición de conocimientos científico-tecnológicos y el dominio de las competencias básicas, profesionales y sociales requerido por una o varias ocupaciones definidas en un campo ocupacional amplio, con inserción en el ámbito económico-productivo. (INET, 2018)

2.2.2.1. Instrucción

> Se conoce como instrucción militar, por lo tanto, a la formación que reciben los integrantes de las fuerzas armadas para que puedan ejercer sus funciones con éxito. Esta instrucción implica la enseñanza de diversos conocimientos, desde el uso de armas hasta nociones de estrategia militar, pasando por la preparación física y la capacitación jurídico-militar. La instrucción militar se desarrolla tanto en las aulas como en simuladores, polígonos de tiro y en eventuales terrenos de operaciones. (Pérez & Merino, Definición de instrucción militar , 2012)
>
> Por todo ello podemos establecer que la instrucción militar se conforma o sustenta en los siguientes pilares: instrucción de combate, instrucción en orden cerrado, formación académica específica militar, instrucción físico-militar, instrucción de tiro y formación jurídico militar.
>
> En este caso hay que explicar que la formación específica citada es aquella gracias a la cual los soldados aprenden todo lo necesario sobre los procedimientos operativos y sobre los reglamentos. Mientras, en el caso de la

formación jurídico militar, lo que se consigue es que conozcan todo lo que concierne a las leyes, penas, derechos y castigos.

Instrucción es un término asociado al verbo instruir (transmitir un saber, facilitar el aprendizaje) que también se utiliza para nombrar al reglamento que tiene una finalidad específica, al acervo de conocimientos y al curso seguido por un procedimiento en marcha.

Militar, por su parte, está vinculado a la milicia y a lo bélico. La noción puede referirse a los soldados, las infraestructuras o las entidades que componen las fuerzas armadas. (Pérez & Merino, 2012)

En concreto, podemos matizar un poco más este segundo término determinando que tiene su origen etimológico en el latín y más exactamente en el vocablo militaris que puede definirse como "relativo o perteneciente a los soldados" y que ha dado lugar a otras palabras en castellano como milicia o militarismo, por ejemplo.

Fundamental se considera dentro de su ámbito correspondiente que los soldados reciban la correspondiente instrucción militar y es que, en primer lugar, se considera que es básica para que puedan llevar a cabo sus tareas y misiones de la manera más eficaz y eficiente.

No obstante, de la misma forma se establece también que aquella es importante para que los citados individuos sepan no sólo cómo hacer sus funciones sino también el motivo de que tengan que acometerlas. Se trata, por tanto, de establecer el sentido de su labor y de que entiendan el importante papel que desempeñan en el marco político-social. (Pérez & Merino, 2012)

Los militares se encargan de defender la integridad y la soberanía de un territorio. Esto quiere decir que, en circunstancias excepcionales, pueden hacer uso de la fuerza y de las armas. Una parte de la instrucción militar, por lo tanto, está orientada a cómo y cuándo recurrir a la fuerza.

Las fuerzas armadas responden al gobierno de cada país y deben actuar según los parámetros fijados por la Constitución Nacional. Por eso la instrucción militar, cuya extensión varía de acuerdo al trabajo que deberá desarrollar el soldado, incluye nociones legales y sobre las normativas del cuerpo. Uno de los objetivos de la instrucción militar es evitar excesos por parte de los soldados. (Pérez & Merino, 2012)

2.2.2.2. Entrenamiento

El entrenamiento es la adquisición de habilidades, capacidades y conocimientos como resultado de la exposición a la enseñanza de algún tipo de oficio, carrera o para el desarrollo de alguna aptitud física o mental y que está orientada a reportarle algún beneficio o utilidad al individuo que se somete a tal o cual aprendizaje.

Existen diferentes tipos de entrenamiento de acuerdo a ese fin que se tenga y que mencionamos. Entre los más populares y conocidos por todos, nos encontramos con el entrenamiento físico que es aquel que se practica recurrentemente con el objetivo de lograr una adecuada resistencia física, ya sea para lograr un buen estado físico y por consiguiente de salud, o el entrenamiento del personal que tiene lugar en algunas empresas para preparar a los futuros ocupantes de un determinado cargo dentro de la organización y que por su especificidad requiere de una aclimatación previa o bien, también

es común que algunas empresas que por ejemplo se dedican a la tecnología, algo que siempre es sabido está en un constante cambio, usen el entrenamiento como un recurso para mantener siempre al tanto de las novedades y cambios a sus empleados, aún aquellos que hace tiempo se desempeñan en la misma. (Pérez & Merino, 2008)

2.2.2.3. Herramientas Académicas

Primera herramienta: Retransmisor de contenidos, generalmente denominado maestro o profesor. Es en este concepto donde más se invierte el presupuesto educativo (probablemente más del 85% de los recursos) y en ese sentido es válido cuestionar la pertinencia y eficacia de mantener un complejo sistema de retransmisores de contenidos, a través de las funciones y efectos que desarrollan.

La gran diferencia está en la actitud del aprendiz, es decir, si necesita el conocimiento o simplemente quiere aprender, al mediador se le releva a su debido segundo plano, el problema es que con el retransmisor de contenidos como centro del proceso educativo, el aprendiz es quien toma la segunda prioridad y entonces la decisión de aprender la toma el que "enseña", sin considerar las condiciones del aprendiz, por ejemplo si tiene voluntad, si tiene necesidad del conocimiento, si es su mejor momento para aprender, si el aprendiz lo puede contextualizar, etc. (Granados, 2014)

Segunda herramienta: Ambientes de aprendizaje desconectados de la realidad, también comúnmente llamados salones de clase. Desconozco el origen de los salones de clase ni por qué se decidió que en esos lugares se podría encontrar un lugar adecuado para aprender, no se parecen en nada a la

vida diaria, los niños no aprenden un idioma en un salón, los niños no aprenden a convivir en un salón cerrado, los deportistas no aprenden su deporte en un salón, los músicos no desarrollan sus talentos en salones parecidos a los de clases, los empresarios no desarrollan sus negocios en salones, en fin prácticamente lo único que se hace en sitios similares a salones de clase son reuniones de trabajo donde normalmente un pequeño grupo de personas se sienta a analizar información que todos proveen y deciden en consecuencia las mejores soluciones normalmente en consenso.

2.3. Definición de Términos Básicos

Amenazas: Actitud expresada o deducida, o una situación, que hacen presumir riesgo, peligro o daño sobre las personas, las entidades o cosas amenazadas. (Jave, 2004)

Aulas Virtuales: Se conoce como aula virtual a un entorno digital que posibilita el desarrollo de un proceso de aprendizaje. Las tecnologías de la información y la comunicación (TIC) permiten que el estudiante acceda al material de estudio y, a su vez, interactúe con el profesor y con otros estudiantes. (Pérez & Merino, 2017)

Biblioteca: Biblioteca podemos referir varias cuestiones. Por un lado se llama biblioteca a cualquier tipo de colección organizada, ya sea de libros o publicaciones en serie, o bien de documentos gráficos o audiovisuales, y que se encuentran disponibles para ser consultados o tomados en préstamo. (Ucha, 2009)

Cursos Militares: Curso de instrucción que se dicta en la Escuela de Inteligencia a Oficiales Subalternos, a fin de capacitarlos para cumplir las funciones de Oficial de Inteligencia o Auxiliares en las diferentes reparticiones de las Fuerzas Armadas. (Jave, 2004)

Destrezas: La destreza es la habilidad o arte con el cual se realiza una determinada cosa, trabajo o actividad y haciéndolo de manera correcta, satisfactoria, es decir, hacer algo con destreza implicará hacerlo y bien. (Ucha, 2010)

Doctrina: Conjunto de principios y su consecuente teoría que aplicados a un medio determinado, teniendo en cuenta sus características y peculiaridades, genera métodos y procedimientos que norman las acciones destinadas a alcanzar una finalidad específica. (Jave, 2004)

Efectividad: Situación de un oficial que está en posesión efectiva de un empleo. Esta situación la adquiere el oficial de las Fuerzas Armadas que se forma en los Centros de Formación de Oficiales. Los Oficiales de los Servicios que se forman en centros no militares, ingresan al servicio como asimilados y adquieren la efectividad posteriormente. (Jave, 2004)

Entrenamiento: Conjunto de ejercicios intelectuales, síquicos y físicos, progresivamente creciente, a que se someten los individuos y las unidades militares con el fin de alcanzar una capacidad suficiente para la ejecución de una función determinada. Puede ser individual, de unidad o de gran unidad. (Jave, 2004)

Habilidades: Hace referencia a la maña, el talento, la pericia o la aptitud para desarrollar alguna tarea. La persona hábil, por lo tanto, logra realizar algo con éxito gracias a su destreza. (Pérez & Merino, 2008)

Instrucción: Documento que se establece en los escalones más elevados del Comando, para guiar y controlar la acción del subordinado en las operaciones en grandes áreas y que abarquen períodos considerables. Siguen, tanto como sea posible, el formato de los planes u órdenes de operaciones. (Jave, 2004)

Internet: Internet proviene de "interconneted networks" ("redes interconectadas"): básicamente se trata de millones de computadoras conectadas entre sí en una red mundial. (Guglielmetti, 2008)

Laboratorios: Gabinete o local donde se realizan estudios y trabajos experimentales de cualquier ciencia o actividad, o donde se realizan ensayos y análisis de productos medicinales, drogas, explosivos, etc. (Jave, 2004)

2.4. Hipótesis

2.4.1. Hipótesis general

Existe una relación directa y significativa entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis general o nula – No existe una relación directa y significativa entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

2.4.2. Hipótesis específicas

Hipótesis especifica N°1: Existe una relación directa y significativa entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis especifica o nula N°1 – No existe una relación directa y significativa entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis especifica N°2: Existe una relación directa y significativa existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis especifica o nula N°2 – No existe una relación directa y significativa existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis especifica N°3: Existe una relación directa y significativa existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

Hipótesis especifica o nula N°3 – No existe una relación directa y significativa existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

2.5. Variables

2.5.1. Definición conceptual

Implementación de la Asignatura de Ciberseguridad: En la era digital se habla de Ciberseguridad, que se asocia a las ciberamenazas, al cibercrimen, pero también a las buenas prácticas para proteger la información y prevenir o detectar los ataques cibernéticos. Las amenazas de la seguridad informática llegan a través de programas dañinos o maliciosos que se instalan en un dispositivo o se penetran por medio de la nube. (CERO, 2019)

Formación Profesional: La Formación Profesional es el conjunto de acciones que tienen como propósito la formación socio-laboral para y en el trabajo, orientada tanto a la adquisición y mejora de las cualificaciones como a la recualificación de los trabajadores. La Formación Profesional permite compatibilizar la promoción social, profesional y personal con la productividad de la economía nacional, regional y local. (INET, 2018)

2.5.2. Definición Operacional

Tabla 1.
Operacionalización de las Variables

VARIABLES	DIMENSIONES	INDICADORES	ÍTEMS
Variable 1 Implementación de la Asignatura de Ciberseguridad	Unidad de Aprendizaje	Doctrina de Ciberseguridad	¿Existe alguna doctrina de ciberseguridad implementada en la Escuela Militar de Chorrillos?
		Tipos de Ciberataques	¿Conoces algún tipo de ciberataque que se podría implementar en la asignatura de ciberseguridad?
		Niveles de Amenazas	¿Tienes conocimiento de los niveles de amenaza que podría existir en la asignatura de ciberseguridad?
	Prácticas Especializadas	Diseñar Medidas de Seguridad	¿Podrías diseñar tu propia medida de seguridad en línea, para tus trabajos académicos?
		Detección de Amenazas	¿Desearías tener cursos especializados para cualquier detección de amenazas cibernéticas?
		Contrarrestar Amenazas	¿Tienes conocimiento de cómo contrarrestar las amenazas de ciberseguridad?
	Herramientas de Estudio	Laboratorios	¿Consideras necesario implementar laboratorios sofisticados para la asignatura de ciberseguridad?
		Bibliotecas Virtuales	¿Desearías tener una biblioteca virtual en la Escuela Militar de Chorrillos para conocer la ciberseguridad?
		Aulas Virtuales	¿Consideras necesario implementar un aula virtual en la Escuela Militar de Chorrillos para llevar la asignatura de ciberseguridad?

VARIABLES	DIMENSIONES	INDICADORES	ÍTEMS
Variable 2 Formación Profesional	Instrucción	Cursos Civiles	¿Existen cursos civiles que brindan la Escuela Militar de Chorrillos para conocer la ciberseguridad?
		Cursos Militares	¿Existen cursos militares ligadas a la ciberseguridad brindadas en la Escuela Militar de Chorrillos?
		Cursos de Idiomas	¿Es necesario los cursos de idioma para conocer la asignatura de ciberseguridad?
	Entrenamiento	Habilidades	¿Es necesario considerar algunas habilidades o tics para conocer la ciberseguridad?
		Destrezas	¿Consideras que existen destrezas en los cadetes de inteligencia para llevar la asignatura de ciberseguridad hacia una alta eficiencia?
		Efectividad	¿Cuánta efectividad se cuenta en el entrenamiento para la formación profesional de los cadetes de inteligencia?
	Herramientas Académicas	Internet	¿Se cuenta con la velocidad de internet adecuada en la Escuela Militar de Chorrillos para la formación profesional de los cadetes?
		Biblioteca	¿Se cuenta con una biblioteca moderna en la Escuela Militar de Chorrillos para la formación profesional de los cadetes de inteligencia?
		Sala Táctica (SATAC)	¿La Sala Táctica (SATAC) cubre las necesidades de los cadetes de inteligencia para la formación profesional?

Fuente: Elaboración Propia

CAPITULO III

MARCO METODOLÓGICO

3.1. Enfoque

El enfoque es cuantitativo, ya que se empleó la recolección y el análisis de los datos, para contestar las preguntas de investigación y probar la hipótesis. Según Calero (2002)

3.2. Tipo

El tipo de investigación utilizado es el de Aplicada. Según Zorrilla (1993) La investigación aplicada, guarda íntima relación con la básica, pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar.

3.3. Diseño

El diseño de la investigación corresponde al no experimental, de carácter transversal; por cuanto, no tuvo como propósito manipular una de las variables a fin de causar un efecto en la otra, sino que se trabajó sobre situaciones ya dadas; y transversal porque el instrumento utilizado para capitalizar los datos de las unidades de estudio se aplicó en una sola oportunidad. Según Hernández, Fernández & Baptista (2003), describe como "los estudios que se realizan sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos".

Clasificado como transaccionales o transversales; son los que se encargan de recolectar datos en momento único, describe variables en ese mismo momento o en un momento dado.

3.4. Método

Descriptiva-correccional. Según Hernández (1998) La investigación descriptiva busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis. Y tanto en la correccional que tiene como propósito evaluar la relación que existe entre dos o más conceptos, categorías o variables (en un contexto en particular).

3.5. Población y muestra

3.5.1. Población

Se establecen una población de 49 Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

3.5.2. Muestra

Es probabilístico de carácter aleatorio, tomando en cuenta los 2 Cadetes de Cuarto; resultando como diferencia:

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

N =	49	Tamaño de la población
Z =	1.96	Nivel de confianza
p =	0.5	Probabilidad de éxito
q =	0.5	Probabilidad de fracaso
d =	0.05	Margen de error

$$n = \frac{(49) * (1.96)^2 * (0.5) * (0.5)}{(0.05)^2 * (49 - 1) + (1.96)^2 * (0.5) * (0.5)}$$

$$n = \frac{47.0596}{1.0804}$$

$$N = 44$$

44 Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019, dando como resultado a la muestra.

3.6. Técnicas para la recolección de datos

Para los Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", participantes en la investigación, el instrumento empleado fue el cuestionario, a través de la técnica de encuesta autoaplicado, siendo este instrumento de recolección de datos semi estructurado y constituido por 18 preguntas (cerradas), correlacionadas por cada indicador, la que tuvo por finalidad determinar la Implementación de la asignatura de Ciberseguridad y la Formación profesional. Los criterios de construcción del instrumento recogida de datos (cuestionario) fueron los siguientes:

El presente cuestionario solo incluye preguntas cerradas, con lo cual se busca reducir la ambigüedad de las respuestas y favorecer las comparaciones entre las respuestas.

Cada indicador de la variable independiente será medido a través de (1) pregunta justificada en cada uno de los indicadores y dimensiones de la variable dependiente, con lo cual se le otorga mayor consistencia a la investigación.

Todas las preguntas serán precodificadas, siendo sus opciones de respuesta las siguientes:

Tabla 2.
Diagrama de Likert

A Totalmente de Acuerdo	B De Acuerdo	C Indeciso	D Desacuerdo	E Totalmente Desacuerdo

Fuente: Desarrollada en 1932 por el sociólogo Rensis Likert

Todas las preguntas reflejan lo señalado en el diseño de la investigación al ser descriptivas-correlacional.

Las preguntas del Cuestionario están agrupadas por indicadores de la variable independiente con lo cual se logra una secuencia y orden en la investigación.

No se ha sacrificado la claridad por la concisión, por el contrario, dado el tema de investigación hay preguntas largas que facilitan el recuerdo, proporcionando al encuestado más tiempo para reflexionar y favorecer una respuesta más articulada.

Las preguntas han sido formuladas con un léxico apropiado, simple, directo y que guardan relación con los criterios de inclusión de la muestra.

Para evitar la confusión de cualquier índole, se han referido las preguntas a un aspecto o relación lógica enumerada como subtítulo y vinculadas al indicador de la variable independiente.

De manera general, en la elaboración del cuestionario se ha previsto evitar, entre otros aspectos: inducir las respuestas, apoyarse en las evidencias comprobadas, negar el tema que se interroga, así como el desorden investigativo.

La precodificación de las respuestas a las preguntas establecidas en la encuesta se precisa en la siguiente tabla:

La utilización de las preguntas cerradas tuvo como base evitar o reducir la ambigüedad de las respuestas y facilitar su comparación. Adjunto a la encuesta se colocó un glosario

de términos especificando aquellos aspectos técnicos presentes en las preguntas determinadas. Además, las preguntas fueron formuladas empleando escalas de codificación para facilitar el procesamiento y análisis de datos, enlazando los indicadores de la variable de causa con cada uno de los indicadores de la variable de efecto, lo que dio la consistencia necesaria a la encuesta.

3.7. Validación y confiabilidad del Instrumento

Para efectos de la validación del instrumento se acudió al Juicio de Expertos Temáticos, para lo cual se sometió el cuestionario de preguntas al análisis de tres profesionales de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", con grado de magíster, cuya apreciación se resumen en el siguiente cuadro y el detalle como anexo.

Tabla 3.
Resultados de la Validación según Expertos

N°	EXPERTOS	% VALIDACIÓN
01	Dr. SILVA CALDERON, JOSEFA MARIA	70.00%
02	Mg. PAUCAR LUNA, JORGE ANASTACIO PEDRO	90.00%
03	Mg. DAVILA ECHEVARRIA, JOSE EDGARDO	82.00%
Promedio		**80.67%**

Fuente: Elaboración Propia

El documento mereció una apreciación promedio de 90% se hace constar fue el instrumento se sujetó para su mejoramiento a una prueba piloto aplicada a los Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Cadetes del Arma de Inteligencia.

Trabajos de investigación realizados en nuestro país y en el extranjero que se indican en los antecedentes de la investigación,

Para validar los instrumentos se sometieran los Ítems a juicio de tres expertos, los cuales evaluaran y asignaran un atributo para cada Ítem, en base a estos resultados se procederá a llenar la hoja resumen de opinión de expertos para determinar el atributo promedio que corresponde a cada Ítem. Los Ítem que obtuvieran un promedio menor a 80 puntos, serán desestimados o modificados en su estructura.

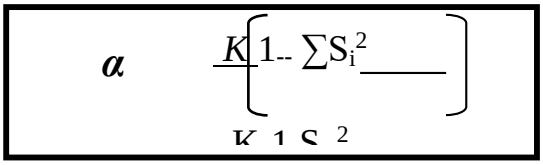
Para la confiabilidad se le aplico el criterio del Alpha de Cronbach.

Se empleó el instrumento descritos en el párrafo a y b: Cuestionarios para las variables, Implementación de la asignatura de Ciberseguridad y la formación profesional mediante el coeficiente de Alpha de Cronbach para comprobar la consistencia interna, basado en el promedio de las correlaciones entre los ítems para evaluar cuanto mejoraría (o empeoraría) la fiabilidad de la prueba si se excluye un determinado ítem, procesado con la aplicación SPSS (Producto de Estadística y Solución de Servicio) versión 22. Su fórmula determina el grado de consistencia y precisión.

Criterio de confiabilidad valores:

- No es confiable -1 a 0
- Baja confiabilidad 0.01 a 0. 49
- Moderada confiabilidad 0.5 a 0.75
- Fuerte confiabilidad 0.76 a 0.89
- Alta confiabilidad 0.9 a 1

- **Coeficiente Alfa de Cronbach**



En donde:

K = El número de ítems

$\sum \mathbf{S_i^2}$ = Sumatoria de Varianzas de los ítems

$\mathbf{S_t^2}$ = Varianza de la suma de los ítems

œ = Coeficiente de Alpha de Cronbach

Este instrumento se utilizó en la prueba piloto de una muestra de 44 entrevistados (Cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos) por cada variable de estudio realizada en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", durante el año 2019.

3.8. Procedimientos para el tratamiento de datos

Los métodos utilizados para el procesamiento de los resultados obtenidos a través de los diferentes instrumentos de recolección de datos, así como para su interpretación posterior, han sido el análisis y la síntesis, que permitió una mejor definición de los componentes individuales del fenómeno estudiado; y, de deducción-inducción, que permitió comprobar a través de hipótesis determinadas el comportamiento de indicadores de la realidad estudiada.

La base de datos y el análisis, recodificación de variables y la determinación de la estadística descriptiva e inferencial. Para las Pruebas de Hipótesis hemos utilizados la Prueba de Independencia de Chi Cuadrada (X^2) con dos variables y con categorías y el Análisis Exploratorio que sirve para comprobar si los promedios provienen de una distribución normal.

3.9. Aspectos éticos

La investigación considera los siguientes criterios éticos:

La investigación tiene un valor social.

La investigación tiene validez aprendizaje, práctica e instrucción.

Para realizar la investigación ha existido un consentimiento informado y un respeto a los participantes.

CAPITULO IV

RESULTADOS

4.1. Descripción

Variable 1: Implementación de la Asignatura de Ciberseguridad

P1: ¿Existe alguna doctrina de ciberseguridad implementada en la Escuela Militar de Chorrillos?

Tabla 4
Unidad de Aprendizaje, Doctrina de Ciberseguridad

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	39	88.64%
Indiferente	5	11.36%
De Acuerdo	0	0.00%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

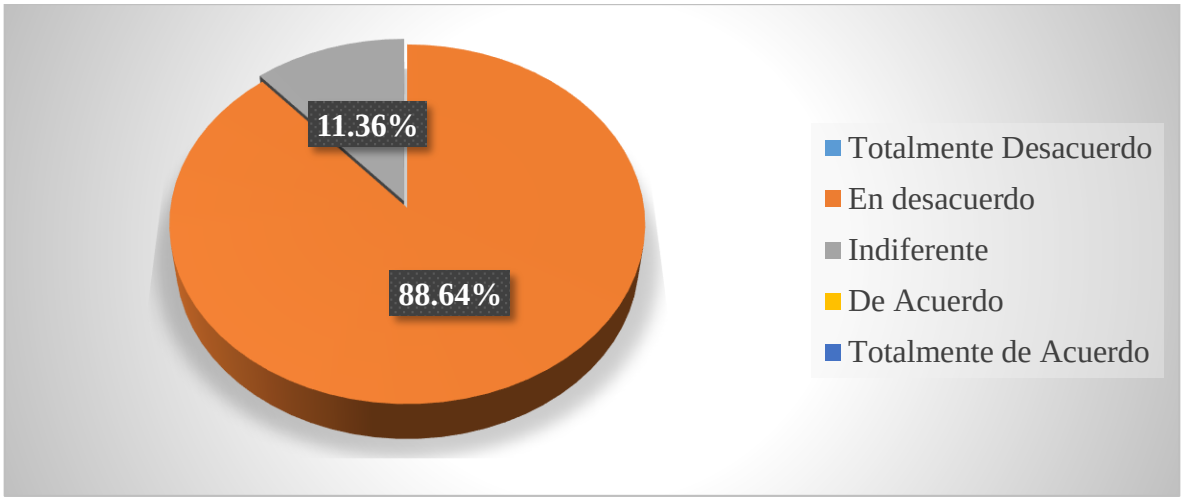


Figura 1. Unidad de Aprendizaje, Doctrina de Ciberseguridad
Fuente: Tabla 4

Interpretación 1: En la Tabla 4 y la Figura 1 se observa que el 88.64% la mayoría determina "En desacuerdo", el 11.36% determina "Indiferente", el 0.00% determina

"Totalmente Desacuerdo", el 0.00% determina "De Acuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que no existe alguna doctrina de ciberseguridad implementada en la Escuela Militar de Chorrillos.

P2: ¿Conoces algún tipo de ciberataque que se podría implementar en la asignatura de ciberseguridad?

Tabla 5
Unidad de Aprendizaje, Tipos de Ciberataques

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	10	22.73%
Indiferente	7	15.91%
De Acuerdo	27	61.36%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

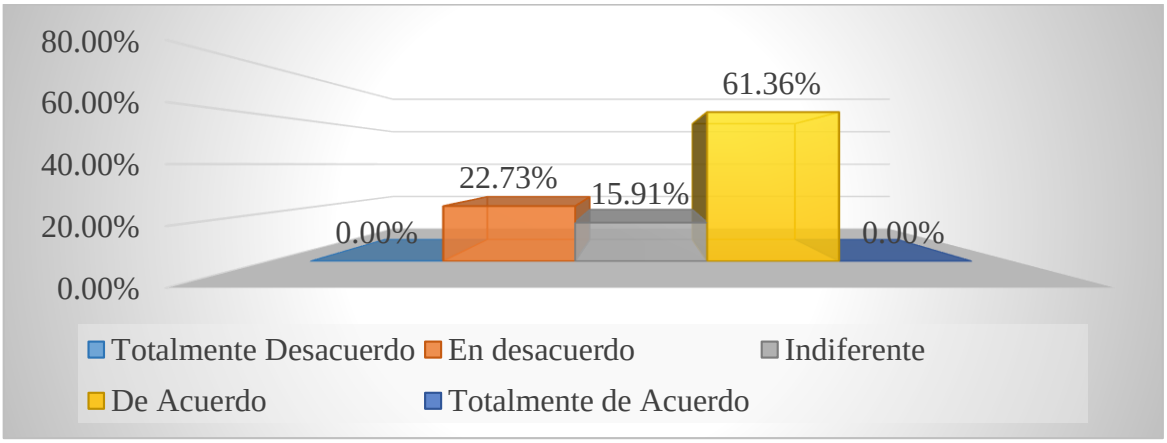


Figura 2. Unidad de Aprendizaje, Tipos de Ciberataques
Fuente: Tabla 5

Interpretación 2: En la Tabla 5 y la Figura 2 se observa que el 61.36% la mayoría determina "De Acuerdo", el 22.73% determina "En desacuerdo", el 15.91% determina "Indiferente", el 0.00% determina "Totalmente Desacuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que algún tipo de ciberataque que se podría implementar en la asignatura de ciberseguridad.

P3: ¿Tienes conocimiento de los niveles de amenaza que podría existir en la asignatura de ciberseguridad?

Tabla 6
Unidad de Aprendizaje, Niveles de Amenazas

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	36	81.82%
Indiferente	0	0.00%
De Acuerdo	8	18.18%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

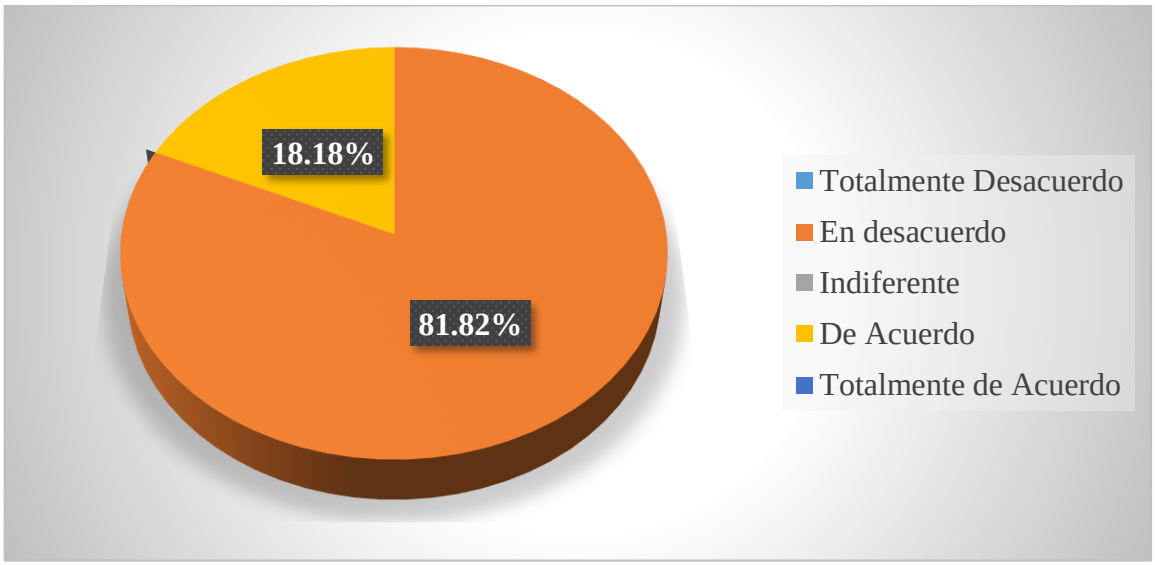


Figura 3. Unidad de Aprendizaje, Niveles de Amenazas
Fuente: Tabla 6

Interpretación 3: En la Tabla 6 y la Figura 3 se observa que el 81.82% la mayoría determina "En desacuerdo", el 18.18% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "Indiferente" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que no tienen conocimiento de los niveles de amenaza que podría existir en la asignatura de ciberseguridad.

P4: ¿Podrías diseñar tu propia medida de seguridad en línea, para tus trabajos académicos?

Tabla 7
Prácticas Especializadas, Diseñar Medidas de Seguridad

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	3	6.82%
En desacuerdo	37	84.09%
Indiferente	0	0.00%
De Acuerdo	4	9.09%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

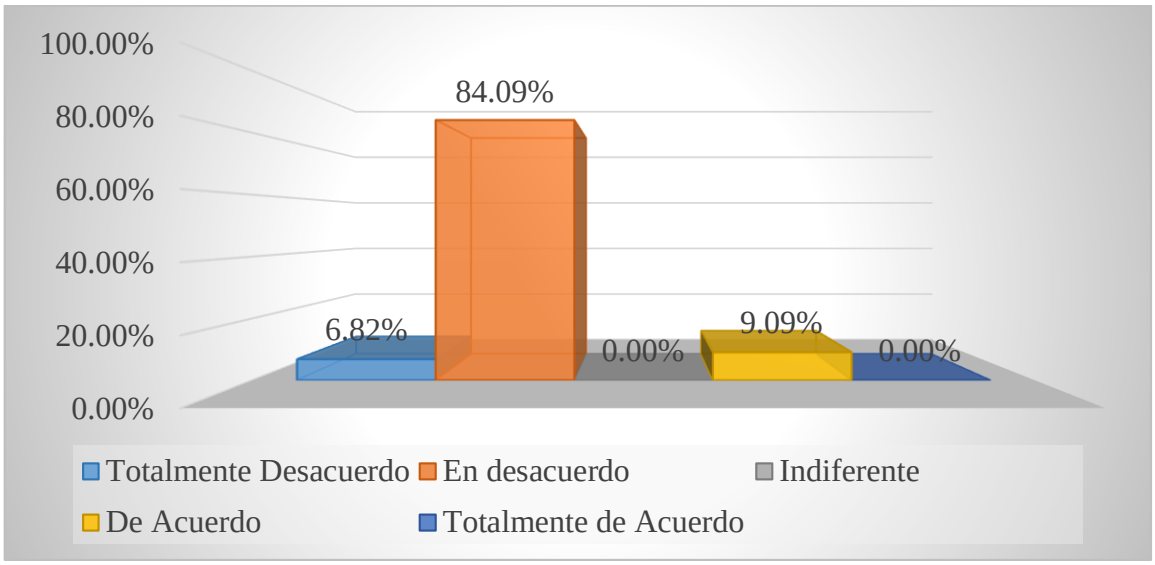


Figura 4. Prácticas Especializadas, Diseñar Medidas de Seguridad
Fuente: Tabla 7

Interpretación 4: En la Tabla 7 y la Figura 4 se observa que el 84.09% la mayoría determina "En desacuerdo", el 9.09% determina "De Acuerdo", el 6.82% determina "Totalmente Desacuerdo", el 0.00% determina "Indiferente" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que no podrán diseñar su propia medida de seguridad en línea, para tus trabajos académicos.

P5: ¿Desearías tener cursos especializados para cualquier detección de amenazas cibernéticas?

Tabla 8
Prácticas Especializadas, Detección de Amenazas

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	4	9.09%
Totalmente de Acuerdo	40	90.91%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

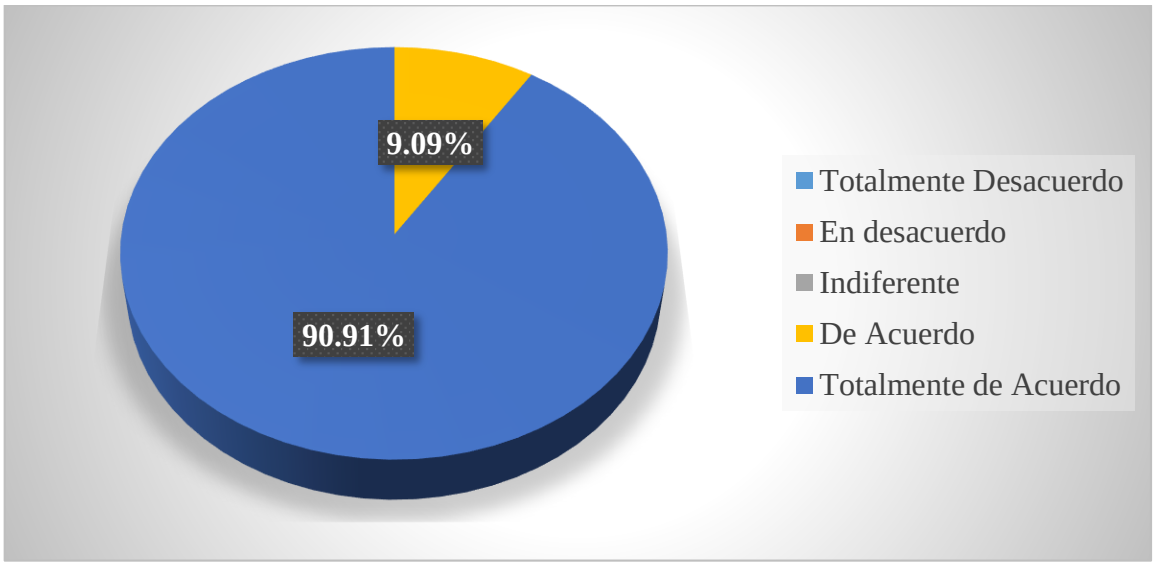


Figura 5. Prácticas Especializadas, Detección de Amenazas
Fuente: Tabla 8

Interpretación 5: En la Tabla 8 y la Figura 5 se observa que el 90.91% la mayoría determina "Totalmente de Acuerdo", el 9.09% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que tener cursos especializados para cualquier detección de amenazas cibernéticas.

P6: ¿Tienes conocimiento de cómo contrarrestar las amenazas de ciberseguridad?

Tabla 9
Prácticas Especializadas, Contrarrestar Amenazas

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	2	4.55%
En desacuerdo	36	81.82%
Indiferente	6	13.64%
De Acuerdo	0	0.00%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

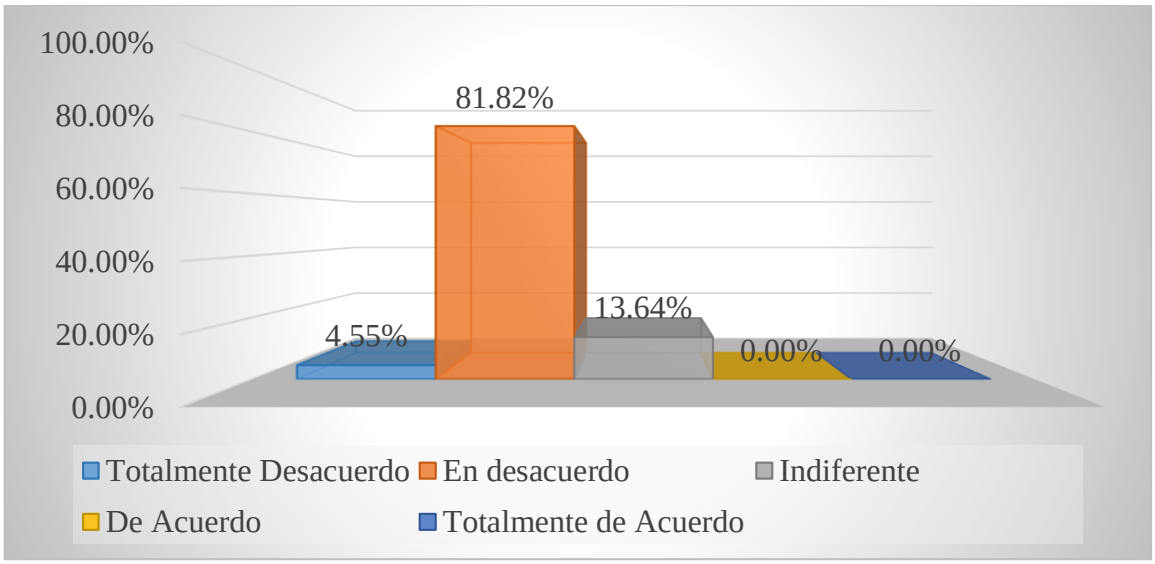


Figura 6. Prácticas Especializadas, Contrarrestar Amenazas
Fuente: Tabla 9

Interpretación 6: En la Tabla 9 y la Figura 6 se observa que el 81.82% la mayoría determina "En desacuerdo", el 13.64% determina "Indiferente", el 4.55% determina "Totalmente Desacuerdo", el 0.00% determina "De Acuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que no tienen conocimiento de cómo contrarrestar las amenazas de ciberseguridad.

P7. ¿Consideras necesario implementar laboratorios sofisticados para la asignatura de ciberseguridad?

Tabla 10
Herramientas de Estudio, Laboratorios

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	5	11.36%
Totalmente de Acuerdo	39	88.64%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

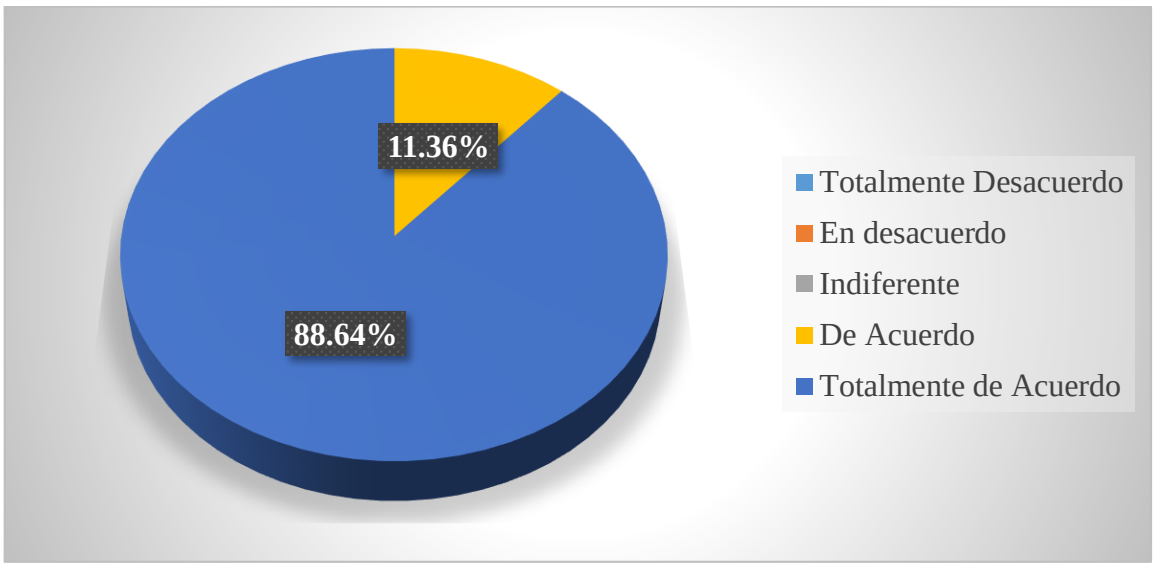


Figura 7. Herramientas de Estudio, Laboratorios
Fuente: Tabla 10

Interpretación: En la Tabla 10 y la Figura 7 se observa que el 88.64% la mayoría determina "Totalmente de Acuerdo", el 11.36% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que es necesario implementar laboratorios sofisticados para la asignatura de ciberseguridad.

P8. ¿Desearías tener una biblioteca virtual en la Escuela Militar de Chorrillos para conocer la ciberseguridad?

Tabla 11
Herramientas de Estudio, Bibliotecas Virtuales

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	4	9.09%
Totalmente de Acuerdo	40	90.91%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

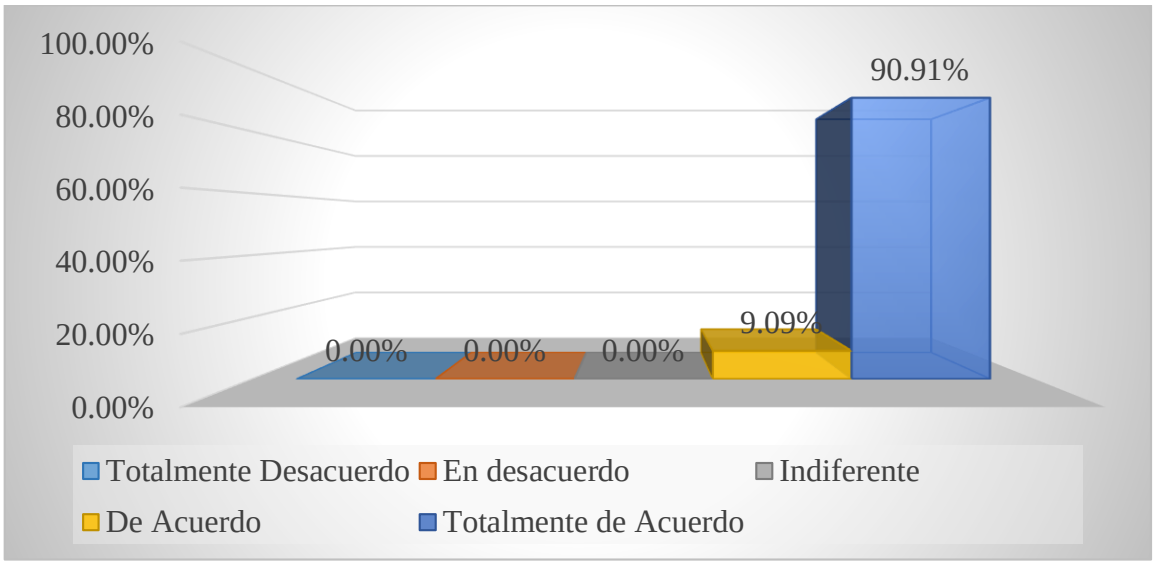


Figura 8. Herramientas de Estudio, Bibliotecas Virtuales
Fuente: Tabla 11

Interpretación: En la Tabla 11 y la Figura 8 se observa que el 90.91% la mayoría determina "Totalmente de Acuerdo", el 9.09% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que tener una biblioteca virtual en la Escuela Militar de Chorrillos para conocer la ciberseguridad

P9. ¿Consideras necesario implementar un aula virtual en la Escuela Militar de Chorrillos para llevar la asignatura de ciberseguridad?

Tabla 12
Herramientas de Estudio, Aulas Virtuales

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	3	6.82%
Totalmente de Acuerdo	41	93.18%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

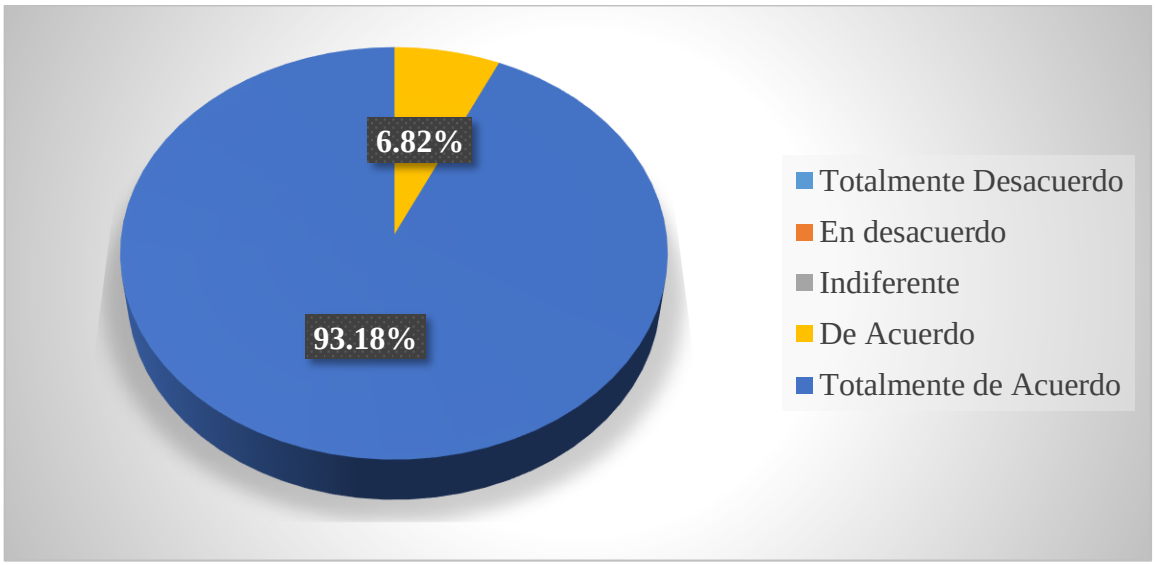


Figura 9. Herramientas de Estudio, Aulas Virtuales
Fuente: Tabla 12

Interpretación: En la Tabla 12 y la Figura 9 se observa que el 93.18% la mayoría determina "Totalmente de Acuerdo", el 6.82% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que es necesario implementar un aula virtual en la Escuela Militar de Chorrillos para llevar la asignatura de ciberseguridad.

Variable 2: Formación Profesional

P10. ¿Existen cursos civiles que brindan la Escuela Militar de Chorrillos para conocer la ciberseguridad?

Tabla 13
Instrucción, Cursos Civiles

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	3	6.82%
En desacuerdo	18	40.91%
Indiferente	3	6.82%
De Acuerdo	20	45.45%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

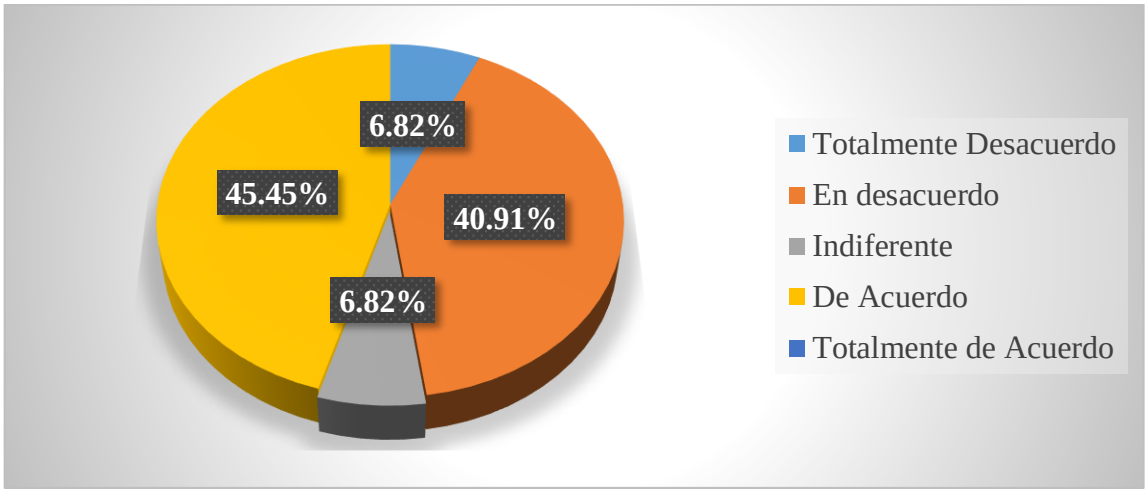


Figura 10. Instrucción, Cursos Civiles
Fuente: Tabla 13

Interpretación: En la Tabla 13 y la Figura 10 se observa que el 45.45% la mayoría determina "De Acuerdo", el 40.91% determina "En desacuerdo", el 6.82% determina "Totalmente Desacuerdo", el 6.82% determina "Indiferente" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que existen cursos civiles que brindan la Escuela Militar de Chorrillos para conocer la ciberseguridad.

P11. ¿Existen cursos militares ligadas a la ciberseguridad brindadas en la Escuela Militar de Chorrillos?

Tabla 14
Instrucción, Cursos Militares

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	39	88.64%
Indiferente	0	0.00%
De Acuerdo	5	11.36%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

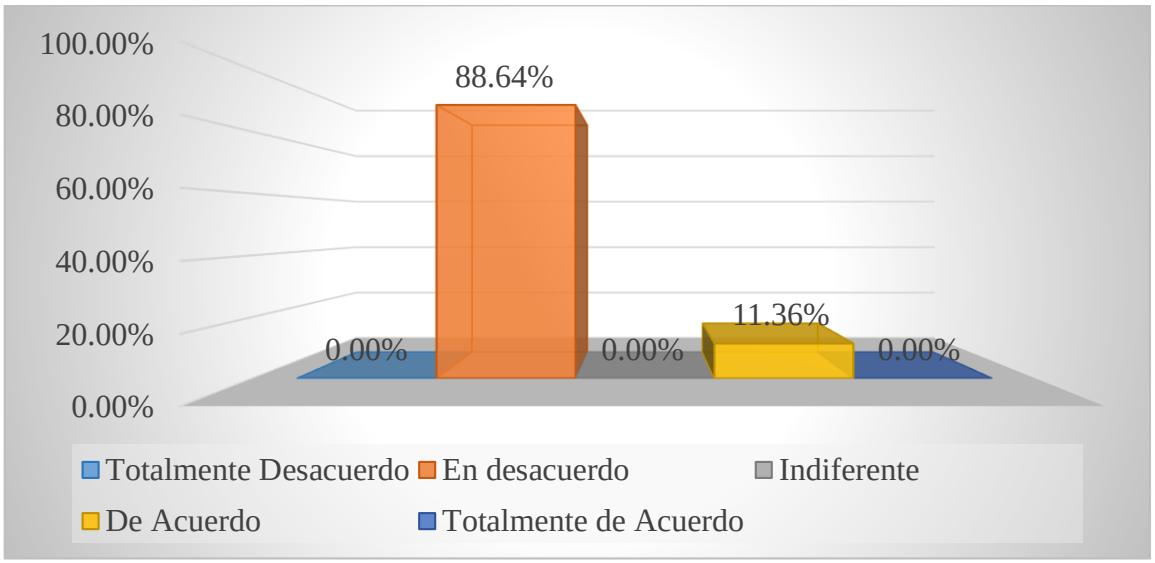


Figura 11. Instrucción, Cursos Militares
Fuente: Tabla 14

Interpretación: En la Tabla 14 y la Figura 11 se observa que el 88.64% la mayoría determina "En desacuerdo", el 11.36% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "Indiferente" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que no existen cursos militares ligadas a la ciberseguridad brindadas en la Escuela Militar de Chorrillos.

P12. ¿Es necesario los cursos de idioma para conocer la asignatura de ciberseguridad?

Tabla 15
Instrucción, Cursos de Idiomas

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	4	9.09%
Totalmente de Acuerdo	40	90.91%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

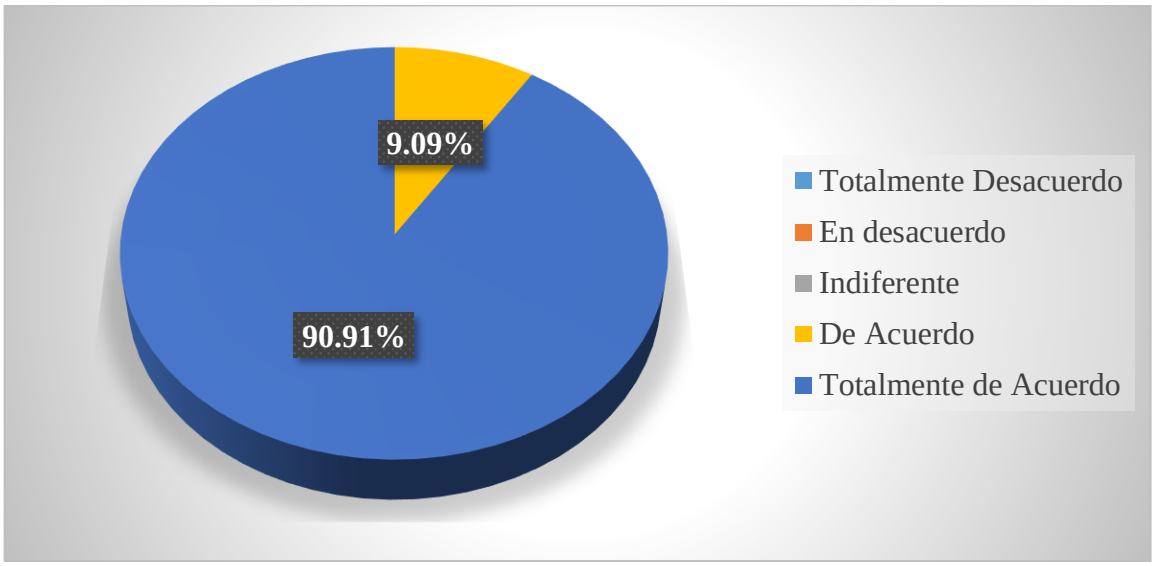


Figura 12. Instrucción, Cursos de Idiomas
Fuente: Tabla 15

Interpretación: En la Tabla 15 y la Figura 12 se observa que el 90.91% la mayoría determina "Totalmente de Acuerdo", el 9.09% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que es necesario los cursos de idioma para conocer la asignatura de ciberseguridad .

P13. ¿Es necesario considerar algunas habilidades o tics para conocer la ciberseguridad?

Tabla 16
Entrenamiento, Habilidades

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	41	93.18%
Totalmente de Acuerdo	3	6.82%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

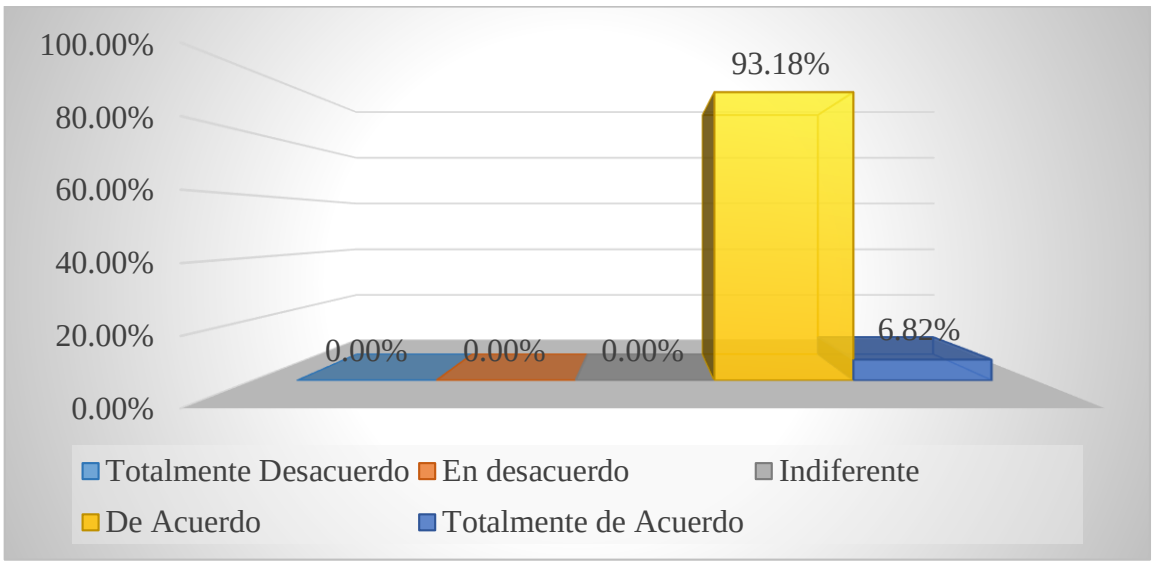


Figura 13. Entrenamiento, Habilidades
Fuente: Tabla 16

Interpretación: En la Tabla 16 y la Figura 13 se observa que el 93.18% la mayoría determina "De Acuerdo", el 6.82% determina "Totalmente de Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que es necesario considerar algunas habilidades o tics para conocer la ciberseguridad.

P14. ¿Consideras que existen destrezas en los cadetes de inteligencia para llevar la asignatura de ciberseguridad hacia una alta eficiencia?

Tabla 17
Entrenamiento, Destrezas

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	39	88.64%
Totalmente de Acuerdo	5	11.36%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

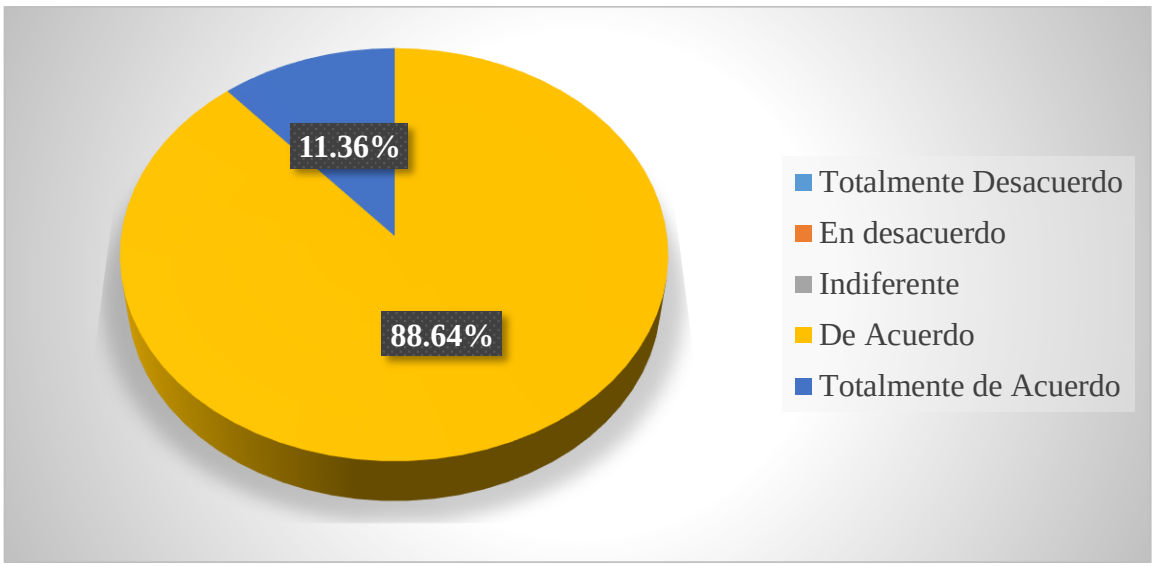


Figura 14. Entrenamiento, Destrezas
Fuente: Tabla 17

Interpretación: En la Tabla 17 y la Figura 14 se observa que el 88.64% la mayoría determina "De Acuerdo", el 11.36% determina "Totalmente de Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que existen destrezas en los cadetes de inteligencia para llevar la asignatura de ciberseguridad hacia una alta eficiencia.

P15. ¿Cuánta efectividad se cuenta en el entrenamiento para la formación profesional de los cadetes de inteligencia?

Tabla 18
Entrenamiento, Efectividad

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	0	0.00%
Indiferente	0	0.00%
De Acuerdo	39	88.64%
Totalmente de Acuerdo	5	11.36%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

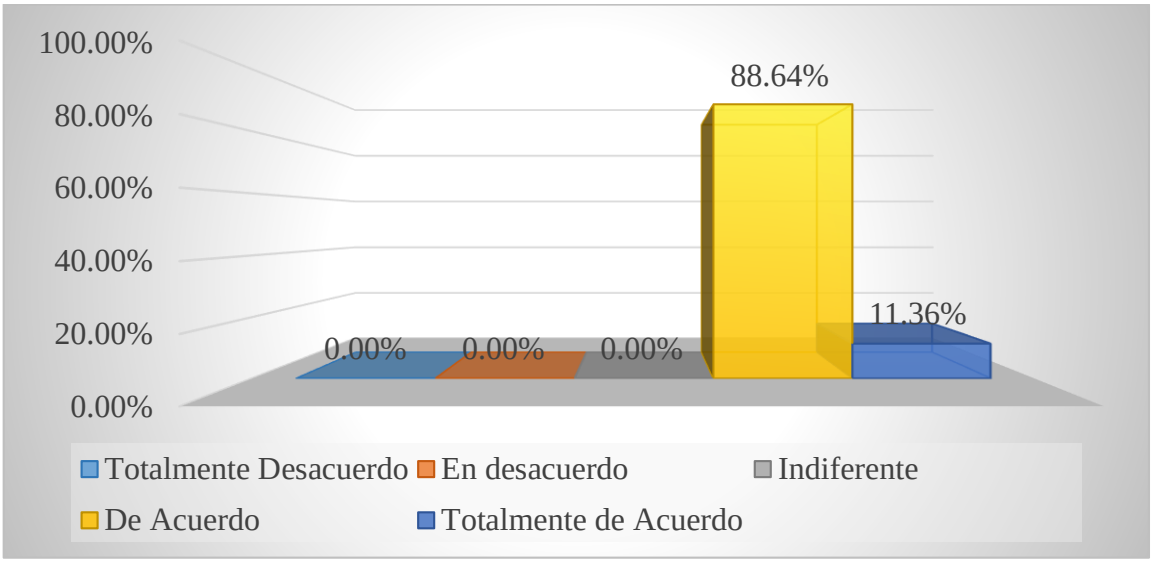


Figura 15. Entrenamiento, Efectividad
Fuente: Tabla 18

Interpretación: En la Tabla 18 y la Figura 15 se observa que el 88.64% la mayoría determina "De Acuerdo", el 11.36% determina "Totalmente de Acuerdo", el 0.00% determina "Totalmente Desacuerdo", el 0.00% determina "En desacuerdo" y el 0.00% determina "Indiferente", tomando en cuenta que la mayoría determinan que se cuenta con efectividad en el entrenamiento para la formación profesional de los cadetes de inteligencia.

P16. ¿Se cuenta con la velocidad de internet adecuada en la Escuela Militar de Chorrillos para la formación profesional de los cadetes?

Tabla 19
Herramientas Académicas, Internet

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0	0.00%
En desacuerdo	28	63.64%
Indiferente	8	18.18%
De Acuerdo	8	18.18%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

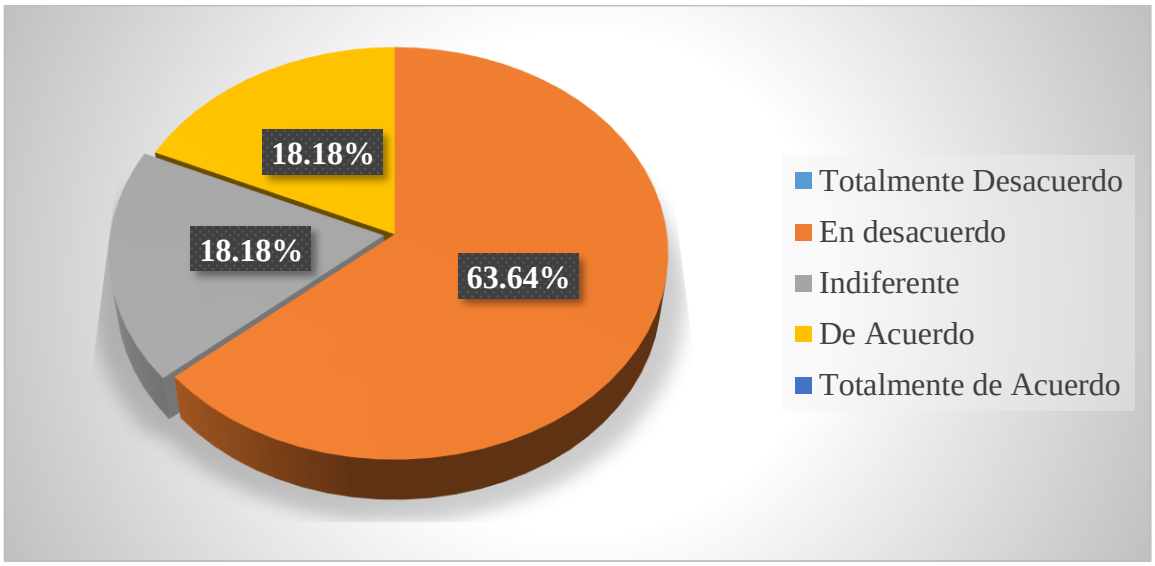


Figura 16. Herramientas Académicas, Internet
Fuente: Tabla 19

Interpretación: En la Tabla 19 y la Figura 16 se observa que el 63.64% la mayoría determina "En desacuerdo", el 18.18% determina "Indiferente", el 18.18% determina "De Acuerdo", el 0.00% determina "Totalmente Desacuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que se cuenta con la velocidad de internet adecuada en la Escuela Militar de Chorrillos para la formación profesional de los cadetes.

P17. ¿Se cuenta con una biblioteca moderna en la Escuela Militar de Chorrillos para la formación profesional de los cadetes de inteligencia?

Tabla 20
Herramientas Académicas, Biblioteca

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	5	11.36%
En desacuerdo	39	88.64%
Indiferente	0	0.00%
De Acuerdo	0	0.00%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

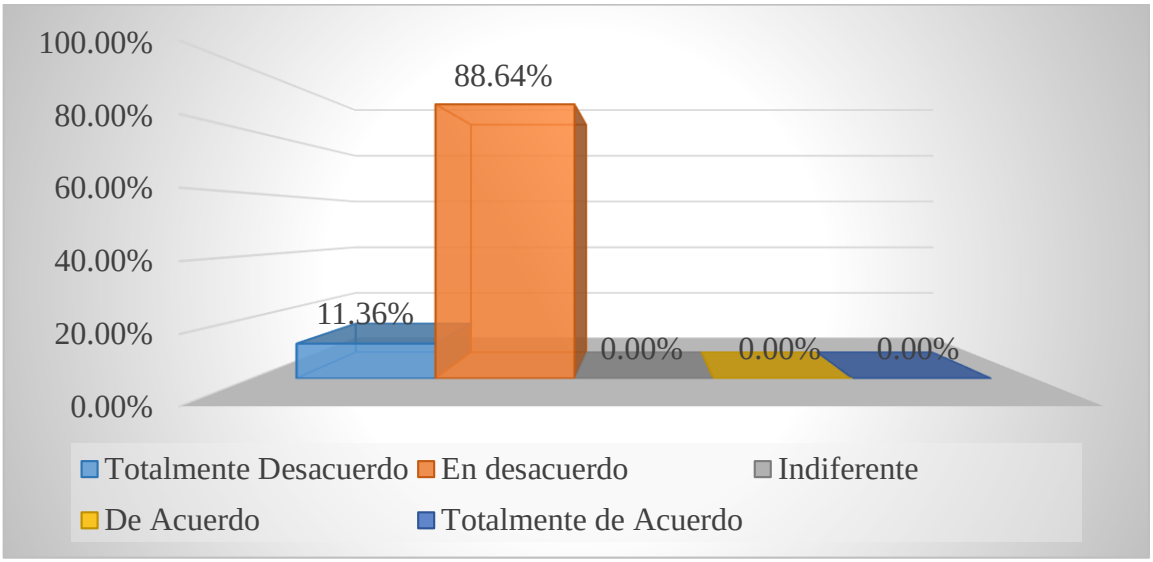


Figura 17. Herramientas Académicas, Biblioteca
Fuente: Tabla 20

Interpretación: En la Tabla 20 y la Figura 17 se observa que el 88.64% la mayoría determina "En desacuerdo", el 11.36% determina "Totalmente Desacuerdo", el 0.00% determina "Indiferente", el 0.00% determina "De Acuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que se cuenta con una biblioteca moderna en la Escuela Militar de Chorrillos para la formación profesional de los cadetes de inteligencia.

P18. ¿El SATAC cubre las necesidades de los cadetes de inteligencia para la formación profesional?

Tabla 21
Herramientas Académicas, SATAC

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	5	11.36%
En desacuerdo	39	88.64%
Indiferente	0	0.00%
De Acuerdo	0	0.00%
Totalmente de Acuerdo	0	0.00%
TOTAL	**44**	**100.00%**

Fuente: Cuestionario aplicada a los cadetes del Arma de Inteligencia de la EMCH "CFB" - 2019.

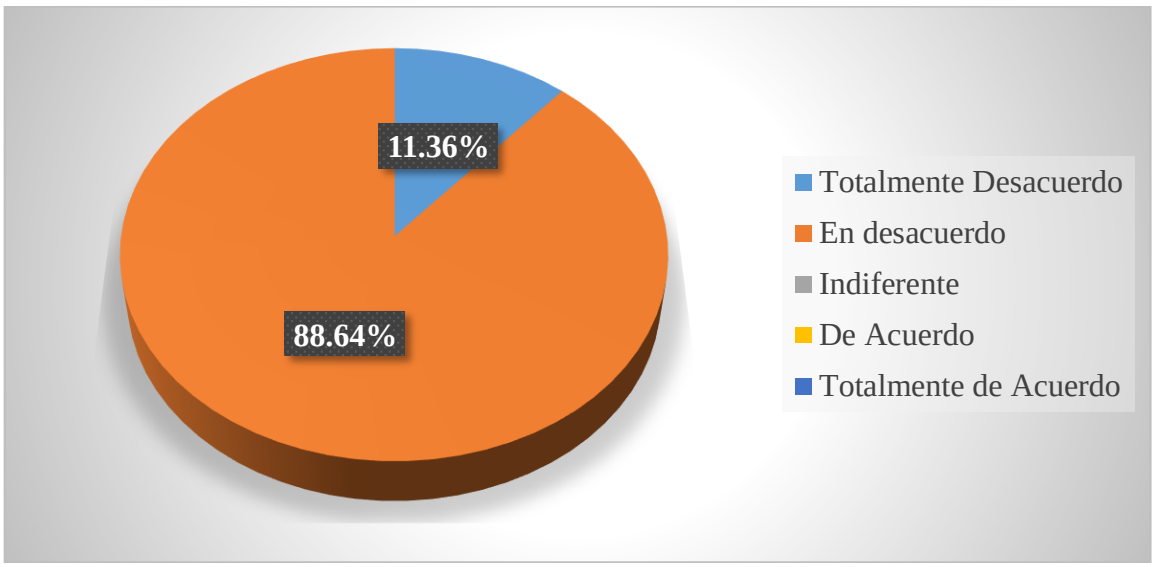


Figura 18. Herramientas Académicas, SATAC
Fuente: Tabla 21

Interpretación: En la Tabla 21 y la Figura 18 se observa que el 88.64% la mayoría determina "En desacuerdo", el 11.36% determina "Totalmente Desacuerdo", el 0.00% determina "Indiferente", el 0.00% determina "De Acuerdo" y el 0.00% determina "Totalmente de Acuerdo", tomando en cuenta que la mayoría determinan que el SATAC cubre las necesidades de los cadetes de inteligencia para la formación profesional.

4.2. Interpretación

La base de datos y el análisis, recodificación de variables y la determinación de la estadística descriptiva e inferencial. Para las pruebas de hipótesis hemos utilizados la prueba de independencia de Chi Cuadrado (X^2) con dos variables con categorías y el análisis exploratorio que sirve para comprobar si los promedios provienen de una distribución normal.

Para la determinación de la prueba de hipótesis, seguimos el criterio más aceptado por la comunidad científica, empleando un nivel de significancia ***α*** del 5% (0,05), y también hemos fijado un nivel de confianza del 95%.

Eso quiere decir que los resultados hallados se comparan con el nivel de significancia ***α*** 5% (0,05). Si el ***p*** Estadístico ***es menor que α,*** entonces se acepta la hipótesis nula. Si el ***p*** Estadístico ***es mayor que α,*** entonces se rechaza la hipótesis nula, y se acepta la hipótesis alternativa.

A. Cálculo de la CHI Cuadrada - Hipótesis General (HG)

HG - Existe una relación directa y significativa entre la Implementación de la asignatura de Ciberseguridad y la formación profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

HG_0 (Nula) – No existe una relación directa y significativa entre la Implementación de la asignatura de Ciberseguridad y la formación profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

- **De los Instrumentos de Medición**

  – Implementación de la Asignatura de Ciberseguridad

Tabla 22.
Instrumentos de Medición, HG V1

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	0.56	1.26%
En desacuerdo	17.56	39.90%
Indiferente	2.00	4.55%
De Acuerdo	6.11	13.89%
Totalmente de Acuerdo	17.78	40.40%
TOTAL	**44**	**100.00%**

  – Formación Profesional

Tabla 23.
Instrumentos de Medición, HG V2

Alternativa	fi	Porcentaje
Totalmente Desacuerdo	1.44	3.28%
En desacuerdo	18.11	41.16%
Indiferente	1.22	2.78%
De Acuerdo	17.33	39.39%
Totalmente de Acuerdo	5.89	13.38%
TOTAL	**44**	**100.00%**

Tabla 24.
Frecuencias observadas, HG

Fo	Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL
Implementación de la Asignatura de Ciberseguridad	1 - a1	18 - b1	2 - c1	6 - d1	18 - e1	**44**
Formación Profesional	1 - a2	18 - b2	1 - c2	17- d2	6 - e2	**44**
TOTAL	**2**	**36**	**3**	**23**	**24**	**88**

- **Aplicamos la fórmula para hallar las frecuencias esperadas:**

Fe: (total de frecuencias de la columna) (total de frecuencias de la fila)

Total general de la frecuencia

$$\text{fe - a\#} = \frac{2 * 44}{88} = 1.00$$

$$\text{fe - b\#} = \frac{36 * 44}{88} = 17.83$$

$$\text{fe - c\#} = \frac{3 * 44}{88} = 1.61$$

$$\text{fe - d\#} = \frac{23 * 44}{88} = 11.72$$

$$\text{fe - e\#} = \frac{24 * 44}{88} = 11.83$$

- **Aplicamos la fórmula:**

$$X^2 = \sum \frac{(fo - fe)^2}{fe}$$

fo= frecuencia observada
fe= frecuencia esperada

Tabla 25.
Aplicación de la fórmula, HG

Celda	fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2/fe$
F - a1 =	1	1.00	-0.44	0.20	0.197530864
F - b1 =	18	17.83	-0.28	0.08	0.004326757
F - c1 =	2	1.61	0.39	0.15	0.093869732
F - d1 =	6	11.72	-5.61	31.48	2.685887309
F - e1 =	18	11.83	5.94	35.34	2.986176317
F - a2 =	1	1.00	0.44	0.20	0.197530864
F - b2 =	18	17.83	0.28	0.08	0.004326757
F - c2 =	1	1.61	-0.39	0.15	0.093869732
F - d2 =	17	11.72	5.61	31.48	2.685887309
F - e2 =	6	11.83	-5.94	35.34	2.986176317
TOTAL				**X^2 =**	**11.93558196**

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

G = (r - 1) (c - 1)

G = (2 - 1) (5 - 1) = 4

Con un (4) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 9.488

Valor encontrado en el proceso: X^2 = 11.936

Tabla 26.
Validación de Chi Cuadrado HG

Chi Cuadrada HG		Implementación de la Asignatura de Ciberseguridad	Formación Profesional
Implementación de la Asignatura de Ciberseguridad	**Coeficiente de correlación**	9.488	11.936
	G. Lib.	.	4
	n	44	44
Formación Profesional	**Coeficiente de correlación**	11.936	9.488
	G. Lib.	4	.
	n	44	44

Interpretación: En relación a la hipótesis general, el valor calculado para la Chi cuadrada (11.936) es mayor que el valor que aparece en la tabla (9.488) para un nivel de confianza de 95% y un grado de libertad (4). Por lo que se adopta la decisión de rechazar la hipótesis general nula y se acepta la hipótesis general alterna.

B. Cálculo de la CHI Cuadrada - Hipótesis Específico 1 (HE1)

HE1 - Existe relación significativa entre la unidad de aprendizaje y la formación profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019.

$HE1_0$ (Nula) – No existe relación significativa entre la unidad de aprendizaje y la formación profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019.

- **De los Instrumentos de Medición**

  - V1 Dimensión 1: Unidad de Aprendizaje

Tabla 27.
Instrumentos de Medición, HE1 V1D1

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Doctrina de Ciberseguridad	0	0.00%	39	88.64%	5	11.36%	0	0.00%	0	0.00%	**44**
Tipos de Ciberataques	0	0.00%	10	22.73%	7	15.91%	27	61.36%	0	0.00%	**44**
Niveles de Amenazas	0	0.00%	36	81.82%	0	0.00%	8	18.18%	0	0.00%	**44**

  - V2 Dimensión 1: Instrucción

Tabla 28.
Instrumentos de Medición, HE1 V2D1

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Cursos Civiles	3	6.82%	18	40.91%	3	6.82%	20	45.45%	0	0.00%	**44**
Cursos Militares	0	0.00%	39	88.64%	0	0.00%	5	11.36%	0	0.00%	**44**
Cursos de Idiomas	0	0.00%	0	0.00%	0	0.00%	4	9.09%	40	90.91%	**44**

Tabla 29.
Frecuencias observadas, HE1

Frecuencia Observada (Fo)		Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL
Unidad de Aprendizaje	Doctrina de Ciberseguridad	0 - a1	39 - b1	5 - c1	0 -d1	0 - e1	**44**
	Tipos de Ciberataques	0 - a2	10 - b2	7 - c2	27 -d2	0 - e2	**44**
	Niveles de Amenazas	0 - a3	36 - b3	0 - c3	8 -d3	0 - e3	**44**
Instrucción	Cursos Civiles	3 - a4	18 - b4	3 - c4	20 -d4	0 - e4	**44**
	Cursos Militares	0 - a5	39 - b5	0 - c5	5 -d5	0 - e5	**44**
	Cursos de Idiomas	0 - a6	0 - b6	0 - c6	4 -d6	40 - e6	**44**
TOTAL		**3**	**142**	**15**	**64**	**40**	**264**

- **Aplicamos la fórmula para hallar las frecuencias esperadas:**

Fe: (total de frecuencias de la columna) (total de frecuencias de la fila)

Total general de la frecuencia

$$Fe - a\# = \frac{3 * 44}{264} = 0.5$$

$$Fe - b\# = \frac{142 * 44}{264} = 23.7$$

$$Fe - c\# = \frac{15 * 44}{264} = 2.5$$

$$Fe - d\# = \frac{64 * 44}{264} = 10.7$$

$$Fe - e\# = \frac{40 * 44}{264} = 6.7$$

- **Aplicamos la fórmula:**

$$X^2 = \sum \frac{(fo - fe)^2}{fe}$$

fo= frecuencia observada
fe= frecuencia esperada

Tabla 30.
Aplicación de la formula. HE1

Celda	fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2/fe$
F - a1 =	0	0.5	-0.5	0.25	0.5
F - b1 =	39	23.7	15.33333	235.11	9.9342723
F - c1 =	5	2.5	2.5	6.25	2.5
F - d1 =	0	10.7	-10.66667	113.78	10.66666667
F - e1 =	0	6.7	-6.666667	44.44	6.666666667
F - a2 =	0	0.5	-0.5	0.25	0.5
F - b2 =	10	23.7	-13.66667	186.78	7.892018779
F - c2 =	7	2.5	4.5	20.25	8.1
F - d2 =	27	10.7	16.33333	266.78	25.01041667
F - e2 =	0	6.7	-6.666667	44.44	6.666666667
F - a3 =	0	0.5	-0.5	0.25	0.5
F - b3 =	36	23.7	12.33333	152.11	6.427230047
F - c3 =	0	2.5	-2.5	6.25	2.5
F - d3 =	8	10.7	-2.666667	7.11	0.666666667
F - e3 =	0	6.7	-6.666667	44.44	6.666666667
F - a4 =	3	0.5	2.5	6.25	12.5
F - b4 =	18	23.7	-5.666667	32.11	1.356807512
F - c4 =	3	2.5	0.5	0.25	0.1
F - d4 =	20	10.7	9.333333	87.11	8.166666667
F - e4 =	0	6.7	-6.666667	44.44	6.666666667
F - a5 =	0	0.5	-0.5	0.25	0.5
F - b5 =	39	23.7	15.33333	235.11	9.9342723
F - c5 =	0	2.5	-2.5	6.25	2.5
F - d5 =	5	10.7	-5.666667	32.11	3.010416667
F - e5 =	0	6.7	-6.666667	44.44	6.666666667
F - a6 =	0	0.5	-0.5	0.25	0.5
F - b6 =	0	23.7	-23.66667	560.11	23.66666667
F - c6 =	0	2.5	-2.5	6.25	2.5
F - d6 =	4	10.7	-6.666667	44.44	4.166666667
F - e6 =	40	6.7	33.33333	1111.11	166.6666667
TOTAL				**X^2 =**	**344.0987676**

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

G = (r - 1) (c - 1)

G = (6 - 1) (5 - 1) = 20

Con un (20) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 31.410

Valor encontrado en el proceso: X^2 = 344.099

Tabla 31.
Validación de Chi Cuadrado HE1

Chi Cuadrada HE1		**Unidad de Aprendizaje**	**Instrucción**
Unidad de Aprendizaje	**Coeficiente de correlación**	31.410	344.099
	G. Lib.	.	20
	n	44	44
Instrucción	**Coeficiente de correlación**	344.099	31.410
	G. Lib.	20	.
	n	44	44

Interpretación: En relación a la primera de las hipótesis específicas, el valor calculado para la Chi cuadrada (344.099) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 1 nula y se acepta la hipótesis específica 1 alterna.

C. Cálculo de la CHI Cuadrada - Hipótesis Específico 2 (HE2)

HE2 - Existe relación significativa entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

HE2$_0$ (Nula) – NO existe relación significativa entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

- **De los Instrumentos de Medición**
  - V1 Dimensión 2: Prácticas Especializadas

Tabla 32.
Instrumentos de Medición, HE2 V1D2

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Diseñar Medidas de Seguridad	3	6.82%	37	84.09%	0	0.00%	4	9.09%	0	0.00%	**44**
Detección de Amenazas	0	0.00%	0	0.00%	0	0.00%	4	9.09%	40	90.91%	**44**
Contrarrestar Amenazas	2	4.55%	36	81.82%	6	13.64%	0	0.00%	0	0.00%	**44**

  - V2 Dimensión 2: Entrenamiento

Tabla 33.
Instrumentos de Medición, HE2 V2D2

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Habilidades	0	0.00%	0	0.00%	0	0.00%	41	93.18%	3	6.82%	**44**
Destrezas	0	0.00%	0	0.00%	0	0.00%	39	88.64%	5	11.36%	**44**
Efectividad	0	0.00%	0	0.00%	0	0.00%	39	88.64%	5	11.36%	**44**

Tabla 34.
Frecuencias observadas, HE2

Frecuencia Observada (Fo)		Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL
Prácticas Especializadas	Diseñar Medidas de Seguridad	3 - a1	37 - b1	0 - c1	4 - d1	0 - e1	**44**
	Detección de Amenazas	0 - a2	0 - b2	0 - c2	4 - d2	40 - e2	**44**
	Contrarrestar Amenazas	2 - a3	36 - b3	6 - c3	0 - d3	0 - e3	**44**
Entrenamiento	Habilidades	0 - a4	0 - b4	0 - c4	41 - d4	3 - e4	**44**
	Destrezas	0 - a5	0 - b5	0 - c5	39 - d5	5 - e5	**44**
	Efectividad	0 - a6	0 - b6	0 - c6	39 - d6	5 - e6	**44**
TOTAL		**5**	**73**	**6**	**127**	**5**	**264**

- **Aplicamos la fórmula para hallar las frecuencias esperadas:**

Fe: (total de frecuencias de la columna) (total de frecuencias de la fila)

Total general de la frecuencia

$$\text{Fe - a\#} = \frac{5 * 44}{264} = 0.8$$

$$\text{Fe - b\#} = \frac{73 * 44}{264} = 12.2$$

$$\text{Fe - c\#} = \frac{6 * 44}{264} = 1.0$$

$$\text{Fe - d\#} = \frac{127 * 44}{264} = 21.2$$

$$\text{Fe - e\#} = \frac{53 * 44}{264} = 8.8$$

- **Aplicamos la fórmula:**

$$X^2 = \sum \frac{(fo - fe)^2}{fe}$$

fo= frecuencia observada
fe= frecuencia esperada

Tabla 35.
Aplicación de la fórmula, HE2

Celda	fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2/fe$
F - a1 =	3	0.8	2.166667	4.69	5.633333333
F - b1 =	37	12.2	24.83333	616.69	50.68721461
F - c1 =	0	1.0	-1	1.00	1
F - d1 =	4	21.2	-17.16667	294.69	13.92257218
F - e1 =	0	8.8	-8.833333	78.03	8.833333333
F - a2 =	0	0.8	-0.833333	0.69	0.833333333
F - b2 =	0	12.2	-12.16667	148.03	12.16666667
F - c2 =	0	1.0	-1	1.00	1
F - d2 =	4	21.2	-17.16667	294.69	13.92257218
F - e2 =	40	8.8	31.16667	971.36	109.9654088
F - a3 =	2	0.8	1.166667	1.36	1.633333333
F - b3 =	36	12.2	23.83333	568.03	46.68721461
F - c3 =	6	1.0	5	25.00	25
F - d3 =	0	21.2	-21.16667	448.03	21.16666667
F - e3 =	0	8.8	-8.833333	78.03	8.833333333
F - a4 =	0	0.8	-0.833333	0.69	0.833333333
F - b4 =	0	12.2	-12.16667	148.03	12.16666667
F - c4 =	0	1.0	-1	1.00	1
F - d4 =	41	21.2	19.83333	393.36	18.5839895
F - e4 =	3	8.8	-5.833333	34.03	3.852201258
F - a5 =	0	0.8	-0.833333	0.69	0.833333333
F - b5 =	0	12.2	-12.16667	148.03	12.16666667
F - c5 =	0	1.0	-1	1.00	1
F - d5 =	39	21.2	17.83333	318.03	15.02493438
F - e5 =	5	8.8	-3.833333	14.69	1.663522013
F - a6 =	0	0.8	-0.833333	0.69	0.833333333
F - b6 =	0	12.2	-12.16667	148.03	12.16666667
F - c6 =	0	1.0	-1	1.00	1
F - d6 =	39	21.2	17.83333	318.03	15.02493438
F - e6 =	5	8.8	-3.833333	14.69	1.663522013
TOTAL				**X^2 =**	**419.0980859**

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

G = (r - 1) (c - 1)

G = (6 - 1) (5 - 1) = 20

Con un (20) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 31.410

Valor encontrado en el proceso: X^2 = 419.098

Tabla 36.
Validación de Chi Cuadrado HE2

Chi Cuadrada HE2		**Prácticas Especializadas**	**Entrenamiento**
Prácticas Especializadas	**Coeficiente de correlación**	31.410	419.098
	G. Lib.	.	20
	n	44	44
Entrenamiento	**Coeficiente de correlación**	419.098	31.410
	G. Lib.	20	.
	n	44	44

Interpretación: En relación a la segunda de las hipótesis específicas, Asimismo, el valor calculado para la Chi cuadrada (419.098) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 2 nula y se acepta la hipótesis específica 2 alterna.

D. Cálculo de la CHI Cuadrada - Hipótesis Específico 3 (HE3)

HE3 - Existe relación significativa entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

HE3$_0$ (Nula) – NO existe relación significativa entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019.

- **De los Instrumentos de Medición**
  - V1 Dimensión 3: Herramientas de Estudio

Tabla 37.
Instrumentos de Medición, HE3 V1D3

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Laboratorios	0	0.00%	0	0.00%	0	0.00%	5	11.36%	39	88.64%	**44**
Bibliotecas Virtuales	0	0.00%	0	0.00%	0	0.00%	4	9.09%	40	90.91%	**44**
Aulas Virtuales	0	0.00%	0	0.00%	0	0.00%	3	6.82%	41	93.18%	**44**

  - V2 Dimensión 3: Herramientas Académicas

Tabla 38.
Instrumentos de Medición, HE3 V2D3

fi	Totalmente Desacuerdo		En desacuerdo		Indiferente		De Acuerdo		Totalmente de Acuerdo		TOTAL
Internet	0	0.00%	28	63.64%	8	18.18%	8	18.18%	0	0.00%	**44**
Biblioteca	5	11.36%	39	88.64%	0	0.00%	0	0.00%	0	0.00%	**44**
SATAC	5	11.36%	39	88.64%	0	0.00%	0	0.00%	0	0.00%	**44**

Tabla 39.
Frecuencias observadas, HE3

Frecuencia Observada (Fo)		Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL
Herramientas de Estudio	Laboratorios	0 - a1	0 - 1	0 - c1	5 -d1	39 - e1	**44**
	Bibliotecas Virtuales	0 - a2	0 - b2	0 - c2	4 -d2	40 - e2	**44**
	Aulas Virtuales	0 - a3	0 - b3	0 - c3	3 -d3	41 - e3	**44**
Herramientas Académicas	Internet	0 - a4	28 - b4	8 - c4	8 -d4	0 - e4	**44**
	Biblioteca	5 - a5	39 - b5	0 - c5	0 -d5	0 - e5	**44**
	SATAC	5 - a6	39 - b6	0 - c6	0 -d6	0 - e6	**44**
TOTAL		**10**	**106**	**8**	**20**	**120**	**264**

- **Aplicamos la fórmula para hallar las frecuencias esperadas:**

Fe: (total de frecuencias de la columna) (total de frecuencias de la fila)

Total general de la frecuencia

$$Fe - a\# = \frac{10 * 44}{264} = 1.7$$

$$Fe - b\# = \frac{106 * 44}{264} = 17.7$$

$$Fe - c\# = \frac{8 * 44}{264} = 1.3$$

$$Fe - d\# = \frac{20 * 44}{264} = 3.3$$

$$Fe - e\# = \frac{120 * 44}{264} = 20.0$$

- **Aplicamos la fórmula:**

$$X^2 = \sum \frac{(fo - fe)^2}{fe}$$

fo= frecuencia observada
fe= frecuencia esperada

Tabla 40.
Aplicación de la fórmula, HE3

Celda	fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2/fe$
F - a1 =	0	1.7	-1.666667	2.78	1.666666667
F - b1 =	0	17.7	-17.66667	312.11	17.66666667
F - c1 =	0	1.3	-1.333333	1.78	1.333333333
F - d1 =	5	3.3	1.666667	2.78	0.833333333
F - e1 =	39	20.0	19	361.00	18.05
F - a2 =	0	1.7	-1.666667	2.78	1.666666667
F - b2 =	0	17.7	-17.66667	312.11	17.66666667
F - c2 =	0	1.3	-1.333333	1.78	1.333333333
F - d2 =	4	3.3	0.666667	0.44	0.133333333
F - e2 =	40	20.0	20	400.00	20
F - a3 =	0	1.7	-1.666667	2.78	1.666666667
F - b3 =	0	17.7	-17.66667	312.11	17.66666667
F - c3 =	0	1.3	-1.333333	1.78	1.333333333
F - d3 =	3	3.3	-0.333333	0.11	0.033333333
F - e3 =	41	20.0	21	441.00	22.05
F - a4 =	0	1.7	-1.666667	2.78	1.666666667
F - b4 =	28	17.7	10.33333	106.78	6.044025157
F - c4 =	8	1.3	6.666667	44.44	33.33333333
F - d4 =	8	3.3	4.666667	21.78	6.533333333
F - e4 =	0	20.0	-20	400.00	20
F - a5 =	5	1.7	3.333333	11.11	6.666666667
F - b5 =	39	17.7	21.33333	455.11	25.76100629
F - c5 =	0	1.3	-1.333333	1.78	1.333333333
F - d5 =	0	3.3	-3.333333	11.11	3.333333333
F - e5 =	0	20.0	-20	400.00	20
F - a6 =	5	1.7	3.333333	11.11	6.666666667
F - b6 =	39	17.7	21.33333	455.11	25.76100629
F - c6 =	0	1.3	-1.333333	1.78	1.333333333
F - d6 =	0	3.3	-3.333333	11.11	3.333333333
F - e6 =	0	20.0	-20	400.00	20
TOTAL				**X^2 =**	**304.8660377**

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

G = (r - 1) (c - 1)

G = (6 - 1) (5 - 1) = 20

Con un (20) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 31.410

Valor encontrado en el proceso: $X^2 = 304.866$

Tabla 41.
Validación de Chi Cuadrado HE3

Chi Cuadrada HE3		**Herramientas de Estudio**	**Herramientas Académicas**
Herramientas de Estudio	**Coeficiente de correlación**	31.410	304.866
	G. Lib.	.	20
	n	44	44
Herramientas Académicas	**Coeficiente de correlación**	304.866	31.410
	G. Lib.	20	.
	n	44	44

Interpretación: En relación a la tercera de las hipótesis específicas, Asimismo, el valor calculado para la Chi cuadrada (304.866) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 3 nula y se acepta la hipótesis específica 3 alterna.

4.3. Discusión

En lo relacionado a nuestras hipótesis podemos extraer lo siguiente:

En relación a la hipótesis general, el valor calculado para la Chi cuadrada (11.936) es mayor que el valor que aparece en la tabla (9.488) para un nivel de confianza de 95% y un grado de libertad (4). Por lo que se adopta la decisión de rechazar la hipótesis general nula y se acepta la hipótesis general alterna. Esto quiere decir que existe una relación directa y significativa entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019 ; Validándola, en tal sentido, Anchundia (2017), quien determina que la universidad está llamada a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, apoyada en una cultura de seguridad y defensa, dentro de la universidad y desde la universidad a la sociedad.

Asimismo, en relación a la primera de las hipótesis específicas, el valor calculado para la Chi cuadrada (344.099) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 1 nula y se acepta la hipótesis específica 1 alterna. Esto quiere decir que existe relación significativa entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019 ; Validándola, en tal sentido, Aguirre

(2017), quien determina que es necesaria la creación de una estrategia nacional de ciberseguridad, documento a través del cual los países alinean sus objetivos a nivel nacional en la materia y que abarca también la identificación y protección de las infraestructuras críticas de información utilizadas para brindar servicios esenciales a la población.

Como también, en relación a la segunda de las hipótesis específicas, el valor calculado para la Chi cuadrada (419.098) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 2 nula y se acepta la hipótesis específica 2 alterna. Esto quiere decir que existe relación significativa entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019 ; Validándola, en tal sentido, Taipe (2018), quien determina que los encuestados manifiestan que el realizar una Auditoria de seguridad informática no tiene implicancia en la Ciberseguridad, lo que demuestra que el nivel de conocimiento del personal de Informática, las normas y políticas no tiene un buen nivel de Ciberseguridad.

Por último, en relación a la tercera de las hipótesis específicas, el valor calculado para la Chi cuadrada (304.866) es mayor que el valor que aparece en la tabla (31.410) para un nivel de confianza de 95% y un grado de libertad (20). Por lo que se adopta la decisión de rechazar la hipótesis específica 3 nula y se acepta la hipótesis específica 3 alterna. Esto quiere decir que existe relación significativa entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de

Chorrillos “Coronel Francisco Bolognesi” 2019 Validándola, en tal sentido, Aguirre (2017), quien determina que se deben reforzar para tener un alto grado de madurez en ciberseguridad a nivel nacional. La tecnología está avanzando exponencialmente y las organizaciones y los usuarios están adoptando estas tecnologías, sin conocer los riesgos que conllevan. La generación de una cultura de ciberseguridad es un paso ineludible para el progreso de una sociedad moderna.

CONCLUSIONES

1. Teniendo en consideración la Hipótesis General que señala: Existe una relación directa y significativa entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019; se ha podido establecer un resultado de 54.29% y 52.78% respectivamente. Se concluye que es muy regular la formación que se le brinda al cadete del Arma de Inteligencia, notando la falta de asignatura de ciberseguridad.

2. Teniendo en consideración la Hipótesis Especifica 1 que señala: Existe relación significativa entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019; en un promedio aritmético obtenido por los resultados de cada indicador de un 26.52% y 52.27% respectivamente. Concluyendo así que no existe doctrina en ciberseguridad, lo cadetes tienen los conocimientos necesarios sobre los ciberataques y teniendo un bajo nivel de conocimiento en como contrarrestar las posibles amenazas, en relación al promedio que se obtiene de la instrucción que se lleva actualmente.

3. Teniendo en consideración la Hipótesis Especifica 2 que señala: Existe relación significativa entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019; en un promedio aritmético obtenido por los resultados de cada indicador de un 36.36% y 100.00% respectivamente. Las prácticas especializadas que se llevan actualmente tienen un bajo

conocimiento en diseñar medidas de seguridad, se necesita formación en como detener una posible amenaza y no existe alguna experiencia de como contrarrestarlo.

4. Teniendo en consideración la Hipótesis Especifica 3 que señala: Existe relación significativa entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019; en un promedio aritmético obtenido por los resultados de cada indicador de un 100.00% y 6.06% respectivamente. Se puede demostrar que efectivamente se necesitas las herramientas de estudio como la falta de laboratorios, bibliotecas y aulas virtuales como parte de su formación profesional del cadete del Arma de Inteligencia.

RECOMENDACIONES

1. Recomendar a la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” a implementar esta asignatura de ciberseguridad como parte de la formación profesional para el cadete del Arma de Inteligencia, como nueva unidad de aprendizaje, prácticas especializadas en el extranjero y herramientas de estudio que se puedan integrar tecnologías de última generación.

2. Recomendar para crear nuevas unidades de aprendizaje congruentes para el profesionalismo del oficial egresado de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, y así poder proteger los intereses nacionales. Debido que otros países han creado estructuras para realizar acciones cibernéticas y así poder capacitar a su personal por medio de escuelas de Ciberseguridad.

3. Recomendar tener prácticas especializadas por medio de alianzas internacionales donde motive los intereses propios de cada cadete como parte de su formación profesional y de esta manera estar mejor capacitado en temas tecnológicos respecto a la Ciberseguridad.

4. Recomendar la integración hacia la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” de nuevas herramientas de estudio permitiendo facilitar el desarrollar de la asignatura de Ciberseguridad y poder mejorar el aprovechamiento de nuevas tecnologías generadas cada año.

REFERENCIAS

Aguirre, A. A. (2017). *Tesis de Maestría: "Ciberseguridad en Infraestructuras Críticas de Información".* Buenos Aires, Argentina: Universidad de Buenos Aires.

Anchundia, C. E. (2017). *Tesis de Doctorado: "Ciberseguridad en los sistemas de información de las universidades".* Cuenca, Ecuador: Universidad de Cuenca.

Belluomo, R. (02 de Agosto de 2017). *Consejos para implementar herramientas de ciberseguridad empresarial*. Obtenido de https://www.corporateit.cl/index.php/2017/08/02/consejos-para-implementar-herramientas-de-ciberseguridad-empresarial/

Calero, J. L. (2002). Investigación cualitativa y cuantitativa. Problemas no resueltos en los debates actuales. Rev. Cubana Endocrinol 2000.

CERO. (2019). *Lo que debe saber de ciberseguridad* . Obtenido de https://www.riesgoscero.com/academia/especiales/todo-lo-que-debe-saber-sobre-ciberseguridad

García, R. (17 de Octubre de 2017). *La colaboración, clave para el éxito en ciberseguridad*. Obtenido de https://empresas.blogthinkbig.com/la-colaboracion-clave-para-el-exito-en-ciberseguridad/

Granados, O. (18 de mayo de 2014). *Las herramientas académicas actuales inhiben el aprendizaje*. Obtenido de https://www.liderempresarial.com/las-herramientas-academicas-actuales-inhiben-el-aprendizaje/

Guglielmetti, M. (26 de Junio de 2008). *Internet*. Obtenido de Definición ABC: https://www.definicionabc.com/tecnologia/internet.php

Hernández, E. A. (1998). *Modalidad de la Investigación Científica.* D.F. México: MC Craw.

Hernández, Fernández, & Baptista. (2003). *Metodología de la Investigación.* México: Mc Graw Hill.

INET. (2018). *Formación Profesional*. Obtenido de Instituo Nacional de Educación Tecnológica: http://www.inet.edu.ar/index.php/niveles-educativos/formacion-profesional/

Jave, W. (2004). *Diccionario de Terminos Militares.* Lima, Perú: DEDOC / COINDE 50010 .

OBS. (2019). *Máster en Ciberseguridad: ¿qué aprendemos y por qué es recomendable hacerlo?* Obtenido de https://www.obs-edu.com/int/blog-investigacion/sistemas/master-en-ciberseguridad-que-aprendemos-y-por-que-es-recomendable-hacerlo

Pérez, J., & Merino, M. (2008). *DEFINICIÓN DE ENTRENAMIENTO*. Obtenido de https://definicion.de/entrenamiento/

Pérez, J., & Merino, M. (2008). *Definición de habilidad*. Obtenido de Definicion.de: https://definicion.de/habilidad/

Pérez, J., & Merino, M. (2012). *Definición de instrucción militar* . Obtenido de Definicion.de: https://definicion.de/instruccion-militar/

Pérez, J., & Merino, M. (2017). *Definición de aula virtual*. Obtenido de Definicion.de: https://definicion.de/aula-virtual/

Taipe, D. I. (2018). *Tesis de Maestría: "La Auditoría de Seguridad Informática y su Relación en la Ciberseguridad de la Fuerza Aérea del Perú Año 2017".* Lima, Perú: Escuela Superior de Guerra Aérea.

Ucha, F. (27 de Julio de 2009). *Biblioteca*. Obtenido de Definición ABC: https://www.definicionabc.com/general/biblioteca.php

Ucha, F. (14 de Mayo de 2010). *Destreza*. Obtenido de Definición ABC: https://www.definicionabc.com/deporte/destreza.php

Zorrilla. (1993). la investigación se clasifica en cuatro tipos: básica, aplicada, documental, de campo o mixta.

ANEXOS

Anexo 01: Base de datos

V1	Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL	Totalmente Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo	TOTAL (%)
1	0	39	5	0	0	**44**	0.00%	88.64%	11.36%	0.00%	0.00%	**100.00%**
2	0	10	7	27	0	**44**	0.00%	22.73%	15.91%	61.36%	0.00%	**100.00%**
3	0	36	0	8	0	**44**	0.00%	81.82%	0.00%	18.18%	0.00%	**100.00%**
4	3	37	0	4	0	**44**	6.82%	84.09%	0.00%	9.09%	0.00%	**100.00%**
5	0	0	0	4	40	**44**	0.00%	0.00%	0.00%	9.09%	90.91%	**100.00%**
6	2	36	6	0	0	**44**	4.55%	81.82%	13.64%	0.00%	0.00%	**100.00%**
7	0	0	0	5	39	**44**	0.00%	0.00%	0.00%	11.36%	88.64%	**100.00%**
8	0	0	0	4	40	**44**	0.00%	0.00%	0.00%	9.09%	90.91%	**100.00%**
9	0	0	0	3	41	**44**	0.00%	0.00%	0.00%	6.82%	93.18%	**100.00%**
V2	**Totalmente Desacuerdo**	**En desacuerdo**	**Indiferente**	**De Acuerdo**	**Totalmente de Acuerdo**	**TOTAL**	**Totalmente Desacuerdo**	**En desacuerdo**	**Indiferente**	**De Acuerdo**	**Totalmente de Acuerdo**	**TOTAL (%)**
1	3	18	3	20	0	**44**	6.82%	40.91%	6.82%	45.45%	0.00%	**100.00%**
2	0	39	0	5	0	**44**	0.00%	88.64%	0.00%	11.36%	0.00%	**100.00%**
3	0	0	0	4	40	**44**	0.00%	0.00%	0.00%	9.09%	90.91%	**100.00%**
4	0	0	0	41	3	**44**	0.00%	0.00%	0.00%	93.18%	6.82%	**100.00%**
5	0	0	0	39	5	**44**	0.00%	0.00%	0.00%	88.64%	11.36%	**100.00%**
6	0	0	0	39	5	**44**	0.00%	0.00%	0.00%	88.64%	11.36%	**100.00%**
7	0	28	8	8	0	**44**	0.00%	63.64%	18.18%	18.18%	0.00%	**100.00%**
8	5	39	0	0	0	**44**	11.36%	88.64%	0.00%	0.00%	0.00%	**100.00%**
9	5	39	0	0	0	**44**	11.36%	88.64%	0.00%	0.00%	0.00%	**100.00%**

Anexo 02: Matriz de consistencia

Título: Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2019.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	DISEÑO METODOLÓGICO E INSTRUMENTOS
Problema General ¿Cuál es la relación que existe entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019? **Problema Especifico 1** ¿Cuál es la relación que existe entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019? **Problema Especifico 2** ¿Cuál es la relación que existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019? **Problema Especifico 3** ¿Cuál es la relación que existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019?	**Objetivo General** Determinar la relación que existe entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Objetivo Especifico 1** Determinar la relación que existe entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Objetivo Especifico 2** Determinar la relación que existe entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Objetivo Especifico 3** Determinar la relación que existe entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019.	**Hipótesis General** Existe relación directa y significativa entre la Implementación de la Asignatura de Ciberseguridad y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Hipótesis Especifico 1** Existe relación directa y significativa entre la Unidad de Aprendizaje y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Hipótesis Especifico 2** Existe relación directa y significativa entre las Prácticas Especializadas y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019. **Hipótesis Especifico 3** Existe relación directa y significativa entre las Herramientas de Estudio y la Formación Profesional de los cadetes del Arma de Inteligencia de la EMCH "CFB" 2019.	**Variable 1** Implementación de la Asignatura de Ciberseguridad	Unidad de Aprendizaje	• Doctrina de Ciberseguridad • Tipos de Ciberataques • Niveles de Amenazas	**Tipo investigación** Aplicada Descriptivo-correlacional **Diseño de investigación** No experimental transversal **Enfoque de investigación** Cuantitativo **Técnica** Encuesta **Instrumentos** Cuestionario **Población** 49 Cadetes del Arma de Inteligencia de la EMCH "CFB" **Muestra** 44 Cadetes del Arma de Inteligencia de la EMCH "CFB" **Métodos de Análisis de Datos** Estadística Ji o Chi Cuadrada
				Prácticas Especializadas	• Diseñar Medidas de Seguridad • Detección de Amenazas • Contrarrestar Amenazas	
				Herramientas de Estudio	• Laboratorios • Bibliotecas Virtuales • Aulas Virtuales	
			Variable 2 Formación Profesional	Instrucción	• Cursos Civiles • Cursos Militares • Cursos de Idiomas	
				Entrenamiento	• Habilidades • Destrezas • Efectividad	
				Herramientas Académicas	• Internet • Biblioteca • SATAC	

Anexo 03: Instrumentos de recolección de datos

ESCUELA MILITAR DE CHORRILLOS "CFB"

IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" 2019

Nota: Se agradece anticipadamente la colaboración de los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "CFB" - 2019, que nos colaboraron amablemente.

RESPONDA A LAS SIGUIENTES PREGUNTAS SEGÚN SU CRITERIO, MARQUE CON UNA "X" EN LA ALTERNATIVA QUE LE CORRESPONDE:

ESCALA DE LIKERT							
A Totalmente de Acuerdo		**B De Acuerdo**		**C Indeciso**		**D Desacuerdo**	**E Totalmente Desacuerdo**
N°	**IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD**						
1	¿Existe alguna doctrina de Ciberseguridad implementada en la Escuela Militar de Chorrillos?	**A**	**B**	**C**	**D**	**E**	
2	¿Conoces algún tipo de ciberataque que se podría implementar en la asignatura de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
3	¿Tienes conocimiento de los niveles de amenaza que podría existir en la asignatura de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
4	¿Podrías diseñar tu propia medida de seguridad en línea, para tus trabajos académicos?	**A**	**B**	**C**	**D**	**E**	
5	¿Desearías tener cursos especializados para cualquier detección de amenazas cibernéticas?	**A**	**B**	**C**	**D**	**E**	
6	¿Tienes conocimiento de cómo contrarrestar las amenazas de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
7	¿Consideras necesario implementar laboratorios sofisticados para la asignatura de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	

ESCALA DE LIKERT							
A Totalmente de Acuerdo	**B De Acuerdo**	**C Indeciso**	**D Desacuerdo**	**E Totalmente Desacuerdo**			
8	¿Desearías tener una biblioteca virtual en la Escuela Militar de Chorrillos para conocer la Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
9	¿Consideras necesario implementar un aula virtual en la Escuela Militar de Chorrillos para llevar la asignatura de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
N°	**FORMACIÓN PROFESIONAL**						
1	¿Existen cursos civiles que brindan la Escuela Militar de Chorrillos para conocer la Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
2	¿Existen cursos militares ligadas a la Ciberseguridad brindadas en la Escuela Militar de Chorrillos?	**A**	**B**	**C**	**D**	**E**	
3	¿Es necesario los cursos de idioma para conocer la asignatura de Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
4	¿Es necesario considerar algunas habilidades o tics para conocer la Ciberseguridad?	**A**	**B**	**C**	**D**	**E**	
5	¿Consideras que existen destrezas en los cadetes de inteligencia para llevar la asignatura de Ciberseguridad hacia una alta eficiencia?	**A**	**B**	**C**	**D**	**E**	
6	¿Cuánta efectividad se cuenta en el entrenamiento para la formación profesional de los cadetes de Inteligencia?	**A**	**B**	**C**	**D**	**E**	
7	¿Se cuenta con la velocidad de internet adecuada en la Escuela Militar de Chorrillos para la formación profesional de los cadetes?	**A**	**B**	**C**	**D**	**E**	
8	¿Se cuenta con una biblioteca moderna en la Escuela Militar de Chorrillos para la formación profesional de los cadetes de Inteligencia?	**A**	**B**	**C**	**D**	**E**	
9	¿La Sala Táctica (SATAC) cubre las necesidades de los cadetes de inteligencia para la formación profesional?	**A**	**B**	**C**	**D**	**E**	

Anexo 04: Validación de documentos

HOJA DE EVALUACIÓN DE EXPERTOS

TEMA DE INVESTIGACIÓN:

IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" 2019.

Colocar "x" en el casillero de la pregunta evaluada para las variables

ITEM	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formulada con el lenguaje adecuado							/			
2.OBJETIVIDAD	Está expresado en conductas observables							/			
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia							/			
4.ORGANIZACION	Existe una organización lógica							/			
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad							/			
6.INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación							/			
7. CONSISTENCIA	Basado en aspectos teóricos científicos							/			
8.COHERENCIA	Entre los índices, e indicadores							/			
9.METODOLOGIA	El diseño responde al propósito del diagnostico							/			
10.PERTINENCIA	Es útil y adecuado para la investigación							/			

OBSERVACIONES REALIZADAS POR EL EXPERTO:

.....Ninguna.....

.....

Grado académico:

.....Doctora.....

Apellidos y Nombres:

.....Silva Calderón Josefa María.....

Firma: .....

Post firma: Josefa M. Silva C.

Nº DNI: 06559990

HOJA DE EVALUACIÓN DE EXPERTOS

TEMA DE INVESTIGACIÓN:

IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" 2019.

Colocar "x" en el casillero de la pregunta evaluada para las variables

ÍTEM	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formulada con el lenguaje adecuado									✓	
2.OBJETIVIDAD	Está expresado en conductas observables									✓	
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia									✓	
4.ORGANIZACION	Existe una organización lógica									✓	
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad									✓	
6.INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación									✓	
7. CONSISTENCIA	Basado en aspectos teóricos científicos									✓	
8.COHERENCIA	Entre los índices, e indicadores									✓	
9.METODOLOGIA	El diseño responde al propósito del diagnostico									✓	
10.PERTINENCIA	Es útil y adecuado para la investigación									✓	

OBSERVACIONES REALIZADAS POR EL EXPERTO:

Ninguna

Grado académico:

Maestro

Apellidos y Nombres:

Pascar Luna Jorge

Firma: .....

Post firma: Jorge Pascar Luna

Nº DNI: 10265366

HOJA DE EVALUACIÓN DE EXPERTOS

TEMA DE INVESTIGACIÓN:

IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" 2019.

Colocar "x" en el casillero de la pregunta evaluada para las variables

ÍTEM	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formulada con el lenguaje adecuado								/		
2.OBJETIVIDAD	Está expresado en conductas observables								/		
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia									/	
4.ORGANIZACION	Existe una organización lógica									/	
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad								/		
6.INTENCIONALIDAD	Adecuado para valorar los instrumentos de investigación								/		
7. CONSISTENCIA	Basado en aspectos teóricos científicos								/		
8.COHERENCIA	Entre los índices, e indicadores								/		
9.METODOLOGIA	El diseño responde al propósito del diagnostico								/		
10.PERTINENCIA	Es útil y adecuado para la investigación								/		

OBSERVACIONES REALIZADAS POR EL EXPERTO:

.....

.....

Grado académico:

.....MG.....

Apellidos y Nombres:

.....David Fernando Flores.....

Firma: .....

Post firma: .....

Nº DNI: 09155913

Anexo 05: Constancia emitida por la institución donde se realizó la investigación

Escuela Militar de Chorrillos
"Coronel Francisco Bolognesi"
Alma Máter del Ejército del Perú

CONSTANCIA

Que a los Bachilleres: MALLMA CONDOR ERIK ALFREDO; FLORES AMASIFUEN GIANFRANCO PAUL; identificados con DNI N° 71807249, 73003093; con los que han realizado trabajo de investigación a los cadetes del Arma de Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019; como parte de su tesis IMPLEMENTACIÓN DE LA ASIGNATURA CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI"- 2019, para optar el Título profesional de Licenciado en Ciencias Militares.

Se expide la presente constancia a solicitud de los interesados, para los fines conveniente

Chorrillos, 1 de Enero de 2020

O – 224396679 O+
CH. SOLDEVILLA P.
TTE CRL INF
Jefe del DIDOC de la EMCH
"Coronel Francisco Bolognesi"

Anexo 06: Compromiso de autenticidad del documento

Los bachilleres en Ciencias Militares, INTG MALLMA CONDOR, ERIK ALFREDO; INTG FLORES AMASIFUEN, GIANFRANCO PAUL; autores del trabajo de investigación titulado "IMPLEMENTACIÓN DE LA ASIGNATURA DE CIBERSEGURIDAD Y LA FORMACIÓN PROFESIONAL DE LOS CADETES DEL ARMA DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" 2019"

Declaran:

Que, el presente trabajo ha sido íntegramente a elaborado por los suscritos y que no existe plagio alguno, presentado por otra persona, grupo o institución, comprometiéndonos a poner a disposición del COEDE (EMCH "CFB") y RENATI (SUNEDU) los documentos que acrediten la autenticidad de la información proporcionada; si esto lo fuera solicitado por la entidad.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada.

Nos afirmamos y ratificamos en lo expresado, en señal de lo cual firmamos el presente documento.

Chorrillos, 09 de Diciembre de 2019.

E. MALLMA C.	**G. FLORES A.**
DNI: 71807249	**DNI: 73003093**