ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CFB" – 2024

Tesis para optar el Título Profesional de Licenciado en Ciencias Militares con Mención en Administración

Autores:

Milena Nicool Leyva Vásquez - (0009-0007-6354-2349)

Milagros Lila Flor Llanos Salcedo - (0009-0009-0795-0344)

Revisor General:

Dr. Caller Luna Juan Bautista - (0000-0001-6623-246X)

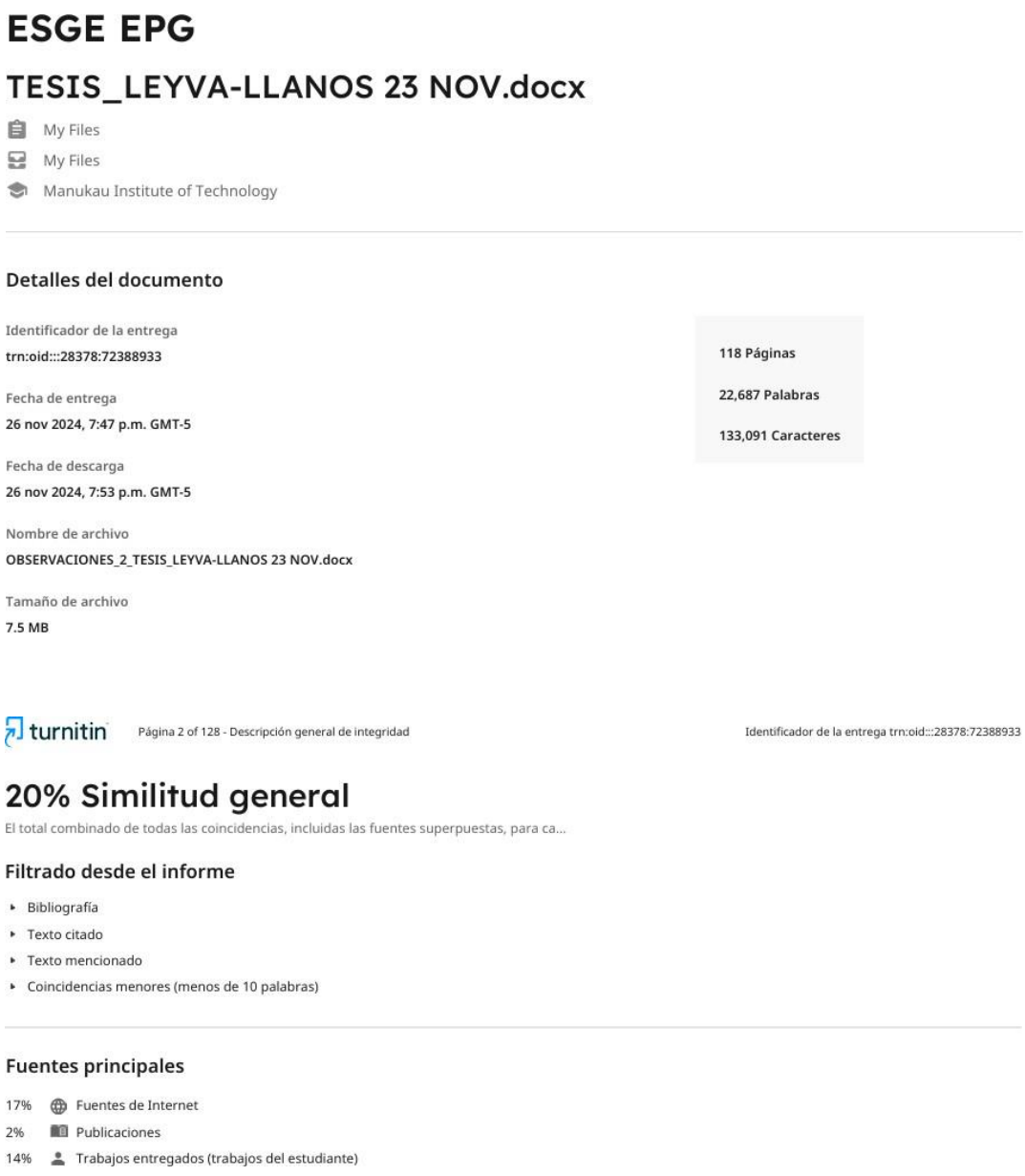
LINEA DE INVESTIGACIÓN

Seguridad pública y ciudadana

Lima – Perú

2024

Grado de Similitud



ESGE EPG

TESIS_LEYVA-LLANOS 23 NOV.docx

My Files

My Files

Manukau Institute of Technology

Detalles del documento

Identificador de la entrega
trn:oid:::28378:72388933

Fecha de entrega
26 nov 2024, 7:47 p.m. GMT-5

Fecha de descarga
26 nov 2024, 7:53 p.m. GMT-5

Nombre de archivo
OBSERVACIONES_2_TESIS_LEYVA-LLANOS 23 NOV.docx

Tamaño de archivo
7.5 MB

118 Páginas

22,687 Palabras

133,091 Caracteres

turnitin Página 2 of 128 - Descripción general de integridad Identificador de la entrega trn:oid:::28378:72388933

20% Similitud general

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

Filtrado desde el informe

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

Fuentes principales

17% Fuentes de Internet

2% Publicaciones

14% Trabajos entregados (trabajos del estudiante)

ESCUELA MILITAR DE CHORRILLOS

"CORONEL FRANCISCO BOLOGNESI"

Declaración Jurada de Autoría

1. Somos autores de la investigación titulada: "MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CFB" – 2024"**.**
2. Que, dicha investigación ha sido íntegramente elaborado por los suscritos y que no existe plagio alguno de ideas, texto, o imagen que corresponda a otra persona, grupo o institución; comprometiéndonos a poner a disposición de la EMCH "CFB", los documentos que acrediten la autenticidad de la información proporcionada; si esto fuera solicitado por la entidad.
3. En tal sentido, asumimos la responsabilidad que corresponde, ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la formación aportada. Y nos comprometemos a salir en defensa de la EMCH "CFB" ante cualquier reclamo de terceros que al respecto pudiese sobrevivir.
4. Finalmente, reconocemos, para todos los efectos, que la EMCH "CFB" actúa como tercero de buena fe y está exenta de cualquier responsabilidad.

En honor de lo afirmado y ratificado, firmamos la presente declaración jurada de autenticidad.

Chorrillos, 02 octubre del 2024

Milena Nicool Leyva Vásquez
DNI: 76562040

Milagros Lila Flor Llanos Salcedo
DNI: 73172364

Autorización de publicación

ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

DEPARTAMENTO DE INVESTIGACIÓN – DINVEST

FORMATO DE AUTORIZACIÓN PARA LA PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA EMCH "CFB" "CFB"

Formato de autorización para la publicación electrónica en la página web del Repositorio Institucional Digital de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso y Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales RENATI.

1. Datos personales

Autor 1: Milena Nicool Leyva Vásquez	**Autor 2:** Milagros Lila Flor Llanos Salcedo
N° DNI: 76562040	**N° DNI:** 73172364
Teléfono: 928592974	**Teléfono:** 999225343
Correo-e: mleyvav@escuelamilitar.edu.pe	**Correo-e:** mllanoss@escuelamilitar.edu.pe
ORCID: 0009-0007-6354-2349	**ORCID:** 0009-0009-0795-0344

2. Datos de la Obra

Título: MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CFB" "CFB"- 2024	
Tipo de obra: Tesis	
Asesor 1: Dr. Juan Bautista Caller Luna	**Asesor 2:**
N° DNI: 07143496	**N° DNI:**
ORCID: 0000-0001-6623-246X	**ORCID:**
Año de publicación: 2024	

3. Declaraciones

El autor declara que:

- La obra original y nuestra propia y exclusiva creación, realizándose sin violar ni usurpar derechos de autores de terceros.
- Con la obra no se ha quebrantado ningún derecho moral o patrimonial de autor.
- No contiene declaraciones difamatorias contra terceros y respeta el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales de las personas.
- Somos titulares de los derechos patrimoniales sobre la obra y no pesa ningún gravamen sobre ella.

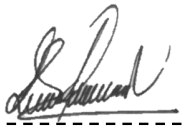
Por tanto, todo lo señalado en el presente formato, en especial lo descrito en el numeral dos, ostenta la condición de Declaración Jurada. Por ello me comprometo a salir en defensa de LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI" ante cualquier reclamación de terceros que al respecto pudiese sobrevenir. Para todos los efectos, LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", actúa como tercero de buena fe.

4. Publicaciones de su investigación en el Repositorio institucional de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

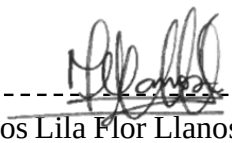
TIPO DE ACCESO A SU INVESTIGACIÓN

Acceso abierto	**X**
Acceso restringido	**(12 a 24 meses)**

JUSTIFICACIÓN (de acceso restringido)



Milena Nicool Leyva Vásquez
DNI: 76562040



Milagros Lila Flor Llanos Salcedo
DNI: 73172364

Agradecimiento

A Dios por su amor infinito y su inagotable bondad. Nos bendice con la capacidad de sonreír ante nuestros logros, que sin su ayuda no serían posibles. Cuando enfrentamos pruebas y caemos, encontramos en Él la fuerza para aprender de nuestros errores y mejorar como seres humanos, creciendo en diversos aspectos de la vida.

A nuestros queridos padres, les expresamos nuestra más profunda gratitud por darnos la vida y por brindarnos las herramientas necesarias para superarnos. Su presencia constante en nuestras vidas ha sido fundamental para forjar la persona que somos hoy. No podemos dejar de expresarles que, gracias a su amor y apoyo incondicional, hemos alcanzado esta meta.

Dedicatoria

A nuestros padres, que nos dieron la vida y la fuerza para crecer, su guía inquebrantable ha sido fundamental para convertirnos en quienes somos. Hoy, más que nunca, reconocemos que este logro es posible gracias a ustedes, y siempre llevaremos esa gratitud en lo más profundo de nuestro ser.

Índice

Página

Índice de Tablas

Página

Índice de Figuras

Página

Resumen

La presente investigación tuvo como objetivo general determinar la relación entre las medidas de contrainteligencia y la seguridad de las instalaciones en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" (EMCH "CFB") durante el año 2024. El estudio se desarrolló bajo un enfoque cuantitativo, empleando un diseño no experimental con alcance descriptivo-correlacional y el método hipotético-deductivo. La población estuvo conformada por 220 cadetes, seleccionándose una muestra de 110 cadetes de cuarto año mediante muestreo probabilístico. La técnica de recolección de datos fue la encuesta, utilizando un cuestionario validado y confiable. Los datos se analizaron mediante estadística descriptiva e inferencial. Los resultados evidenciaron una correlación positiva muy fuerte (0.903) entre las medidas de contrainteligencia y la seguridad de las instalaciones, reflejando que su implementación eficaz mejora significativamente la protección de los recursos y el personal de la EMCH "CFB". Asimismo, se hallaron correlaciones similares entre la seguridad de las instalaciones y factores específicos como la actualización tecnológica (0.884) y la capacitación del personal en técnicas de contrainteligencia (0.895), subrayando la importancia de estos elementos en la prevención de amenazas. Las conclusiones destacan que el fortalecimiento continuo de las estrategias de contrainteligencia es fundamental para mitigar vulnerabilidades y responder adecuadamente a los riesgos internos y externos en un entorno militar cambiante.

Palabras clave: *actualización tecnológica, capacitación, contrainteligencia, instalaciones militares, seguridad militar.*

Abstract

This research aims to determine the relationship between counterintelligence measures and the security of facilities at the Military Academy of Chorrillos "Coronel Francisco Bolognesi" (EMCH "CFB") in 2024. The study followed a quantitative approach, employing a non-experimental design with descriptive-correlational scope and the hypothetical-deductive method. The population consisted of 220 cadets, with a probabilistic sample of 110 fourth-year cadets. Data collection was conducted through a validated and reliable questionnaire survey, and the data were analyzed using descriptive and inferential statistics. The results revealed a very strong positive correlation (0.903) between counterintelligence measures and facility security, indicating that their effective implementation significantly improves the protection of resources and personnel at the EMCH "CFB." Similarly, strong correlations were identified between facility security and specific factors such as technological updating (0.884) and staff training in counterintelligence techniques (0.895), emphasizing the importance of these elements in preventing threats. The conclusions highlight that the continuous strengthening of counterintelligence strategies is crucial to mitigate vulnerabilities and respond effectively to internal and external risks in a changing military environment.

Keywords: *counterintelligence, facility security, military installations, staff training, technological updating.*

Introducción

En un mundo caracterizado por la constante evolución de amenazas y desafíos, la seguridad de las instalaciones militares se convierte en un elemento vital para garantizar la integridad y el funcionamiento adecuado de una institución. En este contexto, la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" (EMCH "CFB") se erige como una entidad emblemática, responsable de formar a las futuras generaciones de líderes militares. La seguridad y la contrainteligencia son fundamentales para mantener la protección de estas instalaciones, y los cadetes, como parte esencial de la institución, también deben estar involucrados en este proceso.

Este trabajo de investigación tuvo como objetivo principal explorar las medidas de contrainteligencia y seguridad en las instalaciones de la EMCH "CFB" desde la perspectiva de los cadetes para el año 2024. Es fundamental comprender cómo los cadetes, como futuros líderes militares, perciben, comprenden y contribuyen a la seguridad de su entorno académico y operativo. Para abordar esta investigación de manera integral y rigurosa, se ha estructurado en cuatro capítulos fundamentales que permitirán profundizar en cada aspecto relevante del estudio.

En el capítulo inicial, se presentó el planteamiento del problema, donde se analizó en detalle la percepción y comprensión de las medidas de contrainteligencia y seguridad por parte de los cadetes de la EMCH "CFB". Se identificaron las principales áreas de preocupación y oportunidades de mejora desde la perspectiva de los propios cadetes, considerando sus experiencias y vivencias en el entorno militar.

El segundo capítulo se dedicó al desarrollo del marco teórico, que proporcionó un sustento conceptual sólido para comprender los fundamentos de la contrainteligencia y la seguridad en contextos militares, enfocándose también en la psicología y la sociología de la seguridad para entender cómo los cadetes interactuaron con las medidas de protección.

El tercer capítulo estuvo destinado al marco metodológico, donde se describieron detalladamente los métodos y técnicas que se emplearon para llevar a cabo el estudio, incluyendo la recopilación de datos mediante encuestas, entrevistas y, posiblemente, observación participante para obtener una comprensión completa de las percepciones y comportamientos de los cadetes en relación con la seguridad y la contrainteligencia.

En el cuarto capítulo, se trataron los aspectos administrativos vinculados a la ejecución del proyecto, abarcando la planificación del tiempo, el presupuesto proyectado, los recursos requeridos y las pautas éticas que guiaron el desarrollo de la investigación. Estos elementos garantizaron la integridad y el rigor del estudio, con especial atención en la participación y el

bienestar de los cadetes a lo largo del proceso investigativo.

CAPÍTULO I:

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción Problemática

En un entorno geopolítico marcado por la creciente complejidad de las amenazas a la seguridad, instituciones militares como la EMCH “CFB” se encuentran en una encrucijada estratégica. Situada en Lima, la EMCH “CFB” representa un bastión de formación para los futuros líderes castrenses del Perú. No obstante, esta prestigiosa institución enfrenta desafíos cruciales en materia de seguridad y contrainteligencia dentro de sus instalaciones. Incidentes recientes han sacudido la confianza en la protección de los cadetes y los recursos institucionales, generando una urgente necesidad de revisar y fortalecer las medidas de seguridad. Como señalan Samaniego y Vergaray (2019), la seguridad de las instalaciones militares no es simplemente una cuestión de proteger activos físicos, sino también de salvaguardar la soberanía y la integridad de la nación ante posibles amenazas internas y externas.

Esta situación problemática surge debido a una serie de factores interrelacionados que ponen de manifiesto la vulnerabilidad de las instalaciones de la EMCH “CFB” y la necesidad de revisar y fortalecer las medidas de seguridad y contrainteligencia. En primer lugar, el entorno cambiante y cada vez más complejo de las amenazas a la seguridad plantea desafíos constantes. Según Martínez (2022), la naturaleza dinámica de estas amenazas, que pueden incluir desde actores externos con intenciones hostiles hasta riesgos internos como la negligencia o la falta de conciencia de seguridad, requiere una vigilancia constante y una capacidad de adaptación por parte de las instituciones militares. Estas amenazas pueden manifestarse en múltiples formas, desde ataques terroristas hasta espionaje industrial y ciberataques sofisticados (Fernández, 2020).

Además, la ubicación estratégica de la EMCH “CFB” en Lima, una ciudad con altos índices de criminalidad y actividad delictiva, aumenta el riesgo de incidentes que puedan afectar la seguridad de las instalaciones y de quienes las ocupan. Como señala Aguirre (2022), "la proximidad a zonas urbanas densamente pobladas también puede facilitar el acceso no autorizado a las instalaciones militares, lo que representa una preocupación adicional para las autoridades" (p. 38). Esta cercanía a áreas urbanas densamente pobladas puede facilitar la

infiltración de individuos o grupos hostiles, así como la realización de actividades de reconocimiento y vigilancia por parte de potenciales adversarios (Cabrera, 2021).

Por otro lado, la tecnología desempeña un papel cada vez más importante en la seguridad de las instalaciones militares, pero también introduce nuevos riesgos. Castillo (2020) advierte que "la creciente dependencia de sistemas de información y comunicación, así como la proliferación de dispositivos conectados a Internet, aumenta la superficie de ataque y la exposición a posibles ciberataques y vulnerabilidades de seguridad". (p.9) Estos sistemas pueden ser susceptibles a ataques cibernéticos, como el robo de información confidencial, la interrupción de operaciones críticas o incluso el control remoto de sistemas de seguridad (Covarrubias y Zadamig, 2020).

Desde una perspectiva global, Jones (2020) afirma que la seguridad de las instalaciones militares es una preocupación fundamental para todas las naciones, dado el panorama de amenazas cambiantes y multifacéticas que enfrentan en el escenario internacional. En un mundo interconectado y en constante evolución, las instituciones militares se encuentran expuestas a una amplia gama de riesgos, que van desde amenazas convencionales como el terrorismo hasta ataques cibernéticos sofisticados y actividades de espionaje por parte de actores estatales y no estatales.

A nivel nacional, Duffield (2020) destaca que el terrorismo, tanto doméstico como internacional, ha sido una preocupación persistente en el país. Aunque Perú ha experimentado una disminución en la actividad terrorista desde el declive del grupo insurgente Sendero Luminoso en la década de 1990, aún persisten grupos remanentes y emergentes que representan una amenaza para la seguridad nacional. Estos grupos pueden tener como objetivo atacar instalaciones militares como parte de su estrategia para desestabilizar al gobierno y sembrar el caos en el país (Comisión Nacional contra el Terrorismo, 2018).

Además, según la Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA, 2019), la presencia del crimen organizado, que incluye el narcotráfico, la minería ilegal y otras actividades ilícitas, plantea desafíos adicionales para la seguridad de las instalaciones militares. Estos grupos criminales suelen operar en zonas remotas y de difícil acceso, donde las instalaciones militares pueden ser blanco de ataques o infiltraciones. Además, la corrupción y la complicidad con actores del crimen organizado dentro de las fuerzas de seguridad pueden debilitar aún más las defensas de las instalaciones militares (Piedrahita, 2020).

La contrainteligencia, entendida como el conjunto de medidas destinadas a prevenir, detectar y contrarrestar las actividades de inteligencia hostil, juega un papel crucial en este contexto (Freire, 2021). La eficacia de las medidas de contrainteligencia no solo influye en la protección de la información sensible y estratégica, sino también en la salvaguarda de la infraestructura y la seguridad de todo el personal militar y civil que labora en estas instalaciones. Sin embargo, a pesar de los esfuerzos continuos por parte de las autoridades militares, existen desafíos significativos en la optimización de las medidas de contrainteligencia y su influencia en la seguridad de la EMCH "CFB".

Como señala Freire (2021), la complejidad de las amenazas actuales, que van desde el espionaje cibernético hasta la infiltración física, requiere un enfoque integral y adaptativo para garantizar la protección efectiva de las instalaciones. Además, la capacitación continua del personal en materia de contrainteligencia y la implementación de tecnologías de vanguardia son aspectos clave para fortalecer las medidas de seguridad (Samaniego y Vergaray, 2019).

Samaniego y Vergaray (2019) sostienen que la seguridad en las instalaciones militares va más allá de la simple protección de activos materiales, involucrando la preservación de la soberanía y la estabilidad nacional frente a amenazas diversas, tanto internas como externas. En este sentido, la presente investigación enfatiza la relevancia de implementar estrategias eficaces para enfrentar los retos de la contrainteligencia y la seguridad, con un enfoque particular en el entorno de la EMCH "CFB".

En este sentido, el presente estudio analizó en profundidad la situación actual, identificó las áreas de mejora y propuso estrategias innovadoras para optimizar las medidas de contrainteligencia y fortalecer la seguridad de las instalaciones de la EMCH "CFB".

1.2 Delimitación de la investigación

1.2.1 Delimitación espacial

La delimitación espacial de esta investigación se centra específicamente en las instalaciones de la EMCH "CFB", ubicada en el distrito de Chorrillos, Lima, Perú. Este enfoque permite un análisis detallado de las medidas de contrainteligencia y su influencia en la seguridad dentro de este contexto específico. Se han examinado todas las áreas físicas y operativas de la

institución militar, incluyendo edificios administrativos, campos de entrenamiento, áreas de alojamiento y cualquier otro espacio relevante para el estudio.

1.2.2 Delimitación temporal

La delimitación temporal de esta investigación ha abarcado el año 2024, el momento actual. Este enfoque permite analizar las medidas de contrainteligencia implementadas en la EMCH "CFB" y su impacto en la seguridad de las instalaciones durante este año específico. Considerar únicamente el año 2024 permite obtener una visión actualizada de las prácticas de seguridad y contrainteligencia en la institución militar, sin perder de vista los posibles cambios en el contexto nacional e internacional que podrían influir en dichas prácticas.

1.2.3 Delimitación teórica:

La delimitación teórica de este estudio se ha centrado en los conceptos y teorías relacionados con la contrainteligencia, la seguridad de instalaciones militares y la gestión de riesgos. Se han utilizado marcos teóricos y modelos conceptuales pertinentes para analizar y comprender la efectividad de las medidas de contrainteligencia en la protección de las instalaciones de la EMCH "CFB". Se consideran también investigaciones previas y estudios relevantes en el campo de la seguridad y la contrainteligencia para fundamentar y contextualizar los hallazgos de esta investigación.

1.3 Formulación del problema

1.3.1 Problema principal

¿Cuál es la relación de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024?

1.3.2 Problemas secundarios

¿Cómo se relaciona la Evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024?

¿Cómo se relaciona la actualización tecnológica en las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" "en el año 2024?

¿Cómo se relaciona la capacitación del personal en técnicas y procedimientos y la seguridad de las instalaciones en cadetes de la EMCH “CFB”en el año 2024?

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Determinar la relación que existe entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

1.4.2 Objetivos específicos

Identificar la relación que existe entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

Establecer la relación que existe entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH “CFB”en el año 2024.

Determinar la relación que existe entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

1.5 Justificación e importancia de la investigación

1.5.1 Justificación

1.5.1.1 Justificación teórica

Desde una perspectiva teórica, esta investigación fue relevante porque permitió ampliar el conocimiento sobre las estrategias y prácticas relacionadas con la contrainteligencia y la seguridad en entornos militares. Al analizar en profundidad cómo la optimización de las medidas de contrainteligencia influyó en la seguridad de las instalaciones de la EMCH “CFB”, se contribuyó al cuerpo existente de conocimientos en este campo, proporcionando nuevas perspectivas y posibles soluciones a los desafíos actuales en materia de seguridad militar. Además, esta investigación sirvió como base para futuros estudios académicos y científicos relacionados con la contrainteligencia y la seguridad en otros contextos similares.

1.5.1.1 Justificación práctica

Desde un punto de vista práctico, revistió una importancia significativa. En primer lugar, dado el papel fundamental que desempeñó esta institución en la formación y preparación de los futuros oficiales del Ejército del Perú, garantizar la seguridad de sus instalaciones fue crucial para preservar la integridad de los recursos humanos y materiales que la componían. Además, en un contexto donde las amenazas a la seguridad nacional y la integridad de las instituciones militares eran cada vez más complejas y variadas, comprender cómo mejorar las medidas de contrainteligencia contribuyó directamente a fortalecer la defensa y protección del país frente a posibles riesgos y adversidades.

1.5.1.3 Justificación metodológica

La investigación metodológica resultó crucial para verificar y apoyar la efectividad de las medidas de contrainteligencia propuestas y su influencia en la seguridad de las instalaciones de la EMCH “CFB”. Mediante un enfoque riguroso y estructurado, esta investigación aseguró la fiabilidad y validez de los resultados, lo que facilitó la creación de recomendaciones prácticas y fundamentadas para fortalecer la seguridad en esta institución militar. Además, al emplear métodos y técnicas apropiadas para la recopilación y análisis de datos, se reforzó la solidez y consistencia de los hallazgos, incrementando su credibilidad y relevancia para los responsables de la seguridad y la gestión de la institución.

1.5.2 Importancia

La investigación sobre medidas de contrainteligencia y seguridad en las instalaciones de la EMCH “CFB” fue crucial, ya que se enfocó en cómo estas medidas impactaron directamente en los cadetes durante su formación. Al analizar detalladamente estas medidas, se pudieron identificar debilidades y oportunidades de mejora, lo que contribuyó tanto a fortalecer la protección de las instalaciones como al desarrollo de líderes militares competentes. Además, al mejorar la seguridad de la EMCH “CFB”, se promovió un entorno más propicio para el aprendizaje y se fortaleció la capacidad del país para hacer frente a amenazas internas y externas, lo que, en última instancia, contribuyó a la seguridad nacional y al bienestar de todos los ciudadanos del Perú.

1.6 Limitaciones de la investigación

De acuerdo con Hernández y Mendoza (2020), fue fundamental identificar los obstáculos presentes en cualquier estudio, pero también señalar las estrategias para superarlos. Durante la conducción de la investigación, las investigadoras se enfrentaron a diversas limitaciones:

El factor tiempo se erigió como un desafío significativo debido a las múltiples actividades que los cadetes debían cumplir; no obstante, se logró superar llevando a cabo la investigación en horas fuera de las actividades programadas por la Escuela Militar. En cuanto a lo económico, se presentaron limitaciones debido a la ausencia de un ingreso fijo por parte de las investigadoras, ya que éramos estudiantes. Sin embargo, esta dificultad fue solventada gracias a la ayuda de nuestros padres. La falta de libros modernos o actualizados en la biblioteca de la Escuela Militar representó otro obstáculo, el cual se superó recurriendo a la bibliografía disponible en el ámbito civil y haciendo uso de libros digitales. La información limitada proporcionada por el Departamento de Seguridad, debido al carácter profesionalmente confidencial de los informes de seguridad de la escuela, representó un desafío adicional para acceder a datos relevantes.

Además, se enfrentó la necesidad de coordinar las investigaciones y las respuestas a los cuestionarios en horarios que se ajustaran a la disponibilidad de los cadetes. Por último, el acceso limitado a las cámaras de seguridad, debido a su actividad reservada, dificultó la recopilación de datos visuales para el estudio. A pesar de estos obstáculos, estuvimos comprometidas a superarlos para garantizar la calidad y la integridad de la investigación.

CAPÍTULO II: Marco Teórico

2.1. Antecedentes

2.1.1. Antecedentes internacionales

El estudio realizado por Machado (2024) en Paraná, Brasil, analizó profundamente el contexto social marcado por relaciones intensas y fluctuantes, intercambios y comunicaciones derivados de la Globalización y el Capitalismo. En este entorno desafiante, las instituciones, incluida la Policía Militar del Paraná (PMPR), enfrentaron la necesidad constante de adaptarse para mantener su relevancia y eficacia. Mientras que las empresas privadas suelen buscar mejoras y optimización, las instituciones públicas, como la PMPR, tendieron a descuidar la estandarización y normatización de las medidas de seguridad interna debido a la falta de competencia directa y la evaluación de resultados bajo criterios diferentes. En este marco, la Seguridad Orgánica (SEGOR) surgió como un componente crucial de la contrainteligencia, cuya función fue proteger los activos e integridad institucional, pero se identificó que la PMPR carecía de un Plan de Seguridad Orgánica formalizado.

El estudio arrojó resultados reveladores. A través de un análisis exhaustivo de fuentes bibliográficas, jurídicas y documentales, se concluyó que la formalización de las medidas de SEGOR era imperativa para el éxito del Plan Estratégico de la PMPR. Esto no solo garantizaría su eficiencia operativa, sino que también contribuiría a su supervivencia y fortalecimiento como institución clave en la seguridad pública de Paraná. Entre los hallazgos más importantes se destacó que la falta de un plan formalizado de seguridad pudo haber generado una vulnerabilidad significativa, afectando directamente la capacidad de la institución para cumplir sus metas estratégicas y, por ende, comprometiendo su sostenibilidad a largo plazo.

Estos resultados fueron sumamente relevantes para nuestra investigación sobre medidas de contrainteligencia y seguridad en las instalaciones de la EMCH “CFB”. Si bien el estudio de Machado (2024) estuvo centrado en la Policía Militar del Paraná (PMPR), las conclusiones extraídas fueron aplicables a nuestro caso. El antecedente subyacente permitió establecer paralelismos en cuanto a la importancia de la formalización de las estrategias de seguridad en instituciones públicas y su impacto en la eficacia operativa.

El estudio realizado por Lecca et al. (2023) sobre el control interno en el comercio electrónico ofreció una contribución significativa a la investigación sobre medidas de

contrainteligencia y seguridad en la EMCH “CFB”. Este estudio puso en relieve la importancia de proteger los datos confidenciales y de evaluar la eficiencia de los sistemas de gestión organizacional, proporcionando un marco de referencia clave para comprender cómo se podían aplicar estas medidas en un entorno dinámico y tecnológico. Mediante una revisión sistemática de artículos publicados en bases de datos académicas de relevancia entre 2018 y 2023, el análisis exhaustivo permitió identificar diversas estrategias y prácticas de control interno, evaluando su efectividad y aplicabilidad en distintos contextos empresariales. Entre los resultados más notables, se concluyó que las organizaciones que implementaron medidas robustas de control interno vieron una mejora significativa en la protección de datos y una mayor confianza en sus sistemas de gestión, destacando la necesidad de establecer protocolos claros y auditables para la gestión de riesgos.

Para nuestra investigación sobre medidas de contrainteligencia y seguridad en la EMCH “CFB”, este estudio ofreció una base sólida para adaptar y aplicar estrategias de control interno en un contexto militar. La revisión de prácticas exitosas en la protección de datos confidenciales y la evaluación de sistemas de gestión proporcionó lecciones valiosas y recomendaciones aplicables a la mejora de la seguridad de instalaciones militares y la protección de información sensible. Los resultados de Lecca et al. (2023) mostraron que una estructura organizacional con controles internos eficientes no solo aumentaba la seguridad, sino también la resiliencia operativa frente a posibles amenazas de seguridad. Estos hallazgos enriquecieron nuestro análisis sobre las mejores prácticas en contrainteligencia, aportando ideas concretas para optimizar las medidas de seguridad en la EMCH “CFB” y otras instituciones militares.

Por otro lado, el estudio de Zalewski (2022), llevado a cabo en la Escuela de Guerra Naval de la Ciudad Autónoma de Buenos Aires, Argentina, cuyo propósito fue comparar la estructura organizativa enfocada en la seguridad física con la normativa legal vigente, también ofrece información crucial. A través de un análisis documental de leyes, reglamentos y entrevistas con expertos en derecho militar y personal de la Armada Argentina, se identificaron dos entidades clave responsables de la seguridad en las instalaciones logísticas militares: las Unidades y Subunidades de Seguridad (de carácter militar) y la Policía de Establecimientos Navales (no militar). Sin embargo, el estudio reveló importantes discrepancias entre la estructura organizacional actual y la normativa legal, lo que podría comprometer la integración y legitimidad del ejercicio de la seguridad física y el mantenimiento del orden público.

Los resultados de este estudio tienen implicaciones directas para nuestra investigación, ya que subrayan la importancia de garantizar que las medidas de seguridad en instalaciones militares estén alineadas con la legislación vigente para asegurar su legitimidad y eficacia. Las discrepancias encontradas en la estructura organizacional de la Armada Argentina resaltan la necesidad de revisar y ajustar continuamente las medidas de seguridad en instalaciones como la EMCH "CFB", asegurando su conformidad legal. Este antecedente, contribuye de manera significativa a la mejora de nuestras estrategias de contrainteligencia y seguridad, proporcionando una perspectiva práctica sobre los desafíos organizacionales y legales en la implementación de medidas efectivas.

El estudio realizado por Zalewski (2022) en la Escuela de Guerra Naval de la Ciudad Autónoma de Buenos Aires, Argentina, tuvo como propósito comparar la estructura organizacional actual encargada de la seguridad física y el mantenimiento del orden público en las instalaciones logísticas militares con la legislación vigente. A través de un análisis exhaustivo que incluyó la revisión documental de leyes, reglamentos y disposiciones, así como entrevistas con personal militar y expertos en derecho militar, se identificaron dos entidades principales responsables de la vigilancia y seguridad en las instalaciones: un sistema militar compuesto por Unidades y Subunidades de Seguridad, y una dependencia no militar denominada Policía de Establecimientos Navales. No obstante, el estudio reveló aspectos discordantes entre la estructura organizacional actual y los marcos legales vigentes, lo que planteó un riesgo de comprometer la integración y legitimidad de las funciones de seguridad física y el mantenimiento del orden público.

Entre los resultados más significativos, se destacó que estas discrepancias pudieron haber generado problemas en la coordinación operativa y legal de las unidades de seguridad. La falta de alineación entre la estructura organizacional y la legislación afectó no solo la eficacia de las medidas de seguridad, sino también su legitimidad frente a posibles auditorías o revisiones jurídicas. Este hallazgo subrayó la necesidad crítica de actualizar y revisar las estructuras de seguridad militar para garantizar su cumplimiento con las normativas vigentes, lo que, en última instancia, fortalecería la capacidad operativa y la autoridad de las instituciones encargadas de la protección de instalaciones militares.

Este antecedente es especialmente valioso para nuestra investigación sobre medidas de contrainteligencia y seguridad en las instalaciones de la EMCH "Coronel Francisco Bolognesi". Si bien el estudio de Zalewski se centra en la Armada Argentina, los hallazgos

resaltan la importancia de garantizar que la estructura organizacional dedicada a la seguridad esté alineada con la normativa vigente para asegurar tanto la eficacia operativa como la legitimidad legal. Las discrepancias identificadas en la Armada Argentina refuerzan la necesidad de revisar y ajustar las medidas de seguridad en la EMCH "CFB", asegurando que estén en conformidad con las leyes aplicables para prevenir riesgos asociados a una estructura desfasada. Además, este estudio proporciona una comprensión más profunda de los desafíos y riesgos vinculados a la implementación de medidas de seguridad en instalaciones militares, aportando lecciones clave sobre la necesidad de una vigilancia continua y la actualización de protocolos de seguridad para mantener la integridad institucional y la autoridad operativa en contextos militares.

2.1.2 Antecedentes nacionales

El estudio de Castillo (2020) en la Dirección de Inteligencia de la Policía Nacional del Perú tuvo como objetivo analizar el tratamiento de los documentos relacionados con delitos contra el patrimonio en la documentación de inteligencia de la institución. Mediante un enfoque cualitativo, básico y descriptivo, participaron oficiales superiores y abogados especializados en la comparación de diversas fuentes de información, como guías de entrevistas, documentos previos y enfoques conceptuales de categorías clave. Los resultados del estudio revelaron una carencia significativa de formación especializada en el manejo de documentos sensibles, lo cual podría comprometer tanto la seguridad jurídica del personal como la eficacia de la inteligencia producida.

Entre los resultados más relevantes, se destacó la urgente necesidad de incluir el tratamiento de documentos criminales en el artículo 2 de las "funciones" del Decreto Legislativo 1267, Ley General de la Policía Nacional del Perú, para otorgar a la institución las facultades legales necesarias en esta materia. Asimismo, se concluyó que un registro incorrecto de datos personales podría derivar en análisis inexactos y poco fiables, lo que pone de relieve la importancia de implementar mecanismos y directrices claras para mejorar la gestión de la información y la inteligencia en la institución. Estos hallazgos subrayan la necesidad de capacitación especializada y la actualización de normativas, elementos críticos para asegurar que los procesos de inteligencia sean sólidos y efectivos.

Este antecedente nacional fue altamente relevante para nuestra investigación sobre medidas de contrainteligencia y seguridad en las instalaciones de la EMCH “Coronel Francisco

Bolognesi". Aunque el estudio de Castillo se ha enfocado en la Policía Nacional del Perú, los problemas identificados, como la falta de formación especializada y la necesidad de mejorar los mecanismos de gestión de la información, son igualmente aplicables en el contexto militar. Los resultados destacan la importancia de contar con sistemas fiables y personal capacitado para garantizar la integridad de la información sensible y la seguridad jurídica de los involucrados. Además, sugieren la revisión de las normativas legales vigentes para asegurar que las capacidades de inteligencia y contrainteligencia se fortalezcan, lo cual es crucial para cualquier institución militar que busque optimizar sus medidas de seguridad y contrainteligencia.

El estudio de Fonseca et al. (2023) se enfocó en identificar nuevos escenarios de seguridad y defensa para las fuerzas armadas del Perú, centrándose en las amenazas y desafíos tanto internos como externos que enfrentan en la actualidad. Utilizando una metodología cuantitativa, el análisis se basa en datos desagregados del Proyecto de Justicia Mundial (PJW) y su correlación con datos del Banco Mundial, evaluando factores interrelacionados con los recursos del sector defensa. Entre los resultados más destacados, se encontró que los índices de orden y seguridad en Perú muestran una menor adherencia al Estado de derecho, lo que representa un desafío significativo para el fortalecimiento de las fuerzas armadas en su misión de proteger la seguridad nacional. Además, el estudio reveló que la asignación y gestión de los recursos del sector defensa son fundamentales para mejorar la capacidad de respuesta de las fuerzas armadas frente a amenazas emergentes, tanto en el plano interno como externo.

Los resultados también subrayaron que, si bien los recursos son críticos, su optimización y adecuada distribución resultan clave para asegurar la preparación de las fuerzas armadas frente a escenarios de riesgo creciente, como el crimen organizado, las amenazas cibernéticas y los conflictos fronterizos. Se destacó la importancia de desarrollar una estrategia de seguridad multidimensional que integre tanto la defensa territorial como la protección de infraestructuras críticas y la gestión de crisis, permitiendo a las fuerzas armadas operar con mayor eficiencia y adaptabilidad en un entorno de seguridad cada vez más complejo.

Este antecedente nacional fue de gran valor para nuestra investigación sobre medidas de contrainteligencia y seguridad en las instalaciones de la EMCH "CFB". Aunque el estudio de Fonseca et al. (2023) se centra en un contexto más amplio relacionado con las fuerzas armadas peruanas, sus hallazgos ofrecen una perspectiva crítica sobre la necesidad de adaptar las estrategias de seguridad en un entorno cambiante. Los resultados indican que la capacidad

de respuesta ante amenazas emergentes está directamente vinculada a la adecuada administración de los recursos, lo que sugiere que las instalaciones militares, como la EMCH "CFB", deben optimizar sus recursos de seguridad y contrainteligencia para hacer frente a nuevos desafíos. Este estudio también enfatiza la relevancia de considerar el contexto nacional e internacional en el diseño de políticas de defensa y seguridad, destacando la necesidad de reforzar la infraestructura de contrainteligencia para responder con eficacia a los riesgos presentes y futuros.

El estudio de Villalba et al. (2020) abordó la filtración de información en redes sociales y sus riesgos para la seguridad física y las instalaciones de los cadetes de cuarto año de la EMCH "CFB" en 2019. Con un enfoque de investigación básico y un nivel descriptivo y correlacional, el diseño es no experimental. La muestra incluyó a 146 cadetes, y los datos se recolectaron mediante encuestas, utilizando dos cuestionarios diseñados específicamente para este grupo, que emplearon la Escala de Likert para medir respuestas. La consistencia interna de los cuestionarios fue validada con el estadístico Alfa de Cronbach. Los resultados mostraron una correlación positiva y significativa entre la filtración de información en redes sociales y la seguridad física e instalaciones de los cadetes, respaldada por el estadístico de Spearman (sig. bilateral = .000 < 0.01; Rho = .734). Estos hallazgos resaltan la necesidad urgente de gestionar eficazmente la información en redes sociales en el ámbito militar, ya que las filtraciones pueden representar una amenaza considerable para la seguridad. Este estudio proporciona una base importante para comprender los riesgos relacionados con el uso de redes sociales en entornos militares, y ofrece información valiosa sobre las medidas de contrainteligencia y seguridad necesarias para proteger las instalaciones militares y garantizar la seguridad de la información sensible.

2.2 Bases teóricas o teorías sustantivas

2.2.1 Base teórica de la variable de estudio 1: Medidas de Contrainteligencia

2.2.1.1 Definición.

Las medidas de contrainteligencia en el ámbito militar, según Freire (2021), son fundamentales para garantizar la protección de las capacidades operativas de una institución militar. Estas medidas incluyen la planificación estratégica destinada a anticipar y neutralizar amenazas externas que busquen acceder a información sensible o comprometer la seguridad institucional. En su investigación, Freire (2021) subraya la importancia de desarrollar un

enfoque basado en las capacidades de contrainteligencia, destacando que la correcta planificación no solo responde a incidentes, sino que también previene riesgos futuros mediante la identificación y mitigación de vulnerabilidades en la estructura organizacional.

La contrainteligencia, como parte integral de la seguridad nacional, también implica la implementación de estrategias diseñadas para proteger tanto los recursos humanos como materiales. Estas estrategias están basadas en un enfoque preventivo, donde la anticipación y la respuesta rápida juegan un papel crucial en la neutralización de amenazas potenciales. De acuerdo con Gill et al. (2020), la teoría de la inteligencia debe evolucionar para enfrentar los nuevos desafíos que plantean los adversarios en un entorno globalizado, donde la tecnología y la sofisticación de los ataques están en constante crecimiento, asimismo, enfatizan que la expansión de las capacidades tecnológicas de los actores hostiles demanda una actualización continua de las técnicas y herramientas de contrainteligencia.

Daza y Torres (2022) complementan esta visión destacando la relevancia de la cultura organizacional y la cultura de seguridad en la eficacia de las medidas de contrainteligencia. Según estos autores, el éxito de las medidas de contrainteligencia no solo depende de los sistemas y protocolos establecidos, sino también de cómo la cultura interna fomenta un ambiente de vigilancia constante y responsabilidad compartida entre el personal. En este sentido, una cultura de seguridad sólida es clave para asegurar la participación de todos los miembros de la organización en la protección de los activos estratégicos.

Además, Cárdenas y Ore (2020) argumentan que la seguridad de las instalaciones es otro componente crítico dentro de las medidas de contrainteligencia. Estos autores resaltan que los entornos de formación militar, como las academias, deben implementar medidas de seguridad que se alineen con los principios de contrainteligencia para proteger a sus cadetes y el equipamiento sensible. Esto no solo incluye la vigilancia física, sino también la adopción de sistemas tecnológicos avanzados para prevenir la infiltración y el espionaje.

Asimismo, Lucero (2013) señala que, en el contexto de las redes sociales, las medidas de seguridad de contrainteligencia deben adaptarse a la rápida expansión de las tecnologías de la información. Según Lucero, las plataformas de redes sociales presentan un alto riesgo para la fuga de información sensible, por lo que es esencial desarrollar estrategias específicas para gestionar estos riesgos.

Como último punto, Estarellas (2023) analiza la contrainteligencia ofensiva como una herramienta eficaz para contrarrestar las operaciones de inteligencia exterior, específicamente en el contexto de la inteligencia rusa. Este autor argumenta que, en situaciones de conflicto asimétrico, la contrainteligencia debe adoptar una postura proactiva, no solo defensiva, para neutralizar a los adversarios mediante operaciones disruptivas y desinformación controlada.

2.2.1.2 Medición

La medición de las medidas de contrainteligencia implica evaluar la efectividad y eficacia de las acciones implementadas para proteger las instalaciones militares y sus activos. Esto puede incluir la realización de evaluaciones de seguridad exhaustivas, la recopilación y análisis de datos de inteligencia, el monitoreo de actividades sospechosas, el seguimiento de la implementación de protocolos de seguridad y la medición del impacto de las contramedidas adoptadas. Además, se pueden utilizar indicadores cuantitativos y cualitativos para evaluar el rendimiento de las medidas de contrainteligencia en términos de reducción de vulnerabilidades, prevención de amenazas y protección de activos críticos (Gill et al., 2020).

La medición de las medidas de contrainteligencia se basa en la evaluación de diversos aspectos, como la eficacia en la detección de amenazas, la rapidez y precisión en la respuesta a incidentes, la capacidad para prevenir filtraciones de información sensible, la eficiencia en el uso de recursos y la adaptabilidad a nuevas y cambiantes formas de amenazas de inteligencia (Acuff, 2022). Esta evaluación puede realizarse mediante métricas específicas, como el número de incidentes detectados y neutralizados, el tiempo de respuesta ante una amenaza, la tasa de éxito en la protección de activos críticos y la satisfacción del personal con los procedimientos de contrainteligencia.

2.2.1.3 Teorías

Teoría de la Seguridad Nacional: Esta teoría sostiene que la seguridad de un Estado es fundamental para su supervivencia y desarrollo, y que las medidas de contrainteligencia son esenciales para proteger los intereses nacionales y preservar la soberanía. En el contexto militar, la contrainteligencia se considera un componente crucial de la seguridad nacional, destinado a salvaguardar la integridad y los activos de la nación frente a amenazas internas y externas (Cabrera, 2021).

Teoría de la Guerra Asimétrica: Esta teoría sugiere que en conflictos donde una parte tiene una ventaja militar significativa, la contrainteligencia puede ser utilizada por la parte más débil para nivelar el campo de juego y aumentar su capacidad de resistencia. En este sentido, las medidas de contrainteligencia pueden ser una herramienta importante para contrarrestar las estrategias de superioridad militar de un adversario más fuerte (Checa, 2020).

Teoría de la Disuasión: Según esta teoría, las medidas de contrainteligencia pueden contribuir a disuadir a los adversarios de emprender acciones hostiles al demostrar la capacidad de detectar y neutralizar amenazas de inteligencia adversa. La efectividad de la contrainteligencia en este sentido radica en su capacidad para hacer que el costo y el riesgo de emprender actividades hostiles superen los beneficios esperados para el adversario (Acuff, 2022).

Teoría de la Gestión de Riesgos: Esta teoría, aplicada al ámbito de la contrainteligencia, sostiene que las organizaciones deben identificar, evaluar y priorizar los riesgos potenciales de inteligencia adversa para gestionarlos de manera efectiva. Según Lecca et al. (2023), la aplicación de medidas de control interno, como auditorías de seguridad y revisiones periódicas de sistemas, permite reducir la exposición a riesgos de filtración o sabotaje. La gestión de riesgos en contrainteligencia implica no solo la identificación de amenazas, sino también la implementación de estrategias proactivas que minimicen las vulnerabilidades, garantizando que las operaciones militares sean resilientes ante posibles intentos de infiltración.

Teoría de la Defensa en Profundidad: Esta teoría sugiere que las medidas de contrainteligencia deben implementarse en múltiples niveles para proporcionar una defensa integral frente a amenazas de inteligencia. Hernández y Mendoza (2020) describen cómo una estrategia de defensa en profundidad abarca la seguridad física, la protección de la información, la ciberseguridad y el control del personal, todo en conjunto para ofrecer una red de protección que dificulta las actividades hostiles. En este contexto, cada nivel de seguridad está diseñado para respaldar y fortalecer a los demás, de modo que, si una capa es comprometida, las demás continúan funcionando como una barrera efectiva contra los ataques.

Teoría de la Confianza y Supervisión: Según Hernández et al. (2022), la cultura organizacional es clave para la efectividad de las medidas de contrainteligencia. Esta teoría sostiene que la creación de una cultura de seguridad depende de establecer mecanismos de confianza entre el personal, junto con una supervisión adecuada para garantizar que todos los

miembros de la organización sean conscientes de sus responsabilidades en cuanto a la protección de la información y los activos críticos. La combinación de confianza y control garantiza que las medidas de contrainteligencia no solo se apliquen a nivel estructural, sino que también sean parte integral de las prácticas diarias de todos los miembros de la organización

2.2.1.4 Dimensionamiento

Dimensión 1: Eficacia

Según Quintero (2020), sostiene que la eficacia se refiere a la capacidad de lograr los resultados deseados de manera exitosa, cumpliendo con los objetivos establecidos. En el contexto del contraterrorismo, la eficacia implica que las medidas y acciones implementadas sean efectivas para prevenir, detectar, neutralizar y responder a amenazas terroristas de manera adecuada y oportuna. Una estrategia, política o programa se considera eficaz si logra sus metas y objetivos de manera satisfactoria, contribuyendo así a mejorar la seguridad y proteger a la población contra posibles ataques terroristas. En resumen, la eficacia en el contraterrorismo se relaciona con la capacidad de las medidas implementadas para cumplir con su propósito y generar resultados positivos en la lucha contra el terrorismo.

Dimensión 2: Actualización tecnológica

Evaluar la infraestructura tecnológica utilizada en las operaciones contraterroristas es fundamental para garantizar su eficacia. Esto incluye sistemas de vigilancia avanzados, análisis de datos en tiempo real, herramientas de detección de explosivos y armas, así como tecnologías de comunicación seguras (Rodríguez y Núñez, 2021). El dimensionamiento de esta dimensión implica determinar si las tecnologías utilizadas están actualizadas, son adecuadas para las necesidades actuales y permiten una respuesta rápida y precisa ante amenazas terroristas. Además, se deben considerar inversiones en investigación y desarrollo de nuevas tecnologías adaptadas a las amenazas emergentes. Es importante también evaluar la interoperabilidad de los sistemas tecnológicos utilizados para asegurar una comunicación efectiva entre las diferentes agencias y unidades involucradas en las operaciones contraterroristas (Rodríguez y Núñez, 2021).

Dimensión 3: Capacitación

Según Hernández et al. (2022) la capacitación del personal encargado de las operaciones contraterroristas es esencial para garantizar su eficacia. Esto incluye tanto a las

fuerzas de seguridad como a otros actores relevantes, como personal militar, agentes de inteligencia, equipos de respuesta rápida y personal de emergencia. El dimensionamiento de esta dimensión implica evaluar la calidad y frecuencia de la capacitación proporcionada, así como la adecuación de los programas de formación a las necesidades específicas del contexto y las amenazas terroristas identificadas. Además, es importante realizar ejercicios y simulacros periódicos para mantener las habilidades y la preparación del personal en situaciones de crisis. Se debe fomentar también la formación interdisciplinaria y el trabajo en equipo entre diferentes unidades y agencias para mejorar la coordinación y la eficacia de las operaciones contraterroristas.

2.2.2. Base teórica de la variable de estudio 2: Seguridad de las Instalaciones

2.2.2.1 Definición

La seguridad de las instalaciones, según Ávila (2016), se define como el conjunto de medidas, políticas y procedimientos destinados a proteger físicamente un lugar específico contra una variedad de amenazas, tanto internas como externas, que podrían comprometer su integridad, funcionamiento o los activos que alberga. Estas medidas incluyen, pero no se limitan a, protocolos de control de acceso, sistemas de vigilancia, dispositivos de detección de intrusiones y controles de seguridad. Su objetivo es prevenir, disuadir, detectar y responder a incidentes adversos como robos, vandalismo, sabotajes, ataques terroristas, incendios y desastres naturales (Elías, 2021).

Un aspecto clave en la seguridad de las instalaciones es la planificación integral, que implica evaluar las posibles vulnerabilidades de una infraestructura en términos de su ubicación, acceso y diseño, así como la implementación de barreras físicas y tecnológicas que mitiguen estos riesgos. Según Jiménez y López (2023), la integración de la ciberseguridad y la seguridad física ha cobrado relevancia en los últimos años, dado que los sistemas automatizados y los dispositivos conectados a redes internas también representan puntos de vulnerabilidad.

La seguridad en el ámbito digital se ha vuelto crítica en instalaciones que dependen de infraestructuras tecnológicas. Según Lecca et al. (2023), la creciente digitalización de los sistemas de control en infraestructuras críticas, como plantas de energía, instalaciones militares o grandes empresas industriales, ha generado la necesidad de incorporar un enfoque dual que combine la seguridad física con la ciberseguridad. La fusión de estas dos áreas permite una

protección más robusta y garantiza la continuidad operativa, protegiendo tanto los datos como los sistemas automatizados de posibles intrusiones cibernéticas y sabotajes.

La seguridad de las personas es otro aspecto fundamental dentro de este contexto. Martínez (2022) subraya que, en sectores como el militar, industrial y empresarial, la protección no solo se centra en los activos físicos o tecnológicos, sino también en las personas que operan y supervisan estas instalaciones. Las medidas de seguridad de las instalaciones deben garantizar que el personal esté capacitado para identificar y reaccionar ante amenazas, mediante simulacros y protocolos de respuesta ante emergencias, minimizando el riesgo tanto para los individuos como para la operación en general.

Además, Pozo (2022) señala que la seguridad de las instalaciones no puede ser vista de manera aislada, sino como parte de un sistema más amplio de seguridad integral que incluye la seguridad física, cibernética y organizacional. Esto implica la adopción de políticas y normativas que regulen el acceso, el manejo de información sensible y el uso de tecnología para prevenir posibles ataques o fallos operativos. En su investigación, Pozo destaca cómo el Estado ecuatoriano ha implementado medidas de ciberseguridad en instalaciones críticas, fortaleciendo tanto las barreras digitales como los sistemas de control físico. Por último, Martínez (2022) resalta la necesidad de una actualización constante en las estrategias de seguridad de las instalaciones debido a la evolución constante de las amenazas, que van desde ataques físicos hasta amenazas cibernéticas complejas. La combinación de enfoques innovadores en seguridad, como la inteligencia artificial para la detección de intrusiones, y tecnologías avanzadas para la protección perimetral, asegura una protección más efectiva de las infraestructuras críticas y los activos estratégicos.

2.2.2.2 Medición

La medición de la seguridad de las instalaciones implica un enfoque integral que evalúa diversos aspectos relacionados con la efectividad y robustez de las medidas de seguridad implementadas. Esto incluye la utilización de métricas cuantitativas y cualitativas para evaluar el desempeño y la eficacia de los sistemas de seguridad en lugar de simplemente contar con un número determinado de medidas de seguridad. Algunas medidas de medición comunes pueden incluir:

Índices de Incidentes: Se refiere a la recopilación y análisis de datos sobre incidentes de seguridad ocurridos en la instalación, como robos, intrusiones, vandalismo, entre otros.

Estos datos permiten identificar tendencias, áreas de vulnerabilidad y evaluar la efectividad de las medidas de seguridad existentes (Flórez, 2022).

Evaluaciones de Riesgos y Vulnerabilidades: Consiste en realizar evaluaciones periódicas para identificar posibles amenazas, vulnerabilidades y riesgos que podrían afectar la seguridad de la instalación. Estas evaluaciones ayudan a priorizar acciones y asignar recursos de manera eficiente para mitigar los riesgos identificados (Carreño et al., 2005).

Auditorías de Seguridad: Implica llevar a cabo auditorías regulares para revisar y evaluar el cumplimiento de los procedimientos de seguridad, políticas y estándares establecidos. Las auditorías pueden identificar áreas de mejora, asegurar el cumplimiento normativo y garantizar la eficacia de los controles de seguridad (Davalos, 2013).

Indicadores de Desempeño: Se refiere al establecimiento de indicadores clave de desempeño (KPIs) relacionados con la seguridad, como el tiempo de respuesta ante emergencias, la tasa de falsas alarmas, la efectividad de los controles de acceso, entre otros. Estos KPIs permiten monitorear el rendimiento de los sistemas de seguridad y tomar medidas correctivas cuando sea necesario (Saavedra, 2022).

Encuestas de Satisfacción del Personal: Consiste en recopilar retroalimentación del personal que trabaja en la instalación para evaluar su percepción sobre la seguridad y los procedimientos implementados. Estas encuestas pueden proporcionar información valiosa sobre áreas de mejora y posibles problemas no identificados mediante otras métricas (Govea y Zuñiga, 2020).

2.2.2.3 Teorías

Las teorías relacionadas con la seguridad de las instalaciones ofrecen perspectivas fundamentales para comprender los principios y enfoques que sustentan la protección de los entornos físicos. Algunas teorías significativas en este ámbito incluyen:

Teoría de la disuasión: Para Piella (2020) esta teoría postula que la visibilidad y la percepción de medidas de seguridad efectivas disuaden a los posibles delincuentes o perpetradores de cometer actos delictivos. Al hacer que el riesgo de ser detectados o capturados sea más alto, se espera que los individuos potencialmente peligrosos sean menos propensos a realizar actividades ilícitas. La disuasión se logra mediante la implementación de medidas de

seguridad visibles, como cámaras de vigilancia, sistemas de alarma y presencia de personal de seguridad, lo que crea un entorno menos propicio para el comportamiento delictivo.

Teoría de la defensa en profundidad: Esta teoría propone la implementación de múltiples capas de protección para asegurar una instalación, en lugar de confiar en una única medida de seguridad. La defensa en profundidad implica la integración de varias medidas, como controles de acceso, sistemas de vigilancia, alarmas, y patrullas de seguridad, que se complementan y refuerzan entre sí. El objetivo es que, si una capa falla, otras estén presentes para prevenir o mitigar cualquier intrusión o amenaza (Briceño, 2021).

Teoría de la gestión de riesgos: Esta teoría se enfoca en identificar, evaluar y gestionar los riesgos relacionados con la seguridad de instalaciones. Propone un enfoque proactivo para detectar vulnerabilidades, evaluar la probabilidad e impacto de los riesgos, y tomar acciones para reducirlos a un nivel aceptable. La gestión de riesgos abarca medidas preventivas, correctivas y de contingencia para proteger los activos y asegurar la continuidad de las operaciones en caso de incidentes (Tamayo et al., 2020).

Estas teorías proporcionan marcos conceptuales importantes para el diseño, la implementación y la evaluación de estrategias de seguridad de instalaciones, ofreciendo una comprensión más profunda de los principios y enfoques que sustentan la protección efectiva de entornos físicos contra amenazas potenciales.

2.2.2.4 Dimensionamiento

Dentro del contexto de la tesis sobre "Medidas de Contrainteligencia y Seguridad de las Instalaciones en Cadetes de la EMCH 'Coronel Francisco Bolognesi' – 2024", el dimensionamiento de las tres dimensiones principales de seguridad de las instalaciones se enriquecería con un análisis detallado de cada aspecto. A continuación, se amplía la información sobre cada dimensión:

Seguridad Física: En el contexto de la EMCH “CFB”, la seguridad física abarca una serie de medidas concretas diseñadas para proteger las instalaciones militares contra amenazas externas. Según Montejo (2013) esto puede incluir la evaluación de la efectividad de las barreras físicas, como las cercas perimetrales y las puertas de acceso controlado, así como la distribución de puntos de control y la visibilidad de la seguridad. Además, se consideraría la presencia de elementos disuasorios, como la iluminación adecuada y la señalización de

seguridad. También se analizarían las prácticas de patrullaje y vigilancia, junto con la disponibilidad de personal de seguridad y la capacidad de respuesta a emergencias físicas.

Seguridad Tecnológica: La seguridad tecnológica se centra en el uso de sistemas y dispositivos avanzados para fortalecer la protección de las instalaciones. En el caso de la EMCH “CFB” "Coronel Francisco Bolognesi", esto podría involucrar la evaluación de la infraestructura de seguridad electrónica, incluidos sistemas de video vigilancia, sensores de movimiento, sistemas de alarma y controles de acceso basados en tecnología biométrica o tarjetas de identificación. Además, se analizaría la integración y la interoperabilidad de estos sistemas, así como su capacidad para proporcionar alertas tempranas y respuestas rápidas ante posibles amenazas.

Seguridad de la Información: Según Ramos y Hurtado (2017), la seguridad de la información consiste en proteger los datos y sistemas informáticos de una institución frente a amenazas cibernéticas y accesos no autorizados. En el caso de la EMCH “CFB”, esto implicaría evaluar la solidez de las medidas de seguridad de la red, los sistemas de información críticos y la protección de datos sensibles. Entre las acciones consideradas estarían la implementación de cortafuegos, sistemas de detección de intrusiones, políticas de gestión de contraseñas y programas de concientización sobre seguridad informática para el personal. Asimismo, se analizarían los procedimientos de respaldo y recuperación de datos, así como la capacidad de respuesta ante incidentes de seguridad cibernética.

Al profundizar en cada dimensión, se obtendría una comprensión más completa de la seguridad de las instalaciones en la EMCH “CFB” lo que permitiría identificar áreas de fortaleza y posibles vulnerabilidades para mejorar la protección integral de la institución militar y sus activos.

2.3. Marco conceptual

2.3.1. Medidas de contrainteligencia

A. Inteligencia de amenazas

La inteligencia de amenazas se refiere al proceso de recopilación, análisis y evaluación de información sobre posibles amenazas y adversarios, con el fin de comprender sus capacidades, intenciones y estrategias. Esta información resulta clave para anticipar y reducir

los riesgos de seguridad, facilitando la toma de decisiones basadas en datos y la implementación de medidas preventivas eficaces. Esto no solo fortalece la protección de los activos de la institución, sino que también garantiza una respuesta proactiva ante posibles amenazas (Castillo, 2020).

B. Análisis de riesgos

El análisis de riesgos consiste en identificar, evaluar y priorizar los riesgos potenciales que podrían comprometer la seguridad de las instalaciones militares. Este proceso permite entender la probabilidad y el impacto de posibles eventos adversos, lo que facilita la implementación de medidas adecuadas para mitigar o gestionar dichos riesgos de forma eficiente (Castillo, 2020).

C. Contramedidas de seguridad

Las contramedidas de seguridad son las acciones o medidas implementadas para contrarrestar o neutralizar las amenazas identificadas. Estas contramedidas pueden incluir controles de acceso, sistemas de vigilancia, protocolos de seguridad física y tecnológica, entre otros, diseñados para proteger las instalaciones militares y sus activos contra posibles ataques o intrusiones (Castillo, 2020).

D. Protección de la información

La protección de la información implica la adopción de medidas destinadas a garantizar la confidencialidad, integridad y disponibilidad de datos sensibles y críticos. Estas medidas incluyen el cifrado de información, la gestión adecuada de identidades y accesos, así como la implementación de políticas de seguridad que prevengan el acceso no autorizado o la divulgación de información confidencial (Castillo, 2020).

E. Cultura de seguridad

La cultura de seguridad está vinculada a las actitudes, valores y comportamientos de individuos y organizaciones respecto a la seguridad. Una cultura de seguridad robusta fomenta la conciencia y el compromiso de todos los miembros de la institución militar en la protección de sus instalaciones, impulsando la adopción de buenas prácticas de seguridad en todas las actividades, tanto operativas como administrativas (Castillo, 2020).

F. Resiliencia operativa

La cultura de seguridad se relaciona con las actitudes, valores y conductas de los individuos y organizaciones en torno a la seguridad. Una cultura de seguridad bien establecida refuerza la conciencia y el compromiso de todos los miembros de la institución militar en proteger las instalaciones, promoviendo la implementación de prácticas seguras en todas las actividades, ya sean operativas o administrativas (Duffield, 2020).

G. Evaluación de vulnerabilidades

La evaluación de vulnerabilidades implica la identificación y análisis de las debilidades o puntos críticos en la seguridad de las instalaciones militares. Este proceso permite detectar áreas susceptibles a amenazas, facilitando la implementación de medidas correctivas para fortalecer la protección y reducir los riesgos de posibles ataques o intrusiones. Este proceso permite comprender las posibles brechas de seguridad y los riesgos asociados, facilitando la toma de decisiones para fortalecer la protección y mitigar las vulnerabilidades identificadas (Duffield, 2020).

H. Gestión de crisis

La gestión de crisis se refiere a las acciones y procesos implementados para manejar situaciones de emergencia o crisis de manera efectiva. Esto incluye la coordinación de equipos de respuesta, la comunicación con las partes interesadas y la toma de decisiones bajo presión para minimizar el impacto y restablecer la normalidad lo antes posible (Duffield, 2020).

I. Continuidad del negocio

La continuidad del negocio se refiere a la planificación y preparación necesarias para asegurar que las operaciones y servicios esenciales continúen durante y después de eventos disruptivos. Esto abarca la identificación de funciones críticas, la implementación de planes de recuperación, y la realización de pruebas y ejercicios para garantizar la resiliencia de la organización frente a posibles interrupciones (Martínez, 2022).

J. Ciberseguridad

La ciberseguridad se enfoca en proteger sistemas, redes y datos digitales frente a ataques cibernéticos y amenazas informáticas. Esto abarca la detección y prevención de

intrusiones, la gestión de vulnerabilidades, y la respuesta a incidentes, con el fin de asegurar la integridad y disponibilidad de la información en entornos digitales (Covarrubias y Zadamig, 2020).

2.3.2. Seguridad de instalaciones

A. Control de acceso

El control de acceso se refiere a las medidas y sistemas implementados para regular y gestionar el ingreso a las instalaciones militares, asegurando que solo personas autorizadas tengan acceso a áreas restringidas o activos críticos. Esto puede incluir la utilización de sistemas de identificación, tarjetas de acceso, barreras físicas y controles biométricos (Samaniego y Vergaray, 2020).

B. Seguridad perimetral

La seguridad perimetral implica la protección de los límites físicos de las instalaciones militares, incluyendo vallas, muros, puertas y sistemas de vigilancia para prevenir intrusiones no autorizadas desde el exterior. Esto incluye la implementación de medidas de detección y respuesta para identificar y neutralizar posibles amenazas en la periferia de las instalaciones (Castillo, 2020).

C. Detección y alerta temprana

La detección y alerta temprana se refiere a la capacidad de identificar y notificar rápidamente sobre posibles amenazas o intrusiones, permitiendo una respuesta inmediata y la implementación de contramedidas para minimizar el impacto. Esto puede incluir la utilización de sistemas de vigilancia, sensores de intrusión y alarmas para detectar actividades sospechosas (Martínez, 2022).

D. Gestión de incidentes

La gestión de incidentes implica la respuesta organizada y coordinada ante eventos adversos o incidentes de seguridad, con el objetivo de minimizar el impacto y restaurar la normalidad lo antes posible. Esto incluye la activación de equipos de respuesta, la recolección de información, la evaluación de riesgos y la implementación de acciones correctivas (Martínez, 2022).

E. Interoperabilidad de sistemas de seguridad

La interoperabilidad de sistemas de seguridad se refiere a la capacidad de diferentes sistemas y tecnologías de seguridad para comunicarse, compartir información y colaborar de manera efectiva en la protección de las instalaciones militares. Esto garantiza una respuesta coordinada y sinérgica ante amenazas y eventos adversos (Duffield, 2020).

F. Gestión de identidades y accesos

La gestión de identidades y accesos se refiere al control y administración de las identidades digitales y los privilegios de acceso de los usuarios a los sistemas y datos de la organización. Esto abarca la autenticación de usuarios, la autorización de accesos, y la gestión de credenciales, con el objetivo de garantizar la seguridad de la información y los recursos (Samaniego y Vergaray, 2020).

2.4 Operacionalización de variables

Tabla 1

Operacionalización de variable 1 (medidas de contrainteligencia)

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	ÍTEMS	ESCALA DE MEDICIÓN
Medidas de Contrainteligencia	Según Freire (2021), son las estrategias y acciones adoptadas para detectar, prevenir y neutralizar actividades de espionaje, sabotaje o infiltración por parte de agentes hostiles. Estas medidas protegen la seguridad y los intereses de una organización contra amenazas externas.	La variable "Medidas de Contrainteligencia" será evaluada mediante un instrumento que calificará la efectividad y aplicación de las estrategias y acciones de contrainteligencia dentro de la organización. Los ítems específicos para considerar incluirán la tasa de detección de amenazas, el tiempo de respuesta ante incidentes, la frecuencia de actualización de sistemas, la participación en programas de capacitación, entre otros.	**D1**: Eficacia	Tasa de detección de amenazas.	Nominal tipo Likert
				Tiempo promedio de respuesta ante incidentes.	
				Porcentaje de contramedidas efectivas implementadas	
			D2: Actualización Tecnológica	Frecuencia de actualización de sistemas de seguridad.	
				Implementación de tecnologías de vanguardia en contrainteligencia.	
				Evaluación de la compatibilidad entre los sistemas tecnológicos utilizados y las necesidades de contrainteligencia.	
				Participación del personal en programas de capacitación en contrainteligencia.	
			D3: Capacitación	Evaluación del nivel de competencia adquirido por el personal en técnicas de contrainteligencia.	
				Retroalimentación y mejora continua de los programas de capacitación en contrainteligencia	

Tabla 2

Operacionalización de variable 2 (seguridad de instalaciones)

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	ITEMS	ESCALA DE MEDICIÓN
Seguridad de Instalaciones	Zalewski (2022), sostiene que la seguridad de instalaciones se centra en las medidas y recursos destinados a proteger físicamente un lugar contra amenazas que puedan poner en peligro a las personas, activos y operaciones en ese espacio.	La definición operacional de la seguridad de instalaciones, basada en Zalewski (2022), implica la implementación y el mantenimiento de medidas y recursos con el fin de proteger físicamente un lugar específico contra una amplia gama de amenazas que puedan comprometer la seguridad de las personas, los activos y las operaciones en ese entorno. Esto se traduce en la ejecución de acciones concretas, como la instalación de sistemas de seguridad física, como cercas, cámaras de vigilancia y controles de acceso; la implementación de procedimientos de seguridad, como patrullas de seguridad y protocolos de respuesta a emergencias; y el establecimiento de políticas y prácticas organizacionales destinadas a salvaguardar la integridad de las instalaciones.	**D1**: Seguridad Física	Control de acceso	Nominal tipo Likert
				Vigilancia perimetral	
				Iluminación adecuada	
			D2: Seguridad Tecnológica	Firewall y antivirus	
				Monitoreo de redes	
				Respaldos regulares	
				Políticas de acceso	
				Encriptación de datos	
			D3: Seguridad de Información	Concienciación del personal	

2.5 Formulación de la hipótesis

2.5.1 Hipótesis general

Existe relación entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

2.5.2 Hipótesis específicas

Hipótesis específica 01:

Existe relación entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

Hipótesis específica 02:

Existe relación entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

Hipótesis específica 03:

Existe relación entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de investigación

La investigación se basó en el método cuantitativo, el cual siguió una estructura secuencial y probatoria con etapas bien definidas. Comenzó con la formulación del problema, seguida por la definición de los objetivos y preguntas de investigación, lo que permitió desarrollar las hipótesis y variables que serían medidas y analizadas mediante un enfoque estadístico. El propósito del método cuantitativo fue identificar patrones de comportamiento y validar teorías a través de la recopilación de datos, su cuantificación numérica y el análisis estadístico (Hernández y Mendoza, 2020).

3.2. Tipo de investigación

La investigación se realizó de carácter básico, reconocida por su naturaleza fundamental, esencial y pura. Su objetivo fue generar conocimiento, validar, fundamentar o modificar teorías y establecer nuevos conocimientos. Para alcanzar este propósito, observó y recopiló información de la realidad problemática, analizó los datos relacionados con las variables y determinó la validez de las hipótesis planteadas. Una vez comprobadas, estas hipótesis se integraron al nuevo conocimiento científico. Cabe destacar que este tipo de investigación no persiguió fines económicos, ya que su objetivo principal fue aumentar significativamente los conocimientos científicos sin buscar su aplicación práctica (Ñaupas et al., 2023).

3.3. Método de investigación

El estudio se desarrolló bajo un enfoque cuantitativo, empleando el método hipotético-deductivo como marco principal de investigación. Este método implicó la formulación de hipótesis basadas en teorías previas, las cuales fueron sometidas a pruebas empíricas mediante la recolección de datos. Para ello, se utilizaron técnicas formales y herramientas estadísticas avanzadas que permitieron no solo la recopilación rigurosa de datos, sino también su análisis detallado. El proceso de análisis estuvo orientado a identificar y cuantificar las relaciones de causa y efecto entre las variables clave, permitiendo así determinar cuáles de ellas tuvieron un mayor impacto en el fenómeno bajo estudio. Además, este enfoque permitió generar conclusiones generalizables que contribuyeron al conocimiento científico y a la toma de decisiones informadas en el área específica de investigación (Bernal, 2023).

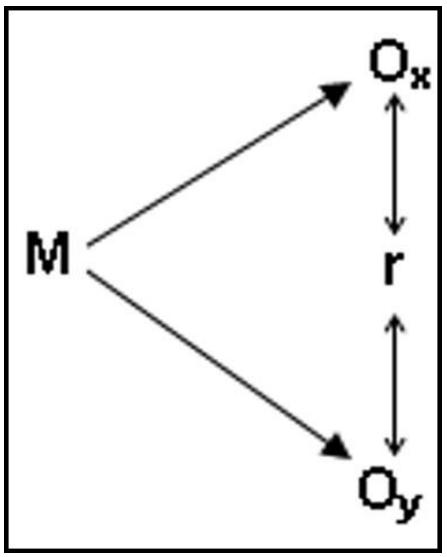
3.4. Alcance de investigación

El estudio adoptó un enfoque descriptivo-correlacional, que permitió explorar y caracterizar las posibles relaciones o asociaciones entre dos o más variables clave en el contexto del uso de simuladores de combate para fortalecer las medidas de contrainteligencia y seguridad en las instalaciones de la Escuela Militar. Este enfoque no solo se enfocó en la descripción detallada de las variables, sino también en la evaluación de la magnitud y dirección de las relaciones entre ellas.

Mediante el uso de técnicas estadísticas correlacionales, se buscó identificar patrones y tendencias que pudieran indicar cómo la implementación de simuladores de combate influyó en la eficacia de las estrategias de contrainteligencia y seguridad. Además, el estudio consideró variables contextuales que pudieran moderar o mediar estas relaciones, ofreciendo una visión integral que contribuyó al desarrollo de políticas y prácticas más efectivas dentro del ámbito militar (Hernández y Mendoza, 2020).

Figura 1

Esquema del diseño de investigación.



Donde:

M = Muestra

Ox = Variable 1: Medidas de Contrainteligencia.

Oy = Variable 2: Seguridad de Instalaciones.

r = Relación entre las variables de estudio

3.5. Diseño de la investigación

La investigación siguió un diseño no experimental, lo que significó que no se manipularon las variables, sino que se observaron y analizaron las relaciones entre ellas. De acuerdo con Hernández y Mendoza (2020), en un estudio cuantitativo, las variables se miden y se estudia su relación. El nivel de la investigación fue descriptivo, ya que se evaluó el conocimiento de los cadetes en función de las dimensiones propuestas para el proyecto. En resumen, se examinó la relación entre variables de manera descriptiva, sin intervención experimental.

3.6. Población, muestra y unidad de estudio

3.6.1. Población

La población estudiada en esta investigación estuvo compuesta por los cadetes de cuarto año de la EMCH “CFB”. Este grupo específico incluyó a estudiantes en etapas avanzadas de su formación militar, quienes habían sido instruidos en conceptos relacionados con la inteligencia, lo que representó una muestra significativa de aquellos que habían superado la fase inicial de su entrenamiento.

La selección de este grado se basó en la premisa de que los cadetes de cuarto año poseían un conocimiento y experiencia considerables en tácticas y técnicas de inteligencia de combate, lo que permitió una evaluación más precisa de la efectividad de las medidas de contrainteligencia y seguridad en las instalaciones. Esta población fue clave para comprender en profundidad los impactos y beneficios de la metodología propuesta en la tesis.

Tabla 3

Población.

AÑO DE ESTUDIO	CANTIDAD
INFANTERÍA	84
CABALLERÍA	29
ARTILLERÍA	31
INGENIERÍA	22
COMUNICACIONES	19
INTELIGENCIA	13
MATERIAL DE GUERRA	11
INTENDENCIA	11
TOTAL	220

Nota: Información obtenida de la sección personal de la compañía de cuarto año.

3.6.2. Muestra

En el estudio titulado "Medidas de Contrainteligencia y Seguridad de las Instalaciones en Cadetes de la EMCH 'CFB' – 2024", se utilizó un muestreo probabilístico tipo intencionado. Este tipo de muestreo, aunque probabilístico, se caracterizó por la selección deliberada de subgrupos específicos dentro de la población total, asegurando que todas las categorías relevantes estuvieran representadas en la muestra (Hernández y Mendoza, 2020).

La población total constó de 220 cadetes distribuidos en las siguientes especialidades: Infantería (84 cadetes), Caballería (29 cadetes), Artillería (31 cadetes), Ingeniería (22 cadetes), Comunicaciones (19 cadetes), Inteligencia (13 cadetes), Material de Guerra (11 cadetes) e Intendencia (11 cadetes).

Se tomó una muestra del 50% de la población total, lo que permitió obtener una representación más robusta y precisa de cada subgrupo, dado que se esperaba que existieran diferencias significativas entre las especialidades en cuanto a las medidas de contrainteligencia y seguridad. La fórmula para calcular el tamaño de la muestra para cada subgrupo fue utilizada según lo propuesto por Hernández y Mendoza (2020).

$$n_i = \frac{N_i}{N} \times n$$

Donde:

n_i = Tamaño de la muestra para el subgrupo i.

N_i = Tamaño de la población para el subgrupo i.

N= Tamaño de la población total (220 cadetes)

N = Tamaño de la muestra total a seleccionar.

El cálculo para el 50% de la población total es:

$n = 220 \times 0.50 = 110$

De acuerdo con el muestreo probabilístico tipo intencionado; los tamaños muestrales para cada subgrupo fueron:

Infantería: n1 = 84 / 220 × 110 = 42
Caballería: n2 = 29 / 220 × 110 = 14
Artillería: n3 = 31 / 220 × 110 = 15
Ingeniería: n4 = 22 / 220 × 110 = 11
Comunicaciones: n5 = 19 / 220 × 110 =10
Inteligencia: n6 = 13 / 220 × 110 = 6
Material de Guerra: n7 = 11 / 220 × 110 = 6
Intendencia: n8 = 11 / 220 × 110 = 6

De esta manera, la muestra total está compuesta por 110 cadetes, distribuidos de acuerdo con las proporciones de cada subgrupo. Este enfoque asegura una representación adecuada de todas las especialidades, proporcionando una base sólida para el análisis detallado de las medidas de contrainteligencia y seguridad en la EMCH "CFB". Con un tamaño de muestra del 50% aproximadamente, se garantiza una mayor precisión y representatividad en los resultados obtenidos.

3.7. *Técnica e instrumento para la recolección de datos*

3.7.1. Técnica de recolección de datos

La recolección de datos en esta investigación, según Hernández y Mendoza (2020), se realizó principalmente mediante encuestas. Se diseñaron encuestas estructuradas que fueron administradas a los cadetes de cuarto año de la EMCH "CFB". Estas encuestas contenían

preguntas cerradas que abordaban aspectos específicos relacionados con la importancia de la contrainteligencia y la seguridad de las instalaciones en el contexto de la escuela militar.

Las preguntas fueron formuladas para evaluar la percepción de los cadetes sobre la efectividad de esta metodología, identificar posibles áreas de mejora y recopilar datos demográficos relevantes. La aplicación de estas encuestas permitió obtener datos cuantitativos que respaldaron de manera sólida el análisis de la importancia de los simuladores de combate en la formación militar de los cadetes de la Escuela Militar de Chorrillos.

3.7.2 *Instrumento de recolección de datos*

La recolección de datos se realizó mediante cuestionarios, utilizando una escala ordinal para las variables, dado que esta ofrece características como utilidad, versatilidad, objetividad y simplicidad (Robles, 2023). En este contexto, se aplicó una encuesta para identificar el nivel de conocimiento que poseían los cadetes encuestados respecto a la contrainteligencia y la seguridad de las instalaciones.

Este cuestionario tuvo la siguiente estructura:

Tabla 4

Escala de Likert.

Alternativas según Likert	
1	Muy en desacuerdo
2	Algo en desacuerdo
3	Ni de Acuerdo Ni en desacuerdo
4	Algo de acuerdo
5	Muy de acuerdo

3.7.3 Validez - confiabilidad de instrumentos de medición

La validez y la confiabilidad de un instrumento de medición fueron esenciales para garantizar que los resultados reflejaran con precisión lo que se pretendía evaluar. La validez se refirió a la capacidad del instrumento para medir correctamente el nivel de conocimientos en contrainteligencia y seguridad de las instalaciones, asegurando que las preguntas cubrieran de manera adecuada todos los aspectos relevantes del tema. La validez de contenido fue clave, pues aseguró que el cuestionario abordara todos los puntos críticos. Si bien fue importante medir conocimientos generales, también lo fue incluir preguntas que diferenciaron a los cadetes

con un conocimiento más profundo. La validez de constructo y de criterio también jugaron un rol importante, ya que verificaron que el cuestionario midiera correctamente los conceptos teóricos y que sus resultados se relacionaran con el desempeño real de los cadetes en situaciones prácticas (Hernández y Mendoza, 2020).

Por otro lado, la confiabilidad del instrumento se refirió a su consistencia al aplicarse en diferentes momentos o por diferentes evaluadores. Un cuestionario confiable debía arrojar resultados similares si se aplicaba en las mismas condiciones o si era evaluado por diferentes personas. En este contexto, si los cadetes tenían un nivel homogéneo de conocimientos, la confiabilidad podría ser alta, ya que los resultados serían más uniformes. Sin embargo, si las preguntas no capturaban diferencias sutiles en el nivel de conocimiento, esto podría limitar la utilidad del instrumento para discriminar entre los diferentes niveles de competencia entre los cadetes (Hernández y Mendoza, 2020).

3.8. Procesamiento y método de análisis de datos

3.8.1. Técnica para el procesamiento de datos

Para el procesamiento y análisis de los datos recopilados mediante las encuestas, se implementó la técnica de procesamiento batch debido a su eficacia en el manejo de grandes volúmenes de información. Inicialmente, se realizó un análisis descriptivo utilizando herramientas estadísticas para examinar las frecuencias y distribuciones de las respuestas cuantitativas, lo que proporcionó una visión general de las percepciones y experiencias de los cadetes. Posteriormente, se aplicaron métodos cuantitativos y pruebas de correlación para identificar posibles relaciones y patrones entre las variables de interés.

Además, se emplearon herramientas especializadas de software estadístico para facilitar la presentación visual y mejorar la comprensión de los resultados, lo que contribuyó a la validez y robustez de las conclusiones obtenidas en el estudio.

3.8.2. Método de análisis de datos

Análisis descriptivo. Se llevó a cabo un análisis descriptivo con el objetivo de presentar los resultados de las encuestas de manera clara y precisa, evitando ambigüedades. Se buscó destacar las preferencias expresadas por los encuestados, detallando minuciosamente las tendencias identificadas. Este análisis fue fundamental para proporcionar una visión

inequívoca de las percepciones y opiniones de los cadetes con respecto a la contrainteligencia y la seguridad de las instalaciones. La información detallada resultante fue utilizada como referencia principal al comunicar las conclusiones y recomendaciones derivadas del estudio a las autoridades pertinentes, con el objetivo de respaldar de manera sólida y fundamentada las decisiones que puedan derivarse de la investigación (Sanchez y Reyes, 2023).

Análisis inferencial. En esta fase de análisis, se procedió a verificar las hipótesis mediante el uso de estadísticos estandarizados, con énfasis en la correlación de Spearman. Esta técnica permitirá evaluar la relación entre variables y determinar la significancia estadística de las asociaciones identificadas. La elección de la correlación de Spearman se basó en su capacidad para analizar relaciones no lineales y su robustez frente a datos atípicos.

Este enfoque estadístico brindó una comprensión más profunda de la posible dependencia entre diferentes aspectos evaluados en la investigación. Los resultados obtenidos de este análisis inferencial constituyeron una contribución valiosa para respaldar conclusiones más sólidas y respuestas a las preguntas de investigación planteadas, fortaleciendo la fundamentación de las recomendaciones derivadas del estudio.

3.9. Aspectos éticos

El juicio de expertos se realizó con la participación de profesionales altamente calificados, con amplia experiencia y profundo conocimiento en el ámbito temático de la investigación. Estos expertos fueron seleccionados cuidadosamente por su destacada trayectoria y habilidades especializadas, lo que aportó un valor significativo al contexto del estudio. Su intervención en el proceso de evaluación y juicio proporcionó una perspectiva valiosa y rigurosa, enriqueciendo la calidad y confiabilidad de los resultados obtenidos. La inclusión de expertos de alto nivel garantizó un análisis robusto y fundamentado, contribuyendo de manera significativa a la validez y solidez de las conclusiones y recomendaciones de la investigación.

Queremos resaltar que nuestro trabajo fue completamente original, abordando un tema poco explorado hasta el momento. Esta elección se hizo con el propósito de generar un mayor interés en la capacitación en inteligencia, promoviendo un ambiente laboral más enriquecedor basado en el respeto mutuo. Nos dedicamos con constancia y disciplina para crear un impacto

positivo en la formación de los futuros egresados, buscando que cada práctica contribuyera al bien común y fomentara un entorno profesional caracterizado por la justicia y la transparencia. A través de mejoras en la capacitación, aspiramos a que los participantes alcanzaran sus objetivos de manera más eficiente y ética.

CAPÍTULO IV.

RESULTADOS

4.1. Análisis descriptivo

El análisis descriptivo de los resultados de esta investigación tiene como objetivo principal ofrecer una visión clara sobre la implementación y efectividad de las medidas de contrainteligencia y seguridad en la EMCH “CFB” durante 2024. A través de la recopilación de datos mediante encuestas y entrevistas, se explora la percepción de los cadetes en relación con los protocolos de seguridad, su conocimiento sobre las medidas vigentes y su evaluación de la eficacia de estas. Este enfoque descriptivo permite identificar patrones y tendencias en áreas clave como el control de accesos, los sistemas de vigilancia, la protección de la información sensible y la capacitación en seguridad.

4.1.1 Resultados sobre el nivel de la Variable 1: Medidas de Contrainteligencia

Tabla 5

Nivel de la Variable 1: Medidas de Contrainteligencia.

Nivel	Frecuencia	Porcentaje
Bajo	50	44%
Medio	25	22%
Alto	38	34%
Total	**113**	**100%**

La Tabla 5 refleja que el 44% de los encuestados considera que las medidas de contrainteligencia en la EMCH “CFB” están en un nivel bajo, lo que indica una preocupación significativa sobre la efectividad de los protocolos actuales. Esta percepción de ineficacia por parte de casi la mitad de los cadetes sugiere que las medidas implementadas no están cumpliendo con las expectativas de seguridad necesarias para proteger la información y las instalaciones. Este grupo podría estar experimentando fallas en la capacitación, lagunas en los controles de acceso o vulnerabilidades tecnológicas que afectan su confianza en las estrategias vigentes.

Por otro lado, un 22% percibe las medidas de contrainteligencia como de nivel medio, lo que sugiere que las consideran parcialmente efectivas, aunque con margen de mejora. Mientras tanto, un 34% las evalúa como de nivel alto, lo que indica que, para un grupo

considerable de cadetes, los protocolos de seguridad son satisfactorios.

4.1.2 Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones

Tabla 6

Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones.

Nivel	Frecuencia	Porcentaje
Bajo	42	37%
Medio	31	27%
Alto	40	35%
Total	113	100%

Los resultados de la Tabla 6 proporcionan información sobre el nivel percibido de seguridad en las instalaciones de la EMCH “CFB”. Un 37% de los cadetes considera que el nivel de seguridad es bajo, lo que sugiere que una proporción significativa de los encuestados percibe que las instalaciones no cuentan con las medidas adecuadas para protegerse de amenazas potenciales. Esto podría estar relacionado con deficiencias en la infraestructura física, en los sistemas de vigilancia o en los protocolos de control de acceso, lo que pone de manifiesto la necesidad de una revisión integral de los mecanismos de seguridad. Además, un 27% de los encuestados evalúa la seguridad como media, lo que indica que algunos aspectos de las medidas de protección son adecuados, pero que aún quedan áreas por mejorar para garantizar un entorno completamente seguro.

Por otro lado, un 35% de los cadetes percibe la seguridad de las instalaciones como alta, lo que muestra que una parte significativa de los encuestados tiene una percepción positiva de las medidas implementadas. Sin embargo, el hecho de que el 64% de los cadetes clasifique el nivel de seguridad como bajo o medio sugiere que aún hay trabajo por hacer para mejorar la seguridad general en las instalaciones.

4.1.3 *Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones*, Dimensión 1 (Seguridad Física)

Tabla 7

Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones.

Nivel	Frecuencia	Porcentaje
Bajo	42	37%
Medio	31	27%
Alto	40	35%
Total	113	100%

Los resultados de la Tabla 7 muestran la percepción de los cadetes sobre el nivel de seguridad física en las instalaciones de la EMCH “CFB”. Un 37% de los encuestados considera que el nivel de seguridad física es bajo, lo que revela que una porción significativa de los cadetes percibe deficiencias en aspectos clave como la protección del perímetro, el control de accesos o la vigilancia en áreas críticas de la instalación. Esta percepción puede indicar vulnerabilidades en la infraestructura o en la implementación de barreras físicas que podrían exponer las instalaciones a riesgos de seguridad. Además, un 27% evalúa la seguridad física como media, lo que sugiere que, aunque existen ciertas medidas, estas no son suficientes para ofrecer una protección integral.

Por otra parte, un 35% de los cadetes califica la seguridad física como alta, lo que muestra que un porcentaje considerable de los encuestados valora positivamente las medidas implementadas para la protección física de las instalaciones. Sin embargo, la combinación de un 64% que percibe un nivel bajo o medio de seguridad física indica la necesidad de reforzar aspectos fundamentales, como el mantenimiento de barreras físicas, la mejora de los sistemas de monitoreo y la implementación de controles de acceso más rigurosos.

4.1.4 *Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones*, Dimensión 2 (Seguridad Tecnológica)

Tabla 8

Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones, Dimensión 2 (Seguridad Tecnológica).

Nivel	Frecuencia	Porcentaje
Bajo	43	38%
Medio	30	27%
Alto	40	35%
Total	113	100%

Los resultados de la Tabla 8 revelan la percepción de los cadetes sobre el nivel de seguridad tecnológica en las instalaciones de la EMCH “CFB”. Un 38% de los encuestados considera que el nivel de seguridad tecnológica es bajo, lo que indica que una gran parte de los cadetes percibe que las tecnologías utilizadas para proteger las instalaciones, como sistemas de vigilancia, detección de intrusos o seguridad informática, no son lo suficientemente robustas o modernas para enfrentar las amenazas actuales. Esta percepción podría estar relacionada con la falta de inversión en tecnología avanzada o con el mantenimiento inadecuado de los sistemas ya instalados, lo que pone en evidencia áreas críticas que requieren mejoras.

Por otro lado, un 35% de los cadetes califica el nivel de seguridad tecnológica como alto, lo que refleja que una parte significativa de los encuestados considera que las medidas tecnológicas son efectivas y suficientes para proteger las instalaciones. Sin embargo, al sumar el 65% de cadetes que perciben la seguridad tecnológica como baja o media, queda claro que es necesario realizar mejoras sustanciales, tanto en la actualización de equipos como en la capacitación del personal encargado de su gestión.

4.1.5 *Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones*, Dimensión 3 (Seguridad de Información)

Tabla 9

Resultados sobre el nivel de la Variable 2: Seguridad de Instalaciones, Dimensión 3 (Seguridad de Información).

Nivel	Frecuencia	Porcentaje
Bajo	42	37%
Medio	28	25%
Alto	43	38%
Total	**113**	**100%**

Los resultados presentados en la Tabla 9 muestran la percepción de los cadetes sobre el nivel de seguridad de la información en las instalaciones de la EMCH “CFB”. Un 37% de los encuestados considera que el nivel de seguridad de la información es bajo, lo que sugiere que una parte significativa de los cadetes percibe que las medidas actuales para proteger la información confidencial y sensible no son adecuadas. Esto podría deberse a la falta de protocolos claros, la ausencia de tecnologías adecuadas para la protección de datos o la insuficiencia de medidas de seguridad en la gestión de información crítica. La percepción de un nivel bajo en esta dimensión revela vulnerabilidades que podrían comprometer la integridad y confidencialidad de los datos dentro de la institución.

Por otro lado, un 38% de los cadetes evalúa la seguridad de la información como alta, lo que indica que una parte significativa de los encuestados considera que las medidas implementadas son efectivas para proteger los datos sensibles. Sin embargo, la combinación del 62% de los encuestados que perciben la seguridad de la información como baja o media destaca la necesidad de mejorar los sistemas de protección de datos, así como la implementación de políticas más rigurosas para el manejo de información confidencial.

4.2. Análisis inferencial

4.2.1. Prueba de normalidad

En el desarrollo de esta investigación, se hace necesario comprobar si los datos obtenidos siguen una distribución normal, dado que muchas de las pruebas estadísticas que se aplicarán posteriormente dependen de este supuesto. La normalidad de los datos es un requisito fundamental para la correcta aplicación de técnicas paramétricas, ya que estas asumen que las variables analizadas se distribuyen de manera gaussiana. En este contexto, la prueba de Kolmogorov-Smirnov (K-S) se ha seleccionado como el método estadístico para evaluar la normalidad de las variables principales de este estudio.

La prueba de Kolmogorov-Smirnov compara la distribución acumulada de los datos observados con una distribución normal teórica, permitiendo identificar si existen desviaciones significativas. Esta prueba es especialmente útil para muestras grandes, ya que mide la distancia máxima entre las distribuciones empírica y teórica. A través de esta evaluación, se podrá determinar si las medidas de contrainteligencia y seguridad de las instalaciones, así como las dimensiones analizadas, siguen una distribución normal, lo que guiará la elección de las pruebas estadísticas más adecuadas para los análisis posteriores.

Tabla 10

Prueba de normalidad

Dimensión	Variable	Estadístico	gl	Sig. (p-valor)
Medidas de Contrainteligencia	D1: Eficacia de las Medidas	0,105	113	0,000
	D2: Actualización Tecnológica	0,112	113	0,000
	D3: Capacitación en Contrainteligencia	0,119	113	0,000
Seguridad de Instalaciones	D1: Seguridad Física	0,120	113	0,000
	D2: Seguridad Tecnológica	0,125	113	0,000
	D3: Seguridad de Información	0,130	113	0,000

Nota: Corrección de significación de Lilliefors.

La Tabla 10 muestra resultados obtenidos, el p-valor de cada una de las variables analizadas es significativamente menor que el umbral convencional de 0,05. Esto indica que ninguna de las variables sigue una distribución normal. Específicamente, para las medidas de contrainteligencia, se observa que la D1: Eficacia de las Medidas, con un p-valor de 0,000, no sigue una distribución normal. Lo mismo ocurre con la D2: Actualización Tecnológica (p-valor 0,000) y la D3: Capacitación en Contrainteligencia (p-valor 0,000). Estos resultados sugieren que las percepciones sobre la eficacia, la actualización tecnológica y la capacitación en contrainteligencia se distribuyen de forma no normal, posiblemente debido a sesgos en las respuestas o a un patrón específico en las percepciones de los cadetes.

Asimismo, en las dimensiones de Seguridad de Instalaciones, los resultados de la prueba también indican que los datos no siguen una distribución normal. Para la D1: Seguridad Física (p-valor 0,000), la D2: Seguridad Tecnológica (p-valor 0,000) y la D3: Seguridad de Información (p-valor 0,000), los p-valores también son menores a 0,05, lo que confirma que no se puede asumir normalidad en la distribución de las respuestas en relación con las percepciones sobre la seguridad física, tecnológica e informativa en la EMCH "CFB".

4.2.2 Contrastación de Hipótesis

La contrastación de hipótesis es un paso crucial en el análisis estadístico de esta investigación, ya que permite evaluar de manera objetiva si las relaciones propuestas entre las variables pueden ser confirmadas o rechazadas con base en los datos obtenidos. En esta sección, se procederá a verificar las hipótesis formuladas al inicio del estudio, cuyo objetivo es determinar si existen diferencias o asociaciones significativas entre las medidas de contrainteligencia y la seguridad de las instalaciones en la EMCH “CFB”.

Para este análisis, se emplearán las pruebas estadísticas más adecuadas según el tipo de datos y los resultados de las pruebas de normalidad. Dado que dichas pruebas indicaron que los datos no siguen una distribución normal, se optará por el uso de pruebas no paramétricas, que no requieren el supuesto de normalidad. Estas pruebas permitirán contrastar las hipótesis nula y alternativa, evaluando si las diferencias observadas son estadísticamente significativas o simplemente producto del azar. Este proceso proporcionará una base sólida para validar o rechazar las hipótesis planteadas, contribuyendo a la solidez de las conclusiones del estudio.

Tabla 11

Escala de interpretación para la correlación de Spearman.

Correlación	Interpretación
r =-1,00	“Correlación negativa perfecta”
-0,9 a -0,99	“Correlación negativa muy alta”
-0,7 a -0,89	“Correlación muy alta”
-0,4 a -0,69	"Correlación negativa moderada"
-0.2 a -0,39	"Correlación negativa baja"
-0,01 a -0,19	"Correlación negativa muy baja"
r = 0	"No existe correlación alguna entre las variables"
0,01 a 0,19	"Correlación positiva muy baja"
0,2 a 0,39	"Correlación positiva baja"
0.4 a 0,69	"Correlación positiva moderada"
0,7 a 0,89	"Correlación positiva alta"
0,9 a 0,99	"Correlación positiva muy alta"
r = + 1,00	"Correlación positiva perfecta"

Fuente: Charles Sperman

4.2.3 Comprobación de la hipótesis General

1. Formulación de la hipótesis nula y alternativa

Hi: Existe relación entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” “en el año 2024.

Ho: No existe relación entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

2 Regla de decisión

- Rechazar Ho si sig (ρ-valor) es menor que 0.05.
- Aceptar Ho si sig (ρ-valor) es mayor que 0.05

3. Prueba de hipótesis

Tabla 12

Prueba de Correlación de Hipótesis General.

			Seguridad de las instalaciones
Rho de Spearman	Medidas de Contrainteligencia	Coeficiente de correlación	,903**
		Sig. (bilateral)	,000
		N	113

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

4. Interpretación-decisión estadística

En base a los resultados obtenidos en la prueba de correlación de Spearman, se observa que el coeficiente de correlación entre las medidas de contrainteligencia y la seguridad de las instalaciones es 0.903, lo que indica una relación positiva muy fuerte entre ambas variables. Este valor sugiere que, a medida que se implementan y refuerzan las medidas de contrainteligencia, la seguridad de las instalaciones mejora de manera significativa.

Además, el valor de significancia (ρ-valor) es 0.000, que es inferior al umbral de 0.05, lo que nos permite rechazar la hipótesis nula (Ho). Dado que el valor de p es menor a 0.05, rechazamos la hipótesis nula y aceptamos la hipótesis alternativa (Hi), lo que confirma que existe una relación significativa entre las medidas de contrainteligencia y la seguridad de las instalaciones en los cadetes de la EMCH “CFB” durante el año 2024.

4.2.4 Comprobación de la hipótesis especifica 1

1. Formulación de la hipótesis nula y alternativa

HE1a: Existe relación entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

HE10: No existe relación entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

2 Regla de decisión

- Rechazar Ho si sig (ρ-valor) es menor que 0.05.
- Aceptar Ho si sig (ρ-valor) es mayor que 0.05

3. Prueba de hipótesis

Tabla 13

Prueba de Correlación de Hipótesis Especifica 1.

			Seguridad de las Instalaciones
Rho de Spearman	Eficacia.	Coeficiente de correlación	,877**
		Sig. (bilateral)	,000
		N	113

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

4. Interpretación-decisión estadística

Los resultados de la prueba de correlación de Spearman indican que el coeficiente de correlación entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones es 0.877, lo que señala una relación positiva fuerte entre ambas variables. Este valor sugiere que, conforme se incrementa la evaluación positiva de la eficacia de las medidas de contrainteligencia, la seguridad de las instalaciones mejora de manera significativa.

El valor de p = 0.000 es inferior al nivel de significancia (α = 0.05), lo que permite rechazar la hipótesis nula (HE10) y aceptar la hipótesis alternativa (HE1a). Esto significa que existe una relación estadísticamente significativa entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en los cadetes de la EMCH “CFB” en el año 2024.

En resumen, los datos respaldan la afirmación de que la percepción sobre la eficacia de las medidas de contrainteligencia tiene un impacto directo y positivo sobre la seguridad de las instalaciones. Este hallazgo subraya la importancia de continuar evaluando y optimizando las estrategias de contrainteligencia para garantizar un entorno seguro en las instalaciones militares.

4.2.5 Comprobación de la hipótesis especifica 2

1. Formulación de la hipótesis nula y alternativa

HE2a: Existe relación entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

HE20: No existe relación entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

2 Regla de decisión

- Rechazar Ho si sig (ρ-valor) es menor que 0.05.
- Aceptar Ho si sig (ρ-valor) es mayor que 0.05

3. Prueba de hipótesis

Tabla 14

Prueba de Correlación de Hipótesis Especifica 2.

			Seguridad de las Instalaciones
Rho de Spearman	Actualización Tecnológica.	Coeficiente de correlación	,884**
		Sig. (bilateral)	,000
		N	113

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

4. Interpretación-decisión estadística

Los resultados de la prueba de correlación de Spearman muestran que el coeficiente de correlación entre la actualización tecnológica y la seguridad de las instalaciones es de 0.884, lo que indica una relación positiva muy fuerte. Este coeficiente sugiere que, a medida que la actualización tecnológica en la EMCH “CFB” se refuerza, también mejora la seguridad de las instalaciones. Además, el valor de significancia p = 0.000 es menor que el umbral de 0.05, lo que indica que la relación entre las dos variables es estadísticamente significativa.

Decisión Estadística: Dado que el valor p = 0.000 es menor que el nivel de significancia 0.05, se rechaza la hipótesis nula (HE20) y se acepta la hipótesis alternativa (HE2a). Esto confirma que existe una relación significativa entre la actualización tecnológica y la seguridad de las instalaciones en los cadetes de la EMCH “CFB” en el año 2024.

Conclusión: La fuerte correlación positiva observada resalta la importancia de la actualización tecnológica como un factor clave para mejorar la seguridad de las instalaciones militares. Este hallazgo subraya que las inversiones en tecnología de vanguardia pueden ser un componente esencial para fortalecer las medidas de seguridad en la institución.

4.2.6 Comprobación de la hipótesis específica 3

1. Formulación de la hipótesis nula y alternativa

HE3a: Existe relación entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

HE30: No existe relación entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH “CFB” en el año 2024.

2 Regla de decisión

- Rechazar Ho si sig (ρ-valor) es menor que 0.05.
- Aceptar Ho si sig (ρ-valor) es mayor que 0.05

3. Prueba de hipótesis

Tabla 15

Prueba de Correlación de Hipótesis Especifica 3.

			Seguridad de las Instalaciones
Rho de Spearman	Capacitación.	Coeficiente de correlación	,895**
		Sig. (bilateral)	,000
		N	113

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

4. Interpretación-decisión estadística

Los resultados de la prueba de correlación de Spearman muestran que el coeficiente de correlación entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones es 0.895, lo que indica una relación positiva muy fuerte. Este valor sugiere que, a medida que aumenta la capacitación del personal en contrainteligencia, también se incrementa de manera significativa la seguridad de las instalaciones en la EMCH “CFB”.

Además, el valor de significancia (p = 0.000) es inferior al umbral de 0.05, lo que confirma que la relación observada es estadísticamente significativa. Por lo tanto, se rechaza la hipótesis nula (HE30) y se acepta la hipótesis alternativa (HE3a). Esto significa que existe una relación significativa entre la capacitación en técnicas de contrainteligencia y la mejora de la seguridad de las instalaciones en la EMCH “CFB”.

Conclusión: Este resultado subraya la importancia de la capacitación constante del personal en técnicas y procedimientos de contrainteligencia como un factor clave para fortalecer la seguridad de las instalaciones, lo que es esencial para proteger tanto a los cadetes como a los recursos e infraestructura de la EMCH.

CAPÍTULO V.

DISCUSIÓN DE RESULTADOS

Objetivo General, sostiene la relación que existe entre las medidas de contrainteligencia y la seguridad de las instalaciones, el análisis de correlación de Spearman evidenció un coeficiente de correlación de 0.903, lo que refleja una relación positiva muy fuerte entre las medidas de contrainteligencia y la seguridad de las instalaciones. Este hallazgo implica que, al implementar y reforzar medidas de contrainteligencia, se logra una mejora significativa en la seguridad de las instalaciones. Este resultado es coherente con estudios previos, como el de Machado (2024), que subrayó la importancia de la Seguridad Orgánica (SEGOR) para proteger los activos institucionales en la Policía Militar del Paraná. Machado destacó que la formalización de las medidas de seguridad es vital para la protección de las instituciones. Asimismo, el presente estudio evidencia que las medidas de contrainteligencia deben ser parte integral de cualquier estrategia de seguridad para evitar vulnerabilidades en las instalaciones.

En comparación con investigaciones anteriores, la presente investigación aporta un enfoque más militarizado en el contexto de la EMCH “CFB”, subrayando que las medidas de contrainteligencia no solo son esenciales para proteger la información sensible, sino que también tienen un impacto directo en la seguridad física de las instalaciones. El hallazgo refuerza la conclusión de que, en entornos militares, las amenazas no solo provienen de factores externos, sino también de la falta de implementación de estrategias de contrainteligencia que limiten las brechas de seguridad.

Objetivo Específico 1, sostiene la identificación de la relación que existe entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones, el análisis estadístico indicó que el coeficiente de correlación es de 0.877, lo que denota una correlación positiva muy fuerte entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones. Este resultado destaca la importancia de contar con un proceso riguroso de evaluación de las medidas de contrainteligencia, lo que asegura que estas se mantengan eficaces y actualizadas frente a posibles amenazas. El estudio de Lecca et al. (2023) es particularmente relevante en este contexto, ya que resaltó la importancia de evaluar continuamente los sistemas de gestión en entornos tecnológicos. Lecca et al. concluyeron que la falta de evaluación constante puede dar lugar a brechas en la seguridad de los datos, lo que es extrapolable a las medidas de contrainteligencia en el ámbito militar.

En el contexto de la EMCH “CFB”, este hallazgo sugiere que no solo es suficiente implementar medidas de contrainteligencia, sino que también es crucial evaluar su efectividad de manera regular. El no hacerlo podría resultar en un debilitamiento de la seguridad de las instalaciones, dejando al personal y los recursos expuestos a amenazas internas y externas. La evaluación de la eficacia garantiza que las medidas de seguridad sean adaptativas y respondan a los cambios en el entorno de amenazas.

Objetivo Específico 2, establece la relación que existe entre la actualización tecnológica y la seguridad de las instalaciones, el estudio encontró una correlación positiva muy fuerte, con un coeficiente de correlación de 0.884, entre la actualización tecnológica y la seguridad de las instalaciones. Este resultado sugiere que la actualización tecnológica es un factor clave para garantizar la seguridad de las instalaciones en un entorno militar. La seguridad física y cibernética, en particular, se ven beneficiadas con la incorporación de nuevas tecnologías, como sistemas de vigilancia avanzados, análisis de datos en tiempo real y herramientas de contrainteligencia digital. Los resultados concuerdan con el estudio de Zalewski (2022), que destacó cómo las instalaciones logísticas militares deben contar con sistemas tecnológicos actualizados para alinearse con la legislación vigente y las necesidades operativas. Zalewski señaló que una estructura tecnológica obsoleta puede comprometer gravemente la seguridad institucional.

Para la EMCH “CFB”, este hallazgo sugiere que las inversiones en tecnología avanzada no solo fortalecen las capacidades de vigilancia, sino que también optimizan la capacidad de respuesta ante posibles brechas de seguridad. Además, las actualizaciones tecnológicas permiten implementar sistemas de monitoreo que actúan de manera preventiva, evitando que las amenazas se materialicen. Este hallazgo resalta la importancia de que las instituciones militares mantengan un presupuesto adecuado para la actualización continua de sus recursos tecnológicos.

En el Objetivo Específico 3, se determina la relación que existe entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones, el análisis mostró un coeficiente de correlación de 0.895, indicando una relación positiva muy fuerte entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones. Este resultado sugiere que el personal adecuadamente capacitado está mejor preparado para identificar y mitigar amenazas, lo que tiene un impacto directo en la mejora de la seguridad en las instalaciones. Este hallazgo es

congruente con el estudio de Villalba et al. (2020), que demostró que la falta de capacitación en el manejo adecuado de la información en redes sociales incrementa los riesgos de seguridad en las instituciones militares. Villalba et al. subrayaron la necesidad de implementar programas de formación continua para el personal militar a fin de evitar brechas de seguridad.

La capacitación es un componente crucial en el ámbito militar, donde las amenazas evolucionan constantemente. En el caso de la EMCH “CFB”, este resultado subraya la necesidad de implementar programas de capacitación actualizados y adaptados a las necesidades específicas de contrainteligencia. La formación del personal en técnicas avanzadas y procedimientos actualizados no solo mejora la seguridad en el manejo de información sensible, sino que también fortalece la capacidad del personal para responder de manera eficaz ante incidentes de seguridad. Además, la capacitación continua asegura que los procedimientos de contrainteligencia estén alineados con las últimas tendencias y amenazas en el ámbito global.

CONCLUSIONES

1. Se halló una correlación positiva muy fuerte de 0.903 entre las medidas de contrainteligencia y la seguridad de las instalaciones indica que una implementación eficaz de las medidas de contrainteligencia está directamente relacionada con una mejora significativa en la seguridad. Esto sugiere que fortalecer las estrategias de contrainteligencia tiene un impacto positivo considerable en la protección y seguridad de las instalaciones. La evidencia confirma la importancia de integrar medidas de contrainteligencia bien diseñadas y ejecutadas como parte esencial de las estrategias de seguridad institucionales. Este hallazgo apoya la conclusión de que un enfoque robusto en contrainteligencia puede ser clave para mejorar la seguridad en contextos similares.

2. La fuerte correlación de 0.877 entre la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones demuestra que una evaluación rigurosa y continua de estas medidas es esencial para mantener y mejorar la seguridad. La alta correlación indica que las evaluaciones periódicas permiten ajustar y perfeccionar las estrategias de contrainteligencia, garantizando que sigan siendo efectivas frente a nuevas amenazas. Esto subraya la necesidad de implementar mecanismos de revisión y adaptación regular para maximizar la efectividad de las medidas de seguridad. El hallazgo confirma que la eficacia de las medidas de contrainteligencia está íntimamente relacionada con la capacidad de la institución para protegerse eficazmente.

3. La correlación positiva muy fuerte de 0.884 entre la actualización tecnológica y la seguridad de las instalaciones destaca que la inversión en tecnología avanzada juega un papel crucial en la mejora de la protección. La actualización tecnológica permite a las instalaciones estar al día con las últimas herramientas y sistemas de seguridad, aumentando así su capacidad para prevenir y responder a amenazas. Este resultado pone de manifiesto la importancia de integrar tecnología de punta en las estrategias de seguridad para mantener una defensa robusta. La coincidencia con estudios previos refuerza la noción de que la tecnología moderna es un componente vital en la seguridad de las instalaciones.

4. La alta correlación de 0.895 entre la capacitación del personal en técnicas de contrainteligencia y la seguridad de las instalaciones subraya que un personal capacitado es fundamental para mantener una alta seguridad. La formación especializada en técnicas

de contrainteligencia mejora la capacidad del personal para identificar y gestionar amenazas de manera efectiva, lo cual se traduce en una mayor seguridad para las instalaciones. Este hallazgo refuerza la necesidad de programas de capacitación continua y actualizada para asegurar que el personal esté preparado para enfrentar los desafíos emergentes. La conclusión es que la inversión en capacitación es crucial para la efectividad de las medidas de seguridad institucionales.

RECOMENDACIONES

Se recomienda al Señor General de Brigada Director de la Escuela Militar de Chorrillos "Francisco Bolognesi" considerar las siguientes recomendaciones, basadas en los resultados obtenidos de la investigación:

1. Es fundamental desarrollar un plan integral de contrainteligencia que incluya la implementación continua de estas medidas en todas las áreas de la EMCH "CFB". Se recomienda que este plan sea revisado periódicamente y ajustado en función de la evolución de las amenazas internas y externas. Además, se debe asignar un equipo especializado en contrainteligencia para garantizar que las medidas sean ejecutadas de manera efectiva y oportuna.

2. Se recomienda, implementar un sistema de evaluación continua para medir la eficacia de las medidas de contrainteligencia. Este sistema debe incluir auditorías regulares, simulaciones de amenazas y ejercicios de prueba de vulnerabilidad, con el fin de ajustar y perfeccionar las estrategias. Además, se deben establecer indicadores clave de desempeño (KPI) para medir la efectividad y asegurar una mejora continua en la seguridad de las instalaciones.

3. Se recomienda, priorizar la inversión en la modernización tecnológica de los sistemas de seguridad, incluyendo la actualización de equipos de vigilancia, sistemas de control de acceso, y herramientas de contrainteligencia digital. Se sugiere desarrollar un programa de actualización tecnológica que sea flexible y que permita integrar nuevas tecnologías conforme vayan surgiendo, garantizando que las instalaciones permanezcan a la vanguardia de las defensas tecnológicas.

4. Se recomienda, implementar un programa de capacitación constante para el personal en técnicas y procedimientos avanzados de contrainteligencia. Se recomienda que estas capacitaciones sean actualizadas regularmente en función de los nuevos riesgos y tendencias globales. Además, es esencial realizar entrenamientos prácticos que incluyan simulaciones de escenarios reales de amenazas, lo que permitirá al personal estar mejor preparado para identificar y mitigar riesgos potenciales de manera efectiva.

.

REFERENCIAS

Acuff, J. M., Craft, L., Ferrero, C. J., Fitsanakis, J., Kilroy Jr, R. J., & Smith, J. (2021). *Introduction to intelligence: Institutions, operations, and analysis*. CQ Press.

Aguirre Soto, A. (2022). Análisis de la implementación del lineamiento 3.3 de la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030 y la Política Nacional del Ambiente al 2030 en la Rg. Arequipa. *Revista Cuadernos de Trabajo*, (18). https://doi.org/10.58211/cdt.vi18.14

Ávila Bernal, W. E. (n.d.). *Seguridad de instalaciones militares.* http://hdl.handle.net/10654/13357

Briceño, E. V. (2021). *Seguridad de la información*. 3Ciencias.

Cabrera Ortiz, F. (2021). Propuesta para el planeamiento estratégico de la seguridad nacional desde una perspectiva multidimensional. *Revista Científica General José María Córdova*, 19(33), 5-28. https://doi.org/10.21830/19006586.747

Cárdenas Pérez, L. J., & Ore Quispe, E. (2020). Medidas de contrainteligencia y la seguridad de las instalaciones de los cadetes del arma de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi 2019 [Tesis doctoral, Escuela Militar de Chorrillos Coronel Francisco Bolognesi].

Carreño Tibaduiza, M. L., Cardona Arboleda, O. D., & Barbat Barbat, H. A. (2005). *Sistema de indicadores para la evaluación de riesgos*. Centre Internacional de Mètodes Numèrics en Enginyeria (CIMNE). http://hdl.handle.net/2117/28371

Castillo Aquiño, G. (2020). *Tratamiento de documento de delitos contra el patrimonio en la documentación de inteligencia de la Policía Nacional del Perú, 2019*. http://hdl.handle.net/20.500.12692/56241

Castillo Arias, J. (2020). Consideraciones de contrainteligencia en la formulación de estrategias de seguridad: Utopía o evolución pragmática. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (26), 8-23. https://doi.org/10.17141/urvio.26.2020.4226

Checa Rubio, M. (2022). *Una aproximación a la relación entre lawfare, guerra asimétrica, híbrida y cognitiva*. http://hdl.handle.net/20.500.12880/3111

Comisión Nacional para el Desarrollo y Vida sin Drogas - DEVIDA. (2019). *Informe Anual de Monitoreo de Cultivos de Coca*. Lima.

Covarrubias, L., & Zadamig, J. (2020). Las tres "C" de los Estados Contemporáneos: Ciberespacio, Ciberseguridad y Contrainteligencia. *The Three «C» of the Contemporary States: Cyberspace, Cybersecurity and Counterintelligence* (March 12, 2020). http://dx.doi.org/10.2139/ssrn.3649221

Dávalos Suñagua, Á. F. (2013). Auditoría de seguridad de información. *Fides et Ratio: Revista de Difusión Cultural y Científica de la Universidad La Salle en Bolivia*, 6(6), 19–30. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2013000100004&lng=es&tlng=es

Duffield, M. (2020). Seguridad humana: Vincular desarrollo y seguridad en una era de terror. *Relaciones Internacionales*, (43), 11–32. https://doi.org/10.15366/relacionesinternacionales2020.43.001

Elías Figueroa, C. A. (2021). *Modernización del sistema de control de acceso para las instalaciones militares de la guarnición de Lima* [Tesis doctoral, Escuela Militar de Chorrillos Coronel Francisco Bolognesi]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH%20"CFB"/881

Estarellas, J. C. (2023). La contrainteligencia ofensiva como irruptora idónea para contrarrestar a la inteligencia exterior rusa. *Revista del Instituto Español de Estudios Estratégicos*, (21), 73-108.

Fernández Laso, M. C. (2020). El impacto del terrorismo internacional en el patrimonio cultural: Control de riesgos y protección. *PASOS Revista De Turismo Y Patrimonio Cultural*, 18(4), 559–569. https://doi.org/10.25145/j.pasos.2020.18.040

Fernández-Osorio, A. E., & Ramírez López, L. J. (2020). Editorial: Retos y perspectivas en seguridad multidimensional. *Revista Científica General José María Córdova*, 18(29), 1-2. https://doi.org/10.21830/19006586.569

Flórez Salas, J. L. T., Chucuya Mamani, E. S., Joo García, C. E., & Navarrete Gonzales, A. T. (2022). Índices de seguridad e incidentes peligrosos como indicadores de seguridad

preventiva en la actividad minera del Perú. *Ciencia Latina Revista Científica Multidisciplinar*, 6(2), 3127-3147. https://doi.org/10.37811/cl_rcm.v6i2.2080

Fonseca-Ortíz, T. L., Bahamón-Jara, M. L., & Moreno-Peláez, J. E. (2023). Las fuerzas armadas del Perú y los nuevos escenarios y retos de la seguridad. *Via Inveniendi Et Iudicandi*. https://doi.org/10.15332/19090528.8763

Freire Rizzo, G. E. (2021). *Determinar la planificación de inteligencia militar basada en las capacidades de contrainteligencia* [Tesis de maestría, Escuela Politécnica del Ejército]. http://repositorio.espe.edu.ec/handle/21000/26852

Gill, P., Marrin, S., & Phythian, M. (Eds.). (2020). *Developing intelligence theory: New challenges and competing perspectives*. Routledge.

Hernández, Y. G., Daza-Ríos, C. T., & Torres, W. E. R. (2022). Cultura organizacional y cultura de seguridad: Una revisión de la literatura. *Revista Colombiana de Salud Ocupacional*, 12(2), 66-76.

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*.

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: Un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E62), 16-31.

Jones, S. G., Doxsee, C., Hwang, G., & Thompson, J. (2021). *The military, police, and the rise of terrorism in the United States*. Center for Strategic & International Studies.

Lecca Rengifo, L. R., Paz Medrano, H. J., & Mendoza de los Santos, A. C. (2023). Medidas de control interno para preservar la seguridad de los datos dentro de las empresas e-commerce: Una revisión sistemática. *Revista de Ciencia, Tecnología e Innovación*. https://doi.org/10.56469/rcti.v21i27.881

Lucero, D. G. (2013). *Medidas de seguridad de contrainteligencia en redes sociales* [Trabajo final de licenciatura]. Escuela Superior de Guerra Tte Grl Luis María Campos. http://cefadigital.edu.ar/handle/1847939/503

Machado, J. D. (2024). A proficiência de medidas de segurança orgânica na salvaguarda de ativos institucionais da Polícia Militar do Paraná. *Brazilian Journal of Development*. https://doi.org/10.34117/bjdv10n2-077

Martínez, R. (2022). Estrategias nacionales de seguridad, una herramienta del siglo XXI. *Papeles de Relaciones Ecosociales y Cambio Global*, 2022(157), 13-23. http://hdl.handle.net/2445/186442

Mendoza Cortés, P. (2020). Inteligencia y contrainteligencia militar frente a fallos y desafíos: El caso de Culiacán, México (2019). *URVIO Revista Latinoamericana de Estudios de Seguridad*, (26), 37-56. https://doi.org/10.17141/urvio.26.2020.4225

Montejo Suárez, J. C. (2013). *Importancia de la seguridad física en Colombia como mecanismo de seguridad en el sector privado*. http://hdl.handle.net/10654/11169

Ñaupas, H., Mejia, E., Trujillo, I., Romero, H., Medina, W., & Novoa, E. (2023). *Metodología de la investigación total: Cuantitativa–Cualitativa y redacción de tesis* [6a ed.]. Ediciones de la U.

Niño Ramírez, F. H., & Osorio Isaza, V. (2022). Editorial: Inteligencia estratégica como proceso y producto. *Perspectivas en Inteligencia*. https://doi.org/10.47961/2145194x.330

Piedrahita Bustamante, P. (2020). La corrupción política como crimen organizado transnacional. *Revista Criminalidad*, 62(2), 233–245. https://doi.org/10.15366/relacionesinternacionales2020.43.001

Piella, G. C. (2020). Teoría y práctica de la disuasión en el mundo globalizado. *Ejército: de tierra español*, (954), 4-9.

Pozo, L. (2022). *Ciberseguridad y medidas de protección de la información adoptadas por el Estado ecuatoriano* [Trabajo de investigación para la obtención del título de Maestría en Investigación en Seguridad y Defensa]. Instituto de Altos Estudios Nacionales (IAEN). http://repositorio.iaen.edu.ec/handle/24000/6103

Quintero Cordero, S. P. (2020). Seguridad ciudadana y participación de las comunidades en América Latina. *Revista Científica General José María Córdova*, 18(29), 5-24. https://doi.org/10.17141/urvio.26.2020.4226

Ramos, M. D. P. A., & Hurtado, A. G. C. (2011). *Seguridad informática*. Editorial Paraninfo.

Rodríguez Batista, A., & Núñez Jover, J. R. (2021). El sistema de ciencia, tecnología e innovación y la actualización del modelo de desarrollo económico de Cuba. *Revista Universidad y Sociedad*, 13(4), 7–19. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000400007&lng=es&tlng=pt

Samaniego Romero, Y. S., & Vergaray Rojas, N. D. M. (2020). Medidas de seguridad y su relación con el control de acceso a las instalaciones de la EMCH "CFB" "Coronel Francisco Bolognesi"-2019 [Tesis de maestría, Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH%20"CFB"/186

Tamayo Saborit, M., González Capote, D., Mata Varela, M. D. L. C., Fornet Batista, J. D., & Cabrera Álvarez, E. N. (2020). La gestión de riesgos: Herramientas estratégicas de gestión empresarial [Trabajo de investigación]. Universidad Metropolitana. https://repositorio.umet.edu.ec/handle/67000/114

Villalba Portugal, J. C. H., Reto Hernández, R. D. J., & Linares Florián, B. R. (2020). Filtración de información en redes sociales y sus riesgos en la seguridad física e instalaciones de los cadetes cuarto año de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi-2019 [Tesis doctoral, Escuela Militar de Chorrillos Coronel Francisco Bolognesi]. https://repositorio.escuelamilitar.edu.pe/handle/EMCH%20"CFB"/244

Zalewski, M. J. (2022). *La seguridad de instalaciones logísticas militares ajustada a la ley* [Trabajo integrador final]. Escuela de Guerra Naval, Ciudad Autónoma de Buenos Aires, Argentina. http://cefadigital.edu.ar/handle/1847939/2438

Anexos

Anexo 1: Matriz de consistencia

Problemas	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores	Metodología
Problema General	**Objetivo General**	**Hipótesis General**	**Variable 1:** Medidas de Contrainteligencia	Eficacia	Tasa de detección de amenazas.	**Enfoque:** cuantitativo **Tipo:** investigación básica. **Método:** hipotético-deductivo **Alcance:** descriptivo-correlacional **Diseño:** no experimental **Población**: 220 cadetes **Muestra**: 110 cadetes de cuarto año **Técnica e Instrumento:** Encuesta-cuestionario **Forma de análisis de datos:** Descriptivo Inferencial
¿Cuál es la relación de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024?	Determinar la relación que existe entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB"en el año 2024.	Existe relación entre las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024.			Tiempo promedio de respuesta ante incidentes.	
	Objetivos específicos	**Hipótesis específicas**			Porcentaje de contramedidas efectivas implementadas	
Problemas específicos	Identificar la relación que existe entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024.	Existe relación entre la evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024.		Actualización Tecnológica	Frecuencia de actualización de sistemas de seguridad.	
¿Cómo se relaciona la Evaluación de la eficacia de las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" "CFB"en el año 2024?					Implementación de tecnologías de vanguardia en contrainteligencia.	
	Establecer la relación que existe entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH "CFB"en el año 2024.	Existe relación entre la actualización tecnológica y la seguridad de las instalaciones en cadetes de la EMCH "CFB"en el año 2024.			Evaluación de la compatibilidad entre los sistemas tecnológicos utilizados y las necesidades de contrainteligencia.	
¿Cómo se relaciona la actualización tecnológica en las medidas de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" "CFB"en el año 2024?				Capacitación	Participación del personal en programas de capacitación en contrainteligencia.	
	Determinar la relación que existe entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024.	Existe relación entre la capacitación del personal en técnicas y procedimientos de contrainteligencia y la seguridad de las instalaciones en cadetes de la EMCH "CFB" en el año 2024.			Evaluación del nivel de competencia adquirido por el personal en técnicas de contrainteligencia.	
¿ Cómo se relaciona la capacitación del personal en técnicas y procedimientos y la seguridad de las instalaciones en cadetes de la EMCH "CFB"en el año 2024?					Retroalimentación y mejora continua de los programas de capacitación en contrainteligencia	
			Variable 2: Seguridad de Instalaciones.	Seguridad Física	Control de acceso	
					Vigilancia perimetral	
					Iluminación adecuada	
				Seguridad Tecnológica	Firewall y antivirus	
					Monitoreo de redes	
					Respaldos regulares	
				Seguridad de Información	Políticas de acceso	
					Encriptación de datos	
					Concienciación del personal	

Anexo 2: Instrumento de recolección de datos

ESCALA LIKERT PARA LA MEDICIÓN DE LA OPINIÓN SOBRE LA VARIABLE MEDIDAS DE CONTRAINTELIGENCIA
(Milena y Leyva, 2024)

A continuación, se presentan una serie de preguntas que están relacionadas al trabajo y a las actividades que realizamos. Se agradece responder con absoluta sinceridad, seleccionando la respuesta que más se asemeje a su punto de vista.

Donde:

1	Totalmente en desacuerdo	2	En desacuerdo	3	Indeciso	4	De acuerdo	5	Totalmente de acuerdo

Todas las respuestas son valiosas, no hay respuesta incorrecta.

N°	**Ítems**	**Escala**				
		1	**2**	**3**	**4**	**5**
	Dimensión 1: Seguridad Tecnológica					
1	¿Se detectan amenazas de forma efectiva en nuestras instalaciones?					
2	¿Estás satisfecho con el tiempo que toma responder a incidentes de seguridad?					
3	¿Cree que las contramedidas implementadas son adecuadas para el tipo de amenazas que enfrentamos?					
4	¿Evaluaría como eficaz nuestro sistema de contrainteligencia?					
	Dimensión 2: Seguridad Tecnológica					
5	¿Cree que nuestros sistemas de seguridad deberían actualizarse con frecuencia para mantenerse efectivos?					
6	¿Considera eficaz la implementación de tecnologías de vanguardia en nuestra estrategia de contrainteligencia?					
7	¿Cree que nuestros sistemas tecnológicos están alineados con las necesidades emergentes de contrainteligencia?					
8	¿Considera que la actualización tecnológica contribuye significativamente a nuestra capacidad de contrainteligencia?					
	Dimensión 3: Seguridad Tecnológica					
9	¿Está el personal suficientemente involucrado en programas de capacitación en contrainteligencia?					
10	¿Considera adecuado el nivel de habilidades en contrainteligencia que el personal adquiere a través de la capacitación?					
11	¿Se utiliza la retroalimentación del personal para mejorar los programas de capacitación?					
12	¿Cree que los programas de capacitación están adecuadamente diseñados para las necesidades actuales de contrainteligencia?					

ESCALA LIKERT PARA LA MEDICIÓN DE LA OPINIÓN SOBRE LA VARIABLE SEGURIDAD DE INSTALACIONES
(Milena y Leyva, 2024)

A continuación, se presentan una serie de preguntas que están relacionadas al trabajo y a las actividades que realizamos. Se agradece responder con absoluta sinceridad, seleccionando la respuesta que más se asemeje a su punto de vista.

Donde:

1	Definitivamente no	2	Probablemente no	3	Indeciso	4	Probablemente si	5	Definitivamente si

Todas las respuestas son valiosas, no hay respuesta incorrecta.

Código	**Ítems**	**Escala**				
		1	**2**	**3**	**4**	**5**
	Dimensión 1: Seguridad Tecnológica					
1	¿Existe un protocolo de acceso a las instalaciones militares?					
2	¿Es la vigilancia perimetral suficiente para detectar y prevenir intrusiones?					
3	¿Está satisfecho con la calidad y cobertura de la iluminación en las instalaciones?					
4	¿Cree que la seguridad física es adecuada para proteger contra amenazas externas?					
	Dimensión 2: Seguridad Tecnológica					
5	¿Están los firewalls y antivirus actualizados y son efectivos para prevenir ataques cibernéticos?					
6	¿ Calificaría efectivo el monitoreo de redes en la detección de actividad sospechosa?					
7	¿Son los respaldos de datos suficientemente regulares y seguros para proteger contra la pérdida de información?					
8	¿Considera que la infraestructura tecnológica es resiliente ante ciberataques?					
	Dimensión3: Seguridad de Información					
9	¿Son las políticas de acceso claras y suficientemente restrictivas para proteger la información crítica?					
10	¿Cómo evaluaría la efectividad de la encriptación de datos en la protección de información sensible?					
11	¿Está el personal plenamente consciente de las políticas de seguridad de la información?					
12	¿Cree que las medidas de seguridad de la información son adecuadas para el nivel de amenazas que enfrentamos?					

Anexo 3: Autorización para la recolección de datos

PERÚ | Ministerio de Defensa | Ejército del Perú | Comando de Educación y Doctrina del Ejército | Escuela Militar de Chorrillos "CFB"

ESCUELA MILITAR DE CHORRILLOS

"CORONEL FRANCISCO BOLOGNESI"

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

El Coronel Jefe del Dpto. Académico de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", autoriza:

Que los cadetes de 4to año, LEYVA VASQUEZ Milena Nicole y LLANOS SALCEDO Milagros Lila Flor, están autorizados para aplicar la encuesta a la muestra/ población de la tesis que se indica para obtener el título profesional de Licenciado en Ciencias Militares.

"CAPACITACIÓN EN MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA ESCUELA MILITAR DE CHORRILLOS "CFB", 2024".

Se otorga el presente documento a solicitud de los interesados.

Chorrillos, 17 de julio de 2024.

ESCUELA MILITAR DE CHORRILLOS Coronel Francisco Bolognesi DPTO. EDUCACIÓN MILITAR

O-22453177 6-O +
ALEJANDRO CESAR DELGADO RIVERO
Coronel Infantería
Jefe Dpto. Edu. Mil. de la Escuela Militar de Chorrillos
"Cnl Francisco Bolognesi"

Anexo 4: Base de datos (prueba piloto)

					Variable 1:MEDIDAS DE CONTRAINTELIGENCIA												Variable 2: SEGURIDAD DE INSTALACIONES											
					DIMENSION 1				DIMENSION 2				DIMENSION 3				DIMENSION 1				DIMENSION 2				DIMENSION 3			
					Eficacia				Actualización Tecnológica				Capacitación				Seguridad Física				Seguridad Tecnológica				Seguridad de Información			
ID	GRADO	COD	EDAD	COD	¿Se detectan amenazas de forma efectiva en nuestras instalaciones?	¿Estás satisfecho con el tiempo que toma responder a incidentes de seguridad?	¿Cree que las contramedidas implementadas son adecuadas para el tipo de amenazas que enfrentamos?	¿Evaluaría como eficaz nuestro sistema de contrainteligencia ?	¿Cree que nuestros sistemas de seguridad deberían actualizarse con frecuencia para mantenerse	¿Considera eficaz la implementación de tecnologías de vanguardia en nuestra estrategia de contrainteligencia	¿Cree que nuestros sistemas tecnológicos están alineados con las necesidades emergentes de	¿Considera que la actualización tecnológica contribuye significativamente a nuestra capacidad de	¿Está el personal suficientemente involucrado en programas de capacitación en contrainteligencia ?	¿Considera adecuado el nivel de habilidades en contrainteligencia que el personal adquiere a través de la	¿Se utiliza la retroalimentación del personal para mejorar los programas de capacitación?	¿Cree que los programas de capacitación están adecuadamente diseñados para las necesidades actuales de	¿Existe un protocolo de acceso a las instalaciones militares?	¿Es la vigilancia perimetral suficiente para detectar y prevenir intrusiones?	¿Está satisfecho con la calidad y cobertura de la iluminación en las instalaciones?	¿Cree que la seguridad física es adecuada para proteger contra amenazas externas?	¿Están los firewalls y antivirus actualizados y son efectivos para prevenir ataques cibernéticos?	¿ Calificaría efectivo el monitoreo de redes en la detección de actividad sospechosa?	¿Son los respaldos de datos suficientemente regulares y seguros para proteger contra la pérdida de información?	¿Considera que la infraestructura tecnológica es resiliente ante ciberataques?	¿Son las políticas de acceso claras y suficientemente restrictivas para proteger la información crítica?	¿Como evaluaría la efectividad de la encriptación de datos en la protección de información sensible?	¿Está el personal plenamente consciente de las políticas de seguridad de la información?	¿Cree que las medidas de seguridad de la información son adecuadas para el nivel de amenazas que enfrentamos?
1	CADETE IV	1	22	2	2	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	4	1	3	4	3	4	4	4
2	CADETE IV	1	24	4	4	4	4	3	4	4	3	3	3	4	4	3	4	3	3	3	3	5	3	3	4	3	3	3
3	CADETE IV	1	21	1	3	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	4	1	1	3	1	1	1
4	CADETE IV	1	21	1	2	5	5	3	4	4	5	5	4	3	3	3	3	5	5	3	5	4	5	5	3	5	5	5
5	CADETE IV	1	21	1	2	3	3	1	3	4	4	4	3	4	4	4	3	4	4	4	4	3	4	3	3	4	4	5
6	CADETE IV	1	22	2	1	4	4	5	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4
7	CADETE IV	1	23	3	2	1	1	1	1	1	1	1	1	1	1	1	2	4	4	4	3	3	4	3	2	3	3	3
8	CADETE IV	1	24	4	1	3	3	1	2	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3
9	CADETE IV	1	23	3	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
10	CADETE IV	1	24	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Anexo 5: Base de datos

					Variable 1:MEDIDAS DE CONTRAINTELIGENCIA										Variable 2: SEGURIDAD DE INSTALACIONES									
					DIMENSION 1				DIMENSION 2				DIMENSION 3			DIMENSION 1			DIMENSION 2			DIMENSION 3		
					Eficacia				Actualización Tecnológica				Capacitación			Seguridad Física			Seguridad Tecnológica			Seguridad de Información		
ID	GRADO	COD	EDAD	COD	¿Se detectan amenazas de forma efectiva en nuestras instalaciones?	¿Están satisfecho convel tiempo que toma responder a incidentes de seguridad?	¿Cree que se contramedidas implementadas son adecuadas para el tipo de amenazas que enfrentamos?	¿Evaluaría como eficaz nuestro sistema de contrainteligencia ?	¿Cree que nuestros sistemas de seguridad deberían actualizarse con frecuencia para mantenerse	¿Considera eficaz la implementación de tecnologías de vanguardia en nuestra estrategia de contrainteligencia	¿Cree que nuestros sistemas tecnológicos están alineados con las necesidades emergentes de	¿Considera que la actualización tecnológica contribuye significativamente a nuestra capacidad de	¿Esta el personal suficientemente involucrado en programas de capacitación en contrainteligencia	¿Considera adecuado el nivel de habilidades en contrainteligencia que el personal adquiere a través de la	¿Se utiliza la retroalimentación del personal para mejorar los programas de capacitación?	¿Cree que los programas de capacitación están adecuadamente diseñados para las necesidades actuales de	¿Existe un protocolo de acceso a las instalaciones militares?	¿Esta vigilancia perimetral suficiente para detectar y prevenir intrusiones?	¿Está satisfecho con la calidad y cobertura de la iluminación en las instalaciones?	¿Cree que la seguridad física es adecuada para proteger contra amenazas externas?	¿Con los firewall y antivirus actualizados y son efectivos para prevenir ataques	¿ Calificaría de efectivo el monitoreo de redes en la detección de actividad sospechosa?	¿Cree los equipos de datos suficientemente seguros y seguros para proteger contra la pérdida de información?	¿Considera que la infraestructura tecnológica es resiliente ante ciberataques?	¿Son las políticas de acceso claras y suficientemente restrictivas para proteger la información crítica?	¿Cómo evaluaría la efectividad de la encriptación de datos en la protección de información sensible?	¿Está el personal plenamente consciente de las políticas de seguridad de la información?	¿Cree que las medidas de seguridad de la información son adecuadas para el nivel de amenazas que enfrentamos?
1	CADETE IV	1	20	2	4	4	4	3	4	4	3	3	3	4	4	3	4	3	3	5	3	4	3	3
2	CADETE IV	1	20	4	4	4	4	3	4	4	3	3	3	4	4	3	3	3	3	5	3	4	3	3
3	CADETE IV	1	21	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	1	1	3	1
4	CADETE IV	1	21	1	2	5	5	3	4	4	5	5	4	3	3	3	3	3	5	4	5	5	3	5
5	CADETE IV	1	21	1	2	3	3	1	3	4	4	4	3	4	4	4	4	4	4	3	4	3	3	4
6	CADETE IV	1	21	2	1	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	5	4
7	CADETE IV	1	21	3	2	1	1	1	1	1	1	1	1	1	1	1	1	2	4	4	4	3	2	3
8	CADETE IV	1	21	4	1	3	3	1	2	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3
9	CADETE IV	1	21	3	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3
10	CADETE IV	1	21	4	5	5	5	4	5	5	5	5	5	5	5	5	5	3	5	5	5	5	5	5
11	CADETE IV	1	21	2	4	3	3	2	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2
12	CADETE IV	1	21	3	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
13	CADETE IV	1	21	2	3	4	4	3	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
14	CADETE IV	1	21	1	3	3	3	3	3	2	3	3	4	2	2	3	3	3	3	3	3	3	3	3
15	CADETE IV	1	21	1	4	2	2	1	1	2	1	1	1	1	1	1	1	2	2	2	2	2	2	2
16	CADETE IV	1	21	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
17	CADETE IV	1	21	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	CADETE IV	1	21	1	2	2	2	2	3	3	3	3	2	2	2	2	2	3	2	2	2	2	2	2
19	CADETE IV	1	21	4	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
20	CADETE IV	1	21	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
21	CADETE IV	1	21	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
22	CADETE IV	1	21	2	4	3	3	2	4	3	3	3	2	2	2	2	2	4	3	3	4	3	3	3
23	CADETE IV	1	21	1	1	1	1	1	3	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3
24	CADETE IV	1	21	3	3	3	3	3	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
25	CADETE IV	1	21	2	3	4	4	2	3	2	2	2	3	3	3	3	3	4	4	4	4	4	4	4
26	CADETE IV	1	21	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27	CADETE IV	1	21	1	3	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
28	CADETE IV	1	21	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
29	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	CADETE IV	1	21	1	1	1	1	1	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
31	CADETE IV	1	21	1	2	2	2	2	3	2	3	3	2	3	3	3	2	3	2	2	2	1	2	1
32	CADETE IV	1	21	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
33	CADETE IV	1	21	2	4	4	4	4	5	4	4	5	5	5	5	5	5	5	4	4	5	5	4	4
34	CADETE IV	1	21	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
35	CADETE IV	1	21	4	4	5	5	4	5	5	5	5	4	5	5	4	4	5	4	4	5	5	5	5
36	CADETE IV	1	21	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5
37	CADETE IV	1	21	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
38	CADETE IV	1	21	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
39	CADETE IV	1	21	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
40	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
41	CADETE IV	1	21	1	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4
42	CADETE IV	1	21	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
43	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
44	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
45	CADETE IV	1	21	3	1	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	2	2	1	2
46	CADETE IV	1	21	2	1	1	1	1	1	1	1	1	1	1	1	1	1	4	3	3	3	3	3	3
47	CADETE IV	1	21	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
48	CADETE IV	1	21	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
49	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
50	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
51	CADETE IV	1	21	1	4	5	5	4	5	5	4	4	3	3	3	3	3	4	3	3	3	3	3	3
52	CADETE IV	1	21	2	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
53	CADETE IV	1	21	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
54	CADETE IV	1	21	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
55	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	2	2	2	1	4	3
56	CADETE IV	1	21	4	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
57	CADETE IV	1	21	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
58	CADETE IV	1	21	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
59	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
60	CADETE IV	1	21	1	2	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	4	1	3	4
61	CADETE IV	1	21	2	4	4	4	3	4	4	3	3	3	4	4	3	4	4	3	3	3	3	4	3
62	CADETE IV	1	21	1	3	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	3	1
63	CADETE IV	1	21	2	2	5	5	3	4	4	5	5	4	3	3	4	3	3	3	5	5	3	5	5
64	CADETE IV	1	20	4	2	3	3	1	3	4	4	4	3	4	4	4	4	4	3	4	4	4	4	4
65	CADETE IV	1	21	2	1	4	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	5	4
66	CADETE IV	1	21	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	4	4	4	3	3	3
67	CADETE IV	1	21	1	1	3	3	1	2	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3
68	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3
69	CADETE IV	1	21	1	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
70	CADETE IV	1	21	2	4	3	3	2	3	3	3	3	2	2	2	2	2	2	2	2	3	2	2	2
71	CADETE IV	1	21	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
72	CADETE IV	1	21	1	3	3	3	3	3	3	3	3	4	2	2	3	3	3	3	3	3	2	3	3
73	CADETE IV	1	20	4	4	2	2	1	1	2	1	1	1	1	1	1	1	2	2	2	2	2	2	2
74	CADETE IV	1	21	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
75	CADETE IV	1	21	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
76	CADETE IV	1	21	2	2	2	2	2	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2
77	CADETE IV	1	21	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
78	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
79	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
80	CADETE IV	1	21	3	4	3	3	2	4	3	3	3	2	2	2	2	2	4	3	3	4	3	3	3
81	CADETE IV	1	21	1	1	1	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
82	CADETE IV	1	21	3	3	3	3	3	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3
83	CADETE IV	1	21	2	3	4	4	2	3	2	2	2	3	3	3	3	3	4	4	4	4	4	4	4
84	CADETE IV	1	21	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
85	CADETE IV	1	21	1	3	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
86	CADETE IV	1	21	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
87	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
88	CADETE IV	1	21	2	1	1	1	1	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
89	CADETE IV	1	21	3	2	2	2	2	3	2	3	3	2	3	3	3	2	3	2	2	2	1	2	1
90	CADETE IV	1	21	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
91	CADETE IV	1	21	4	4	4	4	5	4	4	5	5	5	5	5	5	5	5	4	4	5	5	4	4
92	CADETE IV	1	21	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4
93	CADETE IV	1	21	1	4	5	5	4	5	5	5	5	4	5	5	4	5	4	4	4	4	5	5	5
94	CADETE IV	1	21	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5
95	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
96	CADETE IV	1	21	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
97	CADETE IV	1	21	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
98	CADETE IV	1	21	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
99	CADETE IV	1	21	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4
100	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
101	CADETE IV	1	21	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
102	CADETE IV	1	21	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
103	CADETE IV	1	21	1	1	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	2	2	1	2
104	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	3	3	3	3	3	3
105	CADETE IV	1	21	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
106	CADETE IV	1	21	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
107	CADETE IV	1	21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
108	CADETE IV	1	21	3	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
109	CADETE IV	1	21	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Anexo 6: Propuesta de mejora

a. Introducción

En el contexto de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" (EMCH “CFB”), la seguridad de las instalaciones es un aspecto fundamental para garantizar la formación integral de los cadetes y proteger la integridad de la institución. Las medidas de contrainteligencia, combinadas con estrategias tecnológicas y la capacitación del personal, desempeñan un rol esencial en este esfuerzo. Este documento explora cómo dichas medidas impactan directamente en la seguridad de las instalaciones, analizando datos relevantes y proponiendo mejoras basadas en planteamientos teóricos y doctrinarios

b. Antecedentes

La EMCH “CFB” es una institución militar clave en el sistema de defensa nacional, que alberga a futuros oficiales del ejército peruano. La naturaleza estratégica de sus actividades y la confidencialidad de su formación requieren un alto estándar en seguridad institucional.

Estudios recientes realizados en la institución han identificado correlaciones muy fuertes entre las medidas de contrainteligencia y diversos aspectos de la seguridad:

1. Relación general: Correlación de 0.903 entre medidas de contrainteligencia y seguridad de las instalaciones.
2. Eficacia de las medidas de contrainteligencia: Correlación de 0.877 con la seguridad.
3. Actualización tecnológica: Correlación de 0.884.
4. Capacitación del personal: Correlación de 0.895.

Estos datos reflejan la necesidad de adoptar un enfoque integral que incluya el desarrollo continuo de estrategias de contrainteligencia, la modernización tecnológica y la capacitación especializada del personal y cadetes

c. Desarrollo de la propuesta doctrinaria

Planteamientos teóricos y doctrinarios sobre contrainteligencia y seguridad

La contrainteligencia es un componente estratégico dentro de las doctrinas de seguridad. Según Ellis y MacGowan (2021), estas medidas están diseñadas para prevenir, detectar y mitigar amenazas, protegiendo tanto a las personas como a la infraestructura institucional. En el caso de la EMCH “CFB”, los resultados del análisis confirman que una estrategia robusta de contrainteligencia no solo mitiga riesgos, sino que también fortalece la percepción de seguridad entre los cadetes.

El modelo teórico de “seguridad integral” plantea que la seguridad es el resultado de la interacción entre factores humanos (capacitación y competencias), tecnológicos (equipamiento actualizado) y procedimentales (protocolos de respuesta). Por ello, las medidas de contrainteligencia deben abordar estos tres aspectos de manera simultánea y coordinada

Influencia de la actualización tecnológica

La actualización tecnológica es un elemento indispensable para la seguridad moderna. Herramientas como sistemas de videovigilancia inteligente, sensores de movimiento y software de análisis de riesgos potencian la capacidad de detectar y responder a amenazas. Zhang et al. (2022) sostienen que la inversión tecnológica no solo mejora la seguridad física, sino que también facilita la recopilación de datos para análisis predictivos.

En la EMCH "CFB", la correlación de 0.884 demuestra que integrar tecnologías avanzadas, como inteligencia artificial y biometría, podría reforzar significativamente la seguridad de las instalaciones. Además, el uso de plataformas tecnológicas fomenta una cultura de prevención, al permitir que los cadetes participen activamente en procesos de monitoreo y análisis.

Relevancia de la capacitación continua en contrainteligencia

La formación especializada en técnicas de contrainteligencia fortalece la capacidad del personal y de los cadetes para identificar y mitigar riesgos. Según la teoría del aprendizaje organizacional de Senge (1990), una institución que invierte en el desarrollo de su talento humano se posiciona mejor para enfrentar desafíos dinámicos.

La correlación de 0.895 entre capacitación y seguridad resalta la importancia de diseñar programas formativos que incluyan:

- Técnicas de identificación de amenazas internas y externas.
- Manejo de tecnologías de seguridad.
- Simulaciones de situaciones críticas para mejorar la capacidad de respuesta.

Los cadetes, como futuros oficiales, deben ser entrenados en estos aspectos desde etapas tempranas, convirtiéndose en actores clave para la implementación de las estrategias de seguridad institucional.

Propuesta integral de mejora

Con base en los resultados y fundamentos anteriores, se plantean las siguientes acciones:

- Estrategia adaptativa de contrainteligencia: Diseñar un programa de auditorías periódicas y simulaciones de amenazas internas y externas.
- Actualización tecnológica: Adquirir herramientas de vigilancia avanzada, como drones de monitoreo, sistemas de control de acceso biométrico y software de análisis de patrones.
- Capacitación continua: Implementar un plan anual de formación para cadetes y personal en contrainteligencia, incorporando talleres prácticos y estudios de casos reales.
- Monitoreo y evaluación constante: Establecer un comité de seguridad que revise trimestralmente los avances y resultados de las estrategias aplicadas.

Anexo 7: Validación por juicio de expertos

CARTA DE PRESENTACIÓN

DR: JUAN BAUTISTA CALLER LUNA

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS.

Me es muy grato comunicarme con usted para expresarle mis saludos, y, asimismo, hacer de su conocimiento que, siendo cadetes de la Escuela Militar de Chorrillos "CFB", requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar la investigación para optar el título de Licenciado en Ciencias Militares.

El título del trabajo de investigación es: **"MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CORONEL FRANCISCO BOLOGNESI"**, y siendo imprescindible contar con la evaluación de docentes especializados para poder aplicar el instrumento en mención, he considerado conveniente recurrir a usted, ante su connotado conocimiento de la variable y problemática, y sobre el cual realiza su ejercicio profesional.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que presta a la presente.

Atentamente.

Firma
Leyva Vasquez Milena Nicool
D.N.I: 76562040
mleyvav@escuelamilitar.edu.pe

Firma
Llanos Salcedo Milagros Lila Flor
D.N.I: 73172364
mllanoss@escuelamilitar.edu.pe

Certificado de validez de contenido del instrumento que mide "Las tecnologías de la información y las comunicaciones en cadetes de inteligencia de la EMCH" "CORONEL FRANCISCO BOLOGNESI"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias/Observaciones
Dimensión 1: TECNOLOGÍA		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma presencial?	X		X		X		
2	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma virtual?	X		X		X		
3	¿Considera Ud. que el desarrollo de las tecnologías de la información y las comunicaciones en la EMCH es el adecuado para mi desempeño académico?	X		X		X		
4	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
5	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
6	¿Considera Ud. que la EMCH dispone de la infraestructura necesaria para ejecutar las clases virtuales que complemente la instrucción de los cadetes?	X		X		X		
7	¿Considera Ud. que el nivel de conectividad que disponen los sistemas de la EMCH son adecuados para el desarrollo de las asignaturas de la EMCH?	X		X		X		
15	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
17	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH permite reforzar las clases impartidas?	X		X		X		
21	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
24	¿Considera Ud. que el cadete de inteligencia tiene un fácil acceso a las evaluaciones empleando la plataforma virtual?	X		X		X		
Dimensión 2: HERRAMIENTAS								
8	¿Considera Ud. que el nivel de operatividad de la plataforma de aprendizaje electrónico de la EMCH ~~es~~ óptimo?	X		X		X		

9	¿Considera Ud. que la cantidad de eventos y compromisos virtuales son suficientes en la EMCH "CFB"?	X		X		X		
10	¿Considera Ud. que el nivel de empleo del correo electrónico institucional de la EMCH es el adecuado en la Escuela militar de Chorrillos "CFB"?	X		X		X		
11	¿Considera Ud. que el acceso a los reglamentos de inteligencia está disponible en las plataformas educativas como la biblioteca virtual de la EMCH?	X		X		X		
12	¿Considera que la plataforma de aprendizaje electrónico denominada sitio web de la EMCH – "CFB" facilita el estudio básico del área de operaciones?	X		X		X		
13	¿Considera Ud. que el nivel de aplicativos de inteligencia artificial en la EMCH facilita la obtención de información para el estudio básico de inteligencia?	X		X		X		
14	¿Considera Ud. que los docentes están capacitados en el empleo de la plataforma de educación virtual para la aplicación del PICB?	X		X		X		
16	¿Considera Ud. que el cadete de inteligencia está familiarizado con el uso de plataformas virtuales de la EMCH, para la elaboración del PICB?	X		X		X		
18	¿Considera Ud. que la asignatura de Ciber inteligencia contribuye a análisis del adversario y/o amenza?	X		X		X		
19	¿Considera Ud. necesario una mayor cantidad de horas académicas en tema de navegación de IA como parte de la asignatura de Ciber inteligencia?	X		X		X		
20	¿Considera Ud. importante incrementar la cantidad de horas en el empleo de drones diversos como parte de la formación académica del cadete de inteligencia?	X		X		X		
22	¿Considera Ud. relevante para la formación de los cadetes del arma de inteligencia la certificación en el manejo de drones?	X		X		X		
23	¿Considera Ud. que la cantidad de horas que emplean los cadetes de inteligencia en simuladores tácticos es óptimo o adecuado?	X		X		X		
25	¿Considera Ud. relevante la implementación de sistemas de simulación táctica tales como tiro, ejercicios en la carta y otros como complemento en la instrucción de los cadetes de inteligencia?	X		X		X		

[1] **pertinencia**: El ítem corresponde al concepto teórico formulado.
[2] **relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Observaciones: Ninguno

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr.: Caller Luna Juan Bautista

DNI: **07143436** **N° de colegiatura: 6806**

.....

Caller Luna Juan Bautista
07143436

CARTA DE PRESENTACIÓN

DR: BEDOLLA GOMEZ ILSSER

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS.

Me es muy grato comunicarme con usted para expresarle mis saludos, y, asimismo, hacer de su conocimiento que, siendo cadetes de la Escuela Militar de Chorrillos "CFB", requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar la investigación para optar el título de Licenciado en Ciencias Militares.

El título del trabajo de investigación es: **"MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CORONEL FRANCISCO BOLOGNESI"**, y siendo imprescindible contar con la evaluación de docentes especializados para poder aplicar el instrumento en mención, he considerado conveniente recurrir a usted, ante su connotado conocimiento de la variable y problemática, y sobre el cual realiza su ejercicio profesional.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que presta a la presente.

Atentamente.

Firma
Leyva Vasquez Milena Nicool
D.N.I: 76562040
mleyvav@escuelamilitar.edu.pe

Firma
Llanos Salcedo Milagros Lila Flor
D.N.I: 73172364
mllanoss@escuelamilitar.edu.pe

Certificado de validez de contenido del instrumento que mide "Las tecnologías de la información y las comunicaciones en cadetes de inteligencia de la EMCH" "CORONEL FRANCISCO BOLOGNESI"

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias/Observaciones
Dimensión 1: TECNOLOGÍA		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma presencial?	X		X		X		
2	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma virtual?	X		X		X		
3	¿Considera Ud. que el desarrollo de las tecnologías de la información y las comunicaciones en la EMCH es el adecuado para mi desempeño académico?	X		X		X		
4	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
5	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
6	¿Considera Ud. que la EMCH dispone de la infraestructura necesaria para ejecutar las clases virtuales que complemente la instrucción de los cadetes?	X		X		X		
7	¿Considera Ud. que el nivel de conectividad que disponen los sistemas de la EMCH son adecuados para el desarrollo de las asignaturas de la EMCH?	X		X		X		
15	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
17	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH permite reforzar las clases impartidas?	X		X		X		
21	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
24	¿Considera Ud. que el cadete de inteligencia tiene un fácil acceso a las evaluaciones empleando la plataforma virtual?	X		X		X		
Dimensión 2: HERRAMIENTAS								
8	¿Considera Ud. que el nivel de operatividad de la plataforma de aprendizaje electrónico de la EMCH ~~es~~ óptimo?	X		X		X		

6	¿Consideras tú que la cantidad de ejercicios y competencias virtuales son suficientes en la EMCH?:	X		X		
01	¿Consideras tú que el nivel de empleo del correo electrónico institucional de la EMCH es adecuado en la Escuela militar de Chorrillos "CEB"?:	X	X			X
11	¿Consideras tú que el acceso a los registramientos de inteligencia está disponible en plataformas educativas como la plataforma virtual de la EMCH?:	X	X			X
21	¿Consideras que la plataforma de aprendizaje electrónico desarrollada sitio web de la EMCH – "CEB" Facilita el estudio básico del área de operaciones?:	X	X			X
31	¿Consideras tú que el nivel de aplicativos de inteligencia artificial en la EMCH facilita la obtención de información para el estudio básico de inteligencia?:	X	X			X
41	¿Consideras tú que los docentes según capacitados en el empleo de la plataformas educación virtual para la aplicación del DICE?:	X	X			X
91	¿Consideras tú que el cadete de inteligencia está familiarizado con el uso de plataformas virtuales de la EMCH, para la elaboración del DICE?:	X	X			X
81	¿Consideras tú que la asignatura de Ciber inteligencia contribuye a analizar del adversario y/o amenaza?:	X	X			X
02	¿Consideras tú necesario que mayor cantidad de horas académicas en tema de navegación de IA como parte de la asignatura de Ciber inteligencia?:	X	X			X
22	¿Consideras tú importante incrementar la cantidad de horas en el empleo de dronas diversos como parte de la formación académica del cadete de inteligencia?:	X	X			X
42	¿Consideras tú relevante para la formación de los cadetes del arma de inteligencia la certificación en el manejo de dronas?:	X				X
62	¿Consideras tú que la cantidad de horas que emplean los cadetes de inteligencia en simuladores tácticos es óptimo o adecuado?:	X	X			X
52	¿Consideras tú relevante la implementación de sistemas de simulación tácticos tales como mio, electricios en la carta y otros como complemento en la instrucción de los cadetes de inteligencia?:	X		X		

pertinencia: El ítem corresponde al concepto teórico formulado.

relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

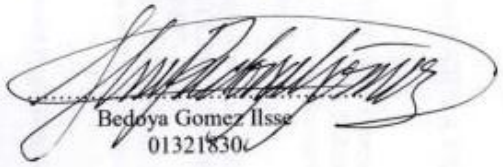
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [ ]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr.: Bedoya Gomez Ilsse

DNI: **01321830** **N° de colegiatura:** .....



Bedoya Gomez Ilsse
01321830

CARTA DE PRESENTACIÓN

DR: CALLA COLANA GODOFREDO JORGE

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS.

Me es muy grato comunicarme con usted para expresarle mis saludos, y, asimismo, hacer de su conocimiento que, siendo cadetes de la Escuela Militar de Chorrillos "CFB", requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar la investigación para optar el título de Licenciado en Ciencias Militares.

El título del trabajo de investigación es: **"MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA EMCH "CORONEL FRANCISCO BOLOGNESI"**, y siendo imprescindible contar con la evaluación de docentes especializados para poder aplicar el instrumento en mención, he considerado conveniente recurrir a usted, ante su connotado conocimiento de la variable y problemática, y sobre el cual realiza su ejercicio profesional.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de operacionalización de las variables.
- Certificado de validez de contenido de los instrumentos.
- Protocolo de evaluación

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que presta a la presente.

Atentamente.

Firma
Leyva Vasquez Milena Nicool
D.N.I: 76562040
mleyvav@escuelamilitar.edu.pe

Firma
Llanos Salcedo Milagros Lila Flor
D.N.I: 73172364
mllanoss@escuelamilitar.edu.pe

Certificado de validez de contenido del instrumento que mide "Las tecnologías de la información y las comunicaciones en cadetes de inteligencia de la EMCH" "CORONEL FRANCISCO BOLOGNESI"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias/Observaciones
Dimensión 1: TECNOLOGÍA		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma presencial?	X		X		X		
2	¿Considera Ud. ¿Que la infraestructura en tecnología de información y comunicaciones de la EMCH "CFB" permiten desarrollar adecuadamente las asignaturas en forma virtual?	X		X		X		
3	¿Considera Ud. que el desarrollo de las tecnologías de la información y las comunicaciones en la EMCH es el adecuado para mi desempeño académico?	X		X		X		
4	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
5	¿Es importante que mis actividades académicas virtuales mantengan un buen nivel operativo?	X		X		X		
6	¿Considera Ud. que la EMCH dispone de la infraestructura necesaria para ejecutar las clases virtuales que complemente la instrucción de los cadetes?	X		X		X		
7	¿Considera Ud. que el nivel de conectividad que disponen los sistemas de la EMCH son adecuados para el desarrollo de las asignaturas de la EMCH?	X		X		X		
15	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
17	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH permite reforzar las clases impartidas?	X		X		X		
21	¿Considera Ud. que el sistema administrativo educativo "Jaguar" de la EMCH es adecuado para el proceso educativo?	X		X		X		
24	¿Considera Ud. que el cadete de inteligencia tiene un fácil acceso a las evaluaciones empleando la plataforma virtual?	X		X		X		
Dimensión 2: HERRAMIENTAS								
8	¿Considera Ud. que el nivel de operatividad de la plataforma de aprendizaje electrónico de la EMCH ~~es~~ óptimo?	X		X		X		

9	¿Considera Ud. que la cantidad de eventos y compromisos virtuales son suficientes en la EMCH "CFB"?	X		X		X		
10	¿Considera Ud. que el nivel de empleo del correo electrónico institucional de la EMCH es el adecuado en la Escuela militar de Chorrillos "CFB"?	X		X		X		
11	¿Considera Ud. que el acceso a los reglamentos de inteligencia está disponible en las plataformas educativas como la biblioteca virtual de la EMCH?	X		X		X		
12	¿Considera que la plataforma de aprendizaje electrónico denominada sitio web de la EMCH – "CFB" facilita el estudio básico del área de operaciones?	X		X		X		
13	¿Considera Ud. que el nivel de aplicativos de inteligencia artificial en la EMCH facilita la obtención de información para el estudio básico de inteligencia?	X		X		X		
14	¿Considera Ud. que los docentes están capacitados en el empleo de la plataforma de educación virtual para la aplicación del PICB?	X		X		X		
16	¿Considera Ud. que el cadete de inteligencia está familiarizado con el uso de plataformas virtuales de la EMCH, para la elaboración del PICB?	X		X		X		
18	¿Considera Ud. que la asignatura de Ciber inteligencia contribuye a análisis del adversario y/o amenza?	X		X		X		
19	¿Considera Ud. necesario una mayor cantidad de horas académicas en tema de navegación de IA como parte de la asignatura de Ciber inteligencia?	X		X		X		
20	¿Considera Ud. importante incrementar la cantidad de horas en el empleo de drones diversos como parte de la formación académica del cadete de inteligencia?	X		X		X		
22	¿Considera Ud. relevante para la formación de los cadetes del arma de inteligencia la certificación en el manejo de drones?	X		X		X		
23	¿Considera Ud. que la cantidad de horas que emplean los cadetes de inteligencia en simuladores tácticos es óptimo o adecuado?	X		X		X		
25	¿Considera Ud. relevante la implementación de sistemas de simulación táctica tales como tiro, ejercicios en la carta y otros como complemento en la instrucción de los cadetes de inteligencia?	X		X		X		

[1] **pertinencia**: El ítem corresponde al concepto teórico formulado.
[2] **relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Observaciones: _____

Opinión de aplicabilidad: **Aplicable [ ]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador Dr.: CALLA COLANA GODOFREDO JORGE

DNI: **25413288** **N° de colegiatura:** .....

.....
CALLA COLANA GODOFREDO JORGE
25413288

Anexo 8: Dictamen Revisor General (DINVEST)

PERÚ | Ministerio de Defensa | Ejército del Perú | Comando de Educación y Doctrina del Ejército | Escuela Militar de Chorrillos "CFB"

"Año del Bicentenario, de la consolidación de nuestra independencia y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DICTAMEN DEL REVISOR

VISTA LA TESIS:

"CAPACITACIÓN EN MEDIDAS DE CONTRAINTELIGENCIA Y SEGURIDAD DE LAS INSTALACIONES EN CADETES DE LA ESCUELA MILITAR DE CHORRILLOS "CFB" , 2024",

Y levantadas las observaciones prescritas durante el proceso de revisión de la referida tesis, presentada por los (las) graduandos (das):

LEYVA VÁSQUEZ, Milena Nicool.
LLANOS SALCEDO, Milagros Lila Flor.

SE CONSIDERA:

Que ha sido elaborada conforme a lo dispuesto por el artículo 41. ° del Reglamento del Sistema de Investigación de la EMCH "CFB" 2022 – 2026, declarándose que:

La Tesis se encuentra en situación de apto para la sustentación y que la DINVEST gestione la emisión de la Resolución Directoral que determine lugar y fecha para dicha sustentación.

Lima, 09 de diciembre de 2024

Mg. María Soledad Alza Salvatierra
Docente Revisor.
DNI: 40469174

Anexo 9: Acta de sustentación (DINVEST)

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho."

ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

ACTA DE SUSTENTACIÓN DE TESIS DE LA PROMOCIÓN CXXXI

En el distrito de Chorrillos de la ciudad de Lima, siendo las 11:00 horas del día 20 de diciembre de 2024, se dio inicio a la sustentación de la Tesis titulada:

Medidas de contrainteligencia y seguridad de las instalaciones en cadetes de la EMCH "CFB" - 2024

Presentada por:

- BACH. Leyva Vásquez Milena Nicool
- BACH. Llanos Salcedo Milagros Lila Flor

Ante el Jurado de Sustentación de Tesis nombrado por la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y conformado por:

- Presidente: Dr. Yataco Velasquez, Luis Andrés
- Secretario: Mg. Alva Salvatierra, María Soledad
- Vocal: Dra. Baldeón Canchan, Maritza Roxana.

Concluida la sustentación, los miembros del Jurado dictaminaron:

APROBADA POR EXCELENCIA ( ); APROBADA POR UNANIMIDAD ( ); APROBADA POR MAYORÍA (X); OBSERVADA ( ); DESAPROBADA ( )

Siendo las 11:45 horas del día 20 de diciembre de 2024, se dio por concluido el presente acto académico, firmando los miembros del Jurado.

VOCAL

SECRETARIO

PRESIDENTE