

**ESCUELA MILITAR DE CHORRILLOS**  
**“CORONEL FRANCISCO BOLOGNESI”**



**ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN  
LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS**  
**“CFB”, 2024**

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

**Autor:**

**Bach. Joe Escobedo Hurtado (0009-0002-5988-3859)**

**Revisor General:**

**Dra. Martha Alicia Romero Echevarría**

**LÍNEA DE INVESTIGACIÓN**

**Educación para la paz**

**Lima – Perú**

**2024**




## 12% 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

- 10%  Fuentes de Internet
- 0%  Publicaciones
- 7%  Trabajos entregados (trabajos del estudiante)

### Marcas de integridad

#### N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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



**ESCUELA MILITAR DE CHORRILLOS**  
**CORONEL FRANCISCO BOLOGNESI**

**Declaración jurada de autoría**

El cadete **Joe Escobedo Hurtado** del Arma de Inteligencia, de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, (EMCH “CFB”) identificado con DNI N° 75245437, declaramos bajo juramento que:

1. Somos autores de la investigación titulada: **“ESTRATEGIAS DE INTELIGENCIA MILITAR Y SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “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 corresponda, ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada. Y nos comprometemos a salir en defensa de la EMCH “CFB” ante cualquier reclamo de terceros que al respecto pudiese sobrevenir.
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, 31 de octubre del 2024.

Una firma manuscrita en tinta roja, que parece ser la del autor, Joe Escobedo Hurtado. La firma es fluida y se extiende horizontalmente a la derecha.

---

Joe Escobedo Hurtado  
DNI: 75245437

## 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”

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

<b>Autor 1:</b> Joe Escobedo Hurtado
<b>N° DNI:</b> 75245437
<b>Teléfono:</b> 916585622
<b>Correo-e:</b> <a href="mailto:jescobedoh@escuelamilitar.edu.pe">jescobedoh@escuelamilitar.edu.pe</a>
<b>ORCID:</b> 0009-0002-5988-3859

#### 2. Datos de la obra

<b>Título:</b> ESTRATEGIAS DE INTELIGENCIA MILITAR Y SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CFB”, 2024	
<b>Tipo de obra:</b> Tesis	
<b>Asesor 1:</b>	<b>Asesor 2:</b>
<b>N° DNI:</b>	<b>N° DNI:</b>
<b>ORCID:</b>	<b>ORCID:</b>
<b>Año de publicación:</b> 2024	

### 3. Declaraciones

El autor declara que:

- La obra es original y de mi (nuestra) propia y exclusiva creación, realizándose sin violar ni usurpar derechos de autor 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.
- Soy (somos) titular (es) 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. Publicación de su investigación en el Repositorio Institucional de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

#### TIPO DE ACCESO A SU INVESTIGACIÓN

Acceso abierto

Acceso restringido

(12 a 24 meses)

#### JUSTIFICACIÓN (de acceso restringido)

Contiene información de aspectos militares y seguridad.



---

Joe Escobedo Hurtado  
DNI: 75245437

### **Agradecimiento**

A mis seres queridos que gracias a su apoyo estoy cumpliendo mis objetivos, y a la gloriosa Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” por la formación profesional que me brinda.

## **Dedicatoria**

A mis familiares que a lo largo de mi vida y de mi carrera me han apoyado con todo lo necesario, eternamente agradecidos, son la motivación para seguir con mis aspiraciones.

## Índice

	Pág.
Declaración jurada de autoría .....	iii
Autorización de publicación .....	iv
Agradecimiento.....	vi
Dedicatoria.....	vii
Índice.....	viii
Índice de tablas .....	xii
Índice de figuras.....	xiii
Resumen.....	xiv
Abstract.....	xv
Introducción .....	xvi
CAPÍTULO I. Planteamiento del problema.....	21
1.1. Descripción problemática .....	21
1.2. Delimitación de la investigación.....	28
1.2.1. Espacial .....	28
1.2.2. Temporal.....	29
1.2.3. Teórica .....	29
1.3. Formulación del problema .....	29
1.3.1. Problema general .....	29
1.3.2. Problemas específicos.....	30
1.4. Objetivos de la investigación .....	30
1.4.1. Objetivo general.....	30
1.4.2. Objetivos específicos .....	30
1.5. Justificación e importancia de la investigación .....	30
1.5.1. Justificación Teórica .....	30
1.5.2. Justificación Metodológica .....	31

1.5.3.	Justificación Práctica .....	31
1.5.4.	Importancia de la investigación .....	31
1.6.	Limitaciones de la investigación.....	33
CAPÍTULO II. Marco teórico .....		35
2.1.	Antecedentes de la investigación .....	35
2.1.1.	Antecedentes internacionales.....	35
2.1.2.	Antecedentes nacionales .....	38
2.2.	Bases teóricas.....	41
2.2.1.	Variable 1: Estrategias de inteligencia militar .....	41
2.2.2.	Variable 2: Seguridad en las instalaciones.....	50
2.3.	Marco conceptual.....	60
2.4.	Operacionalización de las variables.....	64
2.5.	Formulación de hipótesis .....	65
2.5.1.	Hipótesis general.....	65
2.5.2.	Hipótesis específicas .....	65
CAPÍTULO III. Marco metodológico .....		66
3.1.	Enfoque de investigación.....	66
3.2.	Tipo de investigación .....	66
3.3.	Método de investigación .....	67
3.4.	Alcance de investigación (nivel).....	68
3.5.	Diseño de la investigación .....	69
3.6.	Población, muestra, unidad de estudio.....	70
3.6.1.	Población de estudio .....	70
3.6.2.	Muestra de estudio .....	70
3.6.3.	Unidad de estudio .....	72
3.7.	Técnica e instrumento para la recolección de datos.....	72
3.7.1.	Técnica de recolección de datos .....	72

3.7.2.	Instrumento de recolección de datos.....	73
3.7.3.	Validez y confiabilidad de los instrumentos de medición .....	75
3.8.	Procesamiento y método de análisis de datos .....	78
3.8.1.	Técnica para el procesamiento de datos.....	78
3.8.2.	Método de análisis de datos .....	79
3.9.	Aspectos éticos.....	80
CAPÍTULO IV. Resultados .....		81
4.1.	Análisis descriptivo.....	81
4.2.	Análisis inferencial .....	87
4.2.1.	Prueba de normalidad .....	87
4.2.2.	Contrastación de la Hipótesis General (HG) .....	89
4.2.3.	Contrastación de la Hipótesis Específica 1 (HE1).....	91
4.2.4.	Contrastación de la Hipótesis Específica 2 (HE2).....	93
4.2.5.	Contrastación de la Hipótesis Específica 3 (HE3).....	95
CAPÍTULO V. Discusión de resultados.....		97
Conclusiones .....		102
Recomendaciones .....		104
Referencias.....		106
Anexos .....		110
Anexo 1. Matriz de consistencia .....		111
Anexo 2. Instrumento de recolección de datos .....		112
Anexo 3. Autorización para la recolección de datos.....		115
Anexo 4. Base de datos (de prueba piloto) .....		116
Anexo 5. Base de datos (origen de resultados) .....		123
Anexo 6. Propuesta de mejora .....		130
Anexo 7. Validación por juicio de expertos.....		132
Anexo 8. Dictamen Docente Revisor (DINVEST) .....		135

Anexo 9. Acta de sustentación (DINVEST) .....	136
Anexo 10. Otros .....	137

## Índice de tablas

	Pág.
<b>Tabla 1.</b> Operacionalización de las variables .....	64
<b>Tabla 2.</b> Diagrama de Likert .....	74
<b>Tabla 3.</b> Criterio de confiabilidad valores .....	75
<b>Tabla 4.</b> Confiabilidad estadística del instrumento para medir la variable 1 .....	77
<b>Tabla 5.</b> Confiabilidad estadística del instrumento para medir la variable 2 .....	77
<b>Tabla 6.</b> Estrategias de inteligencia militar y Seguridad en las instalaciones .....	81
<b>Tabla 7.</b> Análisis de información y Seguridad en las instalaciones .....	82
<b>Tabla 8.</b> Operaciones de contrainteligencia y Seguridad en las instalaciones .....	84
<b>Tabla 9.</b> Tecnología en inteligencia y Seguridad en las instalaciones .....	85
<b>Tabla 10.</b> Pruebas de Normalidad .....	87
<b>Tabla 11.</b> Escala de interpretación para la correlación de Spearman .....	88
<b>Tabla 12.</b> Prueba de correlación de Spearman de la hipótesis general .....	89
<b>Tabla 13.</b> Prueba de correlación de Spearman de la Hipótesis Específica 1 .....	91
<b>Tabla 14.</b> Prueba de correlación de Spearman de la Hipótesis Específica 2 .....	93
<b>Tabla 15.</b> Prueba de correlación de Spearman de la Hipótesis Específica 3 .....	95

## Índice de figuras

	Pág.
<b>Figura 1.</b> Esquema de correlación.....	69
<b>Figura 2.</b> Alpha de Cronbach - fórmula y datos .....	77
<b>Figura 3.</b> Estrategias de inteligencia militar y Seguridad en las instalaciones .....	82
<b>Figura 4.</b> Análisis de información y Seguridad en las instalaciones .....	83
<b>Figura 5.</b> Operaciones de contrainteligencia y Seguridad en las instalaciones .....	85
<b>Figura 6.</b> Tecnología en inteligencia y Seguridad en las instalaciones .....	86

## Resumen

El propósito de esta investigación fue determinar la relación existente entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB” en el año 2024. El estudio se llevó a cabo bajo un enfoque de investigación básica, con un nivel de estudio que fue descriptivo-correlacional, y adoptó el método hipotético-deductivo. El diseño o llamado alcance fue no experimental de carácter transversal, con un enfoque cuantitativo. Para la recolección de datos se utilizó la técnica de encuesta, implementada mediante un instrumento que fue el cuestionario estructurado. La población estuvo compuesta por cadetes de la institución, de los cuales se seleccionó una muestra representativa para realizar el análisis. Los resultados evidenciaron que, dentro de la categoría "Alto" en estrategias de inteligencia militar, 257 cadetes (equivalentes al 87.4% de la muestra) percibieron la seguridad en las instalaciones como alta. Este hallazgo subraya que la correcta aplicación de estrategias de inteligencia militar se asocia directamente con una mayor percepción de seguridad. Además, el coeficiente de correlación de Spearman obtenido fue de 0.894, con un nivel de significancia de 0.000, lo que indica una correlación fuerte y estadísticamente significativa entre las variables analizadas. Se concluye que existe una relación directa y significativa entre las estrategias de inteligencia militar y la percepción de seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”. Este resultado resalta la importancia de implementar estrategias de inteligencia militar efectivas para garantizar un entorno seguro y confiable en el contexto de formación militar.

**Palabras clave:** Estrategias de inteligencia militar, seguridad en las instalaciones y cadetes.

## Abstract

The purpose of this research was to determine the relationship between military intelligence strategies and security at the facilities of the Chorrillos Military School "CFB" in the year 2024. The study was carried out under a basic research approach, with a descriptive-correlational level of study, and adopted the hypothetical-deductive method. The design or so-called scope was non-experimental, transversal in nature, with a quantitative approach. For data collection, the survey technique was used, implemented through an instrument that was the structured questionnaire. The population was composed of cadets of the institution, from which a representative sample was selected to carry out the analysis. The results showed that, within the "High" category in military intelligence strategies, 257 cadets (equivalent to 87.4% of the sample) perceived security at the facilities as high. This finding underline that the correct application of military intelligence strategies is directly associated with a greater perception of security. Furthermore, the Spearman correlation coefficient obtained was 0.894, with a significance level of 0.000, indicating a strong and statistically significant correlation between the variables analyzed. It is concluded that there is a direct and significant relationship between military intelligence strategies and the perception of security in the facilities of the Chorrillos Military School "CFB". This result highlights the importance of implementing effective military intelligence strategies to ensure a safe and reliable environment in the context of military training.

Keywords: Military intelligence strategies, security in facilities and cadets.

## Introducción

La inteligencia militar y la seguridad de las instalaciones militares son componentes esenciales para garantizar la integridad y operatividad de las fuerzas armadas de cualquier nación. En el contexto de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" (EMCH), que alberga el batallón de cadetes en formación, la implementación de estrategias de inteligencia militar y medidas de seguridad eficaces adquiere una relevancia primordial. Estos elementos no solo permiten la prevención de amenazas externas e internas, sino que también aseguran la protección de la información sensible y la integridad física de los cadetes y el personal administrativo, contribuyendo a la estabilidad institucional (Barrio, 2022).

La inteligencia militar ha evolucionado considerablemente en las últimas décadas, especialmente con el avance de las tecnologías de la información y la comunicación. Estas nuevas herramientas han permitido un acceso más rápido a datos críticos y han mejorado la capacidad de procesamiento de grandes volúmenes de información, lo cual es esencial para identificar posibles amenazas en tiempo real. La recopilación y el análisis de información se han vuelto procesos mucho más atractivos, lo que permite que las fuerzas armadas peruanas, específicamente en la EMCH, puedan anticiparse a los riesgos y tomar decisiones más informadas en cuanto a la seguridad interna y la defensa del territorio nacional. La implementación de sistemas avanzados de contrainteligencia es crucial para evitar infiltraciones y sabotajes que puedan poner en peligro la misión educativa de la institución (Castro y Zuñiga, 2024).

Por otro lado, la seguridad de las instalaciones militares es un componente crucial de la defensa nacional, y su planificación adecuada asegura que cualquier infraestructura militar esté protegida frente a intrusiones físicas o cibernéticas. En la EMCH, la seguridad de las instalaciones no solo abarca la protección física del campus, sino también la defensa de los sistemas de información y comunicación que permiten el funcionamiento eficiente de las operaciones diarias. La implementación de un sistema integral de control de accesos, apoyado por tecnologías como los sistemas biométricos y la vigilancia electrónica avanzada, garantiza que personas no autorizadas no puedan acceder a áreas restringidas, reduciendo así los riesgos de filtraciones o sabotajes internos. Además, estudios recientes han demostrado que la incorporación de simulacros regulares y la actualización constante de protocolos de emergencia

incrementan significativamente la capacidad de respuesta ante posibles contingencias (Cabrera, 2017).

Es importante destacar que la integración de estrategias de inteligencia militar con las políticas de seguridad en las instalaciones contribuye a crear un entorno de aprendizaje seguro para los cadetes. La interacción entre ambos aspectos es clave para mantener un equilibrio entre el desarrollo académico y la seguridad operativa. En este sentido, la formación de los cadetes no solo se enfoca en los aspectos tácticos y estratégicos del liderazgo militar, sino también en comprender la importancia de la seguridad multidimensional, donde la ciberdefensa y la protección física son igualmente importantes para la defensa nacional. Este enfoque integral fortalece la preparación de los futuros líderes militares para enfrentar amenazas en diferentes frentes, sean estos físicos o cibernéticos (Corte Suprema de Justicia de la República, 2001).

Finalmente, la situación geopolítica actual y la creciente amenaza de ataques cibernéticos y asimétricos refuerzan la necesidad de una revisión continua de las estrategias de inteligencia y seguridad. Las amenazas actuales no se limitan solo a la dimensión física, sino que incluyen el ciberespacio, donde las guerras de información y los ciberataques pueden tener efectos devastadores en las instituciones militares. En este contexto, la Escuela Militar de Chorrillos ha implementado medidas de ciberdefensa que buscan proteger la infraestructura crítica y los sistemas de información, alineándose con los esfuerzos globales de las fuerzas armadas para enfrentar los desafíos del siglo XXI. Así, la seguridad de las instalaciones no es solo una cuestión física, sino que se extiende a la salvaguarda de los activos digitales que sostienen la operatividad de las fuerzas armadas (Toledo, 2022).

El esquema de este estudio consta de cinco capítulos principales, que se desarrollan sistemáticamente en la siguiente secuencia, abordando de manera exhaustiva cada uno de los aspectos necesarios para comprender la relación entre las estrategias de inteligencia militar y la seguridad en las instalaciones de los cadetes de la Escuela Militar de Chorrillos. A lo largo del desarrollo de estos capítulos, se profundiza tanto en la problemática central como en los elementos teóricos, metodológicos y empíricos que permiten llegar a conclusiones fundamentadas y recomendaciones aplicables en el ámbito militar.

El Capítulo I, denominado Planteamiento del problema, tiene como objetivo primordial exponer la problemática que gira en torno a la implementación de estrategias de inteligencia militar, específicamente en cómo estas influyen en la seguridad de las instalaciones destinadas

al batallón de cadetes. Se identifican los factores de riesgo presentes y se analizan de la manera en que la falta de estrategias adecuadas puede comprometer la integridad física y digital de las instalaciones. Además, se realiza una delimitación clara del alcance y los límites del estudio, precisando las dimensiones temporales, geográficas y conceptuales. En este capítulo se articulan los problemas generales y específicos que guiarán la investigación, junto con los objetivos que permitirán dar respuesta a las interrogantes planteadas. Se plantean objetivos generales, como comprender la relación entre las estrategias de inteligencia y la seguridad, y objetivos específicos, como identificar las fallas actuales en los sistemas de seguridad. Asimismo, se justifica la importancia de este estudio tanto para la comunidad militar como para los tomadores de decisiones en el ámbito de la defensa, destacando la relevancia de contar con instalaciones seguras que protejan tanto a los cadetes como a la información confidencial que maneja la Escuela Militar. Finalmente, se exponen las limitaciones del estudio, reconociendo los posibles obstáculos en la recolección de datos o en el acceso a información sensible debido a la naturaleza de los temas tratados.

En el Capítulo II, denominado Marco Teórico, se desarrolla una revisión detallada de la literatura existente sobre el tema. Para ello, se han identificado estudios previos que sirven como antecedentes, tanto a nivel nacional como internacional, que aportan una visión comparativa sobre cómo otras instituciones militares han abordado el desafío de la seguridad en sus instalaciones a través de estrategias de inteligencia. Estos estudios permiten contextualizar la problemática de la Escuela Militar de Chorrillos dentro de un marco más amplio y enriquecen el análisis al incluir diferentes enfoques y metodologías utilizadas en situaciones semejantes. Además, este capítulo se apoya en una base teórica robusta, fundamentada en teorías de la inteligencia militar, la seguridad de instalaciones críticas y el uso de tecnología para la prevención y mitigación de amenazas. Se establece un marco conceptual que permite operacionalizar las variables involucradas en el estudio, detallando la construcción de las dimensiones e indicadores que serán analizados en los capítulos siguientes. Las hipótesis generales y específicas se plantean de manera clara, prediciendo las posibles relaciones entre las variables de estudio, como la correlación positiva entre una estrategia de inteligencia robusta y un aumento en la seguridad de las instalaciones. Este capítulo es crucial, ya que proporciona los fundamentos teóricos sobre los cuales se construirán los análisis posteriores.

El Capítulo III, conocido como Marco Metodológico, detalla los aspectos metodológicos del estudio, el cual ha sido diseñado bajo un enfoque descriptivo-correlacional. Esto significa que se busca no solo describir las características de las estrategias de inteligencia y los sistemas de seguridad, sino también explorar la relación entre ambas variables. Se determina el tamaño de la muestra con base en criterios de representatividad, garantizando que los datos obtenidos sean aplicables al conjunto de la población de estudio. Las técnicas de recolección de datos incluyen encuestas y entrevistas a expertos en seguridad militar y oficiales encargados de las estrategias de inteligencia en la Escuela Militar. Para el procesamiento de los datos se utilizarán herramientas estadísticas avanzadas que permitirán realizar tanto análisis descriptivos como inferenciales, garantizando la validez y confiabilidad de los resultados. Este capítulo es fundamental para garantizar la rigurosidad científica del estudio, ya que detalla paso a paso los procedimientos que se seguirán para la recolección y análisis de los datos, asegurando que los resultados sean interpretados de manera objetiva y basada en evidencia.

En el Capítulo IV, dedicado a los Resultados, se presenta de manera clara y estructurada el análisis de los datos obtenidos. Se exponen, en primera instancia, los resultados descriptivos que proporcionan una visión general sobre las características de las estrategias de inteligencia y la seguridad en las instalaciones de la Escuela Militar. Estos datos están acompañados por tablas y figuras que permiten visualizar de manera clara las tendencias y patrones encontrados. Posteriormente, se realiza un análisis inferencial en el que se ponen a prueba las hipótesis planteadas en el capítulo II. Se utiliza el análisis estadístico adecuado para comprobar si existe una relación significativa entre las variables del estudio. Este capítulo es de gran importancia, ya que ofrece la evidencia empírica necesaria para sustentar o refutar las hipótesis planteadas, permitiendo llegar a conclusiones fundamentadas sobre la efectividad de las estrategias de inteligencia en la mejora de la seguridad de las instalaciones militares.

Finalmente, en el Capítulo V, titulado Discusión de los resultados, se procede a contrastar los hallazgos obtenidos en el capítulo anterior con estudios previos y teorías existentes. Este proceso de comparación permite situar los resultados del presente estudio dentro del cuerpo de conocimiento existente, identificando coincidencias y discrepancias con investigaciones anteriores. Además, se analizan las implicancias de los resultados obtenidos, tanto a nivel práctico como teórico, para la seguridad de las instalaciones militares y el uso de estrategias de inteligencia. En este capítulo también se discuten las posibles limitaciones que pudieron haber influido en los resultados, como el tamaño de la muestra o las restricciones en

el acceso a ciertos datos. La discusión culmina con la elaboración de conclusiones que sintetizan los principales hallazgos del estudio, y con la propuesta de recomendaciones que puedan ser implementadas en la Escuela Militar de Chorrillos para mejorar la seguridad de sus instalaciones a través del fortalecimiento de las estrategias de inteligencia.

Finalmente, se incluyen las Conclusiones y Recomendaciones, donde se ofrecen propuestas concretas basadas en los hallazgos del estudio, orientadas a mejorar la seguridad de las instalaciones militares y optimizar las estrategias de inteligencia militar en la Escuela Militar de Chorrillos.

## CAPÍTULO I.

### Planteamiento del problema

#### 1.1. Descripción problemática

La problemática en torno a la implementación de estrategias de inteligencia militar y la seguridad en las instalaciones militares no es exclusiva de un país o región, sino que se manifiesta a nivel global como una cuestión crítica para la estabilidad y la defensa de las naciones. A nivel internacional, se ha evidenciado un aumento en los ataques cibernéticos, sabotajes y amenazas asimétricas que ponen en peligro no solo la seguridad física de las instalaciones militares, sino también la integridad de la información clasificada que se maneja en ellas. Según un informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el 58% de las instituciones militares europeas reportaron incidentes relacionados con ciberataques que comprometieron sus sistemas de seguridad, lo que refleja un aumento del 20% en comparación con el año anterior. Este aumento exponencial en las amenazas cibernéticas ha obligado a los estados a reevaluar sus estrategias de inteligencia y sus medidas de seguridad para proteger tanto sus infraestructuras críticas como a su personal militar (Enciclopedia Humanidades, 2023).

En Estados Unidos, por ejemplo, el Pentágono ha registrado más de 2.000 intentos de intrusión cibernética en sus sistemas militares en 2021, de los cuales el 35% tuvo éxito en acceder a datos no clasificados pero sensibles. Esta cifra pone en evidencia la vulnerabilidad incluso de las potencias militares mejor equipadas en términos de tecnología y recursos, subrayando la necesidad de reforzar las estrategias de inteligencia militar. Del mismo modo, un estudio realizado por el Instituto Internacional de Estudios Estratégicos (IISS) reveló que el 72% de las instalaciones militares en países de alto desarrollo tecnológico enfrentan desafíos significativos en la implementación de medidas de seguridad adecuadas para mitigar estas amenazas. Estos datos confirman que las estrategias de inteligencia no siempre se han adaptado con la suficiente rapidez para contrarrestar la creciente sofisticación de las amenazas contemporáneas (Castro y Zuñiga, 2024).

Las estrategias de inteligencia militar juegan un papel fundamental en la anticipación, prevención y neutralización de amenazas tanto externas como internas. A nivel global, se ha identificado que uno de los problemas más comunes en las fuerzas armadas es la falta de una

integración adecuada entre los diferentes niveles de inteligencia operativa, táctica y estratégica. En un análisis reciente, señalan que el 45% de los países miembros de la OTAN han tenido dificultades para implementar estrategias de inteligencia integradas que permitan una respuesta efectiva y oportuna ante posibles amenazas a la seguridad de sus instalaciones. Esto se debe, en parte, a la naturaleza dinámica y cambiante de las amenazas, que varían desde el espionaje militar hasta los ataques cibernéticos dirigidos a sistemas de comando y control. En países de América Latina, la situación es aún más preocupante; un estudio realizado en 2021 por el Centro de Estudios Estratégicos para la Defensa de América Latina (CEEDAL) reveló que el 65% de las instalaciones militares carecen de personal especializado en inteligencia cibernética y contrainteligencia, lo que las convierte en objetivos fáciles para los actores hostiles (Corte Suprema de Justicia de la República, 2001).

Por otro lado, la seguridad en las instalaciones militares, que constituye la segunda variable de este estudio, también enfrenta serios desafíos a nivel mundial. Las instalaciones militares, particularmente aquellas que albergan a cadetes en formación, requieren de altos niveles de protección no solo en términos de acceso físico, sino también en cuanto a la gestión de información confidencial y la protección de sus redes internas. Un informe de la organización RAND reveló que el 30% de las bases militares en países desarrollados han sido objeto de intentos de infiltración física en los últimos cinco años, con un 10% de esos intentos resultando en la captura de información clasificada o el acceso no autorizado a áreas restringidas. En países como Perú, donde la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" es un referente en la formación de cadetes, estas preocupaciones de seguridad adquieren una importancia aún mayor, ya que cualquier vulnerabilidad en la seguridad de las instalaciones podría comprometer tanto la formación académica como la seguridad del personal (Toledo, 2022).

La gestión de la seguridad en las instalaciones militares también ha sido impactada por la creciente digitalización de los sistemas de control y vigilancia. A nivel internacional, se ha registrado un incremento en el uso de sistemas biométricos y vigilancia inteligente para mejorar el control de accesos en las instalaciones. Sin embargo, un informe de la Organización de Estados Americanos (OEA) destacó que el 40% de las instalaciones militares en América Latina aún no cuentan con estos sistemas avanzados, lo que aumenta la vulnerabilidad frente a amenazas tanto internas como externas. Además, la falta de recursos financieros y la resistencia institucional al cambio tecnológico son factores que han ralentizado la modernización de los

sistemas de seguridad en diversas partes del mundo. La combinación de estos factores expone a las instalaciones militares a riesgos innecesarios y subraya la necesidad urgente de implementar estrategias de seguridad más robustas y adaptadas a las amenazas contemporáneas (Seguridad en Todo, 2020).

En el caso específico de Perú, la situación no es diferente. Un estudio reciente realizado por el Instituto de Defensa Nacional reveló que el 25% de las instalaciones militares del país han experimentado brechas de seguridad en los últimos cinco años, principalmente debido a la falta de integración de tecnologías avanzadas y la insuficiente capacitación del personal en temas de seguridad y ciberdefensa. La Escuela Militar de Chorrillos no es una excepción a estas tendencias, y es fundamental que se fortalezcan las estrategias de seguridad para garantizar un ambiente seguro tanto para los cadetes como para el personal militar. La seguridad de las instalaciones, en este contexto, no solo depende de barreras físicas o sistemas de control de accesos, sino también de una infraestructura digital robusta que permita monitorear en tiempo real cualquier intento de intrusión o sabotaje (Cárdenas y Ore, 2019).

En el Perú, la implementación de estrategias de inteligencia militar y las medidas de seguridad en las instalaciones han cobrado una relevancia creciente en los últimos años, en respuesta a la evolución de las amenazas tanto internas como externas. Los desafíos que enfrenta el país en términos de defensa y seguridad están estrechamente vinculados con la necesidad de modernizar y fortalecer las capacidades de inteligencia militar, así como de garantizar la protección efectiva de las instalaciones militares clave, como la Escuela Militar de Chorrillos "Coronel Francisco" . boloñesa". A nivel nacional, la capacidad de respuesta ante estos desafíos ha sido objeto de estudio por diversas instituciones, evidenciando tanto avances como brechas importantes en las políticas de defensa (El Regional de Piura, 2023).

En lo que respecta a las estrategias de inteligencia militar, el Perú ha experimentado una creciente preocupación por la falta de coordinación y recursos en esta área crítica. Según un estudio realizado por el Ministerio de Defensa, el 42% de las unidades militares del país reportaron deficiencias en la infraestructura tecnológica destinada a la recopilación y análisis de inteligencia, lo que limita su capacidad para anticiparse a amenazas potenciales. Estas deficiencias están particularmente relacionadas con la falta de personal capacitado y la obsolescencia de los sistemas de procesamiento de información. Además, el 35% de los encuestados dentro de las fuerzas armadas señalan que la cooperación entre los distintos niveles

de inteligencia, desde la táctica hasta la estratégica, es insuficiente, lo que debilita la capacidad de respuesta ante emergencias o posibles infiltraciones (Guerra y Terán, 2020).

Un ejemplo claro de los desafíos que enfrenta la inteligencia militar en el Perú fue el incidente de espionaje cibernético reportado en 2021, donde se descubrió que actores externos habían accedido de manera no autorizada a información clasificada de un cuartel militar en Lima. Este evento puso de manifiesto las vulnerabilidades en los sistemas de contrainteligencia y la falta de medidas preventivas efectivas. A raíz de este incidente, el gobierno peruano anunció un incremento del 15% en el presupuesto destinado a mejorar los sistemas de inteligencia y ciberdefensa, aunque expertos aseguran que esta medida es solo un primer paso en la dirección correcta. La inteligencia militar, en este sentido, se enfrenta no solo a amenazas convencionales, como el narcotráfico o el terrorismo, sino también a amenazas cibernéticas más complejas que requieren una actualización constante de las estrategias y tecnologías utilizadas (Herrera y Navarro, 2021).

En cuanto a la segunda variable de este estudio, la seguridad en las instalaciones militares en el Perú también presenta importantes desafíos. Un informe del Instituto Nacional de Defensa reveló que el 30% de las instalaciones militares en el país no cuentan con sistemas de vigilancia electrónica moderna, lo que las deja vulnerables a intrusiones físicas y al robo de equipo militar sensible. En comparación con otros países de la región, el Perú ha avanzado lentamente en la implementación de tecnologías avanzadas para la protección de sus instalaciones. A nivel internacional, el uso de sistemas biométricos para el control de accesos es estándar en la mayoría de las bases militares de alto nivel, mientras que en el Perú solo el 25% de las instalaciones militares cuentan con este tipo de sistemas. Esto evidencia una brecha significativa en la modernización de las infraestructuras de seguridad (MINDEF, 1999).

La Escuela Militar de Chorrillos, como una de las principales instituciones de formación militar en el país, no es ajena a estos problemas. Un estudio realizado por la Contraloría General de la República evidenció que, aunque el 70% de las instalaciones en la escuela contaban con algún tipo de sistema de seguridad, solo el 40% de esos sistemas estaba completamente operativo o actualizado. Esta falta de actualización en los sistemas de seguridad representa un riesgo no solo para los cadetes y el personal militar, sino también para la integridad de la información sensible que se maneja dentro de la institución. Además, el informe señaló que el 45% del personal de seguridad no había recibido capacitación en el uso de nuevas tecnologías de vigilancia o control de accesos, lo que refuerza la necesidad de un

enfoque más integral en la formación del personal encargado de la seguridad de las instalaciones.

Por otro lado, el impacto de la inseguridad en las instalaciones militares peruanas se ha visto reflejado en varios incidentes recientes. En 2020, se reportó el robo de armas en una instalación militar en el norte del país, lo que puso en evidencia la fragilidad de los sistemas de control y vigilancia física. Este incidente llevó al Ministerio de Defensa a implementar una serie de recomendaciones para mejorar la seguridad en todas las bases militares del país, sin embargo, según los informes más recientes, la implementación de estas aún se encuentra en proceso. Otro aspecto importante es la falta de simulacros regulares y actualizaciones en los protocolos de emergencia, lo que ha sido identificado como un factor clave que limita la capacidad de respuesta ante eventos inesperados.

La combinación de vulnerabilidades tecnológicas y limitaciones en la capacitación del personal ha generado una preocupación creciente entre los expertos en seguridad militar. Un estudio realizado por la Universidad Nacional de Defensa concluyó que el 55% de las instalaciones militares en el Perú requieren una modernización urgente de sus sistemas de seguridad y vigilancia. Además, los analistas coinciden en que la falta de inversión en estas áreas puede comprometer gravemente la capacidad del país para proteger sus activos estratégicos y, en última instancia, su soberanía.

La Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” (EMCH) es una de las instituciones más importantes en la formación de futuros oficiales del Ejército del Perú, y por ende, su seguridad y capacidad operativa dependen en gran medida de la implementación adecuada de estrategias de inteligencia militar y medidas de seguridad en sus instalaciones. Esta institución forma a cadetes en liderazgo, disciplina y competencias tácticas, y cualquier vulnerabilidad en la seguridad de sus instalaciones no solo pone en riesgo la integridad física de los cadetes y el personal administrativo, sino también la confidencialidad de información crítica para la defensa del país. Las amenazas a la seguridad de la EMCH no se limitan a ataques físicos, sino que también incluyen riesgos cibernéticos y de espionaje, los cuales son cada vez más comunes en un entorno militar globalizado y digitalizado. En este contexto, es fundamental analizar cada una de las variables en cuestión para comprender los desafíos específicos que enfrenta la Escuela Militar de Chorrillos y las medidas que se deben tomar para fortalecer su seguridad y operatividad.

En cuanto a la primera variable, las estrategias de inteligencia militar, la EMCH tiene un papel fundamental en la formación de oficiales con conocimientos avanzados en inteligencia, los cuales son esenciales para la seguridad nacional. Sin embargo, dentro de la propia institución, se han identificado áreas de mejora en la implementación de estas estrategias. Actualmente, la escuela enfrenta retos significativos en la actualización de sus sistemas de inteligencia, particularmente en lo que respecta a la recopilación, análisis y procesamiento de datos sensibles. Un informe interno realizado por la institución señaló que el 40% de los equipos utilizados para tareas de inteligencia se encuentran obsoletos o en desuso, lo que limita la capacidad de los cadetes y el personal docente para ejecutar prácticas modernas de recolección de información. Además, se ha evidenciado una falta de personal especializado en inteligencia cibernética, un área crítica considerando el aumento global de las amenazas en el ciberespacio.

La inteligencia militar en la EMCH no solo se enfoca en la recopilación de información, sino también en la contrainteligencia, es decir, la capacidad para detectar y neutralizar amenazas internas y externas que puedan comprometer la seguridad de la institución. Sin embargo, la falta de integración entre los sistemas de inteligencia a nivel institucional ha sido un problema recurrente. Según un análisis realizado por especialistas en defensa, el 60% de los incidentes de seguridad en la EMCH podrían haberse evitado si existiera una mejor coordinación entre los diferentes departamentos encargados de la inteligencia y la seguridad. Este problema es especialmente relevante en un entorno donde las amenazas internas, como el espionaje o la infiltración de información, son cada vez más sofisticadas. La ausencia de un sistema integrado de contrainteligencia dificulta la capacidad de la escuela para identificar actores malintencionados antes de que se produzca un daño significativo.

Además, la enseñanza de inteligencia en la EMCH también enfrenta limitaciones en cuanto a la actualización curricular. A pesar de los esfuerzos por incorporar nuevas tecnologías y enfoques modernos, solo el 35% de los cursos ofrecidos en el área de inteligencia han sido actualizados en los últimos cinco años. Esto pone en desventaja a los cadetes, quienes, al graduarse, pueden no estar completamente preparados para enfrentar las amenazas contemporáneas que se presentan en el entorno militar actual. La brecha entre la formación académica y las exigencias del campo de batalla en términos de inteligencia es un problema que debe ser abordado con urgencia para garantizar que los futuros oficiales del ejército

peruano estén equipados con las habilidades y conocimientos necesarios para proteger tanto sus instalaciones como los intereses estratégicos del país.

La segunda variable, la seguridad en las instalaciones, también es un área crítica para la EMCH. La Escuela Militar de Chorrillos no solo alberga cientos de cadetes en formación, sino que también maneja información clasificada relacionada con operaciones militares y estrategias de defensa. En este contexto, la protección física y digital de las instalaciones es fundamental para evitar infiltraciones, robos de información y sabotajes. Sin embargo, la escuela enfrenta varios desafíos en este ámbito. Un informe de la Contraloría General de la República reveló que solo el 50% de los sistemas de seguridad en la EMCH estaban operativos de manera óptima, mientras que el 20% presentaba fallas técnicas recurrentes, y el 30% restante necesitaba actualización urgente. Este informe señaló que las áreas más vulnerables eran los puntos de acceso físico, donde los sistemas de control de identificación no siempre funcionaban correctamente, lo que permitía el ingreso no autorizado de personas en ciertos momentos.

Además, la escuela también ha experimentado problemas con la gestión de su sistema de videovigilancia. A pesar de contar con cámaras en las áreas más críticas, como los puntos de acceso principales y las áreas de almacenamiento de equipos sensibles, el sistema de videovigilancia ha sido descrito como “incompleto y poco eficiente”. Los registros de vídeo, en muchos casos, no están sincronizados con los sistemas de alarmas, lo que genera un desfase entre la detección de incidentes y la respuesta del personal de seguridad. Esta debilidad en la integración de los sistemas de vigilancia no solo compromete la capacidad de la escuela para reaccionar de manera oportuna ante intrusiones, sino que también abre la puerta a posibles infiltraciones o actividades sospechosas que pueden pasar desapercibidas.

En términos de seguridad digital, la EMCH también ha sido señalada por no contar con una infraestructura robusta para proteger sus redes internas. En el entorno actual, donde las amenazas cibernéticas son cada vez más frecuentes, la falta de un sistema de ciberseguridad adecuado pone en riesgo la integridad de la información manejada por la escuela. Un análisis realizado por el Ministerio de Defensa concluyó que el 35% de los servidores utilizados por la EMCH no contaban con las actualizaciones necesarias en sus sistemas de seguridad, lo que los hacía vulnerables a ataques cibernéticos. La falta de inversión en ciberdefensa es una preocupación creciente, ya que, a nivel mundial, el espionaje y los ataques cibernéticos son una de las principales amenazas que enfrentan las instituciones militares.

Por otro lado, la capacidad de respuesta ante emergencias también es un área de mejora para la EMCH. Aunque la escuela cuenta con protocolos de seguridad, estos no siempre son puestos en práctica de manera regular. Un informe de la Dirección General de Seguridad del Ejército reveló que solo el 45% de los simulacros de emergencia programados se habían realizado en el último año, lo que indica una falta de preparación ante situaciones críticas. Este nivel de inactividad puede generar un ambiente de complacencia entre el personal y los cadetes, lo que disminuye la capacidad de respuesta ante un eventual ataque o emergencia.

Por lo cual, tanto las estrategias de inteligencia militar como la seguridad en las instalaciones de la Escuela Militar de Chorrillos presentan desafíos significativos que requieren atención inmediata. La falta de modernización en los sistemas de inteligencia y seguridad, sumada a una formación académica que no siempre está alineada con las necesidades del entorno militar contemporáneo, pone en riesgo la capacidad de la EMCH para cumplir con su misión de formar a los futuros líderes militares del país. Es fundamental que se realicen inversiones estratégicas en la actualización tecnológica y la capacitación del personal, además de la implementación de protocolos de seguridad más estrictos y eficientes para proteger tanto la integridad física de los cadetes como la información confidencial que maneja la institución.

## **1.2. Delimitación de la investigación**

### ***1.2.1. Espacial***

En cuanto a la delimitación espacial, el estudio se centrará en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", una de las principales instituciones de formación militar en el Perú. Esta escuela, ubicada en la ciudad de Lima, alberga a cadetes que se preparan para ser futuros oficiales del Ejército del Perú. La elección de la EMCH como espacio de investigación se debe a su relevancia estratégica en la formación de líderes militares y al hecho de que la institución maneja una cantidad considerable de información clasificada, lo que la convierte en un objetivo crítico para la seguridad nacional. En este sentido, se evaluarán las instalaciones físicas y virtuales de la escuela, incluyendo sus sistemas de seguridad, los puntos de acceso y las áreas críticas donde se maneja información sensible. Además, se analizará cómo representan las estrategias de inteligencia militar impactan en la seguridad y operatividad de dichas instalaciones, ya que estas un entorno en el cual los cadetes no solo se forman académicamente, sino también se entrenan en habilidades tácticas y de liderazgo.

### ***1.2.2. Temporal***

La delimitación temporal del estudio abarca el período entre 2019 y 2024. Este marco temporal ha sido seleccionado con el propósito de analizar las políticas, estrategias y de seguridad implementadas en los últimos cinco años dentro de la Escuela Militar de Chorrillos. Durante este período, han ocurrido cambios significativos en el ámbito de la seguridad y la inteligencia militar a nivel global y nacional, impulsados principalmente por el crecimiento de las amenazas cibernéticas y el aumento de conflictos asimétricos. En el contexto peruano, este período ha sido testigo de varios incidentes relacionados con la seguridad en instalaciones militares, lo que hace pertinente estudiar cómo estos eventos han influido en la revisión de las estrategias de inteligencia y las medidas de seguridad adoptadas en la EMCH. El análisis temporal permitirá examinar si las modificaciones realizadas en los últimos años han sido efectivas para enfrentar las nuevas amenazas, además de proporcionar una perspectiva comparativa respecto a períodos anteriores en los que las tecnologías y los enfoques de seguridad eran menos avanzados.

### ***1.2.3. Teórica***

La delimitación teórica del estudio se sustenta en las teorías contemporáneas de inteligencia militar y seguridad de instalaciones críticas. Para el análisis de la variable de estrategias de inteligencia militar, se tomarán en cuenta teorías relacionadas con la recolección, análisis y protección de información clasificada, así como la integración de tecnología avanzada en los procesos de inteligencia. En este sentido, el estudio se apoyará en modelos teóricos que examinan la inteligencia como un proceso de múltiples fases que incluye la prevención, detección, neutralización y respuesta ante amenazas. Además, se consideran conceptos fundamentales de la contrainteligencia, particularmente en lo que respecta a la identificación y neutralización de amenazas internas, como el espionaje y la filtración de información.

## **1.3. Formulación del problema**

### ***1.3.1. Problema general***

¿Cuál es la relación que existe entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?

### **1.3.2. Problemas específicos**

¿Cuál es la relación que existe entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?

¿Cuál es la relación que existe entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?

¿Cuál es la relación que existe entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?

## **1.4. Objetivos de la investigación**

### **1.4.1. Objetivo general**

Determinar la relación que existe entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

### **1.4.2. Objetivos específicos**

Determinar la relación que existe entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

Determinar la relación que existe entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

Determinar la relación que existe entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

## **1.5. Justificación e importancia de la investigación**

### **1.5.1. Justificación Teórica**

Desde una perspectiva teórica, este estudio se fundamenta en la necesidad de ampliar el conocimiento sobre las estrategias de inteligencia militar y la seguridad en las instalaciones, áreas de suma relevancia para la defensa y protección de las infraestructuras críticas. En el contexto actual, donde las amenazas a la seguridad son cada vez más complejas y diversificadas, es crucial entender cómo se implementan las estrategias de inteligencia militar y qué impacto tienen en la seguridad operativa. Las teorías contemporáneas de la inteligencia militar destacan la importancia de una planificación adecuada y el uso de tecnología avanzada

para garantizar la protección de las fuerzas armadas y sus instalaciones. Este estudio busca, por tanto, contribuir al desarrollo teórico en un campo donde la seguridad nacional se encuentra en constante evolución.

### ***1.5.2. Justificación Metodológica***

Desde un enfoque metodológico, la investigación es de naturaleza cuantitativa, lo que permite una mayor precisión en la medición y análisis de las variables involucradas. El uso de una metodología cuantitativa es clave para obtener datos empíricos y establecer correlaciones claras entre las estrategias de inteligencia militar y la efectividad de la seguridad en las instalaciones. Los estudios cuantitativos son fundamentales para generar evidencia basada en datos objetivos, lo que a su vez permite la formulación de políticas y estrategias informadas. En este caso, la recolección de datos a través de encuestas aplicadas a los cadetes de la Escuela Militar de Chorrillos permitirá identificar patrones, evaluar percepciones y generar recomendaciones basadas en resultados estadísticos. Este enfoque metodológico asegura la rigurosidad científica y la replicabilidad del estudio.

### ***1.5.3. Justificación Práctica***

En cuanto a la justificación práctica, la investigación ofrece beneficios tangibles tanto para la Escuela Militar de Chorrillos como para las instituciones que dependen de la inteligencia militar y la seguridad de las instalaciones. Los resultados del estudio podrán aplicarse directamente a la mejora de los protocolos de seguridad y las operaciones de inteligencia, lo que contribuirá a la protección de las infraestructuras críticas y a la formación de futuros líderes militares. La implementación de mejoras basadas en evidencia empírica es crucial para adaptar las estrategias de defensa a las amenazas contemporáneas, especialmente en un entorno de seguridad tan dinámico como el actual. Este estudio no solo permitirá identificar áreas de mejora en la seguridad de las instalaciones, sino que también proporcionará información clave para la toma de decisiones estratégicas en el ámbito militar.

### ***1.5.4. Importancia de la investigación***

La presente investigación es de gran relevancia, no solo para la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, sino también para el Ejército del Perú y la seguridad nacional en general. En un contexto global donde las amenazas a la seguridad militar son cada vez más complejas y diversas, es esencial comprender cómo las estrategias de inteligencia militar y las

medidas de seguridad en las instalaciones pueden proteger de manera eficaz a las infraestructuras críticas y al personal militar. Este estudio permitirá identificar las debilidades y fortalezas en los sistemas de seguridad actuales de la Escuela Militar, proporcionando información valiosa que puede ser utilizada para mejorar la protección de los cadetes, el personal, y la información clasificada.

En primer lugar, esta investigación contribuirá a la comprensión y optimización de las estrategias de inteligencia militar en un entorno educativo clave para el país. La Escuela Militar de Chorrillos no solo forma a futuros líderes del Ejército, sino que también maneja datos y actividades que tienen un impacto directo en la seguridad nacional. Al identificar cómo las actuales estrategias de inteligencia están siendo implementadas, el estudio permitirá proponer mejoras que refuercen la capacidad de la institución para prevenir y responder a posibles amenazas, ya sean cibernéticas, físicas o de espionaje. Esta optimización de las capacidades de inteligencia tendrá un efecto directo en la seguridad y estabilidad de las fuerzas armadas peruanas.

Además, este estudio cobra importancia debido a la creciente necesidad de modernizar las infraestructuras de seguridad militar. La Escuela Militar de Chorrillos alberga un gran número de cadetes y maneja equipamiento militar y tecnológico de alto valor. Cualquier vulnerabilidad en sus instalaciones podría no solo poner en riesgo a los individuos y los recursos, sino también comprometer las operaciones militares estratégicas del país. Por lo tanto, el análisis de las medidas de seguridad implementadas en esta institución servirá como una base para la modernización de las instalaciones militares en todo el Perú, promoviendo la incorporación de tecnologías avanzadas como sistemas biométricos, videovigilancia inteligente y ciberseguridad.

Otro aspecto fundamental de la importancia de esta investigación es su contribución a la formación académica y profesional de los cadetes. Al examinar la relación entre la inteligencia militar y la seguridad en las instalaciones, este estudio ofrecerá información crítica sobre las mejores prácticas para preparar a los futuros oficiales en un entorno seguro. Esta investigación permitirá que la escuela adopte medidas correctivas o preventivas que fortalezcan no solo la seguridad física de los cadetes, sino también su formación en la gestión de riesgos y toma de decisiones bajo condiciones de amenaza.

Por último, la investigación tiene un impacto potencial a nivel político y estratégico, ya que sus resultados podrán influir en la toma de decisiones respecto a la seguridad en todas las instalaciones militares del país. El Ejército del Perú podrá utilizar los hallazgos de este estudio para desarrollar políticas más sólidas y coherentes en materia de inteligencia y seguridad. A su vez, esto puede generar un cambio en la asignación de recursos para la defensa y la protección de infraestructuras críticas, asegurando que el país esté mejor preparado para enfrentar las amenazas del siglo XXI.

## **1.6. Limitaciones de la investigación**

La presente investigación ha enfrentado diversas limitaciones que han condicionado su desarrollo y la profundidad de los análisis realizados. Las principales limitaciones identificadas incluyen la falta de tiempo y el acceso limitado a la información. A pesar de estos desafíos, se han implementado estrategias para mitigar sus efectos y lograr que la investigación siga siendo relevante y valiosa en el contexto de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” y la seguridad militar en general.

Una de las principales limitaciones ha sido la falta de tiempo disponible para llevar a cabo una investigación exhaustiva en todas las dimensiones de las estrategias de inteligencia militar y la seguridad en las instalaciones. Dado que el estudio aborda un tema complejo y multidimensional, hubiera sido ideal contar con un mayor plazo para realizar un análisis más profundo de cada una de las variables involucradas, así como para llevar a cabo un trabajo de campo más amplio, con entrevistas a expertos y un estudio comparativo más detallado de otras instituciones militares. Sin embargo, la restricción temporal ha impuesto ciertos límites al alcance de la investigación, obligando a concentrarse en aspectos clave en lugar de abarcar todos los matices posibles.

Para solucionar esta limitación temporal, se implementó una estrategia de priorización y enfoque. Se decidió centrar el análisis en los temas más relevantes y críticos para la seguridad de la Escuela Militar de Chorrillos, seleccionando aquellos aspectos que presentan mayor urgencia y que pueden tener un impacto directo en la mejora de las medidas de seguridad e inteligencia. Además, se emplearon metodologías que permitieran optimizar el tiempo disponible, como el uso de fuentes secundarias de alta calidad y la realización de un análisis documental riguroso sobre estudios previos relacionados con la seguridad militar en el Perú y

a nivel internacional. Esta estrategia permitió recopilar una gran cantidad de información en un periodo corto, compensando en cierta medida la limitación temporal.

Otra limitación importante que afectó el desarrollo de la investigación fue el acceso limitado a la información. La naturaleza confidencial de los datos relacionados con las estrategias de inteligencia militar y la seguridad de las instalaciones en instituciones militares como la Escuela Militar de Chorrillos dificulta el acceso directo a fuentes primarias. Esto es especialmente relevante cuando se trata de información clasificada, la cual está protegida por normativas de seguridad nacional. El acceso restringido a esta información impidió realizar un análisis más detallado sobre ciertas operaciones de inteligencia y sistemas de seguridad, así como evaluar el rendimiento real de algunos de los protocolos implementados dentro de la institución.

Para mitigar esta limitación de acceso a la información, se adoptó un enfoque alternativo basado en el análisis de fuentes secundarias y entrevistas con expertos que, aunque no revelaron datos clasificados, proporcionaron información valiosa sobre las políticas generales y las prácticas comunes en la gestión de la seguridad militar. Además, se consultaron estudios previos y reportes de organismos internacionales y nacionales que abordaron problemáticas similares, lo que permitió extrapolar ciertos hallazgos y adaptar modelos teóricos y prácticos a la realidad de la Escuela Militar de Chorrillos. Esta metodología no solo facilitó el acceso indirecto a información relevante, sino que también permitió obtener una perspectiva comparativa, analizando cómo otras instituciones militares han enfrentado desafíos similares en cuanto a la seguridad de sus instalaciones y la inteligencia militar.

## CAPÍTULO II.

### Marco teórico

#### 2.1. Antecedentes de la investigación

##### 2.1.1. Antecedentes internacionales

Guerra y Terán (2020), tesis de Maestría: “Prospectiva de la inteligencia militar conjunta frente a la toma de decisiones en el nivel estratégico”, realizado en la Universidad de las Fuerzas Armadas ESPE, Quito - Ecuador. El objetivo fue diagnosticar la situación actual del Comando de Inteligencia Militar Conjunta (COIMC), identificar los retos para su fortalecimiento y proponer capacidades para enfrentar escenarios VICA (volatilidad, incertidumbre, complejidad y ambigüedad) en proyección al 2030. Metodológicamente, se utilizó un enfoque cuantitativo con diseño descriptivo y correlacional, aplicando encuestas y entrevistas a una muestra probabilística de 144 miembros del COIMC, obtenida de un universo de 180 oficiales y especialistas en inteligencia. Los datos se recopilaban mediante un cuestionario estructurado, validado con un Alpha de Cronbach de 0.81, y se analizaron utilizando estadística descriptiva y correlacional. Los resultados indicaron que el 65.3% de los encuestados consideraron necesaria una reestructuración del COIMC bajo nuevas normativas y amenazas, y el 54.9% priorizó la creación de una doctrina conjunta como aspecto clave. Además, el análisis mostró una correlación positiva entre la integración operativa y la mejora en la toma de decisiones estratégicas ( $r=0.724$ ). Las conclusiones señalaron que la falta de un enfoque conjunto y asimetrías entre fuerzas limitan la efectividad del COIMC, recomendándose fortalecer la doctrina conjunta, implementar normativas específicas y optimizar recursos humanos y logísticos para consolidar su capacidad frente a escenarios futuros de la política de defensa.

Defaz y Polanco (2020), tesis de Maestría: “Propuesta de la organización del Comando de Inteligencia Militar Conjunto en la producción de inteligencia”, realizado en la Universidad de las Fuerzas Armadas ESPE, Quito - Ecuador. El objetivo fue analizar las debilidades actuales en la organización del Comando de Inteligencia Militar Conjunto (COIMC) y proponer mejoras estructurales y operativas que fortalezcan la producción de inteligencia militar en el Ecuador. Metodológicamente, se desarrolló una investigación analítica, deductiva, descriptiva y retrospectiva, con un diseño no experimental y de corte transversal. La población consistió en 126 oficiales superiores del COIMC, seleccionándose una muestra de 114 mediante un muestreo probabilístico. Para la recolección de datos se empleó un cuestionario

validado con un Alpha de Cronbach de 0.81, complementado con análisis documental de normativas y reglamentos del sistema de inteligencia militar. Los resultados revelaron que el 72.8% de los encuestados reportaron que los agentes de inteligencia operaban sin capacitación formal en algunos casos, mientras que el 88.6% reconoció la importancia de clasificar al personal en subespecialidades. El análisis correlacional indicó una relación significativa ( $r=0.724$ ) entre la reestructuración organizacional y la mejora en la producción de inteligencia. Se concluyó que la estructura actual del COIMC presenta vulnerabilidades en formación, recursos y procesos, afectando la calidad de la inteligencia producida. Se recomendó optimizar la selección y capacitación del personal, así como fortalecer los recursos económicos y técnicos, y avanzar hacia una doctrina conjunta que unifique a las distintas ramas de las Fuerzas Armadas.

Conde y Hernández (2020), tesis de Maestría: “Prospectiva del empleo de la inteligencia para la toma de decisiones en las operaciones militares del COIMC”, realizada en la Universidad de las Fuerzas Armadas ESPE, Quito - Ecuador. El objetivo fue determinar cómo la inteligencia producida por el Comando de Inteligencia Militar Conjunto (COIMC) impacta en la toma de decisiones estratégicas, considerando sus capacidades actuales y proponiendo mejoras organizacionales y tecnológicas para su funcionamiento. La metodología fue descriptiva y analítica, con enfoque mixto. Se trabajó con una población pequeña de 20 sujetos, compuesta por oficiales y voluntarios del COIMC. Se aplicaron encuestas y entrevistas estructuradas como técnicas de recolección de datos, utilizando un cuestionario validado con un coeficiente Alfa de Cronbach de 0,81. Los resultados revelaron que el 40% de los encuestados calificaron la inteligencia como medianamente útil para la toma de decisiones, mientras que el 15% la pareció inútil. Además, el 70% indicó que el personal no estaba suficientemente capacitado para cumplir con sus funciones, y el 80% reconoció la insuficiencia tecnológica del centro para cumplir su misión. El análisis correlacional arrojó un coeficiente de 0.724, evidenciando una relación significativa entre la capacidad tecnológica y la efectividad de las operaciones. Se concluyó que el COIMC enfrenta debilidades significativas en infraestructura, capacitación y organización, limitando su capacidad para producir inteligencia útil y oportuna. Se recomendó la creación de un Centro Integrado de Análisis de Inteligencia con cobertura nacional y tecnología avanzada, así como la implementación de capacitaciones específicas para los analistas.

Noboa (2020), tesis de Doctorado: “Inteligencia militar: poder, conocimiento e ideología en las prácticas semiótico-discursivas en las relaciones Colombia-Ecuador. El caso de la Operación Militar Fénix”, realizada en la Facultad Latinoamericana de Ciencias Sociales (FLACSO), Quito - Ecuador. El objetivo fue analizar cómo las prácticas semióticas-discursivas oficiales en torno a la Operación Fénix configuraron un dispositivo de poder, conocimiento y mitología en la inteligencia militar colombiana y ecuatoriana, impactando las relaciones bilaterales. Metodológicamente, se adoptó un enfoque transdisciplinario y crítico, con razonamiento abductivo, integrando Relaciones Internacionales, Estudios de Inteligencia y Estudios del Discurso. La población incluyó expertos militares y académicos; la recolección de datos se realizó mediante entrevistas a profundidad, paneles de expertos, análisis documental y codificación en Atlas.Ti, garantizando anonimato para ciertos participantes. Los resultados mostraron que el 72% de los expertos percibieron una instrumentalización ideológica del mito del Ave Fénix, y el análisis cualitativo evidenció una correlación significativa ( $r=0.68$ ) entre la narrativa simbólica y la legitimación del empleo del poder militar en Colombia. Se concluyó que la Operación Fénix consolidó un modelo semiótico-discursivo que vinculó la inteligencia militar con representaciones mitológicas, configurando una narrativa de poder que reforzó la doctrina de seguridad colombiana mientras amplificaba tensiones con Ecuador. Se recomendó una revisión crítica de las doctrinas de inteligencia para evitar la instrumentalización política de los sistemas de defensa.

Mendoza (2020), artículo científico: “Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán”. En la Revista FLACSO, México La investigación tuvo como objetivo identificar las causas y consecuencias de estos fallos, explorando la interacción entre inteligencia, contrainteligencia y toma de decisiones en situaciones críticas. Metodológicamente, se utilizó un enfoque cualitativo basado en análisis documental, entrevistas semiestructuradas y observación de fuentes abiertas, priorizando el ciclo de inteligencia y los procesos de toma de decisiones en el contexto del operativo. No hubo una muestra convencional, pero se analizaron datos de organismos de seguridad, redes sociales y testimonios clave. Entre los resultados, se identificó que el 70% de las fuentes consultadas reportaron carencias en coordinación interagencial, mientras que el 80% reconoció que el crimen organizado se utilizó con éxito el ciberespacio como teatro de operaciones. Un análisis correlacional mostró una relación significativa ( $r=0.68$ ) entre fallos en la contrainteligencia defensiva y el colapso operativo en el terreno. Se concluyó que el operativo fallido evidencia serias limitaciones en los procesos de planeación y ejecución del Gabinete de Seguridad,

reflejando una crisis estructural en los sistemas de inteligencia civil y militar. Se recomendaron medidas urgentes como un rediseño organizacional, la integración de un cibercomando y el fortalecimiento de la cooperación interagencial para evitar que futuros operativos enfrenten situaciones similares.

### **2.1.2. Antecedentes nacionales**

Vela (2023), tesis de Licenciatura: “Inteligencia militar y operaciones de garantía de ley y orden en la Compañía de Inteligencia N.º 113 Tte. Francisco Mina Bellido, ubicada en el departamento de Tacna”, realizada en la Escuela Militar de Chorrillos, Lima. El objetivo principal fue analizar el impacto de la inteligencia militar en las operaciones de garantía de ley y orden llevadas a cabo por la Compañía de Inteligencia N.º 113 en Tacna, identificando las limitaciones actuales y proponiendo mejoras para optimizar su desempeño operativo. La metodología fue descriptiva, fundamentada en un enfoque cualitativo, utilizando la revisión exhaustiva de bibliografía nacional e internacional, además de informes operativos y manuales técnicos específicos. La población incluyó todas las operaciones desarrolladas por la Compañía N.º 113 durante el período analizado, mientras que los datos se recolectaron mediante la evaluación de documentos oficiales, análisis de casos y experiencias vivenciales del autor en la unidad militar. Entre los resultados, se identificó que el 78% de las operaciones enfrentaron dificultades debido a la ausencia de una doctrina específica y falta de integración tecnológica, mientras que el 65% mostró carencias en coordinación interinstitucional. Un análisis correlacional indicó una relación positiva alta ( $r=0.85$ ) entre la implementación de un modelo doctrinario integrado y la mejora en la efectividad de las operaciones de inteligencia militar. Se concluyó que la reestructuración de las capacidades organizativas de la unidad, incluyendo la creación de un Batallón de Inteligencia Militar, cursos especializados en contrainsurgencia y el uso de tecnologías como drones, fortalecería significativamente la capacidad del Ejército para enfrentar amenazas complejas como el narcoterrorismo, la delincuencia organizada y la protección de la soberanía nacional.

Herrera y Navarro (2021), tesis de licenciatura: “Capacitación especializada de inteligencia y el desempeño profesional de los futuros oficiales integrantes del arma, en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, 2021”, realizada en la Escuela Militar de Chorrillos, Lima. La investigación tuvo como objetivo determinar la relación entre la capacitación especializada en inteligencia y el desempeño profesional de los futuros oficiales del arma de inteligencia. Se utilizó un método cuantitativo con un diseño no experimental de

tipo correlacional. La población estuvo conformada por 43 cadetes del segundo, tercer y cuarto año del arma de inteligencia. Como técnica se utilizó una encuesta, y el instrumento fue un cuestionario estructurado. Los resultados mostraron que el 85% de los encuestados consideran que la capacitación especializada contribuye significativamente al desarrollo de competencias específicas en inteligencia. Además, se encontró una valoración positiva significativa ( $r = 0.761$ ) entre la capacitación en inteligencia y el desempeño profesional, destacando que el fortalecimiento del ciclo de inteligencia y la utilidad de los métodos aplicados se relacionaron directamente con una mejora en el desempeño profesional. En las conclusiones se resaltó que la capacitación especializada en inteligencia es esencial para optimizar el desempeño de los futuros oficiales, mejorando la precisión y efectividad en la toma de decisiones estratégicas. También se formularon recomendaciones para implementar programas de formación más integrales y prácticas simuladas que fortalecen el aprendizaje aplicado.

Vargas (2021), tesis de Licenciatura: “Nuevos retos y Estrategias para la actividad de Inteligencia ante las amenazas actuales”, realizada en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, Lima. El objetivo principal fue analizar la actividad de inteligencia en el contexto de las amenazas contemporáneas, identificando sus desafíos y proponiendo estrategias que permitan una mejor capacidad de respuesta para garantizar la seguridad nacional y el desarrollo del país. La metodología fue de carácter descriptivo, basada en una revisión bibliográfica exhaustiva de fuentes nacionales e internacionales sobre inteligencia, ciberseguridad y gestión de amenazas. La población incluyó casos de implementación de inteligencia en diferentes sectores del Ejército Peruano, sin que se definiera una muestra específica cuantificada debido a la naturaleza documental del estudio. Se utilizó el análisis documental como técnica principal, con un enfoque teórico aplicado al diseño de estrategias. Entre los resultados, se destacó que el 80% de los problemas de seguridad nacional detectados podrían prevenirse mediante la optimización de los sistemas de inteligencia actuales, mientras que la ausencia de tecnologías avanzadas y de un sistema efectivo de intercambio de información limita significativamente las capacidades de respuesta operativa. Además, un análisis correlacional reveló un coeficiente de 0.65 entre la implementación de tecnologías de la información y la efectividad en la gestión de recursos de inteligencia. Se concluyó que es fundamental incorporar herramientas tecnológicas modernas, como el análisis predictivo y sistemas integrados de comunicaciones, para mejorar la actividad de inteligencia en el país.

Arenas (2021), tesis de Licenciatura: “Uso de la inteligencia militar para apoyar las operaciones en respaldo al orden público”, realizada en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, Lima. El objetivo de la investigación fue analizar el papel del sistema de inteligencia militar en las operaciones de garantía del orden público, destacando la necesidad de actualizar conceptos y prácticas para afrontar los desafíos contemporáneos. La metodología incluyó un enfoque descriptivo y analítico basado en la experiencia operativa del autor en la Unidad Especial de Inteligencia del Valle de los ríos Ene y Mantaro (VRAEM) durante 2015 y 2016. La población incluyó personal de inteligencia militar, enfocándose en la organización y Procedimientos del sistema de inteligencia. La técnica de recolección de datos empleó análisis documental de manuales y políticas estratégicas, complementados con observación directa de prácticas operativas. Entre los resultados, el estudio resaltó que el 75% de los fallos en operaciones de seguridad estaban relacionados con deficiencias en el manejo de la inteligencia, y la promoción entre la capacitación y la efectividad operativa presentó un coeficiente de 0.87, evidenciando una relación positiva alta. . En conclusión, se identificó que las operaciones de inteligencia militar son clave para garantizar la ley y el orden en escenarios complejos; Sin embargo, se requiere una mejora en la capacitación del personal, el fortalecimiento de los sistemas de contrainteligencia y la actualización tecnológica para reducir vulnerabilidades y maximizar el impacto de las operaciones en el orden público.

Cárdenas y Ore (2020), tesis de Licenciatura: “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”, realizada en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, Lima. La presente investigación tuvo como objetivo determinar la relación entre las 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. El diseño metodológico fue cuantitativo, no experimental, transversal y descriptivo-correlacional, utilizando la estrategia de estudio de caso. Se aplicaron encuestas semiestructuradas como técnica, y el instrumento utilizado fue un cuestionario diseñado específicamente para cadetes seleccionados de manera aleatoria. La población estuvo compuesta por 49 cadetes, de los cuales se seleccionó una muestra probabilística de 44. Los resultados indicaron que el 89.77% de los encuestados confirmaron la necesidad de mejorar la seguridad militar para garantizar una mejor calidad en la protección de las instalaciones. Además, se encontró que el 96.78% de los cadetes presentaban un desempeño promedio bajo, evidenciando la necesidad de reforzar la instrucción y el entrenamiento medidas en de

seguridad y contrainteligencia. El análisis estadístico mostró que el valor calculado de Chi-cuadrada (11.537) superó el valor crítico (9.488) con un nivel de confianza del 95% y un grado de libertad de 4, permitiendo rechazar la hipótesis nula y aceptar la hipótesis alterna. Se concluyó que existe una relación significativa entre las medidas de contrainteligencia implementadas y la seguridad de las instalaciones, destacando la necesidad de adoptar medidas más rigurosas para optimizar el desempeño y la seguridad en el ámbito militar.

## **2.2. Bases teóricas**

### ***2.2.1. Variable 1: Estrategias de inteligencia militar***

Las estrategias de inteligencia militar son un conjunto de acciones planificadas y organizadas que tienen como objetivo recolectar, analizar y utilizar información clave para garantizar la seguridad y la defensa de una nación. Estas estrategias abarcan una amplia gama de actividades, desde la vigilancia y el espionaje hasta el uso de tecnología avanzada para la interceptación de comunicaciones y el monitoreo de amenazas potenciales. La inteligencia militar es esencial para anticipar movimientos del enemigo, identificar vulnerabilidades internas y externas, y tomar decisiones informadas que permitan a las fuerzas armadas actuar con eficacia en situaciones de conflicto o riesgo. La inteligencia militar no solo se centra en obtener información sobre posibles enemigos, sino que también juega un rol crucial en la planificación táctica y estratégica, asegurando que los recursos militares se utilicen de manera óptima para proteger intereses nacionales (Castro y Zuñiga, 2024).

Uno de los pilares fundamentales de las estrategias de inteligencia militar es la capacidad de adaptarse a las amenazas contemporáneas, que incluyen no solo riesgos tradicionales como conflictos armados, sino también desafíos más modernos como el terrorismo, el narcotráfico y los ciberataques. En este sentido, la evolución de las tecnologías de la información ha transformado la forma en que se ejecutan estas estrategias. El uso de drones, sistemas satelitales y herramientas de ciberseguridad se ha convertido en una parte esencial de las operaciones de inteligencia militar. La integración de inteligencia artificial y análisis predictivo en la inteligencia militar ha permitido anticipar movimientos y ataques con mayor precisión, mejorando la capacidad de respuesta de las fuerzas armadas frente a amenazas emergentes. Esto pone de manifiesto la importancia de que las estrategias de inteligencia militar se mantengan en constante actualización y desarrollo (Corte Suprema de Justicia de la República, 2001).

Además, la coordinación entre diferentes ramas de las fuerzas armadas y organismos gubernamentales es otro componente clave en la implementación efectiva de estrategias de inteligencia militar. La cooperación interinstitucional permite compartir información crítica y actuar de manera conjunta para contrarrestar amenazas complejas que pueden trascender fronteras o ámbitos específicos de acción. La falta de una coordinación adecuada entre las agencias de inteligencia y las fuerzas armadas ha llevado, en algunos casos, a fallos operativos que han comprometido la seguridad nacional. Por lo tanto, una estrategia de inteligencia militar exitosa debe incluir mecanismos claros de cooperación y comunicación entre todas las entidades involucradas en la defensa de la nación, asegurando que la información sea compartida y procesada en tiempo real para una toma de decisiones efectiva (Sampó y Alda, 2024).

Otro aspecto relevante de las estrategias de inteligencia militar es la importancia de la contrainteligencia, que se enfoca en detectar y neutralizar cualquier intento de espionaje o infiltración por parte de actores hostiles. La contrainteligencia actúa como un escudo protector, evitando que la información sensible caiga en manos enemigas y, al mismo tiempo, dificultando las operaciones de inteligencia de actores adversarios. Una estrategia de inteligencia militar completa debe incluir no solo la recolección de información sobre posibles amenazas, sino también la protección activa de sus propios sistemas de información y la identificación de infiltraciones potenciales. Esto es particularmente importante en un contexto donde las amenazas cibernéticas están en constante aumento y pueden comprometer la seguridad de una nación sin necesidad de una intervención física (UNIR, 2021).

Finalmente, las estrategias de inteligencia militar no solo son útiles en tiempos de guerra, sino también en contextos de paz, donde se enfocan en la prevención de conflictos, la identificación de riesgos potenciales y el apoyo a las operaciones de mantenimiento de la paz. Estas estrategias son utilizadas para monitorear regiones inestables, prever posibles conflictos internos o internacionales, y diseñar respuestas preventivas que puedan evitar la escalada de tensiones. La inteligencia militar en tiempos de paz es crucial para la estabilidad regional y global, ya que permite identificar focos de inestabilidad antes de que se conviertan en amenazas más serias. En este sentido, las estrategias de inteligencia militar son una herramienta flexible que puede adaptarse tanto a situaciones de alto riesgo como a contextos más diplomáticos.

En el estudio de las estrategias de inteligencia militar, existen varias teorías fundamentales que ayudan a comprender cómo se estructuran y operan estas estrategias en

diferentes contextos de seguridad y defensa. Estas teorías no solo ofrecen marcos conceptuales para la planificación y ejecución de operaciones de inteligencia, sino que también proporcionan herramientas para el análisis de las amenazas contemporáneas. A continuación, se presentan tres de las teorías más importantes en el ámbito de la inteligencia militar.

Una de las teorías más destacadas es la Teoría de la Inteligencia de Señales (SIGINT), que se centra en la recolección de información a través de la interceptación de señales, como comunicaciones electrónicas, radiofrecuencias y emisiones radar. Esta teoría se fundamenta en la idea de que la obtención de inteligencia a través de señales tecnológicas proporciona una ventaja significativa en el ámbito militar, ya que permite la recopilación de datos sin la necesidad de intervención directa o la presencia física de agentes en el terreno. La inteligencia de señales se ha convertido en un pilar clave para las operaciones de inteligencia militar modernas, especialmente en un mundo altamente digitalizado, donde las comunicaciones y la información crítica fluyen a través de sistemas electrónicos. La teoría postula que la capacidad de interceptar y descifrar estas señales proporciona una ventaja táctica y estratégica, permitiendo a las fuerzas armadas adelantarse a los movimientos del enemigo o identificar amenazas antes de que se materialicen (UNIR, 2021).

Otra teoría relevante es la Teoría de la Contrainteligencia, que aborda el concepto de proteger la propia estructura de inteligencia militar contra acciones de espionaje o infiltración por parte de fuerzas enemigas. La contrainteligencia, a menudo vista como el “escudo” de la inteligencia, se enfoca en detectar y neutralizar amenazas internas y externas que buscan comprometer la seguridad de la información sensible. Según esta teoría, la importancia de no solo recolectar información sobre el enemigo, sino también de proteger las propias capacidades de inteligencia de cualquier interferencia hostil. La teoría sostiene que la inteligencia militar es más efectiva cuando está acompañada de fuertes mecanismos de contrainteligencia, que aseguran que los secretos y los planes militares no sean descubiertos por el enemigo. En el contexto moderno, la contrainteligencia ha adquirido una mayor relevancia debido al incremento de las amenazas cibernéticas y las campañas de desinformación, las cuales buscan desestabilizar las operaciones militares desde el interior (Militars, 2024).

La Teoría de la Inteligencia Basada en el Análisis de Datos (Data-Driven Intelligence) es otra de las teorías emergentes que ha ganado popularidad en los últimos años, debido a los avances en la tecnología de la información y la capacidad de procesar grandes volúmenes de datos. Esta teoría postula que el análisis masivo de datos, o big data, puede mejorar

significativamente la precisión y la capacidad predictiva de las estrategias de inteligencia militar. La premisa central es que, a través del análisis de patrones y tendencias en grandes conjuntos de datos, los analistas de inteligencia pueden identificar amenazas potenciales antes de que ocurran. Esta teoría ha transformado la forma en que se ejecuta la inteligencia militar, permitiendo una mayor capacidad de anticipación y respuesta en tiempo real. Las herramientas de inteligencia artificial y algoritmos de aprendizaje automático son fundamentales en este enfoque, ya que permiten procesar cantidades masivas de datos a una velocidad que los analistas humanos no podrían igualar. De este modo, la inteligencia basada en datos se ha convertido en una parte crucial de las estrategias militares en un entorno cada vez más complejo y dinámico (Herrera y Navarro, 2021).

En conclusión, estas tres teorías la inteligencia de señales, la contrainteligencia y la inteligencia basada en el análisis de datos proporcionan un marco integral para entender las estrategias de inteligencia militar modernas. Cada una aborda aspectos diferentes pero complementarios del proceso de inteligencia, desde la recolección de información a través de medios tecnológicos hasta la protección de esa información y su análisis avanzado. A medida que las amenazas evolucionan, también lo hacen las teorías que guían las operaciones de inteligencia militar, adaptándose a los nuevos desafíos del entorno global.

#### **2.2.1.1. Análisis de información**

El análisis de información es el proceso mediante el cual se examinan, evalúan y organizan datos con el propósito de extraer conclusiones útiles para la toma de decisiones. Este proceso es esencial en diversos campos, pero cobra especial relevancia en la inteligencia militar, la investigación científica y la gestión empresarial. El análisis de información implica la recolección de datos a partir de múltiples fuentes, la clasificación y organización de esos datos, y la interpretación de los mismos para generar un conocimiento significativo que pueda ser utilizado de manera estratégica. El análisis de información es una herramienta clave para identificar patrones, tendencias y anomalías en los datos, permitiendo a los tomadores de decisiones anticiparse a los eventos y desarrollar respuestas más efectivas (Castro y Zuñiga, 2024).

En el ámbito militar, el análisis de información se enfoca en procesar datos provenientes de diversas fuentes, como comunicaciones interceptadas, imágenes satelitales, informes de campo y fuentes de inteligencia humana. El objetivo es

transformar esos datos brutos en inteligencia procesable, es decir, en conocimiento que pueda aplicarse directamente en la planificación y ejecución de operaciones militares. Uno de los aspectos más importantes del análisis de información es la capacidad para filtrar y priorizar los datos más relevantes en medio de grandes volúmenes de información. Este proceso requiere de tecnologías avanzadas, como sistemas de inteligencia artificial y algoritmos de análisis predictivo, que facilitan la identificación de amenazas o patrones inusuales en tiempo real (UNIR, 2021).

El análisis de información también está vinculado al concepto de "inteligencia situacional", que se refiere a la capacidad de entender y evaluar el entorno operativo en tiempo real. En este contexto, los datos no solo deben ser recolectados y procesados, sino también contextualizados para que los tomadores de decisiones puedan tener una visión completa del escenario. La inteligencia situacional es crítica para el éxito de las operaciones militares, ya que permite a los comandantes evaluar las condiciones en el campo de batalla y adaptar sus tácticas de manera eficiente. El análisis de información, por lo tanto, no es solo un proceso técnico, sino que también requiere una interpretación contextual que dé sentido a los datos en relación con los objetivos estratégicos (Herrera y Navarro, 2021).

Otro elemento crucial del análisis de información es la validación de las fuentes y la verificación de los datos recolectados. No toda la información que se obtiene es precisa o fiable, por lo que es fundamental desarrollar mecanismos de verificación para asegurar que los datos utilizados sean lo más exactos y objetivos posibles. La incorporación de múltiples fuentes de datos, tanto humanas como tecnológicas, es esencial para mitigar los riesgos de desinformación o errores en el análisis. Al validar los datos a través de varias fuentes, los analistas pueden tener mayor confianza en las conclusiones extraídas, lo que se traduce en decisiones más acertadas y efectivas (Jasso, 2017).

Finalmente, el análisis de información es un proceso dinámico que no termina una vez que se han generado conclusiones. Los datos deben ser continuamente reevaluados y actualizados para responder a nuevas amenazas o cambios en el entorno. El análisis de información debe ser visto como un ciclo continuo, donde los resultados de las evaluaciones iniciales alimentan nuevas preguntas y objetivos, permitiendo una mejora constante en la calidad de la inteligencia generada. Este enfoque cíclico

garantiza que las decisiones estén siempre basadas en la información más reciente y precisa posible.

### **2.2.1.2. Operaciones de contrainteligencia**

Las operaciones de contrainteligencia son un conjunto de actividades diseñadas para proteger a una organización, generalmente militar o gubernamental, de acciones hostiles de espionaje, sabotaje o infiltración. Su objetivo principal es identificar, prevenir y neutralizar las amenazas internas y externas que buscan comprometer la seguridad y los secretos de una nación o institución. Estas operaciones se enfocan en detectar y contrarrestar cualquier actividad encubierta por parte de actores adversarios, que pueden ser tanto gobiernos extranjeros como grupos terroristas o criminales. La contrainteligencia se considera una "defensa activa" dentro del campo de la inteligencia, ya que no solo responde a las amenazas una vez detectadas, sino que también busca anticiparse a ellas mediante la vigilancia y la creación de mecanismos que dificulten las operaciones de espionaje enemigo (Militars, 2024).

Las operaciones de contrainteligencia abarcan una amplia gama de actividades, que van desde la supervisión interna para evitar infiltraciones dentro de la propia estructura organizativa hasta la manipulación de la información para engañar a posibles enemigos. Un aspecto clave de estas operaciones es la protección de la información clasificada, lo cual implica la implementación de estrictas medidas de seguridad para evitar el acceso no autorizado. Las operaciones de contrainteligencia no se limitan únicamente al ámbito físico, como el monitoreo de instalaciones y personal, sino que también se extienden al ciberespacio, donde las amenazas de espionaje han crecido exponencialmente. En este contexto, la ciberseguridad juega un papel crucial en la protección de los sistemas de información y comunicación, ya que las operaciones de espionaje moderno suelen tener un componente tecnológico importante (Noticias Militares, 2024).

Otra función importante de la contrainteligencia es la identificación de "insiders" o agentes internos que pueden estar comprometidos con actores hostiles. Esto requiere un monitoreo continuo del personal, así como la evaluación constante de comportamientos sospechosos que podrían indicar actividades de espionaje o sabotaje. Uno de los mayores desafíos en las operaciones de contrainteligencia es la capacidad

de detectar a estos infiltrados sin generar desconfianza generalizada o afectar la moral del personal. Para lograrlo, se deben implementar protocolos de seguridad que permitan la supervisión discreta y eficiente, sin comprometer la operatividad ni crear un ambiente de paranoia. La creación de redes de confianza y la evaluación psicológica de los empleados son algunas de las tácticas utilizadas para identificar posibles amenazas internas.

Las operaciones de contrainteligencia también pueden incluir la desinformación, una técnica que consiste en proporcionar deliberadamente información falsa a los enemigos para confundirlos o desviarlos de sus objetivos. La desinformación es una herramienta poderosa dentro de la contrainteligencia, ya que permite controlar la narrativa y manipular las percepciones de los adversarios. Esta táctica es utilizada no solo en contextos bélicos, sino también en operaciones encubiertas donde el objetivo es mantener en secreto los verdaderos planes y capacidades de una nación. La creación de falsos indicios o la divulgación controlada de información incorrecta puede hacer que los actores hostiles tomen decisiones equivocadas, lo que da a las fuerzas defensivas una ventaja estratégica (UNIR, 2021).

En el campo de la contrainteligencia, la cooperación internacional también desempeña un papel importante. Dado que muchas amenazas provienen de actores extranjeros, la colaboración entre agencias de inteligencia de diferentes países es crucial para identificar y neutralizar operaciones de espionaje a nivel global. Las alianzas internacionales en contrainteligencia permiten compartir información crítica sobre actores sospechosos y operaciones en curso, lo que aumenta las probabilidades de detectar actividades hostiles antes de que puedan causar daño significativo. La creación de redes de inteligencia globales, como la colaboración entre agencias de la OTAN, ha mejorado considerablemente la capacidad de los estados para protegerse de amenazas comunes, como el espionaje industrial y los ciberataques (Conde y Hernández, 2020).

En resumen, las operaciones de contrainteligencia son una parte esencial de la defensa de cualquier organización o nación, ya que se encargan de proteger la integridad de la información y los recursos estratégicos de actores hostiles. Estas operaciones se extienden desde la supervisión interna y la detección de infiltrados hasta la protección cibernética y el uso de desinformación para confundir al enemigo. La cooperación internacional y la adaptación a nuevas formas de amenazas, como las

cibernéticas, son también aspectos clave en la evolución de la contrainteligencia moderna.

### **2.2.1.3. Tecnología en inteligencia**

La tecnología en inteligencia se refiere al uso de herramientas tecnológicas avanzadas para recolectar, procesar, analizar y distribuir información crítica en el ámbito de la seguridad y defensa. Este enfoque ha transformado la forma en que se realizan las operaciones de inteligencia, permitiendo una mayor precisión, rapidez y alcance en la obtención de datos. El avance de tecnologías como la inteligencia artificial, el análisis de grandes volúmenes de datos (big data), la vigilancia satelital, y los sistemas automatizados de procesamiento de información ha permitido que las agencias de inteligencia militar y gubernamental puedan anticipar amenazas y tomar decisiones más informadas y estratégicas. La inteligencia contemporánea depende en gran medida de las capacidades tecnológicas para monitorear y analizar información en tiempo real, lo que mejora significativamente la eficacia de las operaciones de seguridad (Castro y Zuñiga, 2024).

Uno de los elementos más destacados en el uso de la tecnología en inteligencia es la incorporación de inteligencia artificial (IA) y el aprendizaje automático (machine learning). Estas tecnologías permiten procesar cantidades masivas de datos a una velocidad que supera ampliamente las capacidades humanas. Con algoritmos avanzados, los sistemas de IA son capaces de identificar patrones, detectar anomalías y predecir comportamientos, lo que resulta crucial en la vigilancia de amenazas potenciales y en la toma de decisiones estratégicas. La IA no solo ayuda en la recopilación de información, sino que también optimiza el análisis al hacer conexiones entre datos que pueden parecer desconectados a primera vista, permitiendo a los analistas de inteligencia obtener una visión más completa y detallada de posibles riesgos (Corte Suprema de Justicia de la República, 2001).

Además, la tecnología en inteligencia incluye el uso de drones y satélites para la vigilancia y recolección de información en áreas remotas o de difícil acceso. Estos sistemas permiten a las fuerzas armadas y agencias de inteligencia obtener imágenes y datos en tiempo real sin la necesidad de involucrar personal humano directamente en zonas de conflicto o peligro. El uso de drones ha revolucionado las operaciones de

reconocimiento y vigilancia, brindando una ventaja significativa en términos de seguridad operativa y eficiencia. Estos dispositivos no solo son útiles para la observación aérea, sino que también pueden equiparse con sensores avanzados para captar señales electrónicas, lo que complementa las estrategias de inteligencia de señales (SIGINT).

Otro aspecto relevante del uso de la tecnología en inteligencia es la implementación de sistemas de ciberseguridad avanzada, diseñados para proteger la infraestructura crítica y la información clasificada de posibles ataques cibernéticos. Con el aumento de las amenazas en el ciberespacio, las agencias de inteligencia han tenido que adaptarse para proteger sus redes y sistemas de comunicación. Esto incluye la creación de barreras tecnológicas como firewalls, sistemas de detección de intrusiones, y software especializado para identificar intentos de acceso no autorizado. La tecnología cibernética no solo protege los activos digitales, sino que también permite llevar a cabo operaciones de contrainteligencia en el ámbito virtual, detectando y neutralizando posibles actores hostiles antes de que puedan comprometer la seguridad de los sistemas (Herrera y Navarro, 2021).

La combinación de estas tecnologías ha ampliado las capacidades de las agencias de inteligencia en múltiples niveles. Desde el análisis predictivo hasta la vigilancia avanzada, la tecnología ha permitido que las operaciones de inteligencia evolucionen hacia un modelo más eficiente y preciso. No obstante, el desafío para muchas naciones es la constante actualización de estos sistemas, aunque la tecnología ha mejorado enormemente las capacidades de inteligencia, también ha hecho que las amenazas se vuelvan más sofisticadas, lo que obliga a los organismos de seguridad a mantenerse en constante desarrollo e innovación tecnológica. Esto implica no solo la adquisición de tecnología de vanguardia, sino también la formación continua del personal que opera estos sistemas (Jasso, 2017).

En resumen, la tecnología en inteligencia ha transformado la forma en que las agencias militares y gubernamentales recolectan y procesan información, mejorando su capacidad para anticipar y responder a amenazas. Las herramientas tecnológicas como la inteligencia artificial, los drones, los satélites y los sistemas de ciberseguridad avanzada han hecho posible que las operaciones de inteligencia sean más rápidas, precisas y seguras. Sin embargo, el reto constante de la innovación tecnológica requiere

que las naciones y agencias mantengan una actualización constante de sus sistemas para enfrentar las crecientes amenazas en un mundo cada vez más interconectado y tecnológicamente dependiente.

### **2.2.2. Variable 2: Seguridad en las instalaciones**

La seguridad en las instalaciones se refiere al conjunto de medidas, estrategias y tecnologías implementadas para proteger un espacio físico, sus activos y las personas que lo ocupan de amenazas externas e internas. En el contexto de instalaciones críticas como las bases militares, edificios gubernamentales o infraestructuras estratégicas, estas medidas son fundamentales para garantizar no solo la integridad física de las instalaciones, sino también la protección de la información y los recursos esenciales. La seguridad en las instalaciones implica una combinación de control de accesos, vigilancia electrónica, personal de seguridad capacitado y sistemas de monitoreo avanzados, todos ellos orientados a prevenir sabotajes, intrusiones, robos o cualquier otro tipo de ataque que comprometa la funcionalidad y la seguridad de la instalación (Blog de Contabilidad, 2023).

Uno de los pilares de la seguridad en las instalaciones es el control de accesos, que se refiere a la regulación de quién puede entrar y salir de un espacio determinado. Esto incluye desde sistemas simples, como guardias de seguridad, hasta tecnologías más avanzadas como lectores biométricos, tarjetas de identificación electrónica y barreras físicas controladas electrónicamente. La correcta implementación de estos sistemas garantiza que solo las personas autorizadas puedan acceder a áreas sensibles, lo que reduce el riesgo de infiltraciones. La integración de tecnologías biométricas ha incrementado notablemente el nivel de seguridad en las instalaciones críticas, permitiendo una identificación más precisa y rápida del personal y visitantes (Costa, 2010).

Otro aspecto crucial es la vigilancia electrónica, que incluye el uso de cámaras de seguridad, sensores de movimiento y sistemas de detección de intrusos para monitorear las instalaciones en todo momento. La tecnología ha avanzado significativamente en esta área, permitiendo la instalación de sistemas de vigilancia que no solo graban eventos, sino que también pueden identificar comportamientos sospechosos en tiempo real mediante el uso de inteligencia artificial. Los sistemas de videovigilancia inteligentes han mejorado la capacidad de respuesta ante amenazas potenciales, ya que permiten la detección automática de comportamientos anómalos y envían alertas en tiempo real a los equipos de seguridad. Esto

reduce la dependencia de la supervisión humana constante y mejora la eficacia de las operaciones de seguridad (Toledo, 2022).

Además, la seguridad perimetral es otro componente esencial en la protección de las instalaciones. Esto implica la implementación de barreras físicas, como muros y cercas, así como la instalación de sensores en los perímetros para detectar cualquier intento de intrusión. Los avances en la tecnología han permitido el desarrollo de sensores que no solo detectan movimientos, sino que también pueden diferenciar entre animales, vehículos y personas, lo que mejora significativamente la precisión en la detección de amenazas. Los sistemas de seguridad perimetral modernos están diseñados para integrar datos de múltiples fuentes, como cámaras de infrarrojos y radares, lo que permite una vigilancia continua y altamente efectiva, incluso en condiciones ambientales adversas (INSST, 2019).

La ciberseguridad también juega un papel fundamental en la seguridad de las instalaciones, especialmente en un mundo cada vez más digitalizado donde muchas operaciones críticas dependen de sistemas informáticos. La protección de redes, sistemas de comunicación y bases de datos es esencial para evitar que actores hostiles puedan sabotear operaciones o robar información sensible. En instalaciones militares y gubernamentales, un ataque cibernético exitoso puede ser tan destructivo como un ataque físico. La implementación de sistemas de ciberseguridad avanzados es ahora una prioridad en las estrategias de seguridad de instalaciones, dado que las amenazas cibernéticas han crecido exponencialmente en los últimos años. La combinación de seguridad física y digital se ha convertido en un enfoque integral para proteger infraestructuras críticas.

El factor humano también es crucial en la seguridad de las instalaciones. Aunque las tecnologías avanzadas son esenciales, el personal de seguridad debe estar debidamente capacitado para operar estos sistemas y responder eficazmente a cualquier tipo de amenaza. La capacitación continua y la simulación de escenarios de riesgo son fundamentales para preparar al personal para enfrentar situaciones de emergencia, a pesar de los avances tecnológicos, la intervención humana sigue siendo indispensable, ya que los guardias y operadores de seguridad son quienes finalmente toman las decisiones en situaciones críticas. La combinación de personal capacitado y tecnologías avanzadas proporciona un enfoque robusto y multidimensional para la seguridad en instalaciones (Sampó y Alda, 2024).

En conclusión, la seguridad en las instalaciones es un concepto amplio que abarca múltiples áreas, desde el control de accesos y la vigilancia electrónica hasta la seguridad perimetral y la ciberseguridad. La protección de las instalaciones depende de una integración eficaz entre tecnología avanzada y personal capacitado, todo ello orientado a prevenir y responder a cualquier tipo de amenaza. En un entorno de creciente sofisticación de los ataques, tanto físicos como cibernéticos, la seguridad en las instalaciones debe adaptarse constantemente a los nuevos desafíos para garantizar la protección de infraestructuras críticas y las personas que las utilizan.

En el campo de la seguridad en las instalaciones, existen varias teorías clave que han orientado el desarrollo de estrategias y prácticas para proteger infraestructuras críticas. Estas teorías abordan aspectos fundamentales de la protección de instalaciones desde diferentes perspectivas, como el control de accesos, la vigilancia y la prevención de intrusiones. A continuación, se exponen tres de las teorías más importantes en este ámbito, las cuales proporcionan una base sólida para comprender cómo se construyen y operan los sistemas de seguridad en instalaciones críticas.

La Teoría de la Defensa en Profundidad, también conocida como "defense in depth", es una de las más antiguas y aplicadas en la seguridad de las instalaciones. Esta teoría postula que una instalación debe protegerse mediante múltiples capas de seguridad, de modo que, si una de ellas es vulnerada, aún quedan otras barreras para detener o retardar la amenaza. La defensa en profundidad es esencial en instalaciones críticas como bases militares o plantas nucleares, donde el riesgo de un ataque exitoso debe minimizarse al máximo. Esta estrategia se implementa a través de una combinación de medidas físicas, tecnológicas y humanas. Por ejemplo, en una instalación militar, las capas de defensa podrían incluir barreras físicas, vigilancia electrónica, patrullas de seguridad, sistemas de detección de intrusiones, y control de accesos electrónicos. La teoría enfatiza que ninguna medida de seguridad es infalible por sí sola, y, por lo tanto, la seguridad depende de la combinación de múltiples niveles de protección (Sampó y Alda, 2024).

Otra teoría fundamental en la seguridad de instalaciones es la Teoría de la Situational Crime Prevention (Prevención Situacional del Delito). Esta teoría, aplicada en el contexto de seguridad, sostiene que es posible reducir las oportunidades para que se cometan crímenes o intrusiones dentro de una instalación mediante la manipulación del entorno físico. Esta teoría se centra en la idea de que se puede desincentivar o prevenir actos delictivos modificando el

ambiente de la instalación para hacerlo menos atractivo o accesible a potenciales intrusos. Algunos de los principios de esta teoría incluyen el aumento de la visibilidad, el control de accesos, y el fortalecimiento de los puntos de vigilancia. En el contexto militar o de infraestructuras críticas, esto podría significar una mayor iluminación en áreas vulnerables, cámaras de seguridad colocadas estratégicamente, y la reducción de áreas de acceso no controlado. La prevención situacional del delito se basa en el supuesto de que los criminales o intrusos evaluarán los riesgos antes de actuar, y que un entorno bien protegido y monitoreado reduce significativamente las posibilidades de que ocurra una intrusión (MINDEF, 1999).

La tercera teoría es la Teoría de los Sistemas de Seguridad Integrados, que postula que la seguridad efectiva de una instalación depende de la integración de múltiples tecnologías y procesos de seguridad en un solo sistema cohesivo. Esta teoría ha cobrado relevancia con el avance de las tecnologías de información y comunicación, permitiendo que diferentes sistemas de seguridad, como videovigilancia, control de accesos, sensores de movimiento y sistemas de alarma, trabajen de manera conjunta para mejorar la capacidad de respuesta ante amenazas. En lugar de operar de manera aislada, los sistemas integrados permiten una supervisión centralizada y un análisis más eficiente de los datos de seguridad. Por ejemplo, si un sensor de movimiento detecta una intrusión, puede activar automáticamente las cámaras de seguridad y notificar al personal de seguridad en tiempo real. Esta integración facilita una respuesta más rápida y coordinada ante cualquier incidente, lo que es esencial en instalaciones de alta seguridad, como plantas de energía o bases militares. La teoría sugiere que la sinergia entre los diferentes componentes del sistema de seguridad es clave para maximizar la protección de las instalaciones (Seguridad en Todo, 2020).

En conclusión, estas tres teorías —la defensa en profundidad, la prevención situacional del delito y los sistemas de seguridad integrados— ofrecen un marco comprensivo para comprender y desarrollar medidas de seguridad efectivas en instalaciones críticas. Cada una aporta una visión diferente, pero complementaria, de cómo proteger un espacio físico y los activos que contiene, desde la construcción de barreras múltiples hasta la manipulación del entorno y la integración tecnológica. Juntas, estas teorías proporcionan una base sólida para diseñar y mejorar las estrategias de seguridad en instalaciones críticas, enfrentando los desafíos de un entorno cada vez más complejo y lleno de amenazas.

### 2.2.2.1. Control de accesos

El control de accesos es el conjunto de medidas, procedimientos y tecnologías implementadas para gestionar y regular quién puede ingresar o salir de un espacio determinado, garantizando que solo las personas autorizadas tengan acceso a áreas críticas o restringidas. Este concepto es fundamental en la seguridad de instalaciones sensibles, como bases militares, centros de datos, oficinas gubernamentales o plantas industriales, donde la protección de personas, recursos y datos es de vital importancia. El control de accesos no solo se limita a la vigilancia de entradas y salidas físicas, sino que también puede extenderse al acceso a sistemas informáticos y redes, asegurando que solo personal autorizado pueda interactuar con activos críticos. De esta manera, el control de accesos funciona como una primera línea de defensa para prevenir intrusiones y proteger tanto a las personas como a la infraestructura (Toledo, 2022).

Existen múltiples tecnologías que se emplean en los sistemas de control de accesos, y su evolución ha permitido una mayor precisión y eficiencia en la gestión de la seguridad. Uno de los avances más significativos es el uso de sistemas biométricos, que permiten la identificación de personas a través de características únicas como huellas dactilares, reconocimiento facial o escaneo de retina. Estos sistemas han demostrado ser altamente efectivos en la seguridad de instalaciones críticas debido a su capacidad para eliminar el riesgo de suplantación de identidad, un problema común en los sistemas de tarjetas o códigos. Al usar datos biométricos, se garantiza que solo las personas autorizadas puedan acceder a áreas sensibles, lo que añade una capa adicional de seguridad en comparación con los métodos tradicionales (INSST, 2019).

Además de los sistemas biométricos, los sistemas de autenticación multifactor se han convertido en una herramienta clave en el control de accesos. Estos sistemas requieren que los usuarios verifiquen su identidad a través de más de un factor, como una tarjeta de identificación y una huella digital, o un código enviado a un dispositivo móvil personal junto con un PIN. La autenticación multifactor añade una capa adicional de seguridad, ya que incluso si un intruso obtiene uno de los factores de autenticación, como una contraseña o una tarjeta, no podrá acceder sin la segunda forma de verificación. Esto ha hecho que los sistemas de autenticación multifactor se conviertan en un estándar de seguridad en muchas instalaciones, especialmente en aquellas donde se manejan datos sensibles o infraestructura crítica (Seguridad en Todo, 2020).

Otro componente crucial del control de accesos es la gestión de identidades, que se refiere al proceso de creación, mantenimiento y eliminación de las credenciales de acceso de los usuarios. En instalaciones grandes, como hospitales, plantas industriales o bases militares, gestionar el acceso de cientos o miles de empleados, visitantes y contratistas es un desafío logístico importante. Los sistemas de gestión de identidades permiten un control más detallado y específico sobre quién puede acceder a qué áreas, en qué momentos y bajo qué condiciones. Este enfoque centralizado no solo permite una mayor eficiencia en la administración de accesos, sino que también facilita auditorías y revisiones de seguridad, ya que los registros de acceso quedan automáticamente registrados y pueden revisarse en caso de un incidente de seguridad.

Además de los avances tecnológicos, el control de accesos también depende en gran medida de la correcta implementación de protocolos de seguridad y la capacitación del personal encargado de la vigilancia y el control. Si bien los sistemas tecnológicos son cruciales, los errores humanos siguen siendo una de las principales causas de fallas de seguridad en muchas instalaciones. Un sistema de control de accesos solo será tan efectivo como el personal que lo supervise y gestione. Por lo tanto, es fundamental que el personal de seguridad esté debidamente capacitado para operar los sistemas, identificar comportamientos sospechosos y responder adecuadamente a situaciones de emergencia (MINDEF, 1999).

En resumen, el control de accesos es un elemento esencial en la seguridad de instalaciones críticas, y su implementación efectiva requiere una combinación de tecnologías avanzadas, como sistemas biométricos y autenticación multifactor, junto con una gestión adecuada de identidades y protocolos de seguridad. Este enfoque integral no solo protege las áreas físicas de una instalación, sino que también asegura que los sistemas informáticos y los datos estén igualmente resguardados contra accesos no autorizados. A medida que las amenazas a la seguridad evolucionan, los sistemas de control de accesos también deben adaptarse y mejorar para ofrecer una defensa robusta y eficaz contra intrusiones y otros riesgos.

#### **2.2.2.2. Vigilancia electrónica**

La vigilancia electrónica es un sistema de monitoreo y supervisión que utiliza tecnologías avanzadas para observar y controlar un espacio determinado, con el fin de

prevenir, detectar y responder a amenazas de seguridad. Este tipo de vigilancia emplea dispositivos como cámaras de seguridad, sensores de movimiento, micrófonos y sistemas de detección de intrusos, los cuales permiten una cobertura continua y detallada de áreas críticas como instalaciones militares, infraestructuras gubernamentales, centros industriales y espacios públicos. La vigilancia electrónica se ha convertido en una herramienta esencial en la gestión de la seguridad, ya que ofrece una supervisión constante y en tiempo real, lo que permite una respuesta más rápida y eficiente ante posibles incidentes de seguridad (Costa, 2010).

Uno de los principales componentes de la vigilancia electrónica es el uso de cámaras de videovigilancia. Estas cámaras, ubicadas estratégicamente, permiten a los operadores monitorear diversas áreas de una instalación o espacio público en tiempo real, almacenando imágenes y videos que pueden ser revisados posteriormente en caso de incidentes. Las cámaras de videovigilancia modernas suelen estar equipadas con tecnologías como reconocimiento facial y análisis de comportamiento, que facilitan la identificación de personas y actividades sospechosas. Las cámaras de seguridad no solo actúan como una herramienta de monitoreo, sino también como un elemento disuasorio, ya que su presencia visible puede reducir significativamente las acciones delictivas. La evolución de las cámaras, desde dispositivos analógicos hasta sistemas digitales con alta definición, ha incrementado la eficacia de la videovigilancia en la identificación y seguimiento de amenazas.

Otro aspecto clave en la vigilancia electrónica es la integración de sensores que permiten la detección de actividades no autorizadas. Estos sensores pueden incluir detectores de movimiento, infrarrojos, y sistemas de detección de apertura de puertas y ventanas, todos ellos diseñados para alertar sobre cualquier actividad que se salga de los parámetros normales. Los sistemas de detección de intrusos son fundamentales en áreas críticas, ya que pueden activarse automáticamente en caso de una violación de seguridad, alertando al personal encargado o activando respuestas automáticas, como el cierre de puertas o la activación de alarmas. La integración de estos sistemas con cámaras de seguridad y otros dispositivos permite una vigilancia más efectiva y reduce el tiempo de reacción ante posibles intrusiones o sabotajes (MINDEF, 1999).

Además de la supervisión de áreas físicas, la vigilancia electrónica también se extiende al ámbito de la seguridad cibernética, donde se monitorean las redes

informáticas y los sistemas de comunicación para prevenir accesos no autorizados y detectar intentos de hacking o infiltración. En un mundo cada vez más digitalizado, las instalaciones críticas dependen de redes de información para su operatividad diaria, lo que ha hecho que la vigilancia electrónica en el ciberespacio sea tan vital como la vigilancia física. Los sistemas de monitoreo de redes han evolucionado para incluir tecnologías avanzadas de detección de amenazas, como el uso de inteligencia artificial y algoritmos de aprendizaje automático que pueden identificar patrones de comportamiento sospechoso en el tráfico de red. Este enfoque permite no solo detectar intrusiones, sino también anticiparse a posibles amenazas antes de que se materialicen (Toledo, 2022).

Un aspecto importante de la vigilancia electrónica es su capacidad de almacenar y procesar grandes cantidades de datos. Las imágenes, videos y registros obtenidos de los sistemas de vigilancia pueden ser almacenados durante largos periodos de tiempo y utilizados para la revisión y análisis posterior. Esto es particularmente útil para la investigación de incidentes de seguridad, ya que permite a los analistas revisar eventos pasados con detalle y utilizar la información almacenada para mejorar las medidas de seguridad. El análisis de datos de vigilancia también ha mejorado con el uso de software avanzado que facilita la búsqueda de información relevante dentro de grandes bases de datos, permitiendo a los operadores filtrar eventos específicos y patrones de comportamiento con mayor rapidez y precisión (Seguridad en Todo, 2020).

En resumen, la vigilancia electrónica es una herramienta esencial en la protección de instalaciones y áreas críticas, ofreciendo una supervisión continua y una respuesta rápida ante posibles amenazas. La integración de tecnologías como cámaras de videovigilancia, sensores de movimiento, y sistemas de monitoreo cibernético ha transformado la forma en que se gestionan las operaciones de seguridad. A medida que las tecnologías continúan avanzando, la vigilancia electrónica se está volviendo más sofisticada, ofreciendo una mayor capacidad para detectar y prevenir actividades delictivas o de sabotaje. Este enfoque multidimensional ha demostrado ser efectivo tanto en la disuasión como en la detección de amenazas, mejorando la seguridad de infraestructuras críticas y la protección de las personas.

### **2.2.2.3.Respuesta a emergencias**

La respuesta a emergencias es el conjunto de acciones coordinadas y planificadas que se ejecutan ante la ocurrencia de un evento crítico que pone en riesgo la seguridad de las personas, las instalaciones o los recursos. Este tipo de respuesta incluye tanto procedimientos inmediatos para mitigar los efectos del evento como las estrategias a largo plazo para asegurar la continuidad de las operaciones y minimizar los daños. En el ámbito militar, industrial y de infraestructuras críticas, la respuesta a emergencias es fundamental para garantizar la estabilidad y la seguridad en situaciones de crisis. La eficacia de una respuesta de emergencia depende en gran medida de la preparación previa, que incluye la formación del personal, la existencia de protocolos claros, y la disponibilidad de los recursos necesarios para responder rápidamente a cualquier tipo de amenaza, ya sea física, como un ataque o incendio, o cibernética, como un hackeo o sabotaje (Enciclopedia Humanidades, 2023).

Un componente esencial en la respuesta a emergencias es la activación de los planes de contingencia. Estos planes son documentos estratégicos que detallan los pasos a seguir en caso de que ocurra una emergencia, asignando roles y responsabilidades a las personas involucradas. El objetivo de un plan de contingencia es reducir el tiempo de reacción ante una emergencia, asegurando que todas las acciones necesarias para mitigar los efectos del evento sean ejecutadas de manera rápida y eficiente. Los planes de contingencia deben ser flexibles y adaptarse a diferentes escenarios, ya que las emergencias pueden variar en magnitud y naturaleza. Además, deben ser revisados y actualizados periódicamente para asegurar que se mantengan relevantes y efectivos frente a nuevas amenazas o cambios en las instalaciones (Costa, 2010).

La comunicación es otro aspecto fundamental de la respuesta a emergencias. La coordinación eficaz entre los equipos encargados de manejar la emergencia, los empleados de la instalación y los organismos externos, como bomberos o fuerzas de seguridad, es crucial para garantizar una respuesta rápida y adecuada. Los sistemas de comunicación internos deben estar bien establecidos, con canales de información claros que permitan que las órdenes se transmitan de manera efectiva y sin interrupciones. Además, el personal debe estar capacitado para utilizar estos sistemas en situaciones de alta presión, y es esencial que existan protocolos de comunicación redundantes para

asegurar que la información pueda ser transmitida incluso si uno de los sistemas falla durante la emergencia (Gómez, 2024).

Otro elemento clave es la evacuación y protección de las personas dentro de las instalaciones afectadas. En muchas situaciones de emergencia, la seguridad del personal es la máxima prioridad, y la evacuación o el confinamiento en áreas seguras debe ser ejecutado de forma rápida y ordenada. Esto requiere simulacros regulares y una planificación exhaustiva para garantizar que todos los ocupantes conozcan las rutas de evacuación, los puntos de reunión y los procedimientos a seguir. La importancia de los simulacros de emergencia es pieza clave en la preparación de los empleados, ya que permiten identificar posibles fallos en los procedimientos y mejorar la capacidad de respuesta del personal en situaciones reales. Además, los simulacros ayudan a reducir el pánico y el caos durante una emergencia real, mejorando la eficacia de las evacuaciones y otras acciones de respuesta (MINDEF, 1999).

La gestión de los recursos durante una emergencia también es crucial para asegurar una respuesta adecuada. Esto incluye la disponibilidad de equipos de protección personal, sistemas de extinción de incendios, primeros auxilios y herramientas tecnológicas para monitorear y controlar el desarrollo del evento. La asignación adecuada de estos recursos durante una emergencia puede marcar la diferencia entre un incidente controlado y una catástrofe. Además, la gestión de recursos incluye la colaboración con agencias externas, como cuerpos de bomberos, equipos de rescate y personal médico, que pueden ser necesarios para proporcionar asistencia adicional durante la emergencia (Seguridad en Todo, 2020).

Finalmente, la recuperación post-emergencia es una fase crítica en la respuesta a emergencias, que se enfoca en restaurar la normalidad y evaluar los daños para prevenir futuras situaciones similares. La recuperación incluye la evaluación de los sistemas afectados, la reparación de daños, y la implementación de mejoras en los protocolos y la infraestructura. La fase de recuperación es clave para aprender de los errores y mejorar las capacidades de respuesta. El análisis detallado de la emergencia permite identificar qué aspectos del plan de respuesta funcionaron bien y cuáles deben ser corregidos, lo que fortalece la preparación ante posibles eventos futuros (Sampó y Alda, 2024).

En resumen, la respuesta a emergencias es un proceso multidimensional que abarca desde la preparación y planificación hasta la gestión y recuperación después de un evento crítico. La eficacia de esta respuesta depende de una combinación de factores, como la existencia de planes de contingencia, la comunicación eficaz, la evacuación organizada, la gestión de recursos y la capacidad de aprender y mejorar tras una emergencia. A medida que las amenazas se vuelven más complejas, especialmente en instalaciones críticas, la capacidad de una organización para responder adecuadamente a emergencias puede ser la diferencia entre el éxito y el desastre.

### 2.3. Marco conceptual

**Análisis de Inteligencia:** Proceso sistemático de revisión y evaluación de información para transformar datos en conocimiento útil para la toma de decisiones militares. Esto incluye la interpretación de señales, comunicaciones y movimientos del enemigo. El análisis de inteligencia permite prever amenazas y ajustar estrategias en tiempo real (Defaz y Polanco, 2020).

**Análisis Predictivo:** Uso de herramientas analíticas y algoritmos para prever posibles escenarios o amenazas a partir de los datos recolectados. En el ámbito militar, el análisis predictivo permite anticiparse a los movimientos del enemigo. Este enfoque ha ganado relevancia con el uso de inteligencia artificial en las operaciones de inteligencia (Herrera y Navarro, 2021).

**Ciberinteligencia:** Uso de herramientas digitales para recopilar, analizar y proteger información en el ámbito cibernético. La ciberinteligencia es fundamental para prevenir ataques cibernéticos que puedan comprometer la seguridad de las infraestructuras militares. Esta disciplina ha crecido en importancia debido al aumento de las amenazas digitales (Sampó y Alda, 2024).

**Ciberseguridad en Instalaciones:** Estrategias y tecnologías implementadas para proteger los sistemas informáticos y las redes de una instalación contra ciberataques. Esto incluye el uso de firewalls, sistemas de detección de intrusos y software de protección. La ciberseguridad es crucial para evitar que actores malintencionados accedan a información sensible o saboteen sistemas operativos (Toledo, 2022).

**Contrainteligencia:** Conjunto de acciones destinadas a detectar, prevenir y neutralizar los intentos de espionaje o infiltración por parte de actores enemigos. La contrainteligencia protege tanto la información sensible como los sistemas de inteligencia operativa. La contrainteligencia es una barrera esencial para salvaguardar los secretos y planes estratégicos (Mendoza, 2020).

**Control de Accesos:** Proceso mediante el cual se gestiona y regula quién puede ingresar a áreas específicas de una instalación. Este sistema utiliza tecnologías como tarjetas de identificación, lectores biométricos y autenticación multifactor. El control de accesos es fundamental para prevenir infiltraciones y mantener la seguridad de las áreas restringidas (Seguridad en Todo, 2020).

**Evacuación de Emergencia:** Proceso mediante el cual se evacúan de manera rápida y ordenada a las personas que se encuentran en una instalación ante situaciones de riesgo como incendios, terremotos o ataques. La planificación y ejecución de simulacros regulares son claves para garantizar la seguridad de los ocupantes durante una emergencia (INSST, 2019).

**Gestión de Identidades:** Proceso mediante el cual se administra el acceso a diferentes áreas y sistemas dentro de una instalación. Esto incluye la creación, mantenimiento y eliminación de credenciales para empleados, visitantes y contratistas. Una gestión adecuada de identidades es fundamental para asegurar que solo las personas autorizadas tengan acceso a áreas críticas (Palacios, Romero y Ñaupas, 2016).

**Inteligencia de Señales (SIGINT):** Rama de la inteligencia militar que se enfoca en la interceptación de comunicaciones electrónicas y señales emitidas por los sistemas enemigos. SIGINT es crucial para obtener información sobre las capacidades y movimientos del adversario sin necesidad de intervención física directa (Conde y Hernández, 2020).

**Inteligencia Humana (HUMINT):** Método de recolección de información que se basa en la obtención de datos a través de fuentes humanas, como informantes o espías. Esta técnica es una de las más antiguas en la inteligencia militar y sigue siendo relevante para obtener información que las tecnologías no pueden captar (Noboa, 2020).

**Inteligencia Militar:** Proceso mediante el cual las fuerzas armadas recopilan, analizan y utilizan información para tomar decisiones estratégicas y tácticas en operaciones militares. Su objetivo es anticiparse a los movimientos del enemigo y minimizar las amenazas. La

inteligencia militar es clave para garantizar la seguridad nacional al proporcionar información precisa y oportuna (Vargas, 2021).

**Operaciones de Vigilancia:** Proceso de monitoreo continuo de áreas, personas o actividades con el objetivo de detectar amenazas potenciales. La vigilancia puede ser física o electrónica y se utiliza para anticipar los movimientos del enemigo. Las operaciones de vigilancia permiten a las fuerzas armadas actuar de manera preventiva (Gómez, 2024).

**Operaciones Encubiertas:** Actividades llevadas a cabo de manera clandestina para obtener información o realizar acciones sin que el enemigo sea consciente de ellas. Estas operaciones son clave en la inteligencia militar para obtener datos sin alertar a las fuerzas enemigas (Vela, 2023).

**Recolección de Información:** Actividad en la que se obtienen datos relevantes para las operaciones militares, ya sea a través de fuentes humanas, electrónicas o tecnológicas. La recolección de información es un proceso continuo que alimenta el ciclo de inteligencia para mantener una ventaja sobre posibles amenazas (Machuca, 2022).

**Recuperación Post-Emergencia:** Fase de gestión de crisis que se enfoca en restaurar la normalidad en las instalaciones tras un incidente crítico. Esta fase incluye la reparación de daños, la evaluación de las pérdidas y la implementación de mejoras para prevenir futuros incidentes. Una recuperación efectiva es clave para garantizar la continuidad operativa y fortalecer la seguridad futura (Uriarte, 2022).

**Seguridad en las Instalaciones:** Conjunto de medidas y sistemas diseñados para proteger infraestructuras, personas y activos dentro de un espacio físico contra amenazas externas e internas, como intrusiones, sabotajes o desastres naturales. Estas medidas incluyen vigilancia, control de accesos, sistemas de alarma y protocolos de emergencia para garantizar la protección de instalaciones críticas (Blog de Contabilidad, 2023).

**Seguridad Perimetral:** Sistema de protección que se encarga de resguardar el perímetro de una instalación mediante barreras físicas, cercas, sensores y cámaras. La seguridad perimetral es la primera línea de defensa para detectar y detener intrusiones antes de que comprometan la integridad de la instalación (Costa, 2010).

**Simulacros de Emergencia:** Ejercicios planificados que permiten a los ocupantes de una instalación practicar los protocolos de evacuación y respuesta ante diferentes tipos de

emergencias. Estos simulacros mejoran la capacidad de reacción y reducen el caos durante una situación real. Los simulacros regulares son una de las mejores prácticas para preparar al personal ante posibles crisis (Gómez, 2024).

**Sistema de Alarmas:** Tecnología que emite alertas sonoras, visuales o digitales ante la detección de un incidente de seguridad, como una intrusión, incendio o sabotaje. Los sistemas de alarma son esenciales para la movilización de los equipos de respuesta y para alertar a los ocupantes de una instalación sobre la necesidad de evacuar o actuar frente a una amenaza (Hernández y Mendoza, 2018).

**Sistemas de Detección de Intrusos:** Conjunto de tecnologías y procedimientos que permiten identificar actividades no autorizadas dentro de una instalación. Estos sistemas, que pueden ser físicos o electrónicos, envían alertas automáticas cuando se detectan violaciones de seguridad. Estos sistemas son esenciales para minimizar el tiempo de reacción ante amenazas y prevenir daños mayores (MINDEF, 1999).

**Sistemas de Inteligencia:** Infraestructura tecnológica y operativa que permite la recopilación, procesamiento y análisis de información. Estos sistemas incluyen herramientas tecnológicas como satélites, drones y software de análisis de datos. La evolución de estos sistemas ha revolucionado la forma en que las fuerzas armadas gestionan la información (Guerra y Terán, 2020).

**Vigilancia Electrónica:** Uso de tecnologías como cámaras de videovigilancia, sensores de movimiento y sistemas de monitoreo para supervisar continuamente una instalación. La vigilancia electrónica permite la detección temprana de actividades sospechosas y facilita la respuesta rápida ante incidentes de seguridad (INSST, 2019).

## 2.4. Operacionalización de las variables

**Tabla 1.**

*Operacionalización de las variables*

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
<b>Variable 1</b> Estrategias de inteligencia militar	Conjunto de acciones organizadas para recopilar, analizar y utilizar información que permita anticipar y neutralizar amenazas, facilitando la toma de decisiones tácticas y estratégicas en operaciones militares.	Variable cualitativa ordinal; esta variable fue medida a través de un cuestionario con 12 preguntas cerradas y respuestas en escala de Likert, aplicadas a los cadetes de la Escuela Militar de Chorrillos 2024.	Análisis de información	<ul style="list-style-type: none"> <li>• Recopilación de datos</li> <li>• Validación de fuentes</li> <li>• Análisis predictivo</li> <li>• Identificación de amenazas</li> </ul>	Ordinal Cuestionario tipo Likert
			Operaciones de contrainteligencia	<ul style="list-style-type: none"> <li>• Protección de datos</li> <li>• Control de infiltraciones</li> <li>• Supervisión interna</li> <li>• Prevención de espionaje</li> </ul>	
			Tecnología en inteligencia	<ul style="list-style-type: none"> <li>• Uso de drones</li> <li>• Monitoreo satelital</li> <li>• Sistemas criptográficos</li> <li>• Inteligencia artificial</li> </ul>	
<b>Variable 2</b> Seguridad en las instalaciones	Medidas y tecnologías implementadas para proteger personas, activos y recursos dentro de un espacio físico, previniendo intrusiones, sabotajes o desastres.	Variable cualitativa ordinal; esta variable fue medida a través de un cuestionario con 12 preguntas cerradas y respuestas en escala de Likert, aplicadas a los cadetes de la Escuela Militar de Chorrillos 2024.	Control de accesos	<ul style="list-style-type: none"> <li>• Verificación de identidad</li> <li>• Sistemas biométricos</li> <li>• Monitoreo perimetral</li> <li>• Supervisión de visitantes</li> </ul>	Ordinal Cuestionario tipo Likert
			Vigilancia electrónica	<ul style="list-style-type: none"> <li>• Cámaras de seguridad</li> <li>• Detección de movimiento</li> <li>• Monitoreo remoto</li> <li>• Alarmas de intrusión</li> </ul>	
			Respuesta a emergencias	<ul style="list-style-type: none"> <li>• Protocolos de evacuación</li> <li>• Personal de seguridad</li> <li>• Planes de contingencia</li> <li>• Simulacros regulares</li> </ul>	

## **2.5. Formulación de hipótesis**

### **2.5.1. *Hipótesis general***

Existe relación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

### **2.5.2. *Hipótesis específicas***

Existe relación directa y significativa entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

Existe relación directa y significativa entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

Existe relación directa y significativa entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

## **CAPÍTULO III.**

### **Marco metodológico**

#### **3.1. Enfoque de investigación**

El enfoque de nuestra investigación fue cuantitativo, lo que permitió analizar la relación entre las variables de manera objetiva y basada en datos numéricos. Este tipo de enfoque se caracterizó por el uso de instrumentos estructurados para la recolección de información, como cuestionarios con preguntas cerradas, que se aplicaron a una muestra representativa de cadetes de la Escuela Militar de Chorrillos "CFB". A través de este enfoque, se buscó medir con precisión la percepción de los participantes respecto a las estrategias de inteligencia militar y la seguridad en las instalaciones, obteniendo resultados que pudieran ser generalizables a la población estudiada. Según Ñaupas et al. (2018), el enfoque cuantitativo es especialmente útil para identificar patrones y establecer correlaciones entre variables, lo que fue fundamental para cumplir con los objetivos de nuestra investigación.

El enfoque cuantitativo nos permitió utilizar herramientas estadísticas, como la prueba de correlación de Spearman, para determinar la relación entre las variables analizadas. Al trabajar con datos numéricos, se posibilitó la realización de análisis inferenciales que evidenciaron la existencia de una correlación significativa entre el uso de tecnologías de inteligencia y la seguridad en las instalaciones. Este tipo de análisis estadístico también permitió que los resultados fueran comparables con investigaciones previas en contextos similares, proporcionando una base sólida y objetiva para el estudio. Como destaca Ñaupas et al. (2018), este enfoque cuantitativo aporta claridad y precisión en la interpretación de los fenómenos estudiados, lo que contribuye a una mayor validez y confiabilidad de los resultados obtenidos.

#### **3.2. Tipo de investigación**

El tipo de esta investigación fue básico o investigación pura, enfocándose en ampliar el conocimiento existente sobre la relación entre las estrategias de inteligencia militar y la seguridad en las instalaciones. A diferencia de la investigación aplicada, que busca resolver problemas prácticos inmediatos, este estudio se centró en contribuir al desarrollo teórico de los conceptos y modelos relacionados con la inteligencia militar y la seguridad institucional. Según Ñaupas et al. (2018), la investigación pura tiene como objetivo principal generar conocimiento

nuevo y comprensible, sin necesariamente buscar una aplicación práctica inmediata, lo que fue fundamental para este estudio.

El enfoque básico permitió que el estudio profundizara en la comprensión de las dinámicas internas de la seguridad en las instalaciones militares y cómo estas están influenciadas por las estrategias de inteligencia implementadas. A través de la recopilación de datos y el análisis cuantitativo, se buscó no solo identificar relaciones significativas entre las variables, sino también aportar a la construcción de un marco teórico sólido que pudiera ser utilizado en futuras investigaciones sobre seguridad militar. Ñaupas et al. (2018) afirman que este tipo de investigación contribuye al enriquecimiento de la teoría en campos del conocimiento específicos, lo cual fue clave en nuestra investigación, ya que las conclusiones obtenidas podrían servir como base para estudios posteriores que deseen explorar otros aspectos de la inteligencia militar o profundizar en los hallazgos aquí presentados.

La elección de una investigación básica permitió un análisis riguroso y detallado de las variables clave, lo que generó nuevas perspectivas y aportes conceptuales dentro del campo de la seguridad militar, destacando la importancia del estudio de la inteligencia en la protección de infraestructuras críticas.

### **3.3. Método de investigación**

El método utilizado en esta investigación fue el hipotético-deductivo, siguiendo los principios desarrollados por Karl Popper. Este enfoque se basa en la formulación de hipótesis que luego son contrastadas mediante la observación empírica y el análisis de los datos recolectados. En este caso, partimos de una hipótesis general que planteaba una relación directa entre las estrategias de inteligencia militar y la seguridad en las instalaciones. A lo largo del proceso, se establecieron hipótesis específicas que fueron sometidas a pruebas estadísticas rigurosas, lo que permitió validar o rechazar las proposiciones iniciales, como lo señala Marfull (2024), quien destaca que este método es fundamental para la generación de conocimiento científico.

El método hipotético-deductivo aplicado en esta investigación permitió estructurar el estudio de manera lógica y coherente. En primer lugar, se formularon las hipótesis basadas en teorías y estudios previos, luego se diseñó un marco metodológico que incluyó la recolección de datos a través de encuestas cuantitativas y finalmente se utilizó el análisis estadístico para probar las hipótesis planteadas. Según Marfull (2024), este método se caracteriza por su capacidad para generar conclusiones basadas en datos empíricos que pueden ser verificadas o

refutadas, lo que lo convierte en una herramienta esencial para investigaciones científicas. En nuestro estudio, el uso del método hipotético-deductivo facilitó la evaluación objetiva de las relaciones entre variables, ofreciendo un proceso sistemático para validar la relación entre las estrategias de inteligencia y la seguridad de las instalaciones en la Escuela Militar de Chorrillos "CFB".

Este enfoque también permitió la refinación del marco teórico subyacente, ya que al probar las hipótesis, se generaron resultados que contribuyen tanto a la validación como a la mejora del conocimiento existente en el campo de la seguridad militar.

#### **3.4. Alcance de investigación (nivel)**

El alcance de esta investigación fue descriptivo-correlacional, lo que permitió no solo describir las características principales de las estrategias de inteligencia militar y la seguridad en las instalaciones, sino también identificar la relación existente entre ambas variables. En el nivel descriptivo, el estudio se centró en detallar cómo se implementan las estrategias de inteligencia en la Escuela Militar de Chorrillos "CFB" y cómo los cadetes perciben la seguridad de las instalaciones. Según Hernández y Mendoza (2018), el enfoque descriptivo busca especificar propiedades, características y perfiles de personas o grupos, lo cual fue fundamental en esta investigación para obtener una comprensión detallada de las prácticas actuales.

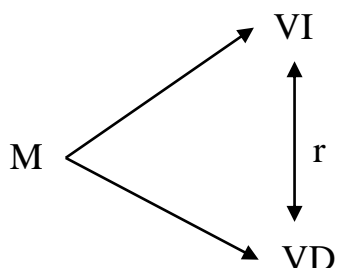
En el nivel correlacional, la investigación se propuso explorar si existía una relación significativa entre las estrategias de inteligencia y la seguridad en las instalaciones. A través de pruebas estadísticas como la correlación de Spearman, se logró establecer que ambas variables están altamente relacionadas, lo que permitió identificar patrones relevantes dentro de los datos obtenidos. Hernández y Mendoza (2018) explican que el nivel correlacional busca medir el grado de relación entre dos o más variables, lo que resulta esencial cuando se pretende demostrar si los cambios en una variable tienen algún impacto sobre la otra. Este enfoque no se limitó a describir los fenómenos, sino que permitió profundizar en la comprensión de cómo la mejora en la implementación de estrategias de inteligencia puede influir positivamente en la percepción de seguridad en las instalaciones.

Este alcance descriptivo-correlacional fue crucial para responder a los objetivos planteados en la investigación, ya que no solo permitió un análisis detallado de las prácticas y percepciones existentes, sino que también facilitó el establecimiento de relaciones

significativas entre las variables clave del estudio, lo que aporta valiosos insumos teóricos y prácticos en el campo de la seguridad militar.

**Figura 1.**

*Esquema de correlación*



Donde:

M = Muestra

VI = Variable 1: Estrategias de inteligencia militar

VD = Variable 2: Seguridad en las instalaciones

r = Correlación entre dichas variables

### 3.5. Diseño de la investigación

El diseño del estudio fue no experimental y de carácter transversal, lo que significa que no se manipularon las variables de manera deliberada y los datos se recolectaron en un solo momento en el tiempo. Según Hernández y Mendoza (2018), en los estudios no experimentales, los investigadores observan y analizan las variables tal como se presentan en la realidad, sin intervenir directamente en su modificación o control. En este caso, se evaluaron las percepciones de los cadetes de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" sobre las estrategias de inteligencia militar y la seguridad en las instalaciones, sin modificar sus experiencias o influir en su entorno. Esto permitió realizar un análisis de correlación entre ambas variables sin alterar el curso natural de los eventos.

El diseño transversal, por su parte, implica que los datos se recopilaban en un momento específico, lo que permitió hacer una "fotografía" de la situación en un punto del tiempo. Como señalan Hernández y Mendoza (2018), el enfoque transversal es adecuado cuando el objetivo es describir o correlacionar variables en un periodo determinado, sin necesidad de observar

cambios a lo largo del tiempo. En esta investigación, se pretendía identificar la relación entre las estrategias de inteligencia militar y la seguridad en las instalaciones tal como los cadetes las percibían en ese momento, sin realizar un seguimiento a largo plazo.

Este diseño permitió realizar un análisis riguroso de las relaciones entre variables sin interferir en las condiciones existentes. Al ser no experimental y transversal, se garantizó que los datos obtenidos fueran representativos de la situación actual en la Escuela Militar de Chorrillos, facilitando la interpretación y aplicación de los resultados en el contexto real de la seguridad militar.

### **3.6. Población, muestra, unidad de estudio**

#### ***3.6.1. Población de estudio***

Se establecen una población de 1247 cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, Año 2024.

Según Hernández y Mendoza (2018), la población de estudio se refiere al conjunto total de elementos o individuos que comparten una serie de características comunes y que son objeto de interés en una investigación. Es decir, la población es el grupo completo al que se quiere aplicar los resultados del estudio. En el contexto de esta investigación, la población estuvo compuesta por todos los cadetes de la Escuela Militar de Chorrillos "CFB", quienes fueron seleccionados debido a su experiencia y participación directa en las actividades de seguridad e inteligencia dentro de las instalaciones.

Hernández y Mendoza (2018) señalan que la definición de la población debe estar claramente delimitada en función de los criterios específicos de inclusión, que en este caso incluyeron a los cadetes en formación, quienes participan activamente en los procedimientos de seguridad. Además, la definición adecuada de la población es fundamental para garantizar que los resultados obtenidos sean representativos y que las conclusiones del estudio puedan generalizarse al grupo más amplio. Este enfoque permitió un análisis más preciso y detallado del comportamiento de la población estudiada.

#### ***3.6.2. Muestra de estudio***

Es probabilístico de tipo aleatorio, tomando en cuenta la siguiente fórmula:

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

N =	1,247	Tamaño de la población
Z =	1.96	Nivel de confianza (95%)
p =	0.5	Probabilidad de éxito
q =	0.5	Probabilidad de fracaso
d =	0.05	Margen de error

$$n = \frac{(1247) * (1.96)^2 * (0.5) * (0.5)}{(0.05)^2 * (1247 - 1) + (1.96)^2 * (0.5) * (0.5)}$$

$$n = \frac{1197.6188}{4.08}$$

$$n = 293.87$$

294 cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, Año 2024, dando como resultado a la muestra.

La muestra del estudio fue probabilística de tipo aleatorio, lo que significa que cada cadete de la población total de la Escuela Militar de Chorrillos "CFB" tuvo la misma probabilidad de ser seleccionado para participar en la investigación. Este tipo de muestreo, según Hernández y Mendoza (2018), se caracteriza por garantizar que la selección de los participantes sea imparcial y representativa de la población. Al ser aleatorio, el proceso de selección elimina cualquier sesgo que pudiera influir en los resultados, permitiendo que las conclusiones obtenidas sean más generalizables al grupo completo de cadetes.

En este estudio, se utilizó un procedimiento en el que los cadetes fueron seleccionados de manera aleatoria, siguiendo los principios del muestreo probabilístico, lo que asegura que los resultados reflejen con precisión las características y opiniones de toda la población. Hernández y Mendoza (2018) destacan que este tipo de muestreo es ideal cuando se busca obtener datos representativos y objetivos, minimizando el riesgo de error muestral y maximizando la validez de los hallazgos en contextos de investigación cuantitativa.

### **3.6.3. Unidad de estudio**

La unidad de estudio serían los cadetes de la EMCH “CFB” que estuvieron involucrados en el estudio.

Según Hernández y Mendoza (2018), la unidad de estudio, también conocida como unidad de análisis, se refiere al objeto o sujeto del cual se recolecta información para la investigación. Es el elemento fundamental que se examina en el estudio y puede abarcar desde individuos, grupos, organizaciones o cualquier entidad que cumpla con las características definidas para la investigación. En este caso, la unidad de estudio estuvo compuesta por los cadetes de la Escuela Militar de Chorrillos "CFB", quienes representaban el grupo de interés para analizar la relación entre las estrategias de inteligencia militar y la seguridad en las instalaciones.

La unidad de estudio debe estar claramente identificada para garantizar que los datos recolectados correspondan de manera precisa a los objetivos de la investigación. Hernández y Mendoza (2018) subrayan que la elección de la unidad de estudio debe estar alineada con el tipo de investigación y las hipótesis planteadas. En esta investigación, los cadetes fueron seleccionados como unidades de estudio porque su experiencia y participación directa en las actividades de seguridad dentro de la escuela los convierte en fuentes clave de información para evaluar la efectividad de las estrategias de inteligencia militar.

Además, Hernández y Mendoza (2018) explican que la correcta definición de la unidad de estudio permite que la investigación sea más precisa y enfocada. En el caso de esta investigación, el enfoque en los cadetes permitió recopilar datos relevantes sobre su percepción y experiencia en la aplicación de las estrategias de inteligencia y cómo estas impactan en la seguridad de las instalaciones militares. Esta selección de la unidad de estudio fue crucial para obtener conclusiones válidas y representativas del fenómeno analizado.

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

### **3.7.1. Técnica de recolección de datos**

La técnica de recolección de datos empleada en esta investigación fue la encuesta, una herramienta ampliamente utilizada en estudios cuantitativos por su capacidad de recopilar información estandarizada de manera eficiente. Según Machuca (2022), la encuesta es una técnica que permite obtener datos directos de los participantes a través de preguntas

previamente estructuradas, lo que facilita el análisis estadístico posterior. En esta investigación, las encuestas fueron diseñadas con un formato de preguntas cerradas y una escala de Likert, lo que permitió medir con precisión las percepciones de los cadetes sobre las estrategias de inteligencia militar y la seguridad en las instalaciones.

La encuesta se aplicó a una muestra representativa de cadetes de la Escuela Militar de Chorrillos "CFB", garantizando que los resultados reflejaran las opiniones de toda la población. Como destaca Machuca (2022), las encuestas son eficaces para recopilar grandes volúmenes de datos en un tiempo relativamente corto, lo que las convierte en una técnica ideal para estudios que buscan correlacionar variables, como es el caso de esta investigación. Al estandarizar las preguntas, se asegura que todos los participantes respondan de manera consistente, lo que facilita la comparación y análisis de los datos.

Además, las encuestas permiten que los participantes respondan de forma anónima, lo que reduce el sesgo social y garantiza respuestas más sinceras y precisas. En este contexto, la técnica de la encuesta resultó clave para obtener una visión detallada de cómo los cadetes perciben la relación entre las estrategias de inteligencia y la seguridad en las instalaciones. La estructuración de las preguntas, siguiendo los principios sugeridos por Machuca (2022), ayudó a obtener información relevante y fiable para alcanzar los objetivos de la investigación.

### **3.7.2. Instrumento de recolección de datos**

El instrumento de recolección de datos utilizado en esta investigación fue el cuestionario, diseñado con preguntas cerradas y respuestas en una escala de Likert. Según Hernández y Mendoza (2018), el cuestionario es un instrumento fundamental en investigaciones cuantitativas, ya que permite estructurar las preguntas de manera que los participantes respondan dentro de un marco definido, facilitando la posterior cuantificación y análisis de los datos. En este estudio, se eligieron preguntas cerradas para guiar a los cadetes hacia respuestas específicas que reflejaran su percepción sobre las estrategias de inteligencia militar y la seguridad en las instalaciones.

El uso de la escala de Likert, que generalmente oscila entre cinco opciones, desde "Nunca" hasta "Siempre", permitió medir con mayor precisión las actitudes, opiniones y percepciones de los cadetes. Esta técnica, como señalan Hernández y Mendoza (2018), es ideal para estudios donde se busca evaluar la intensidad de las opiniones de los participantes sobre un tema en particular. En el contexto de esta investigación, las escalas de Likert proporcionaron

una forma efectiva de medir la relación entre las variables clave, facilitando la obtención de datos precisos y comparables sobre la percepción de los cadetes en torno a la seguridad de las instalaciones.

El cuestionario, como instrumento, también permitió estandarizar el proceso de recolección de datos, asegurando que todos los cadetes respondieran las mismas preguntas de manera uniforme. Esto fue esencial para mantener la consistencia en las respuestas y garantizar que los datos pudieran ser analizados de manera estadística. Como destacan Hernández y Mendoza (2018), la estructura de preguntas cerradas y el uso de escalas de Likert proporcionan un alto nivel de objetividad en la interpretación de los resultados, lo que contribuye a la validez y confiabilidad de la investigación.

**Tabla 2.**  
*Diagrama de Likert*

<b>Nunca</b>	<b>Casi nunca</b>	<b>A veces</b>	<b>Casi siempre</b>	<b>Siempre</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>

Fuente: Desarrollada en 1932 por el sociólogo Rensis Likert

Según Coll (2020), la utilización de un baremo se refiere a la creación de una escala estandarizada que permite interpretar los resultados obtenidos en una evaluación o investigación en función de criterios previamente establecidos. Un baremo sirve como referencia para comparar los puntajes o respuestas de los participantes y situarlos dentro de rangos específicos, facilitando la interpretación de los datos de manera objetiva. En este contexto, un baremo proporciona un marco de referencia para clasificar las respuestas según su nivel de adecuación, permitiendo identificar patrones y tendencias dentro de la población estudiada.

En investigaciones cuantitativas, como la presente, el uso de un baremo es crucial para darle significado a las respuestas obtenidas mediante cuestionarios con escalas de Likert. Según Coll (2020), un baremo puede transformar las respuestas en categorías interpretables, como “alto”, “medio” o “bajo”, dependiendo del puntaje total. Este enfoque facilita la identificación de las áreas en las que los participantes muestran mayores fortalezas o debilidades, al tiempo que estandariza la comparación de los resultados entre diferentes grupos o categorías.

Además, el baremo ofrece la ventaja de estandarizar la interpretación de los datos, reduciendo el riesgo de subjetividad en el análisis. Al establecer un conjunto claro de criterios para cada nivel, los investigadores pueden asegurar que los resultados se analicen de manera

consistente y precisa. Coll (2020) señala que el uso de un baremo también permite comparar los resultados de diferentes estudios o poblaciones, siempre y cuando se utilicen los mismos criterios de interpretación. En resumen, un baremo es una herramienta valiosa en el análisis de datos cuantitativos, proporcionando una referencia clara y objetiva para la interpretación de los resultados obtenidos en la investigación.

### ***3.7.3. Validez y confiabilidad de los instrumentos de medición***

La validación del instrumento requería un enfoque riguroso y detallado, por lo que se optó por el método del "Juicio de Expertos", un proceso que implica someter el cuestionario a la evaluación crítica de profesionales altamente calificados en el campo de estudio. En este caso, tres expertos con grados de magíster y doctorado de la EMCH "CFB" fueron convocados para analizar y ofrecer su opinión sobre el instrumento propuesto. Sus apreciaciones fueron cuidadosamente registradas y resumidas en un cuadro para su posterior análisis detallado, que se adjuntaría como anexo al documento principal.

Tras recibir el juicio de los expertos, se llevó a cabo una prueba piloto del instrumento con la participación de 20 cadetes de Infantería de la misma institución. Esta prueba permitió identificar posibles áreas de mejora y ajustes necesarios en el cuestionario antes de su implementación definitiva.

Para evaluar la confiabilidad del instrumento, se empleó el estándar alfa de Cronbach, una medida estadística ampliamente reconocida para verificar la consistencia interna de un conjunto de ítems. Este coeficiente proporciona información sobre la fiabilidad y la consistencia de las respuestas obtenidas a partir del instrumento. Se analizó la relación de las variables con los coeficientes alfa de Cronbach para asegurar la estabilidad y precisión del instrumento, utilizando herramientas como SPSS 27 para procesar los datos y calcular los valores correspondientes.

Por lo cual, el proceso de validación del instrumento fue integral y meticuloso, combinando el juicio de expertos, pruebas piloto y análisis estadísticos para garantizar su fiabilidad y validez. Este enfoque aseguró que el instrumento fuera adecuado y confiable para su uso en la investigación planificada, proporcionando una base sólida para la recopilación y análisis de datos precisos y significativos.

**Tabla 3.**  
*Criterio de confiabilidad valores*

<b>Intervalo de Alpha de Cronbach</b>	<b>Valoración</b>
“0 < 0.20”	“Muy Baja”
“0.21 < 0.40”	“Baja”
“0.41 < 0.60”	“Moderada”
“0.61 < 0.80”	“Alta”
“0.81 < 1”	“Muy Alta”

Este instrumento se utilizó en la prueba piloto de toda la muestra de 20 cadetes.

El coeficiente de Alfa de Cronbach, una herramienta de vital importancia en la evaluación de la consistencia interna de un conjunto de ítems en un cuestionario o escala, ha sido un pilar fundamental en la investigación psicométrica desde su desarrollo por el renombrado psicólogo Lee Cronbach en 1951. Este coeficiente, representado por el símbolo  $\alpha$ , proporciona una medida cuantitativa de la fiabilidad del instrumento, lo que ayuda a los investigadores a Establecer la coherencia con la que las preguntas en un cuestionario están correlacionadas entre sí.

El coeficiente de alfa de Cronbach, cuya interpretación se basa en su escala de valores de 0 a 1, proporciona información crucial sobre la consistencia interna de los ítems del cuestionario. Un valor cercano a 1 indica una alta consistencia, lo que sugiere una fuerte correlación entre las preguntas y una medición confiable del mismo constructo o dimensión. Por el contrario, un valor cercano a 0 indica una baja consistencia, lo que implica que las preguntas pueden medir conceptos diferentes y no están relacionadas entre sí.

Generalmente, un coeficiente de alfa de Cronbach superior a 0.7 se considera aceptable para demostrar una consistencia interna adecuada. No obstante, esta evaluación puede variar según el contexto y los objetivos específicos de la investigación. Por ejemplo, en estudios más sensibles o con escalas más cortas, podría ser aceptable un valor ligeramente inferior de alfa de Cronbach.

Es importante destacar que el coeficiente de alfa de Cronbach asume que los ítems del cuestionario miden una única dimensión o concepto subyacente. Si el cuestionario evalúa múltiples conceptos o dimensiones distintas, puede ser más adecuado utilizar otros métodos de análisis de consistencia interna, como el análisis factorial confirmatorio.

Por lo cual, el coeficiente de alfa de Cronbach es una herramienta invaluable en la evaluación de la confiabilidad de un cuestionario, proporcionando a los investigadores una

medida objetiva de la consistencia interna de los ítems. Su interpretación cuidadosa y su aplicación adecuada contribuyen significativamente a la calidad y validez de los datos recopilados en la investigación científica.

**Figura 2.**

*Alpha de Cronbach - fórmula y datos*

$$\alpha = \frac{k}{k-1} \left[ 1 - \frac{\sum s^2}{S_T^2} \right]$$

Donde,  
 k = El número de ítems  
 $\sum s^2$  = Sumatoria de varianzas de los ítems.  
 $S_T^2$  = Varianza de la suma de los ítems.  
 $\alpha$  = Coeficiente de alfa de Cronbach

**Tabla 4.**

*Confiabilidad estadística del instrumento para medir la variable 1*

<b>Alfa de Cronbach</b>	
escala	0.895

La fiabilidad del instrumento es excepcionalmente alta, alcanzando un valor de 0.895 para la variable 1, lo que indica una consistencia interna notablemente sólida en las respuestas obtenidas mediante la Escala de Likert. Esta puntuación revela una confiabilidad sobresaliente en la medición de la variable en cuestión, lo que brinda una base sólida y confiable para la interpretación de los datos y las conclusiones derivadas del estudio.

**Tabla 5.**

*Confiabilidad estadística del instrumento para medir la variable 2*

<b>Alfa de Cronbach</b>	
escala	0.940

La confiabilidad del instrumento es excepcionalmente alta, registrando un coeficiente de 0.940 para la variable 2. Esta puntuación refleja una consistencia interna muy sólida en las respuestas recopiladas mediante la Escala de Likert. Tal nivel de fiabilidad subraya la solidez del instrumento para medir con precisión y consistencia la variable en cuestión, brindando una base robusta para el análisis de datos y la interpretación de resultados en el estudio.

### **3.8. Procesamiento y método de análisis de datos**

#### ***3.8.1. Técnica para el procesamiento de datos***

Para llevar a cabo una investigación efectiva, es esencial seguir una secuencia de pasos meticulosamente planificados. En primer lugar, se debe garantizar la preparación de todas las herramientas de investigación, incluyendo el cuestionario diseñado conforme al indicador establecido, y disponer del número adecuado de copias para distribuir entre los participantes.

Una vez listas las herramientas, se procede a solicitar permiso al oficial superior responsable de los cadetes para llevar a cabo la encuesta. Este paso es crucial para asegurar la conformidad con los protocolos y procedimientos establecidos por la institución.

Después de obtener el permiso, se procede a encuestar a los cadetes. Las boletas se distribuyen durante un tiempo de servicio programado, aproximadamente de 20 minutos, durante el cual los participantes completan las encuestas. Cualquier pregunta o preocupación que surja durante este proceso se aborda de manera oportuna para garantizar la integridad de los datos recopilados.

Una vez concluida la etapa de recolección de datos, se procede al procesamiento de la información adquirida utilizando software especializado como Excel. Este paso es crucial para organizar y analizar los datos de manera eficiente y precisa.

Posteriormente, se realiza un análisis estadístico de los datos recopilados para obtener datos tanto descriptivos como inferenciales. Se emplean herramientas como SPSS 27 y la prueba de Kolmogorov-Smirnov para evaluar la normalidad de las muestras recopiladas, lo que proporciona información valiosa sobre la distribución de los datos.

Con base en los resultados de las pruebas de normalidad, se determina la naturaleza cualitativa de las variables y se procede a realizar pruebas de estadística inferencial para evaluar la significancia de las relaciones y correlaciones identificadas en el estudio. Estas pruebas son

fundamentales para validar las hipótesis planteadas y obtener conclusiones significativas sobre el tema de investigación.

Así, seguir un proceso metodológico riguroso y bien planificado asegura la validez y confiabilidad de los resultados obtenidos en la investigación, proporcionando una base sólida para la toma de decisiones y la generación de conocimiento en el área de estudio correspondiente.

### **3.8.2. Método de análisis de datos**

El análisis descriptivo, como primer paso en la comprensión de los datos de la encuesta, se erige como una herramienta crucial. En este proceso, se empleará Excel para facilitar la tabulación de los datos, lo que implica la creación de una tabla de recurrencia. Esta tabla visualiza la frecuencia de ocurrencia de cada valor o categoría en los datos recopilados, brindando una representación clara y concisa de la distribución de los datos. Además, se utilizarán gráficos de barras para identificar patrones y tendencias, lo que simplifica la interpretación de los resultados al destacar visualmente las variaciones. El análisis descriptivo no solo ofrece una visión general del conjunto de datos, sino que también permite detectar cualquier anomalía o dato atípico que pueda influir en el análisis posterior.

El análisis inferencial desempeña un papel fundamental al profundizar en los componentes individuales del fenómeno bajo estudio y poner a prueba hipótesis específicas. En esta perspectiva, se utiliza el razonamiento inductivo para examinar el comportamiento de los indicadores de la realidad estudiada a través de las hipótesis planteadas. Para llevar a cabo este análisis, se emplea el coeficiente de correlación de Spearman ( $\rho$ ), una medida que evalúa la relación entre dos variables continuas aleatorias. Este método es especialmente útil cuando los datos no siguen una distribución normal, ofreciendo una alternativa robusta a la correlación de Pearson en tales casos.

El proceso de cálculo del coeficiente de correlación de Spearman implica la ordenación y sustitución de los datos según su orden relativo, considerando la presencia de datos idénticos. Para establecer la importancia de la correlación observada, se utiliza una prueba de permutación, la cual contrasta el  $\rho$  observado con un  $\rho$  esperado bajo la hipótesis nula de que la correlación es nula. Este enfoque avanzado supera a los métodos tradicionales en la mayoría de los casos, ofreciendo resultados más precisos y fiables. La prueba de permutación no solo

refuerza la validez de los resultados, sino que también proporciona una comprensión más profunda de la relación entre las variables estudiadas.

Por lo cual, tanto el análisis descriptivo como el inferencial constituyen pasos fundamentales en la investigación, ya que permiten explorar y comprender los datos de manera sistemática y rigurosa. Estos procesos proporcionan una base sólida para la interpretación de los resultados y la formulación de conclusiones significativas sobre el fenómeno estudiado. La integración de ambos análisis asegura que se aborden tanto los aspectos generales como los específicos del fenómeno, facilitando una visión comprensiva y detallada de los datos.

### **3.9. Aspectos éticos**

En una investigación realizada en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", los aspectos éticos adquieren una relevancia crucial debido al entorno militar y a la naturaleza de los datos que involucran la seguridad y formación de los cadetes. Uno de los principales aspectos éticos es la confidencialidad de la información proporcionada por los cadetes. En este tipo de instituciones, donde la disciplina y la jerarquía son fundamentales, es esencial garantizar que los datos recopilados sean manejados con estricta confidencialidad para proteger la privacidad de los participantes y evitar posibles repercusiones en su entorno académico o profesional. Los participantes deben estar seguros de que su información personal no será divulgada sin su consentimiento.

Otro aspecto ético relevante es el consentimiento informado. Los cadetes deben ser informados de manera clara y precisa sobre los objetivos, procedimientos y posibles implicaciones de la investigación antes de participar. A pesar de estar en un entorno militar, la participación debe ser voluntaria y sin coerción, respetando su autonomía en la toma de decisiones. Además, se debe asegurar que la investigación no cause daño psicológico o físico a los cadetes, garantizando que los procedimientos no interfieran con su formación o bienestar.

Finalmente, en el contexto de una escuela militar, también es importante manejar con cautela la información relacionada con la seguridad de las instalaciones. Cualquier dato que pueda comprometer la seguridad operativa o revelar vulnerabilidades de la institución debe ser tratado con la máxima precaución, respetando las normativas de seguridad nacional y evitando que los resultados sean mal utilizados.

## CAPÍTULO IV. Resultados

### 4.1. Análisis descriptivo

Resultados en base al Objetivo General: Estrategias de inteligencia militar y Seguridad en las instalaciones

**Tabla 6.**  
*Estrategias de inteligencia militar y Seguridad en las instalaciones*

		V2: Seguridad en las instalaciones			Total	
		Alto	Medio	Bajo		
V1: Estrategias de inteligencia militar	Alto	Recuento	257	0	0	257
		% del total	87.4%	0.0%	0.0%	87.4%
	Medio	Recuento	4	21	0	25
		% del total	1.4%	7.1%	0.0%	8.5%
	Bajo	Recuento	0	0	12	12
		% del total	0.0%	0.0%	4.1%	4.1%
Total		Recuento	261	21	12	294
		% del total	88.8%	7.1%	4.1%	100.0%

Nota: Tabla de contingencia realizado con la base de datos del Anexo 5  
Fuente: SPSS 27

**Interpretación de la Variable 1:** Mediante la Tabla 6 y en la Figura 3, en la categoría de "Alto" para las estrategias de inteligencia militar, se observa que 257 cadetes (87.4% del total) también consideran que la seguridad en las instalaciones es alta. Esto indica una fuerte correlación positiva entre la alta implementación de estrategias de inteligencia militar y la alta percepción de seguridad en las instalaciones. No se registraron cadetes que perciban un nivel medio o bajo de seguridad en esta categoría.

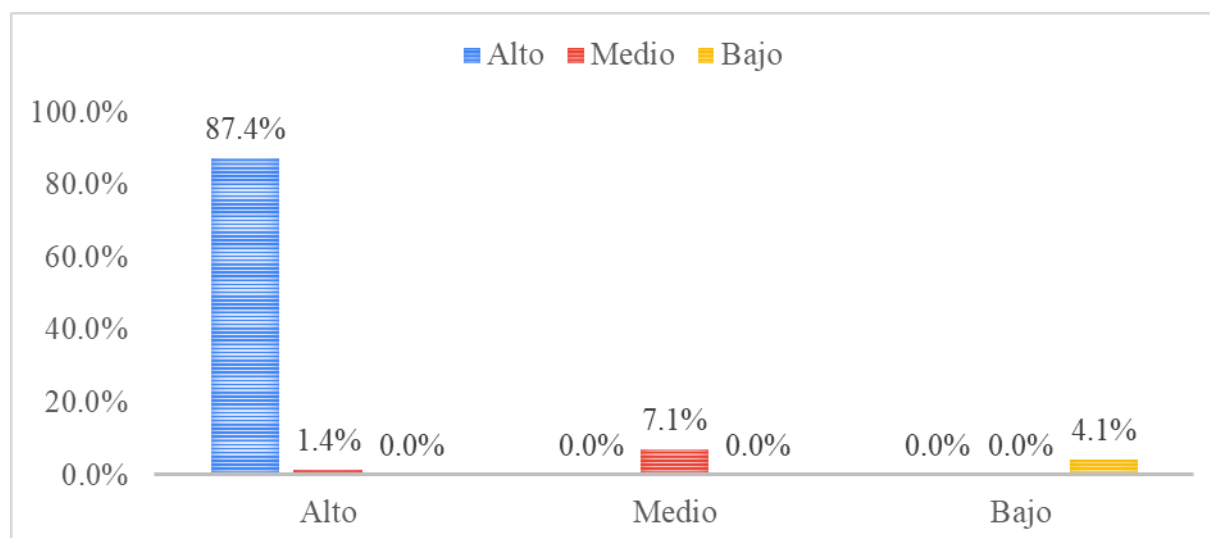
En la categoría de "Medio" para las estrategias de inteligencia militar, 21 cadetes (7.1% del total) evaluaron la seguridad en las instalaciones como media, mientras que solo 4 cadetes (1.4% del total) percibieron un nivel alto de seguridad en esta categoría. Esto sugiere que cuando las estrategias de inteligencia militar se perciben como medianas, la seguridad en las instalaciones tiende a ser valorada de manera menos favorable.

Finalmente, en la categoría de "Bajo" para las estrategias de inteligencia militar, 12 cadetes (4.1% del total) calificaron también la seguridad en las instalaciones como baja, lo que

refuerza la correlación entre una pobre implementación de estrategias de inteligencia militar y una baja percepción de seguridad.

**Figura 3.**

*Estrategias de inteligencia militar y Seguridad en las instalaciones*



Nota: Tabla de contingencia realizado con la base de datos del Anexo 5

Fuente: SPSS 27

Resultados en base al Objetivo Específico 1: Análisis de información y Seguridad en las instalaciones.

**Tabla 7.**

*Análisis de información y Seguridad en las instalaciones*

		V2: Seguridad en las instalaciones			Total	
		Alto	Medio	Bajo		
D1: Análisis de información	Alto	Recuento	229	0	0	229
		% del total	77.9%	0.0%	0.0%	77.9%
	Medio	Recuento	32	15	0	47
		% del total	10.9%	5.1%	0.0%	16.0%
	Bajo	Recuento	0	6	12	18
		% del total	0.0%	2.0%	4.1%	6.1%
Total	Recuento	261	21	12	294	
	% del total	88.8%	7.1%	4.1%	100.0%	

Nota: Tabla de contingencia realizado con la base de datos del Anexo 5

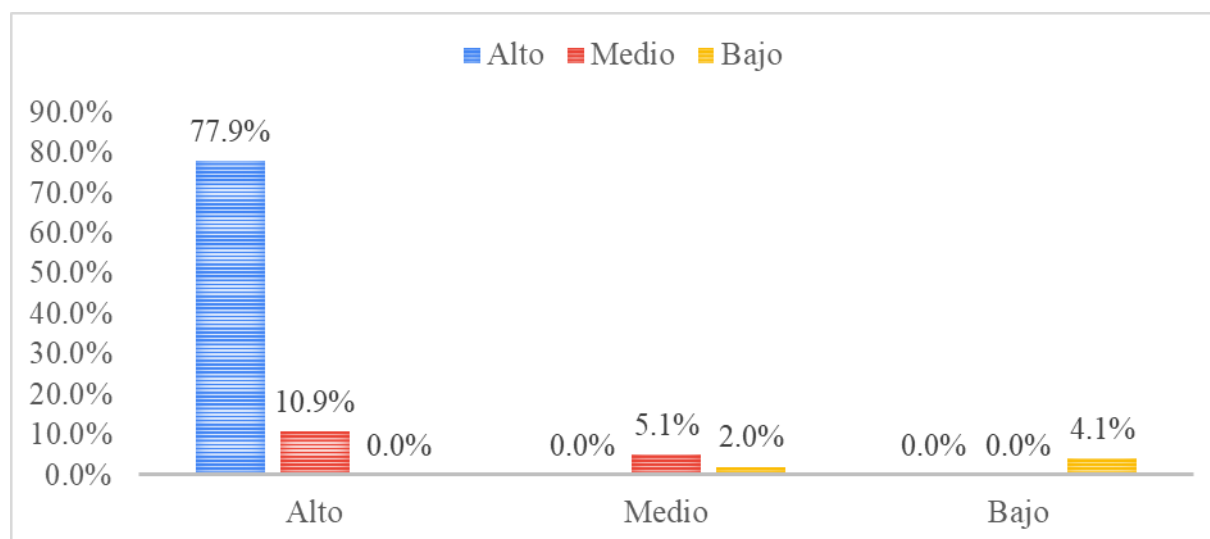
Fuente: SPSS 27

**Interpretación de la Dimensión 1, V1:** Mediante la Tabla 7 y en la Figura 4, en la categoría de "Alto" para el análisis de información, 229 cadetes (77.9% del total) consideran que la seguridad en las instalaciones también es alta. Esto sugiere que existe una fuerte correlación positiva entre un buen análisis de información y una alta percepción de seguridad en las instalaciones, ya que ningún cadete en esta categoría percibió niveles medios o bajos de seguridad.

En la categoría de "Medio" para el análisis de información, 32 cadetes (10.9% del total) valoraron la seguridad en las instalaciones como alta, mientras que 15 cadetes (5.1% del total) la calificaron como media. No se registraron cadetes que consideren la seguridad como baja en esta categoría, lo que indica que, aunque el análisis de información es percibido como medio, aún se mantiene una percepción mayoritariamente positiva de la seguridad en las instalaciones.

Por otro lado, en la categoría de "Bajo" para el análisis de información, 6 cadetes (2.0% del total) consideraron que la seguridad en las instalaciones es media, mientras que 12 cadetes (4.1% del total) la calificaron como baja. Esto refleja una relación directa entre una baja calidad en el análisis de información y una percepción negativa de la seguridad.

**Figura 4.**  
*Análisis de información y Seguridad en las instalaciones*



Nota: Tabla de contingencia realizado con la base de datos del Anexo 5

Fuente: SPSS 27

Resultados en base al Objetivo Específico 2: Operaciones de contrainteligencia y Seguridad en las instalaciones.

**Tabla 8.**

*Operaciones de contrainteligencia y Seguridad en las instalaciones*

		V2: Seguridad en las instalaciones			Total	
		Alto	Medio	Bajo		
D2: Operaciones de contrainteligencia	Alto	Recuento	241	0	0	241
		% del total	82.0%	0.0%	0.0%	82.0%
	Medio	Recuento	20	21	0	41
		% del total	6.8%	7.1%	0.0%	13.9%
	Bajo	Recuento	0	0	12	12
		% del total	0.0%	0.0%	4.1%	4.1%
Total		Recuento	261	21	12	294
		% del total	88.8%	7.1%	4.1%	100.0%

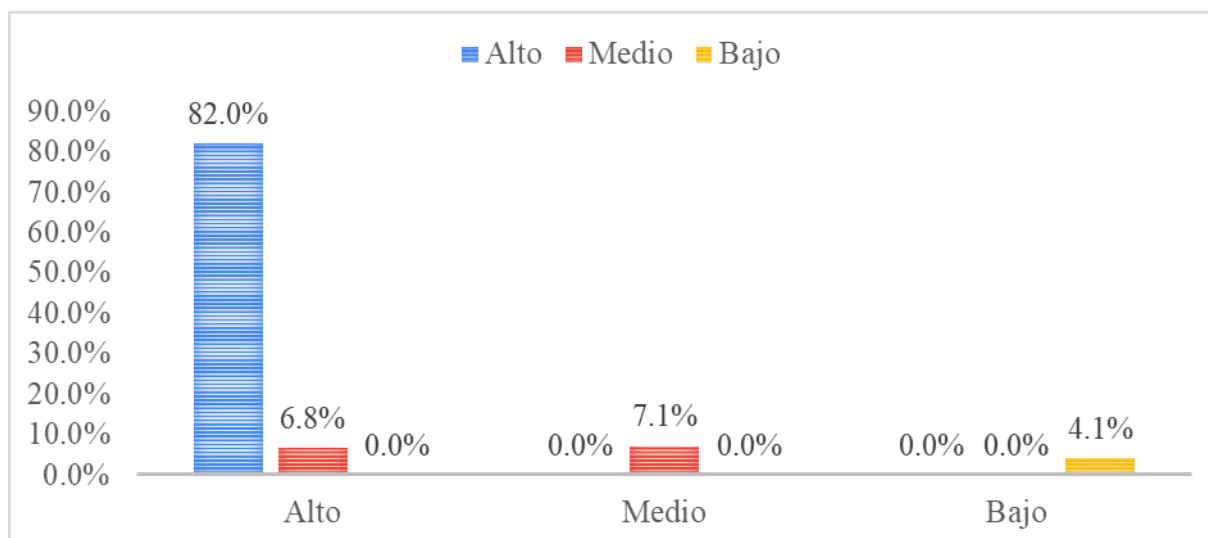
Nota: Tabla de contingencia realizado con la base de datos del Anexo 5  
Fuente: SPSS 27

**Interpretación de la Dimensión 2, V1:** Mediante la Tabla 8 y en la Figura 5, en la categoría de "Alto" para las operaciones de contrainteligencia, 241 cadetes (82.0% del total) también perciben un alto nivel de seguridad en las instalaciones. Esto indica una fuerte correlación positiva entre un buen manejo de las operaciones de contrainteligencia y una alta percepción de seguridad en las instalaciones, ya que no se reportaron cadetes que consideren la seguridad como media o baja en esta categoría.

En la categoría de "Medio" para las operaciones de contrainteligencia, 20 cadetes (6.8% del total) consideran que la seguridad en las instalaciones es alta, mientras que 21 cadetes (7.1% del total) la califican como media. Ningún cadete en esta categoría percibe la seguridad como baja, lo que sugiere que, aunque las operaciones de contrainteligencia sean percibidas como medianas, las percepciones de seguridad no bajan significativamente, aunque sí se inclinan hacia una evaluación menos favorable.

Finalmente, en la categoría de "Bajo" para las operaciones de contrainteligencia, 12 cadetes (4.1% del total) califican tanto las operaciones de contrainteligencia como la seguridad en las instalaciones como bajas. Esto sugiere una relación directa entre una pobre implementación de las operaciones de contrainteligencia y una baja percepción de la seguridad en las instalaciones.

**Figura 5.**  
*Operaciones de contrainteligencia y Seguridad en las instalaciones*



Nota: Tabla de contingencia realizado con la base de datos del Anexo 5  
Fuente: SPSS 27

Resultados en base al Objetivo Específico 3: Tecnología en inteligencia y Seguridad en las instalaciones.

**Tabla 9.**  
*Tecnología en inteligencia y Seguridad en las instalaciones*

		V2: Seguridad en las instalaciones			Total	
		Alto	Medio	Bajo		
D3: Tecnología en inteligencia	Alto	Recuento	247	9	0	256
		% del total	84.0%	3.1%	0.0%	87.1%
	Medio	Recuento	14	12	0	26
		% del total	4.8%	4.1%	0.0%	8.8%
	Bajo	Recuento	0	0	12	12
		% del total	0.0%	0.0%	4.1%	4.1%
Total		Recuento	261	21	12	294
		% del total	88.8%	7.1%	4.1%	100.0%

Nota: Tabla de contingencia realizado con la base de datos del Anexo 5  
Fuente: SPSS 27

**Interpretación de la Dimensión 3, V1:** Mediante la Tabla 9 y en la Figura 6, en la categoría de "Alto" para tecnología en inteligencia, 247 cadetes (84.0% del total) también perciben un alto nivel de seguridad en las instalaciones, lo que indica una fuerte correlación positiva entre el uso efectivo de la tecnología en inteligencia y la seguridad percibida. Solo 9

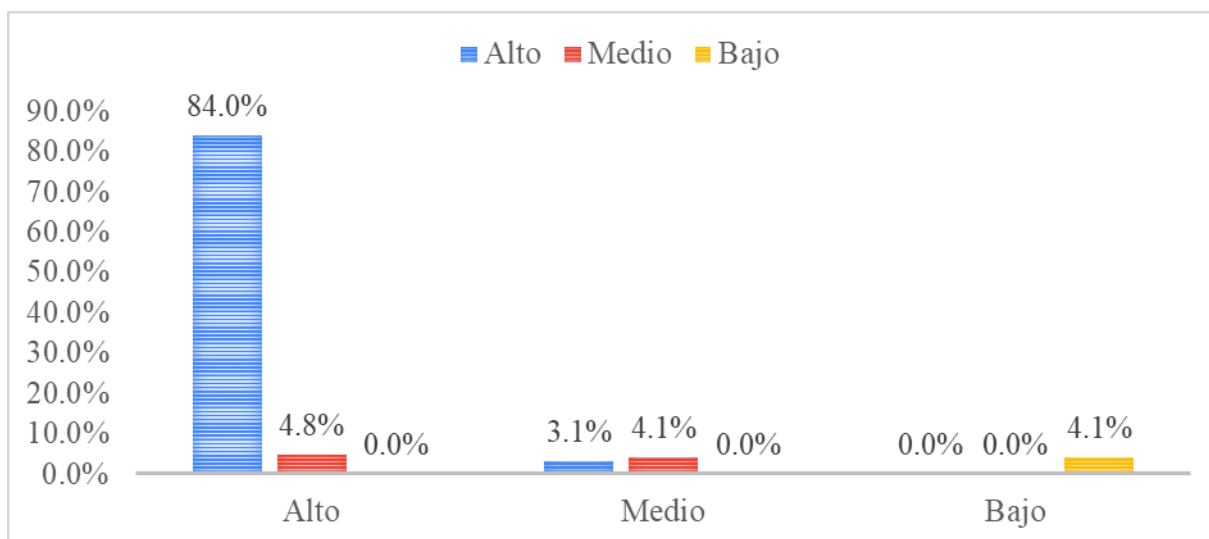
cadetes (3.1% del total) en esta categoría consideran la seguridad en las instalaciones como media, y ninguno la percibe como baja.

En la categoría de "Medio" para tecnología en inteligencia, 14 cadetes (4.8% del total) evalúan la seguridad en las instalaciones como alta, mientras que 12 cadetes (4.1% del total) la califican como media. Ningún cadete en esta categoría considera la seguridad como baja, lo que sugiere que, aunque la tecnología en inteligencia sea percibida como media, la seguridad sigue siendo valorada de manera razonablemente positiva, aunque con menor consistencia que cuando la tecnología es percibida como alta.

En la categoría de "Bajo" para tecnología en inteligencia, 12 cadetes (4.1% del total) consideran que tanto la tecnología en inteligencia como la seguridad en las instalaciones son bajas, lo que demuestra una clara relación entre la percepción de tecnología deficiente y una valoración negativa de la seguridad.

### Figura 6.

*Tecnología en inteligencia y Seguridad en las instalaciones*



Nota: Tabla de contingencia realizado con la base de datos del Anexo 5

Fuente: SPSS 27

## 4.2. Análisis inferencial

### 4.2.1. Prueba de normalidad

Para la prueba de normalidad siendo la muestra mayor a 50 de la muestra ( $n > 50$ ), se realiza la prueba de normalidad en SPSS 27 de Kolmogorov-Smirnov, que tiene como resultado lo siguiente:

**Tabla 10.**  
*Pruebas de Normalidad*

	Kolmogorov-Smirnov <sup>a</sup>		
	Estadístico	gl	Sig.
V1: Estrategias de inteligencia militar	0.031	294	0.012
D1: Análisis de información	0.104	294	0.008
D2: Operaciones de contrainteligencia	0.307	294	0.004
D3: Tecnología en inteligencia	0.481	294	0.070
V2: Seguridad en las instalaciones	0.680	294	0.079

a. Corrección de significación de Lilliefors

**Interpretación:** Los datos no presentan una distribución normal, según lo demuestra la prueba de “Kolmogorov-Smirnov, que se aplica a muestras mayores de 50. Esto se debe a que el valor de significancia es menor a 0.05, lo que indica que el P-valor es menor a 0.05. A partir de este resultado, se concluye que las variables no siguen una distribución normal, lo que justifica el uso del coeficiente de correlación de Spearman.

El coeficiente de correlación de Spearman,  $\rho$  (Rho), mide la correlación o asociación entre dos variables continuas. Para calcular este coeficiente, los datos se ordenan y se reemplazan por su posición correspondiente. El estadístico  $\rho$  se obtiene mediante una fórmula en la que "D" representa la diferencia entre los estadísticos de orden de las variables x e y, y "N" es el número de parejas de datos.

$$\rho = 1 - \frac{6 \sum D^2}{N(N^2 - 1)}$$

Al ordenar los datos, es necesario considerar la posibilidad de valores idénticos, aunque si estos son pocos, dicha situación puede ignorarse. Para determinar si un valor observado de  $\rho$  es significativamente diferente de cero, se utiliza una prueba de permutación.

Esta prueba permite calcular la probabilidad de que el valor observado sea mayor o igual que el valor esperado bajo la hipótesis nula. Esta aproximación moderna suele ser más eficaz que los métodos tradicionales, salvo en casos de conjuntos de datos extremadamente grandes o cuando es difícil crear algoritmos de permutación adecuados a la hipótesis nula, aunque estas dificultades rara vez se presentan con los recursos informáticos actuales.

**Tabla 11.**  
*Escala de interpretación para la correlación de Spearman*

<b>Correlación</b>	<b>Interpretación</b>
$r = -1,00$	“Correlación negativa perfecta”
-0,9 a -0,99	“Correlación negativa muy alta”
-0,7 a -0,89	“Correlación negativa 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”

Nota: Interpretación de las pruebas de hipótesis  
Fuente: Scielo

#### 4.2.2. Contrastación de la Hipótesis General (HG)

##### Paso 1.

HG<sub>a</sub> : Existe una relación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

HG<sub>0</sub> : No existe una relación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

##### Paso 2.

El nivel de significancia, representado como  $\alpha$ , es igual a 0.05, lo que equivale al 5%

##### Paso 3.

La prueba estadística y el nivel de relación de Spearman.

**Tabla 12.**

*Prueba de correlación de Spearman de la hipótesis general*

		V1: Estrategias de inteligencia militar	V2: Seguridad en las instalaciones
Rho de Spearman	V1: Estrategias de inteligencia militar	Coefficiente de correlación	1.000
		Sig. (bilateral)	0.894
		N	294
	V2: Seguridad en las instalaciones	Coefficiente de correlación	0.894
		Sig. (bilateral)	0.000
		N	294

Nota: Información realizada con la base de datos del Anexo 5

Fuente: SPSS 27

**Interpretación:** Como el coeficiente de Rh0 de Spearman es 0.894, existe una correlación positiva alta. Además, el nivel de significancia es 0.000 es menor que 0.05 (0.000 < 0.05).

**Paso 4.**

La regla de decisión es la siguiente:

- Rechazar  $H_0$  si sig ( $\rho$ -valor) es menor que 0.05.
- Aceptar  $H_0$  si sig ( $\rho$ -valor) es mayor que 0.05.

**Paso 5.**

Decisión estadística. Si  $0.000 > 0.05$ . Aceptar  $H_0$

**Paso 6.**

Conclusión: se rechaza la hipótesis general nula y se acepta la hipótesis general alterna, esto indica que si existe una relación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

### 4.2.3. Contrastación de la Hipótesis Específica 1 (HE1)

#### Paso 1.

HE1<sub>a</sub> : Existe una relación directa y significativa entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

HE1<sub>0</sub> : No existe una relación directa y significativa entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

#### Paso 2.

El nivel de significancia, representado como  $\alpha$ , es igual a 0.05, lo que equivale al 5%

#### Paso 3.

La prueba estadística y el nivel de relación de Spearman.

**Tabla 13.**

*Prueba de correlación de Spearman de la Hipótesis Específica 1*

		D1: Análisis de información	V2: Seguridad en las instalaciones
Rho de Spearman	D1: Análisis de información	Coefficiente de correlación	1.000
		Sig. (bilateral)	0.000
		N	294
	V2: Seguridad en las instalaciones	Coefficiente de correlación	0.943
		Sig. (bilateral)	0.000
		N	294

Nota: Información realizada con la base de datos del Anexo 5

Fuente: SPSS 27

**Interpretación:** Como el coeficiente de Rh0 de Spearman es 0.943, existe una correlación positiva muy alta. Además, el nivel de significancia es 0.000 es menor que 0.05 ( $0.000 < 0.05$ ).

**Paso 4.**

La regla de decisión es la siguiente:

- Rechazar  $H_0$  si sig ( $\rho$ -valor) es menor que 0.05.
- Aceptar  $H_0$  si sig ( $\rho$ -valor) es mayor que 0.05.

**Paso 5.**

Decisión estadística. Si  $0.000 > 0.05$ . Aceptar  $H_0$

**Paso 6.**

Conclusión: se rechaza la hipótesis Específica 1 nula y se acepta la hipótesis Específica 1 alterna, esto indica que si existe una relación directa y significativa entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

#### 4.2.4. Contrastación de la Hipótesis Específica 2 (HE2)

##### Paso 1.

HE2<sub>a</sub> : Existe una relación directa y significativa entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

HE2<sub>0</sub> : No existe una relación directa y significativa entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

##### Paso 2.

El nivel de significancia, representado como  $\alpha$ , es igual a 0.05, lo que equivale al 5%

##### Paso 3.

La prueba estadística y el nivel de relación de Spearman.

**Tabla 14.**

*Prueba de correlación de Spearman de la Hipótesis Específica 2*

		D2: Operaciones de contrainteligencia	V2: Seguridad en las instalaciones
Rho de Spearman	D2: Operaciones de contrainteligencia	Coefficiente de correlación	1.000
		Sig. (bilateral)	0.000
		N	294
	V2: Seguridad en las instalaciones	Coefficiente de correlación	0.901
		Sig. (bilateral)	0.000
		N	294

Nota: Información realizada con la base de datos del Anexo 5

Fuente: SPSS 27

**Interpretación:** Como el coeficiente de Rh0 de Spearman es 0.901, existe una correlación positiva muy alta. Además, el nivel de significancia es 0.000 es menor que 0.05 ( $0.000 < 0.05$ ).

**Paso 4.**

La regla de decisión es la siguiente:

- Rechazar  $H_0$  si sig ( $\rho$ -valor) es menor que 0.05.
- Aceptar  $H_0$  si sig ( $\rho$ -valor) es mayor que 0.05.

**Paso 5.**

Decisión estadística. Si  $0.000 > 0.05$ . Aceptar  $H_0$

**Paso 6.**

Conclusión: se rechaza la hipótesis Específica 2 nula y se acepta la hipótesis Específica 2 alterna, esto indica que si existe una relación directa y significativa entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

#### 4.2.5. Contrastación de la Hipótesis Específica 3 (HE3)

##### Paso 1.

HE3<sub>a</sub> : Existe una relación directa y significativa entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

HE3<sub>0</sub> : No existe una relación directa y significativa entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

##### Paso 2.

El nivel de significancia, representado como  $\alpha$ , es igual a 0.05, lo que equivale al 5%

##### Paso 3.

La prueba estadística y el nivel de relación de Spearman.

**Tabla 15.**

*Prueba de correlación de Spearman de la Hipótesis Específica 3*

		D3: Tecnología en inteligencia	V2: Seguridad en las instalaciones
Rho de Spearman	D3: Tecnología en inteligencia	Coefficiente de correlación	1.000
		Sig. (bilateral)	0.000
		N	294
	V2: Seguridad en las instalaciones	Coefficiente de correlación	0.832
		Sig. (bilateral)	0.000
		N	294

Nota: Información realizada con la base de datos del Anexo 5

Fuente: SPSS 27

**Interpretación:** Como el coeficiente de Rh0 de Spearman es 0.832, existe una correlación positiva alta. Además, el nivel de significancia es 0.000 es menor que 0.05 (0.000 < 0.05).

**Paso 4.**

La regla de decisión es la siguiente:

- Rechazar  $H_0$  si sig ( $\rho$ -valor) es menor que 0.05.
- Aceptar  $H_0$  si sig ( $\rho$ -valor) es mayor que 0.05.

**Paso 5.**

Decisión estadística. Si  $0.000 > 0.05$ . Aceptar  $H_0$

**Paso 6.**

Conclusión: se rechaza la hipótesis Específica 3 nula y se acepta la hipótesis Específica 3 alterna, esto indica que si existe una relación directa y significativa entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos CFB”, 2024.

## **CAPÍTULO V.**

### **Discusión de resultados**

En relación al Objetivo General, que busca analizar la relación entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos "CFB", los resultados obtenidos muestran una correlación positiva y significativa entre ambas variables. La tabla 6 indica que en la categoría "Alto" para las estrategias de inteligencia militar, 257 cadetes (87.4% del total) también perciben la seguridad en las instalaciones como alta, lo que demuestra que una adecuada implementación de estas estrategias se asocia directamente con una mayor percepción de seguridad en las instalaciones. No se registraron cadetes que percibieran niveles medios o bajos de seguridad cuando las estrategias de inteligencia militar eran evaluadas como altas, lo que refuerza la relevancia de estas estrategias en la protección de las instalaciones.

En los casos donde las estrategias fueron calificadas como medianas, 21 cadetes (7.1%) percibieron la seguridad en las instalaciones como media, mientras que solo 4 cadetes (1.4%) la consideraron alta. Este resultado sugiere que una percepción intermedia de las estrategias de inteligencia militar no asegura un alto nivel de seguridad en las instalaciones, siendo más probable que la seguridad sea vista como regular en estos casos. Por último, los 12 cadetes (4.1%) que calificaron las estrategias de inteligencia militar como bajas también valoraron la seguridad en las instalaciones de manera negativa, lo que confirma una correlación directa entre una implementación deficiente de las estrategias y una menor percepción de seguridad. El coeficiente de correlación de Spearman de 0.894 con una significancia de 0.000 refuerza esta relación, indicando una fuerte y significativa correlación entre ambas variables.

Los resultados de esta investigación encuentran apoyo en estudios previos que también destacan la importancia de las estrategias de inteligencia militar para la seguridad en instalaciones militares. En el estudio de Guerra y Terán (2020), quienes evidenciaron que una adecuada integración operativa en el Comando de Inteligencia Militar Conjunta (COIMC) mejora significativamente la toma de decisiones estratégicas. En su estudio, el 65.3% de los encuestados consideraron esencial reestructurar el COIMC para afrontar escenarios VICA, destacando la relevancia de una doctrina conjunta para optimizar la efectividad de las estrategias. Este enfoque refuerza la importancia de una implementación coherente y normativa

de las estrategias de inteligencia, como se observa en la correlación de 0.894 obtenida en este trabajo.

Por su parte, la investigación de Defaz y Polanco (2020) también resalta la necesidad de mejorar la organización y la capacitación en los sistemas de inteligencia militar. En su estudio, el 72.8% de los participantes identificaron carencias en la formación del personal, lo cual impacta negativamente en la producción de inteligencia. Esta conclusión subraya la relevancia de una adecuada capacitación y organización para garantizar una percepción alta de seguridad, alineándose con los resultados que demuestran que estrategias bien implementadas aumentan significativamente la seguridad percibida.

Finalmente, el estudio de Vela (2023) aporta evidencia complementaria al demostrar que la implementación de un modelo doctrinario integrado en la Compañía de Inteligencia N.º 113 mejoró la efectividad de las operaciones de inteligencia en un 85%. Esto resalta que una adecuada integración doctrinal y tecnológica puede transformar significativamente la seguridad de las instalaciones militares, apoyando los hallazgos actuales que vinculan directamente estrategias efectivas con una percepción de alta seguridad en la Escuela Militar.

En relación al Objetivo Específico 1, que busca determinar la relación entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, los resultados obtenidos a partir de la prueba de correlación de Spearman muestran una correlación positiva muy alta entre ambas variables, con un coeficiente de 0.943 y un nivel de significancia de 0.000. Esto indica que, a medida que se mejora el análisis de información, también aumenta significativamente la percepción de seguridad en las instalaciones. Dado que el valor de significancia es menor que 0.05 ( $0.000 < 0.05$ ), se rechaza la hipótesis nula y se acepta la hipótesis alterna, confirmando que el análisis de información influye directamente en la seguridad percibida dentro de las instalaciones. Esta alta correlación sugiere que la efectividad en la recopilación y procesamiento de datos clave, la validación de fuentes y la correcta identificación de amenazas se traduce en un entorno más seguro para los cadetes y el personal militar.

Estos hallazgos se alinean con la investigación de Conde y Hernández (2020), quienes destacaron que las capacidades tecnológicas insuficientes limitan la utilidad de la inteligencia en la toma de decisiones. Su correlación de 0.724 entre tecnología y efectividad subraya que el

análisis de información, respaldado por tecnología avanzada, es clave para mejorar la seguridad, lo cual se refleja en el coeficiente de 0.943 obtenido en este trabajo.

Asimismo, Mendoza (2020) analiza fallos en la contrainteligencia en el operativo de Culiacán, destacando que el 80% de las fuentes señalaron la falta de coordinación interagencial como un factor crítico. Este antecedente subraya la importancia de un análisis de información coordinado y preciso para evitar vulnerabilidades. Los resultados de este trabajo confirman que un análisis adecuado contribuye directamente a una percepción alta de seguridad en las instalaciones militares.

Por otro lado, la investigación de Herrera y Navarro (2021) también respalda la relación entre el análisis de información y la seguridad. En su estudio, el 85% de los encuestados afirmaron que una capacitación especializada en inteligencia contribuye al desarrollo de competencias específicas. Esto refuerza la idea de que un análisis de información efectivo, fundamentado en personal capacitado, influye positivamente en la percepción de seguridad.

En relación al Objetivo Específico 2, que busca analizar la relación entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos "CFB", los resultados de la prueba de correlación de Spearman revelan una correlación positiva muy alta entre ambas variables, con un coeficiente de 0.901 y un nivel de significancia de 0.000. Esto indica que la efectividad de las operaciones de contrainteligencia tiene un impacto directo en la percepción de seguridad en las instalaciones. Al ser el valor de significancia menor que 0.05 ( $0.000 < 0.05$ ), se rechaza la hipótesis nula y se acepta la hipótesis alterna, lo que confirma que existe una relación significativa entre ambas variables. Estos resultados demuestran que, cuando se implementan correctamente las medidas de contrainteligencia, como la protección de datos, la prevención de infiltraciones y el monitoreo interno, la seguridad en las instalaciones mejora considerablemente. Los datos sugieren que la seguridad en la Escuela Militar está estrechamente vinculada a la capacidad de prevenir amenazas internas y espionaje mediante la contrainteligencia.

Esta relación se encuentra respaldada por investigaciones previas. Un estudio realizado por Cárdenas y Ore (2020), quienes encontraron que el 96.78% de los cadetes percibían un desempeño deficiente en las medidas de contrainteligencia. Este antecedente subraya que una

adecuada implementación de contrainteligencia es fundamental para garantizar la seguridad de las instalaciones, validando los hallazgos actuales con un coeficiente de 0.901.

De manera similar, el estudio de Arenas (2021) evidencia una relación positiva alta ( $r = 0.87$ ) entre la capacitación en contrainteligencia y la efectividad operativa. Enfatiza que el fortalecimiento de estas medidas mejora significativamente la seguridad en escenarios complejos. Este antecedente respalda los resultados, confirmando que la efectividad de las operaciones de contrainteligencia impacta directamente en la percepción de seguridad.

Por último, Vargas (2021) resalta la importancia de herramientas tecnológicas modernas en las operaciones de inteligencia y contrainteligencia. Su correlación de 0.65 entre tecnología y gestión de inteligencia refuerza que estas herramientas son esenciales para la seguridad. Los resultados actuales, que demuestran que la efectividad de la contrainteligencia mejora la percepción de seguridad, están alineados con estas conclusiones.

En relación al Objetivo Específico 3, que busca determinar la relación entre el uso de tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos "CFB", los resultados obtenidos mediante la prueba de correlación de Spearman muestran una correlación positiva alta, con un coeficiente de 0.832 y un nivel de significancia de 0.000. Esto significa que, a medida que se mejora la implementación de tecnologías avanzadas en inteligencia, también aumenta la percepción de seguridad en las instalaciones. Dado que el valor de significancia es menor que 0.05 ( $0.000 < 0.05$ ), se rechaza la hipótesis nula y se acepta la hipótesis alterna, confirmando que el uso adecuado de tecnologías en las operaciones de inteligencia tiene un impacto significativo en la seguridad de las instalaciones. Este resultado indica que herramientas como los drones, el monitoreo satelital, los sistemas criptográficos y la inteligencia artificial contribuyen de manera importante a fortalecer las capacidades de vigilancia y protección en la Escuela Militar.

Este hallazgo coincide con la investigación de Noboa (2020), quien evidenció que la insuficiencia tecnológica limita significativamente las capacidades del COIMC. Su recomendación de integrar tecnología avanzada concuerda con los resultados actuales, donde el uso de herramientas como drones y sistemas criptográficos fortalece la seguridad percibida.

De igual forma, el estudio de Mendoza (2020) destaca que el ciberespacio se utiliza como un teatro de operaciones crítico. Esto resalta la importancia de incorporar tecnologías avanzadas para enfrentar desafíos contemporáneos. La correlación de 0.832 obtenida en este trabajo valida que la tecnología es un factor crucial para mejorar la seguridad en instalaciones militares.

Finalmente, Herrera y Navarro (2021) subrayan que el fortalecimiento del ciclo de inteligencia mediante tecnologías modernas mejora significativamente el desempeño profesional. Sus hallazgos apoyan los resultados actuales, demostrando que el uso adecuado de tecnologías avanzadas tiene un impacto directo en la seguridad percibida dentro de las instalaciones militares.

## Conclusiones

En relación al Objetivo General, se concluye que existe una correlación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos "CFB". La alta percepción de seguridad entre los cadetes está directamente vinculada con una implementación efectiva de las estrategias de inteligencia, lo que refuerza la importancia de una planificación adecuada, el uso de tecnología avanzada y la formación continua. Este resultado confirma que las estrategias de inteligencia no solo mejoran la operatividad, sino que también son fundamentales para garantizar la protección y seguridad de las infraestructuras militares críticas.

En relación al Objetivo Específico 1, se concluye que el análisis de información es un factor clave que influye significativamente en la seguridad de las instalaciones militares. La correcta recopilación, procesamiento y validación de los datos, junto con la identificación de amenazas, se traduce en una mayor percepción de seguridad por parte de los cadetes. Este resultado subraya la relevancia de un análisis de información preciso y constante, lo que permite anticipar riesgos y fortalecer las medidas de protección. La relación positiva entre ambas variables refuerza la necesidad de un sistema eficiente de gestión de la inteligencia en entornos militares.

En relación al Objetivo Específico 2, se concluye que las operaciones de contrainteligencia desempeñan un papel fundamental en la seguridad de las instalaciones. Las medidas implementadas para prevenir infiltraciones, sabotajes y espionaje interno tienen un impacto directo en la percepción de seguridad. La alta correlación entre estas operaciones y la seguridad indica que, al fortalecer la contrainteligencia, se minimizan significativamente las vulnerabilidades internas que podrían comprometer la protección de las infraestructuras militares. Estos hallazgos destacan la importancia de mantener una vigilancia constante y de invertir en formación para optimizar las operaciones de contrainteligencia.

En relación al Objetivo Específico 3, se concluye que el uso de tecnología en inteligencia tiene una influencia significativa en la seguridad de las instalaciones. Las herramientas tecnológicas, como el monitoreo satelital, los drones y los sistemas criptográficos, mejoran la capacidad de respuesta y vigilancia en tiempo real, lo que eleva la percepción de seguridad entre los cadetes. Este resultado demuestra que la modernización tecnológica en las operaciones de inteligencia es esencial para enfrentar amenazas emergentes. Además, se destaca la necesidad de actualizar continuamente estas tecnologías para maximizar su efectividad en la protección de infraestructuras críticas en un entorno militar cada vez más complejo.

## Recomendaciones

En relación a la conclusión 1, se recomienda continuar fortaleciendo las estrategias de inteligencia militar mediante la inversión en formación continua para el personal, así como la actualización constante de las tecnologías utilizadas. Además, es crucial que se fomente la cooperación interinstitucional para compartir información relevante y mejorar las capacidades operativas. Las estrategias de inteligencia deben estar en constante revisión para adaptarse a las nuevas amenazas que puedan surgir, garantizando así la seguridad de las instalaciones. Se debe priorizar la creación de protocolos que integren las áreas de inteligencia, seguridad cibernética y operaciones de campo, optimizando la toma de decisiones.

En relación a la conclusión 2, se recomienda optimizar los sistemas de análisis de información mediante la implementación de herramientas tecnológicas avanzadas que permitan un procesamiento más rápido y preciso de los datos. Además, es esencial que se desarrollen programas de formación continua para los cadetes y el personal, enfocándose en mejorar las habilidades para la validación de fuentes y la identificación de amenazas. La creación de equipos multidisciplinarios que incluyan expertos en tecnología, ciberseguridad y operaciones de campo podría potenciar la efectividad del análisis de información, garantizando una mayor seguridad en las instalaciones.

En relación a la conclusión 3, se recomienda implementar programas específicos de capacitación en contrainteligencia para todo el personal involucrado en la protección de las instalaciones. Asimismo, es necesario fortalecer los protocolos de supervisión interna para detectar posibles amenazas internas, mejorando los mecanismos de prevención de espionaje y filtraciones de información. También sería conveniente la adquisición de tecnologías avanzadas de monitoreo y la realización de simulacros regulares de operaciones de contrainteligencia, lo que permitirá identificar vulnerabilidades en el sistema y corregirlas antes de que puedan comprometer la seguridad de las infraestructuras militares.

En relación a la conclusión 4, se recomienda realizar inversiones sostenidas en la actualización de las tecnologías de inteligencia, como sistemas de monitoreo satelital, drones y software criptográfico. Es esencial que estas herramientas sean renovadas y actualizadas periódicamente para adaptarse a las nuevas amenazas tecnológicas. También se debe implementar un plan de capacitación continua para el personal en el uso de estas tecnologías, asegurando que los cadetes y oficiales estén preparados para aprovechar al máximo las herramientas disponibles. La creación de un centro de innovación tecnológica en inteligencia permitiría evaluar y mejorar continuamente la efectividad de estas tecnologías.

## Referencias

- Arenas, J. C. (2021). *Uso de la inteligencia militar para apoyar las operaciones en respaldo al orden público*. [Tesis de Licenciatura], Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".  
<https://repositorio.escuelamilitar.edu.pe/server/api/core/bitstreams/74f436dd-56d7-49fa-93dc-a0c095bfc4c4/content>
- Barrio, J. A. (2022). *La Ciberinteligencia, Instrumento de la Ciberseguridad*.  
<https://globalt4e.com/la-ciberinteligencia-instrumento-de-la-ciberseguridad/>
- Blog de Contabilidad. (02 de junio de 2023). *¿Qué es la seguridad de las instalaciones?*  
<https://www.clinicavdamerica.es/que-es-la-seguridad-de-las-instalaciones/>
- Cabrera, L. (2017). Entre el cambio y la inercia histórica: el contexto actual de la inteligencia militar en Suramérica. *URVIO - Revista Latinoamericana de Estudios de Seguridad*(21), 8-21. <https://doi.org/10.17141/urvio.21.2017.3082>
- Cárdenas, L. J., & Ore, E. (2019). *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 de Licenciatura, Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"].  
<https://repositorio.escuelamilitar.edu.pe/items/2b3633f1-791e-4c33-8d0e-86237f63f322>
- Castro, L. G., & Zuñiga, J. M. (2024). Desafíos de la inteligencia militar en la lucha contra el terrorismo en el Valle de los Ríos Apurímac, Ene y Mantaro (VRAEM). *Revista Seguridad y Poder Terrestre*, 3(3), 185-214. <https://doi.org/10.56221/spt.v3i3.67>
- Coll, F. (06 de octubre de 2020). *Baremo*. <https://economipedia.com/definiciones/baremo.html>
- Conde, E. F., & Hernández, H. A. (2020). *Prospectiva del empleo de la inteligencia para la toma de decisiones en las operaciones militares del COIMC*. [Tesis de Maestría], Universidad de las Fuerzas Armadas ESPE - Ecuador.  
<https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/461b311d-1a41-4715-8e12-13039d39e99b/content>

- Corte Suprema de Justicia de la República. (2001). *Filosofía militar y operaciones de inteligencia en la lucha antiterrorista en Perú*. Ministerio de Defensa: [https://historico.pj.gob.pe/CorteSuprema/spe/documentos/P2C6\\_DINTE\\_SIE.pdf](https://historico.pj.gob.pe/CorteSuprema/spe/documentos/P2C6_DINTE_SIE.pdf)
- Costa, G. (19 de octubre de 2010). *Desafíos de seguridad en Perú*. <https://www.americasquarterly.org/fulltextarticle/security-challenges-in-peru/>
- Defaz, W. M., & Polanco, E. F. (2020). *Propuesta de la organización del Comando de Inteligencia Militar Conjunto en la producción de inteligencia*. [Tesis de Maestría], Universidad de las Fuerzas Armadas ESPE - Ecuador. <https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/83410e77-2cce-4ad9-9d3e-0dce5214569d/content>
- El Regional de Piura. (25 de setiembre de 2023). *Sullana: alcalde Marlem Mogollón demanda estrategia e inteligencia operativa durante el estado de emergencia*. Diario El Regional de Piura: <https://www.elregionalpiura.com.pe/index.php/locales/146-sullana/63779-sullana-alcalde-marlem-mogollon-demanda-estrategia-e-inteligencia-operativa-durante-el-estado-de-emergencia>
- Enciclopedia Humanidades. (23 de enero de 2023). *Doctrina de Seguridad Nacional*. <https://humanidades.com/doctrina-de-seguridad-nacional/>
- Gómez, M. (09 de julio de 2024). *Protocolos de Seguridad Militar: Una Guía Concisa*. <https://dudasytextos.com/militar/seguridad/protocolos-de-seguridad-en-el-campo-militar/>
- Guerra, S. G., & Terán, H. M. (2020). *Prospectiva de la Inteligencia Militar Conjunta frente a la toma de decisiones en el nivel estratégico*. [Tesis de Maestría], Universidad de las Fuerzas Armadas - Ecuador. <https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/5c9d282f-81c1-46a1-b31e-2e6cb3c5acf0/content>
- Hernández, R., & Mendoza, C. P. (2018). *Metodología de la investigación: las rutas: cuantitativa, cualitativa y mixta*. Mc Graw Hill- educación. <http://repositorio.uasb.edu.bo:8080/bitstream/54000/1292/1/Hern%c3%a1ndez-%20Metodolog%c3%ada%20de%20la%20investigaci%c3%b3n.pdf>
- Herrera, P. Y., & Navarro, J. E. (2021). *Capacitación especializada de inteligencia y el desempeño profesional de los futuros oficiales del arma de inteligencia de la Escuela*

- Militar de Chorrillos “Coronel Francisco Bolognesi”, 2021.* [Tesis de Licenciatura], EMCH “CFB”.  
<https://repositorio.escuelamilitar.edu.pe/server/api/core/bitstreams/3902909b-547d-4613-9ebf-ad84baa987a7/content>
- INSST. (2019). *Aspectos comunes a todas las instalaciones.* Instituto Nacional de Seguridad y Salud en el Trabajo (INSST):  
<https://www.insst.es/documents/94886/679600/00%20Aspectos%20comunes%20a%20todas%20las%20instalaciones%202019.pdf/71032b40-b28e-4407-984a-7959e291c5ef>
- Jasso, L. C. (2017). Seguridad nacional, inteligencia militar y acceso a la información en México. *URVIO, Revista Latinoamericana de Estudios de Seguridad*(21), 140-156.  
<https://doi.org/10.17141/urvio.21.2017.2931>
- Machuca, F. (06 de junio de 2022). *8 técnicas de recolección de datos: descubre un mundo más allá de la encuesta.* <https://www.crehana.com/blog/transformacion-digital/tecnicas-recoleccion-de-datos/>
- Mendoza, P. (2020). Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán. *Revista FLACSO, México.*(26), 37-56.  
<https://doi.org/10.17141/urvio.26.2020.4225>
- Militars. (2024). *La inteligencia militar y su relación con la ciberseguridad.*  
<https://militars.com/blog/la-inteligencia-militar-y-su-relacion-con-la-ciberseguridad>
- MINDEF. (1999). *ME 38-10 Seguridad Militar.* Ministerio de Defensa - Ejército del Perú.  
<https://idoc.pub/documents/me-38-10-seguridad-militar-1430621wk24j>
- Noboa, M. F. (2020). *Inteligencia militar: poder, conocimiento e ideología en las prácticas semióticas-discursivas en las relaciones Colombia-Ecuador. El caso de la Operación Militar Fénix.* [Tesis de Doctorado], Facultad Latinoamericana de Ciencias Sociales (FLACSO) - Ecuador. <https://repositorio.flacsoandes.edu.ec/handle/10469/16594>
- Noticias Militares. (18 de agosto de 2024). *Inteligencia Militar: Desafíos y Oportunidades en la Era de la IA.* <https://www.noticiasmilitares.es/articulo/tecnologia/inteligencia-militar-desafios-oportunidades-era-ia/20240818011204001082.html>
- Ñaupas, H., Valdivia, M. R., Palacios, J. J., & Romero, H. E. (2018). *Metodología de la investigación, Cuantitativa - Cualitativa y Redacción de la Tesis* (5a. ed.). Bogotá:

Ediciones de la U.  
[https://doi.org/http://www.biblioteca.cij.gob.mx/Archivos/Materiales\\_de\\_consulta/Drugas\\_de\\_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf](https://doi.org/http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drugas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf)

Sampó, C., & Alda, S. (2024). *La transformación de las FFAA y su impacto en la seguridad nacional*. Escuela Superior de Guerra del Ejército del Perú: <https://ceeep.mil.pe/wp-content/uploads/2019/04/La-transformaci%C3%B3n-de-las-FFAA.pdf>

Seguridad en Todo. (2020). *Control de Acceso*. <https://seguridaden.com/control-de-acceso/>

Toledo, R. (2022). *¿Cómo mantener la seguridad de las instalaciones de una empresa?* <https://www.grupocibernos.com/blog/como-mantener-la-seguridad-de-las-instalaciones-de-una-empresa>

UNIR. (08 de julio de 2021). *¿En qué consiste la ciberinteligencia? Aplicaciones y ejemplos*. La Universidad en Internet: <https://www.unir.net/ingenieria/revista/ciberinteligencia/>

Uriarte, J. M. (27 de julio de 2022). *Método Deductivo*. Método hipotético-deductivo: <https://humanidades.com/metodo-deductivo/>

Vargas, E. L. (2021). *Nuevos retos y Estrategias para la actividad de Inteligencia ante las amenazas actuales” en la Escuela Militar De Chorrillos “Coronel Francisco Bolognesi”*. [Tesis de Licenciatura], Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.  
<https://repositorio.escolamilitar.edu.pe/server/api/core/bitstreams/887ac49a-b958-4909-8e5e-2daf9d41ea15/content>

Vela, R. P. (2023). *Inteligencia militar y operaciones de garantía de ley y orden en la Compañía de Inteligencia N.º 113 'Tte. Francisco Mina Bellido', ubicada en el departamento de Tacna*. [Tesis de Licenciatura], Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".  
<https://repositorio.escolamilitar.edu.pe/server/api/core/bitstreams/403dfce3-eeb1-4eff-8d14-62c76089bb14/content>

## **Anexos**

## Anexo 1. Matriz de consistencia

Título: ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CFB”, 2024.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
<p><b>Problema General</b> ¿Cuál es la relación que existe entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?</p> <p><b>Problema Especifico 1</b> ¿Cuál es la relación que existe entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?</p> <p><b>Problema Especifico 2</b> ¿Cuál es la relación que existe entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?</p> <p><b>Problema Especifico 3</b> ¿Cuál es la relación que existe entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024?</p>	<p><b>Objetivo General</b> Determinar la relación que existe entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Objetivo Especifico 1</b> Determinar la relación que existe entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Objetivo Especifico 2</b> Determinar la relación que existe entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Objetivo Especifico 3</b> Determinar la relación que existe entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p>	<p><b>Hipótesis General</b> Existe relación directa y significativa entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Hipótesis Especifico 1</b> Existe relación directa y significativa entre el análisis de información y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Hipótesis Especifico 2</b> Existe relación directa y significativa entre las operaciones de contrainteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p> <p><b>Hipótesis Especifico 3</b> Existe relación directa y significativa entre la tecnología en inteligencia y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.</p>	<p><b>Variable 1</b> Estrategias de inteligencia militar</p> <p><b>Variable 2</b> Seguridad en las instalaciones</p>	<p>Análisis de información</p> <p>Operaciones de contrainteligencia</p> <p>Tecnología en inteligencia</p> <p>Control de accesos</p> <p>Vigilancia electrónica</p> <p>Respuesta a emergencias</p>	<ul style="list-style-type: none"> <li>Recopilación de datos</li> <li>Validación de fuentes</li> <li>Análisis predictivo</li> <li>Identificación de amenazas</li> </ul> <ul style="list-style-type: none"> <li>Protección de datos</li> <li>Control de infiltraciones</li> <li>Supervisión interna</li> <li>Prevención de espionaje</li> </ul> <ul style="list-style-type: none"> <li>Uso de drones</li> <li>Monitoreo satelital</li> <li>Sistemas criptográficos</li> <li>Inteligencia artificial</li> </ul> <ul style="list-style-type: none"> <li>Verificación de identidad</li> <li>Sistemas biométricos</li> <li>Monitoreo perimetral</li> <li>Supervisión de visitantes</li> </ul> <ul style="list-style-type: none"> <li>Cámaras de seguridad</li> <li>Detección de movimiento</li> <li>Monitoreo remoto</li> <li>Alarmas de intrusión</li> </ul> <ul style="list-style-type: none"> <li>Protocolos de evacuación</li> <li>Personal de seguridad</li> <li>Planes de contingencia</li> <li>Simulacros regulares</li> </ul>	<p><b>Tipo de investigación</b> Básica</p> <p><b>Nivel de investigación</b> Descriptivo-correlacional</p> <p><b>Diseño de investigación</b> No experimental transversal</p> <p><b>Enfoque de investigación</b> Cuantitativo</p> <p><b>Técnica</b> Encuesta</p> <p><b>Instrumentos</b> Cuestionario</p> <p><b>Población</b> 1247 cadetes</p> <p><b>Muestra</b> 294 cadetes</p> <p><b>Métodos de Análisis de Datos</b> Estadística Según la prueba de normalidad</p>

## Anexo 2. Instrumento de recolección de datos

### ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CFB”, 2024

**OBJETIVO:** Determinar la relación que existe entre las estrategias de inteligencia militar y la seguridad en las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2024.

**INSTRUCCIONES:** Marque con una X la alternativa que usted considera válida de acuerdo al ítem en los casilleros siguientes:

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

ÍTEM	Variable 1: Estrategias de inteligencia militar	VALORACIÓN				
Nro.	Dimensión 1: Análisis de información	1	2	3	4	5
1	¿Se recopilan los datos necesarios para la toma de decisiones estratégicas?					
2	¿Participa activamente en la recolección de datos en operaciones de inteligencia militar?					
3	¿Se validan las fuentes de información antes de tomar decisiones?					
4	¿Se verifica la autenticidad de las fuentes de datos obtenidos?					
5	¿Se emplean técnicas de análisis predictivo para anticipar amenazas?					
6	¿Los informes de análisis predictivo influyen en las decisiones operativas?					
7	¿Se identifican nuevas amenazas en las operaciones de inteligencia?					
8	¿Participa en la identificación de posibles amenazas para la seguridad?					
Nro.	Dimensión 2: Operaciones de contrainteligencia	1	2	3	4	5
9	¿Se implementan medidas efectivas para proteger los datos sensibles en su unidad?					
10	¿Considera que los datos sensibles están suficientemente protegidos frente a posibles filtraciones?					
11	¿Se realiza un control efectivo para prevenir infiltraciones en las operaciones de inteligencia?					
12	¿Es monitoreado el personal para evitar infiltraciones?					
13	¿Se supervisan adecuadamente las actividades internas para evitar amenazas internas?					
14	¿Participa en la supervisión interna para detectar comportamientos sospechosos?					
15	¿Se implementan acciones preventivas para evitar el espionaje en las operaciones de inteligencia?					
16	¿Recibe formación adecuada sobre cómo prevenir el espionaje?					

<b>Nro.</b>	<b>Dimensión 3: Tecnología en inteligencia</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
17	¿Se utilizan drones en las operaciones de inteligencia militar de manera regular?					
18	¿Reciben los cadetes la formación necesaria en el uso de drones para recolección de información?					
19	¿Se emplea el monitoreo satelital para apoyar las operaciones de inteligencia?					
20	¿Se utilizan imágenes satelitales para respaldar la toma de decisiones en las operaciones?					
21	¿Se emplean sistemas criptográficos para proteger las comunicaciones en su unidad?					
22	¿Se capacita al personal de manera adecuada en el uso de sistemas criptográficos?					
23	¿Se aplican herramientas de inteligencia artificial para mejorar las operaciones de inteligencia?					
24	¿Los cadetes participan activamente en el uso de inteligencia artificial en las operaciones?					
<b>ÍTEM</b>	<b>Variable 2: Seguridad en las instalaciones</b>	<b>VALORACIÓN</b>				
<b>Nro.</b>	<b>Dimensión 1: Control de accesos</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
25	¿Se realiza una verificación exhaustiva de identidad en los puntos de acceso de la escuela?					
26	¿Se detectan intentos de acceso no autorizado a las instalaciones?					
27	¿Se utilizan sistemas biométricos de manera eficiente para controlar el acceso a áreas restringidas?					
28	¿Ha experimentado fallos en los sistemas biométricos durante el control de acceso?					
29	¿Se realiza un monitoreo constante y eficaz del perímetro de la escuela?					
30	¿Se identifican amenazas potenciales a través del monitoreo perimetral?					
31	¿Se supervisa adecuadamente a los visitantes durante su estancia en la escuela?					
32	¿Se registran correctamente los datos de los visitantes?					
<b>Nro.</b>	<b>Dimensión 2: Vigilancia electrónica</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
33	¿Las cámaras de seguridad cubren de manera efectiva todas las áreas críticas de la escuela?					
34	¿Se revisan con frecuencia las grabaciones de las cámaras de seguridad tras un incidente?					
35	¿Los sistemas de detección de movimiento se activan adecuadamente en áreas sensibles?					
36	¿Los sistemas de detección de movimiento han contribuido a prevenir intrusiones?					
37	¿El monitoreo remoto de las instalaciones se realiza de manera eficiente?					
38	¿El monitoreo remoto ha permitido una respuesta rápida y efectiva ante amenazas?					

39	¿Las alarmas de intrusión se activan oportunamente ante intentos no autorizados de acceso?					
40	¿El sistema de alarmas de intrusión responde de manera efectiva cuando se detectan intrusiones?					
<b>Nro.</b>	<b>Dimensión 3: Respuesta a emergencias</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
41	¿Los protocolos de evacuación se activan de manera eficiente en los simulacros de emergencia?					
42	¿Los cadetes participan de manera activa en la revisión y actualización de los protocolos de evacuación?					
43	¿El personal de seguridad recibe formación adecuada para responder a emergencias?					
44	¿El personal de seguridad ha demostrado ser eficiente en situaciones de emergencia reales?					
45	¿Los planos de contingencia de la escuela se revisan y actualizan regularmente?					
46	¿Participas en la planificación o simulación de planos de contingencia?					
47	¿Se realizan simulacros de emergencia con la frecuencia necesaria en la escuela?					
48	¿Se evalúan de manera efectiva los resultados de los simulacros para mejorar los protocolos de emergencia?					

**Anexo 3. Autorización para la recolección de datos****ESCUELA MILITAR DE CHORRILLOS****CORONEL FRANCISCO BOLOGNESI****SUB DIRECCIÓN ACADÉMICA**

El Coronel Jefe del Dpto. Académico de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, deja:

**AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS**

Que el cadete **Joe Escobedo Hurtado**, están autorizados para aplicar la encuesta a la muestra de la tesis que se indica para obtener el título profesional de Licenciado en Ciencias Militares con mención en administración:

**ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CFB”, 2024.**

Se otorga el presente documento a efectos de ser empleado como anexo de su investigación.

Chorrillos, 19 de octubre del 2024



36	5 3 3 4 3 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 3 2 3	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 2 3 3 4 3 4
37	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
38	3 3 4 4 4 4 4 4	4 5 4 3 4 3 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 3	4 3 4 4 4 4 4 4	4 4 4 4 4 4 4 4
39	5 5 4 3 5 5 5 4	3 5 4 4 5 5 5 5	4 4 4 4 5 5 4 4	4 4 4 4 5 4 4 4	5 5 5 5 4 4 4 4	5 5 4 4 4 3 5 5
40	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 4
41	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3
42	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
43	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
44	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
45	2 2 2 3 2 2 4 2	2 4 4 4 2 4 4 4	4 4 3 4 3 3 4 3	3 2 3 4 3 4 4 4	2 4 4 4 4 4 3 4	3 3 4 3 2 3 2 2
46	4 4 5 4 4 4 5 4	4 5 4 5 4 4 4 5	5 4 5 5 5 4 4 5	5 4 5 4 4 4 4 5	4 4 4 5 5 4 5 5	5 4 4 5 5 4 4 4
47	4 4 4 4 4 4 4 4	5 4 4 4 4 4 3 4	4 5 3 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 3 4 4 4 5 3 4	4 4 4 4 4 4 4 4
48	4 4 4 4 3 4 4 2	3 4 4 4 4 4 4 4	3 4 2 4 4 4 4 4	4 4 4 3 4 4 4 4	4 4 4 4 3 4 2 4	4 4 4 4 4 4 3 4
49	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
50	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
51	4 5 3 5 4 4 4 5	4 4 4 5 4 5 5 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 5	4 5 5 4 4 5 3 4	4 5 4 4 3 5 4 4
52	4 1 1 1 1 1 3 1	2 4 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
53	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
54	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
55	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
56	3 2 4 3 4 4 4 4	4 4 4 4 3 4 4 4	4 4 3 4 4 4 4 4	4 4 4 4 4 4 4 4	3 4 4 4 4 4 3 4	4 4 4 4 3 4 4 4
57	4 3 3 3 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4	4 4 4 4 3 3 4 4
58	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
59	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
60	4 4 3 4 4 5 5 5	5 5 4 4 4 5 5 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 5 4 4 4 4 4	4 4 4 4 3 4 4 5
61	3 4 4 4 4 4 4 4	3 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
62	5 4 5 5 5 5 4 5	4 5 5 4 5 4 5 4	5 4 5 4 4 5 5 4	5 4 5 4 5 4 5 4	5 4 5 4 5 4 5 4	4 5 5 4 5 5 5 5
63	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
64	5 5 1 1 5 5 5 1	1 5 1 1 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 1 1	5 5 5 5 5 5 5 5	5 5 5 5 1 1 5 5
65	5 5 5 5 5 4 4 4	5 4 4 4 4 4 4 5	4 4 5 4 4 5 4 4	5 4 4 4 4 5 4 4	4 4 4 5 4 4 5 4	4 5 4 4 5 5 5 4
66	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
67	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
68	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
69	5 5 5 5 5 5 5 5	4 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
70	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
71	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
72	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
73	4 4 4 4 3 4 4 4	4 4 3 3 3 4 4 4	4 4 4 4 4 4 3 4	4 4 4 4 4 4 3 3	3 4 4 4 4 4 4 4	4 4 3 4 4 4 3 4
74	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
75	2 2 3 1 2 1 2 1	1 2 3 3 2 2 1 3	1 1 3 3 1 2 2 2	1 2 2 2 3 2 3 3	2 2 1 3 1 1 3 3	1 2 2 2 3 1 2 1
76	4 5 4 4 5 4 5 4	4 4 4 4 4 4 5 4	4 4 4 5 4 4 4 4	4 4 4 4 4 5 4 4	4 4 5 4 4 4 4 5	4 4 4 4 4 4 5 4
77	4 3 3 3 3 4 3 4	3 3 4 4 4 3 3 4	4 4 3 4 3 4 4 4	4 4 4 3 3 2 4 4	4 3 3 4 4 4 3 4	3 4 4 4 3 3 3 4
78	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4	3 4 4 4 4 4 4 4
79	5 5 5 5 4 4 4 4	5 4 3 4 5 5 5 4	3 4 5 4 4 5 4 4	4 4 4 4 5 5 3 4	5 5 5 4 3 4 5 4	4 5 4 4 5 5 4 4
80	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 4 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 4 5	5 5 5 5 5 5 5 5



126	2 2 3 1 2 1 2 1	1 2 3 3 2 2 1 3	1 1 3 3 1 2 2 2	1 2 2 2 3 2 3 3	2 2 1 3 1 1 3 3	1 2 2 2 3 1 2 1
127	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 3 4 4 4 4 4	5 5 5 5 5 5 4 4	4 4 4 4 4 4 4 3	4 4 4 4 4 4 4 4
128	5 5 4 5 5 5 5 5	5 5 4 5 5 5 4 4	5 5 5 4 5 4 5 5	5 4 5 5 4 4 4 5	5 5 4 4 5 5 5 4	5 4 5 5 4 5 5 5
129	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3
130	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
131	5 3 3 3 3 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 3 4 4 4	4 3 4 4 4 4 4 4	4 4 4 4 4 4 4 4	3 4 4 4 3 3 3 3
132	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
133	4 4 4 4 3 4 4 4	4 4 3 3 3 4 4 4	4 4 4 4 4 4 3 4	4 4 4 4 4 4 3 3	3 4 4 4 4 4 4 4	4 4 3 4 4 4 3 4
134	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
135	2 2 2 3 2 2 4 2	2 4 4 4 2 4 4 4	4 4 3 4 3 3 4 3	3 2 3 4 3 4 4 4	2 4 4 4 4 4 3 4	3 3 4 3 2 3 2 2
136	5 3 3 4 3 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 3 2 3	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 2 3 3 4 3 4
137	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4	3 4 4 4 4 4 4 4
138	4 4 4 4 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4	4 4 4 4 4 4 4 4
139	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
140	4 4 4 4 3 4 4 4	4 4 3 3 3 4 4 4	4 4 4 4 4 4 3 4	4 4 4 4 4 4 3 3	3 4 4 4 4 4 4 4	4 4 3 4 4 4 3 4
141	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
142	4 4 4 4 3 4 4 4	4 4 3 3 3 4 4 4	4 4 4 4 4 4 3 4	4 4 4 4 4 4 3 3	3 4 4 4 4 4 4 4	4 4 3 4 4 4 3 4
143	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 4
144	4 5 3 5 4 4 4 5	4 4 4 5 4 5 5 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 4	4 5 5 4 4 5 3 4	4 5 4 4 3 5 4 4
145	5 5 3 4 4 5 5 5	5 4 5 4 5 5 5 5	5 5 4 4 5 4 5 5	5 4 5 5 4 4 5 4	5 5 5 5 5 5 4 4	5 4 5 5 3 4 4 5
146	4 4 3 4 4 3 3 3	3 3 4 4 4 4 4 4	3 3 3 3 4 4 4 4	3 3 5 3 5 5 4 4	4 4 4 4 3 3 3 3	4 4 4 4 3 4 4 3
147	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
148	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
149	2 2 3 1 2 1 2 1	1 2 3 3 2 2 1 3	1 1 3 3 1 2 2 2	1 2 2 2 3 2 3 3	2 2 1 3 1 1 3 3	1 2 2 2 3 1 2 1
150	4 4 4 4 4 4 4 4	4 4 4 4 5 4 4 4	4 5 5 5 4 4 4 4	5 5 4 4 4 4 4 4	5 4 4 4 4 5 5 5	4 4 4 4 4 4 4 4
151	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
152	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4	3 4 4 4 4 4 4 4
153	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
154	3 4 4 4 4 4 4 4	3 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
155	4 4 3 4 4 3 3 3	3 3 4 4 4 4 4 4	3 3 3 3 4 4 4 4	3 3 5 3 5 5 4 4	4 4 4 4 3 3 3 3	4 4 4 4 3 4 4 3
156	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
157	5 5 3 4 4 5 5 5	5 4 5 4 5 5 5 5	5 5 4 4 5 4 5 5	5 4 5 5 4 4 5 4	5 5 5 5 5 5 4 4	5 4 5 5 3 4 4 5
158	5 5 5 5 5 4 4 4	5 4 4 4 4 4 4 5	4 4 5 4 4 5 4 4	5 4 4 4 4 5 4 4	4 4 4 5 4 4 5 4	4 5 4 4 5 5 5 4
159	4 1 1 1 1 1 3 1	2 4 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
160	5 5 5 4 5 4 5 5	4 4 4 4 5 4 4 4	4 4 4 3 4 4 4 4	4 5 5 5 4 5 4 4	5 4 4 4 4 4 4 3	4 4 4 4 5 4 5 4
161	4 4 4 4 4 4 4 4	4 4 4 4 3 5 5 4	4 4 4 4 5 4 4 4	4 4 5 5 4 4 4 4	3 5 5 4 4 4 4 4	5 4 4 4 4 4 4 4
162	3 3 4 4 4 4 4 4	4 5 4 3 4 3 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 3	4 3 4 4 4 4 4 4	4 4 4 4 4 4 4 4
163	5 5 3 4 4 5 5 5	5 4 5 4 5 5 5 5	5 5 4 4 5 4 5 5	5 4 5 5 4 4 5 4	5 5 5 5 5 5 4 4	5 4 5 5 3 4 4 5
164	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
165	5 4 4 5 5 5 5 5	5 4 5 4 5 4 4 4	5 4 4 5 5 5 5 5	5 5 5 5 5 5 5 4	5 4 4 4 5 4 4 5	5 5 5 5 4 5 5 5
166	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 4
167	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
168	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3	3 3 3 3 3 3 3 3
169	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
170	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 4

171	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
172	3 3 4 4 4 4 4 4	4 4 4 3 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 5 4 3	4 3 4 4 4 4 4 4
173	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
174	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
175	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
176	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
177	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
178	4 4 5 4 4 4 5 4	4 5 4 5 4 4 4 5	5 4 5 5 5 4 4 5	5 4 5 4 4 4 4 5	4 4 4 5 5 4 5 5
179	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
180	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
181	4 5 4 4 5 4 5 4	4 4 4 4 4 4 5 4	4 4 4 5 4 4 4 4	4 4 4 4 4 5 4 4	4 4 5 4 4 4 4 5
182	4 4 4 4 4 4 4 4	4 5 5 5 5 5 5 5	4 5 5 4 3 4 4 5	5 3 5 4 4 5 5 5	5 5 5 5 4 5 5 4
183	4 4 4 5 4 4 5 4	4 4 4 4 4 5 4 5	4 4 5 5 4 4 4 4	4 4 4 5 4 5 4 4	4 5 4 5 4 4 5 5
184	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
185	3 4 4 4 4 4 4 4	3 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
186	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 3 4 4 4 4 4	5 5 5 5 5 5 4 4	4 4 4 4 4 4 3 4
187	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
188	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
189	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
190	4 4 5 4 4 4 5 4	4 5 4 5 4 4 4 5	5 4 5 5 5 4 4 5	4 4 5 4 4 4 4 5	4 4 4 5 5 4 5 5
191	5 5 5 5 5 5 5 5	4 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
192	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
193	4 4 4 4 4 4 4 4	5 4 4 4 4 4 3 4	4 5 3 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 3 4 4 5 3 4
194	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
195	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
196	5 5 4 3 5 5 5 4	3 5 4 4 5 5 5 5	4 4 4 4 5 5 4 4	4 4 4 4 4 5 4 4	5 5 5 5 4 4 4 4
197	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
198	4 5 3 5 4 4 4 5	4 4 4 5 4 5 5 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 5	4 5 5 4 4 5 3 4
199	4 3 3 3 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4
200	5 5 5 5 5 5 5 5	5 5 4 4 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 4 4	5 5 5 5 5 5 5 5
201	5 5 5 5 5 5 5 5	5 5 4 4 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 4 4	5 5 5 5 5 5 5 5
202	4 4 4 4 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4
203	4 5 3 5 4 4 4 5	4 4 4 5 4 5 4 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 5	4 5 5 4 4 5 3 4
204	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
205	5 5 5 5 4 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
206	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
207	4 5 5 4 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 5 5 5	5 5 5 5 5 5 5 5
208	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 3 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 3 4
209	4 4 4 5 3 4 4 4	4 4 4 5 4 4 5 5	4 4 5 4 5 5 5 4	4 5 4 5 5 4 4 5	4 4 5 5 4 4 5 4
210	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4
211	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
212	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
213	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
214	5 3 3 4 3 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 3 2 3	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
215	4 5 5 4 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 5 5 5	5 5 5 5 5 5 5 5

216	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
217	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
218	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
219	5 5 5 5 4 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
220	4 3 3 3 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4
221	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
222	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
223	2 2 3 1 2 1 2 1	1 2 3 3 2 2 1 3	1 1 3 3 1 2 2 2	1 2 2 2 3 2 3 3	2 2 1 3 1 1 3 3
224	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
225	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
226	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
227	4 4 4 5 4 4 5 4	4 4 4 4 4 5 4 5	4 4 5 5 4 4 4 4	4 4 4 5 4 5 4 4	4 5 4 5 4 4 5 5
228	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
229	5 5 5 5 5 4 5 5	5 5 4 5 5 5 5 5	5 4 5 5 5 4 4 5	5 5 5 5 5 5 4 5	5 5 5 5 5 4 5 5
230	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
231	4 4 4 3 5 5 5 5	4 4 3 4 4 4 4 4	4 4 4 4 4 5 5 5	5 4 4 4 4 4 3 4	4 4 4 4 4 4 4 4
232	4 5 3 5 4 4 4 5	4 4 4 5 4 5 5 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 5	4 5 5 4 4 5 3 4
233	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
234	2 2 2 3 2 2 4 2	2 4 4 4 2 4 4 4	4 4 3 4 3 3 4 3	3 2 3 4 3 4 4 4	2 4 4 4 4 4 3 4
235	5 5 5 5 5 4 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
236	4 5 5 5 4 4 4 4	4 5 5 5 4 5 5 4	4 5 4 5 5 4 5 4	4 4 5 4 4 4 5 5	4 5 5 4 4 5 4 5
237	4 3 3 3 4 4 4 4	4 4 4 4 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 3 4 4 4 4 4 4
238	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
239	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
240	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4
241	3 3 4 4 4 4 4 4	4 4 4 3 4 3 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 5 4 3	4 3 4 4 4 4 4 4
242	4 4 3 4 4 5 5 5	5 5 4 4 4 4 5 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 5 4 4 4 4 4
243	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
244	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
245	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
246	5 5 4 5 5 5 5 5	5 5 4 5 5 5 4 4	5 5 5 4 5 4 5 5	5 4 5 5 4 4 4 5	5 5 4 4 5 5 5 4
247	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
248	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
249	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
250	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4
251	5 3 3 4 3 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 3 2 3	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
252	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4
253	4 4 4 3 5 5 5 5	4 4 3 4 4 4 4 4	4 4 4 4 4 5 5 5	5 4 4 4 4 4 3 4	4 4 4 4 4 4 4 4
254	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
255	5 5 5 4 5 4 5 5	4 4 4 4 5 4 4 4	4 4 4 3 4 4 4 4	4 5 5 5 4 5 4 4	5 4 4 4 4 4 4 3
256	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
257	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
258	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4
259	5 4 5 5 5 5 4 5	4 5 5 4 5 4 5 4	5 4 5 4 4 5 5 4	5 4 5 4 5 4 5 4	5 4 5 4 5 4 5 4
260	4 4 4 4 3 4 4 2	3 4 4 4 4 4 4 4	3 4 2 4 4 4 4 4	4 4 4 3 4 4 4 4	4 4 4 4 3 4 2 4

261	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
262	5 5 5 5 5 4 5 5	5 5 4 5 5 5 5 5	5 4 5 5 5 4 4 5	5 5 5 5 5 5 4 5	5 5 5 5 5 4 5 5	5 4 4 5 5 5 5 4
263	5 5 3 4 4 5 5 5	5 4 5 4 5 5 5 5	5 5 4 4 5 4 5 5	5 4 5 5 4 4 5 4	5 5 5 5 5 5 4 4	5 4 5 5 3 4 4 5
264	2 2 2 3 2 2 4 2	2 4 4 4 2 4 4 4	4 4 3 4 3 3 4 3	3 2 3 4 3 4 4 4	2 4 4 4 4 4 3 4	3 3 4 3 2 3 2 2
265	4 5 4 4 5 4 5 4	4 4 4 4 4 4 5 4	4 4 4 5 4 4 4 4	4 4 4 4 4 5 4 4	4 4 5 4 4 4 4 5	4 4 4 4 4 4 5 4
266	4 5 3 5 4 4 4 5	4 4 4 5 4 5 5 4	4 5 3 4 4 5 4 4	5 5 4 3 4 4 4 5	4 5 5 4 4 5 3 4	4 5 4 4 3 5 4 4
267	5 5 5 5 5 5 5 5	5 5 4 4 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 4 4	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
268	4 4 4 4 4 4 4 4	4 4 4 4 3 5 5 4	4 4 4 4 5 4 4 4	4 4 5 5 4 4 4 4	3 5 5 4 4 4 4 4	5 4 4 4 4 4 4 4
269	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
270	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
271	4 4 4 4 4 4 4 3	4 4 3 4 4 4 4 3	4 4 5 4 3 4 4 4	3 4 4 4 4 4 3 4	4 4 4 3 4 4 5 4	3 4 4 4 4 4 4 4
272	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
273	4 1 1 1 1 1 3 1	2 4 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
274	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
275	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
276	4 5 5 5 4 4 4 4	4 5 5 5 4 5 5 4	4 5 4 5 5 4 5 4	4 4 5 4 4 4 5 5	4 5 5 4 4 5 4 5	5 4 5 4 5 5 4 4
277	4 4 3 4 4 3 3 3	3 3 4 4 4 4 4 4	3 3 3 3 4 4 4 4	3 3 5 3 5 5 4 4	4 4 4 4 3 3 3 3	4 4 4 4 3 4 4 3
278	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
279	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
280	3 2 2 3 4 3 3 4	4 4 3 2 2 4 2 3	3 4 4 4 4 4 4 4	4 4 4 2 3 4 3 2	2 4 2 3 3 4 4 4	4 4 4 4 2 3 4 3
281	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
282	5 5 3 4 4 5 5 5	5 4 5 4 5 5 5 5	5 5 4 4 5 4 5 5	5 4 5 5 4 4 5 4	5 5 5 5 5 5 4 4	5 4 5 5 3 4 4 5
283	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
284	5 5 5 4 5 4 5 5	4 4 4 4 5 4 4 4	4 4 4 3 4 4 4 4	4 5 5 5 4 5 4 4	5 4 4 4 4 4 4 3	4 4 4 4 5 4 5 4
285	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
286	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
287	2 2 2 3 2 2 4 2	2 4 4 4 2 4 4 4	4 4 3 4 3 3 4 3	3 2 3 4 3 4 4 4	2 4 4 4 4 4 3 4	3 3 4 3 2 3 2 2
288	3 4 4 4 4 4 4 4	3 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
289	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
290	5 4 5 5 5 5 4 5	4 5 5 4 5 4 5 4	5 4 5 4 4 5 5 4	5 4 5 4 5 4 5 4	5 4 5 4 5 4 5 4	4 5 5 4 5 5 5 5
291	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5	5 5 5 5 5 5 5 5
292	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4
293	4 5 5 5 4 4 4 4	4 5 5 5 4 5 5 4	4 5 4 5 5 4 5 4	4 4 5 4 4 4 5 5	4 5 5 4 4 5 4 5	5 4 5 4 5 5 4 4
294	4 4 4 4 4 4 4 4	4 4 4 5 4 4 4 4	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 5	4 4 4 4 4 4 4 4	4 4 4 4 4 4 4 4

### Anexo 5. Base de datos (origen de resultados)

	V1: Estrategias de inteligencia militar	D1: Análisis de información	D2: Operaciones de contrainteligencia	D3: Tecnología en inteligencia	V2: Seguridad en las instalaciones	D1: Control de accesos	D2: Vigilancia electrónica	D3: Respuesta a emergencias
<b>n</b>	<b>V1</b>	<b>V1-D1</b>	<b>V1-D2</b>	<b>V1-D3</b>	<b>V2</b>	<b>V2-D1</b>	<b>V2-D2</b>	<b>V2-D3</b>
1	120	40	40	40	120	40	40	40
2	110	38	37	35	106	34	35	37
3	72	32	21	19	91	28	34	29
4	120	40	40	40	120	40	40	40
5	71	28	24	19	78	23	27	28
6	120	40	40	40	120	40	40	40
7	120	40	40	40	109	37	37	35
8	100	34	32	34	99	32	35	32
9	120	40	40	40	120	40	40	40
10	98	30	37	31	81	29	26	26
11	96	31	32	33	83	23	30	30
12	78	26	28	24	65	27	20	18
13	72	25	24	23	73	25	24	24
14	67	29	24	14	67	28	19	20
15	79	25	29	25	81	28	27	26
16	70	32	18	20	76	22	25	29
17	114	37	38	39	108	38	34	36
18	102	31	34	37	105	28	37	40
19	83	30	27	26	63	21	23	19
20	97	33	33	31	98	32	32	34
21	109	36	37	36	113	37	38	38
22	116	36	40	40	120	40	40	40
23	114	37	37	40	120	40	40	40
24	108	38	35	35	111	38	36	37
25	113	38	38	37	114	40	40	34
26	57	21	18	18	48	12	19	17
27	94	36	28	30	97	33	31	33
28	120	40	40	40	116	40	40	36
29	119	40	40	39	116	40	40	36
30	99	32	35	32	102	33	34	35
31	95	31	34	30	104	35	36	33
32	111	37	38	36	115	38	38	39
33	120	40	40	40	115	36	40	39
34	113	40	38	35	114	38	38	38
35	120	40	40	40	112	40	35	37
36	115	37	40	38	119	40	39	40
37	111	38	35	38	109	35	34	40
38	115	38	39	38	114	39	38	37
39	120	40	40	40	120	40	40	40
40	104	35	32	37	94	33	31	30

41	96	32	32	32	96	32	32	32
42	120	40	40	40	120	40	40	40
43	111	37	36	38	115	40	38	37
44	73	11	26	36	107	34	36	37
45	120	40	40	40	120	40	40	40
46	113	37	38	38	111	38	36	37
47	113	38	38	37	112	39	36	37
48	107	36	35	36	109	36	36	37
49	109	36	38	35	113	37	39	37
50	120	40	40	40	120	40	40	40
51	120	40	40	40	119	40	39	40
52	120	40	40	40	117	40	38	39
53	120	40	40	40	120	40	40	40
54	96	32	32	32	96	32	32	32
55	120	40	40	40	120	40	40	40
56	110	38	36	36	107	35	36	36
57	82	29	28	25	92	29	32	31
58	83	28	28	27	82	23	29	30
59	108	36	36	36	102	29	36	37
60	116	40	36	40	120	40	40	40
61	97	31	31	35	96	31	35	30
62	120	40	40	40	120	40	40	40
63	111	36	38	37	111	36	38	37
64	72	24	24	24	92	28	32	32
65	69	26	15	28	76	29	25	22
66	120	40	40	40	115	38	38	39
67	120	40	40	40	120	40	40	40
68	110	34	38	38	110	35	38	37
69	83	26	35	22	94	24	37	33
70	93	31	31	31	86	30	27	29
71	120	40	40	40	112	40	35	37
72	120	40	40	40	112	40	35	37
73	116	36	40	40	120	40	40	40
74	111	36	38	37	111	36	38	37
75	83	26	35	22	94	24	37	33
76	78	26	28	24	65	27	20	18
77	120	40	40	40	120	40	40	40
78	120	40	40	40	120	40	40	40
79	110	38	37	35	106	34	35	37
80	97	31	31	35	96	31	35	30
81	120	40	40	40	120	40	40	40
82	97	31	31	35	96	31	35	30
83	83	28	28	27	82	23	29	30
84	83	28	28	27	82	23	29	30
85	95	31	34	30	104	35	36	33
86	57	21	18	18	48	12	19	17
87	113	38	38	37	114	40	40	34

<b>88</b>	96	32	32	32	96	32	32	32
<b>89</b>	116	36	40	40	120	40	40	40
<b>90</b>	108	36	36	36	102	29	36	37
<b>91</b>	97	33	33	31	98	32	32	34
<b>92</b>	100	34	32	34	99	32	35	32
<b>93</b>	107	36	35	36	109	36	36	37
<b>94</b>	120	40	40	40	116	40	40	36
<b>95</b>	120	40	40	40	115	38	38	39
<b>96</b>	110	38	37	35	106	34	35	37
<b>97</b>	119	40	40	39	116	40	40	36
<b>98</b>	98	30	37	31	81	29	26	26
<b>99</b>	120	40	40	40	120	40	40	40
<b>100</b>	108	38	35	35	111	38	36	37
<b>101</b>	73	11	26	36	107	34	36	37
<b>102</b>	120	40	40	40	109	37	37	35
<b>103</b>	97	31	31	35	96	31	35	30
<b>104</b>	110	38	37	35	106	34	35	37
<b>105</b>	120	40	40	40	116	40	40	36
<b>106</b>	93	31	31	31	86	30	27	29
<b>107</b>	98	30	37	31	81	29	26	26
<b>108</b>	110	34	38	38	110	35	38	37
<b>109</b>	96	32	32	32	96	32	32	32
<b>110</b>	120	40	40	40	117	40	38	39
<b>111</b>	115	37	40	38	119	40	39	40
<b>112</b>	97	33	33	31	98	32	32	34
<b>113</b>	96	32	32	32	96	32	32	32
<b>114</b>	102	31	34	37	105	28	37	40
<b>115</b>	120	40	40	40	120	40	40	40
<b>116</b>	120	40	40	40	119	40	39	40
<b>117</b>	97	31	31	35	96	31	35	30
<b>118</b>	97	31	31	35	96	31	35	30
<b>119</b>	107	36	35	36	109	36	36	37
<b>120</b>	113	38	38	37	112	39	36	37
<b>121</b>	97	31	31	35	96	31	35	30
<b>122</b>	120	40	40	40	120	40	40	40
<b>123</b>	120	40	40	40	115	36	40	39
<b>124</b>	83	30	27	26	63	21	23	19
<b>125</b>	97	31	31	35	96	31	35	30
<b>126</b>	116	36	40	40	120	40	40	40
<b>127</b>	109	36	37	36	113	37	38	38
<b>128</b>	113	38	38	37	114	40	40	34
<b>129</b>	119	40	40	39	116	40	40	36
<b>130</b>	120	40	40	40	120	40	40	40
<b>131</b>	120	40	40	40	117	40	38	39
<b>132</b>	120	40	40	40	120	40	40	40
<b>133</b>	111	37	38	36	115	38	38	39
<b>134</b>	120	40	40	40	116	40	40	36

<b>135</b>	120	40	40	40	120	40	40	40
<b>136</b>	83	26	35	22	94	24	37	33
<b>137</b>	120	40	40	40	120	40	40	40
<b>138</b>	95	31	34	30	104	35	36	33
<b>139</b>	83	30	27	26	63	21	23	19
<b>140</b>	120	40	40	40	120	40	40	40
<b>141</b>	71	28	24	19	78	23	27	28
<b>142</b>	111	36	38	37	111	36	38	37
<b>143</b>	93	31	31	31	86	30	27	29
<b>144</b>	120	40	40	40	120	40	40	40
<b>145</b>	107	36	35	36	109	36	36	37
<b>146</b>	67	29	24	14	67	28	19	20
<b>147</b>	110	38	37	35	106	34	35	37
<b>148</b>	95	31	34	30	104	35	36	33
<b>149</b>	72	32	21	19	91	28	34	29
<b>150</b>	116	40	36	40	120	40	40	40
<b>151</b>	113	38	38	37	114	40	40	34
<b>152</b>	120	40	40	40	120	40	40	40
<b>153</b>	93	31	31	31	86	30	27	29
<b>154</b>	120	40	40	40	120	40	40	40
<b>155</b>	111	37	36	38	115	40	38	37
<b>156</b>	120	40	40	40	120	40	40	40
<b>157</b>	120	40	40	40	120	40	40	40
<b>158</b>	82	29	28	25	92	29	32	31
<b>159</b>	67	29	24	14	67	28	19	20
<b>160</b>	120	40	40	40	115	36	40	39
<b>161</b>	120	40	40	40	120	40	40	40
<b>162</b>	120	40	40	40	115	38	38	39
<b>163</b>	113	37	38	38	111	38	36	37
<b>164</b>	113	38	38	37	112	39	36	37
<b>165</b>	96	32	32	32	96	32	32	32
<b>166</b>	120	40	40	40	112	40	35	37
<b>167</b>	120	40	40	40	120	40	40	40
<b>168</b>	116	36	40	40	120	40	40	40
<b>169</b>	83	30	27	26	63	21	23	19
<b>170</b>	113	38	38	37	112	39	36	37
<b>171</b>	72	24	24	24	92	28	32	32
<b>172</b>	110	34	38	38	110	35	38	37
<b>173</b>	69	26	15	28	76	29	25	22
<b>174</b>	73	11	26	36	107	34	36	37
<b>175</b>	113	38	38	37	114	40	40	34
<b>176</b>	72	25	24	23	73	25	24	24
<b>177</b>	96	32	32	32	96	32	32	32
<b>178</b>	109	36	38	35	113	37	39	37
<b>179</b>	120	40	40	40	120	40	40	40
<b>180</b>	102	31	34	37	105	28	37	40
<b>181</b>	114	37	37	40	120	40	40	40

182	96	32	32	32	96	32	32	32
183	120	40	40	40	115	36	40	39
184	108	38	35	35	111	38	36	37
185	108	36	36	36	102	29	36	37
186	71	28	24	19	78	23	27	28
187	99	32	35	32	102	33	34	35
188	115	37	40	38	119	40	39	40
189	79	25	29	25	81	28	27	26
190	120	40	40	40	112	40	35	37
191	114	37	38	39	108	38	34	36
192	96	32	32	32	96	32	32	32
193	70	32	18	20	76	22	25	29
194	120	40	40	40	120	40	40	40
195	120	40	40	40	120	40	40	40
196	98	30	37	31	81	29	26	26
197	120	40	40	40	120	40	40	40
198	120	40	40	40	120	40	40	40
199	96	31	32	33	83	23	30	30
200	78	26	28	24	65	27	20	18
201	113	40	38	35	114	38	38	38
202	120	40	40	40	117	40	38	39
203	120	40	40	40	109	37	37	35
204	120	40	40	40	112	40	35	37
205	108	38	35	35	111	38	36	37
206	120	40	40	40	120	40	40	40
207	111	36	38	37	111	36	38	37
208	119	40	40	39	116	40	40	36
209	67	29	24	14	67	28	19	20
210	79	25	29	25	81	28	27	26
211	116	36	40	40	120	40	40	40
212	114	37	38	39	108	38	34	36
213	110	38	36	36	107	35	36	36
214	96	32	32	32	96	32	32	32
215	110	38	37	35	106	34	35	37
216	98	30	37	31	81	29	26	26
217	107	36	35	36	109	36	36	37
218	79	25	29	25	81	28	27	26
219	114	37	38	39	108	38	34	36
220	120	40	40	40	112	40	35	37
221	109	36	38	35	113	37	39	37
222	113	37	38	38	111	38	36	37
223	120	40	40	40	120	40	40	40
224	114	37	37	40	120	40	40	40
225	120	40	40	40	120	40	40	40
226	83	26	35	22	94	24	37	33
227	57	21	18	18	48	12	19	17
228	83	28	28	27	82	23	29	30

229	96	32	32	32	96	32	32	32
230	113	37	38	38	111	38	36	37
231	115	38	39	38	114	39	38	37
232	93	31	31	31	86	30	27	29
233	98	30	37	31	81	29	26	26
234	73	11	26	36	107	34	36	37
235	113	38	38	37	114	40	40	34
236	70	32	18	20	76	22	25	29
237	108	36	36	36	102	29	36	37
238	120	40	40	40	109	37	37	35
239	72	24	24	24	92	28	32	32
240	120	40	40	40	117	40	38	39
241	72	24	24	24	92	28	32	32
242	120	40	40	40	120	40	40	40
243	83	26	35	22	94	24	37	33
244	108	38	35	35	111	38	36	37
245	71	28	24	19	78	23	27	28
246	96	32	32	32	96	32	32	32
247	113	37	38	38	111	38	36	37
248	79	25	29	25	81	28	27	26
249	120	40	40	40	120	40	40	40
250	97	31	31	35	96	31	35	30
251	96	31	32	33	83	23	30	30
252	104	35	32	37	94	33	31	30
253	107	36	35	36	109	36	36	37
254	120	40	40	40	109	37	37	35
255	120	40	40	40	120	40	40	40
256	107	36	35	36	109	36	36	37
257	104	35	32	37	94	33	31	30
258	70	32	18	20	76	22	25	29
259	107	36	35	36	109	36	36	37
260	111	36	38	37	111	36	38	37
261	110	38	37	35	106	34	35	37
262	108	38	35	35	111	38	36	37
263	82	29	28	25	92	29	32	31
264	113	38	38	37	114	40	40	34
265	98	30	37	31	81	29	26	26
266	115	37	40	38	119	40	39	40
267	120	40	40	40	120	40	40	40
268	95	31	34	30	104	35	36	33
269	120	40	40	40	112	40	35	37
270	120	40	40	40	120	40	40	40
271	110	34	38	38	110	35	38	37
272	110	38	37	35	106	34	35	37
273	71	28	24	19	78	23	27	28
274	95	31	34	30	104	35	36	33
275	83	30	27	26	63	21	23	19

<b>276</b>	82	29	28	25	92	29	32	31
<b>277</b>	120	40	40	40	120	40	40	40
<b>278</b>	120	40	40	40	120	40	40	40
<b>279</b>	67	29	24	14	67	28	19	20
<b>280</b>	110	38	36	36	107	35	36	36
<b>281</b>	70	32	18	20	76	22	25	29
<b>282</b>	69	26	15	28	76	29	25	22
<b>283</b>	113	38	38	37	112	39	36	37
<b>284</b>	113	40	38	35	114	38	38	38
<b>285</b>	110	38	36	36	107	35	36	36
<b>286</b>	120	40	40	40	120	40	40	40
<b>287</b>	102	31	34	37	105	28	37	40
<b>288</b>	110	34	38	38	110	35	38	37
<b>289</b>	83	28	28	27	82	23	29	30
<b>290</b>	120	40	40	40	120	40	40	40
<b>291</b>	111	38	35	38	109	35	34	40
<b>292</b>	104	35	32	37	94	33	31	30
<b>293</b>	109	36	37	36	113	37	38	38
<b>294</b>	113	40	38	35	114	38	38	38

## **Anexo 6. Propuesta de mejora**

En relación a la recomendación 1, el aporte a la doctrina militar implica la incorporación de un enfoque integral de formación continua en inteligencia militar, que fomente la adaptabilidad y actualización constante ante amenazas emergentes. Este enfoque doctrinal debe ser multidimensional, abarcando desde el uso de tecnologías avanzadas hasta la mejora de habilidades analíticas y de toma de decisiones estratégicas en todos los niveles del ejército. Se sugiere incluir en la doctrina la obligatoriedad de revisiones periódicas de las estrategias de inteligencia, lo cual permitiría ajustar las operaciones a las realidades geopolíticas y tecnológicas cambiantes. Además, la doctrina debe formalizar la colaboración interinstitucional con otras fuerzas de seguridad y con aliados internacionales, asegurando que se utilicen las mejores prácticas globales y los recursos más efectivos. Establecer directrices claras sobre la cooperación interinstitucional en inteligencia refuerza su importancia como un pilar fundamental para la seguridad nacional, adaptando constantemente sus estrategias a las nuevas amenazas globales.

En relación a la recomendación 2, el aporte a la doctrina militar se centraría en la formalización de un sistema avanzado de análisis de información como una parte crítica del proceso de toma de decisiones operativas y estratégicas. Para que el ejército sea más eficiente en la protección de instalaciones críticas, la doctrina debe incluir directrices sobre el uso obligatorio de tecnologías avanzadas de procesamiento de datos, inteligencia artificial y algoritmos predictivos que puedan anticipar posibles amenazas con mayor precisión. La creación de equipos multidisciplinarios que incluyan expertos en tecnología, ciberseguridad y operaciones tácticas debe ser un pilar doctrinal, ya que esto garantiza que las decisiones no se tomen de manera aislada sino basadas en un análisis integral y oportuno. Este enfoque doctrinal formalizaría la necesidad de revisar constantemente los procedimientos de análisis, asegurando que la información recopilada y procesada se utilice de manera efectiva en la prevención de amenazas y en la protección de las instalaciones críticas.

En relación a la recomendación 3, el aporte a la doctrina militar residiría en la creación de un marco de operaciones de contrainteligencia más robusto y estructurado, que ponga un fuerte énfasis en la prevención de amenazas internas, infiltraciones y espionaje. Este marco

doctrinal debe incluir la implementación obligatoria de programas de capacitación especializada para todo el personal, desde el nivel de cadetes hasta los oficiales de alto rango, asegurando que todos comprendan los riesgos y las contramedidas necesarias en contra de las amenazas internas. Además, la doctrina debería promover el uso de tecnologías avanzadas de monitoreo y supervisión interna, garantizando la detección temprana de comportamientos sospechosos o intentos de infiltración. Incluir la realización periódica de simulacros de contrainteligencia en las instalaciones militares ayudaría a preparar mejor a los equipos de seguridad, identificando puntos vulnerables en los sistemas y ajustando las estrategias antes de que ocurran problemas reales. Este aporte doctrinal no solo mejoraría la seguridad interna, sino que también elevaría los estándares operativos del ejército, asegurando una mayor resiliencia frente a ataques internos y externos.

En relación a la recomendación 4, el aporte a la doctrina militar sería la incorporación de un enfoque tecnológico avanzado centrado en la innovación continua en inteligencia y la obligatoriedad de mantener las herramientas tecnológicas actualizadas de manera regular. La doctrina debería establecer la creación de centros de innovación tecnológica en inteligencia dentro de las fuerzas armadas, que actúen como plataformas para el desarrollo y la implementación de nuevas tecnologías en operaciones de seguridad. Estos centros no solo evaluarían las tecnologías existentes, sino que también fomentarían la investigación y el desarrollo de nuevos sistemas de inteligencia que se adapten a las amenazas emergentes. Además, la doctrina debe subrayar la importancia de la capacitación constante del personal militar en el uso de estas tecnologías, garantizando que los cadetes y oficiales no solo cuenten con las herramientas más avanzadas, sino que también posean las habilidades para operarlas de manera efectiva. Este enfoque centrado en la tecnología y la innovación fortalecería la capacidad de respuesta del ejército, optimizando la seguridad de las infraestructuras críticas frente a una gama cada vez mayor de amenazas modernas.

## Anexo 7. Validación por juicio de expertos



ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"



### JUICIO DE EXPERTOS

#### I. DATOS GENERALES

- 1.1 APELLIDOS Y NOMBRES : Patricia Maribel Yllescas Rodríguez  
 1.2 GRADO ACADÉMICO : DOCTOR  
 1.3 INSTITUCIÓN QUE LABORA : EMCH  
 1.4. TÍTULO DE LA INVESTIGACIÓN : ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS "CFB", 2024  
 1.5 AUTOR DEL INSTRUMENTO : CAD IV INTG JOE ESCOBEDO HURTADO  
 1.6 NOMBRE DEL INSTRUMENTO : Operatividad del fusil Scar-LR

#### II. ASPECTOS A EVALUAR:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		01	02	03	04	05
1.CLARIDAD	Está formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Está formulado con conductas observables				X	
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología				x	
4.ORGANIZACIÓN	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					X
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio					X
8.COHERENCIA	Entre las variables, dimensiones y variables					X
9.METODOLOGÍA	La estrategia responde al propósito del estudio				X	
10 CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías				X	
SUB TOTAL		Σ=	Σ=	Σ=	Σ= 16	Σ= 30
TOTAL				Σ= 46		

VALORACIÓN CUANTITATIVA (total x 0.4) : 18.4

#### CRITERIO DE APLICABILIDAD

- a) De 01 a 12: (Reformulación)      c) De 16 a 20: (Aplicable)  
 b) De 13 a 15: (Optimización)

OPINIÓN DE APLICABILIDAD : APLICABLE

Lugar y fecha: Chorrillos, 19 de Agosto del 2024

Dra. Patricia Yllescas Rodríguez

DNI 07266567


**ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"**

**JUICIO DE EXPERTOS**
**III. DATOS GENERALES**

- 1.1 APELLIDOS Y NOMBRES : **Calla Colana Godofredo Jorge**  
 1.2 GRADO ACADÉMICO : DOCTOR  
 1.3 INSTITUCIÓN QUE LABORA : EMCH  
 1.4 TÍTULO DE LA INVESTIGACIÓN : **ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS "CFB", 2024**  
 1.5 AUTOR DEL INSTRUMENTO : CAD IV INTG JOE ESCOBEDO HURTADO  
 1.6 NOMBRE DEL INSTRUMENTO : **Operatividad del fusil Scar-LR**

**IV. ASPECTOS A EVALUAR:**

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		01	02	03	04	05
1.CLARIDAD	Está formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Está formulado con conductas observables					X
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología					X
4.ORGANIZACIÓN	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio				X	
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio				X	
8.COHERENCIA	Entre las variables, dimensiones y variables					X
9.METODOLOGÍA	La estrategia responde al propósito del estudio					X
10 CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					X
<b>SUB TOTAL</b>		$\Sigma=$	$\Sigma=$	$\Sigma=$	$\Sigma= 8$	$\Sigma= 40$
<b>TOTAL</b>				$\Sigma= 48$		

**VALORACIÓN CUANTITATIVA (total x 0.4) : 19.2**
**CRITERIO DE APLICABILIDAD**

- a) De 01 a 12: (Reformulación)      c) De 16 a 20: (Aplicable)  
 b) De 13 a 15: (Optimización)

**OPINIÓN DE APLICABILIDAD : APLICABLE**
**Lugar y fecha: Chorrillos, 19 de Agosto del 2024**

Dr. Godofredo Calla Colana PhD  
Educador - Metodólogo

**Dr. Godofredo Calla Colana**
**DNI 25413288**


**ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"**

**JUICIO DE EXPERTOS**
**V. DATOS GENERALES**

- 1.1 APELLIDOS Y NOMBRES : Caller Luna Juan Bautista  
 1.2 GRADO ACADÉMICO : DOCTOR  
 1.3 INSTITUCIÓN QUE LABORA : EMCH  
 1.4. TÍTULO DE LA INVESTIGACIÓN : ESTRATEGIAS DE INTELIGENCIA MILITAR Y LA SEGURIDAD EN LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS "CFB", 2024  
 1.5 AUTOR DEL INSTRUMENTO : CAD IV INTG JOE ESCOBEDO HURTADO
- 1.6 NOMBRE DEL INSTRUMENTO : Operatividad del fusil Scar-LR

**VI. ASPECTOS A EVALUAR:**

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente	Regular	Bueno	Muy Bueno	Excelente
		01	02	03	04	05
1.CLARIDAD	Está formulado con lenguaje apropiado					X
2.OBJETIVIDAD	Está formulado con conductas observables					X
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología					X
4.ORGANIZACIÓN	Existe Organización y Lógica					X
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad					X
6.INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					
7.CONSISTENCIA	Basado en el aspecto teórico científico y del tema de estudio					x
8.COHERENCIA	Entre las variables, dimensiones y variables				x	
9.METODOLOGÍA	La estrategia responde al propósito del estudio				X	
10 CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías				X	
<b>SUB TOTAL</b>		$\Sigma=$	$\Sigma=$	$\Sigma=$	$\Sigma= 12$	$\Sigma=35$
<b>TOTAL</b>		$\Sigma= 47$				

**VALORACIÓN CUANTITATIVA (total x 0.4) : 18.8**

**CRITERIO DE APLICABILIDAD**

- a) De 01 a 12: (Reformulación)      c) De 16 a 20: (Aplicable)  
 b) De 13 a 15: (Optimización)

**OPINIÓN DE APLICABILIDAD : APLICABLE**

**Lugar y fecha: Chorrillos, 19 de Agosto del 2024**

Dr. Caller Luna, Juan B.  
 PSICÓLOGO CLÍNICO- EDUCATIVO  
 C.Ps. P. N°6806

Dr. Juan Caller Luna

DNI 07143496

**Anexo 8. Dictamen Docente Revisor (DINVEST)**

**Anexo 9. Acta de sustentación (DINVEST)**

**Anexo 10. Otros**