ESCUELA MILITAR DE CHORRILLOS

"CORONEL FRANCISCO BOLOGNESI"

Uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos "CFB" Lima, 2025

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

Autores:

Bach. Gonzalo Cayo Saldivar (0000-0002-7803-8362)

Bach. Gabriel Isaac Ccenhua Gómez (0009-0007-0462-9112)

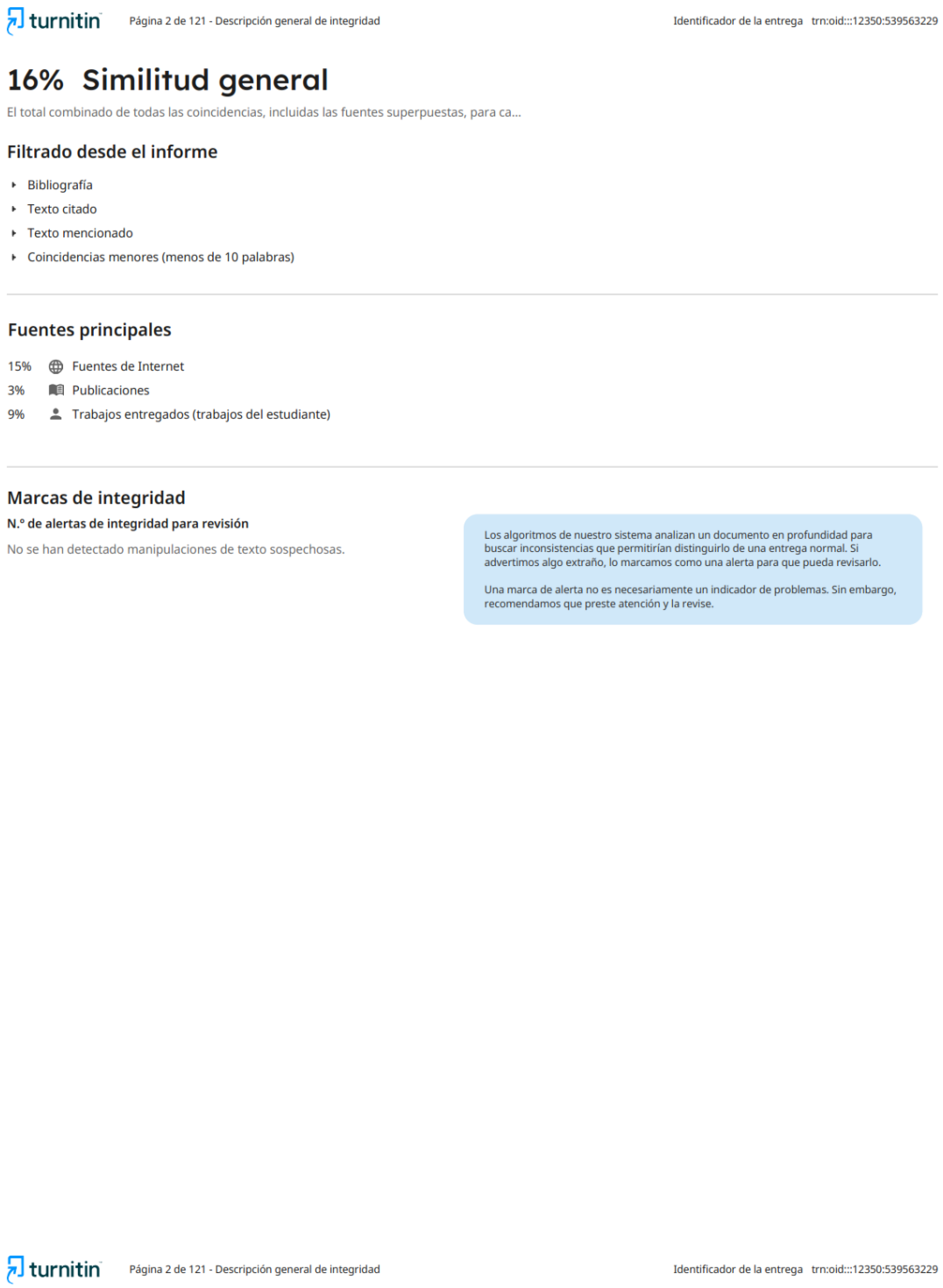
Asesor:

Dr. Edwin Vásquez Mora (000-0001-8834-8826)

Lima – Perú

2025

Grado de similitud



turnitin Página 2 de 121 - Descripción general de integridad Identificador de la entrega trn:oid:::12350:539563229

16% Similitud general

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

Filtrado desde el informe

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

Fuentes principales

15% Fuentes de Internet
3% Publicaciones
9% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° 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.

turnitin Página 2 de 121 - Descripción general de integridad Identificador de la entrega trn:oid:::12350:539563229

Declaración jurada de autoría

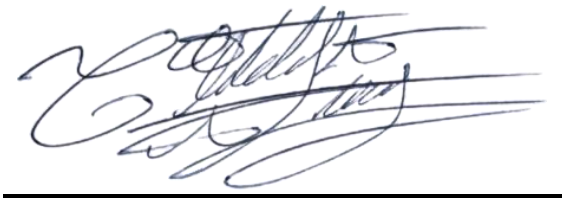
Los bachilleres **Gonzalo Cayo Saldivar y Gabriel Isaac Ccenhua Gómez** del Arma de Inteligencia, de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", (EMCH "CFB") identificados con DNI N° 77035279 y Nº 70410780 respectivamente, declaramos bajo juramento que:

1. Somos autores de la investigación titulada: **"Uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos "CFB" Lima, 2025"**.
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 2025.

Gonzalo Cayo Saldivar
DNI: 77035279



Gabriel Isaac Ccenhua Gómez
DNI: 70410780

Autorización de publicación

DEPARTAMENTO DE INVESTIGACIÓN – DINVEST

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

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

1. Datos personales

Autor 1: Gonzalo Cayo Saldivar	**Autor 2:** Gabriel Isaac Ccenhua Gómez
N° DNI: 77035279	**N° DNI:** 70410780
Teléfono: 937378328	**Teléfono:** 966159956
Correo-e: gcayos@escuelamilitar.edu.pe	**Correo-e:** gccenhuag@escuelamilitar.edu.pe
ORCID: 0000-0002-7803-8362	**ORCID:** 0009-0007-0462-9112

2. Datos de la obra

Título: Uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos "CFB" Lima, 2025
Tipo de obra: Tesis
Asesor: Dr. Edwin Vásquez Mora
N° DNI: 43343660
ORCID: 000-0001-8834-8826
Año de publicación: 2025

3. Declaraciones

Los autores declaran 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"

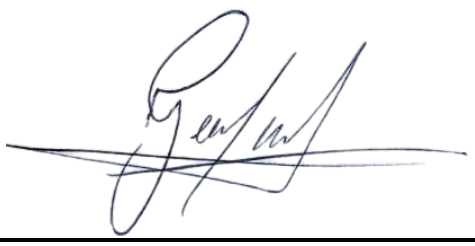
TIPO DE ACCESO A SU INVESTIGACIÓN

Acceso abierto ☐

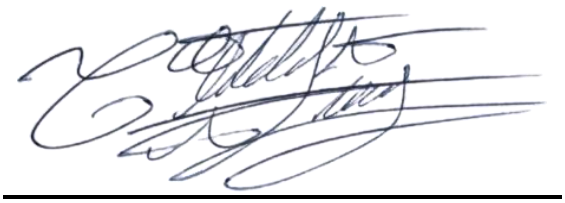
Acceso restringido ☒ **(12 a 24 meses)**

JUSTIFICACIÓN (de acceso restringido)

Información vulnerable militar



Gonzalo Cayo Saldivar
DNI: 77035279



Gabriel Isaac Ccenhua Gómez
DNI: 70410780

Agradecimiento

A Dios, por darnos la fortaleza, sabiduría y perseverancia necesarias para culminar esta importante etapa de nuestra formación académica y personal. Su guía ha sido fundamental en cada paso que hemos dado.

A nuestros padres, por su amor incondicional, apoyo constante y sacrificios realizados para que pudiéramos alcanzar nuestras metas. Sin su respaldo, este logro no hubiera sido posible.

A nuestros instructores y maestros de la Escuela Militar de Chorrillos “CFB”, por compartirnos sus conocimientos, experiencia y valores que han forjado nuestro carácter y profesionalismo. Gracias por su dedicación y compromiso con nuestra formación.

Dedicatoria

A nuestros padres, por ser la inspiración y el pilar fundamental que nos ha motivado a seguir adelante y superar cada desafío con valentía y esfuerzo.

A la Escuela Militar de Chorrillos “CFB”, por brindarnos un espacio de aprendizaje, disciplina y crecimiento integral que ha marcado de manera indeleble nuestro camino hacia la excelencia militar.

Índice

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

El objetivo del estudio fue determinar la relación existente entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” durante el año 2025. La metodología empleada fue de enfoque cuantitativo, tipo básico y nivel descriptivo-correlacional, aplicando el método hipotético-deductivo y un diseño no experimental de corte transversal. La población de la investigación estuvo conformada por 1,226 cadetes, de los cuales se seleccionó una muestra representativa de 293 cadetes mediante muestreo probabilístico aleatorio. Para la recolección de datos se utilizó la técnica de la encuesta, aplicando como instrumento un cuestionario estructurado con preguntas cerradas y escala Likert, dirigido a los cadetes participantes. Los resultados demostraron que un alto porcentaje de los cadetes que reportaron un uso elevado de drones también percibieron altos niveles de seguridad en las instalaciones, destacando que el 39.9% presentó ambas condiciones, mientras que un 34.8% percibió uso alto de drones y seguridad media. Por otro lado, entre quienes reportaron bajo Uso de drones, predominó la percepción de baja seguridad. El análisis inferencial, utilizando la prueba de correlación de Spearman, evidenció un coeficiente de 0.848 y un nivel de significancia de 0.000, lo que confirma una correlación positiva alta y significativa entre ambas variables. Se concluyó que el mayor Uso de drones se asocia con una mejor percepción de seguridad en la Escuela Militar, recomendándose fortalecer la integración de esta tecnología en los programas de formación y operación institucional.

Palabras claves: Uso de drones, seguridad de las instalaciones y cadetes.

Abstract

The objective of this study was to determine the relationship between drone use and facility security at the Colonel Francisco Bolognesi Military School in Chorrillos through 2025. The methodology employed was a quantitative, basic approach with a descriptive-correlational level, applying the hypothetical-deductive method and a non-experimental cross-sectional design. The research population consisted of 1,226 cadets, from which a representative sample of 293 was selected through random probability sampling. Data collection was conducted using a survey technique, using a structured questionnaire with closed-ended questions and a Likert scale, addressed to participating cadets. The results showed that a high percentage of cadets who reported high drone use also perceived high levels of security at the facilities. 39.9% reported both conditions, while 34.8% perceived high drone use and medium security. On the other hand, among those who reported low drone use, the perception of low security predominated. The inferential analysis, using the Spearman correlation test, showed a coefficient of 0.848 and a significance level of 0.000, confirming a high and significant positive correlation between the two variables. It was concluded that increased drone use is associated with improved perceptions of security at the Military Academy, and it is recommended that the integration of this technology into training programs and institutional operations be strengthened.

Keywords: Drone use, facility security, and cadets.

INTRODUCCIÓN

La incorporación de aeronaves pilotadas a distancia en ámbitos de seguridad ha pasado de ser un experimento a constituir un componente habitual de los sistemas modernos de vigilancia y protección de recintos estratégicos, debido a su capacidad para ampliar el alcance de observación, reducir tiempos de respuesta y operar con menor exposición del personal en superficie (ICAO, 2024). En tal escenario, el "Uso de drones" se entiende como el empleo planificado de plataformas, sensores y procedimientos que habilitan conciencia situacional táctica en tiempo real, un objetivo que diversas propuestas de arquitectura de sistemas han estandarizado para facilitar su adopción por entidades de seguridad (Al-Dosari et al., 2024).

Para instalaciones extensas con perímetros complejos (como las de una escuela militar) los drones permiten patrullaje aéreo, apoyan la detección temprana de anomalías e integran analítica de video y telemetría georreferenciada, elevando el umbral de disuasión y la probabilidad de detección efectiva (Villarino et al., 2025). La literatura de defensa también insiste en que la integración doctrinal y los protocolos de mando-control son decisivos para que los UAV pasen de ser "herramientas" a "capacidades" orgánicas de seguridad perimetral con reglas de empleo, interoperabilidad y ciclos de decisión bien definidos (NATO, 2020).

El marco regulatorio resulta crítico en la fase de diseño metodológico porque condiciona clases operativas, licencias, zonas, alturas y responsabilidades, por lo que cualquier despliegue en el Perú debe alinearse a la Ley N.° 30740 y a la normativa técnica de la DGAC bajo el MTC (MTC, 2019). Asimismo, la armonización con las SARPs y material guía de la OACI sobre RPAS ofrece principios de seguridad operacional (autorización, reglas de vuelo, comunicaciones, evitación de colisiones) que estructuran la evaluación de riesgos y los requisitos de competencia del personal (ICAO, 2025).

Junto a los beneficios, emergen amenazas asociadas al uso malicioso de sUAS y a la necesidad de doctrinas C-UAS; por ello, la planificación de seguridad de instalaciones debe considerar simultáneamente el empleo de drones para vigilancia y la protección frente a drones hostiles (DoD, 2021). En términos de política pública y costos de ciclo de vida, evaluaciones recientes subrayan que las decisiones sobre capacidades C-UAS, coordinación interagencial y severidad del riesgo condicionan la sostenibilidad de estas soluciones en entornos gubernamentales y militares (CRS, 2025).

Existe evidencia local relevante para el caso EMCH “CFB”: estudios de su propio repositorio muestran la pertinencia de sistemas anti-drones para la seguridad aérea de la Escuela y discuten lineamientos de implementación, competencia de operadores y factibilidad de adopción gradual (Vásquez Tarrillo, 2021). A la par, trabajos sobre empleo de drones en la instrucción de cadetes aportan un sustrato organizacional y pedagógico que facilita la alfabetización tecnológica necesaria para integrar estas plataformas en funciones de seguridad de instalaciones (Serrano Saavedra, 2023).

Finalmente, el componente de seguridad de la información y ciberseguridad es determinante: enlaces de mando-control, telemetría y video deben protegerse con esquemas ligeros de cifrado, gestión de claves y segmentación de redes para preservar integridad, disponibilidad y confidencialidad durante operaciones en campus militares (Sarkar, 2025). Además, revisiones sobre Internet de Drones advierten sobre vectores de ataque y recomiendan marcos de gestión de riesgos que integren pruebas de penetración, monitoreo de tráfico y cumplimiento regulatorio, aspectos que esta investigación incorporará al conceptualizar la relación entre Uso de drones y seguridad de instalaciones (Samanth et al., 2022).

El esquema de este estudio consta de cinco capítulos principales, que se desarrollan sistemáticamente en la siguiente secuencia:

El Capítulo I, denominado Planteamiento del problema, aborda la descripción problemática que existen con Uso de drones con el objetivo de incidir en seguridad de las instalaciones de los cadetes. Además, se da la delimitación de la investigación, identificar y articular los siguientes problemas y objetivos: generales y específicos, justificación, importancia y limitaciones del estudio.

En el desarrollo del Capítulo II es el Marco Teórico, se constató que los estudios relacionados con este tema formaron los antecedentes internacionales y nacionales. Por lo tanto, se apoya en una base teórica para transformaciones de dimensiones correspondientes y también en un marco conceptual. Para este estudio se construyeron hipótesis generales y específicas, detallando el funcionamiento de las variables.

En el Capítulo III, conocido como Marco de Metodológico, se determinó que el diseño de este estudio sería descriptivo y correlativo. Además, se determinaron el tamaño de la muestra, las técnicas de recolección y procesamiento de datos.

El Capítulo IV versa sobre los resultados, dando detalles sobre el análisis descriptivo tratándose sobre la interpretación de los resultados estadísticos adjuntando las tablas y figuras correspondientes. Y sobre el análisis inferencial con la comprobación de las hipótesis, existe una relación significativa entre las variables del análisis.

Por último, el Capitulo V trata sobre la discusión de los resultados, contrastándolo con trabajos semejantes y comparándolos con el presente estudio.

Finalmente, se elaboraron las conclusiones y recomendaciones propuestas.

CAPÍTULO I.
PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción problemática

A escala internacional, el crecimiento del parque de drones y su uso operativo han creado un nuevo umbral de exposición para la seguridad física: solo en Estados Unidos se registraron 822 039 drones a julio de 2025, con 433 407 registros comerciales (≈53 %) y 460 375 pilotos remotos certificados, mientras que en Europa la autoridad de seguridad aérea reportó 12 accidentes e incidentes graves en 2023 y que en el 66 % de esos sucesos no hubo personas afectadas en tierra ni en el aire (FAA, 2025). Estos volúmenes y tasas ilustran que la masificación tecnológica incrementa la probabilidad de contactos no deseados con la seguridad de instalaciones, al tiempo que muestra que una gran parte de los eventos no deriva en daños cuando existe gestión de riesgos y cumplimiento regulatorio (EASA, 2024).

Además de los conteos de flota, los incidentes reportados por fuerzas policiales y gestores de infraestructuras críticas describen patrones de uso indebido: en el Reino Unido se notificaron más de 6 000 incidentes relacionados con drones durante 2023, de los cuales aproximadamente el 11 % constituyó delito, una señal del amplio rango de comportamientos que van desde operaciones inocuas hasta amenazas a sitios sensibles (ProtectUK, 2024). En paralelo, la Unión Europea adoptó en 2023 una Comunicación específica para contrarrestar los riesgos de drones no cooperativos, definiendo líneas de acción regulatorias, operativas y de intercambio de información que los Estados deben articular con gestores de instalaciones y fuerzas de seguridad (European Commission, 2023).

En este contexto, el uso de drones se entiende como la capacidad institucional de planificar, operar e integrar aeronaves no tripuladas, sensores y flujos de datos para misiones de reconocimiento, vigilancia del perímetro, verificación de alarmas y apoyo a la respuesta; su valor reside en generar conciencia situacional aérea de bajo costo y con menor exposición del personal, siempre bajo procedimientos, segregación del espacio aéreo y evaluación de riesgos (ICAO, 2023). La disponibilidad de operadores calificados y marcos de competencia reflejada, por ejemplo, en el número de pilotos

remotos certificados y el cumplimiento de requisitos de identificación/zonificación es un prerrequisito para que el empleo de drones transite de “herramienta” a “capacidad” en seguridad de instalaciones (FAA, 2025).

Por su parte, la seguridad de las instalaciones abarca el conjunto de medidas de protección preventiva y de respuesta orientadas a reducir la probabilidad y el impacto de intrusiones, sabotaje, vigilancia hostil y otras amenazas, integrando diseño ambiental, control de accesos, detección, demoras y procedimientos de intervención (ISO, 2021). Los lineamientos especializados para UAS en protección de sitios como los de la autoridad nacional de protección del Reino Unido insisten en planificar barreras físicas y tecnológicas, protocolos de detección/seguimiento, coordinación con autoridades competentes y revisión periódica conforme evolucionan las capacidades de los drones y de las contramedidas (NPSA, 2023).

El problema se complejiza porque la misma tecnología que habilita vigilancia útil para custodiar perímetros también puede emplearse de manera maliciosa contra esas instalaciones: la Interpol ha publicado guías para probar y evaluar capacidades C-UAS, subrayando que la preparación debe cubrir desde la detección y la identificación hasta la decisión coordinada y la neutralización proporcional conforme al marco legal (INTERPOL, 2023). A nivel de políticas públicas, análisis del Congreso de Estados Unidos sobre programas Counter-UAS resaltan la urgencia de inversiones y la necesidad de gobernanza interagencial para atender amenazas crecientes contra activos militares y de infraestructura crítica (CRS, 2025).

A la par, la superficie de ataque digital de los ecosistemas con drones enlaces de mando y control, telemetría, video, apps y nubes exige controles ciber y de privacidad integrados al ciclo operativo: recomendaciones recientes establecen requisitos para seleccionar tecnologías de detección compatibles con planes de seguridad y para cifrar datos, minimizar exposición y evaluar impactos de privacidad antes de las misiones (CISA, 2025). Informes sectoriales de auditoría pública también aconsejan cautela con proveedores y configuraciones, enfatizando entrenamiento, gestión de claves y segmentación de redes para preservar disponibilidad, integridad y confidencialidad en operaciones cercanas a instalaciones sensibles (Utah State Auditor, 2024).

Desde la perspectiva metodológica y doctrinal, manuales técnicos reconocidos en el entorno de la OTAN recomiendan abordar el riesgo de drones bajo un enfoque de sistemas, con responsabilidades claras entre protección de la fuerza, defensa aérea y seguridad de instalaciones, y con integración de sensores, procedimiento de mando-control y reglas de empleo proporcionadas (JAPCC, 2020). En el ámbito civil de la aviación, guías de gestión de incidentes con drones en aeródromos proponen identificar peligros, usar marcos de gestión de seguridad existentes y fortalecer la coordinación con la policía local para responder a incursiones no autorizadas alrededor de infraestructuras críticas (EASA, 2021).

En síntesis, el problema internacional que fundamenta esta investigación es doble: por un lado, el rápido Uso de drones expande la capacidad de vigilancia y respuesta de los administradores de instalaciones; por otro, su disponibilidad crea una presión de riesgo que obliga a consolidar estándares de diseño seguro, desarrollar operadores competentes, incorporar tecnologías de detección/neutralización y alinear ciberseguridad con la física, bajo marcos normativos y de cooperación interinstitucional ya delineados por organismos multilaterales y agencias especializadas (European Commission, 2023). Este punto de partida justifica estudiar empíricamente la relación entre empleo de drones y seguridad de instalaciones en un campus militar, donde la criticidad del activo, la necesidad de tiempos de respuesta bajos y la coordinación con autoridades aeronáuticas y de defensa vuelven prioritario un enfoque integral basado en evidencia (ICAO, 2023).

A nivel nacional, el entorno de seguridad ofrece un telón de fondo objetivo para esta investigación: en el semestre móvil enero–junio de 2024, el 27,7% de la población urbana de 15 y más años fue víctima de algún hecho delictivo y el 16,7% de esas víctimas formalizó denuncia, lo que marca un aumento respecto a semestres previos (INEI, 2024). Como reflejo del estrés operativo sobre instalaciones críticas, el Instituto Nacional Penitenciario reportó más de 600 intervenciones a visitantes durante 2025 y comunicó casos específicos de intentos de ingreso de ilícitos mediante drones en establecimientos como el penal de Cajamarca (INPE, 2025).

Ejemplos recientes muestran el uso institucional de drones para reforzar la seguridad pública: con motivo de APEC Perú 2024, el Ministerio del Interior destacó el despliegue de equipamiento tecnológico de última generación para protección de

autoridades y sedes, contexto en el que los sistemas aéreos no tripulados se integran a vigilancia, inteligencia y respuesta (Ministerio del Interior, 2024). En 2025, el propio sector Interior y el Gobierno Regional de La Libertad entregaron 40 drones a la PNP para ampliar capacidades de patrullaje e investigación, estableciendo una frecuencia de dotación tangible que respalda la adopción operativa a nivel nacional (Ministerio del Interior, 2025).

En el plano normativo y organizacional, el marco peruano exige registro y autorizaciones para operar RPAS, con procedimientos y requisitos definidos por la Dirección General de Aeronáutica Civil del MTC; el propio sector ha comunicado la simplificación del trámite y los pasos obligatorios para operar, reforzando trazabilidad y control sobre flota, pilotos y misiones (MTC, 2025). Complementariamente, lineamientos institucionales señalan que la DGAC es la autoridad encargada de asegurar que el uso de aeronaves pilotadas a distancia se realice dentro de la ley y con criterios de seguridad operacional, lo que estructura la gobernanza técnica que sustenta el empleo de drones en el país (CENEPRED, 2017).

En relación con el uso de drones, en el contexto peruano el uso efectivo implica planificar misiones, capacitar operadores, integrar sensores y asegurar la cadena de datos para vigilancia, reconocimiento o verificación de alertas, con protocolos que reduzcan la exposición del personal y mejoren la conciencia situacional aérea (Reyes Valdivia, 2022). La literatura académica nacional y casuística profesional incluida la producción de la Escuela Militar de Chorrillos muestra que estas plataformas, debidamente estandarizadas y con perfiles de competencia del operador, pueden aportar información oportuna para la toma de decisiones en apoyo a agencias del orden y a la seguridad de instalaciones (Rodríguez Herrera, 2021).

En cuanto a la seguridad de las instalaciones, su alcance comprende prevención, detección, control de accesos, demoras y respuesta ante amenazas físicas o híbridas, y en el caso peruano el diagnóstico de criminalidad y victimización justifica fortalecer barreras físicas y tecnológicas, así como la coordinación interinstitucional que soporta los planes de seguridad de predios públicos y estratégicos (INEI, 2024). Como evidencia de aplicación, el INPE ha institucionalizado medidas de vigilancia perimetral con monitoreo aéreo mediante drones alrededor de establecimientos penitenciarios y

zonas aledañas, integrando estos sistemas a sus procedimientos para reducir intentos de intrusión y el uso ilícito del espacio aéreo cercano a instalaciones críticas (INPE, 2025).

En la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” (EMCH “CFB”), el uso de drones se configura como una capacidad formativa y operativa que potencia el reconocimiento, la obtención de inteligencia y la verificación rápida de alertas en el campus, al proporcionar conciencia situacional aérea de bajo costo y con menor exposición del personal (Rodríguez Herrera, 2021). La evidencia producida por su propia comunidad académica militar muestra que, cuando se estandarizan perfiles de competencia y procedimientos, los drones migran de “herramienta” a “capacidad” que optimiza la seguridad en unidades de élite y, por extensión, es transferible a la protección de instalaciones educativas militares por su arquitectura modular de sensores, misión y enlace de datos (Puma Espirilla, 2020).

Para que esa capacidad sea sostenible dentro de EMCH “CFB”, su empleo debe alinearse con el régimen nacional de RPAS: inscripción del equipo, licenciamiento/competencia del operador, limitaciones de zona/altura y responsabilidad operacional; estos requisitos, definidos por la DGAC del MTC, condicionan la planificación de vuelos en entorno urbano, la selección de equipos y la integración con protocolos internos de seguridad (MTC, 2024). A nivel didáctico y doctrinal, la Escuela dispone de trabajos y guías de instrucción que abordan modos de operación, simuladores, maniobrabilidad y empleo seguro en apoyo al entrenamiento de cadetes, lo que permite institucionalizar la formación de pilotos remotos y asegurar trazabilidad técnica del empleo en el recinto (EMCH “CFB”, 2021).

En el caso de la seguridad de las instalaciones, los propios estudios alojados en el repositorio de EMCH documentan patrones de aceptación y percepción de eficacia entre cadetes respecto de tecnologías de vigilancia: por ejemplo, frente a la pregunta “¿Considera Usted que la utilización de drones aumentará la seguridad de la EMCH CFB?”, un 34 % respondió a favor, 38 % se mostró indiferente y 29 % no estuvo de acuerdo; y, en tecnología visual complementaria, otro 34 % confirmó la influencia de más cámaras en la mejora de la seguridad (EMCH “CFB”, 2024). Estas cifras, sumadas a resultados coherentes en tecnología sensorial y radiofrecuencia, justifican que la gestión de la seguridad del campus priorice integración de video, sensores de acceso y patrullaje aéreo como medidas preventivas y de verificación de incidentes, coherentes

con el enfoque nacional de fortalecimiento tecnológico de la custodia de recintos y eventos (Ministerio del Interior, 2024).

Dado el carácter militar del activo, la seguridad perimetral también exige contemplar el contradron: la EMCH "CFB" cuenta con investigación específica que evaluó la implementación de un sistema anti-drones para salvaguardar su espacio aéreo, con recomendaciones de factibilidad y de articulación con la seguridad de instalaciones, lo que refleja el doble rol de la tecnología aérea como aliada y potencial amenaza si es usada por terceros (Vásquez Tarrillo, 2021). La gestión integral del riesgo, por tanto, combina empleo propio de drones para vigilancia, cumplimiento de la normativa DGAC y procedimientos de detección/alerta frente a incursiones no autorizadas, asegurando que cualquier operación aérea (propia o de terceros) se someta a registro, autorización y reglas claras de operación sobre áreas pobladas y zonas sensibles del campus (MTC, 2024).

1.2. Delimitación de la investigación

1.2.1. Espacial

La investigación se delimitó espacialmente al interior del campus de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", en Av. Escuela Militar s/n, distrito de Chorrillos, Lima, concentrando el análisis en áreas académicas, de entrenamiento y zonas perimetrales donde operan rutinas de control, patrullaje y vigilancia, y restringiendo la observación a los entornos y procesos bajo gobernanza institucional de la EMCH "CFB" para evitar inferencias más allá de sus límites físicos *(SEACE, 2021)*. Asimismo, se excluyeron espacios aledaños no administrados por la Escuela y se estableció que cualquier referencia al espacio aéreo se circunscribiera a operaciones de estudio en el recinto y bajo la normativa peruana vigente para RPAS, sin extrapolar a otros predios militares o civiles *(Congreso de la República, 2018)*.

1.2.2. Temporal

La delimitación temporal abarcó del 1 de enero al 31 de diciembre de 2025, periodo que coincide con la disponibilidad y madurez operativa de procedimientos administrativos nacionales para registro y operación de drones, lo que permite observar el uso efectivo de estas tecnologías y su articulación con prácticas de seguridad de

instalaciones en un mismo ciclo anual *(MTC, 2025)*. Esta ventana incorpora el contexto de seguridad ciudadana reportado por el sistema estadístico nacional en 2025 para el semestre móvil inmediato previo, a fin de situar los riesgos generales del entorno sin alterar el foco empírico en el campus militar, y evita comparaciones con años no equivalentes en normativa o dotación tecnológica *(INEI, 2025)*.

1.2.3. Teórica

La delimitación teórica acota la Variable 1 (Uso de drones) al empleo institucional de sistemas de aeronaves pilotadas a distancia (RPAS) entendidos como plataforma, estación de control y enlace C2, en misiones de reconocimiento, verificación de alertas y vigilancia del perímetro, con énfasis en competencia del operador, seguridad operacional y trazabilidad de datos conforme a marcos internacionales de referencia (ICAO, 2025). A su vez, la Variable 2 (seguridad de las instalaciones) se restringe al conjunto de medidas de protección preventiva y de respuesta en un entorno construido control de accesos, detección, demoras, procedimientos y diseño ambiental tomando como guía las directrices CPTED de la familia ISO 22341 para reducir oportunidad y temor al delito en instalaciones específicas, sin extenderse a seguridad pública amplia ni a defensa aérea más allá de la interfase con el recinto (ISO, 2021).

1.3. Formulación del problema

1.3.1. Problema general

¿Cuál es la relación que existe entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025?

1.3.2. Problemas específicos

¿Cuál es la relación que existe entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025?

¿Cuál es la relación que existe entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025?

¿Cuál es la relación que existe entre la gestión tecnológica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025?

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Determinar la relación que existe entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

1.4.2. Objetivos específicos

Determinar la relación que existe entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Determinar la relación que existe entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Determinar la relación que existe entre la gestión tecnológica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

1.5. Justificación e importancia de la investigación

1.5.1. Justificación teórica

La justificación teórica de este estudio descansa en dos pilares complementarios: la estandarización internacional de los sistemas de aeronaves pilotadas a distancia como capacidad técnicamente definida (plataforma, estación de control y enlace C2) que permite operacionalizar el constructo “Uso de drones” con criterios de seguridad operacional, trazabilidad y gobernanza técnica (ICAO, 2025). A su vez, el constructo “seguridad de las instalaciones” se ancla en el marco CPTED de la norma ISO 22341, que orienta el diseño del entorno construido para prevenir oportunidades de intrusión y reducir el temor al delito mediante principios verificables de control natural, vigilancia y refuerzo territorial (ISO, 2021).

1.5.2. Justificación metodológica

Metodológicamente, se adopta un enfoque cuantitativo de tipo básico (puro), con diseño no experimental y alcance descriptivo-correlacional, porque las variables se

observan tal como ocurren en el campo (sin manipulación ni asignación aleatoria) y se miden con instrumentos estandarizados para describir su comportamiento y estimar la fuerza/dirección de su relación en un corte transversal (López Valverde, 2023). Este encuadre es pertinente en contextos organizacionales similares, donde la literatura de tesis y artículos aplicados valida la idoneidad de diseños correlacionales para evaluar asociaciones entre prácticas tecnológicas y resultados de seguridad, con análisis soportados en coeficientes paramétricos o no paramétricos y criterios de validez y confiabilidad consistentes (Flores Zevallos & Sandoval Rosario, 2022).

1.5.3. Justificación práctica

En el plano práctico, la investigación aporta evidencia útil para la toma de decisiones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi": cuantificar el uso de drones en misiones de reconocimiento, verificación de alertas y vigilancia del perímetro, y contrastarlo con indicadores de seguridad de las instalaciones permite identificar brechas de capacitación, tecnología y protocolo, así como priorizar inversiones donde la relación empírica sea más consistente (Vásquez Tarrillo & Paredes Urrutia, 2021). Además, al alinearse con la normativa peruana de la DGAC/MTC sobre registro de equipos, competencia del operador y condiciones operativas, los hallazgos se traducen en recomendaciones aplicables que fortalecen la sostenibilidad regulatoria y operativa del empleo de RPAS en campus militares (MTC, 2024).

1.5.4. Importancia de la investigación

La importancia de esta investigación radica en que aporta evidencia empírica para consolidar el uso de drones como capacidad institucional con fundamento técnico y doctrinal, al alinear la conceptualización del sistema RPAS (plataforma, estación de control y enlace C2) con estándares internacionales que favorecen operaciones seguras y trazables en entornos sensibles (ICAO, 2025). Asimismo, refuerza la seguridad de las instalaciones al enmarcarla en principios CPTED que orientan el diseño y la gestión del entorno construido para disuadir intrusiones y reducir el temor al delito mediante vigilancia natural, control de accesos y refuerzo territorial (ISO, 2021).

En el plano regulatorio y de gobernanza, el estudio es pertinente porque traduce la normativa peruana sobre RPAS en criterios operativos verificables (registro de

equipos, competencia del operador y condiciones de vuelo) necesarios para planificar misiones en campus militares y para asegurar cumplimiento durante la adopción tecnológica (MTC, 2024). Al incorporar la Ley N.° 30740 como marco de referencia, la investigación fortalece la capacidad de la EMCH “CFB” para tomar decisiones compatibles con el régimen nacional y para estandarizar procedimientos internos que garanticen seguridad operacional y responsabilidad institucional (Congreso de la República, 2018).

Desde la perspectiva aplicada, la relevancia se expresa en la posibilidad de vincular cuantitativamente el uso de drones con resultados de seguridad de instalaciones, identificando brechas de capacitación, integración tecnológica y protocolos que, una vez priorizadas, aumentan la eficacia del patrullaje aéreo, la verificación de alertas y la respuesta en el perímetro de la Escuela (Vásquez Tarrillo, 2021). Además, al apoyarse en producción académica de la propia EMCH sobre empleo de drones, el estudio crea un puente directo entre evidencia local y mejora continua, facilitando que los hallazgos se traduzcan en formación de operadores, interoperabilidad de sensores y ajustes de procedimientos dentro del recinto (Baquero & Vásquez, 2019).

1.6. Limitaciones de la investigación

Las principales limitaciones se relacionaron con el tiempo disponible para el trabajo de campo dentro de la EMCH “CFB”, debido a calendarios académicos y actividades militares que comprimieron las ventanas para aplicar instrumentos y realizar observaciones. Para mitigarlo, se priorizó un cronograma por franjas alineado a rutinas de formación y descansos, se adoptó recolección digital (formularios en línea y tabulación automática) para reducir tiempos de captura, y se ejecutaron pilotos breves que permitieron depurar ítems antes de la medición definitiva, evitando retrabajos. Además, se capacitó a un equipo de apoyo en instrucciones estandarizadas, se implementó muestreo oportunista con cadetes disponibles sin alterar la estructura de la muestra prevista, y se cerró el levantamiento con ventanas extra de verificación para minimizar datos faltantes, manteniendo la coherencia con el diseño no experimental y el nivel descriptivo-correlacional.

La segunda limitación fue la información limitada sobre ciertos procedimientos internos y registros operativos sensibles (p. ej., incidencias de seguridad y protocolos específicos de vuelo RPAS), lo que restringió la profundidad de algunos cruces. Se afrontó mediante triangulación de fuentes (percepciones de cadetes, observación estructurada en perímetro y revisión documental pública), el uso de indicadores proxy validados (frecuencia de patrullaje aéreo percibido, tiempos de verificación de alertas y percepción de control de accesos), y la sistematización de normativa y guías oficiales para sustentar constructos cuando no existían datos expositivos. Adicionalmente, se aplicaron controles de calidad (consistencia interna y análisis de valores atípicos), se documentaron supuestos y alcances para evitar sobreinferencias y se dejaron líneas de investigación futura que contemplan acceso ampliado a registros institucionales bajo convenios y salvaguardas éticas, garantizando trazabilidad y rigor pese a las restricciones.

CAPÍTULO II.
MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Fernández (2024), en su tesis doctoral sobre el uso de sistemas RPAS en seguridad ciudadana en la Guardia Civil, tuvo por propósito analizar el papel de estas plataformas en la protección pública, describiendo el marco jurídico, los usos policiales y los desafíos operativos que plantearon. La metodología se enmarcó en un enfoque cualitativo, jurídico-doctrinal y descriptivo, sustentado en revisión de normas, doctrina especializada, informes institucionales y experiencias operativas. No se definieron población ni muestra numérica, sino un corpus documental seleccionado por relevancia. La técnica consistió en análisis documental y comparado de leyes, políticas públicas e informes de agencias como FRONTEX, privilegiando el razonamiento jurídico y operativo. Concluyó que los RPAS aportaron ventajas decisivas para vigilancia, control fronterizo, búsqueda y rescate, gestión de emergencias y lucha contra delitos como terrorismo o narcotráfico; este antecedente contribuye a nuestra investigación el relievar la importancia del uso de drones en actividades de seguridad y vigilancia.

Mazza (2024), en su tesis de maestría en la Escuela de Guerra Naval, analizó la factibilidad de un sistema integrado de Inteligencia, Vigilancia y Reconocimiento basado en UAV para apoyar la defensa y el control de espacios marítimos argentinos. Empleó un enfoque descriptivo-analítico y de factibilidad con revisión normativa y doctrinal, análisis de capacidades nacionales de I+D y evaluación del despliegue de medios y bases aeronavales en la Patagonia. No definió universos ni tamaños muestrales, trabajó con un corpus documental y casos operativos pertinentes. La técnica consistió en análisis documental y comparado de leyes, directivas de defensa, informes técnicos y experiencias, sin cuestionarios ni escalas. Concluyó que el empleo de UAV fue viable y conveniente para funciones IVR, vigilancia de fronteras y seguridad marítima, lo cual tendría relación con nuestra segunda variable, seguridad de instalaciones porque respalda la idea de que un buen empleo táctico del dron aumenta la capacidad de seguridad.

Araos y Ruíz (2023), en una tesis de licenciatura en la Universidad de Chile, tuvieron por objetivo identificar y analizar derechos constitucionales potencialmente afectados por el uso de drones y revisar la jurisprudencia nacional para determinar cuándo su empleo implicó vulneración. La metodología se basó en análisis jurídico-doctrinal y revisión sistemática de jurisprudencia y normativa sobre RPA en Chile, incorporando los principios de proporcionalidad e intensa reserva legal. No delimitaron universo estadístico; trabajaron con corpus normativo y sentencias relevantes. La técnica consistió en análisis documental y jurisprudencial de decisiones de Cortes y órganos de la Administración, junto con el marco aeronáutico y de protección de datos. Concluyeron en que se puede demostrar mediante el marco legal el uso de drones, poniendo en evidencia que el uso de drones también depende del cumplimiento normativo y del modo de operación.

Bustamante y Xolo (2021), en una tesis de licenciatura del Instituto Tecnológico Superior de San Andrés Tuxtla, propusieron un mecanismo terrestre adaptable a drones para apoyar la búsqueda de personas en zonas de difícil acceso y reducir el riesgo para rescatistas. La investigación se enmarcó en diseño y modelación mecatrónica, de alcance ingenieril y descriptivo, orientada a especificar la solución, sus funciones previstas y la integración con plataformas UAV, según constó en la ficha del repositorio. No definieron universos cuantitativos; trabajaron con requerimientos operativos de escenarios de rescate. La técnica correspondió al propio proceso de diseño y modelación (diseño conceptual y funcional sustentado en su justificación de uso en sismos, bosques u otros entornos). Relacionamos este mecanismo terrestre acoplado a drones con nuestra segunda variable, seguridad de instalaciones porque incrementa la efectividad en seguridad y protección del área donde se utilicé.

Vidal (2021), en un ensayo académico de la Universidad Militar Nueva Granada, proyectó la incorporación de drones en vigilancia y seguridad privada para una empresa del sector, resaltando su potencial para inspección, seguimiento y monitoreo. Desarrolló un estudio descriptivo y argumentativo de carácter documental, exponiendo tipologías, aplicaciones civiles y componentes, y examinando el marco regulatorio colombiano. No definió universos cuantitativos; trabajó con un corpus de fuentes técnicas y normativas relevantes. La técnica consistió en análisis documental y comparado de lineamientos de la autoridad aeronáutica, revisión de literatura técnica y

elaboración de tablas de clasificación y especificaciones, incluyendo una ficha de equipo comercial. Concluyó que los drones mejoraron cobertura, tiempo de respuesta y seguridad del personal y relacionamos este factor con nuestro objetivo de la variable de seguridad de instalaciones mediante el uso sistemático del dron que genera mejores condiciones de vigilancia y protección.

2.1.2. Antecedentes nacionales

Artica (2025), en la Universidad de Lima, analizó cómo la operación de drones en prevención de riesgos laborales debía compatibilizarse con el régimen peruano de protección de datos personales, precisando obligaciones y salvaguardas de cumplimiento. Desarrolló un enfoque cualitativo y jurídico-doctrinal basado en el análisis de ley, reglamento y normativa aeronáutica para RPAS, más revisión bibliográfica especializada. No definió muestra cuantitativa, sino un corpus de normas, doctrina y antecedentes relevantes en seguridad y salud en el trabajo. Empleó análisis documental y matrices de criterios de licitud, proporcionalidad y seguridad para guiar decisiones sobre uso de drones en centros de trabajo. Concluyó que el empleo era viable si se realizaban evaluaciones de impacto, se acotaban finalidades y tiempos de conservación, se adoptaban medidas técnicas y organizativas, se aseguraba base legal y transparencia con trabajadores, y se integraban protocolos de SST con gobernanza de datos, recomendando políticas internas, capacitación y auditoría continuas para una implementación responsable y eficaz.

Delgado (2024), en la Universidad Señor de Sipán, determinó si operadores de drones podían ser responsables por daños patrimoniales y lesiones durante manifestaciones, y precisó el marco normativo aplicable. Empleó un enfoque cualitativo, jurídico-doctrinal y descriptivo, sustentado en análisis de normas, principios de responsabilidad civil y regulaciones sobre RPAS, privilegiando el razonamiento teórico. No definió universos ni tamaños muestrales; trabajó con corpus documental y normativo pertinente. Utilizó revisión y análisis de leyes, reglamentos y lineamientos administrativos sobre operación en espacio público y tutela de derechos, verificando mediante argumentación jurídica. Concluyó que la responsabilidad del operador se activa por incumplimiento de deberes de seguridad y autorizaciones; que el

incumplimiento genera sanciones y deber de reparar; y que se requiere un marco regulatorio claro y eficaz que proteja derechos en contextos de protesta, reforzando aplicación estricta de normas vigentes y protocolos operativos acordes.

Rodríguez (2021), en la Escuela Militar de Chorrillos, propuso mejorar el empleo de drones como medio de obtención de datos de inteligencia para apoyar operaciones policiales, destacando su utilidad para proveer imágenes y datos oportunos al mando. Desarrolló un enfoque cualitativo, propositivo y descriptivo de corte documental, sustentado en su experiencia en la Dirección Nacional de Inteligencia Policial de Panamá y en la revisión de literatura y modelos de empleo. Estructuró diagnóstico y propuesta de mejora con diseño y arquitectura operativa. No definió universo cuantitativo, sino corpus normativo-técnico y experiencia operativa. Recurrió a análisis documental de normativa, doctrina y antecedentes internacionales y nacionales, y a sistematización de la experiencia para modelar procedimientos y capacidades. Concluyó que los drones aportaron conciencia situacional decisiva, y que su adopción debía enmarcarse en planificación de fuerza, adiestramiento específico, procedimientos estandarizados y adquisición adecuada de plataformas y sensores para acelerar decisiones y reducir riesgos.

Pérez y Villar (2021), en la Pontificia Universidad Católica del Perú, propusieron un sistema de videovigilancia con aeronaves pilotadas a distancia para fortalecer la seguridad ciudadana en San Martín de Porres. Desarrollaron un estudio aplicado de diseño de solución con revisión de antecedentes, construcción de prototipo y evaluación de deseabilidad, factibilidad y viabilidad. No definieron muestras cuantitativas; trabajaron con corpus documental y evidencia secundaria oficial del sector Interior. Emplearon análisis de normativa, estadísticas del MININTER y experiencias operativas comparadas, además de especificación técnica del prototipo y presupuesto tentativo por unidad. Reportaron victimización en Lima Norte entre 2014 y 2018 con valores elevados y brechas frente a Lima Metropolitana y el nivel nacional. Concluyeron que un sistema de drones interconectados, con sensores ópticos y térmicos, podía mejorar vigilancia y respuesta, condicionado a marcos regulatorios, protocolos operativos, capacitación del personal y sostenibilidad presupuestal para asegurar continuidad y eficacia.

Canchaya (2021), en la Universidad Nacional del Centro del Perú, demostró que complementar la supervisión presencial de protección contra sobretensiones en líneas de transmisión con supervisión remota mediante drones mejoraba fiabilidad y eficiencia. Presentó investigación aplicada, de nivel descriptivo, explicativo y correlacional; empleó métodos analítico-sintético e hipotético-deductivo, con diseño preexperimental O→X→M. La población se enfocó en proyectos y registros de supervisión del sistema eléctrico de Junín; la muestra incluyó casos con VANT, registrando interceptación del rayo, conducción y dispersión. Utilizó observación directa, entrevistas a operarios y acopio de reportes técnicos para cuadros comparativos. Reportó ahorro de 62 días (55.9%) y rendimiento de 44 versus 20 estructuras/día con drones frente a supervisión tradicional. Concluyó que los drones incrementaron productividad, redujeron costos, riesgos y tiempos, y mejoraron calidad de supervisión, exigiendo protocolos, capacitación y despliegue de sensores para consolidar una supervisión más segura, eficaz y sostenible.

2.2. Bases teóricas

2.2.1. Variable 1: Uso de drones

Definición

El “Uso de drones” se comprende como el empleo institucional y planificado de un sistema RPAS que integra aeronave no tripulada, estación de piloto remoto y enlace C2, con procedimientos, roles y documentación que permiten ejecutar misiones bajo criterios de seguridad operacional (ICAO, 2017). Desde la perspectiva regulatoria, implica también responsabilidades del piloto remoto, requisitos de aeronavegabilidad/operación y límites operativos definidos para garantizar conductas seguras y trazables en el espacio aéreo (FAA, 2021).

En la práctica, el uso de drones se operacionaliza por riesgo y entorno: categorías open, specific y certified organizan el tipo de misión, el nivel de autorización y la mitigación requerida, mientras que subcategorías A1–A2–A3 determinan distancias respecto de personas, masa de la aeronave y formación del operador (EASA, 2025). Así, planificar trayectorias, alturas y zonas deja de ser una decisión ad hoc para convertirse en un cumplimiento técnico-jurídico explícito de guías y reglamentos publicados por las autoridades aeronáuticas competentes (AESA, 2025).

Como capacidad técnica, el uso de drones articula plataforma–carga útil–procesamiento: sensores electro-ópticos/infrarrojos, LiDAR y telemetría se integran con algoritmos de fusión de datos para producir conciencia situacional y apoyar decisiones en vigilancia, verificación de alertas e inspecciones en tiempo casi real (Al-Dosari et al., 2024). La literatura de revisión reciente documenta que la eficacia de estas misiones depende de la planificación de rutas, la detección robusta de objetos y la calidad del vínculo comunicación–control, que en conjunto elevan el rendimiento operativo y la confiabilidad de la misión (Laghari et al., 2024).

Otra dimensión del uso de drones es la competencia del operador y la gobernanza de la operación: la certificación del piloto remoto, la evaluación del entorno, las listas de verificación y el reporte de sucesos constituyen salvaguardas esenciales para una operación segura y responsable (FAA, 2021). En paralelo, los estándares y procedimientos internacionales para RPAS definen roles (piloto remoto, piloto al mando, estación de control), documentación y requisitos de enlace C2, aportando un lenguaje común para diseñar y auditar misiones (ICAO, 2017).

El Uso de drones también abarca la protección del dato y del enlace: revisiones técnicas recomiendan cifrado ligero, gestión de claves y autenticación adecuada al limitado presupuesto energético de los UAV para preservar integridad, disponibilidad y confidencialidad en la comunicación con la estación de control (Sarkar, 2025). En instalaciones críticas, las guías federales sobre tecnologías de detección UAS aportan criterios de selección e integración para mejorar la conciencia del dominio aéreo, distinguir entre detección y neutralización, y alinear la operación con el marco legal aplicable (CISA, 2025).

Cuando se traslada a contextos nacionales con regulación propia, el uso de drones incorpora registro del RPAS, acreditación del piloto/operador y trazabilidad de la misión; por ejemplo, en Perú la autoridad aeronáutica (DGAC/MTC) establece pasos, requisitos y verificaciones para operar legalmente estas aeronaves (MTC, 2025). Asimismo, en campus militares y entornos educativos de defensa, tesis institucionales muestran que el empleo de drones y las capacidades anti-drones se conectan con la seguridad de las instalaciones, reforzando que el concepto comprende tanto el empleo como la protección frente a usos no cooperativos (Vásquez Tarrillo, 2021).

Teorías

La Teoría Unificada de Aceptación y Uso de la Tecnología (UTAUT) explica por qué los operadores e instituciones adoptan y utilizan drones, sosteniendo que la expectativa de desempeño, la expectativa de esfuerzo, la influencia social y las condiciones facilitadoras determinan la intención de uso y el uso efectivo, por lo que programas de formación, soporte técnico, dotación de infraestructura y claridad normativa influyen directamente en la probabilidad de que el sistema RPAS sea empleado de forma sostenida (Venkatesh, Morris, Davis & Davis, 2003). En entornos de seguridad y aviación, este marco se potencia al alinearse con guías operacionales de la OACI que especifican componentes del RPAS, roles, documentación, requisitos de enlace C2 y criterios de seguridad operacional, dando base institucional para que los determinantes de UTAUT se traduzcan en conductas observables de adopción y uso en misiones de vigilancia, reconocimiento y verificación de alertas (ICAO, 2024).

La Teoría del Ajuste Tarea–Tecnología (Task–Technology Fit, TTF) postula que el rendimiento mejora cuando las funcionalidades de la tecnología se corresponden con las exigencias de la tarea y con las habilidades del usuario, de modo que la efectividad del uso de drones depende de que payloads, autonomía, maniobrabilidad, calidad sensorial y flujos de datos calcen con las tareas de patrullaje, seguimiento de intrusiones, verificación de alarmas o inspección del perímetro (Goodhue & Thompson, 1995). La extensión de TTF con constructos de aceptación (p. ej., autoeficacia y actitudes) muestra que la combinación de buen ajuste técnico y disposición a usar robustece el desempeño, ofreciendo una base para diseñar la selección de plataformas, protocolos de misión y criterios de entrenamiento que maximicen resultados en seguridad de instalaciones (Dishaw & Strong, 1999).

La Teoría de la Conciencia Situacional (Situation Awareness, SA) describe cómo los operadores construyen y mantienen una representación útil del entorno mediante percepción (nivel 1), comprensión (nivel 2) y proyección (nivel 3), y por qué fallas en cualquiera de estos niveles degradan la toma de decisiones durante operaciones dinámicas, aspecto crítico cuando el piloto remoto gestiona cargas útiles, amenazas y restricciones del espacio aéreo desde estaciones a distancia (Endsley, 1995). En operaciones con UAS, la evidencia empírica y las revisiones en aviación muestran que instrumentos, interfaces, entrenamiento y procedimientos de coordinación impactan la

SA observable, por lo que la configuración del sistema, la gestión del enlace y la estandarización de briefings/debriefings son palancas directas para sostener SA alta durante misiones de vigilancia y respuesta (Cuevas, 2017).

En conjunto, estas teorías se dimensionan en la variable “Uso de drones” como: Capacitación operativa (UTAUT y SA orientan competencias, actitudes y mantenimiento de SA), Aplicación táctica (TTF y SA guían el calce entre tareas y misiones de vigilancia/alerta), y Gestión tecnológica (UTAUT y TTF informan selección de plataformas, integración de sensores y soporte/infraestructura).

Dimensión 1. Capacitación operativa

La capacitación operativa se entiende como el proceso sistemático mediante el cual una organización desarrolla y verifica en su personal los conocimientos, habilidades y actitudes necesarias para operar un sistema de aeronave pilotada a distancia (RPAS) con seguridad operacional, trazabilidad y cumplimiento normativo, incluyendo currículo, requisitos de evaluación y criterios de calificación de instructores y centros de entrenamiento (ISO, 2023). En la práctica, esta capacitación abarca desde fundamentos de reglamentación y gestión del riesgo hasta procedimientos normalizados de operación, listas de verificación y reporte de sucesos, con énfasis en la competencia observable del piloto remoto y del equipo de apoyo para asegurar misiones repetibles y auditables (FAA, 2025).

En el esquema europeo, la capacitación se estructura por categorías y subcategorías operativas que determinan contenidos formativos y modalidad de evaluación: el piloto remoto debe superar formación teórica básica A1/A3, y para operar en A2 o en escenarios estándar (STS) acreditar competencias adicionales mediante examen oficial con umbrales de aprobación explícitos y, cuando corresponda, formación práctica supervisada (AESA, 2025). A su vez, los reguladores establecen entidades de evaluación reconocidas y certificaciones de competencia del piloto que precisan los resultados de aprendizaje, los métodos de examen y los criterios de calidad, creando un circuito formativo-certificador que vincula directamente la capacitación con la autorización operacional (CAA, 2025).

Desde la perspectiva de desempeño humano, la capacitación operativa integra simulación y entrenamiento basado en escenarios para consolidar habilidades de vuelo,

gestión de carga útil y toma de decisiones bajo presión: la evidencia experimental muestra que el pre-entrenamiento en simuladores mejora la precisión, la eficiencia y la percepción de carga de trabajo de pilotos de RPAS, acelerando la transferencia al entorno real (Somerville, 2024). De forma complementaria, los métodos de prueba estandarizados del NIST para sUAS proveen pistas de evaluación repetibles (en interiores, exteriores contenidos y escenarios operacionales) que permiten medir objetivamente la pericia del piloto, comparar resultados entre equipos y anclar la progresión formativa a métricas verificables (NIST, 2022).

En contextos nacionales, la capacitación operativa se operacionaliza al ritmo de la gobernanza local: en el Perú, el Ministerio de Transportes y Comunicaciones, a través de la DGAC, publica requisitos secuenciados para examen, acreditación y tarjeta de piloto RPAS, y reporta volúmenes de acreditaciones que cuantifican la expansión del ecosistema formativo, lo que favorece la disponibilidad de operadores competentes para misiones de seguridad institucional (MTC, 2025). Esta articulación entre formación, evaluación y acreditación permite que los contenidos curriculares y las prácticas de vuelo se traduzcan en competencias medibles, alineadas con la autorización de operaciones y con los estándares internacionales de entrenamiento de personal involucrado en RPAS (MTC, 2025).

Por su carácter continuo, la capacitación operativa incorpora recurrencia de conocimientos y mantenimiento de competencia mediante cursos y evaluaciones periódicas que actualizan al piloto remoto sobre cambios regulatorios, gestión del riesgo y lecciones aprendidas, asegurando vigencia para operar en categorías profesionales y específicas (FAA, 2024). En paralelo, la literatura reciente sobre conciencia situacional en aviación y sistemas no tripulados respalda que programas de instrucción que refuercen percepción, comprensión y proyección del entorno elevan la calidad de decisiones y la seguridad, por lo que la capacitación debe incluir módulos explícitos de SA y evaluación asociada (Fang, 2025).

Dimensión 2. Aplicación táctica

La aplicación táctica del dron es el “aterrizaje” de la doctrina en misiones concretas: traducir objetivos de protección de un sitio en tareas, rutas, alturas, sensores y reglas de empleo que maximizan la conciencia situacional y minimizan la exposición

del personal, integrando el dron al dispositivo de seguridad (patrullaje del perímetro, verificación de alarmas, reconocimiento puntual y apoyo a la intervención) (NPSA, 2023). En términos operativos, supone articular cargas útiles (EO/IR, altímetros, radiogoniómetros), coordinación mando-control y procedimientos de despliegue/devolución del vector, bajo una arquitectura que combine vigilancia preventiva y respuesta a incidentes con criterios de interoperabilidad y mando claro propios del entorno de seguridad de instalaciones (JAPCC, 2020).

Como ciclo de misión, la aplicación táctica ordena la operación en fases: preparación (evaluación de riesgos, zonas, alturas y NOTAM locales), ejecución (patrón de búsqueda, puntos de observación, reglas de identificación) y explotación (registro, custodia de video y lecciones aprendidas); este enfoque por fases es consistente con los manuales de gestión de incidentes con drones, que recomiendan preparación rigurosa, coordinación con actores locales y procedimientos diferenciados para incidentes accidentales o maliciosos (EASA, 2021). A nivel de seguridad pública e infraestructuras críticas, los marcos de respuesta propuestos para contrarrestar UAS no cooperativos añaden funciones tácticas como detección, clasificación, verificación visual y decisión coordinada, de modo que las tácticas del dron "propio" y las tácticas "anti-dron" conviven dentro del mismo plan de seguridad del sitio (INTERPOL, 2023).

En un dispositivo por capas, la aplicación táctica coloca al dron dentro de un sistema de sistemas que integra sensores en tierra, control de accesos, CCTV analítico y, cuando es legalmente viable, tecnologías de detección UAS para elevar la conciencia del dominio aéreo alrededor de la instalación; las guías operativas insisten en definir requisitos de capacidad, seleccionar tecnologías acordes al entorno y ensanchar el plan de seguridad con procedimientos de entrenamiento y ejercicios conjuntos (CISA, 2025). Esta visión por capas convive con metodologías nacionales de amenaza UAS que detallan vectores de riesgo (reconocimiento hostil, entrega de cargas, uso cinético o ciberataques), y permiten ajustar patrones de patrullaje, reglas de reacción y umbrales de escalamiento en la operación diaria (NPSA, 2025).

Para sostener su eficacia, la aplicación táctica demanda medición de desempeño con pruebas estandarizadas y métricas comparables que conecten maniobrabilidad, identificación de objetivos y fiabilidad del enlace con resultados operativos; en este terreno, los métodos de prueba NIST para sUAS ofrecen pistas y escenarios puntuables

que cuantifican destrezas del piloto y capacidades de la plataforma en tareas tipo (búsqueda de objetivos, vuelo preciso, gestión de carga útil) (NIST, 2022). Complementariamente, la literatura técnica reciente impulsa metodologías de evaluación de sistemas counter-drone (detección/seguimiento/identificación) con criterios de desempeño replicables, de modo que la táctica se fundamente en datos de prueba y comparaciones objetivas entre configuraciones antes de su despliegue operativo (De Cubber, 2025).

Dimensión 3. Gestión tecnológica

La gestión tecnológica en sistemas de aeronaves pilotadas a distancia se entiende como la administración integral del ciclo de vida del activo desde la planificación y adquisición hasta la operación, mantenimiento, actualización y retiro articulando personas, procesos y plataformas bajo procedimientos normalizados para asegurar seguridad operacional, trazabilidad y valor sostenido del sistema (ISO, 2023). En este enfoque, la flota RPAS se gestiona como un portafolio de capacidades alineado con objetivos de la organización, aplicando principios de gestión de activos para gobernar decisiones sobre desempeño, costo, riesgo y sostenibilidad a lo largo del tiempo (ISO, 2024).

Operativamente, la gestión tecnológica establece criterios de selección y configuración (plataforma, cargas útiles, estaciones de control, baterías y repuestos), define planes de mantenimiento preventivo/correctivo y controla versionado de firmware y software para sostener confiabilidad y reducir fallas, usando procedimientos y roles descritos para operaciones seguras de UAS (ISO, 2023). La calidad de la integración se valida con métodos de prueba estandarizados que permiten medir maniobrabilidad, precisión de sensores y desempeño de tareas tipo en pistas comparables, cerrando el ciclo entre especificación, verificación y mejora continua (NIST, 2022).

Dado que los RPAS generan y transportan datos sensibles de video, telemetría y comando-control, la gestión tecnológica incorpora un sistema de gestión de seguridad de la información para proteger confidencialidad, integridad y disponibilidad a través de políticas, controles y mejora continua, con un marco de referencia reconocido para establecer, implementar y mantener el ISMS (ISO/IEC, 2022). En instalaciones críticas,

también integra lineamientos para detección de UAS no cooperativos y su acoplamiento a planes de seguridad por capas, definiendo requisitos, evaluación y selección de tecnologías de detección compatibles con el contexto legal y operativo (CISA, 2025).

La conformidad regulatoria es un eje de la gestión tecnológica: la arquitectura, los procedimientos y la documentación deben alinearse con el marco internacional para RPAS airworthiness, operaciones, licensing, C2 y detect-and-avoid como base de gobernanza técnica y coordinación con el servicio de tránsito aéreo (ICAO, 2024). A nivel nacional, la gobernanza se operacionaliza en requisitos escalonados para operar RPAS (solicitud, examen, acreditación de piloto y condiciones operativas), que aseguran trazabilidad del operador y del equipo, y definen límites y responsabilidades en misiones sobre áreas pobladas (MTC, 2025).

Finalmente, la gestión tecnológica cierra el bucle con medición de desempeño y mejora continua: indicadores de disponibilidad, confiabilidad, costo del ciclo de vida y efectividad de misión se integran al sistema de gestión de activos para priorizar inversiones, renovar plataformas y actualizar sensores según evidencia, preservando el valor del activo y la continuidad operativa (ISO, 2024). En paralelo, guías operacionales recientes proveen criterios para ajustar configuraciones y procedimientos en categorías open/specific, incluyendo operaciones BVLOS a muy baja altura, de manera que la tecnología se administre como capacidad adaptable al riesgo y al entorno (EASA, 2025).

2.2.2. Variable 2: Seguridad de las instalaciones

Definición

La seguridad de las instalaciones es el conjunto integrado de medidas preventivas y reactivas que, en un entorno construido específico, buscan disuadir, detectar, demorar y responder frente a amenazas intencionales y riesgos oportunistas mediante diseño ambiental, procedimientos, tecnología y personas (ISO, 2021). Bajo este enfoque, la doctrina CPTED aporta lineamientos para reducir oportunidades y temor al delito desde la arquitectura y la gestión del espacio, mientras que metas operativas de seguridad física proponen controles mínimos y verificables para elevar el desempeño de organizaciones diversas (CISA, 2023).

Operativamente, la seguridad se despliega por capas que combinan perímetro (cercos, portales, PIDS), control de accesos, CCTV con analítica, iluminación, patrullaje y protocolos de respuesta, secuenciadas por criticidad del activo y probabilidad/impacto de las amenazas (NPSA, 2021). La estandarización de estas capas se articula con procesos de gestión para edificios y campus (determinación del nivel de seguridad de la instalación y customización de contramedidas) que unifican criterios de evaluación y documentación a lo largo del ciclo de vida del sitio (ISC, 2024).

La gobernanza del riesgo sostiene la selección de medidas: identificar activos–amenazas–vulnerabilidades, estimar riesgo, tratarlo con controles proporcionales y monitorizar desempeño, siguiendo principios y proceso de ISO 31000 que son aplicables a cualquier organización (ISO, 2018). En instalaciones públicas y críticas, el Risk Management Process del Interagency Security Committee ofrece un marco operativo para fijar el nivel de seguridad, mapear contramedidas y alinear verificación y mejora continua con las decisiones de inversión y operación (ISC, 2021).

La evidencia científica respalda la aportación del diseño ambiental y la gestión del lugar: revisiones de la literatura muestran que CPTED mejora resultados de seguridad al optimizar vigilancia natural, control territorial y mantenimiento, ofreciendo una base empírica para priorizar intervenciones en sitios sensibles (Cozens & Love, 2015). En paralelo, los estándares actualizados consolidan guías específicas por tipologías de instalaciones (p. ej., entornos residenciales) que extienden y operacionalizan el cuerpo de conceptos de ISO 22341 al nivel de pautas prácticas de sitio (ISO, 2025).

La dimensión humana es inseparable de la tecnología: una cultura de seguridad madura (normas compartidas, conductas esperadas, liderazgo comprometido y comunicación efectiva) es requisito para que políticas y sistemas funcionen en la práctica y para reducir riesgos de insider y de reconocimiento hostil (NPSA, 2020). En ese marco, las buenas prácticas y guías de planificación de recursos de seguridad física proveen métodos para profesionalizar equipos, entrenar, evaluar y sostener el rendimiento del programa en el tiempo (CISA, 2025).

Finalmente, la seguridad de instalaciones modernas es convergente: integra la capa física con la digital en un programa único de gestión, armonizando inventarios de

activos, telemetría, alarmas, video y acceso con riesgos cibernéticos asociados a sistemas de seguridad, lo que permite detección y respuesta coordinadas y métricas comunes de desempeño (CISA, 2024). Esta integración se apoya en marcos de riesgo y en la alineación entre funciones de operaciones, TI y seguridad corporativa para priorizar inversiones, cerrar brechas y sostener la continuidad operativa del sitio (ISC, 2024).

Teorías

La Teoría de la Prevención del Delito mediante el Diseño Ambiental (CPTED) concibe la seguridad de las instalaciones como un resultado del diseño del entorno construido y de su gestión cotidiana (visibilidad natural, control de accesos, refuerzo territorial y mantenimiento) para disuadir, dificultar y detectar conductas oportunistas, proponiendo un proceso estructurado de análisis del sitio, tratamiento del riesgo y verificación de resultados (ISO, 2021). La evidencia académica muestra que, aplicada con rigor metodológico y con participación de usuarios y gestores, CPTED reduce oportunidades delictivas y el temor al delito, aportando criterios de intervención comparables y transferibles entre tipologías de instalaciones y escalas espaciales (Cozens & Love, 2015).

La Prevención Situacional del Delito (SCP) explica la seguridad como manejo de oportunidades, prescribiendo tácticas que aumentan el esfuerzo y el riesgo del infractor, reducen las recompensas y las excusas, y eliminan provocaciones, de modo que “endurecer” el objetivo, controlar accesos, gestionar la circulación, etiquetar bienes y afinar la vigilancia conforman un catálogo de medidas seleccionadas por problema y contexto (Clarke, 1995). Las guías públicas y revisiones gubernamentales refuerzan su carácter preventivo primario, exigiendo diagnóstico específico, hipótesis de mecanismo y evaluación de resultados para justificar cada intervención en edificios, campus o infraestructuras críticas (Australian Institute of Criminology, 2003).

La Teoría de la Actividad Rutinaria (RAT) sostiene que la ocurrencia delictiva requiere la convergencia espacio-temporal de un ofensor motivado, un objetivo adecuado y la ausencia de un guardián capaz, de modo que la seguridad de instalaciones se diseña como administración de guardianías formales (personal, barreras, control de accesos) e informales (uso del espacio, visibilidad), reduciendo la exposición y la adecuación del objetivo (Cohen & Felson, 1979). Esta perspectiva informa la arquitectura de programas de seguridad al traducirse en esquemas

de vigilancia natural y tecnológica, rutinas de ocupación, normas de conducta y protocolos de respuesta, y en esta tesis se operacionaliza explícitamente en Control perimetral, Protección infraestructural y Seguridad informacional (Miró, 2014).

Dimensión 1. Control perimetral

El control perimetral es la gestión deliberada del límite externo de una instalación para disuadir, detectar, demorar y permitir la respuesta frente a intrusiones, combinando barreras físicas, procedimientos y tecnologías en una arquitectura por capas que se integra con el resto del programa de seguridad (NPSA, 2025). En términos prácticos, define cómo se diseña, equipa, opera y mantiene el perímetro vallas, portones, caminos de ronda, puntos de control y su supervisión alineándolo con principios de prevención situacional y de diseño ambiental que reduzcan oportunidades y eleven el umbral operativo del intruso (ISO, 2021).

Sus componentes técnicos articulan medios de detección y verificación temprana (PIDS montados en barrera o en suelo, analítica de CCTV, iluminación de seguridad, y control de accesos) con procedimientos de evaluación y despacho, de modo que una alarma confiable se confirme visualmente y active una respuesta proporcional (NPSA, 2023). Así, el control perimetral no solo "cierra" físicamente el contorno, sino que crea un anillo sensorizado y gestionado que limita puntos de entrada, organiza rutas de vigilancia y estandariza prácticas de seguridad efectivas para recintos diversos (CISA, 2023).

Desde la gobernanza del riesgo, el control perimetral se planifica con un proceso formal que identifica activos–amenazas–vulnerabilidades, fija el nivel de seguridad de la instalación y selecciona contramedidas proporcionadas, documentando criterios y responsables a lo largo del ciclo de vida (ISC, 2024). En ese marco, guías operativas y cuadernos de planificación ofrecen plantillas y listas de verificación para implementar planes de seguridad, medir el desempeño y priorizar mejoras con base en evidencia y recursos disponibles (CISA, 2023).

Finalmente, un control perimetral maduro incorpora evaluación técnica y mejora continua: ensayos y esquemas de evaluación comparables para PIDS, criterios de mantenimiento y pruebas de aceptación/puesta en marcha, y métricas de detección–falsas alarmas–tiempos de respuesta que retroalimentan decisiones de inversión (NPSA,

2024). La literatura científica complementa esta práctica al describir protocolos de detección de intrusión perimetral basados en visión y fusión sensorial que fortalecen la verificación y reducen la carga del operador en entornos exteriores complejos (Lohani et al., 2022).

Dimensión 2. Protección infraestructural

La protección infraestructural es el conjunto de decisiones de diseño y gestión que "endurecen" el edificio y sus sistemas críticos (envolvente, estructura, espacios técnicos y redes de soporte) para que, desde la concepción del sitio hasta la operación diaria, el recinto resista, absorba o desvíe amenazas con proporcionalidad y trazabilidad; en este sentido, conecta la arquitectura del lugar con un proceso de prevención y reducción del riesgo que parte del análisis del entorno construido y culmina en contramedidas verificables del tipo separación, refuerzo y control técnico (ISO, 2021). En la práctica, implica traducir principios de seguridad protectiva en requisitos de proyecto y de operación que unifican criterios para fachadas, cubiertas, salas de equipos, rutas de evacuación y puntos de servicio, con una visión holística que integra al personal, los procedimientos y la tecnología del edificio (NPSA, 2021).

Su núcleo técnico combina diseño por amenaza y resiliencia del activo: establecer distancias de resguardo y configuraciones del sitio, incorporar mitigación frente a impacto vehicular hostil, especificar detalles de refuerzo estructural y de la envolvente (anclajes, marcos, protección del vidrio), y evaluar efectos como sobrepresión y caída progresiva para que el edificio mantenga estabilidad y funcionalidad ante eventos extremos (FEMA, 2020). Esta lógica por capas se complementa con guías especializadas de Hostile Vehicle Mitigation que ordenan la selección e integración de barreras, la gestión de accesos vehiculares y la compatibilidad entre flujos urbanos y medidas de contención sin sacrificar proporcionalidad ni usabilidad del espacio (NPSA, 2024).

La protección infraestructural se gobierna con un proceso de gestión del riesgo que fija el nivel de seguridad del inmueble, alinea amenazas, vulnerabilidades y consecuencias, y deriva en un Plan de Seguridad del Sitio con objetivos, responsables, mantenimiento y verificación periódica; este encuadre permite que los tratamientos (arquitectónicos, estructurales y de operación) sean proporcionales y auditables en el

tiempo (Interagency Security Committee, 2024). En la fase de planificación, la guía nacional de security planning recomienda estructurar requisitos detallados del sitio y del edificio (standoff, controles de acceso a salas críticas, caminos de ronda, rutas de intervención, coordinación con otros anillos de seguridad) para asegurar coherencia entre diseño, obra y operación (NPSA, 2025).

Finalmente, la protección infraestructural se expresa en la continuidad de servicios esenciales: proteger cuartos eléctricos, gabinetes de comunicaciones, HVAC y redes de agua contra intrusión, sabotaje o efectos colaterales, introducir redundancias y segregación de compartimentos, y medir desempeño con indicadores de disponibilidad, confiabilidad y costo del ciclo de vida para orientar inversiones y mejoras (Interagency Security Committee, 2025). En sectores de alta criticidad, lineamientos técnicos recientes reafirman que la priorización de medidas físicas, la evaluación de riesgos y la verificación de controles deben seguir un enfoque basado en amenaza y vulnerabilidad, aplicando buenas prácticas replicables para infraestructura y edificios operativos (NERC, 2025).

Dimensión 3. Seguridad informacional

La seguridad informacional es el conjunto de políticas, procesos, controles y responsabilidades que protegen el valor de los activos de información (en cualquier formato y a lo largo de su ciclo de vida) asegurando confidencialidad, integridad y disponibilidad mediante un sistema de gestión explícito y medible (ISO, 2022). En términos de gobernanza práctica, esta protección se articula como un programa continuo que identifica y prioriza riesgos, define resultados esperados y alinea capacidades organizacionales con funciones como Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar para sostener la continuidad del negocio y la resiliencia operativa (NIST, 2024).

La implementación efectiva de la seguridad informacional se traduce en controles técnicos, administrativos y físicos seleccionados por riesgo y evaluados con criterios de suficiencia y eficacia, empleando catálogos normalizados de control que facilitan el diseño, la auditoría y la mejora continua (NIST, 2020). En paralelo, la vigilancia del escenario de amenazas y tendencias (ransomware, explotación de vulnerabilidades, compromisos de la cadena de suministro y campañas de ingeniería

social) permite ajustar la postura de seguridad y orientar inversiones hacia medidas con mayor impacto marginal en el contexto real de la organización (ENISA, 2023).

En instalaciones modernas, la seguridad informacional es convergente: integra la ciberseguridad con la seguridad física en un único modelo de gobierno, datos y respuesta, eliminando silos entre equipos, procesos y tecnologías para tratar amenazas que cruzan dominios y para coordinar decisiones durante incidentes complejos (CISA, 2024). Esta convergencia se apoya en estándares y guías para la protección de edificios y campus que definen niveles de seguridad, contramedidas proporcionadas y verificación sistemática, de modo que los requisitos informacionales se alinean con el programa general de seguridad del sitio (ISC, 2024).

La dimensión humana y cultural es inseparable del componente técnico: políticas claras, roles definidos, formación continua, gestión de terceros y métricas de desempeño sostienen el programa y reducen errores, fraudes y fallas de cumplimiento, por lo que la función de Gobernar del marco de ciberseguridad exige evidencias de liderazgo, políticas, gestión de riesgos y comunicación interna y externa (NIST, 2024). En ese marco, el desarrollo de una cultura de ciberseguridad (valores, normas y comportamientos compartidos) es condición para que los controles se ejecuten de forma consistente y para que la organización aprenda y se adapte frente a cambios tecnológicos y del entorno de amenazas (ENISA, 2018).

Cuando la operación involucra tecnologías de alto flujo de datos y exposición mixta (videovigilancia, telemetría, sensores distribuidos, redes OT/ICS o plataformas aéreas no tripuladas) la seguridad informacional requiere segmentación de redes, cifrado y gestión de claves, registros y monitoreo, tratamiento de incidentes y continuidad, todo mapeado a requisitos regulatorios y a evidencias de cumplimiento (ENISA, 2025). La columna vertebral de este esfuerzo es un sistema de gestión certificable que asegure política, análisis de riesgos, controles, auditorías y mejora continua, con alcance sobre la información, los procesos y los proveedores críticos que participan en su tratamiento (ISO, 2022).

2.3. Marco conceptual

Búsqueda y cribado (search & screening): conjunto de medidas para inspeccionar personas, pertenencias, vehículos y correspondencia al ingreso o salida, con tecnologías y

procesos proporcionales al riesgo, y valor adicional de disuasión y procedimientos de búsqueda de áreas (NPSA, 2024).

Carga útil (payload): sensores o equipos transportados para cumplir la misión (cámaras, EO/IR, multiespectrales, LiDAR, altavoces, dispensadores o radios) cuya integración condiciona energía, masa, balance, enlace de datos y requisitos de desempeño de la plataforma *(Rattanaamporn et al., 2025)*.

Categorías operativas (abierta, específica, certificada): clasificación regulatoria basada en el nivel de riesgo; la categoría abierta cubre operaciones de bajo riesgo con subcategorías A1/A2/A3, la específica exige autorización u otros medios como escenarios estándar, y la certificada se reserva para riesgos altos con exigencias similares a la aviación tripulada *(EASA, 2024)*.

CCTV analítico: sistema de videovigilancia que combina cámaras con análisis de video y operación desde una sala de control para disuadir, detectar y registrar conductas anómalas en perímetros, áreas internas y puntos críticos, apoyando la verificación de alarmas y la coordinación de la respuesta en tiempo real (NPSA, 2022).

Centro de control de seguridad (SCR): núcleo operativo que recibe señales de CCTV, PIDS, alarmas e información del personal, y coordina comunicaciones, políticas, resiliencia y respuesta, requiriendo diseño ergonómico, dotación competente y procedimientos estandarizados (NPSA, 2023).

Control de accesos (ACS): conjunto de medidas, dispositivos y procedimientos que limitan y registran quién entra, dónde y cuándo dentro de una instalación, integrando credenciales físicas o biométricas, niveles de autorización, auditoría de eventos y políticas de zonas para proteger activos sensibles y facilitar una respuesta proporcional ante incidentes (NPSA, 2024).

CPTED (prevención del delito mediante diseño ambiental): enfoque de planeamiento que usa vigilancia natural, control territorial, control de accesos y mantenimiento para disuadir comportamientos ilícitos y reducir temor, con lineamientos internacionales aplicables a entornos nuevos o existentes (ISO, 2021).

Cribado vehicular: controles en puntos de acceso que combinan inspección visual, tecnologías de detección y protocolos escalonados para reducir el ingreso de explosivos, armas

u otros materiales prohibidos, con efecto disuasivo y procedimientos adaptados al flujo y amenaza (NPSA, 2023).

Distancia de resguardo (standoff): separación controlada entre amenazas potenciales y estructuras u ocupantes que reduce efectos de explosión y fragmentos, lograda mediante retrocesos edilicios, control vehicular y barreras anti-embestida como parte de un enfoque de protección contra explosivos (NPSA, 2024).

Enlace C2 (mando y control): canal de datos de telemando y telemetría que permite gestionar el vuelo y mantener conciencia situacional, con requisitos de desempeño y confiabilidad adecuados para operaciones dentro y fuera de línea de vista, en bandas protegidas para aviación cuando aplique *(ICAO, 2017)*.

EO/IR (electro-óptico/infrarrojo): sensores de imagen visibles y térmicos usados para reconocimiento, búsqueda y vigilancia diurna/nocturna, donde la fusión de bandas mejora la detección, identificación y seguimiento en escenarios operacionales complejos *(Khawaja et al., 2022)*.

Espacios protegidos: áreas internas (p. ej., salas de control o servidores) diseñadas para ofrecer protección reforzada frente a explosiones y fragmentos cuando evacuar no es posible, definidas a partir de una amenaza de diseño y una evaluación de riesgos (NPSA, 2021).

Estación de piloto remoto (RPS): interfaz y conjunto de equipos desde donde se controla la aeronave, incluyendo consolas, enlaces, antenas y software de misión, considerada parte del sistema sujeto a control de configuración y a criterios de aeronavegabilidad del conjunto RPAS *(ICAO, 2025)*.

Georreferenciación RTK/PPK: técnicas de posicionamiento GNSS en tiempo real o posproceso que elevan la precisión planimétrica y altimétrica, reduciendo dependencia de puntos de control y habilitando productos cartográficos con errores del orden de centímetros cuando se aplican buenas prácticas *(Czyża et al., 2023)*.

Gestión de visitantes: proceso estructurado para verificar identidades, validar motivos de visita, establecer condiciones de acceso, supervisar desplazamientos y detectar documentación fraudulenta, con énfasis en concienciación del personal y procedimientos de entrada robustos para reducir riesgos de intrusión o reconocimiento hostil (NPSA, 2025).

Gestión del riesgo: marco directivo y de procesos para identificar, analizar, evaluar y tratar riesgos en instalaciones, integrando principios y terminología normalizados que permiten decisiones proporcionales, mejora continua y resiliencia organizacional (ISO, 2018).

Identificación remota (Remote ID): capacidad del dron para transmitir en vuelo su identificación y posición junto con la ubicación del control, facilitando supervisión, cumplimiento y respuesta de autoridades y terceros autorizados durante la operación *(FAA, 2025)*.

Iluminación de seguridad: diseño fotométrico que asegura niveles, uniformidad y ubicación adecuados para apoyar la detección humana y por cámara, evitar el deslumbramiento y mejorar la vigilancia en perímetros, accesos y rutas críticas durante operación nocturna y condiciones de baja visibilidad (NPSA, 2015).

LiDAR aerotransportado: sensor activo que emite pulsos láser para generar nubes de puntos 3D de alta resolución, con ventajas en vegetación densa y modelado urbano; su integración en UAV permite cartografías centimétricas y reconstrucciones detalladas en entornos críticos *(Bartmiński et al., 2023)*.

Lista de verificación (pre-vuelo): conjunto estructurado de comprobaciones de aeronave, baterías, enlace C2, firmware, condiciones del área y documentación antes del despegue, recomendada en guías y circulares para estandarizar la seguridad operativa y reducir omisiones humanas *(FAA, 2016)*.

Mantenimiento preventivo: programa documentado de inspecciones, sustituciones y pruebas funcionales de aeronave, batería, hélices, motores, sensores, RPS y antenas, escalable al tipo de UAS y la severidad operacional para garantizar aeronavegabilidad continuada *(ISO, 2023)*.

Medidas contra explosión en acristalamientos: especificación y ensayo de sistemas de vidrio y marcos capaces de mitigar o resistir cargas de explosión, reduciendo esquirlas y manteniendo el conjunto en marco para proteger ocupantes y continuidad operativa (NPSA, 2025).

Mitigación de vehículo hostil (HVM): empleo de bolardos, barreras, jardineras estructurales y estrategias de diseño vial para impedir o desacelerar impactos intencionales, establecer líneas de defensa escalonadas y preservar distancias de seguridad, integrándose con control de accesos y planes de respuesta (NPSA, 2025).

Obscuración de fachadas: técnicas en vidrio y envolventes para impedir vigilancia hostil hacia interiores sin perder visibilidad operativa, complementando otras medidas de cierre y control para proteger procesos sensibles y personal (NPSA, 2025).

PIDS (sistema perimetral de detección de intrusos): sensores montados en barrera o libres en campo que detectan cortes, escaladas o vibraciones en el cerramiento y se integran con CCTV e iluminación para confirmar eventos y dirigir la intervención, seleccionándose según tipo de cerca, entorno y tasas de falsas alarmas aceptables (NPSA, 2023).

Piloto remoto: persona certificada y responsable de planificar, ejecutar y supervisar el vuelo, con competencias reguladas para conocer limitaciones operacionales, autorizar misiones y aplicar procedimientos normales y de emergencia; en regímenes como Part 107 la certificación acredita dominio de normas, meteorología, espacio aéreo y gestión del riesgo *(FAA, 2024)*.

Plan de seguridad del sitio (SSP): documento vivo que consolida evaluación de amenazas, medidas de disuasión-detección-retardo-mitigación-respuesta, roles, capacitación, mantenimiento y ejercicios, asegurando proporcionalidad del control físico frente a riesgos terroristas y estatales (NPSA, 2025).

Requisito operacional (OR): especificación previa y clara de qué debe lograr una solución de seguridad (alcance, desempeño, integración y límites) para seleccionar tecnologías y procedimientos adecuados, alinear inversiones con el riesgo y comprobar eficacia en explotación (NPSA, 2020).

RPAS (Sistema de Aeronave Pilotada a Distancia): conjunto integrado por la aeronave no tripulada, la estación del piloto remoto, el enlace de mando y control, y elementos asociados necesarios para la operación segura en espacio aéreo; el enfoque internacional lo trata como un sistema completo sujeto a requisitos de aeronavegabilidad, certificación y gestión de riesgos, diferenciándolo de usos recreativos simplificados *(ICAO, 2025)*.

SORA (evaluación de riesgos operacionales): metodología estandarizada para la categoría específica que estima el riesgo terrestre y en el aire, define el nivel de integridad requerido (SAIL) y asigna objetivos de seguridad operacionales y mitigaciones proporcionadas al concepto de operación *(JARUS, 2024)*.

Telemetría: datos descendentes en tiempo real sobre estado del dron (posición, actitud, energía, enlace y salud de sistemas) que sustentan la toma de decisiones y el cumplimiento de requisitos de desempeño del enlace C2 en operaciones de diversa complejidad *(JARUS, 2023)*.

U-space/UTM: conjunto de servicios digitales para gestionar tráfico de UAS a baja altura, habilitando acceso escalable y seguro mediante funciones como identificación de red, autorización de vuelo, información dinámica del espacio aéreo y gestión estratégica/táctica de conflictos *(EASA, 2025)*.

VLOS/BVLOS: alcance visual del piloto o del observador para mantener contacto directo con la aeronave (VLOS) frente a operaciones que lo exceden (BVLOS), con implicaciones sobre mitigaciones técnicas, organización de tripulación y autorización según el marco aplicable *(FAA, 2020)*.

Zonas geográficas UAS (geo-zones): porciones de espacio aéreo donde las operaciones se facilitan, restringen o excluyen por razones de seguridad, privacidad, seguridad pública o medio ambiente, publicadas en formatos comunes para la conciencia situacional de operadores *(EASA, 2025)*.

Zonificación de seguridad: establecimiento de áreas diferenciadas con reglas de acceso, restricciones tecnológicas y control de dispositivos para minimizar espionaje y filtraciones, delimitando zonas de conversación segura y espacios con exclusión de móviles según sensibilidad de la información tratada (NPSA, 2023).

2.4. Operacionalización de las variables

Tabla 1.
Operacionalización de las variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA DE MEDICIÓN
Variable 1 Uso de drones	El Uso de drones se refiere a la implementación, manejo y aprovechamiento de vehículos aéreos no tripulados para tareas de observación, vigilancia y apoyo en la seguridad, empleando tecnología aérea para maximizar la eficiencia y reducir riesgos humanos (FAA, 2021).	El Uso de drones será evaluado a través de un cuestionario con escala de Likert aplicado a los cadetes, incluyendo preguntas cerradas que medirán aspectos de capacitación, aplicación táctica y gestión tecnológica durante actividades de vigilancia y seguridad en la escuela militar.	Capacitación operativa	• Entrenamiento técnico • Certificación piloto • Simulador vuelo • Evaluación desempeño	1, 2 3, 4 5, 6 7, 8	Siempre (5) Casi siempre (4) A veces (3) Casi nunca (2) Nunca (1)
			Aplicación táctica	• Reconocimiento aéreo • Vigilancia perímetro • Apoyo logístico • Cobertura eventos	9, 10 11, 12 13, 14 15, 16	
			Gestión tecnológica	• Mantenimiento preventivo • Actualización software • Integración sistemas • Gestión datos	17, 18 19, 20 21, 22 23, 24	
Variable 2 Seguridad de las instalaciones	La seguridad de las instalaciones comprende el conjunto de acciones, recursos y tecnologías destinados a proteger la infraestructura militar, el personal y los bienes, mediante sistemas de control, vigilancia y respuesta ante riesgos físicos, tecnológicos y cibernéticos (ISO, 2021).	La seguridad de las instalaciones será medida mediante un cuestionario de escala de Likert dirigido a los cadetes, utilizando preguntas cerradas para valorar percepciones sobre control perimetral, protección infraestructural y seguridad informacional en la Escuela Militar de Chorrillos.	Control perimetral	• Monitoreo continuo • Detección intrusos • Respuesta inmediata • Supervisión accesos	25, 26 27, 28 29, 30 31, 32	Siempre (5) Casi siempre (4) A veces (3) Casi nunca (2) Nunca (1)
			Protección infraestructural	• Inspección estructural • Detección anomalías • Evaluación riesgos • Mantenimiento correctivo	33, 34 35, 36 37, 38 39, 40	
			Seguridad informacional	• Protección datos • Control accesos • Monitoreo redes • Prevención ciberataques	41, 42 43, 44 45, 46 47, 48	

2.5. Formulación de hipótesis

2.5.1. Hipótesis general

HG: Existe relación significativa entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

2.5.2. Hipótesis especificas

HE1: Existe relación significativa entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

HE2: Existe relación significativa entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

HE3: Existe relación significativa entre la gestión tecnológica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

CAPÍTULO III.
MARCO METODOLÓGICO

3.1. Enfoque de investigación

El enfoque cuantitativo fue empleado en esta investigación con el propósito de obtener datos objetivos y medibles que permitieran analizar la relación entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Según Ñaupas et al. (2018, p. 140), el enfoque cuantitativo se caracteriza por la recolección y análisis de datos numéricos, facilitando la aplicación de técnicas estadísticas que evidencian patrones, relaciones y tendencias entre variables. Este método permitió estructurar instrumentos de recolección de datos, como cuestionarios con escala Likert, que fueron aplicados de manera sistemática a la población objeto de estudio, garantizando la validez y confiabilidad de los resultados.

Además, el enfoque cuantitativo facilitó la interpretación rigurosa de los datos a través de análisis estadísticos descriptivos e inferenciales, permitiendo comprobar hipótesis y determinar la fuerza y dirección de la relación entre las variables. Este proceso se ajustó a los lineamientos metodológicos recomendados por Ñaupas et al. (2018), quienes señalan que este enfoque es ideal para investigaciones que buscan explicar fenómenos sociales o técnicos desde una perspectiva empírica y verificable. De este modo, se logró un análisis preciso y sistemático que fundamentó las conclusiones del estudio.

3.2. Tipo de investigación

La investigación se enmarcó como aplicada porque partió de un problema práctico (elevar la seguridad de las instalaciones) y orientó el uso del conocimiento disponible sobre RPAS hacia soluciones concretas y transferibles al contexto de la EMCH “CFB”. Se asumió que la finalidad inmediata fue intervenir sobre la realidad institucional mediante lineamientos operativos, protocolos y criterios de decisión basados en evidencia, tal como se caracterizó la investigación aplicada al privilegiar la utilidad y el cambio en el entorno de estudio (Ñaupas et al., 2018, p. 115).

En coherencia con ese enfoque, se operacionalizaron variables y dimensiones para medir el fenómeno, se evaluó su asociación y se tradujeron los hallazgos en propuestas de

mejora factibles (p. ej., estandarización de misiones, gestión tecnológica y capacitación), priorizando la pertinencia y la factibilidad de implementación por encima de la mera explicación teórica. Así, el estudio vinculó teoría y práctica con el propósito de optimizar procesos y resultados de seguridad en condiciones reales, cumpliendo el rasgo definitorio de la investigación aplicada: producir conocimiento útil que orientó decisiones y acciones inmediatas en el campo de aplicación (Ñaupas et al., 2018, p. 115).

3.3. Método de investigación

El método empleado en esta investigación fue el hipotético-deductivo, basado en los postulados de Karl Popper, el cual se centra en la formulación de hipótesis que luego son sometidas a pruebas empíricas para su posible refutación o verificación (Marfull, 2024). Este enfoque permitió establecer proposiciones claras sobre la relación entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, las cuales fueron contrastadas mediante la recolección y análisis de datos cuantitativos. La aplicación del método hipotético-deductivo facilitó un proceso sistemático y riguroso, orientado a la validación objetiva de las hipótesis planteadas, garantizando la validez científica del estudio.

Además, este método propicia un ciclo continuo de revisión y ajuste teórico, ya que las hipótesis pueden ser modificadas o rechazadas en función de los resultados obtenidos, lo que contribuye al avance progresivo del conocimiento (Marfull, 2024). La metodología adoptada favoreció una investigación estructurada, donde la deducción lógica y la evidencia empírica interactuaron para ofrecer conclusiones fundamentadas, coherentes con el marco teórico y los objetivos planteados. Así, el método hipotético-deductivo resultó adecuado para abordar el fenómeno estudiado desde una perspectiva científica rigurosa y objetiva.

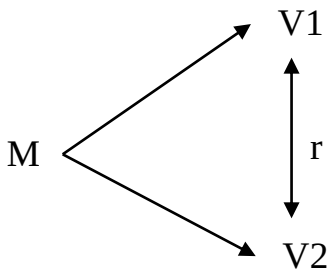
3.4. Alcance de investigación (nivel)

El alcance de la investigación fue descriptivo-correlacional, orientado a identificar y analizar las características y relaciones entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Según Hernández y Mendoza (2018), la investigación descriptiva se enfoca en detallar, caracterizar y explicar fenómenos tal como ocurren en su contexto natural, proporcionando un panorama claro y detallado de las variables estudiadas (p. 108). Este nivel permitió describir con precisión los

aspectos operativos, tácticos y tecnológicos vinculados al Uso de drones, así como la percepción y medidas relacionadas con la seguridad institucional.

Asimismo, el componente correlacional de la investigación tuvo como finalidad determinar el grado y la dirección de la relación entre las variables consideradas, en este caso, cómo el uso de drones se asocia con la mejora en la seguridad de las instalaciones (Hernández & Mendoza, 2018, p. 109). Este enfoque facilitó la cuantificación de la fuerza del vínculo entre ambas variables mediante técnicas estadísticas, contribuyendo a entender no solo las características individuales, sino también las interacciones que permiten prever comportamientos y resultados en contextos similares. De esta forma, el estudio ofreció información relevante para la toma de decisiones y el diseño de estrategias en el ámbito militar.

Figura 1.
Esquema de correlación



Donde:

M = Muestra

V1 = Variable 1: Uso de drones

V2 = Variable 2: Seguridad de las instalaciones

r = Correlación entre dichas variables

3.5. Diseño de la investigación

El diseño del estudio fue no experimental, de carácter transversal, lo que permitió observar y analizar las variables sin intervenir ni manipular las condiciones del entorno, tal como lo explican Hernández y Mendoza (2018, p. 174). Este tipo de diseño es apropiado para investigaciones que buscan describir fenómenos tal como se presentan en su contexto natural, sin modificar las variables, lo cual es esencial para mantener la validez externa y la

representatividad de los datos recolectados. En este caso, el estudio examinó la relación entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos, considerando las condiciones y percepciones actuales de los participantes.

Por otro lado, el carácter transversal del diseño implica que la recolección de datos se realizó en un único momento temporal, proporcionando una instantánea o corte en el tiempo que refleja el estado actual de las variables (Hernández & Mendoza, 2018, p. 176). Esta modalidad permite realizar análisis descriptivos y correlacionales que ofrecen información valiosa sobre la relación entre las variables en un contexto específico, sin requerir seguimiento longitudinal o experimental. Así, este diseño facilitó un análisis eficiente, práctico y adecuado para responder a los objetivos planteados en la investigación.

3.6. Población, muestra, unidad de estudio

3.6.1. Población de estudio

La población del estudio, constituida por 1,226 cadetes, representa el conjunto total de elementos que poseen las características que interesan al investigador para el desarrollo de la investigación, conforme a la definición proporcionada por Hernández y Mendoza (2018, p. 174). La población es entendida como el universo o totalidad de individuos, objetos o eventos que cumplen con criterios específicos y sobre los cuales se pretende obtener información relevante para responder al problema de investigación. En este caso, la población está conformada por todos los cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, quienes forman el grupo objetivo para evaluar la relación entre el uso de drones y la seguridad de las instalaciones.

El conocimiento detallado de esta población es fundamental para diseñar adecuadamente la muestra, seleccionar los instrumentos de recolección de datos y garantizar que los resultados obtenidos sean representativos y generalizables dentro del contexto estudiado. Hernández y Mendoza (2018) destacan que comprender la naturaleza y características de la población permite delimitar el alcance del estudio y asegurar que las conclusiones reflejen fielmente las condiciones del grupo investigado, optimizando la pertinencia y aplicabilidad de la investigación.

3.6.2. Muestra de estudio

La muestra del estudio estuvo constituida por 293 cadetes, selección realizada mediante una fórmula estadística de muestreo que garantizó la representatividad y precisión de los resultados dentro del universo total de 1,226 cadetes.

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

N =	1,226	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

$$n = \frac{(1226) * (1.96)^2 * (0.5) * (0.5)}{(0.05)^2 * (1226 - 1) + (1.96)^2 * (0.5) * (0.5)}$$

$$n = \frac{1177.4504}{4.02}$$

$$n = 292.69$$

Según Hernández y Mendoza (2018), el muestreo probabilístico es un procedimiento mediante el cual cada elemento de la población tiene una probabilidad conocida y distinta de cero para ser seleccionado, lo que permite obtener una muestra representativa y disminuir el sesgo en la selección (p. 196). Esta característica es fundamental para asegurar que los hallazgos del estudio puedan ser generalizados y reflejen con exactitud las características y percepciones de la población estudiada.

El tipo de muestreo utilizado fue aleatorio, que consiste en un proceso en el cual todos los elementos de la población tienen la misma oportunidad de ser incluidos en la muestra (Hernández & Mendoza, 2018, p. 161). Este método facilita la obtención de una muestra equilibrada y homogénea, permitiendo que las inferencias estadísticas sean confiables y válidas. En el contexto de esta investigación, el muestreo probabilístico aleatorio fue adecuado para seleccionar a los cadetes que participaron en la evaluación

del uso de drones y la seguridad de las instalaciones, garantizando que los resultados obtenidos no estuvieran influenciados por criterios subjetivos o sesgos en la selección. Esta rigurosidad metodológica contribuyó a fortalecer la validez interna y externa del estudio, optimizando la calidad y relevancia de las conclusiones obtenidas.

3.6.3. Unidad de estudio

La unidad de estudio en esta investigación fue el cadete de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", entendida como el elemento básico o individual sobre el cual se recopilan los datos y se realizan las observaciones dentro del proceso investigativo. Según Hernández y Mendoza (2018, p. 198), la unidad de estudio es aquella entidad o sujeto específico que representa la base de análisis en una investigación, permitiendo segmentar la población para facilitar la recolección y análisis de la información. Esta unidad puede ser una persona, un grupo, un objeto o un evento, siempre y cuando posea las características relevantes para responder a los objetivos planteados en el estudio.

En el contexto de la presente investigación, el cadete constituye la unidad de estudio porque representa al individuo que interactúa directamente con la variable "Uso de drones" y cuya percepción y experiencia son fundamentales para comprender la influencia de esta tecnología en la seguridad de las instalaciones. La identificación clara y precisa de la unidad de estudio permite focalizar el diseño del instrumento de recolección de datos y asegurar que la información recopilada sea pertinente y específica, favoreciendo un análisis detallado y contextualizado. Asimismo, delimitar la unidad de estudio facilita la organización y sistematización del trabajo de campo, optimizando recursos y tiempo. De esta manera, la elección del cadete como unidad de estudio contribuye a la validez y relevancia del estudio, al centrar el análisis en el actor principal involucrado en el fenómeno investigado.

3.7. Técnica e instrumento para la recolección de datos

3.7.1. Técnica de recolección de datos

La técnica de recolección de datos utilizada en esta investigación fue la encuesta, considerada una herramienta fundamental para obtener información directa y estructurada de los sujetos involucrados en el estudio. Según Machuca (2022), la

encuesta permite recopilar datos de manera sistemática mediante la aplicación de instrumentos previamente diseñados, facilitando la cuantificación y análisis posterior de las respuestas. Esta técnica es especialmente útil cuando se busca conocer percepciones, opiniones, actitudes o comportamientos de una población amplia, garantizando un acercamiento estandarizado que favorece la comparabilidad de la información recolectada.

En el presente estudio, la encuesta fue aplicada a los cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” para evaluar la relación entre el uso de droness y la seguridad de las instalaciones. El diseño del cuestionario incluyó preguntas cerradas estructuradas en escala Likert, lo que permitió medir con precisión el grado de acuerdo o percepción de los participantes respecto a las variables estudiadas. La encuesta facilitó la recolección de datos en un tiempo relativamente corto y con un control adecuado sobre la calidad de la información, gracias a la estandarización de las preguntas y la posibilidad de aplicarla en formato presencial o digital (Machuca, 2022). Además, esta técnica permitió cubrir una muestra representativa y obtener resultados cuantificables que contribuyeron a un análisis riguroso y objetivo, alineado con el enfoque cuantitativo 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 específicamente para recopilar información precisa y estructurada sobre la relación entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Conforme a Hernández y Mendoza (2018, p. 251), el cuestionario es un instrumento valioso en investigaciones cuantitativas, especialmente cuando se emplean preguntas cerradas que facilitan la obtención de datos homogéneos y comparables. Este formato permite a los participantes seleccionar respuestas dentro de un rango establecido, lo que simplifica el análisis estadístico y aumenta la confiabilidad de los resultados.

En este caso, el cuestionario incluyó preguntas cerradas estructuradas en escalas de Likert, las cuales son ampliamente utilizadas para medir actitudes, percepciones y opiniones en niveles graduados de acuerdo o frecuencia. Las escalas de Likert facilitaron captar el grado de aceptación o rechazo de los cadetes frente a aspectos

relacionados con la capacitación operativa, aplicación táctica y gestión tecnológica del uso de drones, así como la percepción sobre la seguridad de las instalaciones. La estandarización del instrumento permitió garantizar la uniformidad en la recolección de datos y facilitó la interpretación cuantitativa, ofreciendo un panorama claro y detallado de las variables en estudio. Además, la aplicación de este cuestionario favoreció una recolección ágil y eficiente, adaptándose a las condiciones institucionales y respetando los protocolos de la Escuela Militar, lo que contribuyó a la obtención de información pertinente y de calidad.

Tabla 2.
Diagrama de Likert

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

Fuente: Desarrollada en 1932 por el sociólogo Rensis Likert

La utilización de un baremo consiste en la aplicación de una escala o tabla de referencia que permite interpretar, clasificar y cuantificar los resultados obtenidos en una investigación o evaluación, facilitando así la comparación y el análisis de los datos de manera sistemática y objetiva. Según Coll (2020), el baremo es una herramienta fundamental para otorgar significado a las respuestas o mediciones, al establecer puntos de corte o categorías que delimitan rangos de valores y permiten identificar niveles, grados o grados de una variable en estudio. Esta sistematización contribuye a la estandarización de los criterios de evaluación, garantizando que los resultados sean comparables y puedan ser interpretados con rigor científico, independientemente del contexto o la población.

El uso del baremo es especialmente relevante en investigaciones cuantitativas donde se manejan escalas de medición, como las escalas de Likert, pues ayuda a transformar datos numéricos en indicadores comprensibles que facilitan la toma de decisiones o la formulación de conclusiones. Además, Coll (2020) enfatiza que la construcción de un baremo debe considerar aspectos psicométricos, como la validez y confiabilidad, para asegurar que las categorías o rangos definidos reflejen con precisión las características reales del fenómeno evaluado. De esta manera, la utilización de baremos no solo permite interpretar los datos de forma estandarizada, sino que también fortalece la calidad metodológica del estudio, al proveer un marco claro para la comparación y análisis de resultados, favoreciendo la coherencia y la consistencia en la presentación de los hallazgos.

3.7.3. Validez y confiabilidad de los instrumentos de medición

Dimensión 1. 3.7.3.1. 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.

Tabla 3.
Evaluación de expertos

N°	EXPERTOS	DNI	VALORACIÓN CUANTITATIVA
01	Dr. VASQUEZ MORA, EDWIN	43343660	885
02	Dr. ZAVALETA RAMOS, HUMBERTO	43903557	885
03	Mg. ZEA MELODIAS, RODOLFO	29388850	885
	Promedio		**885**

Nota: Anexo 7

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 Inteligencia de la misma institución. Esta prueba permitió identificar posibles áreas de mejora y ajustes necesarios en el cuestionario antes de su implementación definitiva.

Dimensión 2. 3.7.3.2. Validez y confiabilidad de los instrumentos de medición

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 4.
Criterio de confiabilidad valores

Intervalo de Alpha de Cronbach	Valoración
"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"

Nota: Este instrumento se utilizó en la prueba piloto

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 α, 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.
sT^2= Varianza de la suma de los ítems.
α = Coeficiente de alfa de Cronbach

Tabla 5.
Confiabilidad estadística del instrumento para medir la variable 1

Alfa de Cronbach	N de elementos
0.831	24

La confiabilidad del instrumento es muy alta, alcanzando un valor de 0.831 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 6.
Confiabilidad estadística del instrumento para medir la variable 2

Alfa de Cronbach	N de elementos
0.797	24

La confiabilidad del instrumento es alta, alcanzando un valor de 0.797 para la variable 2, 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.

3.8. Procesamiento y método de análisis de datos

3.8.1. Técnica para el procesamiento de datos

Para el procesamiento de datos se siguió un procedimiento sistemático que inició con la preparación de las herramientas de investigación, donde se diseñó y elaboró el cuestionario conforme a los indicadores previamente establecidos en el marco teórico y operativo, asegurando la cantidad suficiente de copias para todos los participantes y facilitando su aplicación ordenada y efectiva. Posteriormente, se gestionó la solicitud de permiso ante el oficial superior responsable de los cadetes, garantizando que la recolección de datos cumpliera con los protocolos institucionales y las normas éticas correspondientes, lo que permitió un ambiente adecuado y la colaboración de los participantes durante la encuesta.

La distribución de las encuestas se realizó durante un tiempo de servicio programado de aproximadamente veinte minutos, en el cual se aclararon todas las dudas y se brindó soporte para que los participantes respondieran con precisión y confianza. Una vez recolectados los cuestionarios, se procedió al procesamiento de datos utilizando software especializado como Excel, que facilitó la organización, limpieza y codificación de la información obtenida, permitiendo un manejo eficiente y ordenado de los datos para su posterior análisis.

Para el análisis estadístico se empleó el programa SPSS versión 27, aplicando inicialmente la prueba de Kolmogorov-Smirnov para determinar la normalidad de las muestras, lo cual orientó la selección de pruebas estadísticas adecuadas. Se realizaron análisis descriptivos para identificar tendencias y características básicas de las variables, y análisis inferenciales para evaluar las relaciones entre las variables mediante pruebas correlacionales, garantizando la validación de las hipótesis

formuladas. Finalmente, con base en los resultados estadísticos obtenidos, se generaron conclusiones sólidas que sustentaron las decisiones y recomendaciones para el área de estudio, contribuyendo a una interpretación rigurosa y objetiva del fenómeno investigado.

3.8.2. Método de análisis de datos

El método de análisis de datos empleado en esta investigación combinó técnicas descriptivas e inferenciales para lograr una comprensión integral de la relación entre el uso de drones y la seguridad de las instalaciones en la Escuela Militar de Chorrillos. Inicialmente, se aplicó un análisis descriptivo que permitió organizar y resumir la información recolectada mediante tablas y figuras. Estas representaciones gráficas facilitaron la identificación de patrones, frecuencias, distribuciones y tendencias en las variables estudiadas, ofreciendo una visión clara y detallada del comportamiento general de la muestra. La interpretación de estos datos descriptivos permitió establecer un contexto preciso y fundamentado sobre las características predominantes en la percepción y experiencia de los participantes respecto a las dimensiones de capacitación operativa, aplicación táctica y gestión tecnológica del uso de drones.

Para profundizar en las relaciones entre las variables, se realizó un análisis inferencial que comenzó con la aplicación de la prueba de normalidad Kolmogórov-Smirnov, la cual determinó si los datos seguían una distribución normal o no. Este paso fue crucial para seleccionar las pruebas estadísticas adecuadas que garantizaran la validez de los resultados. Dado que las variables no cumplieron con la normalidad, se optó por emplear la prueba no paramétrica de correlación de Spearman, la cual permitió evaluar la fuerza y dirección de la relación entre el uso de drones y la seguridad institucional sin suponer distribuciones específicas. La prueba de Spearman ofreció resultados estadísticamente significativos, permitiendo validar las hipótesis planteadas y confirmar la existencia de asociaciones relevantes entre las variables. Este enfoque metodológico aseguró un análisis riguroso, confiable y apropiado para la naturaleza de los datos obtenidos en la investigación.

3.9. Aspectos éticos

Los aspectos éticos en una investigación realizada en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" revisten una importancia fundamental debido a la naturaleza sensible de la institución y la información manejada. Se debe garantizar la confidencialidad y

el anonimato de los participantes, respetando su privacidad y asegurando que los datos recopilados no sean divulgados sin consentimiento explícito. Además, es imprescindible obtener las autorizaciones correspondientes de las autoridades militares competentes, quienes supervisan que la investigación se realice conforme a los protocolos institucionales y normativas vigentes. Este respeto por las jerarquías y regulaciones asegura que la investigación no afecte el funcionamiento ni la seguridad de la institución.

Asimismo, se debe velar por el consentimiento informado de los participantes, explicándoles claramente los objetivos, beneficios y posibles riesgos del estudio, y asegurando que su participación sea voluntaria y sin presiones. La ética también implica evitar cualquier tipo de daño físico, psicológico o reputacional a los involucrados, manteniendo un trato respetuoso y profesional durante todo el proceso. Finalmente, la transparencia en la presentación de resultados y la honestidad en la interpretación de los datos son principios esenciales para salvaguardar la integridad científica y la credibilidad de la investigación dentro del contexto militar y académico.

CAPÍTULO IV.
RESULTADOS

4.1. Análisis descriptivo

Resultados en base al Objetivo General: Uso de drones y Seguridad de las instalaciones

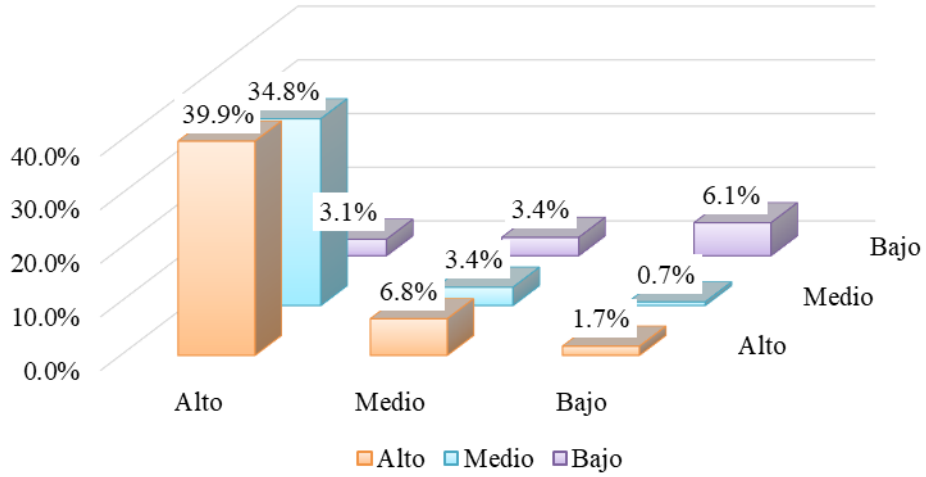
Tabla 7.

Uso de drones y Seguridad de las instalaciones

			V2. Seguridad de las instalaciones			
			Alto	Medio	Bajo	Total
V1. Uso de drones	Alto	Recuento	117	102	9	228
		% del total	39.9%	34.8%	3.1%	77.8%
	Medio	Recuento	20	10	10	40
		% del total	6.8%	3.4%	3.4%	13.7%
	Bajo	Recuento	5	2	18	25
		% del total	1.7%	0.7%	6.1%	8.5%
Total		Recuento	142	114	37	293
		% del total	48.5%	38.9%	12.6%	100.0%

Nota: Tabla de contingencia realizado con la base de datos del Anexo 05
Fuente: SPSS 27

Figura 3.
Uso de drones y Seguridad de las instalaciones



Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Interpretación de la Variable 1 y la Variable 2: Mediante la Tabla 7 y en la Figura 3, los resultados muestran que un alto porcentaje de cadetes que reportaron un uso elevado de drones también perciben un alto nivel de seguridad en las instalaciones. Específicamente, el

39.9% de los participantes manifestó un alto Uso de droness acompañado de una alta percepción de seguridad, mientras que un 34.8% consideró que aunque el uso de droness era alto, la seguridad era media. Esta predominancia indica una posible asociación positiva entre el empleo de drones y la mejora en la percepción de seguridad dentro de la institución.

Por otro lado, la tabla muestra que entre los cadetes que percibieron un bajo Uso de droness, un 6.1% señaló un bajo nivel de seguridad en las instalaciones, y solo un pequeño porcentaje (1.7%) manifestó alta seguridad a pesar de un uso reducido de drones. Esto sugiere que la insuficiente integración de esta tecnología podría estar relacionada con una menor sensación de protección. Además, la mayoría de los cadetes, un 48.5%, evaluó la seguridad de las instalaciones como alta, lo que coincide con la proporción que reportó un uso elevado de drones, reforzando la idea de que la tecnología contribuye a fortalecer las medidas de vigilancia y control.

Asimismo, el 13.7% de los participantes indicó niveles medios tanto en el uso de droness como en la seguridad, reflejando una posición intermedia que puede estar vinculada a limitaciones en la implementación o percepción de la efectividad de los drones. En conclusión, estos datos sugieren una tendencia donde el mayor Uso de droness se asocia con una mejor percepción de la seguridad en las instalaciones, mientras que niveles bajos o medios en su uso coinciden con percepciones menos optimistas, lo que resalta la importancia de promover el empleo de esta tecnología para fortalecer la seguridad institucional.

Resultados en base al Objetivo Específico 1: Capacitación operativa y Seguridad de las instalaciones.

Tabla 8.

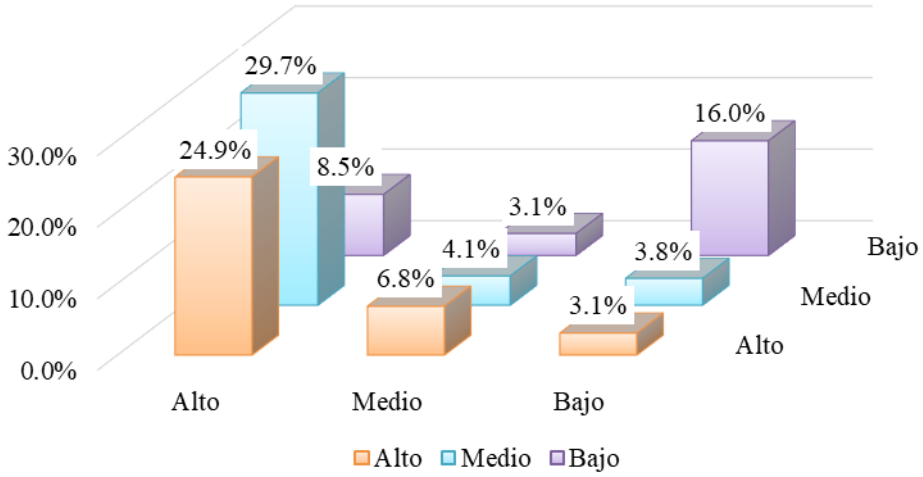
Capacitación operativa y Seguridad de las instalaciones

			V2. Seguridad de las instalaciones			
			Alto	Medio	Bajo	Total
D1. Capacitación operativa	Alto	Recuento	73	87	25	185
		% del total	24.9%	29.7%	8.5%	63.1%
	Medio	Recuento	20	12	9	41
		% del total	6.8%	4.1%	3.1%	14.0%
	Bajo	Recuento	9	11	47	67
		% del total	3.1%	3.8%	16.0%	22.9%
Total		Recuento	102	110	81	293
		% del total	34.8%	37.5%	27.6%	100.0%

Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Figura 4.

Capacitación operativa y Seguridad de las instalaciones



Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Interpretación de la Dimensión 1 de la Variable 1 y la Variable 2: Mediante la Tabla 8 y en la Figura 4, se observa que la mayoría de los cadetes que indicaron un alto nivel de capacitación operativa también percibieron altos niveles de seguridad en las instalaciones, con un 24.9% manifestando ambas condiciones. Sin embargo, una proporción significativa, el 29.7%, aunque con alta capacitación operativa, percibió un nivel medio de seguridad, lo que sugiere que, a pesar del entrenamiento, existen factores adicionales que influyen en la percepción de seguridad institucional.

Por otro lado, dentro del grupo que manifestó una capacitación operativa media, se encuentra que un 6.8% de los participantes también percibió un alto nivel de seguridad, mientras que el 4.1% reportó un nivel medio y el 3.1% bajo. Esto refleja una distribución más equilibrada, indicando que el nivel intermedio de capacitación genera percepciones variadas sobre la seguridad, posiblemente relacionadas con la eficacia del entrenamiento o la aplicación práctica del mismo.

Es notable que, entre los cadetes con baja capacitación operativa, el 16% percibió un nivel bajo de seguridad en las instalaciones, lo que podría indicar una correlación directa entre la falta de preparación técnica y una menor confianza en la protección del entorno. Además, un 3.1% de los que reconocieron baja capacitación operativa consideraron la seguridad alta, lo que podría obedecer a otros factores externos o experiencias personales.

En conjunto, la tabla sugiere que una mayor capacitación operativa tiende a asociarse con percepciones más positivas de seguridad en las instalaciones, mientras que la disminución

en el nivel de capacitación coincide con percepciones más bajas de seguridad, resaltando la importancia de la formación para fortalecer la confianza y efectividad en la protección institucional.

Resultados en base al Objetivo Específico 2: Aplicación táctica y Seguridad de las instalaciones.

Tabla 9.

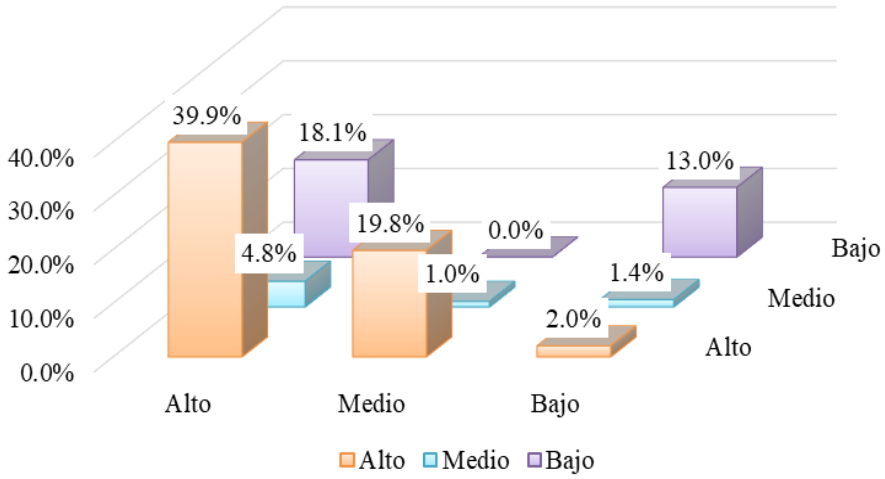
Aplicación táctica y Seguridad de las instalaciones

			V2. Seguridad de las instalaciones			
			Alto	Medio	Bajo	Total
D2. Aplicación táctica	Alto	Recuento	117	14	53	184
		% del total	39.9%	4.8%	18.1%	62.8%
	Medio	Recuento	58	3	0	61
		% del total	19.8%	1.0%	0.0%	20.8%
	Bajo	Recuento	6	4	38	48
		% del total	2.0%	1.4%	13.0%	16.4%
Total		Recuento	181	21	91	293
		% del total	61.8%	7.2%	31.1%	100.0%

Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Figura 5.

Aplicación táctica y Seguridad de las instalaciones



Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Interpretación de la Dimensión 2 de la Variable 1 y la Variable 2: Mediante la Tabla 9 y en la Figura 5, un aspecto destacado es que el 39.9% de los participantes percibió un alto nivel de aplicación táctica junto con una alta percepción de seguridad, lo que indica una

asociación fuerte entre una adecuada aplicación táctica y la confianza en la protección de las instalaciones. Esto sugiere que cuando las acciones tácticas son ejecutadas eficazmente, los cadetes sienten que las instalaciones están mejor resguardadas.

Por otro lado, el 18.1% manifestó un alto nivel de aplicación táctica, pero percibió un bajo nivel de seguridad, lo cual puede reflejar que a pesar de la implementación de tácticas, existen factores o limitaciones que afectan la percepción general de seguridad, como deficiencias en recursos o falta de integración tecnológica. Este contraste muestra que la aplicación táctica, aunque crucial, no es el único factor que determina la percepción de seguridad.

En el nivel medio de aplicación táctica, se observa que un 19.8% de cadetes percibió alta seguridad y solo un 1% indicó seguridad media, mientras que ningún participante consideró baja seguridad, lo que indica que una aplicación táctica moderada aún contribuye positivamente a la sensación de seguridad. Finalmente, en el grupo de baja aplicación táctica, un 13% consideró baja la seguridad, lo que evidencia una correlación directa entre la falta de acciones tácticas y una percepción negativa sobre la seguridad institucional.

En conjunto, los datos revelan que un mayor nivel de aplicación táctica se relaciona con una mejor percepción de seguridad, aunque existen matices que sugieren que la aplicación táctica debe complementarse con otros factores para fortalecer la confianza y protección en las instalaciones.

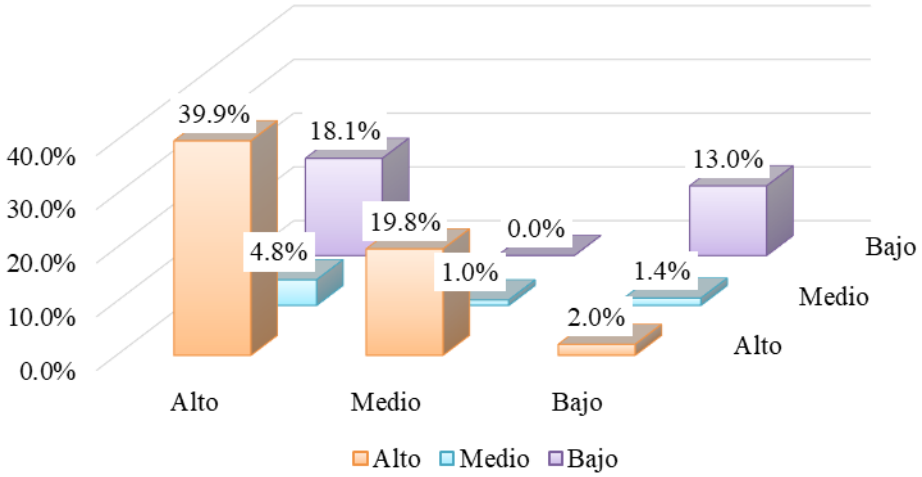
Resultados en base al Objetivo Específico 3: Gestión tecnológica y Seguridad de las instalaciones.

Tabla 10.
Gestión tecnológica y Seguridad de las instalaciones

			V2. Seguridad de las instalaciones			
			Alto	Medio	Bajo	Total
D3. Gestión tecnológica	Alto	Recuento	117	14	53	184
		% del total	39.9%	4.8%	18.1%	62.8%
	Medio	Recuento	58	3	0	61
		% del total	19.8%	1.0%	0.0%	20.8%
	Bajo	Recuento	6	4	38	48
		% del total	2.0%	1.4%	13.0%	16.4%
Total		Recuento	181	21	91	293
		% del total	61.8%	7.2%	31.1%	100.0%

Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Figura 6.
Gestión tecnológica y Seguridad de las instalaciones



Nota: Tabla de contingencia realizada con la base de datos del Anexo 05
Fuente: SPSS 27

Interpretación de la Dimensión 3 de la Variable 1 y la Variable 2: Mediante la Tabla 10 y en la Figura 6, se observa que un 39.9% de los participantes que manifestaron un alto nivel de gestión tecnológica también percibieron un alto nivel de seguridad en las instalaciones. Este dato sugiere que una gestión tecnológica eficaz, que probablemente incluye el mantenimiento adecuado, actualización de sistemas y manejo eficiente de datos, está asociada a una mayor confianza en la protección de la infraestructura militar. Sin embargo, también es importante destacar que un 18.1% reportó alta gestión tecnológica, pero percibió un bajo nivel de seguridad, lo que puede indicar que, a pesar de la gestión, existen otros factores o limitaciones que afectan la percepción general de seguridad.

En cuanto a la gestión tecnológica media, el 19.8% de los cadetes señaló un alto nivel de seguridad, mientras que un pequeño porcentaje, 1%, percibió seguridad media y ninguno manifestó baja seguridad. Esto indica que un nivel intermedio de gestión tecnológica puede ser suficiente para generar confianza positiva, aunque quizá con áreas susceptibles a mejora. Por otro lado, el grupo que expresó baja gestión tecnológica mostró que un 13% de los cadetes percibió baja seguridad, reflejando una posible relación directa entre deficiencias en la gestión tecnológica y una percepción negativa respecto a la seguridad.

En resumen, los datos indican una tendencia clara: niveles más altos de gestión tecnológica tienden a correlacionarse con percepciones más favorables sobre la seguridad de las instalaciones, mientras que una gestión deficiente puede contribuir a inseguridades y

vulnerabilidades dentro del entorno militar, evidenciando la necesidad de fortalecer los procesos tecnológicos para mejorar la protección institucional.

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 11.
Pruebas de Normalidad

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
V1. Uso de drone	0.318	293	0.000
D1. Capacitación operativa	0.086	293	0.000
D2. Aplicación táctica	0.806	293	0.000
D3. Gestión tecnológica	0.852	293	0.000
V2. Seguridad de las instalaciones	0.001	293	0.000

a. Corrección de significación de Lilliefors

Interpretación: La prueba de normalidad evidenciada en el Tabla 11, muestra que los datos no se encuentran normalmente distribuidos, de acuerdo con la prueba "Kolmogorov-Smirnov, que se utiliza para muestras mayores a 50, ello debido a que la Sig. es menor a 0.05, es decir el P-valué < 0.05; lo que nos permite concluir que las variables presentan una distribución no normal por lo cual se efectúa el siguiente estadístico de correlación de Spearman.

El coeficiente de correlación de Spearman, ρ (Rh0) "es una medida de la correlación (la asociación o interdependencia) entre dos variables aleatorias continuas. Para calcular ρ, los datos son ordenados y reemplazados por su respectivo orden".

El estadístico ρ viene dado por la expresión:

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

Donde "D" es la diferencia entre los correspondientes estadísticos de orden de x - y. "N" es el número de parejas.

Se tiene que considerar la existencia de datos idénticos a la hora de ordenarlos, aunque si éstos son pocos, se puede ignorar tal circunstancia

La aproximación moderna al problema de averiguar si un valor observado de ρ es significativamente diferente de cero (siempre tendremos $-1 \leq \rho \leq 1$) es calcular la probabilidad de que sea mayor o igual que el ρ esperado, dada la hipótesis nula, utilizando un test de permutación. Esta aproximación es casi siempre superior a los métodos tradicionales, a no ser que el conjunto de datos sea tan grande que la potencia informática no sea suficiente para generar permutaciones (poco probable con la informática moderna), o a no ser que sea difícil crear un algoritmo para crear permutaciones que sean lógicas bajo la hipótesis nula en el caso particular de que se trate (aunque normalmente estos algoritmos no ofrecen dificultad).

Tabla 12.

Escala de interpretación para la correlación de Spearman

Correlación	Interpretación
r = -1,00	Correlación negativa perfecta
-0,9 a -0,99	Correlación negativa muy alta
-0,7 a -0,89	Correlación 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_a : Existe una relación significativa entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

HG_0 : No existe una relación significativa entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Paso 2.

El nivel de significancia, representado como α, 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 general

			V1. Uso de drones	V2. Seguridad de las instalaciones
Rho de Spearman	V1. Uso de drones	Coeficiente de correlación	1.000	0.848
		Sig. (bilateral)		0.000
		N	293	293
	V2. Seguridad de las instalaciones	Coeficiente de correlación	0.848	1.000
		Sig. (bilateral)	0.000	
		N	293	293

Nota: Información realizada con la base de datos del anexo 05
Fuente: SPSS 27

Interpretación: Como el coeficiente de Rh0 de Spearman es 0.848, 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 H0 si sig (ρ-valor) es menor que 0.05.
- Aceptar H0 si sig (ρ-valor) es mayor que 0.05.

Paso 5.

Decisión estadística. Si 0.000 > 0.05. Aceptar H0

Paso 6.

Conclusión: se rechaza la hipótesis general nula y se acepta la hipótesis general alterna, esto indica que, si existe una relación significativa entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

4.2.3. Contrastación de la Hipótesis Específica 1 (HE1)

Paso 1.

$HE1_a$: Existe una relación significativa entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

$HE1_0$: No existe una relación significativa entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Paso 2.

El nivel de significancia, representado como α, 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 1

			D1. Capacitación operativa	V2. Seguridad de las instalaciones
Rho de Spearman	D1. Capacitación operativa	Coeficiente de correlación	1.000	0.983
		Sig. (bilateral)		0.000
		N	293	293
	V2. Seguridad de las instalaciones	Coeficiente de correlación	0.983	1.000
		Sig. (bilateral)	0.000	
		N	293	293

Nota: Información realizada con la base de datos del anexo 05
Fuente: SPSS 27

Interpretación: Como el coeficiente de Rh0 de Spearman es 0.983, 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 H0 si sig (ρ-valor) es menor que 0.05.
- Aceptar H0 si sig (ρ-valor) es mayor que 0.05.

Paso 5.

Decisión estadística. Si 0.000 > 0.05. Aceptar H0

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 significativa entre la capacitación operativa del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

4.2.4. Contrastación de la Hipótesis Específica 2 (HE2)

Paso 1.

$HE2_a$: Existe una relación significativa entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

$HE2_0$: No existe una relación significativa entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Paso 2.

El nivel de significancia, representado como α, 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 2

			D2. Aplicación táctica	V2. Seguridad de las instalaciones
Rho de Spearman	D2. Aplicación táctica	Coeficiente de correlación	1.000	0.854
		Sig. (bilateral)		0.000
		N	293	293
	V2. Seguridad de las instalaciones	Coeficiente de correlación	0.854	1.000
		Sig. (bilateral)	0.000	
		N	293	293

Nota: Información realizada con la base de datos del anexo 05
Fuente: SPSS 27

Interpretación: Como el coeficiente de Rh0 de Spearman es 0.854, 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 H0 si sig (ρ-valor) es menor que 0.05.
- Aceptar H0 si sig (ρ-valor) es mayor que 0.05.

Paso 5.

Decisión estadística. Si 0.000 > 0.05. Aceptar H0

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 significativa entre la aplicación táctica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

4.2.5. Contrastación de la Hipótesis Específica 3 (HE3)

Paso 1.

$HE3_a$: Existe una relación significativa entre la gestión tecnológica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

$HE3_0$: No existe una relación significativa entre la gestión tecnológica del dron y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

Paso 2.

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

Paso 3.

La prueba estadística y el nivel de relación de Spearman.

Tabla 16.
Prueba de correlación de Spearman de la Hipótesis Específica 3

			D3. Gestión tecnológica	V2. Seguridad de las instalaciones
Rho de Spearman	D3. Gestión tecnológica	Coeficiente de correlación	1.000	0.925
		Sig. (bilateral)		0.000
		N	293	293
	V2. Seguridad de las instalaciones	Coeficiente de correlación	0.925	1.000
		Sig. (bilateral)	0.000	
		N	293	293

Nota: Información realizada con la base de datos del anexo 05
Fuente: SPSS 27

Interpretación: Como el coeficiente de Rh0 de Spearman es 0.925, 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 H0 si sig (ρ-valor) es menor que 0.05.

- Aceptar H0 si sig (ρ-valor) es mayor que 0.05.

Paso 5.

Decisión estadística. Si 0.000 > 0.05. Aceptar H0

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 significativa entre la gestión tecnológica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025”.

CAPÍTULO V.
DISCUSIÓN DE RESULTADOS

En relación a la Hipótesis General, la correlación de Spearman entre el uso de drones y la seguridad de las instalaciones es $\rho = 0.848$ con $p = 0.000$ y $N = 293$, magnitud que se interpreta como positiva alta y estadísticamente significativa. Bajo la regla de decisión (rechazar H0 si $p < 0.05$), corresponde rechazar la hipótesis nula y aceptar la hipótesis alternativa, confirmando una relación significativa entre ambas variables. Dado que se trata de variables ordinales categorizadas (alto/medio/bajo), el uso de Spearman es adecuado para capturar la dependencia monótona observada en la tabla de contingencia; además, la coherencia entre el gran tamaño del coeficiente y la concentración de frecuencias en los cuadrantes altos refuerza la lectura de que el despliegue de drones se integra funcionalmente al sistema de vigilancia, verificación de alertas y control, elevando la percepción de protección en el campus. Con todo, por el diseño no experimental transversal, el hallazgo es asociativo (no causal), por lo que deben considerarse posibles covariables institucionales que también contribuyen a la mejora percibida.

Al contrastar estos resultados con Fernández (2024), quien analiza jurídicamente el empleo de RPAS en la Guardia Civil, se observa convergencia en el mecanismo operativo: mayor presencia aérea y mayor capacidad de verificación elevan la efectividad preventiva y de respuesta, lo que se traduce en entornos más seguros. El matiz de ese antecedente (exigir regulación reforzada, protocolos estrictos y capacitación especializada) ayuda a explicar el pequeño pero no nulo 3.1% de “uso alto–seguridad baja”: incluso con tecnología intensiva, si persisten brechas en gobernanza, la percepción de seguridad puede no alcanzar su máximo; por ello, el resultado empírico de $\rho = 0.848$ no solo avala la dirección de la relación, sino que sugiere que el perfeccionamiento normativo–operativo es palanca para desplazar esos casos residuales hacia seguridad alta.

El diálogo con Pérez y Villar (2021), quienes proponen un sistema de videovigilancia con drones para un distrito de Lima y documentan su pertinencia en contextos de victimización elevada, refuerza el valor de la integración táctica: cuando los drones se articulan con sensores EO/IR, CCTV y protocolos de despacho, se incrementan cobertura, oportunidad y calidad de la verificación, con retornos perceptibles en la seguridad. Nuestros datos explican por qué el 34.8% reporta “uso alto–seguridad media”: esa franja probablemente corresponde a fases de maduración operativa (rutas, ventanas horarias, analítica de video, coordinación de patrullas)

en las que la capacidad ya está desplegada pero aún puede optimizarse; al cerrar esas brechas, es razonable esperar una migración progresiva hacia “seguridad alta”, manteniendo el cumplimiento regulatorio y la proporcionalidad en la operación.

En consonancia con Canchaya (2021), quien evidencia ganancias de eficiencia y productividad al incorporar drones en supervisión técnica de infraestructura eléctrica (ahorro de tiempos, más estructuras por día y reducción de riesgos), nuestros resultados sugieren un puente entre rendimiento operativo y seguridad percibida: cuando el dron acorta tiempos de verificación, amplía cobertura con menor exposición de personal y aporta registros objetivos, la valoración de seguridad tiende a mejorar. Esta lectura ayuda a comprender que la asociación positiva no solo es un fenómeno de “presencia tecnológica”, sino de desempeño: allí donde el empleo del dron se traduce en eficiencia observable y respuesta oportuna, la percepción de seguridad se eleva; cuando esos atributos no se consolidan aún, la seguridad se estabiliza en el nivel medio.

En síntesis, la evidencia descriptiva e inferencial converge en una asociación positiva alta entre Uso de drones y seguridad de las instalaciones, y los antecedentes discutidos respaldan que esa relación se potencia cuando confluyen tres condiciones: gobernanza regulatoria y protocolos claros (Fernández), integración táctica con ecosistemas de vigilancia y operación (Pérez y Villar) y eficiencia operativa demostrable en la ejecución cotidiana (Canchaya). Para capitalizar el hallazgo y desplazar la masa situada en “seguridad media” hacia “seguridad alta”, se sugiere profundizar en tres frentes complementarios: capacitación operativa orientada a competencias y reglas de empleo, aplicación táctica con optimización de rutas, ventanas y analítica, y gestión tecnológica que asegure mantenimiento, datos trazables e interoperabilidad con el resto del sistema; con ello, la institución podrá sostener los efectos favorables observados, resguardar la legitimidad del uso y avanzar hacia un programa de seguridad integral más robusto y medible.

En relación a la Hipótesis Específica 1, la correlación de Spearman entre capacitación operativa y seguridad de las instalaciones alcanza $\rho = 0.983$ con $p = 0.000$ y $N = 293$, magnitud muy alta y estadísticamente significativa. Conforme a la regla de decisión (rechazar H0 si $p < 0.05$), corresponde rechazar la hipótesis nula y aceptar la alternativa, confirmando una relación significativa: a mayor capacitación, mayor seguridad percibida. La cercanía a 1 indica una dependencia monótona casi perfecta, congruente con la concentración observada en los cuadrantes de “capacitación alta–seguridad alta/media”. No obstante, al ser un diseño no

experimental transversal, la inferencia es asociativa; conviene atender posibles factores concomitantes (madurez de protocolos, interoperabilidad con CCTV, tiempos de despacho, fatiga de turnos) que pueden explicar por qué una fracción con alta formación aún reporta seguridad media o baja. Aun con esa cautela, el tamaño del efecto orienta la gestión: invertir en currículo, práctica supervisada y evaluación de competencia debería traducirse en mejoras medibles en la percepción y el desempeño de seguridad.

En contraste con la experiencia propositiva-operativa de Rodríguez (2021) en la EMCH, donde el uso de drones como medio de obtención de datos de inteligencia exige planificación de fuerza, adiestramiento específico y procedimientos estandarizados, nuestros resultados refuerzan empíricamente la premisa formativa: la institucionalización de perfiles de competencia se asocia con mayor seguridad percibida. El tramo de 29.7% en "alta capacitación–seguridad media" puede interpretarse, a la luz de ese antecedente, como un estado de maduración: la formación existe, pero aún faltan horas de vuelo, prácticas en escenarios y cierres de brecha entre lo enseñado y lo ejecutado bajo condiciones reales para que la percepción migre a "seguridad alta".

A la luz del estudio descriptivo-argumentativo de Vidal (2021) en seguridad privada (que subraya que la incorporación de drones complementa al personal y demanda inversión, capacitación y observancia regulatoria, la asociación $\rho = 0.983$ aporta una confirmación cuantitativa: la formación operativa no solo habilita el uso seguro, sino que media el salto de la tecnología a resultados de seguridad. Donde el currículo integra operación de sensores EO/IR, gestión de evidencias, reglas de empleo y coordinación con patrullas, la percepción tiende a alta; donde la capacitación es incipiente o fragmentada, la seguridad se estabiliza en media. Este encuadre ayuda a leer el 8.5% de alta capacitación con seguridad baja: allí podrían coexistir entrenamiento reciente con ecosistemas aún no integrados (analítica de video, protocolos de despacho o mantenimiento de flota), lo que sugiere priorizar ejercicios conjuntos y ajustes de procedimiento.

Finalmente, el trabajo de factibilidad IVR de Mazza (2024) en el dominio marítimo (que propone una red de bases, procedimientos y entrenamiento especializado para sostener operaciones UAV) ofrece una lección trasladable al campus: la capacidad no es solo plataforma, es gente entrenada + doctrina + soporte. Nuestros datos muestran que la cadena formativa (teoría–simulación–campo–evaluación) está fuertemente vinculada con la seguridad percibida; cuando esa cadena se cierra con estándares de competencia y sostenimiento

(mantenimiento, baterías, repuestos, software), la percepción sube; cuando hay cuellos de botella logísticos o vacíos doctrinales, aparece la meseta de seguridad media aun con capacitación alta. La recomendación, siguiendo la lógica de Mazza, es alinear currículo, plan de sostenimiento y gobernanza para que la formación se traduzca de manera estable en efectividad operacional.

En síntesis, los resultados describen y confirman una relación muy alta entre capacitación operativa y seguridad de las instalaciones: la formación robusta desplaza las percepciones hacia seguridad alta, mientras que la formación baja se asocia con seguridad baja. El diálogo con los antecedentes seleccionados converge en tres vectores de acción: currículo por competencias con práctica supervisada, integración táctica de la tripulación RPAS con el ecosistema de vigilancia y sostenimiento/logística que garantice continuidad. Al reforzar estos frentes (con especial foco en el segmento que hoy reporta “alta capacitación–seguridad media” , la institución puede convertir capacitación en desempeño y consolidar el tránsito hacia un programa de seguridad institucional más robusto, medible y sostenido en el tiempo.

En relación a la Hipótesis Específica 2, la correlación de Spearman entre aplicación táctica y seguridad de las instalaciones es $\rho = 0.854$ con $p = 0.000$ y $N = 293$, un tamaño alto y estadísticamente significativo. Conforme a la regla de decisión, corresponde rechazar H0 y aceptar HE2a, validando que, a mayor aplicación táctica, mayor seguridad percibida. La magnitud del coeficiente es coherente con la fuerte concentración en el cuadrante alto–alto, pero la presencia del 18.1% alto–bajo recuerda que se trata de un corte transversal no experimental: la relación es monótona y robusta, no causal, y conviene considerar covariables institucionales que pueden amortiguar el efecto de la táctica en determinados contextos operativos.

A la luz del antecedente Araos y Ruíz (2023), que examina la constitucionalidad del uso de drones respecto de la inviolabilidad del hogar y la vida privada, parte de la disonancia alto–bajo puede explicarse por fricción jurídico-perceptiva: aun con despliegue táctico intenso, si la comunidad percibe dudas sobre límites, proporcionalidad o necesidad, la confianza (componente esencial de la seguridad percibida) se resiente. En un campus militar con interacción con entornos vecinos, la táctica tiene que dialogar con garantías y protocolos de minimización (zonas de vuelo, ángulos de toma, custodia de evidencias, autorización y registro), de modo que el operador no solo “haga más”, sino que haga lo correcto según estándares de idoneidad y proporcionalidad. Bajo ese prisma, el 18.1% de alto–bajo es

compatible con escenarios donde la ejecución es intensa pero la legitimidad percibida o la claridad normativa no acompañan, dejando margen para fortalecer la comunicación institucional, la señalización del perímetro sensible y las evaluaciones de impacto ex ante.

El antecedente Artica (2025), centrado en protección de datos personales en el uso de drones en entornos laborales, aporta otra clave: la aplicación táctica que no se acompaña de gobernanza informacional (finalidades específicas, mínimos de captación, tiempos de conservación, seguridad de los repositorios, roles y auditoría) puede activar percepciones de riesgo que neutralizan los beneficios operativos. Nuestros datos lo sugieren en dos sentidos: primero, la "meseta" de aplicación alta–seguridad media (4.8%) y el bloque alto–bajo (18.1%) indican que existe margen para alinear la explotación del material (video, telemetría, registros) con políticas de datos claras que afiancen la confianza; segundo, el desempeño del tramo medio sin casos de seguridad baja apunta a que estructuras normativas sólidas pueden compensar parcialmente la menor intensidad táctica, elevando la seguridad percibida con una táctica suficiente pero bien gobernada. En suma, la eficacia táctica necesita un ISMS operativo para que el valor de la vigilancia aérea llegue a la percepción de seguridad sin activar alarmas de privacidad.

Por su parte, Delgado (2024), al analizar la responsabilidad del operador de drones en contextos de movilizaciones sociales, recuerda que la aplicación táctica debe incorporar reglas de seguridad operacional y de riesgo a terceros: separación, zonas de exclusión, coordinación con autoridades, verificación previa de equipos y estándares de actuación para evitar daños y litigios. Trasladado al campus, esto implica que la táctica no se mida solo por "cantidad de vuelos" o "cobertura" sino por calidad procedimental: briefings y debriefings, listas de verificación, triaje de alertas, tiempos de despacho y protocolos de custodia de evidencia. La presencia de alta aplicación–baja seguridad puede emerger cuando la intensidad no va acompañada de calidad ni de garantías de seguridad operacional percibidas por usuarios y personal, o cuando incidentes menores (falsas alarmas, fallas de enlace, eventos de mantenimiento) erosionan la confianza pese al esfuerzo táctico.

En síntesis, los resultados muestran una asociación positiva alta entre aplicación táctica y seguridad de las instalaciones, pero también dejan ver zonas de mejora donde la táctica por sí sola no alcanza. La discusión con los antecedentes seleccionados sugiere tres líneas de acción complementarias para convertir "aplicación" en "seguridad" de manera sostenida: i) legitimidad jurídica y proporcionalidad operativa que blinde la táctica desde su diseño (Araos

y Ruíz), ii) gobernanza del dato y protección de la información para transformar vigilancia en confianza (Artica), y iii) calidad procedimental y responsabilidad del operador como parte de la táctica misma, midiendo desempeño por estándares de seguridad y coordinación, no solo por intensidad (Delgado). Si se robustecen estas tres palancas en paralelo (sin perder la integración con el resto de capas de seguridad y con la logística de sostenimiento, es razonable esperar una migración de los casos hoy ubicados en alto–bajo hacia alto–alto, consolidando el aporte de la aplicación táctica al programa integral de seguridad de la EMCH "CFB".

En relación a la Hipótesis Específica 3, la correlación de Spearman entre gestión tecnológica y seguridad es $\rho = 0.925$ con $p = 0.000$ y $N = 293$, magnitud muy alta y estadísticamente significativa. Atendiendo la regla de decisión ($p < 0.05 \rightarrow$ rechazar H0), corresponde rechazar la hipótesis nula y aceptar la alternativa (HE3a): a mejor gestión tecnológica, mayor seguridad percibida. La cercanía del coeficiente a 1 es coherente con la fuerte concentración en gestión alta–seguridad alta y con la ausencia de seguridad baja en el tramo medio, pero la existencia del bloque gestión alta–seguridad baja (18.1%) recuerda que se trata de un corte transversal no experimental: la relación es monótona y robusta, no causal, y puede estar modulada por covariables como el grado de integración con otras capas de seguridad, la madurez de procedimientos, la curva de aprendizaje de los turnos y la confiabilidad de la flota (baterías, hélices, firmware, enlaces C2).

La evidencia de Bustamante y Xolo (2021) (quienes diseñan un mecanismo terrestre acoplable a drones para rescate en zonas de difícil acceso) aporta una lección directamente trasladable a la gestión tecnológica: el desempeño no depende solo de "tener" tecnología, sino de integrar subsistemas, sustentar decisiones con requisitos operativos y cerrar el ciclo de pruebas–verificación–mejora. Allí donde el diseño y la integración son sólidos, se ganan eficiencia y seguridad; donde faltan validación y sostenimiento, emergen fallas operativas que pueden explicar parte del 18.1% con gestión alta–seguridad baja (capacidad instalada pero todavía sin disponibilidad estable, sin repuestos críticos, o con flujos de explotación de video/telemetría poco maduros), lo que frena que la ventaja tecnológica sea percibida en el día a día.

El antecedente Pérez y Villar (2021) (que proponen un sistema de videovigilancia con drones para un distrito de Lima) refuerza que la gestión tecnológica eficaz es, sobre todo, arquitectura e integración: drones + sensores EO/IR + CCTV + procedimientos de despacho + sostenimiento (energía, baterías, repuestos, licencias). La pauta de nuestros datos en el tramo

medio (19.8% con seguridad alta y 0% con seguridad baja) es consistente con esa idea: una gestión “moderada pero bien ensamblada” puede sostener percepciones altas de seguridad sin necesidad de un despliegue maximalista, siempre que existan roles claros, listas de verificación, matrices de interoperabilidad y criterios de aceptación técnica que aseguren continuidad de servicio y trazabilidad de evidencias.

En línea con Fernández (2024) (quien, desde el análisis jurídico-doctrinal en la Guardia Civil, subraya que los RPAS aportan valor siempre que se fortalezcan la regulación, la capacitación especializada y los protocolos, la gestión tecnológica debe incluir gobernanza: control de configuración, políticas de conservación de datos, protección de derechos, acreditación de operadores y protocolos de legitimidad (autorizaciones, zonas, horarios, custodia de material). Una operación muy tecnificada que no cierre ese bucle puede producir disonancia: mucha actividad tecnológica sin confianza institucional, lo que se alinea con el hallazgo del 18.1% de gestión alta–seguridad baja. La ruta de mitigación pasa por alinear el sostenimiento técnico con la legalidad y proporcionalidad del empleo, de modo que la calidad tecnológica se convierta en seguridad percibida.

En síntesis, los resultados describen y confirman una relación muy alta entre gestión tecnológica y seguridad: donde la gestión es sólida, la seguridad se valora como alta; donde es débil, la seguridad se resiente. Las tres investigaciones discutidas apuntan a un mismo vector: convertir tecnología en seguridad requiere integración de subsistemas y pruebas (Bustamante y Xolo), arquitectura operativa y sostenimiento (Pérez y Villar) y gobernanza normativa–procedimental (Fernández). Si la institución prioriza estas tres palancas de forma coordinada con indicadores de disponibilidad y tiempos de respuesta, planes de mantenimiento y actualización, y protocolos de legitimidad y explotación de datos, es razonable esperar una migración de casos hoy situados en gestión alta–seguridad baja hacia gestión alta–seguridad alta, consolidando el aporte de la gestión tecnológica al programa integral de seguridad de la EMCH “CFB”.

CONCLUSIONES

En relación al Objetivo General, se ha determinado que existió una relación positiva alta entre el uso de sistemas aéreos no tripulados y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2025. Asimismo, de los resultados se ha determinado que la falta de lineamientos claros y de medios propios para este tipo de vigilancia mantuvo brechas de control, lo que en los cadetes limitó la sensación de respaldo tecnológico en su seguridad y, en la Escuela Militar de Chorrillos “CFB”, dejó vulnerabilidades abiertas en la protección de sus instalaciones.

En relación al Objetivo Específico 1, se ha determinado que existió una relación positiva muy alta entre la capacitación operativa proyectada en drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2025. Asimismo, de los resultados se ha determinado que la formación específica en esta tecnología fue escasa y poco sistemática, lo que en los cadetes redujo las oportunidades de entrenarse en vigilancia aérea y, en la Escuela Militar de Chorrillos “CFB”, limitó la preparación institucional para incorporar estos medios en el futuro.

En relación al Objetivo Específico 2, se ha determinado que existió una relación positiva alta entre la aplicación táctica planificada de los drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2025. Asimismo, de los resultados se ha determinado que el empleo táctico se mantuvo principalmente en el plano teórico y de ensayo, lo que en los cadetes generó una experiencia práctica limitada con esta capacidad y, en la Escuela Militar de Chorrillos “CFB”, impidió consolidar procedimientos rutinarios de empleo.

En relación al Objetivo Específico 3, se ha determinado que existió una relación positiva muy alta entre la gestión tecnológica prevista de los drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB”, 2025. Asimismo, de los resultados se ha determinado que la gestión tecnológica se encontraba poco desarrollada, sin estructuras definidas para mantenimiento e integración de datos, lo que en los cadetes dificultó comprender el ciclo completo de operación de estos sistemas y, en la Escuela Militar de Chorrillos “CFB”, postergó la creación de una base técnica que sustentara su implementación.

RECOMENDACIONES

En relación a la conclusión del Objetivo General, que el Señor General de Brigada Director de la Escuela Militar de Chorrillos “CFB” considere que, ante la falta de lineamientos claros y de medios propios para la vigilancia mediante sistemas aéreos no tripulados, se formulen directivas específicas y un plan de implementación progresiva; frente a las brechas de control en la seguridad de las instalaciones, se integren estos medios futuros de observación al esquema de vigilancia existente mediante procedimientos y responsabilidades claramente definidos; de esta manera, las recomendaciones favorecerán a los cadetes al reforzar su sensación de respaldo tecnológico y confianza en la protección durante su formación, y a la Escuela Militar de Chorrillos “CFB” al reducir vulnerabilidades y fortalecer un sistema de seguridad más coherente y preventivo.

En relación a la conclusión del Objetivo Específico 1, que el Señor General de Brigada Director de la Escuela Militar de Chorrillos “CFB” considere que, ante la formación específica escasa en el empleo de sistemas aéreos no tripulados, se diseñen e incorporen módulos formativos teórico–prácticos en los planes de estudio; y al mantenerse poco sistematizada dicha capacitación, se establezcan programas regulares de entrenamiento con contenidos y evaluaciones estandarizadas; con ello, las recomendaciones favorecerán a los cadetes al ampliar sus oportunidades de entrenarse en vigilancia aérea y fortalecer sus competencias profesionales, y a la Escuela Militar de Chorrillos “CFB” al incrementar su nivel de preparación institucional para la futura incorporación de estas capacidades.

En relación a la conclusión del Objetivo Específico 2, que el Señor General de Brigada Director de la Escuela Militar de Chorrillos “CFB” considere que, ante el empleo táctico situado principalmente en el plano teórico y de ensayo, se planifiquen ejercicios de aplicación simulada que articulen los sistemas aéreos no tripulados con otros medios de seguridad; y frente a la limitada experiencia práctica en esta capacidad, se promuevan escenarios de entrenamiento progresivo que permitan al personal practicar procedimientos tácticos estandarizados; así, las recomendaciones favorecerán a los cadetes al fortalecer su experiencia operativa y su seguridad para actuar en situaciones reales, y a la Escuela Militar de Chorrillos “CFB” al avanzar hacia la consolidación de procedimientos rutinarios de empleo que robustezcan su esquema de protección.

En relación a la conclusión del Objetivo Específico 3, que el Señor General de Brigada Director de la Escuela Militar de Chorrillos “CFB” considere que, ante una gestión tecnológica poco desarrollada de los sistemas aéreos no tripulados, se estructuren órganos o responsables específicos para su administración, mantenimiento y actualización; y al no contarse con esquemas definidos de integración de datos, se implementen protocolos y plataformas que permitan registrar, procesar y difundir la información generada por estos medios; de este modo, las recomendaciones favorecerán a los cadetes al facilitar la comprensión del ciclo completo de operación tecnológica y fortalecer su formación en gestión de sistemas, y a la Escuela Militar de Chorrillos “CFB” al crear una base técnica sólida que sustente la futura implementación y uso eficaz de estas capacidades.

REFERENCIAS

Araos Henríquez, C., & Ruíz Díaz, J. (2023). *Constitucionalidad del uso de droness como forma de intromisión no presencial, en el contexto del derecho a la inviolabilidad del hogar.* [Tesis de Licenciatura], Universidad de Chile, Facultad de Derecho. https://repositorio.uchile.cl/bitstream/handle/2250/193739/Constitucionalidad-del-uso-de-drones-como-forma-de-intromision-no-presencial.pdf

Artica Martínez, R. (2025). *Protección de datos personales en el uso de los drones aplicado a la prevención de riesgos laborales.* [Trabajo de Suficiencia Profesional], Universidad de Lima. https://repositorio.ulima.edu.pe/handle/20.500.12724/22712

Bustamante Chipol, D., & Xolo Campechano, J. (2021). *Diseño de mecanismo terrestre para drones de rescate en zona de difícil acceso.* [Tesis de Licenciatura], Instituto Tecnológico Superior de San Andrés Tuxtla (TecNM). https://rinacional.tecnm.mx/handle/TecNM/1223

Canchaya Huaytalla, B. (2021). *El VANT o dron como tecnología de supervisión remota en la protección contra sobretensiones de frente rápido en las líneas de transmisión de la región Junín.* [Tesis de Licenciatura], Universidad Nacional del Centro del Perú. https://repositorio.uncp.edu.pe/server/api/core/bitstreams/54b9065e-08d7-43ea-86ee-5c8e5456a0a7/content

Coll, F. (06 de octubre de 2020). *Baremo*. https://economipedia.com/definiciones/baremo.html

Colomina, I., & Molina, P. (2014). Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing, 92,* 79–97. https://doi.org/10.1016/j.isprsjprs.2014.02.013

Cronbach, L. J., & Meehl, P. E. (1955). Validez de constructo en pruebas psicológicas. *Psychological Bulletin, 52*(4), 281-302. https://doi.org/10.1037/h0040957

Cybersecurity and Infrastructure Security Agency (CISA). (2025). *UAS Detection, Assessment, and Mitigation for Critical Infrastructure: Considerations.* CISA. https://www.cisa.gov/resources-tools/resources/uas-detection-assessment-and-mitigation-critical-infrastructure

Delgado Vega, W. (2024). *Uso de droness en movilizaciones sociales.* [Tesis de Licenciatura], Universidad Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/13091

Dishaw, M., & Strong, D. (1999). Extending the Technology Acceptance Model with Task–Technology Fit Constructs. *Decision Support Systems, 29*(2), 219–226. https://doi.org/10.1016/S0167-9236(99)00038-8

Endsley, M. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors, 37*(1), 32–64. https://doi.org/10.1518/001872095779049543

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Aviation Safety Agency (EASA). (2025). *Civil drones (Unmanned aircraft) (Categories and rules (Open/Specific/Certified)*. https://www.easa.europa.eu/en/domains/civil-drones-rpas

Federal Aviation Administration (FAA). (1 de enero de 2024). *Become a Drone Pilot (Part 107)*. https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot

Federal Emergency Management Agency (FEMA). (2003). *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426).* FEMA. https://www.cisa.gov/resources-tools/resources/reference-manual-mitigate-potential-terrorist-attacks-against-buildings

Fernández Chiclano, R. (2024). *Utilización de sistemas RPAS en labores de protección de seguridad ciudadana en la Guardia Civil.* [Tesis de Doctorado], Universidad Católica San Antonio de Murcia (UCAM). https://repositorio.ucam.edu/handle/10952/9015

Goodhue, D., & Thompson, R. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly, 19*(2), 213–236. https://doi.org/10.2307/249689

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

IBM. (2024). *Software IBM SPSS*. https://www.ibm.com/es-es/spss

Instituto Nacional de Estadística e Informática (INEI). (2023). *Nota de prensa: víctimas de violencia familiar (mujeres 15–49 años).* https://www.inei.gob.pe/prensa/noticias/el-356-de-mujeres-de-entre-15-y-49-anos-ha-sido-victima-de-violencia-familiar-en-los-ultimos-12-meses-14657/

Interagency Security Committee (ISC). (2021). *Risk Management Process for Federal Facilities (RMP).* CISA. https://www.cisa.gov/isc

International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk management (Guidelines.* ISO. https://www.iso.org/standard/65694.html

International Organization for Standardization (ISO). (2021). *ISO 22341:2021 Security and resilience (Protective security (Guidelines for Crime Prevention through Environmental Design (CPTED).* ISO. https://www.iso.org/standard/77686.html

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection (Information security management systems (Requirements.* ISO. https://www.iso.org/standard/82875.html

INTERPOL. (2023). *Framework for Countering Unmanned Aircraft Systems (UAS).* INTERPOL. https://www.interpol.int/How-we-work/Innovation/Countering-drones

Joint Authorities for Rulemaking on Unmanned Systems (JARUS). (2024). *SORA – Specific Operations Risk Assessment (v2.0).* JARUS. https://jarus-rpas.org/content/jorus-sora-package

Khawaja, W. Z., Gupta, Y., Feng, Y., & Zaidi, S. (2019). Survey of Air-to-Ground Propagation Channel Models for Unmanned Aerial Vehicles. *IEEE Communications Surveys & Tutorials, 21*(3), 2361–2391. https://doi.org/10.1109/COMST.2019.2892934

Kolgomorov, A. (1933). Sobre la determinación empírica de una ley de distribución. *Giornale dell'Istituto Italiano degli Attuari, 4*, 83-91. https://zbmath.org/59.1166.03

Likert, R. (1932). Una técnica para la medición de la actitud. *Archives of Psychology*(140), 5-55. https://legacy.voteview.com/pdf/Likert_1932.pdf

Lohani, B., & et al. (2022). Perimeter Intrusion Detection Using Computer Vision: A Survey. *IEEE Access, 10*, 95903–95927. https://doi.org/10.1109/ACCESS.2022.3204021

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/

Marfull, A. (2024). El método hipotético deductivo de Karl Popper. *Agenda Juárez: marginalidad, vulnerabilidad y suburbanización del capital*, 16-20. https://www.academia.edu/119569960/El_metodo_hipotetico_deductivo_de_Karl_Popper

Mazza, M. (2024). *Tecnología UAV (Aeronaves No Tripuladas) para aplicarse en la defensa, vigilancia y control de los espacios marítimos.* [Tesis de Maestría], Escuela de Guerra Naval (Argentina). https://cefadigital.edu.ar/handle/1847939/2693

Ministerio de Transportes y Comunicaciones del Perú (MTC). (2025). *Requisitos para operar drones (RPAS) en el Perú*. https://www.gob.pe/mtc/acciones-y-programas/rpas-drones

National Institute of Standards and Technology (NIST). (2022). *Standard Test Methods for Small Unmanned Aircraft Systems (sUAS).* NIST. https://www.nist.gov/programs-projects/standard-test-methods-small-unmanned-aircraft-systems-suas

National Institute of Standards and Technology (NIST). (2024). *NIST Cybersecurity Framework (CSF) 2.0.* NIST. https://www.nist.gov/cyberframework

National Protective Security Authority (NPSA). (2023). *Perimeter Security Guidance.* NPSA. https://www.npsa.gov.uk/guidance/perimeter-security

National Protective Security Authority (NPSA). (2025). *Hostile Vehicle Mitigation Guidance.* NPSA. https://www.npsa.gov.uk/guidance/hostile-vehicle-mitigation

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/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf

Organización de Aviación Civil Internacional (OACI). (2017). *Manual sobre Sistemas de Aeronaves Pilotadas a Distancia (RPAS), Doc 10019.* OACI. https://www.icao.int/safety/UA/Pages/default.aspx

Perez Renteria, L., & Villar Casani, M. (2021). *Sistema aéreo de vigilancia por drones para prevenir y disminuir el nivel de inseguridad ciudadana en el distrito de San Martín de Porres, Lima 2020.* [Tesis de Maestría], Pontificia Universidad Católica del Perú, Escuela de Posgrado. https://tesis.pucp.edu.pe/server/api/core/bitstreams/a0afb0eb-25ef-45a3-a8d3-86d4b878f23e/content

Rodríguez Herrera, J. (2021). *Uso de droness como medios de obtención de datos de inteligencia en operaciones de apoyo a la Policía Nacional de Panamá.* [Trabajo de Suficiencia Profesional], Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". https://repositorio.escuelamilitar.edu.pe/handle/20.500.14803/495

Smirnov, N. (1939). Sobre las desviaciones de la curva de distribución empírica (resumen en ruso y francés). *Matematicheskii Sbornik*, *48*(6), 3-26. https://doi.org/10.1214/aoms/1177730256

Spearman, C. E. (1904). Inteligencia general determinada y medida objetivamente. *The American Journal of Psychology, 15*(2), 201-292. https://doi.org/10.2307/1412107

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Vidal Benítez, R. (2021). *La aplicación de drones a los servicios de vigilancia y seguridad privada.* [Ensayo académico], Universidad Militar Nueva Granada. https://repository.umng.edu.co/handle/10654/38982

Anexos

Anexo 1. Matriz de consistencia

Título: Uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
Problema General ¿Cuál es la relación que existe entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025? **Problema Especifico 1** ¿Cuál es la relación que existe entre la capacitación operativa del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025? **Problema Especifico 2** ¿Cuál es la relación que existe entre la aplicación táctica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025? **Problema Especifico 3** ¿Cuál es la relación que existe entre la gestión tecnológica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025?	**Objetivo General** Determinar la relación que existe entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Objetivo Especifico 1** Determinar la relación que existe entre la capacitación operativa del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Objetivo Especifico 2** Determinar la relación que existe entre la aplicación táctica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Objetivo Especifico 3** Determinar la relación que existe entre la gestión tecnológica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.	**Hipótesis General** Existe relación significativa entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Hipótesis Especifico 1** Existe relación significativa entre la capacitación operativa del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Hipótesis Especifico 2** Existe relación significativa entre la aplicación táctica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025. **Hipótesis Especifico 3** Existe relación significativa entre la gestión tecnológica del drone y la seguridad de las instalaciones de la Escuela Militar de Chorrillos “CFB” Lima, 2025.	**Variable 1** Uso de drones	Capacitación operativa	• Entrenamiento técnico • Certificación piloto • Simulador vuelo • Evaluación desempeño	**Enfoque de investigación** Cuantitativo **Tipo de investigación** Aplicada **Método de investigación** Hipotético-Deductivo **Nivel de investigación** Descriptivo-Correlacional **Diseño de investigación** No experimental transversal **Técnica** Encuesta **Instrumentos** Cuestionario **Población** 1226 cadetes **Muestra** 293 cadetes **Métodos de Análisis de Datos** Estadística Según la prueba de normalidad
				Aplicación táctica	• Reconocimiento aéreo • Vigilancia perímetro • Apoyo logístico • Cobertura eventos	
				Gestión tecnológica	• Mantenimiento preventivo • Actualización software • Integración sistemas • Gestión datos	
			Variable 2 Seguridad de las instalaciones	Control perimetral	• Monitoreo continuo • Detección intrusos • Respuesta inmediata • Supervisión accesos	
				Protección infraestructural	• Inspección estructural • Detección anomalías • Evaluación riesgos • Mantenimiento correctivo	
				Seguridad informacional	• Protección datos • Control accesos • Monitoreo redes • Prevención ciberataques	

Anexo 2. Instrumento de recolección de datos

Uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos "CFB" Lima, 2025

OBJETIVO: Determinar la relación que existe entre el uso de drones y la seguridad de las instalaciones de la Escuela Militar de Chorrillos "CFB" Lima, 2025.

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: USO DE DRONES	VALORACIÓN				
Nro.	**Dimensión 1. Capacitación operativa**	**1**	**2**	**3**	**4**	**5**
1	¿Considero que recibir entrenamiento técnico sobre el uso de drones es fundamental para mejorar las operaciones en la Escuela Militar?					
2	¿Creo que la capacitación técnica en drones debería formar parte obligatoria de nuestra formación militar?					
3	¿Considero importante contar con una certificación oficial para operar drones dentro de la institución?					
4	¿Pienso que obtener una certificación como piloto de drones aumentaría la profesionalización en el uso de esta tecnología?					
5	¿Considero que el uso de simuladores de vuelo para drones facilitaría el aprendizaje y la práctica segura?					
6	¿Pienso que la implementación de simuladores de drones mejoraría la preparación operativa de los cadetes?					
7	¿Creo que realizar evaluaciones periódicas del desempeño en el manejo de drones es necesario para garantizar la efectividad?					
8	¿Considero que la evaluación formal del uso de drones contribuiría a mejorar nuestras habilidades técnicas?					
Nro.	**Dimensión 2. Aplicación táctica**	**1**	**2**	**3**	**4**	**5**
9	¿Pienso que los drones son necesarios para realizar reconocimiento aéreo en zonas difíciles de alcanzar?					
10	¿Considero que el reconocimiento aéreo con drones mejoraría la seguridad y el control del terreno?					
11	¿Creo que la vigilancia del perímetro mediante drones es una necesidad para fortalecer la seguridad institucional?					
12	¿Considero que los drones podrían cubrir eficazmente las áreas de vigilancia que actualmente no se supervisan?					
13	¿Pienso que los drones podrían brindar apoyo logístico en operaciones donde el acceso es complicado?					
14	¿Considero que el uso de drones para transporte y entrega en la escuela facilitaría las tareas operativas?					

15	¿Creo que los drones serían útiles para cubrir eventos y actividades militares desde una perspectiva aérea?					
16	¿Considero que la cobertura de eventos con drones permitiría una mejor supervisión y control?					
Nro.	**Dimensión 3. Gestión tecnológica**	**1**	**2**	**3**	**4**	**5**
17	¿Pienso que es necesario implementar un programa de mantenimiento preventivo para los drones?					
18	¿Considero que el mantenimiento adecuado de los drones es fundamental para su operación segura y continua?					
19	¿Creo que la actualización constante del software de los drones es necesaria para mantener su eficiencia?					
20	¿Considero que contar con software actualizado en los drones mejoraría su desempeño y funcionalidad?					
21	¿Pienso que los drones deben integrarse con otros sistemas tecnológicos de la institución para optimizar su uso?					
22	¿Considero que la integración tecnológica entre drones y sistemas de vigilancia existentes es indispensable?					
23	¿Creo que la gestión adecuada de los datos recolectados por drones es vital para la toma de decisiones?					
24	¿Considero que se debe establecer un sistema eficiente para almacenar y analizar la información proporcionada por drones?					
ÍTEM	**VARIABLE 2: SEGURIDAD DE LAS INSTALACIONES**	**VALORACIÓN**				
Nro.	**Dimensión 1. Control perimetral**	**1**	**2**	**3**	**4**	**5**
25	¿Considero que es necesario implementar un monitoreo continuo del perímetro para prevenir incidentes?					
26	¿Pienso que la vigilancia constante del perímetro fortalecería la seguridad de la escuela?					
27	¿Creo que se deben mejorar los sistemas para detectar intrusos en las instalaciones de forma temprana?					
28	¿Considero que la detección rápida de intrusos es fundamental para evitar riesgos mayores?					
29	¿Pienso que la capacidad de respuesta inmediata ante amenazas debe ser prioritaria en la escuela?					
30	¿Considero que se necesitan protocolos eficaces para actuar rápidamente frente a incidentes de seguridad?					
31	¿Creo que el control y supervisión estricta de los accesos es esencial para la seguridad institucional?					
32	¿Considero que los puntos de acceso deben estar vigilados permanentemente para evitar entradas no autorizadas?					
Nro.	**Dimensión 2. Protección infraestructural**	**1**	**2**	**3**	**4**	**5**
33	¿Pienso que las instalaciones deben ser inspeccionadas regularmente para garantizar su integridad estructural?					
34	¿Considero que la inspección constante ayuda a prevenir daños y accidentes en la infraestructura?					
35	¿Creo que es necesario contar con sistemas para detectar anomalías que puedan comprometer la seguridad física?					
36	¿Considero que la detección temprana de fallas o irregularidades contribuye a la protección de las instalaciones?					

37	¿Pienso que se deben realizar evaluaciones periódicas de riesgos para anticipar posibles amenazas?					
38	¿Considero que la identificación de riesgos es clave para diseñar medidas de protección adecuadas?					
39	¿Creo que el mantenimiento correctivo oportuno es indispensable para conservar la funcionalidad de la infraestructura?					
40	¿Considero que resolver rápidamente las fallas detectadas evita problemas mayores y garantiza la seguridad?					
Nro.	**Dimensión 3. Seguridad informacional**	**1**	**2**	**3**	**4**	**5**
41	¿Pienso que es fundamental proteger los datos sensibles de la institución frente a accesos no autorizados?					
42	¿Considero que la seguridad de la información es vital para la integridad de las operaciones militares?					
43	¿Creo que el control de accesos digitales debe ser riguroso para evitar vulneraciones de seguridad?					
44	¿Considero que solo personal autorizado debe tener acceso a sistemas y datos críticos?					
45	¿Pienso que el monitoreo constante de las redes informáticas es necesario para detectar amenazas cibernéticas?					
46	¿Considero que se deben implementar sistemas que permitan supervisar la actividad en las redes institucionales?					
47	¿Creo que se deben fortalecer las medidas preventivas para evitar ataques cibernéticos en la institución?					
48	¿Considero que la capacitación en ciberseguridad es esencial para prevenir vulnerabilidades en los sistemas?					

Anexo 3. Autorización para la recolección de datos

"Año de la recuperación y consolidación de la economía peruana"

ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

El Coronel Jefe del Departamento de Educación Militar de la Escuela Militar de Chorrillos

"Coronel Francisco Bolognesi", autoriza:

Que los Cadetes de 4to año de Inteligencia, CAYO SALDÍVAR Gonzalo y CCENHUA GÓMEZ Gabriel Isaac, están autorizados para aplicar la encuesta a la muestra/población (Cadetes de la EMCH) para obtener información para el desarrollo de la tesis titulada:

"Uso de drones y su relación con la seguridad de las instalaciones de la Escuela Militar de Chorrillos " CFB," Lima 2025"

Se otorga el presente documento a solicitud de los interesados.

Chorrillos, 01 de julio 2025

O – 2534020793 – O +
ALAN HARRY GARCÍA QUISPE
Coronel Infantería
Jefe Dpto. Edu. Mil. de la Escuela Militar de Chorrillos
"Cnl Francisco Bolognesi"

Anexo 4. Base de datos (de prueba piloto)

	Variable 1: Uso de drone																								Variable 2: Seguridad de las instalaciones															
	D1: Capacitación operativa								D2: Aplicación táctica								D3: Gestión tecnológica								D1: Control perimetral								D2: Protección infraestructural								D3: Seguridad informacional							
n	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**	**P14**	**P15**	**P16**	**P17**	**P18**	**P19**	**P20**	**P21**	**P22**	**P23**	**P24**	**P25**	**P26**	**P27**	**P28**	**P29**	**P30**	**P31**	**P32**	**P33**	**P34**	**P35**	**P36**	**P37**	**P38**	**P39**	**P40**	**P41**	**P42**	**P43**	**P44**	**P45**	**P46**	**P47**	**P48**
1	4	5	3	4	4	4	5	4	3	4	4	5	5	4	4	3	5	2	2	3	4	4	5	4	4	5	5	5	4	4	4	3	3	4	4	4	4	3	3	3	5	5	5	4	5	5	5	4
2	5	3	5	4	4	5	5	2	5	4	5	4	4	3	5	4	5	5	5	5	4	3	5	3	5	4	4	4	3	5	3	4	4	3	4	4	3	4	5	3	4	3	4	4	5	5	3	3
3	4	4	5	5	2	4	3	4	4	3	3	4	4	5	2	5	4	5	3	4	4	5	4	4	5	5	5	2	4	4	4	4	4	4	5	3	3	3	5	5	4	5	4	4	5	4	4	5
4	3	3	4	3	5	5	4	4	4	5	3	4	5	5	2	4	5	4	5	5	4	5	3	4	5	5	3	4	4	4	5	5	5	4	5	4	5	1	4	4	2	4	5	5	4	4	5	5
5	5	4	4	4	4	3	3	4	4	5	5	5	3	4	5	3	4	5	5	5	5	3	5	3	5	5	4	4	3	4	4	3	5	5	4	5	3	5	5	5	2	5	4	5	5	5	4	4
6	3	4	4	5	4	3	5	3	5	4	5	3	5	3	5	5	4	5	3	4	4	3	5	5	5	4	3	4	5	4	5	5	4	5	3	4	5	5	5	3	5	5	5	5	1	4	3	3
7	5	4	4	2	3	4	4	4	4	2	4	4	5	5	4	4	5	3	5	4	4	5	2	5	5	3	5	4	5	4	4	5	4	5	4	4	3	3	2	5	5	5	4	5	4	4	3	5
8	5	2	4	5	5	5	5	3	3	5	4	3	4	5	3	4	5	5	5	5	4	4	5	5	5	5	4	5	5	4	5	4	5	3	3	4	5	5	5	4	5	4	5	4	4	5	5	5
9	4	3	2	5	4	3	4	4	4	4	5	5	4	4	3	4	4	4	4	5	5	3	5	3	3	5	3	4	4	4	4	4	4	4	4	5	4	3	4	5	5	5	4	5	4	4	3	4
10	5	5	5	5	3	5	4	5	4	4	2	5	5	3	5	5	2	4	4	3	4	4	4	3	4	5	4	5	3	4	5	3	4	4	4	5	5	3	5	5	4	4	5	5	5	4	4	5
11	5	4	2	4	5	5	4	3	3	3	5	5	5	4	4	5	5	5	5	4	5	5	4	4	5	3	4	3	4	5	4	5	3	3	4	5	5	4	5	5	4	4	4	5	5	4	5	5
12	5	3	4	5	5	4	5	5	4	4	5	5	5	4	5	5	4	5	5	5	5	5	4	3	5	4	3	4	5	3	5	4	4	4	3	5	3	4	4	4	4	4	4	4	3	5	4	4
13	4	5	4	5	5	5	4	5	5	3	5	5	4	3	5	3	4	3	5	3	5	3	4	5	5	4	4	5	4	4	5	4	4	5	3	4	4	4	4	2	3	3	5	3	4	5	5	5
14	3	3	3	3	4	4	4	3	3	4	4	4	3	5	5	5	5	5	3	5	4	5	5	5	4	3	4	5	4	5	4	5	4	4	5	3	4	5	5	3	4	5	3	3	5	4	5	3
15	2	4	4	5	4	4	4	4	4	5	5	5	5	4	5	3	4	4	5	3	3	5	5	5	5	4	4	5	4	5	4	5	5	4	5	3	5	4	3	4	5	5	4	4	4	3	4	5
16	4	5	4	3	5	5	3	5	3	3	3	4	5	5	5	3	4	4	4	4	4	5	5	4	4	4	4	5	5	3	5	5	4	4	5	5	5	5	4	5	5	4	5	4	5	3	4	4
17	5	4	3	5	5	4	4	4	5	4	4	5	4	4	4	5	3	4	3	2	5	4	4	5	4	4	5	5	5	3	4	3	4	3	4	5	4	4	4	3	5	4	3	4	5	5	5	5
18	5	5	5	5	5	5	3	2	4	4	5	3	4	5	5	5	4	5	4	4	4	5	5	4	5	4	3	5	4	3	4	4	5	2	5	4	5	4	4	5	3	5	5	4	3	5	4	5
19	4	5	5	4	5	4	4	3	4	5	4	3	4	4	5	4	5	5	5	5	4	5	3	4	4	5	3	5	5	3	5	4	4	5	4	3	3	3	4	3	4	4	4	2	3	5	2	5
20	5	5	3	4	5	5	3	5	5	3	5	4	3	4	3	5	4	5	3	4	5	3	5	3	3	4	4	5	4	4	4	3	4	5	3	5	3	5	4	5	3	2	5	5	5	5	3	5

Anexo 5. Base de datos (origen de resultados)

	V1: Uso de drones	D1: Capacitación operativa	D2: Aplicación táctica	D3: Gestión tecnológica	V2: Seguridad de las instalaciones	D1: Control perimetral	D2: Protección infraestructural	D3: Seguridad informacional
n	**V1**	**V1-D1**	**V1-D2**	**V1-D3**	**V2**	**V2-D1**	**V2-D2**	**V2-D3**
1	94	33	32	29	100	34	28	38
2	102	33	34	35	93	32	30	31
3	94	31	30	33	100	33	32	35
4	98	31	32	35	101	35	32	34
5	100	31	34	35	103	32	37	34
6	99	31	35	33	100	35	34	31
7	95	30	32	33	100	35	30	35
8	103	34	31	38	108	37	34	37
9	95	29	33	33	98	31	33	34
10	98	37	33	28	104	33	35	36
11	103	32	34	37	103	33	34	36
12	109	36	37	36	96	33	31	32
13	102	37	33	32	98	35	30	33
14	97	27	33	37	99	34	33	32
15	101	31	36	34	103	36	33	34
16	99	34	31	34	106	35	37	34
17	99	34	35	30	100	33	31	36
18	105	35	35	35	100	32	34	34
19	103	34	33	36	92	34	29	29
20	99	35	32	32	98	31	34	33
21	98	36	31	31	103	32	35	36
22	99	31	34	34	99	34	30	35
23	104	34	37	33	91	28	34	29
24	105	35	34	36	103	32	35	36
25	102	32	32	38	96	35	29	32
26	96	32	32	32	92	29	30	33
27	97	31	33	33	98	36	33	29
28	91	33	30	28	103	34	35	34
29	95	32	31	32	99	33	36	30
30	100	33	31	36	103	36	36	31
31	99	30	33	36	96	29	32	35
32	101	31	36	34	104	34	34	36
33	101	34	35	32	107	34	36	37
34	107	37	33	37	101	30	34	37
35	101	36	33	32	103	35	32	36
36	105	35	33	37	101	31	33	37
37	100	34	32	34	103	35	35	33
38	102	35	34	33	103	36	39	28
39	91	32	28	31	102	34	33	35
40	101	34	35	32	104	37	33	34
41	102	34	34	34	98	30	31	37
42	98	32	32	34	103	35	32	36
43	100	35	34	31	100	30	33	37
44	96	34	30	32	94	34	30	30
45	99	33	35	31	95	33	30	32
46	89	28	31	30	95	29	36	30
47	94	33	30	31	100	31	34	35
48	107	35	38	34	97	33	32	32
49	96	32	31	33	106	39	33	34
50	96	31	34	31	104	34	34	36

51	104	36	34	34	98	32	35	31
52	103	36	33	34	99	36	32	31
53	98	30	33	35	101	34	30	37
54	94	31	32	31	106	34	37	35
55	88	32	30	26	95	32	32	31
56	102	33	34	35	98	32	34	32
57	98	36	33	29	102	32	35	35
58	101	32	32	37	98	32	32	34
59	99	36	31	32	103	38	34	31
60	99	33	34	32	100	32	33	35
61	99	30	35	34	97	35	29	33
62	102	34	35	33	102	35	33	34
63	96	32	35	29	114	39	39	36
64	104	34	32	38	100	36	33	31
65	103	36	34	33	101	34	33	34
66	97	30	35	32	91	32	29	30
67	99	32	33	34	104	31	37	36
68	99	35	28	36	99	34	33	32
69	97	31	31	35	97	31	35	31
70	103	35	33	35	100	32	34	34
71	90	30	32	28	94	33	27	34
72	98	33	33	32	99	34	32	33
73	99	34	34	31	102	34	33	35
74	94	31	32	31	98	37	30	31
75	107	38	36	33	100	32	34	34
76	94	27	33	34	110	37	38	35
77	103	32	38	33	92	31	29	32
78	99	33	35	31	96	32	32	32
79	99	31	34	34	98	32	33	33
80	100	36	32	32	102	32	38	32
81	103	33	35	35	103	34	37	32
82	96	34	31	31	97	31	32	34
83	108	36	36	36	102	32	36	34
84	97	34	32	31	105	34	34	37
85	96	28	31	37	101	30	36	35
86	97	31	33	33	101	38	33	30
87	104	37	34	33	98	36	32	30
88	101	32	34	35	99	37	33	29
89	101	35	33	33	91	29	30	32
90	107	34	37	36	99	30	36	33
91	102	36	33	33	102	36	33	33
92	105	37	33	35	99	33	33	33
93	104	34	37	33	105	38	31	36
94	98	30	34	34	97	35	32	30
95	98	33	31	34	99	34	32	33
96	98	32	35	31	97	29	35	33
97	102	33	36	33	105	36	33	36
98	107	34	36	37	105	34	35	36
99	99	32	32	35	100	31	35	34
100	100	34	35	31	95	31	32	32
101	94	37	28	29	103	35	36	32
102	101	34	35	32	101	34	33	34
103	101	38	33	30	107	37	33	37
104	99	31	35	33	107	37	35	35
105	107	35	39	33	100	33	31	36
106	101	35	34	32	100	32	34	34
107	102	36	31	35	96	30	34	32

108	92	34	27	31	110	36	38	36
109	100	33	34	33	104	32	35	37
110	98	31	34	33	99	32	35	32
111	96	29	34	33	96	36	29	31
112	103	34	33	36	97	33	32	32
113	105	35	35	35	104	37	36	31
114	98	31	33	34	95	32	30	33
115	100	37	32	31	98	33	34	31
116	102	37	33	32	97	32	33	32
117	99	34	30	35	96	34	32	30
118	92	34	29	29	93	32	31	30
119	96	30	32	34	94	32	34	28
120	102	33	35	34	104	35	34	35
121	97	35	26	36	103	35	35	33
122	97	31	29	37	102	36	31	35
123	98	36	31	31	92	31	30	31
124	102	34	32	36	90	33	30	27
125	100	33	34	33	96	30	34	32
126	103	35	34	34	96	31	34	31
127	99	33	34	32	91	28	31	32
128	105	36	37	32	100	33	34	33
129	101	36	32	33	97	32	32	33
130	95	31	31	33	94	35	30	29
131	103	33	34	36	99	31	32	36
132	99	31	36	32	102	36	30	36
133	103	36	34	33	100	33	37	30
134	93	32	27	34	98	30	34	34
135	96	29	35	32	92	30	33	29
136	98	34	33	31	103	35	34	34
137	101	36	31	34	95	34	32	29
138	102	33	33	36	99	32	34	33
139	94	31	35	28	100	35	36	29
140	99	33	33	33	98	32	31	35
141	97	31	33	33	97	34	31	32
142	90	28	32	30	98	38	31	29
143	103	37	34	32	103	38	32	33
144	99	29	35	35	104	36	34	34
145	104	30	36	38	106	34	35	37
146	102	34	38	30	100	33	35	32
147	102	33	35	34	100	34	31	35
148	106	36	35	35	94	34	31	29
149	94	32	30	32	103	34	33	36
150	99	32	34	33	101	30	36	35
151	93	32	30	31	97	32	35	30
152	94	34	31	29	88	32	30	26
153	94	30	33	31	101	35	35	31
154	99	31	37	31	107	38	37	32
155	97	30	31	36	99	33	33	33
156	98	30	35	33	103	37	30	36
157	98	33	34	31	90	32	27	31
158	98	32	34	32	99	33	36	30
159	99	34	31	34	98	35	34	29
160	96	29	36	31	104	35	34	35
161	102	31	38	33	105	38	34	33
162	92	34	29	29	96	33	32	31
163	98	34	29	35	95	32	28	35
164	93	31	31	31	98	31	35	32

165	99	32	34	33	99	31	33	35
166	92	34	27	31	97	30	35	32
167	100	36	30	34	92	35	30	27
168	91	31	29	31	92	32	34	26
169	96	32	30	34	98	32	34	32
170	103	38	28	37	100	31	35	34
171	98	33	32	33	100	33	37	30
172	104	37	33	34	98	32	31	35
173	103	34	37	32	104	38	32	34
174	101	35	35	31	97	29	34	34
175	101	32	35	34	102	36	36	30
176	98	32	35	31	97	36	30	31
177	101	36	33	32	104	33	37	34
178	95	31	33	31	96	31	30	35
179	98	32	32	34	97	31	32	34
180	98	30	36	32	105	33	35	37
181	95	31	33	31	106	38	31	37
182	94	34	31	29	101	36	32	33
183	106	31	38	37	91	28	30	33
184	98	34	37	27	105	34	35	36
185	104	38	35	31	103	35	37	31
186	102	36	36	30	100	34	34	32
187	102	33	34	35	106	35	34	37
188	98	35	32	31	93	31	31	31
189	99	36	31	32	97	27	35	35
190	97	35	30	32	95	30	33	32
191	95	35	26	34	99	35	32	32
192	99	33	31	35	99	32	36	31
193	99	32	34	33	102	37	33	32
194	95	30	32	33	105	35	34	36
195	101	37	31	33	100	33	34	33
196	104	37	35	32	98	34	32	32
197	106	35	37	34	98	31	30	37
198	102	33	32	37	105	36	37	32
199	103	36	33	34	98	36	27	35
200	96	34	32	30	100	32	35	33
201	103	38	34	31	97	33	30	34
202	104	32	36	36	109	37	35	37
203	99	34	31	34	93	32	29	32
204	100	35	34	31	99	33	33	33
205	99	35	32	32	97	30	35	32
206	102	32	34	36	98	28	33	37
207	102	34	36	32	98	34	33	31
208	105	37	33	35	94	34	30	30
209	98	31	34	33	107	36	36	35
210	94	31	31	32	104	33	38	33
211	96	33	32	31	97	30	34	33
212	101	35	32	34	98	34	31	33
213	108	39	32	37	104	34	33	37
214	99	33	30	36	104	32	35	37
215	99	33	34	32	101	29	35	37
216	106	35	38	33	97	37	30	30
217	102	33	36	33	95	30	31	34
218	107	36	34	37	99	32	37	30
219	98	32	34	32	104	32	37	35
220	105	34	38	33	97	32	34	31
221	103	35	32	36	105	34	36	35

222	108	36	37	35	103	35	32	36
223	109	36	36	37	104	36	34	34
224	100	30	33	37	100	35	34	31
225	104	31	38	35	102	34	36	32
226	105	39	33	33	99	34	34	31
227	93	30	31	32	105	34	35	36
228	99	32	35	32	94	28	34	32
229	104	34	35	35	101	35	33	33
230	101	32	34	35	96	29	32	35
231	98	30	34	34	100	36	35	29
232	91	28	28	35	104	35	35	34
233	101	30	36	35	100	35	33	32
234	109	35	37	37	93	31	30	32
235	97	32	32	33	88	30	26	32
236	96	33	30	33	99	31	33	35
237	94	29	32	33	103	32	38	33
238	103	34	33	36	102	34	33	35
239	99	30	36	33	98	30	32	36
240	105	36	34	35	91	29	32	30
241	108	37	36	35	102	34	35	33
242	97	33	30	34	104	34	38	32
243	97	33	30	34	100	35	31	34
244	97	32	33	32	99	33	33	33
245	104	35	36	33	101	34	33	34
246	99	32	34	33	99	31	34	34
247	94	30	34	30	104	34	34	36
248	101	34	35	32	93	30	32	31
249	98	33	35	30	102	33	35	34
250	102	33	35	34	104	35	33	36
251	98	32	34	32	107	35	36	36
252	104	31	35	38	101	32	35	34
253	102	34	35	33	100	32	35	33
254	106	33	36	37	100	33	35	32
255	100	29	36	35	100	30	34	36
256	102	31	32	39	96	33	30	33
257	96	29	32	35	102	34	34	34
258	98	31	34	33	96	35	33	28
259	99	32	33	34	98	32	31	35
260	96	30	32	34	97	32	32	33
261	108	34	36	38	104	35	32	37
262	94	35	30	29	103	36	36	31
263	95	31	29	35	99	35	31	33
264	100	31	37	32	103	33	34	36
265	103	31	34	38	99	34	33	32
266	105	34	32	39	105	35	31	39
267	103	36	36	31	99	32	33	34
268	96	32	32	32	95	31	34	30
269	96	30	31	35	95	31	32	32
270	104	36	34	34	100	35	31	34
271	107	37	37	33	100	33	32	35
272	99	31	35	33	104	35	35	34
273	98	29	36	33	104	35	33	36
274	98	32	33	33	103	35	35	33
275	105	36	33	36	102	34	36	32
276	100	30	33	37	94	33	29	32
277	104	30	36	38	92	32	31	29
278	103	34	36	33	90	27	30	33

279	104	32	35	37	103	31	37	35
280	91	29	30	32	99	32	33	34
281	97	30	34	33	100	36	31	33
282	102	33	35	34	92	30	30	32
283	97	34	32	31	100	35	33	32
284	87	29	27	31	97	31	35	31
285	90	29	28	33	105	35	36	34
286	96	33	32	31	97	32	33	32
287	103	34	34	35	93	29	32	32
288	99	32	31	36	97	35	30	32
289	100	33	33	34	97	31	34	32
290	100	35	33	32	99	34	34	31
291	96	33	31	32	98	31	32	35
292	104	35	35	34	102	36	29	37
293	101	32	34	35	104	34	34	36

Anexo 6. Propuesta de mejora

En relación a la Objetivo General, se propone mejorar la infraestructura tecnológica y logística para la implementación efectiva del uso de drones en la Escuela Militar de Chorrillos "CFB". Esto implica la inversión en equipos de última generación, la creación de áreas especializadas para almacenamiento, mantenimiento y operación, así como la capacitación continua del personal técnico y operativo. Además, se recomienda establecer alianzas estratégicas con fabricantes y expertos en tecnología UAV para mantener actualizados los sistemas y obtener soporte técnico especializado. También es fundamental diseñar un plan de integración tecnológica que contemple la interoperabilidad de los drones con otros sistemas de vigilancia y defensa existentes en la institución. Se sugiere, asimismo, la creación de un centro de mando y control que permita la monitorización en tiempo real de las operaciones aéreas, optimizando la respuesta ante situaciones críticas. Estas acciones contribuirán a que el uso de drones no solo sea una mejora tecnológica aislada, sino un elemento integral de la seguridad institucional, aumentando la efectividad y la confianza en la protección de las instalaciones.

En relación a la Objetivo Específico 1, la propuesta de mejora está enfocada en fortalecer y diversificar los programas de capacitación operativa en drones. Se recomienda implementar un currículo estructurado que combine teoría y práctica, utilizando simuladores de vuelo para reducir riesgos y mejorar el aprendizaje antes de la operación en campo real. Además, es esencial incorporar evaluaciones periódicas y certificaciones que garanticen el dominio de habilidades técnicas y tácticas. Se debe promover la formación multidisciplinaria, integrando conocimientos en mantenimiento, normativa legal y ciberseguridad, para formar operadores completos y conscientes de las responsabilidades inherentes. También se sugiere la realización de talleres y cursos de actualización que mantengan a los cadetes al día con los avances tecnológicos y tácticos. Esta mejora en la capacitación asegurará un uso eficiente y seguro de los drones, aumentando la confianza en las capacidades operativas del personal y, por ende, la seguridad institucional.

En relación a la Objetivo Específico 2, se plantea optimizar la aplicación táctica del dron mediante la elaboración y estandarización de protocolos operativos que definan roles, procedimientos y flujos de trabajo claros durante las misiones de vigilancia y reconocimiento. Se recomienda la incorporación de ejercicios y simulacros regulares que permitan evaluar la eficacia de las tácticas y mejorar la coordinación entre operadores y otros equipos de seguridad. Asimismo, es importante fomentar la integración de drones con otros sistemas tecnológicos y

de inteligencia para maximizar la cobertura y calidad de la información recolectada. Se sugiere desarrollar un sistema de análisis y retroalimentación que permita identificar áreas de mejora en la aplicación táctica, facilitando ajustes y perfeccionamiento continuo. Estas acciones fortalecerán la capacidad operativa, incrementarán la efectividad de las misiones y mejorarán la percepción de seguridad entre el personal y la institución.

En relación a la Objetivo Específico 3, la propuesta de mejora consiste en consolidar un sistema integral de gestión tecnológica para drones que incluya planes de mantenimiento preventivo rigurosos, actualización constante del software y protocolos para la gestión eficiente de datos. Se recomienda establecer un equipo especializado responsable de la supervisión y optimización de estos procesos, asegurando la disponibilidad y operatividad continua de los equipos. Además, es fundamental implementar medidas de seguridad informática que protejan la integridad y confidencialidad de la información recopilada, así como políticas claras sobre el uso y manejo de datos. También se sugiere la inversión en herramientas tecnológicas avanzadas que permitan la integración fluida de drones con otros sistemas de seguridad y control institucional. Estas mejoras garantizarán la sostenibilidad y eficacia de la gestión tecnológica, reforzando la protección y confianza en la seguridad de las instalaciones militares.

Anexo 7. Validación por juicio de expertos

ESCUELA MILITAR DE CHORRILLOS "CFB"
4TO AÑO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

APELLIDOS Y NOMBRES DEL INFORMANTE-EXPERTO	INSTITUCIÓN DONDE LABORA EXPERTO	NOMBRE DEL INSTRUMENTO	AUTOR DEL INSTRUMENTO
DR. VASQUEZ MORA EDWIN	Ejército del Perú	Cuestionario (encuesta)	CAD IV INTG CAYO SALDIVAR GONZALO CAD IV INTG CCENHUA GOMEZ GABRIEL ISAAC

TÍTULO DE LA INVESTIGACIÓN:
USO DE DRONES Y SU RELACION CON LA SEGURIDAD DE LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS, "CFB" 2025

I. ASPECTOS DE EVALUACIÓN

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	DEFICIENTE 0 - 20	REGULAR 21 - 40	BUENA 41 - 60	MUY BUENA 61 - 85	EXCELENTE 86 - 100	SUB TOTAL
1. Claridad	Esta formulado con lenguaje apropiado.					100	100
2. Objetividad	Esta expresado en conductas Observables.					100	100
3. Actualización	Está adecuado al avancede la ciencia y la tecnologia.				85		85
4.Organizacion	Esta organizado en forma Lógica.					100	100
5. Suficiencia	Comprende aspectos cuantitativos				85		85
6. Intencionalidad	Es adecuado para medir los aspectos de interés				85		85
7. Consistencia	Está basado en aspectos teóricos científicos.				85		85
8. Coherencia	Entre las variables, dimensiones, indicadores e Ítems.				85		85
9. Metodología.	La estrategia responde al propósito de la investigación.					100	100
10. Pertinencia	Las dimensiones consideradas permiten evaluar la variable en su conjunto.			60			60
TOTAL							**885**
TOTAL (en %) / 10							**88.5**

II. PROMEDIO DE VALORACIÓN: 88.5%

III. OPINIÓN DE APLICACIÓN

Valoración cuantitativa: 88.5
Valoración cualitativa: Excelente
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	Nº DE TELEFONO
Chorrillos, 22 de setiembre 2025	43343660		949675428

ESCUELA MILITAR DE CHORRILLOS "CFB"
4TO AÑO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

APELLIDOS Y NOMBRES DEL INFORMANTE-EXPERTO	INSTITUCIÓN DONDE LABORA EXPERTO	NOMBRE DEL INSTRUMENTO	AUTOR DEL INSTRUMENTO
DR. ZAVALETA RAMOS HUMBERTO	Ejército del Perú	Cuestionario (encuesta)	CAD IV INTG CAYO SALDIVAR GONZALO CAD IV INTG CCENHUA GOMEZ GABRIEL ISAAC

TÍTULO DE LA INVESTIGACIÓN:
USO DE DRONES Y SU RELACION CON LA SEGURIDAD DE LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS, "CFB" 2025

I. ASPECTOS DE EVALUACIÓN

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	DEFICIENTE 0 - 20	REGULAR 21 - 40	BUENA 41 - 60	MUY BUENA 61 - 85	EXCELENTE 86 - 100	SUB TOTAL
1. Claridad	Esta formulado con lenguaje apropiado.					100	100
2. Objetividad	Esta expresado en conductas Observables.					100	100
3. Actualización	Está adecuado al avancede la ciencia y la tecnología.					100	100
4.Organizacion	Esta organizado en forma Lógica.				85		85
5. Suficiencia	Comprende aspectos cuantitativos				85		85
6. Intencionalidad	Es adecuado para medir los aspectos de interés				85		85
7. Consistencia	Está basado en aspectos teóricos científicos.				85		100
8. Coherencia	Entre las variables, dimensiones, indicadores e Ítems.				85		100
9. Metodología.	La estrategia responde al propósito de la investigación.					100	100
10. Pertinencia	Las dimensiones consideradas permiten evaluar la variable en su conjunto.			60			60
TOTAL							**885**
TOTAL (en %) / 10							**88.5**

II. PROMEDIO DE VALORACIÓN: 88.5%

III. OPINIÓN DE APLICACIÓN

Valoración cuantitativa: 91.5
Valoración cualitativa: Excelente
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
Chorrillos, 22 de setiembre 2025	43903557		988557277

pESCUELA MILITAR DE CHORRILLOS "CFB"
4TO AÑO
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

APELLIDOS Y NOMBRES DEL INFORMANTE-EXPERTO	INSTITUCIÓN DONDE LABORA EXPERTO	NOMBRE DEL INSTRUMENTO	AUTOR DEL INSTRUMENTO
DR. ZEA MELODIAS RODOLFO	Ejército del Perú	Cuestionario (encuesta)	CAD IV INTG CAYO SALDIVAR GONZALO CAD IV INTG CCENHUA GOMEZ GABRIEL ISAAC

TÍTULO DE LA INVESTIGACIÓN:
USO DE DRONES Y SU RELACION CON LA SEGURIDAD DE LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS, "CFB" 2025

I. ASPECTOS DE EVALUACIÓN

Indicadores de evaluación del instrumento	Criterios Cualitativos Cuantitativos	DEFICIENTE	REGULAR	BUENA	MUY BUENA	EXCELENTE	SUB TOTAL
		0 - 20	21 - 40	41 - 60	61 - 85	86 - 100	
1. Claridad	Esta formulado con lenguaje apropiado.					100	100
2. Objetividad	Esta expresado en conductas Observables.					100	100
3. Actualización	Está adecuado al avancede la ciencia y la tecnología.				85		85
4.Organizacion	Esta organizado en forma Lógica.					100	100
5. Suficiencia	Comprende aspectos cuantitativos				85		85
6. Intencionalidad	Es adecuado para medir los aspectos de interés				85		85
7. Consistencia	Está basado en aspectos teóricos científicos.				85		85
8. Coherencia	Entre las variables, dimensiones, indicadores e Ítems.				85		85
9. Metodología.	La estrategia responde al propósito de la investigación.					100	100
10. Pertinencia	Las dimensiones consideradas permiten evaluar la variable en su conjunto.			60			60
TOTAL							**885**
TOTAL (en %) / 10							**88.5**

II. PROMEDIO DE VALORACIÓN: 88.5%

III. OPINIÓN DE APLICACIÓN

Valoración cuantitativa: 88.5
Valoración cualitativa: Excelente.
Opinión de aplicabilidad: El instrumento es válido y se puede aplicar.

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N° DE TELEFONO
Chorrillos, 22 de setimbre 2025	29388850		996597713

Anexo 8. Dictamen Final Revisor

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

"Año de la recuperación y consolidación de la economía peruana"

ESCUELA MILITAR DE CHORRILLOS CRL. FRANCISCO BOLOGNESI

DICTAMEN FINAL

VISTA LA TESIS:

Estilos de aprendizaje y el rendimiento académico de los cadetes de cuarto año de Infantería de la Escuela Militar de Chorrillos "CFB", 2025 presentado por los graduandos:

Gonzalo Cayo Saldivar
Gabriel Isaac Ccenhua Gómez

CONSIDERANDO:

Que ha sido elaborada conforme a lo dispuesto por el artículo 41. ° del Reglamento del Sistema de Investigación de la EMCH "CFB" 2022 – 2026, y levantadas las observaciones prescritas durante el proceso del análisis y revisión de la referida tesis, los suscritos:

Mg RENGIFO RENGIFO LEWIS: Revisor Temático
Dr INFANTES RIVERA PEDRO: Revisor Metodológico

Dictaminamos que, la tesis en referencia, esta expedita para ser sustentada, el día, hora, lugar y ante el jurado que determine la Resolución Directoral de la Escuela Militar de Chorrillos "CFB" para cuyo efecto, firmamos el presente dictamen.

.

Lima, 05 de diciembre de 2025

Mg LEWIS RENGIFO RENGIFO
Revisor Temático
DNI: 43302563

Dr PEDRO INFANTES RIVERA
Revisor Metodológico
DNI: 43289833

Anexo 9. Acta de sustentación

"Año de la recuperación y consolidación de la economía peruana"

ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

ACTA DE SUSTENTACIÓN DE TESIS DE LA PROMOCIÓN CXXXII

En el distrito de Chorrillos de la ciudad de Lima, siendo las 11.00 horas del día 23 de diciembre de 2025, se dio inicio a la sustentación de la Tesis titulada:

Uso de Drones y su relación con la Seguridad de las Instalaciones de la Escuela Militar de Chorrillos "CFB" Lima 2025

Presentada por:

BACH. Cayo Saldivar Gonzalo

BACH. Cecilia Gomez Gabriel Ispac

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

Presidente: Dr. Yataco Velasquez Luis Andres.

Secretario Msc Zea Melodias Rodrigo

Vocal : Dra Baldeon Espichan Maritza Roxana

Concluida la sustentación, los miembros del Jurado dictaminaron:

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

Habiendo obtenido la nota de: trece (13)

Siendo las 11.40 horas del día 23 de diciembre de 2025, se dio por concluido el presente acto académico, firmando los miembros del Jurado.

DNI: 10646760
VOCAL Dra Maritza Baldeon Espichan

DNI: 25337850
SECRETARIO
Msc Rodrigo Zea Melodias

DNI: 45329465
PRESIDENTE
Dr. Luis A. Yataco Velasquez

Anexo 10. Otros