COMANDO DE EDUCACIÓN Y DOCTRINA DEL EJÉRCITO
ESCUELA MILITAR DE CHORRILLOS

TRABAJO DE SUFICIENCIA PROFESIONAL PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES CON MENCIÓN EN ADMINISTRACIÓN

COMUNICACIONES OPERATIVAS EN EL BATALLÓN DE COMUNICACIONES N° 113 Y LA INTEGRACIÓN DE PROTOCOLOS DIGITALES Y CAPACITACIÓN TÁCTICA ESPECIALIZADA

PRESENTADO POR EL BACHILLER:

Silva Avila David Alonso

CÓDIGO ORCID N° 0009 0006 3829 7577

LIMA – PERÚ

2025

6% 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

6% Fuentes de Internet
1% Publicaciones
3% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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

DEDICATORIA

A mi familia, por su paciencia y respaldo constante. A mis instructores y superiores, por su guía profesional.

AGRADECIMIENTO

Al Batallón de Comunicaciones N° 113 por facilitar el desarrollo de esta experiencia, a mi asesor por sus observaciones técnicas y a mis compañeros de trabajo por su compromiso en cada actividad.

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de suficiencia profesional propone el Sistema Táctico Integrado de Comunicaciones Digitales (STICD) como solución integral a las deficiencias críticas identificadas en las comunicaciones operativas del Batallón de Comunicaciones N° 113 durante el período 2023-2024. A partir de la experiencia directa como Comandante de Compañía y la formación especializada en Operaciones Cibernéticas, se diagnosticó que los tiempos de transmisión de órdenes alcanzaban 15-20 minutos, existía 12% de pérdida de información crítica y solo 15% del personal contaba con capacitación en tecnologías digitales, lo cual limitaba severamente la efectividad táctica de la unidad. La propuesta integra cinco componentes innovadores: la Plataforma Digital Táctica Offline COMSEG-113 que funciona sin internet mediante tablets ruguerizadas con encriptación AES-256, el Centro de Operaciones Modernizado COC 4.0 con Muro Situacional Digital interactivo, los Protocolos Digitales Estandarizados incluyendo codificación dinámica, el Programa de Capacitación Escalonada COMTAC-113 diferenciado por niveles jerárquicos, y el Simulador Táctico SIM-COM 113 para entrenamiento virtual. Se proyecta reducir 70% los tiempos de transmisión, eliminar completamente la pérdida de información y capacitar al 100% del personal en un plazo de doce meses, posicionando al Batallón como unidad modelo en comunicaciones tácticas digitales del Ejército del Perú.

Palabras clave: Comunicaciones militares, protocolos digitales, ciberseguridad operativa, capacitación táctica, modernización tecnológica.

INTRODUCCIÓN

La investigación profesional que se presenta en el trabajo de suficiencia profesional es el resultado de la experiencia directa como Comandante de Compañía de Comunicaciones del Batallón de Comunicaciones N° 113, que pertenecía a la 3ra Brigada de Comunicaciones - Agrupamiento "José Olaya" del Ejército del Perú, durante los años 2023 y 2024. Las razones personales justificativas de esta investigación giran en torno a la inquietud profesional provocada por la observación, prácticamente a diario, de las deficiencias críticas en las comunicaciones operativas de la unidad bajo mi mando y las consecuencias que dichas deficiencias estaban ocasionando en la capacidad de respuesta táctica, en la seguridad de la información y en la eficaz ejecución de operaciones. Esta inquietud se vio reforzada por la formación especializada en Operaciones Cibernéticas que obtuve durante el año 2020 y por el Curso Táctico de Comunicaciones.

Desde el ámbito profesional, la responsabilidad inherente al mando de aproximadamente cien efectivos militares y la misión institucional de proporcionar comunicaciones seguras para la III División del Ejército, en la Región Militar del Sur exigían la reflexión sobre la manera de adoptar sistemas que permitiesen sustituir aquellos que eran obsoletos, pero que no resultaban eficientes en las operaciones modernas. La ubicación del Batallón en Tiabaya, Arequipa, con su geografía complicada que era urbana, rural y montañosa, pero difícilmente conectada con la alta estratificación de la calidad de las señales, la escasa conectividad y la escasa diversidad en los sistemas de comunicación que no estaban directamente relacionados con el medio militar desarrollado, exigían que las propuestas técnicas adoptadas incorporasen características específicas que eran propias del contexto que se obtenía.

El presente trabajo se desarrolla a través de tres capítulos que abordan respectivamente la problemática expuesta y la solución propuesta. El Capítulo I expone la información general sobre el Batallón de Comunicaciones N° 113. Para ello, se proporcionan datos sobre su ubicación geográfica, en Tiabaya, Arequipa, su misión institucional: proveer apoyo de comunicaciones a la III División del Ejército; así también las funciones que desempeñé el propio trabajo de investigación como Comandante de Compañía desde los años 2023-2024, incluyendo la planificación de entrenamiento táctico, la administración de recursos y la ejecución de ciberseguridad. El Capítulo II desarrolla el marco

teórico que da soporte a la propuesta, en el que también se recogen antecedentes internacionales y nacionales sobre modernización de las comunicaciones militares, operaciones de información y gestión del conocimiento de las fuerzas armadas contemporáneas, así como las bases teóricas sobre comunicaciones tácticas, protocolos digitales, criptografía militar, inteligencia artificial aplicada a las comunicaciones y ciberseguridad operativa, y que proporcionan el soporte conceptual necesario para entender la importancia estratégica de las comunicaciones digitales en el marco militar actual.

El Capítulo III constituye el núcleo del trabajo, presentando la descripción detallada de la experiencia profesional mediante cuatro secciones fundamentales: primero, el campo de aplicación que delimita el ámbito geográfico, funcional, temporal y poblacional de la propuesta; segundo, el tipo de aplicación que caracteriza la innovación tecnológica, organizacional y pedagógica que representa el Sistema Táctico Integrado de Comunicaciones Digitales (STICD); tercero, el diagnóstico exhaustivo de la situación actual que identifica deficiencias críticas en rapidez de transmisión de órdenes, coordinación entre unidades, seguridad de la información y efectividad táctica, cuantificando mediante indicadores concretos las brechas entre la situación actual y los estándares deseados; y cuarto, la propuesta de innovación que describe detalladamente los cinco componentes del STICD: la Plataforma Digital Táctica Offline COMSEG-113, el Centro de Operaciones Modernizado COC 4.0, los Protocolos Digitales Estandarizados, el Programa de Capacitación Escalonada COMTAC-113 y el Simulador Táctico SIM-COM 113, incluyendo especificaciones técnicas, cronogramas de implementación, presupuestos detallados e indicadores de éxito medibles.

Y por último, el trabajo finaliza con una reflexión a partir de los efectos esperados de la implementación del STICD, ya que, aunque la propuesta presentada no se ha materializado en la realidad, se espera lograr una reducción del 70 % de los tiempos de transmisión de órdenes, así como una eliminación total de la pérdida de información crítica y la capacitación total del 100% de los trabajadores y trabajadoras en protocolos digitales y ciber operativos de seguridad y defensa. De igual forma, se incluyen recomendaciones estratégicas orientadas a la obtención de una correcta

implementación del STICD: la propuesta de una estrategia de implementación por fases, iniciando con una compañía piloto, la mejora del establecimiento de alianzas estratégicas con instituciones académicas y ejércitos del campo aliado a los efectos de reducir costes y del garantizar soporte técnico para las unidades del Cucho y el ejercicio Nacional, la recomendación de realizar la documentación del proceso de implementación con el fin de que el modelo de implementación del STICD sea replicado por otras unidades del Ejército del Perú. Finalmente, este trabajo es no sólo un mero cumplimiento de un trabajo académico, sino es ante todo una contribución profesional en la orientación por modernizar las capacidades operacionales en el Batallón de Comunicaciones N° 113 y el Ejército del Perú en el terreno de la ciberseguridad e información.

CAPÍTULO I: INFORMACIÓN GENERAL

1.1. Descripción de la Dependencia

El Batallón de Comunicaciones N° 113 es una unidad operativa del Ejército del Perú perteneciente a la 3ra Brigada de Comunicaciones - Agrupamiento "José Olaya", ubicado en la Carretera Variante de Uchumayo Km 8.5, distrito de Tiabaya, provincia y departamento de Arequipa. Esta unidad tiene como propósito fundamental proporcionar apoyo de comunicaciones tácticas y estratégicas a las unidades militares de la III División del Ejército, garantizando el enlace operacional permanente y seguro en la Región Militar del Sur.

1.2. Tipo de actividad que desarrolló (función y puesto)

Comandante de Compañía de Comunicaciones, ejerciendo el comando directo sobre aproximadamente 80 a 100 efectivos militares. Esta función implicó la planificación, organización, dirección y control de todas las actividades operativas, administrativas e instructivas de la compañía, así como el empleo táctico de la unidad en ejercicios militares y operaciones reales.

1.3. Lugar y fecha

Tiabaya, Arequipa - Período 2023 y 2024.

1.4. Misión

Comandar y dirigir la Compañía de Comunicaciones asegurando la operatividad permanente de los sistemas de comunicaciones tácticas, la instrucción especializada del personal, el mantenimiento de equipos y la disposición inmediata para el apoyo en operaciones militares, ejercicios de adiestramiento y actividades de ayuda a la comunidad en la jurisdicción de la III División del Ejército.

1.5. Visión

Consolidar una Compañía de Comunicaciones altamente capacitada, tecnológicamente actualizada y operativamente eficiente, capaz de garantizar comunicaciones seguras, rápidas y confiables en cualquier escenario operacional, constituyéndose como unidad modelo en la integración de nuevas tecnologías y protocolos digitales dentro del Batallón de

Comunicaciones N° 113 y la 3ra Brigada de Comunicaciones del Ejército del Perú.

1.6. Funciones del puesto que ocupó

Como Comandante de Compañía ejerció las siguientes funciones principales: planificar y supervisar el entrenamiento táctico y técnico del personal en comunicaciones militares; dirigir la instalación, operación y mantenimiento de redes de comunicaciones en ejercicios y operaciones reales; administrar los recursos humanos, materiales y logísticos asignados a la compañía; coordinar con el Comando del Batallón y otras compañías para garantizar la interoperabilidad comunicacional; evaluar permanentemente la capacidad operativa de la unidad; implementar medidas de seguridad de la información y ciberseguridad en las comunicaciones; conducir el planeamiento y ejecución de operaciones de apoyo de comunicaciones; supervisar el cumplimiento de protocolos y procedimientos establecidos; y velar por el bienestar, disciplina y desarrollo profesional del personal bajo su mando.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes Internacionales

En el ámbito de la investigación militar contemporánea, diversos estudios abordan la evolución de las operaciones y la necesidad de adaptar estructuras y procedimientos a entornos operativos complejos. Guerrero (2025), en su trabajo "Las operaciones de información en el nivel táctico (CTTO)", afirma que el concepto de conflictos ha dejado de estar circunscrito a la idea de guerra como concepto clásico individual de armas y se ha ampliado hacia un entorno operacional que entiende las operaciones en distintas dimensiones, abarcando desde la dimensión informativa, cognitiva, física hasta la de datos. Con el objetivo general de crear una organización específica para el Componente Terrestre en el Teatro de Operaciones, el autor menciona la propuesta de crear una estructura con expertos y un oficial de información que esté constituido en el Estado Mayor para gestionar la coordinación de las Capacidades Relacionadas con la Información, y propone una perspectiva metodológica que está en consonancia con leyes nacionales y doctrinas internacionales para afectar el entorno informativo del oponente y proteger el del propio con el objetivo de contribuir al éxito del desarrollo de las operaciones tácticas.

De forma complementaria, Hernández Corchete (2022) en "La maniobra de la información. El papel estratégico de la comunicación en el Ejército de Tierra 4.0", explora el papel trascendental de la comunicación en la futura Fuerza 35 del Ejército español. La investigación, a través de una metodología que recoge el análisis de la visión del el Jefe del Estado Mayor, la mirada al modelo de Brigada 2035 y la realización de entrevistas al personal responsable de comunicación, establece que no solo hay que dominar el campo de batalla, sino que también hay que dominar el ciber-espacio y que hay que llegar a la superioridad en el dominio cognitivo. Esta investigación concluye que la integración de maniobra informativa y maniobra física en las operaciones multidominio es necesaria para obtener ventaja informativa y resolver con éxito los enfrentamientos directos.

En el contexto de la gestión del conocimiento, Gómez (2023) en "Diseño de un modelo de gestión del conocimiento para el Batallón de Mantenimiento

de Comunicaciones del Ejército Nacional (BAMCE)", propone un modelo integrado que combina la gestión del conocimiento con la inteligencia de negocios. El objetivo principal que persigue esta investigación, por tanto, es dar a conocer el procedimiento a seguir a la hora de capturar, organizar y usar el conocimiento interno y externo, que a su vez sirva de apoyo a la toma de decisiones organizativas y estratégicas. La metodología que se propone como resonancia de la investigación hace el recorrido de forma secuencial avanzando en el diagnóstico y su evaluación, el diseño y el desarrollo, la implementación y el despliegue, por último, el monitoreo como la mejora continua. En conclusión, el autor considera que, si bien existe madurez en la gestión del conocimiento por parte de la Fuerza, el Batallón de Mantenimiento de Comunicaciones debe tener su específica receta a las demandas del conocimiento.

2.1.2. Antecedentes Nacionales

A nivel nacional, Percca (2024) en "Capacidades de Operaciones de Información y su Influencia en las Operaciones y Acciones Terrestres Unificadas, 2021", se propuso conocer la influencia de las unidades con capacidades de operaciones de información en el desempeño de las operaciones terrestres unificadas. Empleando un enfoque cualitativo de tipo teórico-empírico y el método hermenéutico-cualitativo, la investigación utilizó técnicas como la entrevista, la observación y el análisis documental con un muestreo por expertos. Los resultados determinaron que el desarrollo de estas unidades en las Grandes Unidades de Batalla permite crear efectos en el ambiente de la información, brindando una ventaja decisiva sobre el adversario. Como conclusión principal, el estudio presenta la propuesta de elaborar un manual doctrinario de operaciones de información para el Ejército.

En el ámbito de la respuesta a desastres, Mendoza, Salinas y Zamora (2025) en "Sistema Integrado de Coordinación y Respuesta Aérea (SICRA) para enfrentar la deficiente planificación de las operaciones aéreas de la Dirección Aviación Policial para el tratamiento o atención frente al riesgo por silencio sísmico en Lima Metropolitana durante los años 2020–2024", abordan el problema de la limitada capacidad de respuesta aérea ante un riesgo sísmico inminente. Identificaron como causas principales la insuficiencia presupuestaria,

la capacitación inadecuada, la metodología de planificación ineficiente y la coordinación interinstitucional limitada. Como solución, proponen el Sistema Integrado de Coordinación y Respuesta Aérea, una plataforma tecnológica con componentes de mapeo, gestión de recursos, comunicaciones, inteligencia artificial y reportes. Concluyen que la implementación de este sistema, que requiere una inversión cuantificada, es viable y necesaria para optimizar significativamente la respuesta ante emergencias.

Finalmente, Ortega y Calizaya (2025) en "Desafíos en la implementación de las TIC durante las operaciones y acciones terrestres unificadas de la 3a brigada blindada, Moquegua 2025", exploran los obstáculos técnicos, humanos y organizacionales que surgen al integrar las Tecnologías de la Información y Comunicaciones en el campo de batalla. El estudio aborda problemas de interoperabilidad de los sistemas de comunicación, la capacitación del personal, la seguridad de la información y la adaptación de la doctrina militar. Los autores concluyen que su investigación desarrolla una propuesta excelente para optimizar la implementación de las TIC en la brigada, con el objetivo de mejorar la eficiencia, la eficacia y la capacidad de respuesta, generando un efecto multiplicador para la mejora continua de las unidades militares.

2.2. Bases teóricas

2.1. Comunicaciones operativas en el ámbito militar

2.1.1. Fundamentos de las Comunicaciones Militares Tácticas

Las comunicaciones operacionales son el sistema nervioso de cualquier operación militar moderna, han evolucionado hacia arquitecturas integradas que soportan la transmisión de voz, datos y vídeo en ambientes operacionales complejos, son las comunicaciones militares en un mundo donde la digitalización y la hiperconexión son garantía de éxito para cualquier operación y es un eje fundamental en la coordinación de unidades geográficamente dispersas (Oh et al., 2024). El mercado de comunicaciones militares es reflejo de su importancia creciente, el tamaño del mercado mundial de comunicación militar, valorado en USD 33.12 millones en 2023 y pronosticado en USD 60.40 millones hasta 2032, pone de manifiesto la enorme inversión que se está

realizando en capacidades comunicativas avanzadas (Military Tactical Radio Market, 2024).

2.1.2. Redes Tácticas y Movilidad Operacional

Las arquitecturas de la red táctica moderna han de ser capaces de soportar comunicaciones en movimiento y en alta movilidad. Monzon Baeza et al. (2025) explican que la integración de la Inteligencia Artificial en las comunicaciones y redes tácticas está transformando las guerras modernas o las tácticas de defensa modernas que favorecen un intercambio de datos seguro, una conciencia situacional en tiempo real y la toma de decisiones autónoma desde diferentes dominios de la táctica subyacente.

Las comunicaciones tácticas abarcan todas las tecnologías de las comunicaciones para lucha a pie de campo, constituyéndose en un compendio heterogéneo de formas y de tecnologías que diseñadas para ser operacionales en situaciones donde el entorno de conflicto o lucha puede expresarse como DIL (desconectado, intermitente y limitado) que resumen así las diferencias a las que deben hacer frente ingenieros y operadores de redes tácticas (Hybrid Technology for Military Communication, 2024).

2.1.3. Modernización de Sistemas de Comunicación

Las fuerzas armadas del planeta han comenzado programas completos de modernización que sustituyen sistemas de comunicación analógica obsoletos por radios tácticas digitales y en consecuencia con un mejor rendimiento y buena fiabilidad, teniendo que a su vez las radios tácticas soportar las arquitecturas de seguridad de confianza cero, las cuales hacen que las radios tácticas a su vez deban soportar protocolos continuos de autenticación y autorización para validar credenciales de usuario y la integridad del dispositivo antes de ser capaces de establecer enlaces de comunicación (Military Tactical Radio Market, 2024).

2.2. Protocolos digitales en comunicaciones militares

2.2.1. Criptografía y Seguridad de la Información

La encriptación representa la parte más importante de las comunicaciones militares seguras. Kumar y Khan (2024a) argumentan que la seguridad de datos de las comunicaciones militares no es negociable, siendo que el uso de encriptación de extremo a extremo en los sistemas de mensajería es crucial, un mecanismo que permite que los mensajes solo sean legibles por el remitente y el destinatario esperado. Los protocolos de encriptación avanzada, incluido el Estándar de Encriptación Avanzada (AES) y la Criptografía de Curva Elíptica (ECC), son factores esenciales de la comunicación militar segura para la seguridad de los datos a los que pueden acceder los sistemas de comunicación sobre canales como satélites o redes móviles privadas.

La gestión de claves representa uno de los aspectos que más influyen en la seguridad, ya que el material de claves criptográfico, proporcionado por los proveedores especializados a través de los Sistemas de Gestión de Claves, es la armadura digital que protege los sistemas de armas habilitados por red. Las nuevas tecnologías están eliminando la necesidad de transporte físico con capacidades de distribución de claves sobre la red (Military Computing Security, 2024).

2.2.2. Blockchain y Tecnologías Emergentes

Kumar y Khan (2024b) sostienen que la adopción de la tecnología blockchain ha surgido como una solución productiva para combatir contra las ciber amenazas en desarrollo, gracias a su modelo descentralizado y resistente a la manipulación. La blockchain, por su registro de distribución, ofrece soluciones potentes para garantizar la integridad de datos, así como el control de acceso en operaciones militares.

Aseri et al. (2024) aseguran que la sinergia de blockchain y de computación cuántica está revolucionando la propia tecnología militar: la seguridad de algunas vulnerabilidades de sistemas digitales se ha trasladado de un modelo de eslabón débil, donde el atacante debe comprometer un eslabón solamente, a un modelo de vulnerabilidad de mayoría comprometida, donde

un atacante no puede explotar un eslabón débil.

2.2.3. Inteligencia Artificial en los Protocolos de Comunicación

La adición de sistemas de detección en tiempo real de amenazas, habilitados por IA, facilita a las redes militares la detección y neutralización de las amenazas de origen cibernético en la medida en que surgen. Las soluciones de encriptación habilitadas por IA iniciarían dinámicamente, ajustes en los protocolos de encriptación en función de los análisis de red y de amenazas potenciales en tiempo real, identificando anomalías, detectando intrusiones y encriptando durante un ataque, como respuesta a las amenazas entrantes (Oh et al., 2024).

2.2.4. Criptografía Post-Cuántica

La creciente amenaza que representa la computación cuántica está impulsando al sector de defensa en el desarrollo de protocolos de encriptación ante ataques de este tipo. Esta amenaza ha resuelto el desarrollo de nuevos algoritmos criptográficos resistentes frente a ataques cuánticos. La criptografía post cuántica supone una nueva dirección de investigación para la comunicación militar a largo plazo (Aseri et al., 2024).

2.2.5. Estandarización e interoperabilidad

Kumar y Khan (2024c) insisten en que los sistemas de mensajería militar deben facilitar un intercambio de información seguro, fiable y rápido entre muchas zonas operativas, desde las operaciones de campo táctico hasta los centros de comando estratégico, lo que implica comunicaciones en tiempo real bajo las condiciones más extremas. La integración de formatos estandarizados mejora el intercambio de información esencial para la misión al proporcionar una gama completa de formatos de mensajes militares estandarizados, aguanta para hacer surgir la interoperabilidad para las fuerzas aliadas.

2.2.6. Amenazas emergentes y ciberseguridad

El panorama siempre creciente de las amenazas cibernéticas puede considerarse como un motor, el motor del mercado de seguridad de las comunicaciones militares. Surtir a los ataques cibernéticos, por ejemplo,

ransomware, espionaje y operaciones disruptivas, plantea varios riesgos que pueden amenazar la seguridad nacional e infraestructuras militares y con los ataques venidos no solo de hackers informáticos o sino de terroristas, organizaciones criminales, extremistas políticos, movimientos de fanatismos religiosos o servicios de inteligencia extranjeros. La amenaza a las tecnologías de la información no ha sido como hoy en día (Weng, 2024).

2.3. Términos básicos

1. Comunicaciones Tácticas

Diferentes tecnologías de comunicación que operan en el campo de batalla y que se han creado para trabajar en un entorno disruptivo definido como DIL (desconectado, intermitente y limitado), que permiten el intercambio de información operacional en tiempo real (Hybrid Technology for Military Communication, 2024).

2. Encriptación de Extremo a Extremo

Método de seguridad que permite que un mensaje se pueda leer solo por el remitente y el destinatario previsto a través de protocolos criptográficos como AES y ECC que protegen la comunicación clasificada (Kumar y Khan, 2024).

3. Blockchain Militar

Arquitectura de registro distribuido que proporciona una estructura descentralizada y a prueba de manipulaciones a la vez que permite garantizar la integridad de los datos y del control de acceso en las operaciones militares (Kumar y Khan, 2024b).

4. Inteligencia Artificial en Comunicaciones

Incorporación de sistemas en los que se detectan amenazas en tiempo real que son capaces de conocer y desactivar una amenaza cibernética, ajustando parámetros en los protocolos de encriptación para controlar las condiciones de la red mediante el análisis (Oh et al., 2024).

5. Criptografía Post-Cuántica

Desarrollo de protocolos de encriptación resistentes a los ataques basados en computación cuántica para proteger las comunicaciones militares contra amenazas tecnológicas futuras (Aseri et al., 2024).

6. Interoperabilidad Comunicacional

Capacidad de los sistemas militares de poder permitir el intercambio seguro, confiable y rápido de información contenidos en los diferentes dominios de operaciones que adopte, con una adecuada estandarización de los formatos de los mensajes militares (Kumar y Khan, 2024c).

7. Gestión de Claves Criptográficas (COMSEC)

Sistema que permite y gestiona el material clave criptográfico que constituye una armadura digital para los sistemas de armas habilitados por red, incluyendo capacidades de distribución de claves sobre la red (Military Computing Security, 2024).

8. Redes Tácticas con IA

La introducción de inteligencia artificial en comunicaciones y redes tácticas que transforman las estrategias de defensa modernas enfocadas en permitir el intercambio seguro y rápido de datos, así como la mejora de la conciencia situacional en tiempo real (Monzón Baeza et al., 2025).

9. Arquitectura de Confianza Cero

Implementación de protocolos continuos de autenticación y autorización en las redes militares que validan la credencial de usuario y la integridad del dispositivo antes de establecer enlaces de comunicación (Military Tactical Radio Market, 2024).

10. Amenazas Cibernéticas Militares

Conjunto de ataques cibernéticos que incluyen ransomware, espionaje y operaciones desfavorables desde hackers, terroristas, organizaciones criminales y servicios de inteligencia de países extranjeros que ponen serios

riesgos para la seguridad nacional (Weng, 2024).

CAPÍTULO III:

DESARROLLO DEL TEMA

SISTEMA TÁCTICO INTEGRADO DE COMUNICACIONES DIGITALES (STICD)

3.1. Campo de aplicación

La presente propuesta de mejora se circunscribe al ámbito de las **comunicaciones operativas militares**, específicamente aplicada al Batallón de Comunicaciones N.° 113 de la 3ra Brigada de Comunicaciones - Agrupamiento "José Olaya" del Ejército del Perú.

3.1.1. Ámbito Geográfico

Ubicación: Carretera Variante de Uchumayo Km 8.5, distrito de Tiabaya, provincia y departamento de Arequipa.

Área de responsabilidad operacional: El Batallón proporciona apoyo de comunicaciones tácticas y estratégicas a las unidades militares de la III División del Ejército en toda la Región Militar del Sur, abarcando:

- Zonas urbanas de la ciudad de Arequipa.
- Áreas periurbanas y rurales del departamento.
- Terreno montañoso (volcanes Misti, Chachani, Pichu Pichu).
- Zonas de difícil acceso con conectividad limitada.

3.1.2. Ámbito Funcional

La propuesta se aplica a tres dimensiones fundamentales de las comunicaciones militares:

A. Comunicaciones Tácticas Operacionales

- Transmisión de órdenes entre escalones de mando.

- Coordinación entre compañías y pelotones en ejercicios y operaciones.
- Reportes situacionales (SITREP) e informes de inteligencia (INTREP).
- Comunicaciones de emergencia y respuesta rápida.

B. Gestión de Información Clasificada

- Seguridad de la información operativa.
- Protocolos de encriptación y ciberseguridad.
- Manejo de comunicaciones según niveles de clasificación.
- Prevención de interceptación y espionaje.

C. Capacitación y Desarrollo del Personal

- Instrucción técnica en sistemas digitales de comunicación.
- Entrenamiento táctico en empleo de nuevas tecnologías.
- Certificación especializada del personal.
- Formación continua en ciberseguridad operativa.

3.1.3. Ámbito Temporal

- Fase 1: Diagnóstico y diseño (2 meses).
- Fase 2: Adquisición y desarrollo (2 meses).
- Fase 3: Capacitación piloto (2 meses).
- Fase 4: Implementación general (3 meses).
- Fase 5: Consolidación (3 meses).

3.1.4. Población Beneficiaria

Directa:

- Personal del Batallón de Comunicaciones N° 113
- Oficiales: 30-40
- Suboficiales: 100-120
- Personal de tropa: 270-340

Indirecta:

- Unidades militares de la III División del Ejército que reciben apoyo de

comunicaciones.

- Estado Mayor de la 3ra Brigada de Comunicaciones.
- Otras unidades de comunicaciones del Ejército (potencial réplica del modelo).

3.2. Tipo de aplicación

La propuesta constituye una **innovación tecnológica y organizacional** de carácter **aplicativo-operacional** que integra tres componentes esenciales:

3.2.1. Innovación Tecnológica

Sistema Táctico Integrado de Comunicaciones Digitales (STICD)

Se trata de una aplicación práctica de tecnologías emergentes adaptadas al contexto militar peruano:

A. Plataforma Digital Táctica Offline "COMSEG-113"

- **Tipo**: Aplicación móvil militar instalada en tablets ruguerizadas
- **Característica distintiva**: Funcionamiento autónomo sin dependencia de internet (crítico para zonas de baja conectividad en Arequipa)
- **Tecnología aplicada**:
    - Mensajería encriptada con algoritmos AES-256.
    - Georreferenciación GPS integrada.
    - Sincronización automática mediante protocolos de red ad-hoc.
    - Verificación biométrica (huella dactilar) para autenticación.

B. Centro de Operaciones de Comunicaciones Modernizado (COC 4.0)

- **Tipo**: Infraestructura física y tecnológica integrada
- **Componentes**:
    - Sistema de visualización multi-pantalla (4 LED 55" + 1 táctil 85").
    - Servidores locales con capacidad de backup automático.
    - Radios digitales con encriptación militar.
    - Sistema de energía ininterrumpida (UPS industrial 8 horas).

C. Simulador Táctico "SIM-COM 113"

- **Tipo**: Software de entrenamiento virtual.
- **Función**: Recreación de escenarios operacionales sin consumo de recursos reales.
- **Metodología**: Gamificación con métricas de desempeño evaluables.

3.2.2. Innovación Organizacional

Protocolos Digitales Estandarizados

Implementación de procedimientos documentados y medibles que transforman la cultura organizacional:

A. Manual Digital de Procedimientos Operacionales (MDPO)

- Digitalización de protocolos tradicionales.
- Acceso instantáneo desde dispositivos móviles.
- Actualizaciones en tiempo real.
- Diagramas de flujo interactivos.

B. Matriz de Responsabilidades Comunicacionales

- Definición clara de tiempos de respuesta por escalón de mando.
- Asignación de responsabilidades específicas.
- Trazabilidad de decisiones y acciones.

C. Sistema de Codificación Digital Dinámica

- Códigos que se renuevan automáticamente cada 24 horas.
- Prevención de interceptación mediante rotación constante.
- Implementación de principios de criptografía aplicada.

3.2.3. Innovación Pedagógica

Programa de Capacitación Escalonada "COMTAC-113"

Modelo de enseñanza diferenciado según niveles jerárquicos y funcionales:

Nivel 1 - Personal de Tropa (20 horas)

- Enfoque: Operación básica de sistemas digitales.
- Metodología: Instrucción práctica con simuladores.

Nivel 2 - Suboficiales (40 horas)

- Enfoque: Gestión táctica y coordinación operacional.
- Metodología: Estudios de caso y ejercicios de campo.

Nivel 3 - Oficiales (60 horas)

- Enfoque: Planificación estratégica y liderazgo en comunicaciones digitales.
- Metodología: Ejercicios de Estado Mayor y análisis de operaciones complejas.

Sistema de certificación: "Licencia Digital STICD" con validación biométrica que acredita competencias específicas.

3.2.4. Clasificación según Naturaleza de la Aplicación

Aplicación Directa: La propuesta surge de la experiencia real como Comandante de Compañía (2023-2024), identificando necesidades concretas observadas en ejercicios tácticos, operaciones y rutinas diarias del Batallón.

Aplicación Técnico-Operacional: Integra conocimientos de:

- Formación en Operaciones Cibernéticas (2020).
- Curso Táctico de Comunicaciones.
- Experiencia en comando de unidades de comunicaciones.

Aplicación Escalable: El modelo STICD puede replicarse en:

- Otras compañías del Batallón N° 113.
- Batallones de comunicaciones de otras brigadas.
- Unidades de armas con necesidades de comunicaciones digitales.

3.3. Diagnóstico

El diagnóstico de la situación de las comunicaciones operativas en el Batallón de Comunicaciones N° 113 se realizará mediante observación participante durante el período de pre aplicación como Comandante de Compañía, complementado con análisis de ejercicios tácticos, revisión de reportes operacionales y consultas con el personal de diferentes niveles jerárquicos.

3.4. Propuesta de innovación

- Módulo de Órdenes: Transmisión y confirmación de lectura.
- Módulo de Reportes: Formatos SITREP, INTREP automatizados.
- Módulo de Coordinación: Chat grupal por escalones de mando.
- Módulo de Emergencia: Alertas prioritarias con notificación sonora.

3.4.1. Objetivo de la propuesta

Modernizar integralmente las comunicaciones operativas mediante el Sistema Táctico Integrado de Comunicaciones Digitales (STICD), reduciendo en 70% los tiempos de transmisión, eliminando pérdida de información crítica y capacitando al 100% del personal en protocolos digitales.

3.4.2. Descripción simple de la propuesta

COMPONENTE 1: PLATAFORMA DIGITAL TÁCTICA OFFLINE "COMSEG-113"

Aplicación móvil militar en tablets ruguerizadas que funciona sin internet.

Tabla 1

Características principales del programa

CARACTERÍSTICA	ESPECIFICACIÓN	BENEFICIO
Funcionamiento offline	Red mesh ad-hoc	Operación en zonas sin cobertura
Encriptación	AES-256, rotación 24h	Protección contra interceptación
Georreferenciación	GPS con mapeo táctico	Ubicación de unidades en tiempo real
Verificación biométrica	Huella dactilar	Autenticación segura
Clasificación multinivel	4 niveles de seguridad	Manejo apropiado de información

Módulos integrados:

Órdenes Operacionales: Transmisión instantánea con confirmación de lectura.

Reportes Automatizados: SITREP e INTREP con formatos estructurados.

Coordinación Táctica: Chat grupal por escalones de mando.

Emergencia y Alertas: Botón de pánico con geolocalización automática.

Administración: Dashboard con métricas en tiempo real.

Tabla 2

Equipamiento

EQUIPO	CANTIDAD
Tablets militares ruguerizadas	50
Licencias software COMSEG-113	50
SUBTOTAL	

COMPONENTE 2: CENTRO DE OPERACIONES MODERNIZADO (COC 4.0)

Tabla 3

Redistribución física

ZONA	FUNCIÓN	NIVEL ACCESO	SUPERFICIE
🔴 Roja	Comunicaciones clasificadas	Solo Comandante y Of. Inteligencia	15 m²
🟡 Amarilla	Operaciones tácticas	Oficiales autorizados	40 m²

🟢 Verde	Coordinación administrativa	Personal COC	25 m²
🔵 Azul	Simulación y entrenamiento	Personal en capacitación	20 m²

Tabla 4
Equipamiento tecnológico

EQUIPAMIENTO	CANT.	ESPECIFICACIONES
Pantallas LED 55"	4	4K, matriz 2x2
Pantalla táctil 85" (Muro Situacional)	1	4K, multi-touch
Servidores (principal + backup)	2	32GB RAM, redundancia
Radios digitales encriptados	10	AES-256, 15km
UPS industrial	2	8h autonomía
Sistema grabación digital	1	30 días, 16 canales
Infraestructura y remodelación	-	Eléctrico, climatización, mobiliario
SUBTOTAL		

Innovación: Muro Situacional Digital (MSD).

Mapa topográfico con unidades geolocalizadas en tiempo real.

Estados operativos por colores (🟢 Operativo / 🟡 Alerta / 🔴 Emergencia).

Paneles informativos: clima, alertas, comunicaciones activas.

Interacción táctil: planificación de rutas, envío de órdenes directo.

COMPONENTE 3: PROTOCOLOS DIGITALES ESTANDARIZADOS

Manual Digital de Procedimientos Operacionales (MDPO)

Plataforma web responsive con acceso desde tablets, disponible offline.

Estructura:

- Fundamentos de comunicaciones digitales.
- Uso de COMSEG-113 paso a paso.
- Protocolos de clasificación de información.
- Procedimientos por tipo de operación.
- Diagramas de flujo operacionales.
- Ciberseguridad operativa.
- Protocolos de contingencia.

Tabla 5

Matriz de Responsabilidades Comunicacionales

NIVEL	RESPONSABILIDAD	TIEMPO MÁXIMO RESPUESTA
Comandante Batallón	Decisiones estratégicas	Inmediato (< 2 min emergencias)
Estado Mayor	Planificación y coordinación	10 minutos
Comandante Compañía	Coordinación táctica	5 minutos
Jefe de Pelotón	Ejecución de misiones	10 minutos
Personal de Tropa	Cumplimiento y confirmación	15 minutos

Sistema de Codificación Digital Dinámica

Códigos tácticos que se generan automáticamente cada 24 horas mediante algoritmos criptográficos.

Tabla 6

Ejemplo de categorías

CATEGORÍA	EJEMPLO	USO
Ubicaciones	ALFA-7, BRAVO-3	Referencias geográficas
Operaciones	VERDE-9, ROJO-1	Tipo de actividad
Personal	DELTA-5, ECHO-2	Identificación de personas clave
Estados	HOTEL-8, INDIA-2	Situación operativa

COMPONENTE 4: PROGRAMA DE CAPACITACIÓN "COMTAC-113"

Formación escalonada por niveles jerárquicos:

Tabla 7

NIVEL 1: Personal de Tropa (20 horas)

MÓDULO	CONTENIDO	HORAS
Uso básico de tablets	Encendido, login biométrico, navegación	4
Seguridad digital	Información clasificada, protección de tablet	4
Reportes	Confirmación de órdenes, reportes de novedad	6

Simulación práctica	Ejercicio con SIM-COM 113 + evaluación	6

Tabla 8

NIVEL 2: Suboficiales (40 horas)

MÓDULO	CONTENIDO	HORAS
Gestión táctica	Transmisión de órdenes, consolidación de reportes	10
Coordinación multicanal	Uso simultáneo COMSEG-113 y radio	8
Crisis comunicacionales	Protocolos ante fallas, toma de decisiones	8
Ciberseguridad operativa	Amenazas, detección, respuesta	8
Prácticas de campo	Ejercicio táctico 2 días + evaluación	6

Tabla 9

NIVEL 3: Oficiales (60 horas)

MÓDULO	CONTENIDO	HORAS
Planificación estratégica	Diseño de arquitecturas comunicacionales	12
Operaciones cibernéticas	Ciberdefensa, inteligencia de amenazas	12
Sistemas complejos	Interoperabilidad, comunicaciones conjuntas	12
Liderazgo digital	Transformación digital, gestión del cambio	12
Ejercicio Estado Mayor	Operación compleja con STICD	12

Certificación Digital "Licencia STICD":

- Código QR único con blockchain.
- Huella biométrica vinculada.
- Vigencia 2 años.
- Verificación instantánea de capacidades.

Cronograma de capacitación:

FASE	GRUPO	PERÍODO	CANTIDAD
1	Oficiales instructores	Mes 1-2	10

FASE	GRUPO	PERÍODO	CANTIDAD
2	Oficiales Nivel 3	Mes 3-4	30
3	Suboficiales Nivel 2	Mes 5-7	100
4	Tropa Nivel 1	Mes 8-10	300
5	Recertificación	Mes 11-12	Rezagados

COMPONENTE 5: SIMULADOR TÁCTICO "SIM-COM 113"

Software de simulación que recrea operaciones militares para entrenar sin gastar recursos reales.

Tabla 10

Escenarios programados

ESCENARIO	DESCRIPCIÓN	OBJETIVO ENTRENAMIENTO
Operación Misti	Comunicaciones en zona montañosa	Manejo de terreno difícil
Defensa Urbana	Coordinación con interferencias	Comunicaciones en ciudad
Emergencia Nacional	Respuesta ante desastre natural	Gestión de crisis
Fallo Total	Actuación sin sistemas digitales	Protocolos de contingencia

Métricas evaluadas:

- Tiempo de respuesta promedio.
- Precisión en transmisión de órdenes.
- Efectividad en coordinación.
- Errores críticos cometidos.
- Capacidad de adaptación.

Tabla 11

Cronograma de Implementación

FASE	ACTIVIDADES	DURACIÓN
FASE 1: Diagnóstico y Diseño	Evaluación técnica, diseño STICD, protocolos, manuales	2 meses

FASE 2: Adquisición y Desarrollo	Compra equipos, desarrollo software, adecuación COC	2 meses
FASE 3: Capacitación Piloto	Instructores, 1ra Compañía piloto, ajustes	2 meses
FASE 4: Implementación General	Capacitación masiva, instalación, operación paralela	3 meses
FASE 5: Consolidación	Migración total, evaluación, optimización	3 meses
TOTAL		12 meses

Tabla 12

Indicadores de Éxito (KPIs)

INDICADOR	**META**	**MEDICIÓN**
Tiempo de transmisión de órdenes	Reducción 70%	Antes: 15min → Después: 4.5min
Personal capacitado	100%	Certificados digitales emitidos
Pérdida de información	0%	Auditoría mensual
Satisfacción del personal	> 85%	Encuesta trimestral
Tiempo respuesta emergencias	< 3 minutos	Registro automático COMSEG-113
Efectividad ejercicios tácticos	> 90%	Evaluación Estado Mayor

El Sistema Táctico Integrado de Comunicaciones Digitales (STICD) transforma las comunicaciones operativas del Batallón N° 113 mediante digitalización, protocolos estandarizados, capacitación especializada e innovación sostenible. La experiencia como Comandante de Compañía del autor (2023-2024) y la formación en Operaciones Cibernéticas (2020) garantizan que esta propuesta es práctica, necesaria y realizable, posicionando al Batallón como unidad modelo en comunicaciones tácticas digitales del Ejército del Perú.

CONCLUSIONES

Durante el cumplimiento del ejercicio del mando de la Compañía de Comunicaciones del Batallón N° 113 durante los años 2023 y 2024 se pudo evidenciar de forma directa y de forma continua las carencias y limitaciones críticas que sufren las comunicaciones operativas en el marco militar contemporáneo. La experiencia cotidiana del mando en una unidad de a cerca de cien efectivos militares permitirá evidenciar que las comunicaciones tradicionales, predominantemente en equipos analógicos y procedimientos no estandarizados, son insuficientes a la hora de presentar la rapidez, la seguridad y la eficiencia que requieren la operativa militar vigente. Esta realidad operacional, junto a la formación especializada en este ámbito de las Operaciones Cibernéticas obtenida en el año 2020- y el Curso Táctico de Comunicaciones, motivó la necesidad profesional de plantear una propuesta que permita una solución de transformación estructural del sistema de trabajo del Batallón en el ámbito de las comunicaciones tácticas y estratégicas.

El Sistema Táctico Integrado de Comunicaciones Digitales (STICD) que se propone es la respuesta directa a las degeneraciones diagnosticadas en el período de mando, donde se constató que el ciclo de transmisión promedio de las órdenes alcanzaba los 15-20 minutos, que se producía una pérdida del 12% de la información crítica en los ejercicios evaluados, y que únicamente el 15% del personal había recibido algún tipo de formación en tecnologías digitales de las comunicaciones.

No se trata de un ejercicio teórico, sino de la sistematización de necesidades reales aparecidas en el campo de batalla, en ejercicios de conjunto y en operaciones de apoyo comunitario en las que las comunicaciones ineficaces pusieron claramente de manifiesto la urgencia de modernizar los procesos actuales de comunicación del Batallón.

Si bien el STICD no es más que un proyecto en un estado todavía previo a su implementación, los resultados esperados están sustentados en la experiencia de las fuerzas armadas de otros países de la región que han probado con éxito la modernización de comunicación, así como en principios

de ingeniería bien establecidos. La implementación total del sistema debería, según los cálculos obtenidos a partir del conocimiento acumulado por el Odona, suponer una reducción del 70 % de los tiempos en la transmisión de órdenes (de 15-20 minutos a menos de 5), lo que supondría un incremento sustancial de la capacidad de respuesta táctica del Batallón. También se espera la total eliminación de la pérdida de la información considerada crítica (mediante el sistema de confirmación biométrica y el sistema de la trazabilidad digital), con cumplimiento del objetivo cero de pérdida de información en las comunicaciones operacionales. Nadie podrá volver a decir que tiene que esperar 20 minutos para utilizar la comunicación, dado que con la capacitación extendida del 100 % del personal (con protocolos digitales y seguridad cibernética operacional) tendrá una transformación. El Batallón se convertirá en una unidad tecnológicamente preparada para la guerra moderna.

En suma, la presente propuesta de suficiencia profesional atiende una necesidad operativa real y urgente que ha surgido a raíz del ejercicio del mando en el Batallón de Comunicaciones N° 113, dando solución global, técnicamente posible y estratégicamente necesaria para articular las comunicaciones operativas de la unidad dada la diferencia entre la situación actual y la deseada, por cuanto los resultados esperados, si bien todavía no se materializan, se proyectan sustentados en un diagnóstico acotado, un benchmarking internacional y principios técnicos con la certeza de que la implementación del STICD sitúa al Batallón, como un modelo de comunicación táctica digital a nivel nacional, al mismo tiempo que contribuye efectivamente con la modernización de las capacidades operacionales del Ejército del Perú en el ámbito cibernético y de la información.

RECOMENDACIÓN

Se propone ejecutar el STICD con una compañía de pruebas y como máximo durante los cuatro primeros meses, para poder detectar y solucionar problemas técnicos u operativos antes de generalizar la ejecución en el Batallón, porque de esta manera se pueden reducir los riesgos, optimizar los recursos y recoger lecciones aprendidas valiosas, que faciliten la ejecución general del sistema.

Se sugiere también establecer convenios con instituciones académicas de ciberseguridad y de comunicaciones digitales, así como revisar la posibilidad de cooperación técnica internacional con ejércitos de países aliados que hayan ejecutado sistemas similares con éxito. Estas alianzas podrían suponer una reducción considerable de los costes en el desarrollo de software, en la provisión de formación específica a un menor coste y en el soporte técnico durante los primeros años de funcionamiento del STICD.

Es muy importante que se lleve la documentación necesaria sobre los procesos, decisiones, problemas y soluciones a los mismos que sacan, se deben documentar de forma exhaustiva, a lo largo de toda la implementación. De esta forma, es posible que otros batallones de comunicación del Ejército puedan trasladar el modelo STICD a gran medida y siguiendo las recomendaciones en la ejecución y gasto del tiempo. Esto, a su vez, forma parte de la tarea de modernización de la comunicación a nivel institucional y puede convertir el Batallón N.° 113 en un centro de capacitación referencial para las comunicaciones tácticas digitales del Ejército del Perú en su conjunto.

REFERENCIAS BIBLIOGRÁFICAS

Aseri, V., Chowdhary, H., Chaudhary, N. K., Pandey, S. K., & Kumar, V. (2024). Revolutionizing military technology: How the fusion of blockchain and quantum computing is driving in defense application. In A. Kumar, N. J. Ahuja, K. Kaushik, D. S. Tomar, & S. B. Khan (Eds.), *Sustainable security practices using blockchain, quantum and post-quantum technologies for real time applications* (pp. 193-203). Springer. https://doi.org/10.1007/978-981-97-0088-2_10

Gomez, J. (2023). Diseño de un modelo de gestión del conocimiento para el Batallón de Mantenimiento de Comunicaciones del Ejército Nacional (BAMCE). https://repository.universidadean.edu.co/server/api/core/bitstreams/daf2cbc8-540d-41e1-a6d9-d73c5767fcfb/content

Guerrero, R. (2025). Las operaciones de información en el nivel táctico (CTTO). https://cefadigital.edu.ar/handle/1847939/3068

Hernández Corchete, S. (2022). La maniobra de la información. El papel estratégico de la comunicación en el Ejército de Tierra 4.0 (No. BOOK-2025-326). Egregius. https://zaguan.unizar.es/record/151732

Hybrid Technology for Military Communication. (2024). *International Journal of Emerging Technologies and Innovative Research, 11*(5), j770-j774. http://www.jetir.org/papers/JETIR2405990.pdf

Kumar, R., & Khan, R. A. (2024a). Securing military computing with the blockchain. *Computer Fraud & Security, 2024*(2), 5-11. https://doi.org/10.12968/S1361-3723(24)70007-4

Kumar, R., & Khan, R. A. (2024b). Military computing security: Insights and implications. *Journal of The Institution of Engineers (India): Series B, 106*(4), 1077-1090. https://doi.org/10.1007/s40031-024-01136-6

Kumar, R., & Khan, R. A. (2024c). Securing communication protocols in military computing. *Network Security, 2024*(2), 8-14.

https://doi.org/10.12968/S1353-4858(24)70011-7

Mendoza, C., Salinas, J., & Zamora, W. (2025) Sistema Integrado de Coordinación y Respuesta Aérea (SICRA) para enfrentar la deficiente planificación de las operaciones aéreas de la Dirección Aviación Policial para el tratamiento o atención frente al riesgo por silencio sísmico en Lima Metropolitana durante los años 2020–2024. https://tesis.pucp.edu.pe/items/686b68d3-1a02-4323-bc26-4d301b1d1654

Military Tactical Radio Market. (2024). *Emergen Research*. https://www.emergenresearch.com/industry-report/military-tactical-radio-market

Monzon Baeza, V., Concha, L., Monzo, C., & Parada, R. (2025). AI-driven tactical communications and networking for defense: A survey and emerging trends. *Manuscript submitted for publication*. https://www.researchgate.net/publication/390570740

Oh, S. J., Cho, S. K., & Seo, Y. (2024). Harnessing ICT-enabled warfare: A comprehensive review on South Korea's military meta power. *IEEE Access, 12*, 46379-46400. https://doi.org/10.1109/ACCESS.2024.3378735

Ortega, E., & Calizaya, J. (2025). Desafíos en la implementación de las TIC durante las operaciones y acciones terrestres unificadas de la 3a brigada blindada, Moquegua 2025. https://repositorio.esge.edu.pe/items/bfeec0a8-0172-4230-97c8-f2c9cf44bf34

Percca, R. (2024). Capacidades de Operaciones de Información y su Influencia en las Operaciones y Acciones Terrestres Unificadas, 2021. https://repositorio.esge.edu.pe/items/7c60f19a-d21b-4925-89cf-19783ff9637b

Weng, Y. (2024). Big data and machine learning in defence. *International Journal of Computer Science and Information Technology, 16*(2), 25-

35.

ANEXOS

ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI

"Alma Mater del Ejército del Perú"

ANEXO 01: INFORME PROFESIONAL PARA OPTAR
EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES

1. DATOS PERSONALES:

1.01	Apellidos y Nombres	SILVA AVILA
1.02	Grado y Arma / Servicio	DAVID ALONSO
1.03	Situación Militar	ACTIVIDAD
1.04	CIP	124362400
1.05	DNI	45335259
1.06	Celular y/o RPM	972505203
1.07	Correo Electrónico	d.s.a887@gmail.com

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	01 abril 2009
2.02	Fecha_ egreso EMCH	31 diciembre 2012
2.04	Fecha de alta como Oficial	01 enero 2013
2.05	Años_ experiencia de Oficial	12 años
2.06	Idiomas	Inglés

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

N°	Año	Lugar	Unidad / Dependencia	Puesto Desempeñado
3.01	2013	TIABAYA	CÍA GUERRA ELECTRÓNICA N° 113	CMDTE DE SECCIÓN
3.02	2014	HUANCANÉ	RCB N° 111	CMDTE DE SECCIÓN
3.03	2015 - 2016	MOQUEGUA	ESC AVIACIÓN	ALUMNO
3.04	2017	SAMEGUA	CÍA CMDO N° 3	EJECUTIVO / S3
3.05	2018 - 2020	EL PEDREGAL	GAC N° 503	CMDTE DE SECCIÓN
3.06	2021	VENECIA	CÍA COM N° 33	JEFE DE PATRULLA
3.07	2022	VENECIA	CÍA COM N° 33	S3 / EJECUTIVO
3.08	2023 - 2024	TIABAYA	BTN COM N°113	CMDTE DE COMPAÑÍA
3.09	2025	MARIANO MELGAR	CÍA COM DE SERVS N° 113	CMDTE DE COMPAÑÍA

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

N°	Año	Dependencia y Período	Denominación	Diploma / Certificación
4.01	2010	ESCUELA MILITAR DE CHORRILLOS (01 MES)	Curso Básico de Natación de Combate	DIPLOMA
4.02	2011	ESCUELA DE SELVA DEL EJÉRCITO (01 MES)	Curso Básico de Supervivencia en Selva	DIPLOMA
4.03	2011	ESCUELA DE MONTAÑA DEL EJÉRCITO (01 MES)	Curso Básico de Supervivencia en Montaña	DIPLOMA
4.04	2012	ESCUELA DE PARACAIDISMO DEL EJÉRCITO (01 MES)	Curso Básico de Paracaidismo Militar	DIPLOMA
4.05	2012	ESCUELA MILITAR DE CHORRILLOS (04 AÑOS)	Ciencias Militares con Mención en Ingeniería	BACHILLER
4.06	2014	ESCUELA DE COMUNICACIONES DEL EJÉRCITO DEL PERÚ (06 MESES)	Curso complementario del Arma de Comunicaciones	DIPLOMA
4.07	2019	ESCUELA DE COMUNICACIONES DEL EJÉRCITO DEL PERÚ (06 MESES)	Curso Básico de Comunicaciones	DIPLOMA

4.08	2020	ESCUELA DE COMUNICACIONES DEL EJÉRCITO DEL PERÚ (06 MESES)	Curso Básico de Operaciones Cibernéticas	DIPLOMA
4.09	2024	ESCUELA DE COMUNICACIONES DEL EJÉRCITO DEL PERÚ (06 MESES)	Curso Táctico de Comunicaciones	DIPLOMA

5. ESTUDIOS DE NIVEL UNIVERSITARIO

N°	Año	Universidad y Período	Bachiller - Licenciado
5.01	2014	INSTITUTO CIENTÍFICO Y TECNOLÓGICO DEL EJÉRCITO (01 AÑO)	BACHILLER EN INGENIERÍA DE TELECOMUNICACIONES
5.02	2018	UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS (01 AÑO)	DIPLOMADO EN GESTIÓN DE DERECHO ADMINISTRATIVO

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

N°	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
6.01	X	X	X
6.02	X	X	X

7. ESTUDIOS DE ESPECIALIZACIÓN

N°	Año	Dependencia y Período	Diploma o Certificado
7.01	X	X	X
7.02	X	X	X

8. ESTUDIOS EN EL EXTRANJERO

N°	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01	X	X	X	X
8.02	X	X	X	X

O – 0004533[illegible]89 - O+
DAVID ALONSO SILVA AVILA
CAP COM
DNI: 45335259