ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

“Desafíos en la implementación de las TIC durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025”

AUTORES:

BACH. EDGAR JONATHAN ORTEGA GOYZUETA
(orcid.org/0009-0002-5104-4049)

BACH. JOYCE PAOLA CALIZAYA MALDONADO
(orcid.org/0000-0001-6398-7306)

Para optar el Grado Académico de

MAESTRO EN CIENCIAS MILITARES

Con mención en Gestión Pública y Planeamiento Estratégico

ASESOR:

Mag. Jorge Luis Bonilla Ferreyra
(orcid.org/0000-0003-2704-8066)

LÍNEA DE INVESTIGACIÓN:

Línea de esfuerzo del plan de transformación institucional

2025

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 021 – 2025/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veinticinco (25) días del mes de setiembre del año dos mil veinticinco, siendo las ..10.00..... horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctora**	**LILIANA RODRIGUEZ SAAVEDRA**	**Presidente**
❖	**Maestro**	**LIZET MILAGROS CACHO DE LA CRUZ**	**Secretario**
❖	**Doctor**	**EDMUNDO WENCESLAO DIAZ KOBASHIKAWA**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 021-2025/SIE/DGI/ESGE-EPG** del 08 de setiembre de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"DESAFÍOS EN LA IMPLEMENTACIÓN DE LAS TIC DURANTE LAS OPERACIONES Y ACCIONES TERRESTRES UNIFICADAS DE LA 3a BRIGADA BLINDADA, MOQUEGUA, 2025"**, presentado por los Bachilleres **EDGAR JONATHAN ORTEGA GOYZUETA y JOYCE PAOLA CALIZAYA MALDONADO,** para optar el Grado Académico de Maestro en Ciencias Militares con mención en Gestión Pública y Planeamiento Estratégico, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

Luego de atender la sustentación presencial, defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de ..... 16.00 .....

En mérito del cual, el jurado ..... aprueba ..... (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Ciencias Militares con mención en Gestión Pública y Planeamiento Estratégico.

Firmado, en Chorrillos a los veinticinco (25) días del mes de setiembre del año dos mil veinticinco.

DRA. LILIANA RODRIGUEZ SAAVEDRA	**MG. LIZET MILAGROS CACHO DE LA CRUZ**	**DR. EDMUNDO WENCESLAO DIAZ KOBASHIKAWA**
PRESIDENTE	**SECRETARIO**	**VOCAL**

DEDICATORIA

A mis padres Valentín y Gladis, cuyo amor y sabiduría han sido mi faro; a mi esposa, mi inspiración, cuyo amor me ha guiado en los momentos más difíciles. A mi hijo Tadeo, la luz de mis ojos, por ser mi mayor motivación. Juntos, somos invencibles.

Edgar Ortega

A mi querido padre Juan, por su amor incondicional, apoyo e impulso para obtener mis metas. A mi querido Ishwor por su paciencia y aliento, a mi querida madre Olga y a mi hermana Sandra por su cariño inmensurable. Este logro les pertenece.

Joyce Calizaya

AGRADECIMIENTOS

Mi primer agradecimiento es para Dios, cuya presencia ha sido constante en este viaje de conocimiento y descubrimiento, y por supuesto, a mi querida compañera de tesis y hermana comunicante, cuyo apoyo y compañerismo han sido fundamentales en este proceso.

Edgar Ortega

A mi querido hermano comunicante Edgar Ortega, por su apoyo durante este trayecto académico. Mi agradecimiento a los oficiales del arma de comunicaciones por su colaboración en esta investigación.

Joyce Calizaya

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El Ejército del Perú analiza las amemazas latentes que enfrenta al país en temas de seguridad, por ello, ha desarrollado el Plan de Transformacional Institucional al 2034, buscando incrementar sus capacidades militares a fin de cumplir con los roles estratégicos propuestos. Sin embargo, en la actualidad, existen grandes unidades que enfrentan desafíos para conducir operaciones y acciones militares.

Luego de identificar los problemas que enfrenta la 3ª Brigada Blindada con relación a las Tecnologías de la Información y Comunicaciones (TICs), se exploraron las limitaciones y obstáculos que surgen al integrar las TICs en el campo de batalla, incluyendo aspectos técnicos, humanos y organizacionales.

El estudio aborda la problemática de la interoperabilidad de los sistemas de comunicación, la capacitación del personal en el uso de nuevas tecnologías, la seguridad de la información en entornos hostiles y la adaptación de la doctrina militar a las capacidades que ofrecen las TICs.

Por tanto, concluimos que nuestra investigación desarrolla una excelente propuesta para optimizar la implementación de las TICs en la 3ª Brigada Blindada, con el objetivo de mejorar la eficiencia, la eficacia y la capacidad de respuesta en el cumplimiento de la misión y que a su vez, la presente investigación genere un efecto multiplicador para los futuros casos de estudio y de esta manera contribuir con la mejora continua de nuestras unidades militares.

Palabras clave: *Tecnologías de la información y comunicaciones (TICs), operaciones terrestres unificadas, brigada blindada, capacitación, doctrina militar, seguridad de la información.*

ABSTRACT

The Peruvian Army analyzes the latent threats that the country faces in security issues, therefore, it has developed the Institutional Transformation Plan for 2034, seeking to increase its military capabilities in order to fulfill the proposed strategic roles. However, currently, there are units that face challenges in conducting military operations and actions.

After identifying the problems faced by the 3rd Armored Brigade in relation to Information and Communications Technologies (ICTs), the limitations and obstacles that arise when integrating ICTs on the battlefield were explored, including technical, human, and organizational aspects.

The study addresses the problems of the interoperability of communication systems, the training of personnel in the use of new technologies, information security in hostile environments and adaptation of military doctrine to the capabilities offered by ICTs.

Therefore, we conclude that our research develops an excellent proposal to optimize the implementation of ICTs in the 3rd Armored Brigade, with the aim of improving efficiency, effectiveness and response capacity in fulfilling the mission and that, it turns, this research generates a multiplier effect for future case studies and in this way contribute to the continuous improvement of our military units.

Keywords: *information and communications technologies (ICTs), unified land operations, armored brigade, training, military doctrine, information security.*

REPORTE DE SIMILITUD

(VISADO POR DGI)

calizaya ortega 28 ABR OBS OK SIN BIBLIOG.docx

Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:453727372

Fecha de entrega
28 abr 2025, 8:00 p.m. GMT-5

Fecha de descarga
28 abr 2025, 8:24 p.m. GMT-5

Nombre de archivo
calizaya ortega 28 ABR OBS OK SIN BIBLIOG.docx

Tamaño de archivo
6.9 MB

151 Páginas

41.280 Palabras

242.255 Caracteres

turnitin Página 1 of 159 - Portada Identificador de la entrega trn:oid:::12350:453727372

turnitin Página 2 of 159 - Integrity Overview Identificador de la entrega trn:oid:::12350:453727372

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 10 words)

Top Sources

6% Internet sources
2% Publications
5% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

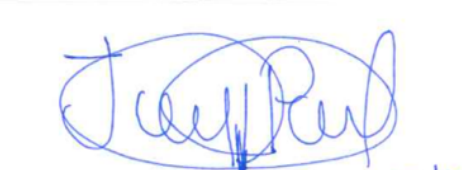
A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

DECLARACIÓN JURADA DE AUTENTICIDAD Y NO PLAGIO

(Grado Académico de Maestro)

Por el presente documento, yo **CALIZAYA MALDONADO Joyce Paola**, identificada con DNI N° **45099729,** egresada del programa de **Comando y Estado Mayor**, informo que ha elaborado el Trabajo de Investigación denominado **"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025",** para optar por el Grado Académico de **Maestro** en la **LXIX Maestría en Ciencias Militares con mención en Gestión Pública y Planeamiento Estratégico,** declaro que este trabajo ha sido desarrollado íntegramente por los autores que suscriben y afirmamos que no existe plagio de ninguna naturaleza. Asimismo, dejamos constancia de que las citas de otros autores han sido correctamente identificadas en el trabajo, por lo que no se ha tomado como propias las ideas de terceros, ya sean de fuentes escritas o de Internet.

Asimismo, afirmamos que somos responsables solidarios de todo su contenido y que, como autor, asumo las consecuencias por cualquier falta, error u omisión en las referencias del documento. Soy consciente de que este compromiso con la autenticidad y la ausencia de plagio puede implicar implicaciones éticas y legales. Por lo tanto, en caso de incumplir con esta declaración, me someto a las disposiciones establecidas en las normas académicas que determine la Escuela Superior de Guerra del Ejército – Escuela de Posgrado y a lo estipulado en el Reglamento interno.

(firma) 

Nombres y apellidos JOYCE PAOLA CALIZAYA MALDONADO

número de DNI 45099729

DECLARACIÓN JURADA DE AUTENTICIDAD Y NO PLAGIO

(Grado Académico de Maestro)

Por el presente documento, yo **ORTEGA GOYZUETA Edgar Jonathan**, identificado con DNI N° **44635865,** egresada del programa de **Comando y Estado Mayor**, informo que ha elaborado el Trabajo de Investigación denominado **"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025",** para optar por el Grado Académico de **Maestro** en la **LXIX Maestría en Ciencias Militares con mención en Gestión Pública y Planeamiento Estratégico,** y declaro que este trabajo ha sido desarrollado íntegramente por los autores que suscriben y afirmamos que no existe plagio de ninguna naturaleza. Asimismo, dejamos constancia de que las citas de otros autores han sido correctamente identificadas en el trabajo, por lo que no se ha tomado como propias las ideas de terceros, ya sean de fuentes escritas o de Internet.

Asimismo, afirmamos que somos responsables solidarios de todo su contenido y que, como autor, asumo las consecuencias por cualquier falta, error u omisión en las referencias del documento. Soy consciente de que este compromiso con la autenticidad y la ausencia de plagio puede implicar implicaciones éticas y legales. Por lo tanto, en caso de incumplir con esta declaración, me someto a las disposiciones establecidas en las normas académicas que determine la Escuela Superior de Guerra del Ejército – Escuela de Posgrado y a lo estipulado en el Reglamento interno.

(firma) 

Nombres y apellidos EDGAR JONATHAN ORTEGA GOYZUETA

número de DNI 44635865

INTRODUCCIÓN

Las operaciones y acciones terrestres unificadas se sustentan en el Manual Fundamental MF 3-1 (Primera edición – 2019), el cual describe conceptos empleados durante el planeamiento, preparación y ejecución de operaciones y acciones terrestres por el Ejército del Perú, con el objetivo de enfrentar las amenazas y desafíos en el cumplimiento de los roles estratégicos asignados por el Estado para la defensa de los intereses nacionales.

Las Grandes Unidades de Combate, en el nivel táctico, son las encargadas de conducir dichas operaciones y acciones militares, siendo un factor demandante, el estar equipados con una adecuada tecnología y que se adapte a nuestras necesidades para hacer frente de manera sostenida los requerimientos en el campo de batalla, teniendo como fin garantizar la seguridad y defensa nacional.

Las TICs se han convertido en un elemento fundamental para el éxito de la operaciones y acciones terrestres unificadas. Sin embargo, la adopción de TICs en el ámbito militar no está exenta de dificultades, especialmente en unidades como la 3ª Brigada Blindada, cuyo despliegue exige una infraestructura y sistema de comando control eficiente y seguro que permita mejorar la toma de decisiones, la coordinación entre unidades, la eficiencia logística y la capacidad de respuesta ante situaciones imprevistas.

La presente investigación busca dar solución al problema principal identificado: ¿Cuáles son los principales desafíos que enfrenta la 3ª Brigada Blindada para la implementación exitosa de las TICs en sus operaciones y acciones terrestres unificadas durante el año 2025?

El objetivo general del estudio es analizar los principales desafíos que enfrenta la 3ª Brigada Blindada para la implementación exitosa de las TICs en sus operaciones y acciones terrestres unificadas durante el año 2025.

Esta investigación se llevará a cabo bajo un enfoque cualitativo, de tipo teórico- empírico. Además, se empleará el método hermenéutico interpretativo para analizar la información recopilada. La población de estudio estará conformada por oficiales de estado mayor del Ejército del Perú y la muestra seleccionada será de diez oficiales de estado mayor del grado de mayor, teniente coronel y coronel, oficiales que por sus años de servicio, experiencia y conocimiento son considerados informantes claves para la comprensión de los desafíos que se investigan.

La estructura de la tesis se organiza en cinco capítulos, según el siguiente detalle:

En el capítulo I, se detalla el planteamiento del problema, la formulación de la pregunta de investigación y la definición de los objetivos.

En el capítulo II, presenta una revisión exhaustiva relacionada con la implementación de las TICs en el ámbito militar, así como los antecedentes.

En el capítulo III, describe el enfoque cualitativo, el tipo teórico empírico, el método hermenéutico interpretativo, la población y muestra de estudio, así como las técnicas de recolección y análisis de datos.

En el capítulo IV, presenta los resultados obtenidos a partir del análisis de la información recopilada, identificando y describiendo los principales desafíos que enfrenta la 3ª Brigada Blindada en la implementación de TICs. Se realiza una síntesis de los hallazgos y se establecen las relaciones entre los diferentes desafíos identificados.

Finalmente, en el capítulo V, se discuten las implicaciones de los hallazgos para la práctica militar y se proponen recomendaciones para afrontar los desafíos identificados.

Los resultados de este estudio podrán ser utilizados por la 3ª Brigada Blindada y otras unidades militares para mejorar su capacidad operativa y su eficiencia en el cumplimiento de su misión. Así mismo, esta investigación sentará las bases para futuros estudios en el campo de la implementación de TICs en el marco militar.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Situación Problemática

En la actualidad, las organizaciones militares están atravesando una transformación sin precedentes, incorporando tecnologías disruptivas como la Inteligencia Artificial (IA) y el Big Data (BD) para hacer más eficientes sus operaciones. No obstante, la incorporación de estas tecnologías plantea desafíos importantes, especialmente en el ámbito terrestre. La 3ra Brigada Blindada, a pesar de estar a la vanguardia en cuanto a la capacidad de asegurar y controlar sus respectivas áreas de responsabilidad, enfrenta el desafío de integrar las Tecnologías de la Información y la Comunicación (TICs) durante sus operaciones y acciones de poder terrestre unificadas. Esta situación se agrava debido a la ausencia de infraestructura, la falta de formación y voluntad para el cambio, así como problemas de ciberseguridad e incompatibilidad de sistemas. Esto conlleva graves consecuencias, como la disminución de la eficacia operativa, la incapacidad de contrarrestar nuevas amenazas y una mayor vulnerabilidad ante ciberataques. Por lo tanto, es esencial desarrollar un esquema viable para la integración de las TICs, considerando tanto sus beneficios como sus posibles desafíos.

Las organizaciones militares, al igual que otras instituciones, están adoptando tecnologías emergentes como Big Data (BD), Inteligencia Artificial (IA), Internet de las Cosas (IoT) y Machine Learning (ML) para optimizar procesos, automatizar tareas y mejorar la detección de amenazas. Si bien esta transformación tecnológica ofrece múltiples beneficios, su implementación requiere una planificación estratégica que contemple la capacitación del personal y la adopción de medidas robustas de ciberseguridad para mitigar posibles riesgos.

En el nivel internacional, según Lodeiro (2021) en su Cuaderno de Trabajo N°9-2021, titulado “Evolución y Proyecciones del Uso de Big Data en Defensa” sostiene la medición

estratégica de la implementación de tecnologías como el BD en el ámbito de la Defensa para potenciar la capacidad operativa, disminuir los riesgos, costos y los problemas que enfrentan o enfrentarán las operaciones militares al presente y futuro. En el marco de estas afirmaciones, enfatiza que las propuestas de integración de BD en la Defensa deben disfrutar de un beneficio real para la defensa nacional y poderse integrar a los sistemas existentes con una probada capacidad de interoperabilidad. Este enfoque resulta muy eficaz para el uso de las bases de datos en la planificación de las operaciones y acciones de la 3ra Brigada Blindada en el horizonte del 2025.

Tecnologías como el Machine Learning (ML), la Inteligencia Artificial (AI), el Big Data (BD), el Internet de las Cosas (IoT), por mencionar algunos, ya se están integrando a las entidades u organizaciones civiles y militares, logrando eficiencias claves en la optimización de procesos, automatización de tareas y en la detección de amenazas que mejoran la eficiencia y protegen la seguridad institucional.

En el contexto de la guerra híbrida, el ciberespacio es un escenario clave en el que las TICs desempeñan un papel fundamental. Su acceso masivo y la posibilidad de manipular información facilitan el uso de tácticas convencionales y no convencionales para influir en la sociedad y debilitar estructuras estatales. Por ello, la integración de TICs en operaciones y acciones terrestres unificadas representa un reto considerable, dada la complejidad y versatilidad de los conflictos actuales, donde la ciberseguridad y la defensa de ciberataques son factores relevantes por atender (Capdevilla, 2022, p. 64).

En el campo militar, el avance de las tecnologías es quizás el más importante para afrontar nuevos retos dadas las herramientas y los recursos disponibles. El rápido desarrollo de la tecnología digital está impactando en todas las esferas, desde la economía hasta las personas, abriendo oportunidades, así como desafíos y amenazas en cada nivel. En este entorno global, surgen nuevos actores que pueden mejorar la productividad y el bienestar en cantidades

adecuadas para muchas naciones. Sin embargo, aquellos que no sean capaces de adaptarse al ritmo y carácter del cambio pueden sufrir grandes desventajas (Fojón, 2020, p. 14).

Fojón (2020) menciona la importancia de las TICs en el marco militar. Las TICs son herramientas clave para mejorar el control y la seguridad en operaciones terrestres unificadas. No obstante, su implementación requiere inversión en infraestructura y capacitación continua del personal para garantizar su uso efectivo en las operaciones. Además, el uso de las TICs puede representar problemas de seguridad porque sus sistemas de información están expuestos a ataques cibernéticos. Así, es muy importante que la 3ra Brigada Blindada realice un estudio efectivo de planeamiento para la adopción de las TICs, en el contexto de sus beneficios y desafíos.

En la región, Espitia Cubillos, Agudelo Calderón y Buitrago Suescun (2020) destacan avances en el uso de tecnologías emergentes, las cuales mejoran el monitoreo y control en las áreas de responsabilidad de las organizaciones militares. El estudio presenta un análisis preliminar del avance tecnológico a nivel mundial basado en la información adquirida en sitios web aprobados de todos los países.

Para fines de análisis, la recopilación de información se organiza en dieciocho (18) categorías con la finalidad de determinar las tendencias más representativas. Los descubrimientos tecnológicos ofrecen un nuevo horizonte en la ejecución de las tareas asignadas. En la actualidad, se prevé un crecimiento en los campos de robótica, sensores y ciberseguridad. Las armas (de corto y largo alcance), los vehículos de combate, la aeronáutica, las telecomunicaciones, y las plataformas en que se incorporan nuevas tecnologías al conjunto del sistema de defensa del país. Nos encontramos en un momento histórico donde potencias como China, Rusia y Estados Unidos, ostentan la cantidad notable de recursos humanos y económicos generados por todas las innovaciones, en contraste, otros países siguen siendo dependientes de estos avances tecnológicos. (Espitia Cubillos, Agudelo Calderón y Buitrago Suescún, 2020, p. 213).

A nivel nacional, las TICs están transformando la seguridad en el Perú, como se evidencia en la incorporación de tecnologías en la Gestión del Riesgo de Desastres (GRD). Las TICs permiten mejorar las coordinaciones con el objetivo de tomar decisiones apropiadas. En la GRD, la comunicación y el procesamiento inmediato de datos permiten identificar zonas de población afectadas, alertar a la población y activar respuestas efectivas. En los servicios militares, las TICs hacen más eficiente y segura la planificación, el control y la evaluación de las operaciones de los institutos armados.

En el nivel nacional, Vega (2021) sostiene que las TICs son herramientas esenciales en la Gestión del Riesgo de Desastres (GRD), especialmente en las fases de preparación y respuesta. Las herramientas virtuales no solo mejoran la gestión de la información, sino que también son muy importantes en la planificación y ejecución de operaciones militares. De esta manera, las redes sociales se convierten en un canal importante para la difusión de información crucial. Por lo tanto, los sistemas de mando y control deben integrarse con estas plataformas de redes sociales para que actúen como sistemas de alerta de desastres. En GRD, las TICs brindan varios beneficios como una mejora en la recopilación y análisis de datos, una comunicación efectiva, la coordinación de acciones y la difusión de información. La interconexión de las redes sociales con los sistemas de mando y control permite conocer de inmediato la situación actual, lo que ayuda a tener las necesidades clave, la información y las alertas de desastres.

Respecto a la región mencionada, Huertas (2023) destaca que la Fuerza Aérea del Perú (FAP) es la encargada de planificar y ejecutar las operaciones aéreas como parte del Componente Aéreo de las Fuerzas Armadas. Estas operaciones coadyuvan al cumplimiento de los objetivos de la Estrategia de Defensa y Seguridad Nacional detallados en la Ley N° 1139, que da primacía a la participación activa en las operaciones militares. Se deben utilizar de manera óptima los recursos de Tecnologías de la Información (TI), lo que es necesario para mejorar la toma rápida de decisiones y se necesita personal capacitado y calificado de acuerdo con la

Doctrina FAP (2021). Esto hace énfasis en la automatización de los procesos operativos de gestión y comando militar.

La Fuerza Aérea del Perú (FAP) está incorporando nuevas tecnologías de información y comunicación (TICs) tanto en sus sistemas de gestión como en sus operaciones para hacerlas más efectivas y garantizar una mejor integración dentro de sus actividades. Esto se fundamenta en su trabajo y forma parte de un cambio dentro de las Fuerzas Armadas. Se espera que las TICs aborden las complejidades del actual entorno de seguridad, particularmente en el ámbito terrestre. El desafío radica en trasladar los éxitos alcanzados en el dominio aéreo al entorno terrestre.

El Perú se propuso lograr sostenibilidad y efectividad operativa a través de la fase de evolución hacia la digitalización dentro del ejército. Sin embargo, la incorporación de nuevas tecnologías en las operaciones y acciones militares está siendo obstaculizada por una infraestructura deficiente, incompatibilidad de sistemas, restricciones presupuestarias y la falta de capacitación. Si estas limitaciones persisten, se generará una desigualdad competitiva que afectará profundamente el correcto funcionamiento de las estructuras existentes. Por lo tanto, la innovación es fundamental para mejorar la toma de decisiones eficientes en el campo de las operaciones militares.

La integración de tecnologías de comunicación e información en operaciones y acciones militares terrestres unificadas presentan un conjunto único de desafíos operativos para la 3ra Brigada Blindada. Estos desafíos representan una amenaza directa para sus capacidades operativas, así como para la seguridad estratégica de sus misiones. Sin embargo, la condición actual de las armas de combate está dictada por una de las principales deficiencias estructurales dentro de los sistemas tecnológicos modernos: la falta de la integración avanzada requerida.

Esta infraestructura, obsoleta e incapaz de abordar la escala y complejidad de los datos producidos por tecnologías emergentes como Big Data, Inteligencia Artificial (IA) y Aprendizaje Automático, crea una situación crítica en la que se ignoran propuestas de valor clave. La falta de

actualización de los sistemas de telecomunicaciones no solo limita la comunicación adecuada, sino que además restringe la capacidad de la brigada para satisfacer las demandas de un entorno de guerra digital cada vez más sofisticado, donde el tiempo y la precisión determinan el éxito. Si esta deficiencia de infraestructura persiste frente a la integración de las TICs por parte de los adversarios existentes, la brigada podría enfrentar una pérdida aún mayor de capacidades estratégicas operacionales globales, lo que los haría cada vez más vulnerables a las tecnologías avanzadas de combate y, en última instancia, perderían su ventaja competitiva.

Además de la deficiencia particularmente problemática en infraestructura, existe un obstáculo cultural y organizativo que impacta de manera significativa en la efectividad de la brigada: la resistencia al cambio. Este tipo de oposición se manifiesta en una falta de voluntad, especialmente entre el personal de mayor edad, para aceptar nuevas tecnologías y herramientas digitales, debido a que se sienten desconectados o escépticos sobre la aplicación de los avances tecnológicos en el ámbito militar. La ausencia de formación continua en TICs y la falta de un proceso formal de gestión del cambio dentro de la organización generan un desfase entre las demandas operativas del contexto actual y la estructura técnica del personal. Esta resistencia cultural afecta no solo la adaptación tecnológica, sino que también tiene efectos secundarios en la cohesión y moral de la unidad, al generar un clima de desconfianza frente al uso de nuevas tecnologías. Si no se desarrollan nuevas estrategias para abordar la necesidad de formación progresiva, esta resistencia al cambio y la brecha existente entre la realidad tecnológica y la preparación humana seguirán creciendo, debilitando la cohesión interna de la brigada y disminuyendo su efectividad en escenarios operativos de alta exigencia.

Las vulnerabilidades en ciberseguridad son otro aspecto clave que condiciona la seguridad operativa de la brigada. El riesgo de ciberataques aumenta con la digitalización del ámbito militar, haciendo que la brigada sea más vulnerable a un mayor número de ataques dirigidos a interrumpir sus comunicaciones o a obtener información estratégica. La infraestructura cibernética obsoleta, así como la ausencia de un sistema sólido de mitigación de amenazas

cibernéticas, colocan a la brigada en una situación de alto riesgo. Estas amenazas pueden provenir de entidades hostiles que utilicen el ciberespacio para lanzar ataques que paralicen las capacidades operativas de la unidad. Además, la desconexión entre las plataformas tecnológicas utilizadas por las diferentes unidades y socios internacionales incrementa la probabilidad de que ocurran brechas de seguridad. La falta de medidas preventivas y modernas en ciberseguridad para reforzar los protocolos de defensa y permitir la interoperabilidad de los sistemas podría hacer que las consecuencias de un ciberataque exitoso sean verdaderamente catastróficas.

La pérdida de confidencialidad de información crítica, la alteración de las redes de comunicación y la incapacidad de coordinar operaciones conjuntas con aliados de manera efectiva podrían perjudicar gravemente las respuestas en tiempo real, interrumpir maniobras tácticas y dejar a la brigada vulnerable en un entorno de guerra híbrida, donde las amenazas cibernéticas y físicas se mezclan de manera arbitraria.

En el contexto de la interoperabilidad, la falta de integración de los sistemas informáticos de la brigada y sus aliados internacionales constituye una gran dificultad para la coordinación interinstitucional en un marco de guerra conjunta. Esta falta de tecnología hace que la brigada no pueda colaborar de manera efectiva con otros aliados a través del intercambio de información crítica, lo que afecta la sincronización de las acciones en tiempo real y la capacidad de reacción ante amenazas comunes. La carencia de interoperabilidad representa una barrera para la ejecución efectiva de operaciones de combate conjunto, donde la integración de datos y la coordinación precisa son esenciales para el éxito de las operaciones. Si estas debilidades en la infraestructura y los protocolos de comunicación no se resuelven, la brigada estará en desventaja operativa frente a fuerzas extranjeras que posean plataformas tecnológicas más avanzadas e integradas, lo que, a su vez, comprometerá su desempeño estratégico en operaciones multinacionales.

Adaptarse a la innovación tecnológica es un desafío estratégico que amenaza con posicionar a la brigada en una desventaja competitiva frente a contrapartes más capacitadas. La

incapacidad para adaptarse a nuevas tecnologías como drones autónomos, robots de combate o inteligencia artificial para análisis predictivo limita la competitividad de la brigada en su capacidad para disuadir y responder rápidamente a las amenazas y dinámicas de combate de la guerra moderna. La ausencia de automatización de procesos, junto con el no uso de Big Data e inteligencia artificial para la predicción de escenarios y el análisis posterior a los eventos, coloca a la brigada en una clara desventaja estratégica, ya que no podrá responder de manera rápida y eficiente a un entorno hostil. Peor aún, dudará en tomar decisiones tácticas, a diferencia de sus adversarios, quienes estarán equipados con estas herramientas avanzadas de alerta. Sin una adopción rápida de estas tecnologías, se perderán agilidad y precisión en las operaciones, lo que puede resultar en graves errores tácticos y fallos operativos en situaciones críticas donde cada segundo es vital.

A menos que se aborden estas brechas en las áreas de infraestructura tecnológica, capacitación, ciberseguridad, interoperabilidad y adaptación tecnológica, la situación de la 3ra Brigada Blindada seguirá siendo cada vez más insostenible. La incapacidad para actualizar la infraestructura tecnológica, junto con la resistencia cultural al cambio, continuará agravando las desventajas operativas, mientras que las brechas de seguridad y la falta de estandarización limitarán la capacidad de la brigada para llevar a cabo operaciones conjuntas de manera efectiva. Con la digitalización continua de los conflictos armados y el uso de tecnologías sofisticadas por parte de los adversarios, la falta de adaptación a estas modificaciones tecnológicas restringirá considerablemente la capacidad de la brigada para competir en el campo de batalla moderno. La pérdida de competitividad y la incapacidad para enfrentar los desafíos estratégicos emergentes no solo reducirán la efectividad operativa de la brigada, sino que también pondrán en peligro la seguridad nacional al exponer las vulnerabilidades de la brigada a fuerzas hostiles.

Para resolver este problema, se utilizarán las subcategorías de desafíos en la Implementación de las TICs y los Impactos de las TICs en las operaciones y acciones terrestres unificadas, como implementación técnica, cultural y organizativa; ciberseguridad; eficiencia

operativa; interoperabilidad; y adopción de innovación tecnológica. Esto ayudará a definir los obstáculos más críticos en la integración de las TICs y los impactos que tienen en la capacidad operativa de la brigada. El enfoque se dirigirá a la eficiencia operativa mediante la modernización de la infraestructura tecnológica existente para habilitar el uso de nuevas herramientas emergentes como la ciberinteligencia, Big Data y Machine Learning. Todo esto es imprescindible para que las decisiones puedan ser tomadas de forma precisa y rápida. La implementación cultural y organizativa se orientará hacia la necesidad de formación y la gestión del cambio, con el objetivo de combatir la resistencia organizativa y la inercia operativa. Además, en el ámbito de la ciberseguridad, la atención estará centrada en las amenazas de ciberataques que pueden poner en riesgo las comunicaciones y las operaciones conjuntas. La subcategoría de eficiencia operativa analizará cómo la falta de tecnología avanzada limita la capacidad de responder a nuevas movilizaciones, mientras que la falta de interoperabilidad se enfocará en la integración tecnológica entre las diferentes unidades y sus socios.

Por último, actualizarse con tecnologías innovadoras permitirá a la organización protegerse de la competencia, que puede adquirir y desarrollar tecnologías disruptivas como drones inteligentes e inteligencia artificial para realizar análisis predictivos. Realizar este tipo de análisis es fundamental para identificar las áreas de mejora y garantizar que la brigada pueda enfrentar los desafíos tecnológicos del futuro, manteniéndose competitiva y operativamente efectiva.

Esta perspectiva intenta identificar los impedimentos y cambios más significativos que garantizarían una adaptación exitosa de la brigada al entorno digital global contemporáneo, lo que garantiza que las capacidades operativas y de defensa estén listas para enfrentar los desafíos tecnológicos y cibernéticos emergentes del futuro cercano.

1.2 Formulación del problema

1.2.1 Problema General

PG: ¿Cuáles son los principales desafíos que enfrenta la 3ª Brigada Blindada para la implementación exitosa de las Tecnologías de la Información y las Comunicaciones (TICs) en sus operaciones y acciones terrestres unificadas durante el año 2025?

1.2.2 Problemas específicos

PE1: ¿Cuáles son las principales limitaciones tecnológicas y de infraestructura que afectan la implementación de las TICs en las operaciones de la 3ª Brigada Blindada?

PE2: ¿Qué nivel de capacitación y preparación tiene el personal militar para utilizar eficazmente las TICs en las operaciones y acciones terrestres?

PE3: ¿Qué barreras organizacionales y culturales están impidiendo la adopción de las TICs en la 3ª Brigada Blindada?

PE4: ¿Qué estrategias y medidas se pueden implementar para superar las vulnerabilidades de ciberseguridad asociadas a la adopción de TICs y lograr la interoperabilidad de los sistemas en las operaciones militares?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

OG: Analizar los principales desafíos que enfrenta la 3ra Brigada Blindada para la implementación exitosa de las TICs en sus operaciones y acciones terrestres unificadas durante el año 2025.

1.3.2 Objetivos específicos

OE1: Identificar las limitaciones tecnológicas e infraestructurales (hardware, software y conectividad) que afectan la implementación de las TICs en las operaciones de la 3ra Brigada Blindada.

OE2: Evaluar el nivel de capacitación y preparación (conocimiento y habilidades) del personal militar en el uso eficaz de TICs durante las operaciones y acciones terrestres.

OE3: Determinar las barreras organizacionales y culturales (cultura, liderazgo y procesos) que dificultan la adopción de las TICs en la 3ª Brigada Blindada.

OE4: Proponer estrategias y medidas (planes de capacitación, mejoras de infraestructura, protocolos de seguridad) para mitigar las vulnerabilidades de ciberseguridad relacionadas con la adopción de TICs y la interoperabilidad de los sistemas en las operaciones militares.

1.4 Justificación de la Investigación

La incorporación de las TICs en las operaciones y acciones terrestres unificadas tiende a mejorar considerablemente su eficiencia, efectividad y seguridad. Sin embargo, existen diversos problemas que pueden dificultar la adopción exitosa de estas tecnologías.

Este estudio busca identificar y analizar los principales desafíos que enfrenta la 3ra Brigada Blindada en la adopción de las TICs para sus operaciones y acciones terrestres unificadas. Además, la investigación tiene como objetivo hacer recomendaciones sobre cómo superar estos desafíos para garantizar la correcta adopción de las TICs en la Brigada.

1.4.1 Justificación teórica:

La investigación se sustenta en las siguientes teorías:

Teoría de Sistemas Complejos y Teoría de la Contingencia: Estas teorías sostienen que las TICs son relevantes para el control de la complejidad y de la incertidumbre dentro de los procesos operativos. Permiten a las organizaciones como la 3ra Brigada Blindada operar en escenarios donde pueden decidir ejecutar cambios en comunicación y ser mucho más efectivos y flexibles (Hernández-Sampieri & Mendoza, 2018).

Teoría de la Difusión de las Innovaciones: Rogers (1962) sostiene que el uso de tecnologías modernas conlleva una cierta previsibilidad. Esta teoría permite analizar cómo se incorporan las TICs en la 3ra Brigada Blindada y los factores que influyen en su adopción. Conocer este proceso facilita la asimilación de las TICs y ayuda a eliminar obstáculos.

Teoría de la Organización: Esta teoría contribuye a la comprensión de la respuesta organizativa y la adaptación a cambios. La adopción de las TICs requiere aprovechar esta importante teoría para poder analizar los efectos que las mismas producen en la organización y funcionamiento de la brigada, y por consiguiente, cómo se modifican las estrategias para el cambio (Scott, 2003).

Teoría de la Gestión del Cambio: Kotter (1996) ofrece un modelo de gestión del cambio que sirve como guía para gestionar un proceso de cambio. Esta teoría es fundamental para desarrollar intervenciones que gestionen la transición hacia el uso de las TICs, asegurando que el personal se adapte y adopte las tecnologías de manera eficiente.

Estas teorías proporcionan un marco conceptual sólido para abordar la adopción de las TICs, al ofrecer información sobre los problemas potenciales y las estrategias necesarias para garantizar el éxito.

1.4.2. Justificación metodológica:

Para comprender las experiencias y percepciones del personal militar sobre la adopción de las TICs, se utilizará un enfoque cualitativo. Este enfoque enfatiza el significado y los procesos por encima de la medición, lo que resulta fundamental para capturar los factores humanos y organizacionales del cambio tecnológico (Mariaca Garron et al., 2022).

Se emplearán los siguientes métodos de recopilación de datos:

Entrevistas en profundidad: Estas proporcionan una vía para captar las percepciones del personal militar, especialmente de los oficiales de alto rango en relación con su planificación y recepción de las TICs. Este tipo de entrevistas permiten recopilar relatos personales significativos sobre los sentimientos y experiencias de los entrevistados.

Grupos focales: Brindan una plataforma para que los oficiales militares de diferentes rangos expresen sus puntos de vista y participen en un diálogo interactivo sobre las TICs. Este enfoque es crucial para identificar patrones, problemáticas y posibles resistencias al cambio dentro de la brigada.

Análisis documental: El análisis de documentos es esencial para comprender el contexto oficial y las políticas que rodean las TICs. Los manuales de procedimientos reflejan el pensamiento institucional en relación con la comunicación y la estrategia de integración de las TICs.

Estas técnicas permiten una mejor comprensión de los obstáculos y actitudes hacia el uso de las TICs, lo que facilita la formulación de recomendaciones prácticas.

1.4.3 Justificación práctica:

La adopción y el uso adecuado de herramientas tecnológicas en la 3ra Brigada Blindada permiten gestionar la unidad de manera eficiente, lo que facilita la toma de decisiones en beneficio de la organización. Las TICs son fundamentales para la coordinación, la comunicación y la gestión de la información, aspectos clave para el éxito de las operaciones y acciones terrestres unificadas. Según Espitia Cubillos, Agudelo Calderón y Buitrago Suescún (2020), el uso de las TICs facilita la agilidad en el acompañamiento ante amenazas, optimiza el nivel de esfuerzo, mejora la seguridad operativa y reduce costos.

Esta investigación es de vital importancia para contrarrestar los problemas derivados de la falta de conocimiento sobre las TICs en la brigada. Su implementación contribuirá a aumentar la eficacia y a reducir los riesgos en las acciones de la 3ra Brigada Blindada, mejorando la efectividad de sus operaciones y acciones terrestres y su rendimiento en combate. Al abordar estas deficiencias, se fortalecerá la capacidad de la brigada para enfrentar nuevas amenazas y optimizar los resultados de sus operaciones, al mismo tiempo que se garantizará una respuesta efectiva a los desafíos asociados con la implementación de herramientas TICs en la estructura militar.

1.5 Viabilidad de la Investigación

La viabilidad de esta investigación se sustenta en una planificación detallada de los recursos, el acceso a la información y la cooperación institucional. El enfoque metodológico será cualitativo, utilizando técnicas como entrevistas en profundidad, guía de observación y análisis documental para obtener datos significativos sobre los desafíos en la implementación de TICs en las operaciones militares. Las entrevistas en profundidad permitirán explorar las experiencias de los oficiales y personal relacionado con las operaciones, mientras que la guía de observación facilitará una evaluación directa del uso de las TICs en el contexto de las operaciones y acciones terrestres unificadas. Además, el análisis documental proporcionará una visión profunda de los protocolos, normativas y documentos internos que guían la implementación de las TICs en la brigada. La recolección de información dependerá de la cooperación con las autoridades de la 3ra Brigada Blindada y de la obtención de los permisos necesarios para acceder a datos sensibles.

Según Hernández, Fernández y Baptista (2010), "la viabilidad de una investigación depende de una correcta planificación de los recursos, el acceso a la información pertinente y la superación de obstáculos logísticos y éticos" (p. 85). Este enfoque metodológico integral asegura la obtención de datos fiables y relevantes para el análisis de los desafíos en la implementación tecnológica en el ámbito militar.

Aunque existen limitaciones potenciales, como la restricción de información confidencial y la disponibilidad de los participantes, la investigación tiene el potencial de generar aportes significativos sobre la optimización del uso de las TICs en las operaciones militares. Los resultados esperados permitirán identificar barreras y proporcionar recomendaciones prácticas para mejorar la implementación de las TICs en las operaciones y acciones terrestres unificadas. La viabilidad del estudio está respaldada por una estructura metodológica sólida, la cooperación de las partes involucradas y el compromiso institucional, lo que asegura la realización exitosa del estudio.

CAPÍTULO II: ESTADO DEL ARTE

2.1. Antecedentes de la investigación

La implementación de las TICs en operaciones militares contemporáneas afronta una cadena de desafíos específicos que reflejan tanto las particularidades del entorno operacional como las características únicas de las fuerzas involucradas. En el contexto de la 3ra Brigada Blindada en Moquegua, Perú, la integración de TICs durante las acciones terrestres unificadas planeadas para el año 2025 se encuentra en una encrucijada clave. La región, conocida por su compleja geografía y las exigencias tácticas de las operaciones blindadas, requiere soluciones tecnológicas adaptadas a estos desafíos. Además, el avance tecnológico global, marcado por la evolución de la IA, el BD y las redes 5G, proporcionan nuevas herramientas pero también plantea nuevos retos en términos de ciberseguridad, interoperabilidad y adaptación logística. Es en este marco que la presente investigación se propone explorar y analizar los obstáculos y las oportunidades para la implementación efectiva de TICs en la 3ra Brigada Blindada, con el objetivo de optimizar las capacidades operacionales y acrecentar la operatividad en el campo de batalla.

2.1.1. Antecedentes Nacionales

Yataco (2020) llevó a cabo la tesis titulada "Optimización de los sistemas de vigilancia de frontera terrestre y franja de frontera para actuar contra delitos fronterizos y ambientales". El objetivo de la investigación fue disminuir la vulnerabilidad del límite terrestre y reforzar la deficiente asistencia del gobierno peruano en esta zona. La metodología empleada fue cualitativa de nivel descriptivo, con un enfoque en el análisis de las estrategias y tecnologías implementadas en la vigilancia fronteriza. La tesis incluye resultados estadísticos favorables que muestran un progreso importante en la eficacia de los sistemas de vigilancia tras la implementación de tecnologías avanzadas. Estos resultados se basan en una evaluación comparativa de datos pre

y post implementación, evidenciando una reducción en los delitos fronterizos y una mayor capacidad de respuesta ante incidentes. La interpretación de estos datos subraya la magnitud de adoptar tecnologías modernas para optimizar la seguridad y proteger el medio ambiente en las zonas fronterizas. En conclusión, la tesis infiere en que la integración de estas tecnologías no solo mejora la eficacia de la vigilancia fronteriza, sino que también fortalece la capacidad del Estado para disuadir actividades ilícitas. El aporte del investigador es altamente relevante para la presente investigación, ya que proporciona evidencia empírica de cómo la implementación de tecnologías puede optimizar la seguridad y gestión en contextos similares, ofreciendo un marco de referencia valioso para la planificación y ejecución de estrategias militares avanzadas.

Briones (2021) realizó la investigación titulada "Capacidades del Sistema de C2 de la 3ra Brigada de Caballería en la Defensa Activa" en la Escuela Superior de Guerra del Ejército del Perú. El estudio, de enfoque cualitativo y metodología hermenéutica, se centró en analizar las capacidades de Comando y Control (C2) en la 3ra Brigada de Caballería, específicamente en su empleo en la Defensa Activa en el área de operaciones. La muestra consistió en seis expertos, y se utilizaron técnicas como la indagación documental, entrevistas y observación directa. Como resultado, se dedujo que la capacidad de C2 de la brigada se ve acotada por la escasez de desarrollo de las capacidades operativas necesarias para respaldar el sistema.

Con respecto a las tecnologías de la información en unidades militares, este antecedente nacional resalta la importancia de contar con capacidades operativas sólidas para respaldar los sistemas de Comando y Control. La investigación de Briones (2021) pone de manifiesto la necesidad de un desarrollo adecuado en este ámbito para garantizar el funcionamiento efectivo de las unidades militares en sus operaciones. Esto señala la trascendencia de contar con tecnologías de información en el contexto militar, donde su correcta implementación y actualización son fundamentales para optimizar las capacidades de las unidades y mejorar su desempeño en el combate.

En el contexto nacional, se reconoce la trascendencia de la inteligencia táctica, militar y policial en la generación de inteligencia estratégica para resguardar la seguridad y defensa del país. De acuerdo con la Revista Académica de la Escuela de Posgrado de la Policía Nacional del Perú, se enfatiza que otorgar inteligencia estratégica al Jefe de Estado y al Consejo de Ministros para la elaboración y realización de las acciones y políticas es esencial para proteger la soberanía nacional y fomentar el bienestar general (ESCPOGRAPNP, 2023, p. 82). Asimismo, se destaca que la inversión en tecnología y su propio crecimiento veloz, así como la inteligencia artificial, plantean desafíos y oportunidades en la producción de inteligencia táctica y estratégica (ESCPOGRAPNP, 2023, p. 94). Estos antecedentes nacionales subrayan la envergadura de poseer un sistema de inteligencia eficaz y actualizado para afrontar las amenazas internas y externas que puedan comprometer la seguridad del país. Este estudio, con metodología cualitativa, se relaciona con la investigación planteada, ya que muestra el valor de las tecnologías de información en el campo militar como complemento de las acciones militares propias, en el marco de búsqueda de información para la producción de inteligencia.

Huamán Baltazar (2021), en su tesis titulada "Análisis de las capacidades en ciberseguridad y ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército, Lima, 2020", se realizó un análisis exhaustivo de las competencias de ciberseguridad y ciberdefensa del mencionado lugar, con el objetivo de describir y explicar cómo estas capacidades preservan la credibilidad, integridad y la accesibilidad de la información en la Dirección de Telemática y Estadística del Ejército. La investigación, presentada en la Escuela Superior de Guerra del Ejército, utilizó una metodología cualitativa basada en el análisis hermenéutico de documentos, complementada con entrevistas y observación para recabar información pertinente. Los resultados indicaron que, aunque las capacidades de ciberseguridad y ciberdefensa otorgan apoyo a los comandos del Ejército, aún están en proceso de implementación y no son completamente específicas. Se destaca el empleo de programas exentos de licencia para resguardar la información.

En conclusión, la implementación de tecnologías de la información en unidades militares en Perú enfrenta retos significativos, principalmente debido a la carencia de especificidad y desarrollo completo de las capacidades de ciberseguridad y ciberdefensa. Este panorama subraya la necesidad de continuar fortaleciendo estas capacidades para asegurar una protección integral de la información crítica en entornos operacionales militares, garantizando así la eficiencia y seguridad en las operaciones militares futuras.

Según Huertas (2023), en su tesis titulada “La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú – Lima 2022”, la protección de la información y la infraestructura de las TICs en entornos militares es sustancial para asegurar la eficacia de las operaciones y acciones terrestres. En este contexto, es crucial considerar la ciberdefensa como un componente fundamental en la planificación y ejecución de acciones militares, especialmente en lo referente a la variable de "Operaciones de Respuesta" en el ámbito de la ciberdefensa. Se destaca la urgencia de establecer protocolos de respuesta ante posibles ciberataques que puedan comprometer la integridad de las TICs utilizadas en operaciones militares. Estos protocolos deben incluir medidas proactivas para detectar, prevenir y neutralizar amenazas cibernéticas, así como estrategias de recuperación y de servicio ininterrumpido en caso de incidentes de seguridad informática. Asimismo, se sugiere la implementación de sistemas de vigilancia y acción preventiva para identificar anomalías en la red y responder de manera rápida y eficaz ante posibles brechas de seguridad que puedan afectar el funcionamiento de las TICs durante operaciones y acciones terrestres. Estas acciones son fundamentales para respaldar la disposición, privacidad e integridad de la información en entornos militares y para mantener la ventaja operativa en un contexto analógico y sujeto a amenazas cibernéticas en evolución constante (p.46).

La implementación de TICs en el Ejército del Perú enfrenta diversos desafíos que deben ser abordados para asegurar su éxito, especialmente en el contexto de la 3ra Brigada Blindada de Moquegua en 2025. Según Quinto Huamán y Picón Huacarpuma (2023), uno de los

principales retos es la infraestructura tecnológica, ya que las fuerzas armadas requieren una construcción robusta que soporte el almacenamiento y procesamiento de datos en gran dimensión, aspecto relevante para la eficiencia de las operaciones militares. Además, la formación continua y especializada del personal militar es indispensable para el manejo adecuado de estas tecnologías y para enfrentar amenazas cibernéticas, lo que incluye no solo conocimientos técnicos, sino también la capacidad de respuesta ante situaciones críticas. La interoperabilidad de los sistemas existentes con nuevas plataformas tecnológicas es otro desafío significativo, siendo fundamental para asegurar un flujo de información sin interrupciones entre diferentes unidades y plataformas, lo cual es vital para las operaciones unificadas. Finalmente, la seguridad y privacidad de los datos son preocupaciones constantes, ya que las operaciones militares generan datos sensibles que deben ser protegidos contra ciberataques mediante la implementación de protocolos de seguridad robustos y prácticas avanzadas de ciberseguridad (Quinto Huamán & Picón Huacarpuma, 2023, pp. 8-11).

Vicaña y Chafloque (2021) examinan en su investigación aspectos teóricos y tecnológicos cruciales, centrándose en el "Sistema de Comando y Control (C2)". Este sistema es esencial para los jefes militares en la toma de decisiones, ya que integra diversos elementos como centros de comando, subsistemas de información, sensores, equipos y medios de comunicación (p.16). Su principal propósito fue proporcionar una visión clara y actualizada del estado de las unidades desplegadas en el área de operaciones. Comprender este sistema es vital para enfrentar los desafíos de implementar TICs en la 3ra Brigada Blindada, ya que un funcionamiento eficiente del sistema de comando y control es fundamental para la toma de decisiones y el control eficaz de las fuerzas durante las operaciones y acciones terrestres unificadas.

2.1.2. Antecedentes Internacionales

Saltos Narváez (2021), en su tesis de maestría "Análisis de las nuevas tecnologías en las TICs y el mando y control (oportunidades y amenazas)", profundiza en los fundamentos del mando y control del ejército ecuatoriano y en el análisis de las falencias del sistema de

comunicaciones por la obsolescencia tecnológica, incompatibilidad de plataformas digitales y herramientas, falta de capacitación tecnológica en pro de los requerimientos actuales en el área de las telecomunicaciones. Según el autor, es necesario la permanente actualización tecnológica de las TICs en la capacidad de mando y control, toda vez que contempla una significativa envergadura en la toma de decisiones, planificación con las demás capacidades militares dentro del sistema de defensa del país. En este sentido, el autor considera que este aspecto reviste particular relevancia para analizar los posibles desafíos y problemas que pueden presentarse en la implementación adecuada de las TICs dentro de las operaciones y acciones terrestres unificadas. Esto se debe a que el correcto despliegue y aprovechamiento de las TICs obedecerá en gran medida a la capacidad del sistema de comando y control para procesar, transmitir y compartir información vital en tiempo real, lo cual constituye un elemento crítico para el éxito de las operaciones militares en el terreno.

Montes Vallejo (2022), en su artículo científico titulado “Inteligencia artificial y el aprendizaje automático en la ciberseguridad “ destaca la relevancia de integrar tecnologías avanzadas, como la inteligencia artificial (IA), el aprendizaje automático y la ciberseguridad, para mejorar las capacidades defensivas y operacionales en el ámbito militar. Estas tecnologías no solo permiten optimizar las operaciones en tiempo real, sino que también contribuyen a reducir la brecha tecnológica y ofrecer ventajas estratégicas clave. En este sentido, subraya la necesidad de sistematizar la innovación tecnológica para alinearla con las capacidades nacionales y asegurar el éxito en las operaciones militares. Esta perspectiva es especialmente relevante para la investigación de maestría sobre los desafíos en la implementación de TICs durante las operaciones y acciones terrestres de la 3ra Brigada Blindada, donde la integración de estas tecnologías emergentes con las capacidades locales es crucial para optimizar los resultados operacionales y estratégicos, mejorando la efectividad en la toma de decisiones y el rendimiento de las operaciones (Montes Vallejo, 2022, p. 25).

Villarrubia (2021), en su tesis de maestría titulada "Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la región Lima", argumenta que las tecnologías emergentes como el 5G tienen el potencial de transformar significativamente las operaciones tácticas y estratégicas en las unidades militares. Esta tecnología avanzada ofrece comunicaciones seguras y encriptadas, gracias a su alta velocidad y baja latencia, lo que es crucial para la coordinación efectiva en tiempo real. Además, el 5G facilita la integración de múltiples dispositivos y sistemas de información, optimizando la toma de decisiones y el funcionamiento de las unidades. Sin embargo, la implementación de esta tecnología presenta desafíos importantes, particularmente en términos de ciberseguridad. Villarrubia destaca que los riesgos asociados con la protección de la información digital en las Fuerzas Armadas requieren medidas preventivas y proactivas, como la encriptación de datos y la detección temprana de amenazas. La cooperación entre los sectores público y privado es esencial para desarrollar soluciones innovadoras que maximicen las capacidades del 5G en el ámbito de la defensa y la seguridad (Villarrubia, 2021, p. 45).

Casale (2022), en su tesis de maestría titulada “La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el nivel operacional”, la rápida evolución tecnológica ha dado lugar a la aparición del ciberespacio como un nuevo dominio transversal que afecta significativamente las operaciones militares. El documento subraya la importancia de establecer procesos y organizaciones específicas para llevar a cabo operaciones de ciberdefensa en el Componente Terrestre del Teatro de Operaciones, debido a la falta de una doctrina rectora sobre este tema en el ámbito táctico. La ciberdefensa se ha transformado en un elemento decisivo para el éxito de las operaciones militares, ya que protege las infraestructuras críticas y asegura el desarrollo continuo de las operaciones en caso de ciberataques. El autor también enfatiza la necesidad de adaptar el marco legal para facilitar el desarrollo de operaciones ofensivas y defensivas en el ciberespacio. Esto incluye la creación de capacidades tecnológicas avanzadas y la formación de personal especializado en ciberseguridad, así como la cooperación

internacional para enfrentar las amenazas globales en el ciberespacio. La incorporación de la ciberdefensa en la planificación y ejecución de operaciones militares es vital para preservar la seguridad y operatividad de los institutos armados en el entorno digital actual (Casale, 2022, pp. 50-51).

Ravera (2024), en su tesis de maestría titulada “El rol y las capacidades cibernéticas de las Fuerzas Armadas de la República Argentina en el marco de los conflictos futuros”, se centra en la conservación de redes, sistemas e infraestructuras cruciales del país contra amenazas y ataques cibernéticos destaca la importancia de salvaguardar redes y sistemas esenciales contra amenazas cibernéticas. En este contexto, se subraya la creación de entidades como el Comité de Infraestructuras Críticas de la Defensa, que tiene como objetivo la protección de los activos digitales que soportan el sistema de defensa nacional. Además, se menciona el rol de la coordinación centralizada a través de políticas de ciberdefensa que optimizan la respuesta ante incidentes. Este enfoque es especialmente relevante para la investigación sobre la implementación de tecnologías de la información y comunicación (TICs) en operaciones militares, como es el caso de la 3ra Brigada Blindada, ya que estas estrategias son clave para asegurar la continuidad de las operaciones y proteger las infraestructuras críticas de las amenazas cibernéticas emergentes (Ravera, 2024, p. 112).

Matiz y Fernández (2023), en su investigación titulada "Del uso de la inteligencia artificial como medio y método en los conflictos armados", analizan cómo las tecnologías emergentes, como la inteligencia artificial (IA), se están utilizando en los conflictos armados para mejorar la eficiencia y precisión de las operaciones militares. Los autores destacan que la IA no solo optimiza la toma de decisiones, sino que también puede ser crucial en la reducción de errores humanos y en el aumento de la capacidad de respuesta ante situaciones críticas. Sin embargo, también subrayan los desafíos éticos, legales y operacionales que surgen con la integración de estas tecnologías, especialmente en lo relacionado con la autonomía de los sistemas y la protección de datos sensibles. Este análisis es particularmente relevante para la 3ra Brigada

Blindada de Moquegua, ya que la implementación de TICs en sus operaciones debe abordar estas cuestiones éticas y legales para garantizar su uso responsable y eficiente, respetando las normativas nacionales e internacionales. (Matiz y Fernández, 2023, pp. 45-52).

Alcántara (2023) en su investigación de tipo básica sobre “Análisis de la aplicación de ML en sistemas de defensa”, destaca el valor de la innovación tecnológica en el campo militar para acrecentar las competencias, la toma de decisiones y la seguridad en las operaciones. La integración de tecnologías avanzadas como el machine learning en unidades militares puede proporcionar grandes ventajas estratégicas significativas, pero es fundamental abordar de manera integral aspectos éticos, legales y de seguridad para garantizar un uso responsable y efectivo de estas herramientas en el contexto nacional. El autor empleó la técnica de recolección de datos en base a la búsqueda y recopilación de información de proyectos recientes financiados por el Ministerio de Defensa de España, además se identificaron ventajas en la aplicación del machine learning en sistemas de defensa, analizando la evolución de este y se estudiaron los casos de uso en operaciones tácticas. Este enfoque es relevante para nuestro estudio de investigación ya que basándonos en la información recopilada sobre el utilidad del Machine Learning (ML) en sistemas de defensa, se puede concluir que la implementación de TICs en unidades militares del sector defensa pueden ofrecer ventajas significativas en términos de eficiencia, precisión y capacidad operativa.

2.2. Bases Teóricas

2.2.1. Teorías empleadas

2.2.1.1 Modelo de aceptación de tecnología (TAM).

Propuesto por Davis (1989), es fundamental para comprender cómo los usuarios adoptan nuevas tecnologías. En el ámbito militar, este modelo resulta útil para explicar cómo los soldados y comandantes pueden estar dispuestos a utilizar sistemas tecnológicos avanzados, tales como redes de comunicación, sistemas de mando y control, y plataformas de inteligencia artificial. Según Davis, la aceptación de una tecnología depende principalmente de dos factores clave: la

utilidad percibida y la facilidad de uso percibida. En el caso de las fuerzas armadas, si los miembros perciben que una nueva tecnología les permitirá realizar sus tareas de manera más eficiente o efectiva, es más probable que la adopten. Sin embargo, si consideran que la tecnología es compleja o difícil de usar, podrían resistirse a su implementación. Este fenómeno es particularmente relevante cuando se integran plataformas de comunicación y sistemas de inteligencia, como el Sistema de Comando y Control (C2), que permite a los oficiales tomar decisiones informadas basadas en datos en tiempo real. La percepción de la utilidad y la facilidad con la que se integra la tecnología en las operaciones cotidianas puede ser un factor determinante para su aceptación.

2.2.1.2 Teoría de la resistencia al cambio

Presentada por Dent y Goldberg (1999), señala que la resistencia al cambio es un fenómeno común cuando se introducen nuevas tecnologías en cualquier organización, y las fuerzas armadas no son la excepción. Esta resistencia puede manifestarse de diversas maneras, como la reticencia a aprender nuevas habilidades, la desconfianza en la efectividad de la tecnología, o la preferencia por métodos tradicionales. En el contexto militar, la resistencia al cambio es especialmente significativa debido a la estructura jerárquica de las fuerzas armadas y su fuerte enfoque en la disciplina y la rutina. La introducción de nuevas tecnologías, como los sistemas automatizados de mando y control, puede generar resistencia, ya que muchos oficiales y soldados prefieren métodos tradicionales con los que se sienten cómodos y que conocen bien. Además, existe el temor de que la adopción de estas tecnologías pueda reducir el control humano sobre las decisiones operativas o incluso que se vea reemplazado por las máquinas, lo que aumenta la resistencia a su integración.

2.2.1.3 Teoría de la gestión del cambio de Kotter (1996)

Este enfoque proporciona un marco estructurado para gestionar de manera efectiva los procesos de cambio en las organizaciones. El modelo propuesto incluye ocho pasos fundamentales, como la creación de un sentido de urgencia, la formación de una coalición de

poder, el desarrollo de una visión clara para el cambio y la consolidación de los logros mediante la integración de nuevas prácticas. En el ámbito militar, la implementación de Tecnologías de la Información y Comunicación (TICs) no solo implica la incorporación de herramientas tecnológicas avanzadas, sino también la necesidad de llevar a cabo una gestión del cambio organizacional adecuada para garantizar una transición exitosa. La adopción de tecnologías innovadoras, tales como redes de comunicaciones seguras o el uso de inteligencia artificial en la toma de decisiones, debe ir acompañada de un proceso que aborde las barreras culturales, las preocupaciones sobre la seguridad y la capacitación de los usuarios finales. Para asegurar que el cambio sea sostenible y efectivo a largo plazo, es esencial que los líderes militares sigan los pasos propuestos por Kotter, con el fin de garantizar una adopción exitosa de estas nuevas tecnologías.

En relación con la adopción de innovaciones dentro de las fuerzas armadas, la Teoría de la Difusión de Innovaciones de Rogers (2003) describe cómo una innovación se propaga a través de una comunidad o sociedad. Rogers identifica varias etapas en este proceso: conocimiento, persuasión, decisión, implementación y confirmación. La adopción de TICs en el ámbito militar se puede observar a través de este ciclo, comenzando con la exploración de nuevas tecnologías hasta su completa implementación en las operaciones militares. Un ejemplo claro de esto es la integración de tecnologías de guerra en red o sistemas avanzados de mando y control, los cuales permiten la integración de datos en tiempo real para mejorar la toma de decisiones en el campo de batalla. La rapidez con que estas innovaciones se difunden depende de varios factores, como la efectividad de la tecnología, la formación de los usuarios y la percepción de la utilidad de estas innovaciones.

2.2.1.4 Modelo de Capacidades Dinámicas

Propuesto por Teece et al. (1997), sugieren que las organizaciones deben ser capaces de adaptarse rápidamente a los cambios del entorno y aprovechar las oportunidades tecnológicas para mantenerse competitivas. En el contexto militar, esto implica que las fuerzas armadas deben integrar y adaptar nuevas tecnologías, como los sistemas TIC, para mejorar su capacidad operativa y estratégica. La adopción de TICs permite el desarrollo de capacidades operacionales dinámicas, lo que posibilita que las fuerzas armadas respondan rápidamente a amenazas emergentes, como ciberataques o guerra electrónica. Gracias a la flexibilidad y agilidad proporcionadas por las TICs, las fuerzas armadas pueden reaccionar de manera eficiente ante situaciones cambiantes en el campo de batalla.

2.2.1.5 Teoría de la Motivación y Expectativa de Vroom (1964)

Establece que las personas toman decisiones basadas en la expectativa de que sus esfuerzos resultarán en una recompensa deseada. En el caso de las TICs en las fuerzas armadas, los miembros de las fuerzas armadas pueden estar motivados a adoptar y proteger estas tecnologías si consideran que sus esfuerzos les traerán beneficios, como la mejora de la seguridad operativa o el éxito en sus misiones. Para garantizar la protección de los sistemas TIC, es fundamental que las fuerzas armadas promuevan la motivación de sus miembros mediante la capacitación en ciberseguridad y la adopción de medidas de seguridad que aseguren la infraestructura tecnológica.

2.2.2. Categoría 1: Desafíos en la implementación de TICs

La implementación de las Tecnologías de la Información y la Comunicación (TICs) en operaciones militares de tipo terrestre, como en las acciones unificadas de la 3ra Brigada Blindada de Moquegua, enfrenta varios desafíos que van desde problemas de infraestructura hasta aspectos organizacionales y humanos. La integración de tecnologías avanzadas como sistemas de comando y control (C2), comunicaciones seguras e inteligencia artificial en escenarios complejos de operaciones militares tiene implicaciones significativas en la efectividad

de las misiones. Sin embargo, estos avances se ven obstaculizados por factores técnicos, humanos y logísticos que requieren un análisis profundo.

Estos desafíos son abordados desde diversas teorías que permiten comprender cómo las fuerzas armadas pueden superar estos obstáculos. Por ejemplo, la Teoría de la Aceptación de Tecnología (Davis, 1989) explica cómo la percepción de los usuarios sobre la utilidad y facilidad de uso de las TICs impacta en su adopción exitosa. La Teoría de la Gestión del Cambio (Kotter, 1996) se aplica para entender cómo los procesos de transformación cultural y organizativa son fundamentales para el éxito de la implementación tecnológica. Estas teorías indican que los retos no son independientes, sino que se interrelacionan, lo que requiere una visión integral que aborde los desafíos técnicos, culturales/organizacionales y de seguridad cibernética de manera conjunta.

En las zonas rurales y terrenos difíciles de Moquegua, la infraestructura tecnológica necesaria para implementar TICs no siempre está disponible. La falta de conectividad en tiempo real, como la baja cobertura de redes móviles o la escasa infraestructura satelital, representa un obstáculo para la implementación de soluciones de comunicación continua entre las unidades militares en el terreno (Muñoz, 2021). A pesar de los avances en comunicaciones móviles y redes de fibra óptica, las áreas más alejadas presentan desafíos logísticos para garantizar que los sistemas de comando y control (C2) puedan mantenerse operativos.

El uso de tecnologías alternas, como comunicaciones satelitales y drones de comunicaciones, puede paliar esta falta de infraestructura convencional. Según Muñoz (2021), la implementación de redes de malla y tecnologías autónomas de comunicación es esencial en estas áreas para mantener la interoperabilidad entre las unidades desplegadas. Estas soluciones requieren una inversión en equipos de alta tecnología y personal capacitado para su uso y mantenimiento, lo que representa un desafío logístico adicional (Muñoz, 2021, p. 211).

Un desafío clave para la implementación de las TICs en las fuerzas armadas es la resistencia al cambio por parte de los integrantes del ejército. Martínez (2020) resalta que las fuerzas armadas, que tradicionalmente operan bajo estructuras jerárquicas y procedimientos

establecidos, pueden enfrentar dificultades para adaptarse a los avances tecnológicos. La mentalidad tradicionalista dentro de las instituciones militares, sumada a la falta de formación en TICs, puede generar barreras psicológicas y culturales que dificultan la integración de nuevas tecnologías.

Una gestión del cambio efectiva, que involucre no solo la capacitación técnica del personal, sino también el desarrollo de una cultura organizacional digital es crucial para superar estas barreras. Fernández (2020) propone que se debe fomentar una mentalidad abierta y una mentalidad digital entre los oficiales y soldados, lo cual puede lograrse mediante el uso de simuladores avanzados y entrenamientos prácticos que permitan familiarizar a los soldados con las herramientas tecnológicas en escenarios controlados (Fernández, 2020, p. 189).

La ciberseguridad es uno de los mayores retos al implementar TICs en el ámbito militar. En operaciones y acciones terrestres, la protección de los datos transmitidos entre unidades y el centro de comando es crucial, ya que cualquier vulnerabilidad podría comprometer la seguridad de la misión. Según López (2019), las amenazas cibernéticas pueden comprometer los sistemas de comunicación, afectando la efectividad de las decisiones estratégicas y operacionales. Ataques informáticos como el phishing o el ransomware pueden destruir bases de datos cruciales o interrumpir la comunicación entre unidades. La necesidad de infraestructuras de ciberseguridad robustas para proteger las redes de información es vital (López, 2019, p. 142).

Para contrarrestar estos riesgos, las fuerzas armadas deben implementar protocolos de seguridad cibernética como el uso de criptografía avanzada, sistemas de autenticación multifactorial y cortafuegos especializados que protejan tanto las comunicaciones de campo como las bases de datos sensibles. González (2020) sostiene que las tecnologías emergentes en el campo de la ciberdefensa deben ser continuamente actualizadas para hacer frente a nuevas amenazas, lo cual requiere de un entrenamiento constante para el personal de seguridad cibernética en el ámbito militar (González, 2020, p. 210).

La implementación de TICs en las fuerzas armadas implica superar barreras tecnológicas, culturales y de seguridad. Entre los desafíos técnicos, las dificultades para integrar sistemas nuevos con los existentes, la gestión de datos y las preocupaciones por la seguridad cibernética son cruciales. En el entorno organizacional, la resistencia cultural y la falta de una capacitación adecuada representan barreras importantes. Además, la seguridad operativa y la protección de la información constituyen desafíos continuos durante la implementación de estas tecnologías. Estos retos se abordan en tres áreas principales: los aspectos técnicos, que incluyen la integración de nuevos sistemas y la gestión de datos; los desafíos organizacionales y culturales, que impactan la adopción y el uso de las TICs en las instituciones militares; y los problemas de seguridad cibernética, que son esenciales para resguardar la información confidencial y asegurar el funcionamiento seguro de las operaciones.

2.2.2.1 Subcategoría 1: Implementación Técnica

La implementación técnica de las TICs en las fuerzas armadas implica superar desafíos sustanciales, como la integración de nuevas tecnologías con los sistemas existentes, la interoperabilidad entre plataformas tecnológicas heterogéneas y la gestión de la infraestructura tecnológica en ambientes de alta exigencia operativa. La transición hacia plataformas avanzadas como la computación en la nube, inteligencia artificial, big data y redes 5G es compleja, especialmente cuando se integran en sistemas militares antiguos que han sido diseñados con arquitecturas y protocolos distintos. Estos sistemas heredados a menudo no son compatibles con las nuevas soluciones tecnológicas, lo que puede generar fallos en la conectividad, demoras operacionales o incluso fallos en la comunicación crítica.

Además, la interoperabilidad de los sistemas es crucial, ya que las fuerzas armadas operan en un entorno conjunto con otras entidades, ya sean nacionales o internacionales. Las diferencias en los protocolos, plataformas y lenguajes de comunicación dificultan la fluidez de la información, creando brechas que pueden comprometer la eficacia de las misiones. Por ejemplo, el uso de sistemas de comando y control avanzados que requieren la integración de datos de

múltiples fuentes, como sensores ena el campo de batalla, satélites y comunicaciones entre unidades, puede verse obstaculizado si los sistemas no están diseñados para trabajar juntos de manera eficiente.

En este contexto, las capacidades dinámicas de las fuerzas armadas, tal como lo plantean Teece et al. (1997) en su teoría, son esenciales para gestionar y reconfigurar rápidamente los sistemas existentes. Las fuerzas armadas deben desarrollar la capacidad de adaptar sus infraestructuras a medida que surgen nuevas tecnologías sin interrumpir la operativa, lo cual se logra mediante un enfoque flexible y de aprendizaje continuo. La teoría de la aceptación de tecnología de Davis (1989) también es relevante aquí, ya que sugiere que la utilidad percibida de las TICs por parte de los usuarios, así como su facilidad de uso percibida, son determinantes clave para asegurar que la integración técnica sea exitosa. Si los oficiales y el personal técnico no perciben que las nuevas herramientas aumentan su eficacia o son fáciles de usar, la implementación puede fallar.

Finalmente, la teoría de la gestión del cambio de Kotter (1996) es fundamental para gestionar la transición tecnológica en las fuerzas armadas. La adopción de nuevas tecnologías no solo depende de la infraestructura técnica, sino de cómo los cambios son gestionados a nivel organizativo. Según Kotter, la implementación exitosa de tecnologías requiere primero la creación de un sentido de urgencia sobre la necesidad del cambio, seguido por la formación de una coalición de apoyo, que en este caso podría ser representada por líderes de diversas ramas militares. De este modo, la implementación técnica de las TICs en las fuerzas armadas no solo depende de la infraestructura, sino también de un proceso estructurado de gestión del cambio que garantice la aceptación y el uso efectivo de las tecnologías por parte de todos los actores involucrados.

2.2.2.2 Subcategoría 2: Cultural Organizativa

La cultura organizativa y la resistencia al cambio son factores decisivos en la implementación de TICs en el ámbito militar. Las fuerzas armadas, debido a su estructura jerárquica y de alta disciplina, suelen ser muy reacias a adoptar nuevas tecnologías, especialmente si estas implican una alteración de las rutinas o del poder centralizado de toma de decisiones. La resistencia al cambio es un fenómeno psicológico que ocurre cuando los miembros de una organización, ya sea por miedo a lo desconocido, por la percepción de que las nuevas tecnologías son innecesarias o por la falta de formación adecuada, se muestran reticentes a incorporar nuevas herramientas en su trabajo diario.

En el caso de las fuerzas armadas, este desafío es particularmente marcado, ya que los militares están acostumbrados a seguir protocolos establecidos, y la adopción de tecnologías digitales puede percibirse como una amenaza a la autonomía o a los métodos tradicionales de mando. La Teoría de la Resistencia al Cambio de Dent y Goldberg (1999) ilustra cómo los individuos y grupos dentro de las organizaciones reaccionan ante la introducción de innovaciones que alteran sus estructuras de poder y operaciones. Este tipo de resistencia puede manifestarse de diversas formas, como la desconfianza hacia las tecnologías nuevas, el temor a la pérdida de control y la dificultad para adaptarse a nuevas formas de trabajo. Las fuerzas armadas deben enfrentar este tipo de resistencia implementando un proceso claro de gestión del cambio, donde se destaquen los beneficios tangibles de las TICs, como el aumento de la eficiencia operativa y la mejora en la toma de decisiones.

Además, la Teoría de la Gestión del Cambio de Kotter (1996) subraya la necesidad de un enfoque estructurado para superar la resistencia. La creación de una coalición de líderes que apoyen la implementación tecnológica y la capacitación adecuada son aspectos esenciales para vencer las barreras culturales y organizativas. Kotter señala que el cambio debe ser liderado desde la cima, lo que implica el compromiso de los altos mandos para promover el cambio como parte de la cultura organizativa, lo que contribuiría a reducir la resistencia interna.

En este contexto, también se puede aplicar la Teoría de la Motivación y Expectativa de Vroom (1964). Esta teoría propone que las personas se motivan a realizar ciertas acciones en función de las expectativas sobre los resultados de sus esfuerzos. En el caso de las TICs, si los miembros del personal militar creen que la adopción de las nuevas tecnologías aumentará sus posibilidades de éxito o les facilitará sus tareas, estarán más dispuestos a aceptarlas y adoptarlas, lo cual resulta fundamental para la implementación efectiva en un entorno tan jerárquico y estructurado como el militar.

2.2.2.3 Subcategoría 3: Seguridad cibernética

La seguridad cibernética es uno de los aspectos más críticos en la implementación de TICs dentro de las fuerzas armadas A medida que las fuerzas armadas dependen en mayor medida de la infraestructura tecnológica para coordinar operaciones y manejar datos sensibles, aumentan los riesgos relacionados con los ciberataques, la filtración de información clasificada y los fallos en las redes de comunicación. Las amenazas cibernéticas, tanto internas como externas, pueden poner en peligro la seguridad operativa y la integridad de las misiones, lo que convierte la protección de los sistemas de información en una prioridad crucial.

En este sentido, la teoría de cibernética de Wiener (1948) juega un papel fundamental, ya que destaca la importancia de controlar y supervisar los sistemas de información en entornos complejos, como los de las fuerzas armadas. Según Wiener, los sistemas cibernéticos deben ser diseñados de manera que no solo permitan un flujo de información eficiente, sino que también cuenten con mecanismos de retroalimentación y autocorrección para identificar y mitigar posibles vulnerabilidades. En el caso de las fuerzas armadas, esto implica la implementación de protocolos de seguridad robustos que incluyan desde la encriptación de datos hasta la creación de sistemas de detección de intrusos para prevenir ataques cibernéticos y fallos en los sistemas críticos.

La Teoría de la Aceptación de Tecnología de Davis (1989) también es relevante en este contexto, ya que la seguridad cibernética solo será adoptada y aplicada de manera efectiva si los

miembros del personal militar consideran que las tecnologías de protección son útiles y fáciles de usar. Si los sistemas de seguridad son percibidos como demasiado complejos o ineficientes, los usuarios pueden ser reacios a utilizarlos correctamente, lo que aumenta el riesgo de brechas de seguridad.

Además, la Teoría de la Motivación y Expectativa de Vroom (1964) se puede aplicar para explicar cómo la motivación de los oficiales y el personal técnico influye en la adopción de medidas de seguridad cibernética. Si los miembros del personal consideran que la protección de los sistemas tecnológicos les permitirá evitar riesgos graves para las operaciones, estarán más motivados para cumplir con los protocolos de seguridad, lo que ayudará a reducir las amenazas cibernéticas.

2.2.3. Categoría 2: Impacto de las TICs en operaciones y acciones terrestres.

El impacto de las Tecnologías de la Información y Comunicación (TICs) en las operaciones y acciones terrestres unificadas se refiere a la transformación radical que estas tecnologías han traído a la naturaleza de las operaciones militares en contextos tanto nacionales como multinacionales. En el caso de la 3ra Brigada Blindada de Moquegua, las TICs son herramientas esenciales para lograr una mayor eficiencia operativa, interoperabilidad entre las distintas unidades y plataformas, y una adaptación continua a los avances tecnológicos en un entorno de alta incertidumbre y dinamismo estratégico.

A través de herramientas avanzadas como los sistemas de comando y control, comunicaciones seguras, y el análisis predictivo, las TICs mejoran la capacidad de los comandantes para tomar decisiones informadas y rápidas, lo que optimiza la gestión de recursos, la coordinación entre unidades dispersas y la seguridad de las tropas en escenarios de combate. Este cambio en las operaciones militares redefine las tácticas, la logística y la respuesta a las amenazas, configurando un entorno más flexible y eficiente en el que los soldados, comandantes y otras unidades están interconectados y sincronizados de forma casi instantánea.

La eficiencia operativa es uno de los pilares más destacados de la implementación de TICs en las operaciones militares. Las TICs permiten que las unidades militares obtengan información crítica en tiempo real, lo que a su vez facilita la toma de decisiones rápidas y precisas, especialmente en escenarios de combate dinámicos donde la capacidad de adaptación es crucial. La adopción de tecnologías como Big Data, GIS (Sistemas de Información Geográfica) y sistemas avanzados de comando y control (C2) ha transformado la forma en que los comandantes supervisan el campo de batalla y toman decisiones operativas.

De acuerdo con Ramos (2020), las TICs proporcionan a los comandantes una visión clara y detallada del terreno, la situación táctica y las posiciones de las tropas aliadas y enemigas. Esta información geoespacial precisa no solo mejora la eficacia en la toma de decisiones, sino que también optimiza la distribución de recursos y las maniobras tácticas. Además, la capacidad de analizar grandes volúmenes de datos en tiempo real permite una respuesta más rápida ante cambios inesperados en el campo de batalla (Ramos, 2020, p. 256). Este proceso de optimización en el contexto de las operaciones de la 3ra Brigada Blindada se encuentra alineado con el Modelo de Capacidades Dinámicas de Teece et al. (1997), que resalta la importancia de adaptarse rápidamente a cambios en el entorno operativo mediante la reconfiguración de los sistemas y la asignación eficiente de recursos. La capacidad para reaccionar y ajustar las tácticas sobre la marcha es crucial para mantener la eficiencia operativa en situaciones de alta presión y alta complejidad.

El Modelo de Capacidades Dinámicas aplicado a las operaciones y acciones terrestres unificadas de la brigada señala que la adaptación continua de las TICs y su integración con los sistemas existentes permite una mejor planificación y ejecución de las misiones militares, reduciendo el tiempo de respuesta y aumentando la efectividad de las fuerzas en el terreno. Esta capacidad de adaptación y reconfiguración también se debe a las plataformas de comunicación y control que garantizan una conexión constante y en tiempo real entre las unidades, lo que facilita la ejecución de maniobras sincronizadas en el contexto de operaciones conjuntas.

La interoperabilidad es otro de los aspectos clave en la implementación de TICs en las operaciones y acciones terrestres unificadas, especialmente en contextos multinacionales o cuando se operan unidades de diversas ramas de las fuerzas armadas. Se refiere a la capacidad de diferentes sistemas, plataformas y tecnologías (que pueden usar diferentes protocolos, arquitecturas y equipos) de trabajar juntos de forma efectiva y sincronizada. Este desafío es particularmente importante para la 3ra Brigada Blindada, dado que las operaciones unificadas a menudo involucran fuerzas aliadas, que operan con sistemas y tecnologías diversas.

El uso de plataformas avanzadas de comando y control facilita la integración de diversas unidades y el intercambio de información a través de diferentes sistemas, desde vehículos blindados hasta sistemas de defensa aérea. Según Martínez (2019), la interoperabilidad de las TICs permite una coordinación más eficiente entre los diferentes componentes del teatro de operaciones. Las unidades de diferentes orígenes deben poder compartir información sin barreras tecnológicas, lo que a su vez reduce la probabilidad de errores tácticos y mejora la sincronización de las maniobras conjuntas (Martínez, 2019, p. 145).

El desafío de la interoperabilidad está también vinculado a los diferentes estándares de comunicación y protocolos entre las distintas plataformas militares. En este sentido, la Teoría de la Difusión de Innovaciones de Rogers (2003) resulta aplicable, ya que explica cómo las innovaciones tecnológicas, como las TICs, se difunden a través de una organización militar y se adoptan solo cuando son compatibles con los sistemas existentes y ofrecen una ventaja operativa clara. En el caso de la 3ra Brigada Blindada, la adopción de nuevas TICs dependerá de su compatibilidad con los sistemas actuales y de la capacitación continua de las tropas para garantizar su uso efectivo en un entorno multinacional y multitecnológico.

La Teoría de Gestión del Cambio de Kotter (1996) también es relevante para la 3ra Brigada Blindada al enfrentar el desafío de la adopción de nuevas TICs. Esta teoría resalta la necesidad de un enfoque estructurado para la gestión del cambio organizacional y cultural, lo que garantiza que los cambios tecnológicos en las plataformas de comunicación y los sistemas

de control sean bien recibidos y eficazmente implementados por todas las unidades involucradas en las operaciones y acciones militares.

La adaptación a la innovación tecnológica es un proceso crucial para las fuerzas armadas, ya que las TICs están en constante evolución y requieren una incorporación continua de nuevas tecnologías para mantenerse competitivas en el campo de batalla. Este proceso implica no solo la adopción de nuevas plataformas tecnológicas, como drones, sensores inteligentes, y sistemas de ciberseguridad avanzada, sino también una transformación en las estrategias operativas, tácticas de combate y en la planificación de las misiones. La rápida adaptación a estas tecnologías tiene un impacto directo en la capacidad operativa y la resiliencia de la brigada frente a nuevas amenazas.

La Teoría de la Difusión de Innovaciones de Rogers (2003) se utiliza para entender cómo las nuevas tecnologías se adoptan gradualmente dentro de la 3ra Brigada Blindada. Rogers explica que las innovaciones son adoptadas inicialmente por los líderes de opinión (en este caso, los comandantes de alto rango) y luego se difunden a las unidades más operativas. La aceptación de nuevas TICs depende de su compatibilidad con las necesidades operativas y la percepción de que estas tecnologías mejorarán la capacidad de las tropas para llevar a cabo sus misiones con éxito.

Por otro lado, el Modelo de Capacidades Dinámicas de Teece et al. (1997) resalta que, para ser efectivas, las fuerzas armadas deben ser capaces de adaptarse y reconfigurarse rápidamente para aprovechar las nuevas tecnologías. En este contexto, la 3ra Brigada Blindada necesita desarrollar capacidades dinámicas que le permitan reconfigurar su estructura, recursos y estrategias de forma ágil y continua para adaptarse a las tecnologías emergentes.

Finalmente, la Teoría de la Motivación y Expectativa de Vroom (1964) también es útil para entender cómo los miembros de la brigada adoptan nuevas tecnologías. Vroom argumenta que la motivación para adoptar TICs dependerá de la percepción de que estas tecnologías mejorarán las probabilidades de éxito en las misiones. Si los miembros de la 3ra Brigada Blindada creen

que las TICs les permitirán ser más eficaces y seguros durante las operaciones, estarán más dispuestos a adaptarse y adoptar nuevas tecnologías.

La implementación de las TICs en las operaciones y acciones terrestres unificadas de la 3ra Brigada Blindada de Moquegua mejora la eficiencia operativa, la interoperabilidad y la adaptación a nuevas tecnologías, a pesar de los desafíos en infraestructura, capacitación y seguridad cibernética. Las teorías de cambio y difusión de innovaciones proporcionan un marco para superar estos obstáculos, optimizando la toma de decisiones, la coordinación y la seguridad de las tropas, fortaleciendo así la capacidad operativa de la brigada en escenarios complejos.

2.2.2.1 Subcategoría 1: Eficiencia operativa

La eficiencia operativa en las operaciones y acciones terrestres militares se ve fuertemente influenciada por las Tecnologías de la Información y Comunicaciones (TICs), que permiten mejorar la toma de decisiones, la coordinación entre unidades y la ejecución de misiones en tiempo real. El uso de sistemas avanzados de comando y control (C2), que integran información de múltiples fuentes como satélites, sensores de campo de batalla y plataformas aéreas no tripuladas, permite a los comandantes tener una visión más clara y precisa de la situación en tiempo real. Esto facilita una respuesta más rápida y una mejor asignación de recursos durante las operaciones militares, lo que resulta en una mayor eficiencia al reducir tiempos de reacción y optimizar la asignación de fuerzas en el terreno.

La Teoría de la Difusión de Innovaciones de Rogers (2003) es muy relevante en este contexto. Rogers explica cómo las innovaciones se difunden a través de una población y cómo su adopción depende de factores como la ventaja relativa de la nueva tecnología (en este caso, las TICs), su compatibilidad con los valores y prácticas existentes, y la facilidad de uso percibida. En las fuerzas armadas, la adopción de tecnologías que mejoran la eficiencia operativa depende en gran medida de su capacidad para integrarse sin problemas con los sistemas existentes y de la formación continua para asegurar que los usuarios (los militares) comprendan cómo utilizar la nueva tecnología en el contexto de sus misiones.

A su vez, el Modelo de Capacidades Dinámicas de Teece et al. (1997) también se aplica aquí, ya que resalta la importancia de las organizaciones para adaptarse rápidamente a cambios en el entorno operativo. Las fuerzas armadas deben desarrollar capacidades dinámicas que les permitan reconfigurar rápidamente sus sistemas de comunicación y ajustar sus operaciones para que puedan reaccionar de manera eficiente a los imprevistos del campo de batalla. Esta capacidad de adaptación a las TICs no solo aumenta la eficiencia, sino que también fortalece la resiliencia de las operaciones militares.

Las redes centradas en la información (network-centric warfare) juegan un papel fundamental en la mejora de la eficiencia operativa. Como señalan Alberts et al. (2000), el modelo de guerra centrada en redes permite la distribución de la información de manera más equitativa entre las unidades, lo que favorece la coordinación y la sincronización de las acciones en tiempo real. La capacidad de compartir datos entre fuerzas de diferentes ramas y países en operaciones multinacionales puede reducir significativamente los tiempos de toma de decisiones, lo que a su vez mejora la eficiencia operativa en el terreno.

2.2.2.2 Subcategoría 2: Interoperabilidad

La interoperabilidad de los sistemas TICs entre diferentes unidades militares es un factor clave para el éxito de las operaciones conjuntas, tanto dentro de un mismo país como en contextos multinacionales. La interoperabilidad se refiere a la capacidad de diferentes sistemas y plataformas (que pueden usar diferentes tecnologías y protocolos) para trabajar juntos y compartir información de manera efectiva y sin interrupciones. Este concepto es esencial cuando se operan en coaliciones internacionales, donde las fuerzas armadas deben ser capaces de integrar y coordinar unidades de diferentes países con diferentes infraestructuras tecnológicas.

El desafío de la interoperabilidad es especialmente evidente cuando los sistemas de comunicación, inteligencia y gestión de recursos no están diseñados para ser compatibles entre sí. El tecnología de la información se convierte en un eslabón crítico para la integración de

diferentes plataformas militares (por ejemplo, aviones, vehículos blindados, sistemas de defensa) y sistemas de gestión de la información en tiempo real.

La Teoría de la Difusión de Innovaciones de Rogers (2003) y el concepto de redes centradas en la información (network-centric warfare) de Alberts et al. (2000) son de gran relevancia aquí. De acuerdo con Rogers, la adopción y la difusión de tecnologías innovadoras en las fuerzas armadas dependen de su compatibilidad con las necesidades operativas existentes y con los sistemas previos en uso. Las tecnologías que se implementan deben ser fácilmente integrables con otras plataformas y además, los operadores deben ser capacitados para utilizarlas en un entorno interconectado y multifuncional.

Según Fredericks y Borenstein (2018) en su estudio sobre interoperabilidad en las fuerzas armadas indican que los desafíos técnicos (como los diferentes estándares de comunicación, protocolos de red y plataformas incompatibles) son una barrera común a la interoperabilidad. La superación de estos desafíos requiere un diseño de sistemas más abierto y flexible, así como el desarrollo de estándares internacionales que faciliten la comunicación entre plataformas diversas.

La Teoría de la Gestión del Cambio de Kotter (1996) también juega un papel clave. En el caso de las fuerzas armadas, la transición hacia sistemas interoperables requiere no solo de una reconfiguración tecnológica, sino también de un cambio organizativo y cultural. Kotter argumenta que un proceso de gestión del cambio estructurado puede facilitar la transición hacia una mayor interoperabilidad, al garantizar que todos los niveles de la organización estén comprometidos con la adopción de nuevos sistemas y protocolos.

2.2.2.3 Subcategoría 3: Adaptación a la innovación tecnológica

La adaptación a la innovación tecnológica es un proceso fundamental en las fuerzas armadas, ya que la rápida evolución de las TICs genera nuevos paradigmas operacionales y modifica la naturaleza de las misiones y las tácticas empleadas. La adopción de tecnologías avanzadas no es simplemente un cambio en los equipos o sistemas utilizados, sino también en

las estrategias operativas y la planificación táctica. Por ejemplo, el uso de drones, sensores inteligentes, sistemas de inteligencia artificial (IA) y ciberseguridad avanzada cambia completamente la forma en que se realizan las misiones de vigilancia, la toma de decisiones en tiempo real y las operaciones de combate.

El proceso de aceptación e incorporación de innovaciones puede seguirse a través del marco teórico de la Teoría de la Difusión de Innovaciones de Rogers (2003), que señala que las tecnologías innovadoras son adoptadas en un proceso gradual, empezando por los líderes de opinión dentro de la organización (en este caso, los oficiales de alto rango) y extendiéndose hacia el resto de la fuerza. Las fuerzas armadas, como organizaciones de alto rendimiento, suelen ser pioneras en la adopción de ciertas tecnologías, especialmente cuando éstas prometen mejorar la capacidad de responder rápidamente a situaciones cambiantes en el campo de batalla.

Por otro lado, el Modelo de capacidades dinámicas de Teece et al. (1997) explica que las fuerzas armadas deben desarrollar capacidades para modificar sus estructuras y estrategias rápidamente en respuesta a cambios tecnológicos. Esto incluye la reconfiguración de recursos, la formación de personal para que pueda manejar nuevas tecnologías y la capacidad de aprender rápidamente de la experiencia operativa para mejorar el uso de las TICs en el futuro.

La Teoría de la Motivación y Expectativa de Vroom (1964) también se puede aplicar en este contexto. Según Vroom, la motivación de los miembros de las fuerzas armadas para adoptar y adaptarse a nuevas tecnologías dependerá de la percepción de que el uso de estas innovaciones mejorará sus probabilidades de éxito en las misiones. Si los miembros de la fuerza creen que las TICs mejorarán su capacidad para cumplir con sus objetivos, estarán más dispuestos a adoptar y adaptarse rápidamente a las innovaciones tecnológicas.

2.3. Marco Conceptual

La integración de las Tecnologías de la Información y la Comunicación (TICs) en las operaciones militares representa un factor clave para mejorar la eficiencia operativa y la capacidad de respuesta en entornos complejos y cambiantes, como los que enfrenta la 3ra Brigada Blindada. Las TICs abarcan una amplia gama de herramientas tecnológicas, como computadoras, redes de comunicación, sistemas de transmisión de datos y satélites, que permiten la creación, almacenamiento, procesamiento y difusión de información a través de distintos canales de telecomunicaciones. En el contexto militar, estas tecnologías son fundamentales para mejorar la coordinación entre unidades, optimizar la toma de decisiones en tiempo real y permitir la interoperabilidad con otras fuerzas, lo cual resulta esencial para garantizar el éxito de las operaciones terrestres unificadas.

El uso de tecnologías emergentes, como la inteligencia artificial, la robótica, la computación cuántica y el blockchain, se ha destacado por su potencial para transformar las operaciones militares. Estas tecnologías ofrecen la posibilidad de mejorar la eficiencia operativa, optimizar los procesos de toma de decisiones y proporcionar ventajas tácticas frente a adversarios más avanzados tecnológicamente (Wu & Lee, 2022). Sin embargo, la integración de estas innovaciones en el ámbito militar presenta varios desafíos, entre los que se encuentran la necesidad de una infraestructura tecnológica adecuada, la capacitación continua del personal y la adaptación a nuevos sistemas de comunicación y control. La implementación exitosa de tecnologías emergentes dependerá de la capacidad de la brigada para adaptarse a estos avances y de la forma en que las TICs puedan integrarse en los sistemas existentes sin generar interrupciones en las operaciones.

El Modelo de aceptación de tecnología (TAM), propuesto por Davis (1989), es un marco útil para comprender los factores que influyen en la adopción de nuevas tecnologías. Este modelo plantea que la adopción de una tecnología depende de la utilidad percibida y la facilidad de uso percibida por los usuarios. En el contexto militar, es esencial que el personal de la 3ra Brigada

Blindada perciba que las TICs mejorarán su desempeño en las operaciones y que estas tecnologías sean fáciles de usar y de integrar en su entorno de trabajo. Además, la aceptación de las TICs también puede estar influenciada por la actitud hacia la tecnología y la presión social dentro de la organización, lo que subraya la importancia de contar con una adecuada estrategia de gestión del cambio y de formación.

La ciberseguridad es un factor clave en la integración de las TICs en las operaciones militares. La protección de los sistemas, redes y datos es fundamental para asegurar la integridad de las comunicaciones y la seguridad de la información en un entorno cada vez más digitalizado. Los ciberataques pueden poner en peligro los sistemas de telecomunicaciones, interrumpir el funcionamiento de equipos esenciales o robar información confidencial, lo que afecta la efectividad de las misiones militares. Según el National Institute of Standards and Technology (2023, p.1), una estrategia de seguridad cibernética sólida debe abordar la protección de la infraestructura, la gestión de riesgos y la respuesta a incidentes. La ciberseguridad debe ser una prioridad para la 3ra Brigada Blindada para evitar vulnerabilidades y garantizar que las TICs sean utilizadas de manera segura y efectiva.

2.4. Definición de Términos Básicos

2.4.1. Análisis de datos en tiempo real

El análisis de datos en tiempo real es el proceso mediante el cual los datos se recopilan, procesan y analizan instantáneamente mientras están siendo generados o recibidos. En el contexto de las operaciones militares, este tipo de análisis permite a los comandantes y unidades actuar de manera inmediata, ajustando tácticas y estrategias en función de la información más reciente disponible. En el ámbito de las TICs militares, el análisis en tiempo real es crucial para la toma de decisiones rápidas y precisas, especialmente en situaciones de combate, donde las condiciones cambian constantemente y la capacidad de adaptarse rápidamente puede marcar la diferencia entre el éxito y el fracaso de una operación (Baugh & Peterson, 2018). Los sistemas de análisis de datos en tiempo real suelen utilizar herramientas avanzadas como la inteligencia

artificial y el aprendizaje automático para detectar patrones y predecir resultados, lo que permite optimizar las operaciones militares.

2.4.2. Ciberseguridad

La ciberseguridad se refiere a las prácticas y medidas diseñadas para proteger los sistemas informáticos, redes y datos frente a ataques, accesos no autorizados, alteraciones o daños. En el contexto militar, la ciberseguridad se convierte en una prioridad crítica debido a la creciente dependencia de las TICs para las operaciones de comando y control (C2). La protección de la infraestructura digital es esencial para evitar que los adversarios alteren las comunicaciones o accedan a datos confidenciales que podrían comprometer la seguridad nacional. En operaciones militares, la ciberseguridad debe abordar riesgos como los ciberataques, las intrusiones y la explotación de vulnerabilidades, lo que requiere un enfoque integral que incluya la protección de redes, la capacitación del personal y la actualización constante de las defensas cibernéticas (Reid, 2020).

2.4.3. Cultura organizacional

Es el sistema compartido de valores, creencias y normas que influyen en el comportamiento de los individuos y grupos dentro de una organización. (Schneider, 1985, p. 2). Está compuesto por elementos que conforman la identidad de la organización y guían las interacciones de sus miembros, así como las partes interesadas externas. La cultura organizacional proporciona identidad, significado, motiva y guía el comportamiento, facilita la coordinación y el control; y adapta la organización al entorno, así mismo existen diversos tipos de cultura como la jerárquica, cultura de mercado y la cultura adhocrática.

2.4.4. Eficiencia operativa

Es la habilidad de una organización para generar bienes o servicios de la forma más eficiente posible, aprovechando al máximo los recursos y reduciendo los costos. En resumen, la eficiencia operativa se refiere a la capacidad de una organización para utilizar sus recursos de manera efectiva y rentable en la producción de bienes o servicios. La eficiencia operativa se mide

por la relación entre los insumos utilizados y los resultados obtenidos. (Slack, Chambers & Johnston, 2013, p.4). Existen diversos factores que influyen en la eficiencia operativa de una organización entre los que se pueden destacar: Procesos, Tecnología, Recursos Humanos y Cultura Organizacional. Así mismo, algunos beneficios que destacan de la eficiencia operativa son: mayor productividad y competitividad.Para ello, se requiere invertir en tecnología para la automatización adecuada de tareas, mejorar la comunicación y el flujo de información y finalmente proporcionar herramientas para la toma de decisiones.

2.4.5. Innovación tecnológica

Consiste en la introducción de nuevas ideas, productos, servicios o procesos que utilizan la tecnología para mejorar el funcionamiento de una organización o la vida de las personas. Implica crear algo valioso con un impacto significativo en el mercado o la sociedad. Es el proceso de aplicar nuevas ideas y tecnologías para mejorar productos, servicios, procesos o sistemas, y puede resultar en nuevos productos, la mejora de los existentes o la creación de nuevos mercados o modelos de negocio (European Commission, 2003, p. 5)

2.4.6. *Interoperabilid*ad

La interoperabilidad es la capacidad de dos o más sistemas o componentes para intercambiar información y funcionar juntos de manera coordinada, sin importar sus diferencias tecnológicas. (International Organization for Standardization, 2008, p.1). Es decir, la interoperabilidad permite la integración de diferentes sistemas y plataformas, lo que a su vez facilita la colaboración, la comunicación y el intercambio de información. Tiene beneficios como la colaboración, aumento de la eficacia, reduce costos y promueve la innovación.

2.4.7. Redes de comunicación

Las redes de comunicación son sistemas de infraestructura tecnológica diseñados para permitir el intercambio de información entre diversas unidades y componentes dentro de una organización, facilitando la coordinación y colaboración. En las operaciones militares, las redes de comunicación no solo incluyen tecnologías de transmisión de datos, sino también sistemas

de comando y control (C2) que aseguran que la información fluya sin interrupciones entre los centros de comando, las unidades en el terreno y otras entidades relevantes. Las redes de comunicación eficaces permiten una mejor interoperabilidad entre unidades y entre distintas ramas de las fuerzas armadas, lo que se traduce en una mayor capacidad para ejecutar operaciones conjuntas y rápidas, contar con redes de comunicación seguras y de alto rendimiento es esencial para la realización de misiones conjuntas con otras fuerzas militares o agencias externas (Kessel, 2021).

2.4.8. Simulación militar

La simulación militar es el proceso mediante el cual se reproducen situaciones de combate o ejercicios tácticos en un entorno virtual, con el fin de entrenar a los soldados o evaluar la efectividad de tácticas y estrategias sin los riesgos asociados a los entrenamientos reales. Las simulaciones pueden incluir escenarios basados en realidad virtual o entornos computarizados en los que las decisiones de los participantes se evalúan en tiempo real. En el contexto de las TICs, las simulaciones juegan un papel crucial en la formación de personal militar, la prueba de nuevos sistemas y tecnologías, así como en la planificación estratégica. A través de la simulación, las fuerzas armadas pueden mejorar la eficiencia operativa y reducir costos, ya que permiten la repetición de escenarios múltiples sin la necesidad de recursos materiales o el desgaste físico de los equipos (Franks & Brown, 2017).

CAPÍTULO III: MÉTODOLOGÍA

3.1. Diseño Metodológico

3.1.1 Enfoque de la investigación

El vigente estudio se empleó el enfoque cualitativo para profundizar las experiencias, apreciaciones y actitudes de los partes relacionadas en la implementación de las TICs en el entorno de las operaciones y acciones terrestres unificadas. La investigación se fundamenta en el trabajo de Hernández - Sampieri & Mendoza (2020), quienes proponen la creación de conocimiento a través de un concepto inicial de experiencias propias, de esta manera, se relaciona con un marco teórico para analizar los desafíos de la implementación de TICs en el sector militar. Este enfoque de investigación permite generar conocimiento mediante la comprensión e interpretación de los fenómenos a través de las descripciones y definiciones producidas por la experiencia de los participantes.

3.1.2 Tipo de investigación

La investigación que se llevará a cabo es de tipo teórico-empírica, ya que combina el análisis de marcos teóricos relevantes con la observación directa y análisis empírico de la realidad operativa de la 3ra Brigada Blindada. Según Hernández, Sampieri y Mendoza (2020), este enfoque se distingue por integrar el conocimiento conceptual con el estudio de fenómenos observables, permitiendo obtener una comprensión más aplicable y fundamentada en datos reales. En el caso de nuestra investigación, este enfoque resulta especialmente adecuado porque no solo busca profundizar en las teorías relacionadas con la implementación de Tecnologías de la Información y la Comunicación (TICs) en el ámbito militar, sino también explorar y analizar de manera sistemática las condiciones concretas y los desafíos prácticos que enfrenta la 3ra Brigada Blindada. A través de este enfoque, se pretende aportar una visión más

integral de los factores que afectan la adopción tecnológica y ofrecer recomendaciones basadas en el análisis empírico de las problemáticas reales, contribuyendo así al fortalecimiento de la eficiencia y efectividad operativa de la institución.

3.1.3 Método de investigación

Se utiliza el método hermenéutico interpretativo, descrito por Vargas (2011), que se enfoca en la interpretación de textos, discursos y acciones para comprender los significados emergentes y las motivaciones subyacentes en las percepciones y prácticas. Este método es particularmente adecuado para explorar la complejidad de la implementación de TICs en el ámbito militar, ya que permite una comprensión profunda de los desafíos enfrentados y la formulación de recomendaciones basadas en la interpretación detallada de las experiencias y perspectivas de los participantes.

3.1.4 Escenario de Estudio

La investigación se llevó a cabo en el contexto específico en la 3ª Brigada Blindada, y se buscó comprender cómo los oficiales de estado mayor, comandantes de la compañía que estaban a cargo de esta unidad, perciben y abordan estos desafíos.

A través de las entrevistas a profundidad, que se realizaron a los oficiales de estado mayor desde el periodo 2024 – 2025, via presencial en las instalaciones de la Escuela Superior de Guerra y con el apoyo de la tecnología, que permite el acceso a las plataformas digitales, se resguardó la confidencialidad de la información, identificando los principales obstáculos y oportunidades para el uso efectivo de las TICs en el cumplimiento de la misión de la brigada, con el fin de proponer recomendaciones que permitan optimizar su implementación y mejorar la eficiencia y eficacia de las operaciones y acciones terrestres unificadas.

3.2. Diseño muestral

3.2.1. Población y Muestra

La muestra de este estudio está compuesta por un grupo selecto (10 participantes) de oficiales del Ejército del Perú, específicamente aquellos que han tenido experiencia en la 3ª

Brigada Blindada de Moquegua y han participado directamente en las operaciones y acciones terrestres realizadas por dicha unidad. Estos oficiales desempeñaron roles clave como asesores durante el desarrollo de estas operaciones, lo que les otorga un conocimiento profundo sobre los desafíos y las dinámicas de implementación de las Tecnologías de la Información y Comunicación (TICs) en el contexto militar. La selección de los participantes se basa en su experiencia directa y su conocimiento especializado, lo que asegura que puedan proporcionar información valiosa y relevante para abordar el tema de investigación.

Según Hernández, Sampieri y Mendoza (2018), la muestra en una investigación debe ser seleccionada cuidadosamente para asegurar que los participantes sean representativos del fenómeno de estudio. En este caso, la muestra no será aleatoria, sino intencionada, ya que se busca obtener datos de aquellos individuos que tengan un conocimiento específico y significativo sobre los retos asociados con la implementación de las TICs en las operaciones y acciones terrestres. Esta estrategia está alineada con el enfoque cualitativo de la investigación, en el que la selección de la muestra se basa en criterios específicos relacionados con el propósito y los objetivos del estudio (Patton, 2002).

3.3 Técnicas e instrumentos de recolección de datos

3.3.1 Técnicas:

3.3.1.1 Entrevistas en profundidad:

La entrevista en profundidad es una técnica cualitativa utilizada para explorar las percepciones, experiencias y actitudes de los participantes respecto a la integración de las Tecnologías de la Información y la Comunicación (TICs) en el entorno operativo militar. Esta técnica permite obtener información detallada y profunda sobre los obstáculos y las oportunidades percibidas por los actores clave involucrados en el proceso de adopción tecnológica. Según Sampieri (2014), las entrevistas en profundidad ofrecen un espacio donde los participantes pueden expresar libremente sus pensamientos, preocupaciones y reflexiones. En este estudio, se entrevistará a oficiales de la brigada, personal de TICs y otros actores

relevantes, con el fin de identificar barreras culturales, resistencias al cambio, problemas de interoperabilidad y otros desafíos operacionales asociados con el uso de tecnologías durante las misiones de campo.

3.3.1.2 Análisis documentario:

El análisis documentario se empleará para revisar la documentación institucional relacionada con la implementación de las TICs en la 3ª Brigada Blindada. A través de este análisis, se obtendrá información sobre las políticas, normativas y estrategias oficiales que guían el uso de tecnologías dentro de la institución. Sampieri (2014) afirma que el análisis de documentos es una técnica que permite comprender los marcos normativos y operativos en los que se desarrollan los procesos organizacionales. En este contexto, los documentos clave que se analizarán incluirán manuales operativos, informes de misiones anteriores, políticas de ciberseguridad y planes estratégicos de integración tecnológica. Este enfoque permite identificar las orientaciones y los lineamientos institucionales que guían el uso de las TICs en las operaciones y acciones terrestres de la brigada.

3.3.1.3 Observación participante:

La observación participante es una técnica que permitirá al investigador integrarse en el entorno de estudio para observar de manera directa los procesos y comportamientos de los participantes en su contexto real. Según Creswell (2014), esta técnica es esencial para obtener datos sobre las dinámicas cotidianas y la interacción de los sujetos con el objeto de estudio. En el caso de esta investigación, la observación se centrará en las interacciones de los miembros de la brigada con las TICs durante las operaciones militares. El investigador será testigo directo de las dificultades que surgen en la práctica, tales como problemas técnicos, falta de formación en el uso de las TICs o resistencia a los cambios tecnológicos, y cómo estas cuestiones afectan la efectividad operativa en tiempo real.

3.3.2 Instrumentos

3.3.2 1 Guía de entrevista en profundidad

La guía de entrevista en profundidad se utilizará para estructurar las entrevistas realizadas a los actores clave de la brigada, como oficiales de TICs, personal militar y otros involucrados en el uso de las tecnologías durante las operaciones. Este instrumento tiene como objetivo captar las percepciones, experiencias y actitudes de los participantes respecto a la implementación de TICs en sus operaciones, explorando las barreras, beneficios y desafíos identificados en la integración de estas tecnologías. Según Creswell (2014), el uso de entrevistas en profundidad es apropiado para obtener datos ricos y detallados sobre el contexto y las vivencias personales de los participantes. La guía se estructura en torno a temas clave como la resistencia al cambio, los problemas operacionales con las TICs, la interoperabilidad y las barreras culturales. La flexibilidad de las entrevistas permite profundizar en temas emergentes y explorar aspectos no anticipados en la fase de diseño de la investigación (Patton, 2002).

3.3.2.2 Guía de análisis documentario

El análisis documentario es un instrumento clave en esta investigación, ya que permitirá examinar las fuentes documentales relacionadas con las políticas, procedimientos y directrices oficiales que guían la implementación de TICs en la 3ª Brigada Blindada. La guía de análisis documentario se ha estructurado para enfocar la revisión de documentos clave como manuales operativos, informes estratégicos, políticas institucionales sobre el uso de TICs, y registros históricos de evaluaciones tecnológicas previas. El análisis documental es un método de recolección de datos que resulta especialmente valioso en estudios cualitativos, pues permite comprender el contexto normativo, estructural y estratégico en el cual se desarrollan los procesos de adopción tecnológica (Sampieri, 2014). Este instrumento permitirá obtener una visión retrospectiva que complementará los datos primarios obtenidos a través de las entrevistas y la observación, permitiendo una triangulación de fuentes para aumentar la validez y la confiabilidad de los hallazgos.

3.3.2.3 Guía de observación participante

La guía de observación participante se utilizará para registrar las observaciones directas sobre las interacciones de los miembros de la brigada con las TICs durante las operaciones de campo. Este instrumento está diseñado para guiar al investigador en la observación de las dinámicas del uso de las tecnologías, los problemas técnicos que surgen durante las misiones, y las respuestas del personal frente a fallos o dificultades en la integración tecnológica. Según Creswell (2014), la observación participante permite al investigador estar inmerso en el contexto de estudio, lo cual es clave para captar la realidad cotidiana de la implementación de TICs en un entorno operativo. La guía de observación se orienta a aspectos como la interacción entre unidades, el uso efectivo de las TICs para la comunicación y coordinación, y la resolución de problemas en tiempo real. Además, se documentarán las posibles reacciones emocionales y conductuales de los actores ante fallos técnicos o barreras operativas, lo que proporcionará una perspectiva compleja de la adopción tecnológica en el contexto militar.

3.3.3 Validación de los Instrumentos

La validación del instrumento de recolección de datos en este estudio se realizó siguiendo los principios metodológicos propuestos por Hernández Sampieri (2014), quien subraya la importancia de que el instrumento sea evaluado por expertos en el área para garantizar que las preguntas sean claras, pertinentes y alineadas con los objetivos de la investigación. En este caso, el instrumento de entrevista fue validado por cinco expertos en el área: el Doctor Cesinario Mondragón Javier, la Magíster Ortiz Guzmán Marlene Evelyn, el Magíster Barzola Pérez Ulises, el Magister Carrillo Espicha Ricardo y el Magíster López García Jorge Rodrigo. Los validadores realizaron una revisión detallada tanto del diseño como de la estructura del instrumento, enfocándose en la claridad, pertinencia y coherencia de las preguntas respecto a los objetivos del estudio. Tras este proceso, los expertos expresaron su conformidad con el instrumento, sugiriendo ajustes específicos para mejorar la precisión y la relevancia de algunas preguntas, con el fin de asegurar una mayor exactitud en la interpretación de las respuestas. Además, se

implementó el procedimiento de member checking, según lo propuesto por Lincoln y Guba (1985), en el cual se devolvieron los resultados preliminares a los participantes para que pudieran validar la exactitud de las interpretaciones realizadas. Los participantes revisaron las transcripciones de sus respuestas y proporcionaron retroalimentación valiosa, lo que permitió ajustar las interpretaciones y fortalecer la fiabilidad de los resultados. La combinación de la validación por expertos y el member checking garantizó que los resultados fueran representativos y fieles a las experiencias y perspectivas de los participantes, asegurando la validez y consistencia de las conclusiones del estudio. Véase el Anexo 4 (Validación de expertos)

3.4 Técnicas para el Procesamiento de la Información

Los datos obtenidos de las entrevistas, observaciones y el análisis documental serán procesados para transformarlos en información válida que permita generar conocimiento sobre el tema de estudio. Según Hernández, Sampieri y Mendoza (2018), el proceso de análisis comienza con la transcripción de las entrevistas, lo que permitirá al investigador familiarizarse con los datos y realizar una lectura detallada. Posteriormente, se llevará a cabo un proceso de codificación, en el cual se identificarán categorías y patrones clave dentro de los datos obtenidos. La codificación se realizará de manera inductiva, es decir, las categorías emergen directamente de los datos, sin la imposición de categorías predefinidas. Esto permite que el análisis sea flexible y se enfoque en los temas relevantes que surjan de las experiencias de los participantes (Patton, 2002).

Además, el análisis de los documentos permitirá contextualizar y enriquecer los hallazgos obtenidos de las entrevistas, al proporcionar información complementaria sobre las políticas y estrategias institucionales. La observación directa, por su parte, proporcionará datos adicionales sobre cómo los participantes interactúan con las TICs en el entorno operativo.

Se empleará la triangulación de datos, técnica recomendada por Lincoln y Guba (1985), para comparar los resultados obtenidos de las entrevistas, las observaciones y los documentos, lo que contribuirá a la validez y credibilidad de los resultados obtenidos en esta investigación.

3.5 Aspectos Éticos

Los oficiales de estado mayor que proporcionen información deben tener la seguridad de que sus opiniones son tratadas con la debida reserva garantizando la confidencialidad de la misma, en ese sentido, se obtuvo previamente el consentimiento informado de los participantes antes de brindar cualquier dato relacionado con el tema de estudio.

Los participantes conocen sobre los objetivos de la investigación, los métodos que fueron empleados y el uso que se dará a los datos, generando confianza para que con libertad expresen sus opiniones y puntos de vista sin temor, cabe mencionar que la participación en esta investigación es voluntaria y basada en la confianza, asegurándonos que se realice de manera objetiva, ya que es un tema que genera un impacto y tiene relevancia en sus resultados, los cuales recaen en la toma de decisiones y en la planificación de operaciones militares.

La oficiales deben ser transparentes en sus métodos y hallazgos y deben evitar cualquier forma de manipulación o falsificación de datos, basandose en principios éticos y sólidos que contribuyan al conocimiento y la mejora de las capacidades del Ejército del Perú. Por lo tanto, al garantizar la confidencialidad, el consentimiento informado, la libertad de participación, la consideración del impacto, la claridad del uso de la información y la integridad de la investigación, se puede asegurar que este estudio contribuya de manera positiva al Ejército del Perú.

CAPÍTULO IV: ANÁLISIS Y SÍNTESIS

4.1. Definición de las Categorías y Sub Categorías

Tabla 1

Categorías y Subcategorías

Categoría	Subcategoría	Definición	Referencia
1. Desafíos en la Implementación de TICs	**1.1Implementación Técnica**	Complejidad en la integración y configuración de sistemas TICs heterogéneos.	Rai, A., & Upadhyay, S. (2020). Challenges and opportunities of implementing cloud computing in the Indian Army. *International Journal of Information and CommunicationTechnology*, 16_(2), 142-158. DOI: 10.1504/IJICT.2020.10023139
	1.2 Cultural Organizativa	Barreras culturales y resistencia al cambio en la adopción de TICs.	Smith, M., & Peterson, K. (2019). Overcoming organizational resistance to change: A case study of the adoption of enterprise resource planning (ERP) systems in the U.S. Army. *Journal of Information Systems Management*, 30(3), 223-238. DOI: 10.1080/08972241.2019.1612441
	1.3 Seguridad Cibernética	Vulnerabilidad y exposición a riesgos de seguridad cibernética.	Pasztor, P., & Shostak, S. (2020). Cyber threats to U.S. military operations. *War on the Rocks*. https://warontherocks.com/tag/cyber/
2. Impacto de las TICs en operaciones y acciones terrestres	**2.1 Eficiencia Operativa**	Reducción del tiempo de respuesta en misiones críticas.	Alberts, D. J., Garstka, J. J., & Stein, F. P. (2016). *Network-centric warfare: Thinking about the future of land forces*. CCRP Press.
	2.2 Interoperabilidad	Integración efectiva entre sistemas TICs de diferentes unidades.	Fredericks, E. P., & Borenstein, N. (2018). Interoperability challenges for the future of joint warfare: A case study of the U.S. Army and the U.S. Marine Corps. *Defense Systems Review*, 17(1), 1-26. DOI: 10.1162/dsrv_a_00827
	2.3 Adaptación a la Innovación Tecnológica	Patrones de aceptación e incorporación de tecnologías innovadoras en las fuerzas armadas, siguiendo el modelo de la Teoría de la Difusión de Innovaciones (TDI) de Everett Rogers.	Rogers, E. M. (2003). *The diffusion of innovations*. Free Press.

Nota: Esta tabla define las categorías y sub categorías detallando la referencia de los autores.

4.2. Soporte de Categorías

Tabla 2

Guía de Entrevista: Definición Integral de Categorías

Categoría	Soporte de Categoría	Subcategoría	Resumen
a) Desafíos en la Implementación de TICs	*"Los desafíos técnicos se relacionan principalmente con la infraestructura existente que no siempre es capaz de adaptarse a las condiciones operativas de combate, y la falta de estandarización entre los sistemas nuevos y antiguos."* (Entrevista 1) *"Uno de los mayores retos es la falta de compatibilidad entre las tecnologías implementadas y las ya existentes en el campo, lo cual afecta la integración total de las TICs."* (Entrevista 2) *"La resistencia de los sistemas en condiciones extremas de temperatura y humedad también ha sido un factor importante que ralentiza la eficacia de las TICs."* (Entrevista 3) *"La falta de equipamiento y presupuesto adecuado dificulta la implementación en su totalidad de estas tecnologías avanzadas."* (Entrevista 7) *"En zonas como Moquegua, las condiciones geográficas y salinas limitan la cobertura de las redes de comunicación, un desafío mayor para*	1. Implementación Técnica	*"Los principales retos técnicos han sido la adaptación de las TICs en entornos de comunicación limitados, la resistencia de los equipos bajo condiciones operativas extremas y la interoperabilidad con sistemas antiguos."* (Entrevista 1) *"La resistencia frente a los ataques de guerra electrónica es otro desafío, ya que nuestras comunicaciones deben mantenerse estables y sin interferencias, incluso cuando hay intentos de bloqueo o interferencia activa."* (Entrevista 2) *"Los nuevos sistemas tecnológicos requieren ser resistentes al clima y deben garantizar la continuidad de las operaciones. Sin embargo, hemos encontrado que algunos dispositivos no han cumplido con estos estándares."* (Entrevista 4) *"La falta de integración perfecta entre los sistemas antiguos y los nuevos sigue siendo uno de los principales obstáculos para la eficiencia operativa de las TICs."* (Entrevista 5) *"En áreas de difícil acceso, la transmisión de señales sigue siendo un reto debido a*

las TICs." (Entrevista 9) *"A pesar de los esfuerzos, las TICs aún no son lo suficientemente adaptables para enfrentar las variaciones extremas en el terreno."* (Entrevista 10) *"A pesar de los avances en la incorporación de tecnologías más modernas, el proceso de adopción ha sido más lento de lo esperado debido a la falta de infraestructura que respalde adecuadamente los nuevos sistemas."* (Entrevista 6) *"El personal más joven se adapta rápidamente a las TICs, mientras que algunos miembros con mayor experiencia muestran resistencias significativas a los cambios tecnológicos."* (Entrevista 8)		*las condiciones geográficas extremas."* (Entrevista 9) *"A pesar de los avances, las TICs todavía enfrentan dificultades en zonas donde el terreno limita las capacidades de la infraestructura."* (Entrevista 10)
	2. Cultural Organizativa	*"El personal muestra cierta preferencia por métodos tradicionales y, en algunos casos, una resistencia a adoptar nuevas tecnologías debido a la falta de familiaridad con ellas. Esto ralentiza la adopción de TICs en toda la brigada."* (Entrevista 1) *"El cambio cultural necesario para aceptar las TICs ha sido difícil de implementar, particularmente entre el personal con más antigüedad en las fuerzas, quienes tienen menos confianza en las nuevas tecnologías."* (Entrevista 2) *"Muchos de los oficiales de mayor rango han expresado dudas sobre la efectividad y la confiabilidad de las TICs en situaciones críticas de combate, lo que genera incertidumbre en su adopción."* (Entrevista 3) *"La capacitación en TICs es vista como un proceso necesario, pero aún existe resistencia en muchas áreas por parte del personal más experimentado, que tiene poca inclinación hacia el uso de tecnologías avanzadas."* (Entrevista 4) *"El cambio organizativo ha sido promovido mediante la integración gradual de las*

		TICs, pero la falta de una estrategia clara ha sido un obstáculo. La formación y la sensibilización siguen siendo claves en este proceso." (Entrevista 5) *"La resistencia cultural ha sido superada parcialmente a través de programas de capacitación y formación continua. Sin embargo, el proceso sigue siendo gradual y con resultados dispares."* (Entrevista 6) *"El personal más joven es más receptivo a las TICs, lo que crea una brecha generacional en la aceptación de nuevas tecnologías, lo cual requiere estrategias específicas para cada grupo de edad."* (Entrevista 8)
	3. Seguridad Cibernética	*"Los principales desafíos incluyen la protección de datos sensibles en entornos operativos y la prevención de interceptaciones. La seguridad cibernética debe ser continua y robusta para contrarrestar las amenazas constantes."* (Entrevista 1) *"La brigada ha implementado medidas preventivas como sistemas de encriptación y capacitación en ciberseguridad para el personal."* (Entrevista 2) *"En el caso de ataques avanzados en tiempo real, persisten brechas que afectan la capacidad de respuesta, especialmente en los sistemas de microondas y redes de datos."* (Entrevista 2) *"A pesar de las medidas preventivas, aún*

			no contamos con un sistema completamente autónomo para la detección y mitigación inmediata de ciberataques." (Entrevista 4) *"Los protocolos de encriptación que se han implementado son clave para proteger la integridad de los datos, pero todavía hay vulnerabilidades en algunas de las redes de comunicación."* (Entrevista 5) *"El personal ha recibido formación especializada en ciberseguridad, sin embargo, la constante evolución de las amenazas cibernéticas requiere una actualización continua de los sistemas de defensa."* (Entrevista 6) *"La falta de equipamiento y la falta de personal capacitado para hacer frente a los ciberataques en tiempo real siguen siendo una limitación importante."* (Entrevista 7) *"Actualmente, las medidas cibernéticas son pasivas y requieren la mejora de la infraestructura para enfrentar ataques modernos."* (Entrevista 7) *"La adaptación a ataques sofisticados sigue siendo una de las principales debilidades dentro de la brigada."* (Entrevista 10)
b) Impacto de las TICs en operaciones y acciones terrestres	*"El impacto de las TICs en la eficiencia operativa ha sido notoriamente positivo, ayudando a mejorar la coordinación entre unidades y facilitando la toma de decisiones en tiempo real."* (Entrevista	1. Eficiencia Operativa	*"La implementación de TICs ha optimizado la comunicación en tiempo real y la coordinación entre unidades, permitiendo tomar decisiones informadas de manera más rápida y eficiente en el campo de*

		2) *"Aunque el uso de TICs mejora la eficacia operativa, la falta de infraestructura en algunas áreas sigue siendo un reto importante."* (Entrevista 3) *"El impacto de las TICs en la toma de decisiones ha permitido decisiones más rápidas, lo que mejora la eficacia de la brigada en la implementación de estrategias."* (Entrevista 2) *"Las unidades aún enfrentan dificultades técnicas en cuanto a la integración con sistemas de armas y otros equipos esenciales en el campo."* (Entrevista 3)
		batalla." (Entrevista 1) *"La falta de infraestructura y conectividad adecuada en ciertos entornos ha dificultado el uso constante de TICs. En zonas de difícil acceso, mantener una operatividad continua sigue siendo un desafío."* (Entrevista 2) *"La logística, el mapeo táctico y la comunicación han mostrado mejoras significativas gracias a las TICs, facilitando la planificación y ejecución de operaciones de manera más ágil y precisa."* (Entrevista 3) *"El tiempo de respuesta y la precisión en la ejecución de órdenes han aumentado considerablemente."* (Entrevista 4) *"A pesar de la mejora en la eficiencia operativa, la falta de recursos y cobertura sigue limitando el rendimiento total de las TICs."* (Entrevista 5) *"La eficiencia operativa también ha mejorado a través de la optimización de los tiempos de despliegue y el uso de tecnología avanzada para hacer ajustes en tiempo real."* (Entrevista 6) *"Sin embargo, la cobertura en ciertas zonas sigue siendo inadecuada y afecta la eficacia total de las TICs."* (Entrevista 10)
	2. Interoperabilidad	*"Las TICs han facilitado una mayor interoperabilidad entre unidades, permitiendo una coordinación más fluida y precisa."* (Entrevista 1)

		"Se han adoptado protocolos de comunicación unificados y realizado capacitaciones cruzadas para que las unidades trabajen juntas sin dificultades técnicas." (Entrevista 2) *"La falta de estandarización entre sistemas de comunicación y equipos de armamento ha sido un desafío. La sincronización entre estos elementos requiere ajustes constantes."* (Entrevista 3) *"La implementación de protocolos de comunicación estandarizados ha sido un paso importante para mejorar la integración entre diferentes unidades."* (Entrevista 4) *"Sin embargo, la falta de estandarización entre los equipos de diversas generaciones sigue creando conflictos de interoperabilidad."* (Entrevista 5) *"A pesar de los avances, algunas unidades aún experimentan dificultades para integrarse completamente debido a la falta de compatibilidad entre los diferentes sistemas utilizados."* (Entrevista 6)
	3. Adaptación a la Innovación Tecnológica	*"La brigada se ha adaptado mediante programas de formación específicos que aseguran el uso efectivo de las nuevas herramientas tecnológicas."* (Entrevista 1) *"Aunque la brigada ha logrado adaptarse a algunas innovaciones tecnológicas, la resistencia al cambio sigue siendo una barrera."* (Entrevista 2) *"La integración de plataformas de realidad*

	aumentada y sistemas de mapeo digital ha mejorado la precisión en la planificación y la ejecución de operaciones, facilitando una respuesta más rápida ante amenazas." (Entrevista 3) *"La adopción de nuevas tecnologías, como drones para inteligencia táctica, ha fortalecido significativamente nuestras capacidades operativas."* (Entrevista 4) *"A pesar de los avances, los problemas de adaptación cultural y la falta de recursos limitan la implementación completa de las TICs."* (Entrevista 5) *"La resistencia al cambio por parte de algunos miembros del personal aún se siente fuerte, lo que limita la implementación total de tecnologías innovadoras en el campo de batalla."* (Entrevista 6) *"La adaptación a las TICs se ha logrado mediante capacitaciones intensivas y la familiarización con los equipos a través de simulaciones, pero la falta de recursos sigue siendo una barrera significativa."* (Entrevista 6) *"Los avances en la integración de tecnologías de innovación en las brigadas están siendo limitados por la falta de infraestructura en las zonas de difícil acceso."* (Entrevista 10)

Nota: La presente tabla, de elaboración propia, muestra el soporte de las categorías y subcategorías de la presente investigación producto de las entrevistas.

Tabla 3

Entrevistas: Soporte de las categorías

Tema	Categorías	Subcategorías	Patrones	Resumen
Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025.	a) Desafíos en la Implementación de TICs	1. Implementación Técnica	• *Adaptación tecnológica* • *Condiciones extremas* • *Falta de infraestructura* • *Obsolescencia tecnológica* • *Desajustes en la integración*	La adaptación tecnológica sigue siendo un desafío clave, especialmente en condiciones extremas (clima y terreno) y con la obsolescencia tecnológica de algunos sistemas existentes. La falta de infraestructura limita la cobertura, y los desajustes en la integración de los sistemas antiguos y nuevos afectan la eficacia de las TICs.
		2. Cultural Organizativa	• *Resistencia cultural* • *Desconfianza en nuevas tecnologías* • *Falta de familiaridad* • *Capacitación insuficiente* • *Dudas sobre efectividad*	Los patrones de resistencia cultural y desconfianza en las TICs son recurrentes, especialmente en el personal más veterano. La falta de familiaridad y capacitación insuficiente afectan la adopción de TICs. Se observan dudas sobre la efectividad de las TICs en situaciones de combate, lo que retrasa su adopción.
		3. Seguridad Cibernética	• *Protección de datos* • *Amenazas externas*	La protección de datos sigue siendo una prioridad, pero brechas en seguridad y la falta de protocolos de detección de ciberataques son desafíos continuos. Las amenazas externas siguen siendo un patrón

		• *Brechas en seguridad* • *Falta de protocolos de detección* • *Ciberataques recurrentes*	preocupante, y los ciberataques recurrentes requieren mejoras en las medidas de seguridad.
b) Impacto de las TICs en operaciones y acciones terrestres	1. Eficiencia Operativa	• *Mejora de la comunicación* • *Coordinación* • *Tiempo de respuesta* • *Optimización de procesos* • *Mejora en toma de decisiones* • *Mejor aprovechamiento de recursos*	Las TICs han mejorado la comunicación en tiempo real y la coordinación eficiente entre unidades, lo que ha llevado a una mejora significativa en la toma de decisiones. Optimización de procesos y mejor aprovechamiento de recursos también son patrones clave. Sin embargo, los problemas de conectividad en ciertas zonas siguen siendo un reto.
	2. Interoperabilidad	• *Coordinación interunidades* • *Protocolos estandarizados* • *Desafíos de integración* • *Falta de estandarización* • *Desajustes en equipos*	La coordinación entre unidades y el uso de protocolos estandarizados son fundamentales. La falta de estandarización sigue siendo una barrera importante para la integración total de las TICs entre las diversas unidades. Los desajustes en equipos de diversas generaciones son otro reto.

	3. Adaptación a la Innovación Tecnológica	• *Resistencia al cambio* • *Adopción gradual* • *Falta de recursos* • *Capacitación continua* • *Ajuste a nuevas plataformas*	La resistencia al cambio sigue siendo un patrón dominante, con un proceso de adopción gradual de nuevas tecnologías. La falta de recursos es otro patrón crítico, afectando la implementación efectiva de TICs. La capacitación continua es esencial para adaptarse a las nuevas plataformas tecnológicas.

Nota: La presente tabla, de elaboración propia, muestra el soporte de las categorías, subcategorías y patrones detectados en el análisis de la presente investigación.

Tabla 4:

Observación: Soporte de las Categorías

Tema	Categorías	Subcategorías	Patrones	Resumen
Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025.	a) Desafíos en la Implementación de TICs	1. Implementación Técnica	• *Condiciones extremas* • *Falta de cobertura* • *Infraestructura insuficiente* • *Falta de señal* • *Problemas de conectividad*	Las TICs enfrentan dificultades en entornos extremos, como interferencias y falta de cobertura en zonas remotas. La infraestructura tecnológica actual no es suficiente para garantizar una comunicación continua. Se requiere mejorar la infraestructura, especialmente en áreas críticas, e implementar tecnologías de conmutación adaptativa para optimizar el funcionamiento de las TICs en condiciones adversas.
		2. Cultural Organizativa	• *Resistencia al cambio* • *Barreras jerárquicas* • *Falta de capacitación* • *Desconfianza tecnológica* • *Bajo conocimiento*	La adopción de TICs se ve ralentizada por la resistencia al cambio cultural dentro de la brigada, donde la falta de comprensión sobre sus beneficios es un obstáculo significativo. Además, las barreras jerárquicas dificultan la toma de decisiones rápidas. Para superar estos desafíos, se recomienda un programa integral de capacitación práctica y la flexibilización organizativa para facilitar la integración de nuevas tecnologías.
		3. Seguridad Cibernética	• *Vulnerabilidad actual* • *Detección proactiva*	La ciberseguridad es un área crítica, ya que los sistemas actuales no ofrecen la protección necesaria ante amenazas avanzadas. Se sugiere la implementación de inteligencia artificial para la detección

			• *Ataques cibernéticos* • *Encriptación insuficiente* • *Brechas de seguridad*	proactiva de patrones de ataque y el fortalecimiento de la encriptación de los datos para asegurar la integridad y confidencialidad de la información durante las operaciones tácticas.
b) Impacto de las TICs en operaciones y acciones terrestres	1. Eficiencia Operativa		• *Mejora operativa* • *Mejora en logística* • *Coordinación eficiente* • *Respuesta rápida* • *Optimización de procesos*	Las TICs han mejorado la eficiencia operativa, especialmente en logística y coordinación en tiempo real. No obstante, la falta de soporte técnico constante y los problemas de conectividad en zonas remotas limitan la continuidad y efectividad de estas mejoras. Se recomienda la implementación de estaciones móviles de respaldo en áreas críticas, lo que garantizaría una operatividad más estable y sostenida en condiciones extremas.
	2. Interoperabilidad		• *Estándares comunes* • *Equipos desactualizados* • *Integración limitada* • *Falta de sincronización* • *Problemas de compatibilidad*	A pesar de los avances en interoperabilidad, las dificultades persisten debido a la falta de estandarización entre los equipos de diferentes unidades y la diversidad de generaciones de tecnología. Es esencial implementar estándares de comunicación comunes y actualizar los sistemas para mejorar la integración y sincronización de las TICs, especialmente en operaciones conjuntas con aliados.
	3. Adaptación a la Innovación Tecnológica		• *Disposición creciente* • *Percepción de complejidad*	Aunque el personal de la brigada está cada vez más dispuesto a adoptar nuevas tecnologías, la percepción de complejidad de las TICs avanzadas genera una transición más lenta. La falta de familiaridad con las

	• *Integración lenta* • *Resistencia a nuevas tecnologías* • *Falta de familiaridad*	herramientas y el temor al cambio son barreras significativas. Se recomienda implementar programas de capacitación continua y un modelo de mentoría, donde los miembros experimentados guíen a los nuevos usuarios, para acelerar la adaptación y asegurar el uso efectivo de las TICs en las operaciones.

Nota: La presente tabla muestra el soporte de las categorías, subcategorías y patrones detectados la Guía de Observación.

Tabla 5:

Revisión documental: Soporte de las categorías

Tema	Categorías	Subcategorías	Patrones	Resumen
Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3a Brigada Blindada, Moquegua, 2025.	a) Desafíos en la Implementación de TICs	1. Implementación Técnica	• *Infraestructura insuficiente* • *Falta de formación técnica* • *Limitada conectividad* • *Modernización tecnológica* • *Carencia de interoperabilidad*	La implementación de TICs enfrenta dificultades relacionadas con la infraestructura insuficiente y la falta de formación técnica especializada en el ámbito militar. El Decreto Supremo N° 085-2023-PCM establece lineamientos estratégicos para la transformación digital, pero la Directiva Única de Funcionamiento del Sistema de Telemática del Ejército (DUFSITELE, 2021) señala que la falta de interoperabilidad entre los sistemas es un reto persistente. La Ley N° 30999 también destaca la importancia de la modernización tecnológica, pero la falta de recursos limita su efectividad en zonas remotas.
		2. Cultural Organizativa	• *Resistencia cultural* • *Barreras jerárquicas* • *Desconfianza hacia las TICs* • *Falta de incentivos* • *Barreras estructurales*	La adopción de TICs en el Ejército se ve afectada por la resistencia cultural y barreras jerárquicas que limitan la rapidez en la adopción de nuevas tecnologías. La Directiva N° 001-2019-PCM enfatiza la importancia de superar estas barreras organizacionales a través de estrategias estructuradas de formación. Además, la falta de incentivos institucionales y la desconfianza tecnológica impiden una mayor digitalización. Es urgente desarrollar programas de formación técnica y

			cambiar las estructuras organizativas para apoyar la transformación digital.
	3. Seguridad Cibernética	• *Vulnerabilidad de sistemas* • *Necesidad de protocolos avanzados* • *Falta de medidas preventivas* • *Deficiencias en la ciberdefensa* • *Insuficiente protección de datos*	Los sistemas de ciberseguridad del Ejército presentan vulnerabilidades críticas. La Política Nacional de Ciberseguridad establece directrices para fortalecer las capacidades de defensa cibernética, pero los Decretos Supremos N° 003-2021-PCM y N° 012-2024-PCM muestran que aún existen deficiencias en los protocolos de seguridad y la protección de datos. Es necesario implementar tecnologías avanzadas de detección, como inteligencia artificial, para anticipar y mitigar los ciberataques.
b) Impacto de las TICs en operaciones y acciones terrestres	1. Eficiencia Operativa	• *Automatización de procesos* • *Reducción de tiempos de respuesta* • *Mejora en toma de decisiones* • *Optimización administrativa*	Las TICs han demostrado ser cruciales para mejorar la eficiencia operativa en el ámbito militar, especialmente a través de la automatización de procesos administrativos, como se detalla en el Decreto Supremo N° 009-2021-PCM. Esto ha resultado en una reducción de tiempos y una mejora significativa en la toma de decisiones estratégicas. La digitalización ha permitido agilizar procesos que previamente eran manuales, aumentando la rapidez de respuesta en situaciones críticas.
	2. Interoperabilidad	• *Diversidad tecnológica* • *Falta de estandarización*	La interoperabilidad sigue siendo un desafío crítico debido a la diversidad tecnológica entre las unidades. El MACOFFAA enfatiza que la falta de estandarización en equipos y sistemas tecnológicos crea dificultades en la

		• *Necesidad de comunicación unificada* • *Protocolos de integración*	integración de TICs. Para optimizar la coordinación y eficacia en las operaciones conjuntas, se debe implementar protocolos de integración y establecer estándares de comunicación unificados.
	3. Adaptación a la Innovación Tecnológica	• *Barreras tecnológicas* • *Resistencia al cambio* • *Falta de formación técnica* • *Necesidad de modernización continua* • *Implementación gradual*	La adaptación tecnológica en las Fuerzas Armadas requiere superar barreras tecnológicas y la falta de formación técnica. Según la DUFSITELE (2021), la modernización continua de los sistemas de telecomunicaciones es esencial, pero la resistencia al cambio sigue siendo una barrera significativa. La implementación gradual de TICs, a través de entornos de simulación digital, puede facilitar una adaptación progresiva y preparar a las unidades para la integración de nuevas tecnologías.

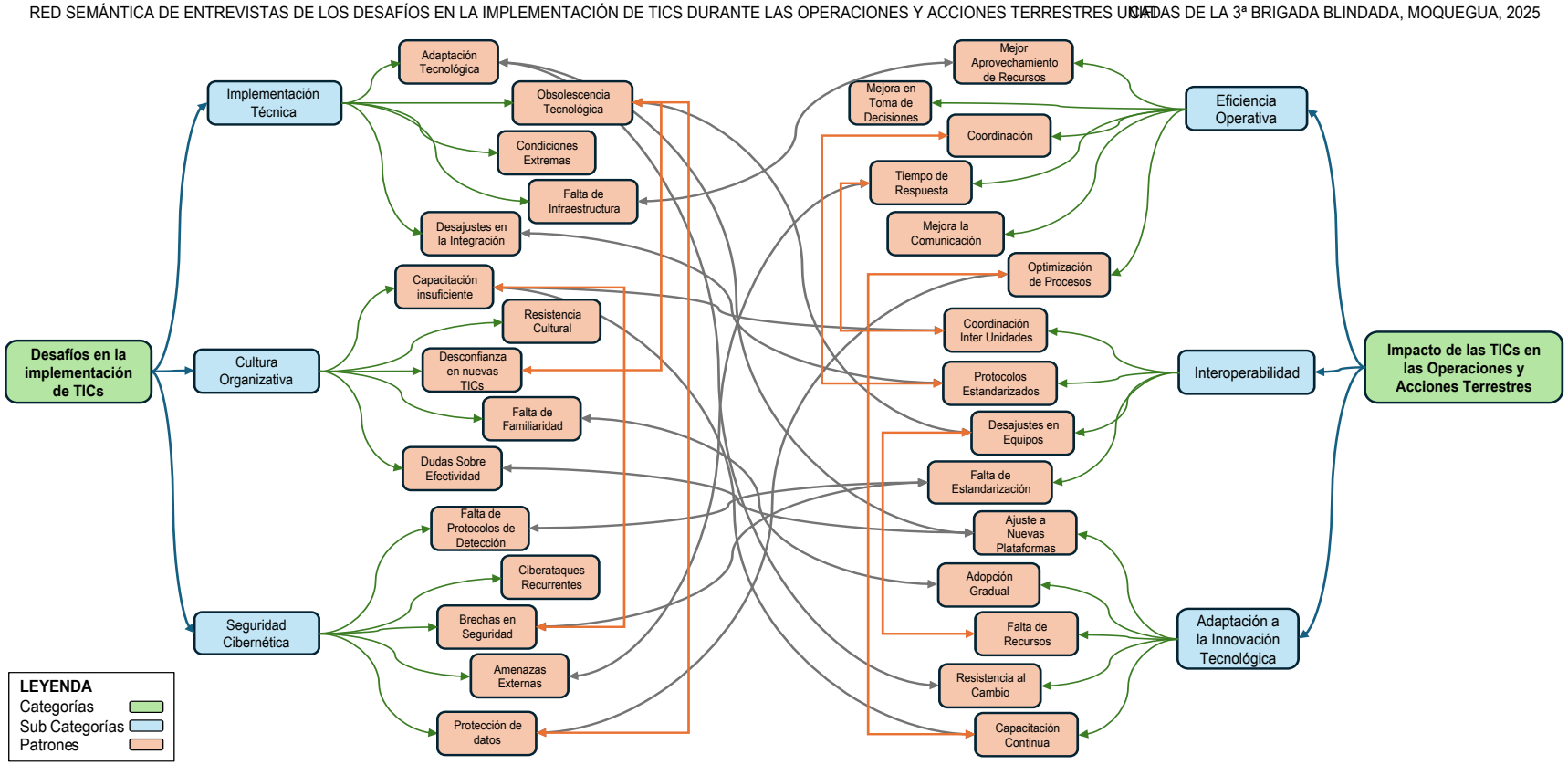
Nota: La presente tabla muestra el soporte de las categorías, subcategorías y patrones detectados la Ficha de Análisis Documental..

4.3. Red semántica

4.3.1. Red semántica de entrevistas

Figura 1

Red semántica de las entrevistas



Nota: La figura, de elaboración propia empleando el software Python y las bibliotecas NetworkX, Matplotlib y NLTK, muestra la red semántica generada a partir del análisis cualitativo de las entrevistas de la presente investigación.

Explicación

A través del análisis de la red semántica generada a partir de las entrevistas, se pudo identificar cómo las distintas categorías y subcategorías relacionadas con la implementación de las tecnologías de la información y comunicación (TIC) se interrelacionan y configuran un panorama de desafíos, oportunidades y limitaciones en el proceso. La red semántica revela que, a pesar de los esfuerzos por incorporar las TIC en el contexto militar, existen barreras estructurales y culturales que impiden una adopción efectiva. En primer lugar, la falta de infraestructura tecnológica adecuada se señala como uno de los principales obstáculos que limitan la capacidad de las fuerzas militares para integrar y utilizar las TIC de manera efectiva. Esta carencia se refleja en la red semántica a través de las conexiones entre la categoría "Desafíos en la Implementación de TICs" y subcategorías como "Falta de Infraestructura" y "Desajustes en la Integración", lo que subraya la importancia de contar con recursos físicos y tecnológicos adecuados para una implementación exitosa.

A su vez, la red semántica destaca la resistencia cultural como otro factor clave que ralentiza el proceso de adopción de las TIC dentro del personal militar. Esta resistencia se refleja en los vínculos entre la subcategoría "Resistencia Cultural" y patrones como "Desconfianza en Nuevas Tecnologías" y "Falta de Familiaridad". Los entrevistados mencionaron que, si bien algunos miembros del personal militar comprenden la importancia de las TIC, existe un escepticismo generalizado hacia su uso, lo que sugiere que la integración de nuevas tecnologías enfrenta barreras psicológicas y de actitud que requieren ser abordadas. Este hallazgo resalta la necesidad de un enfoque de gestión del cambio cultural que se enfoque no solo en los aspectos técnicos, sino también en la sensibilización y capacitación del personal para garantizar una transición exitosa hacia la adopción de las TIC.

La red semántica también muestra que, a pesar de la planificación formal para la implementación de las TIC, los procesos siguen siendo fragmentados y carecen de una visión estratégica integral. Las conexiones entre las subcategorías "Desajustes en la Integración" y

"Falta de Protocolos de Detección" con patrones como "Capacitación Insuficiente" y "Falta de Recursos" reflejan una falta de coordinación y coherencia en las intervenciones. En muchos casos, las iniciativas tecnológicas se implementan sin una planificación clara y sin un enfoque holístico que asegure su integración fluida en los procedimientos operativos del personal militar. Este patrón destaca la necesidad de contar con un marco normativo y una planificación a largo plazo que guíen las intervenciones tecnológicas de manera coherente con los objetivos estratégicos.

Un aspecto crucial identificado en la red semántica es la falta de capacitación continua para el personal militar, lo que limita su capacidad para utilizar plenamente las tecnologías disponibles. Las conexiones entre las subcategorías "Falta de Familiaridad" y "Capacitación Insuficiente" con los patrones "Dudas sobre Efectividad" y "Falta de Recursos" subrayan que la formación no ha sido suficiente ni adaptada a las necesidades específicas del personal. Los entrevistados expresaron que la capacitación inicial no fue suficiente para que el personal adquiriera las habilidades necesarias para utilizar las TIC de manera efectiva. Esto resalta la necesidad de establecer programas de formación continua y de un acompañamiento adecuado para asegurar que las competencias digitales se mantengan actualizadas y se utilicen de manera efectiva en el desempeño de las funciones operativas.

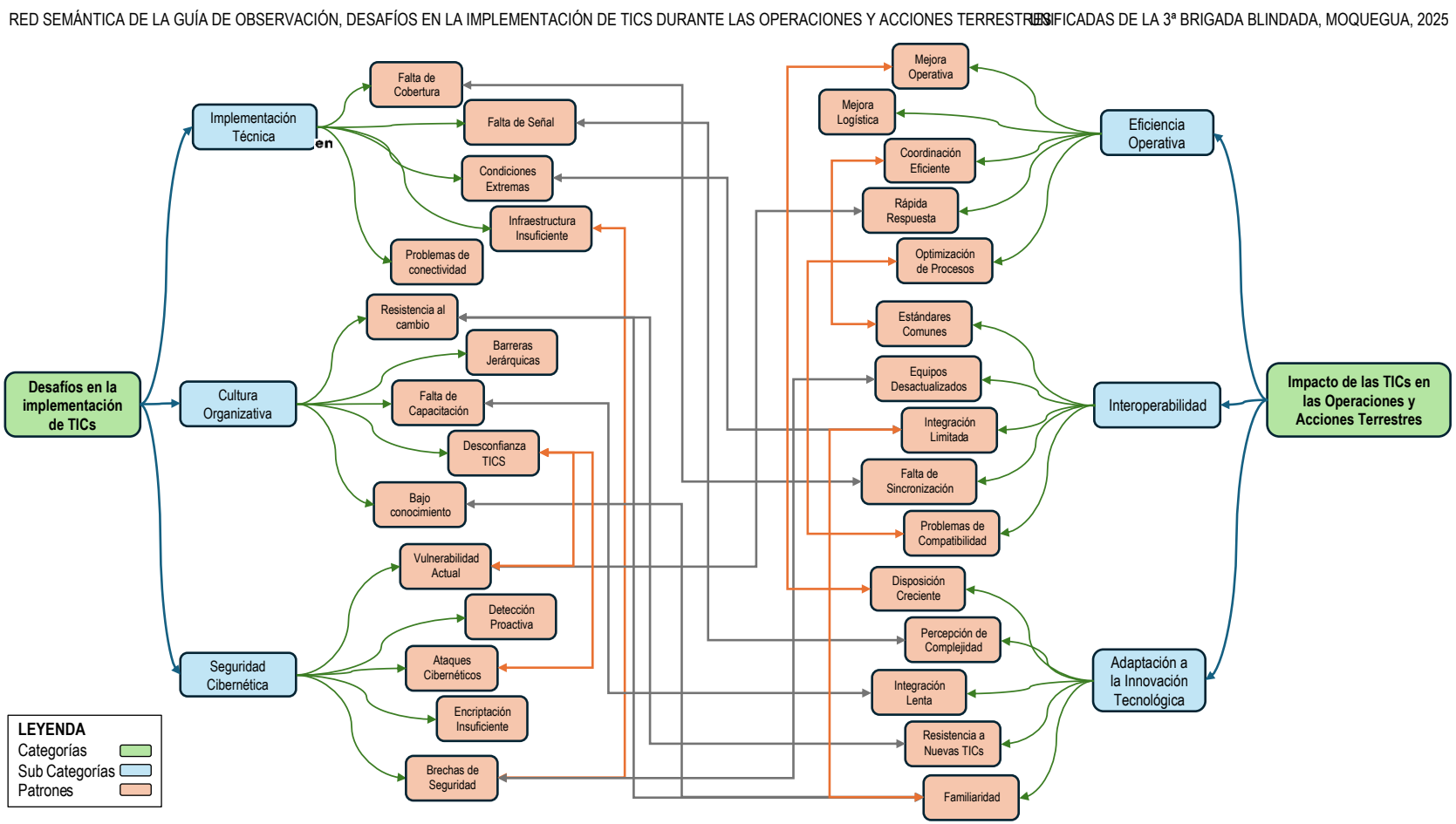
La red semántica también destaca que el proceso de adopción de las TIC no es un proceso lineal, sino que está lleno de desafíos, los cuales deben ser abordados de manera estratégica y adaptable. A pesar de las dificultades, los entrevistados reconocieron que las TIC ofrecen grandes oportunidades para mejorar la eficiencia operativa y la toma de decisiones en el campo militar. Sin embargo, la implementación de las TIC no puede ser exitosa sin superar las barreras culturales, estructurales y técnicas mencionadas. La red semántica pone de manifiesto cómo estos factores interrelacionados limitan el potencial de las TIC, creando un ciclo vicioso de adopción insuficiente.

Finalmente, el análisis de la red semántica resalta la importancia de adoptar un enfoque integral en la implementación de las TIC. No solo se deben considerar los aspectos tecnológicos, sino también los humanos, organizacionales y culturales. Los resultados obtenidos sugieren que una intervención efectiva debe ser más estructurada, con políticas claras, marcos normativos sólidos y una estrategia de capacitación adaptada a las necesidades específicas del personal militar. Este enfoque debe estar orientado a superar las barreras identificadas en la red semántica para garantizar una integración exitosa y sostenible de las TIC en las operaciones y acciones militares.

4.3.2. Red semántica de la guía de observación

Figura 2

Red semántica de la guía de observación



Nota: La figura, de elaboración propia empleando el software Python y las bibliotecas NetworkX, Matplotlib y NLTK, muestra la red semántica generada a partir del análisis cualitativo de la guía de observación de la presente investigación.

Explicación

A través del análisis de la red semántica generada a partir de las guías de observación, se identifican los principales desafíos y oportunidades en la implementación de las tecnologías de la información y la comunicación (TICs) en las operaciones de la 3ª Brigada Blindada. Los datos reflejan cómo las TICs afectan tanto la eficiencia operativa como la coordinación dentro de la brigada, a la vez que destacan las barreras culturales, técnicas y de seguridad que limitan su integración.

En cuanto a los desafíos en la implementación de TICs, la categoría "Implementación Técnica" muestra que las TICs enfrentan grandes dificultades en condiciones extremas, como las interferencias y la falta de cobertura en zonas remotas. Se destaca la necesidad de mejorar la infraestructura tecnológica, particularmente en áreas críticas, con el fin de garantizar la operatividad continua. Un enfoque dual que combine mejoras en infraestructura con tecnologías de conmutación adaptativa podría mejorar significativamente la funcionalidad de las TICs en estos entornos adversos.

En la resistencia cultural y organizativa, se observa que la adopción de nuevas tecnologías enfrenta obstáculos dentro del personal, debido a la falta de comprensión sobre los beneficios de las TICs. Aunque la resistencia es moderada, existen barreras en la cadena de mando que ralentizan la adopción de tecnologías. Un programa integral de capacitación basado en escenarios prácticos y una reestructuración organizacional más flexible permitirían una transición cultural hacia la aceptación y el uso efectivo de las TICs.

La seguridad cibernética es otro factor clave que limita la implementación de las TICs. Se observa que los sistemas de seguridad actuales son vulnerables a amenazas avanzadas. Se recomienda implementar inteligencia artificial (IA) para detectar proactivamente los patrones de ataque y utilizar sistemas de encriptación robustos para proteger los datos críticos en operaciones. Estos cambios permitirían una defensa más rápida y efectiva contra ciberataques.

En cuanto al impacto de las TICs en las operaciones terrestres, se ha identificado que las TICs mejoran la eficiencia operativa, especialmente en áreas como la logística y la comunicación en tiempo real. Sin embargo, la falta de soporte técnico constante en campo y problemas de conectividad en zonas remotas limitan la continuidad de estas mejoras. Para abordar estos problemas, se recomienda el uso de estaciones móviles de respaldo en áreas críticas, lo que garantizaría una operatividad más estable.

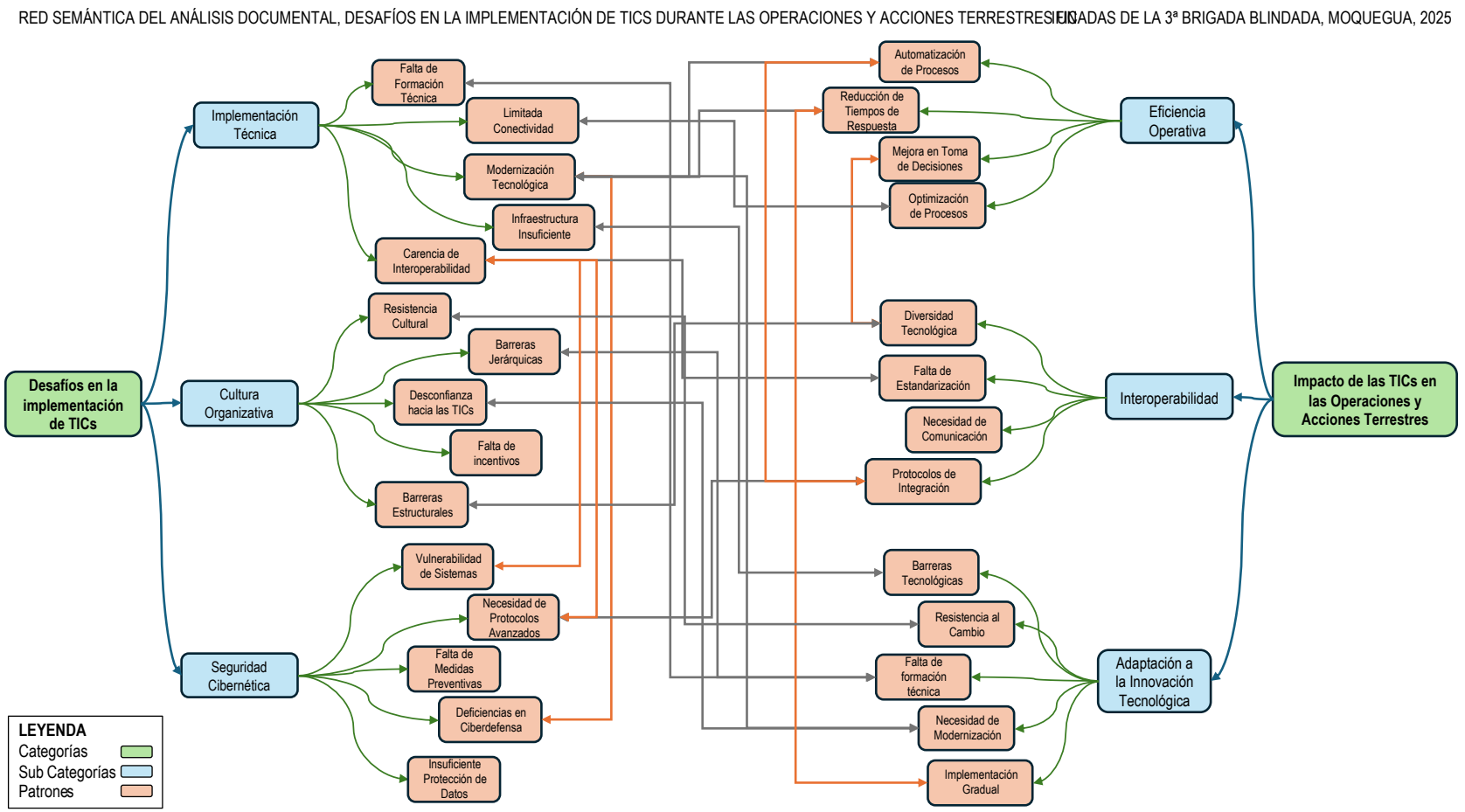
La interoperabilidad ha mejorado gracias a las TICs, pero la falta de estandarización crea dificultades, especialmente en operaciones multinacionales. Se sugiere implementar estándares de comunicación unificados y actualizar progresivamente el equipo, lo que permitiría mejorar la sincronización y cooperación entre unidades y con aliados.

Finalmente, la adaptación a la innovación tecnológica dentro de la brigada muestra una disposición creciente del personal a adoptar nuevas tecnologías, especialmente después de entrenamientos prácticos. No obstante, la percepción de complejidad de las TICs avanzadas genera una transición lenta. Un enfoque que combine programas continuos de actualización con un modelo de mentoría, donde personal experimentado guíe a los nuevos usuarios, aceleraría el proceso de adopción y aseguraría el uso efectivo de las TICs avanzadas en las operaciones.

4.3.3. Red semántica de la guía de análisis documental

Figura 3

Red semántica de la guía de análisis documental



Nota: La figura, de elaboración propia empleando el software Python y las bibliotecas NetworkX, Matplotlib y NLTK, muestra la red semántica generada a partir del análisis cualitativo de la guía de observación de la presente investigación.

Explicación

A través del análisis de la red semántica generada a partir de la ficha de análisis documental, se identifican los principales desafíos y el impacto de la implementación de las Tecnologías de la Información y Comunicación (TICs) en las operaciones de la 3a Brigada Blindada. Este análisis, basado en los documentos clave analizados, revela tanto los obstáculos que enfrenta la institución como las áreas en las que las TICs pueden tener un impacto positivo en su capacidad operativa.

La categoría Desafíos en la Implementación de TICs aborda tres áreas críticas. En primer lugar, la Implementación Técnica muestra que la falta de infraestructura adecuada y la carencia de formación técnica especializada son barreras significativas para la adopción efectiva de las TICs en las operaciones militares. El Decreto Supremo N° 085-2023-PCM y el Decreto Supremo N° 009-2021-PCM proporcionan las bases para la transformación digital, pero las fuerzas armadas aún enfrentan dificultades en la modernización tecnológica debido a estas limitaciones. La Directiva Única de Funcionamiento del Sistema de Telemática del Ejército (DUFSITELE, 2021) también destaca la importancia de la interoperabilidad para garantizar una integración efectiva de los sistemas de telecomunicaciones en el ámbito militar.

La Implementación Cultural y Organizativa es otro desafío importante, ya que la resistencia cultural dentro del Ejército y la falta de incentivos institucionales dificultan la transición hacia una mayor digitalización. La Directiva N° 001-2019-PCM señala que las barreras culturales y organizacionales, sumadas a la falta de capacitación estructurada, han ralentizado la adopción de nuevas tecnologías, generando desconfianza en su aplicabilidad dentro del entorno operativo militar.

En cuanto a la Seguridad Cibernética, la red semántica identifica que las vulnerabilidades en los sistemas de protección de datos y las infraestructuras digitales de las fuerzas armadas representan un riesgo significativo. La Política Nacional de Ciberseguridad, junto con el Decreto Supremo N° 012-2024-PCM, establece los lineamientos para fortalecer las capacidades de

ciberdefensa, pero aún se necesita mejorar los protocolos de seguridad para mitigar el riesgo de ciberataques en las operaciones militares.

En relación con el impacto de las TICs en las operaciones militares, la eficiencia operativa ha mejorado considerablemente a través de la digitalización de procesos administrativos y la automatización de procedimientos, como se indica en el Decreto Supremo N° 009-2021-PCM. Estos avances han permitido reducir los tiempos de respuesta y mejorar la toma de decisiones estratégicas. Sin embargo, el análisis también muestra que la interoperabilidad sigue siendo un reto debido a la diversidad tecnológica que existe entre las unidades militares. El Manual MACOFFAA (2019) subraya la necesidad de protocolos de comunicación estándar para mejorar el intercambio de información y asegurar una mayor eficacia en las operaciones conjuntas.

La adaptación a la innovación tecnológica se presenta como una necesidad crítica para mantener la competitividad operativa. La Directiva DUFSITELE (2021) resalta la importancia de la modernización continua de los sistemas de telecomunicaciones, pero se identifican barreras como la falta de formación técnica específica que impide la integración completa de nuevas herramientas digitales. La implementación de entornos de simulación digital se menciona como una estrategia para facilitar una adaptación progresiva a las innovaciones tecnológicas en las operaciones militares.

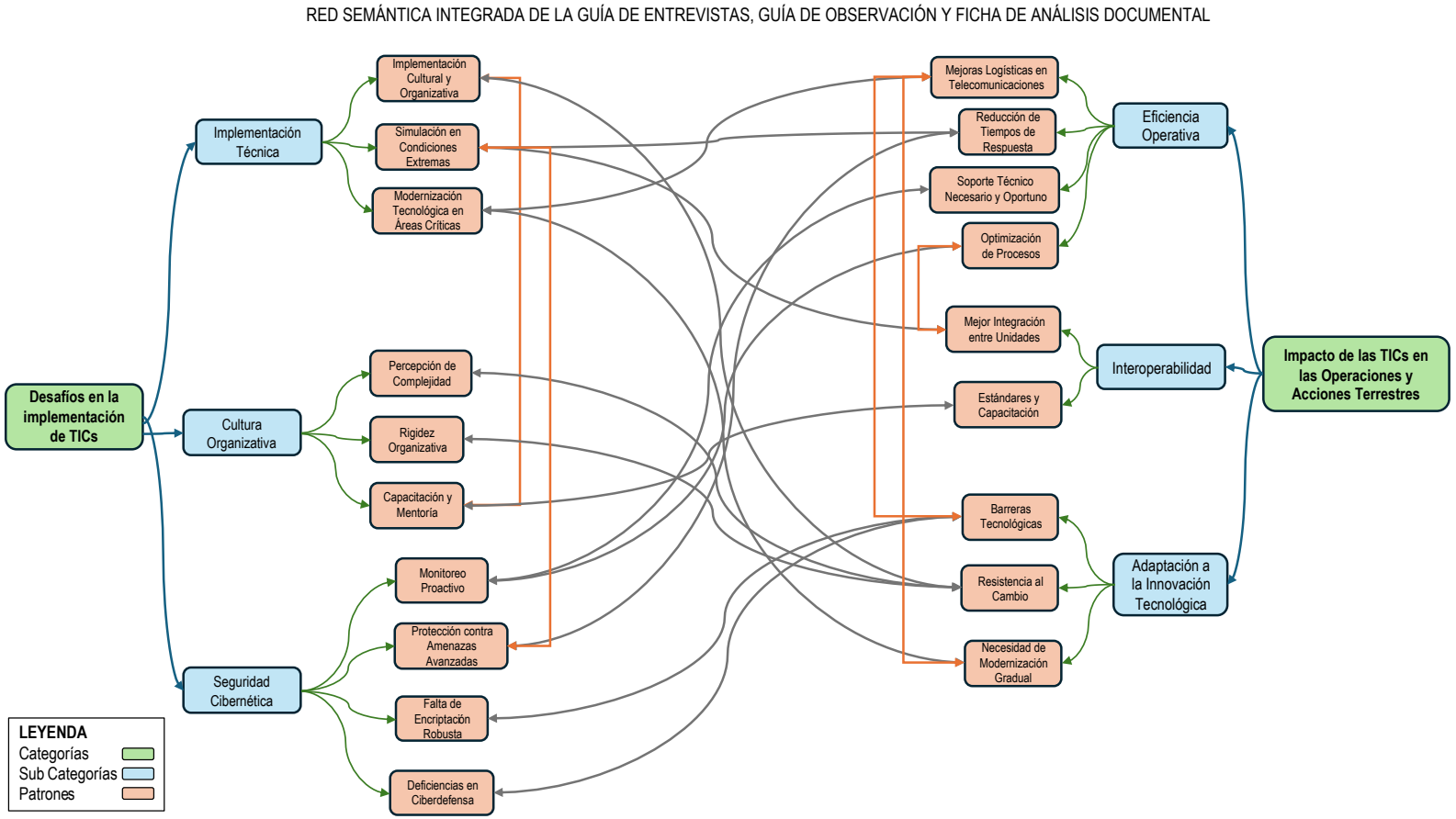
Los patrones clave extraídos de los documentos y reflejados en la red semántica indican que los desafíos técnicos, como la falta de infraestructura y la necesidad de capacitación técnica, son áreas críticas que deben ser abordadas para garantizar una implementación efectiva de las TICs. La resistencia cultural y organizativa dentro de las fuerzas armadas, alimentada por la falta de incentivos institucionales, sigue siendo un obstáculo importante para la adopción de TICs. La seguridad cibernética es otra área que requiere atención urgente, ya que la falta de protocolos adecuados pone en riesgo la integridad de las operaciones. Por otro lado, la digitalización de procesos ha demostrado mejoras significativas en la eficiencia operativa, aunque aún persisten problemas de interoperabilidad debido a la diversidad tecnológica. La necesidad de un enfoque

estandarizado en los sistemas utilizados por las fuerzas armadas sigue siendo un desafío relevante para mejorar la coordinación y la eficacia de las operaciones conjuntas.

4.3.4. Integración de las redes semánticas

Figura 4

Integración de las redes semánticas



Nota: La figura, de elaboración propia empleando el software Python y las bibliotecas NetworkX, Matplotlib y NLTK, muestra la red semántica integrada a partir del análisis cualitativo de la guía de entrevistas, guía de observación y ficha de análisis documental.

Explicación

A través del análisis de la red semántica derivada de la integración de la guía de entrevista, guía de observación y ficha de análisis documental, se evidencian los efectos transformadores de las Tecnologías de la Información y Comunicación (TICs) en las operaciones y acciones militares del Ejército del Perú. La incorporación de las TICs optimiza la eficiencia operativa, mejorando la coordinación en tiempo real y la toma de decisiones tácticas y estratégicas. El uso de sistemas de comunicación segura y herramientas de mapeo avanzado facilita un control más efectivo sobre los recursos y el campo de batalla, contribuyendo a la optimización logística y la ejecución de las acciones militares.

Sin embargo, uno de los desafíos principales es la interoperabilidad entre diferentes unidades y sistemas. Aunque las TICs han mejorado la comunicación interunidades, la falta de estandarización de los sistemas de comunicación sigue siendo una barrera significativa, lo que limita la sincronización de las operaciones. Es crucial establecer protocolos unificados que permitan la integración plena de los diferentes sistemas empleados por las fuerzas militares.

La adaptación a nuevas tecnologías es otro factor decisivo. La red semántica resalta que la capacitación constante del personal es vital para asimilar y utilizar eficazmente las nuevas herramientas tecnológicas. La resistencia al cambio y la falta de experiencia con tecnologías avanzadas pueden ralentizar su implementación, pero a través de entrenamientos prácticos y la integración gradual de tecnologías emergentes, se facilita la transición hacia un modelo de acción militar más digitalizado y ágil.

Finalmente, los patrones recurrentes observados en la red muestran que, aunque persisten ciertos desafíos, las TICs tienen un impacto positivo y sostenido en la capacidad operativa del Ejército del Perú, permitiendo una respuesta más rápida y efectiva ante situaciones críticas. La monitorización constante y la protección de las comunicaciones son elementos esenciales para mantener la eficacia operativa en escenarios de conflicto o en condiciones extremas. En resumen, las TICs representan un elemento fundamental para potenciar las

capacidades de las operaciones y acciones militares, mejorando la resiliencia frente a amenazas cibernéticas y optimizando los recursos logísticos.

4.4. Triangulación

Tabla 6

Triangulación por técnicas de recolección de datos

CATEGORÍA	SUBCATEGORÍAS	ENTREVISTAS	OBSERVACIÓN	DOCUMENTOS	SÍNTESIS INTEGRADA
Desafíos en la Implementación de TICs	Implementación Técnica	- Las entrevistas destacan que las TICs no están suficientemente preparadas para entornos de alta interferencia y dificultades técnicas, como áreas con terreno accidentado y remotas. Esto requiere adaptaciones tecnológicas como sistemas de conmutación en tiempo real. Se menciona que las TICs son más efectivas si se combinan con tecnologías de redundancia de	- Las observaciones reflejan que la infraestructura actual no soporta eficazmente la carga de las TICs en situaciones operativas extremas. La cobertura es insuficiente en zonas clave, como zonas rurales o de difícil acceso. La integración de antenas de alta ganancia y el uso de redes de baja latencia se destacan como soluciones imprescindibles. La resistencia de la	- El Decreto Supremo N° 085-2023-PCM establece un marco para la transformación digital en el sector público y en operaciones militares. Los documentos analizados señalan que la transformación digital debería priorizar la infraestructura tecnológica adecuada, especialmente en zonas remotas. En este contexto, el Decreto Supremo N° 140-2020-PCM resalta la necesidad de actualizar las telecomunicaciones en áreas críticas. El Decreto Supremo N°	La implementación de TICs enfrenta desafíos técnicos principalmente por la insuficiencia de infraestructura para soportar nuevas tecnologías en condiciones extremas. Se requiere un enfoque integral que combine soluciones tecnológicas de vanguardia, como sistemas de conmutación y redundancia de señal, con la actualización de infraestructuras existentes. Los

		señal para garantizar la conectividad, especialmente en situaciones de guerra electrónica o en zonas de alta interferencia.	infraestructura se percibe como una barrera crítica que limita el uso eficiente de las TICs en operaciones de campo.	004-2020-PCM establece lineamientos para mejorar la conectividad en zonas difíciles.	documentos legales y normativos resaltan la importancia de la modernización tecnológica, pero también advierten sobre los limitantes del entorno actual.
	Cultural Organizativa	- Las entrevistas apuntan a una fuerte resistencia cultural hacia la adopción de TICs, principalmente por la falta de comprensión de los beneficios operativos. Muchos miembros del personal no visualizan a las TICs como una herramienta para mejorar su eficiencia, sino como una carga adicional. La capacitación estructurada en el	- Las observaciones revelan que la resistencia cultural no solo se encuentra a nivel de los operativos, sino también a nivel de mando. La rigidez organizativa genera que los procesos de toma de decisiones sean más lentos. Se destaca la necesidad de flexibilizar las estructuras jerárquicas para facilitar la aceptación y	- La Directiva N° 001-2019-PCM identifica la resistencia cultural como una de las barreras más significativas para la implementación exitosa de TICs en el sector público. Los documentos subrayan que es fundamental implementar programas de capacitación y sensibilización, combinados con incentivos para fomentar la aceptación. Además, se recomienda una reestructuración	La resistencia cultural y organizativa sigue siendo un obstáculo central para la implementación de TICs. La clave para superar esta barrera radica en un enfoque integral que incluya formación continua, incentivos institucionales y una reestructuración organizacional para fomentar la adaptación rápida

		uso de TICs es vista como fundamental para superar esta resistencia, especialmente cuando se demuestra de manera práctica cómo las TICs pueden optimizar operaciones diarias.	adopción de las TICs. Además, la falta de un plan claro para la transición digital aumenta la desconfianza hacia estas tecnologías. La falta de incentivos institucionales es otra barrera destacada.	organizacional para facilitar una transición más ágil hacia la adopción tecnológica.	y efectiva. La capacitación práctica, basada en escenarios reales, es crucial para cambiar la mentalidad del personal.
	Seguridad Cibernética	- Vulnerabilidades y protección de datos: En las entrevistas, se destacan las vulnerabilidades de los sistemas actuales, especialmente en cuanto a la protección de datos en comunicación táctica y redes críticas. Se propone el uso de inteligencia artificial para la detección anticipada de ciberataques, así	- Falta de sistemas de respuesta rápida: Las observaciones confirman que los sistemas actuales de ciberseguridad están desactualizados y son incapaces de detectar amenazas avanzadas en tiempo real. Las vulnerabilidades de los sistemas de microondas y las redes móviles son áreas críticas. Se recomienda la	- Marco normativo de ciberseguridad: La Ley N° 30999 y el Política Nacional de Ciberseguridad presentan un enfoque proactivo frente a los riesgos de ciberseguridad. La ley establece un marco normativo para la protección de infraestructuras críticas, y el plan resalta la importancia de los sistemas de IA para anticipar ciberataques y mejorar la resiliencia	La ciberseguridad es una de las áreas críticas en la implementación de TICs. Es necesario un enfoque preventivo que combine la encriptación avanzada, la inteligencia artificial para la detección proactiva de amenazas y sistemas automatizados de respuesta rápida.

		como la implementación de protocolos de encriptación más avanzados para salvaguardar la integridad de los datos. El uso de IA podría ayudar a detectar patrones de ataque antes de que ocurran.	incorporación de sistemas de detección automáticos y de protocolos de encriptación más sólidos para mejorar la seguridad. Además, se mencionan las brechas en la capacidad de respuesta ante ataques sofisticados, lo que exige un sistema de reacción más ágil y efectivo.	de las redes. El Decreto Supremo N° 012-2024-PCM también establece medidas para fortalecer la seguridad cibernética, incluyendo el uso de la autenticación multicapa y protocolos de encriptación más robustos.	La normativa existente está alineada con estos objetivos, pero los sistemas actuales aún tienen brechas significativas que deben ser abordadas para mejorar la seguridad integral de las operaciones.
Impacto de las TICs en Operaciones Terrestres	Eficiencia Operativa	- Las entrevistas indican que las TICs han mejorado significativamente la capacidad de coordinarse en tiempo real, facilitando una toma de decisiones más rápida y eficiente. No obstante, se resalta que la falta de soporte técnico constante limita el	- Las observaciones reflejan que las TICs han optimizado la logística y la comunicación, pero la conectividad en zonas remotas sigue siendo un desafío. Las TICs han permitido una mejor coordinación, pero los problemas	- El Decreto Supremo N° 009-2021-PCM establece que la digitalización de procesos administrativos es fundamental para mejorar la eficiencia operativa en el sector público y militar. La automatización y la digitalización permiten reducir los tiempos de respuesta y optimizar	Las TICs han demostrado tener un impacto positivo en la eficiencia operativa, especialmente en la logística y la coordinación en tiempo real. Sin embargo, las limitaciones de infraestructura en zonas remotas y la

		impacto de estas mejoras. En áreas de alta interferencia, el soporte técnico y la infraestructura adecuada son esenciales para mantener la operatividad.	de conectividad en terrenos difíciles aún afectan la rapidez de la toma de decisiones. Las estaciones móviles de respaldo y la implementación de redes redundantes son recomendaciones claves para asegurar que la eficiencia operativa no se vea comprometida.	los recursos disponibles para la toma de decisiones estratégicas.	falta de soporte técnico en campo afectan la continuidad y efectividad de estas mejoras. Se requiere de un enfoque integral que combine infraestructura robusta, soporte técnico y estrategias de redundancia en las redes para garantizar el éxito en el largo plazo.
	Interoperabilidad	- En las entrevistas se reconoce que la interoperabilidad ha mejorado, pero los problemas de sincronización entre equipos de diferentes generaciones y protocolos siguen siendo un desafío. Se proponen soluciones como la actualización progresiva de	- Las observaciones confirman que la falta de estandarización entre unidades genera dificultades en las operaciones y acciones militares. La diversidad de tecnologías y protocolos crea barreras para la coordinación	- El Manual MACOFFAA (2019) establece que la interoperabilidad es esencial para el éxito en las operaciones. Para ello, es necesario adoptar un enfoque de estandarización de equipos y protocolos de comunicación. El manual sugiere que, a través de pruebas conjuntas y	Aunque la interoperabilidad ha mejorado, sigue siendo un desafío importante debido a la falta de estandarización de los equipos y los protocolos. Es fundamental que se implementen procesos de actualización progresiva y protocolos de

		equipos y la implementación de protocolos unificados de comunicación. Además, se destaca la necesidad de entrenamiento cruzado para garantizar que las unidades trabajen juntas de manera eficiente.	efectiva en entornos complejos. Es fundamental establecer normas de interoperabilidad y protocolos de comunicación unificados para resolver este problema.	capacitación cruzada, las unidades pueden mejorar su coordinación y sincronización.	comunicación unificados, además de capacitación cruzada para mejorar la integración de las unidades.
	Adaptación a la Innovación Tecnológica	- En las entrevistas se señala que, aunque la disposición a adoptar nuevas tecnologías ha aumentado, la transición sigue siendo lenta. Se destaca que las TICs son vistas por muchos como complejas, y se necesita un enfoque continuo de formación para mejorar su adopción. La falta	- Las observaciones sugieren que el personal está dispuesto a adoptar nuevas tecnologías, pero la percepción de que estas son demasiado complejas genera incertidumbre. La capacitación continua y el soporte técnico son fundamentales para superar esta barrera. Se sugiere que los programas	- La DUFSITELE (2021) resalta la necesidad de mantener actualizados los sistemas de telecomunicaciones, pero también advierte sobre las barreras de adaptación tecnológica. La directiva subraya que la adaptación tecnológica es un proceso continuo que debe incluir programas de actualización y simulaciones para	La adaptación tecnológica puede ser acelerada mediante programas de formación continua, simulaciones prácticas y un modelo de mentoría. Es fundamental que las TICs se integren de manera progresiva, permitiendo que el personal se

	de experiencia con tecnologías avanzadas en el personal es otra barrera significativa.	de formación se centren en la familiarización gradual con las TICs avanzadas para facilitar su uso efectivo.	garantizar el dominio de las TICs en situaciones operativas.	familiarice con las nuevas herramientas y tecnologías antes de su implementación total.

Nota: La presente tabla, de elaboración propia, muestra la Triangulación de técnicas de datos de la presente investigación.

CAPÍTULO V: DIÁLOGO TEÓRICO - EMPÍRICO

En función del Objetivo General (OG), se han identificado diversas barreras y oportunidades que influirán en la efectividad de estas tecnologías. El análisis de las mismas, permitirá mejorar la capacidad operativa de la brigada y fortalecer la seguridad en el entorno cibernético, lo que requiere una actualización tanto de las infraestructuras tecnológicas como de las capacidades operativas.

Uno de los principales obstáculos encontrados es la insuficiencia de la infraestructura tecnológica, especialmente en áreas de difícil acceso. Durante las entrevistas con los oficiales, se destacó que “las TICs no están preparadas para operar en terrenos difíciles o en zonas con alta interferencia”. Este problema fue confirmado en las observaciones realizadas durante los ejercicios operacionales, en los cuales se evidenció que la cobertura en áreas rurales y desérticas es insuficiente, lo que limita la efectividad de las TICs en estos entornos. Este hallazgo se alinea con lo que menciona Yataco (2020) en su investigación sobre la optimización de sistemas de vigilancia en zonas fronterizas, donde señala que la falta de infraestructura en áreas remotas impacta negativamente en la efectividad de las TICs. En este contexto, la integración de nuevas tecnologías, como redes de baja latencia y sistemas de redundancia de señal, es crucial para superar estas limitaciones.

A nivel cultural y organizacional, las entrevistas revelaron una fuerte resistencia hacia la adopción de las TICs, especialmente entre los oficiales de mayor antigüedad, quienes consideran que estas tecnologías son más una carga que una herramienta para mejorar la eficiencia operativa. Un oficial mencionó que “muchos prefieren seguir utilizando métodos tradicionales en lugar de adoptar nuevas tecnologías”. Esta resistencia, que también fue observada en el campo en sus ejercicios de comunicaciones, coincide con la Teoría de la Resistencia al Cambio de Dent y Goldberg (1999), que destaca cómo las organizaciones jerárquicas, como las fuerzas armadas, tienden a resistirse a la implementación de nuevas tecnologías que alteran las estructuras establecidas. Este fenómeno está relacionado con la falta de comprensión de los beneficios operativos de las TICs. Según Vicaña y Chafloque (2021), un sistema de comando y control eficiente es esencial para las operaciones, pero este sistema requiere que las organizaciones sean flexibles y adaptables a la tecnología. Para superar esta resistencia, es crucial implementar programas de capacitación que demuestren cómo las TICs pueden optimizar las operaciones

diarias, lo cual se alinea con los principios de Kotter (1996) en su Teoría de la Gestión del Cambio, que establece que la implementación de nuevas tecnologías debe ir acompañada de un proceso de sensibilización y formación estructurada.

En cuanto a la ciberseguridad, las entrevistas destacaron que los sistemas actuales son insuficientes para proteger la información crítica durante las operaciones, lo cual es un riesgo importante. Se mencionó que “aunque tenemos protocolos básicos de seguridad, los ciberataques avanzados siguen siendo una amenaza”. Esta vulnerabilidad coincide con lo que señala Huamán Baltazar (2021) sobre las brechas en la ciberseguridad en las unidades militares peruanas, que aún están en proceso de desarrollo. Además, Casale (2022) resalta la importancia de la ciberdefensa como un factor crítico para proteger las infraestructuras militares de los ciberataques, subrayando la necesidad de contar con un marco legal y tecnológico actualizado. En este sentido, la implementación de inteligencia artificial para la detección temprana de ciberamenazas, como sugieren Raver4 (2023) y Montes Vallejo (2022), sería clave para fortalecer la protección de las TICs en las operaciones de la brigada.

En cuanto al impacto de las TICs en la eficiencia operativa, las entrevistas indicaron que estas tecnologías han mejorado la coordinación y toma de decisiones en tiempo real, pero la falta de soporte técnico adecuado sigue siendo un obstáculo. Como señaló uno de los oficiales, “aunque las TICs nos han ayudado en la coordinación, la falta de soporte técnico constante limita la operatividad”. Este hallazgo coincide con lo que Saltos Narváez (2021) y Montes Vallejo (2022) mencionan sobre la necesidad de actualizar continuamente los equipos y entrenar a los usuarios para mantener la eficiencia operativa. Además, Villarrubia (2021) en su investigación sobre las tecnologías emergentes como el 5G, destaca que este tipo de tecnologías avanzadas pueden facilitar la integración de dispositivos y optimizar la toma de decisiones en tiempo real, pero su implementación enfrenta desafíos en términos de ciberseguridad y adaptabilidad de los sistemas existentes.

En función del Objetivo Específico 1 (OE1), la investigación reveló que una de las principales barreras para la implementación efectiva de las TICs es la insuficiencia de infraestructura tecnológica, especialmente en áreas rurales y de difícil acceso.

De acuerdo con los datos obtenidos de las entrevistas, los oficiales han mencionado de manera recurrente que la infraestructura actual no es suficiente para cubrir las necesidades operativas de la brigada, lo que impide un uso óptimo de las TICs, especialmente en entornos de alta interferencia y terrenos accidentados. Un oficial expresó que “la infraestructura de comunicación en las zonas rurales es deficiente y no soporta las tecnologías que necesitamos implementar”, lo que limita directamente las capacidades operativas de la brigada. Este desafío

se alinea con lo señalado en la investigación de Yataco (2020), quien también destaca cómo la falta de infraestructura adecuada afecta la capacidad de respuesta en áreas de difícil acceso, lo que impide una efectiva implementación de tecnologías avanzadas.

Las observaciones en el campo corroboraron estas afirmaciones, pues se constató que la cobertura es insuficiente en áreas críticas, como las zonas desérticas o de terreno accidentado. La necesidad de una infraestructura robusta que permita una cobertura continua y confiable en todas las zonas operativas es urgente. En este contexto, Quinto Huamán y Picón Huacarpuma (2023) apuntan que uno de los principales retos en las fuerzas armadas peruanas es la infraestructura tecnológica, que debe ser capaz de soportar el almacenamiento y procesamiento de datos a gran escala para asegurar la eficiencia operativa, algo que se refleja claramente en la situación de la brigada. La falta de una infraestructura robusta y actualizada impide que las TICs puedan desempeñar su función de manera efectiva en el contexto militar.

La Teoría de la Gestión del Cambio de Kotter (1996) se muestra particularmente relevante para comprender cómo abordar estas limitaciones. Según Kotter, la implementación de cambios organizacionales exitosos, como la modernización de la infraestructura tecnológica, debe ser un proceso estructurado que considere la creación de un sentido de urgencia, la formación de coaliciones para apoyar el cambio y la integración de nuevas prácticas. En este caso, para superar las barreras tecnológicas en la brigada, es esencial no solo modernizar la infraestructura, sino también gestionar el cambio dentro de la organización, facilitando la transición hacia un modelo tecnológico más avanzado. En cuanto a las soluciones planteadas, las entrevistas sugieren que la implementación de tecnologías avanzadas, como redes de baja latencia, y la incorporación de sistemas de comunicación satelital más robustos, podrían mejorar significativamente la conectividad en áreas remotas. La incorporación de estas tecnologías también fue mencionada por Villarrubia (2021), quien sostiene que el uso del 5G, por ejemplo, puede transformar las operaciones tácticas al proporcionar comunicaciones más rápidas y seguras, una solución que podría ser crucial para las necesidades de la brigada. Esto se alinea con lo indicado por Briones (2021), quien resalta la importancia de contar con un sistema de mando y control (C2) eficaz respaldado por una infraestructura tecnológica moderna, para mejorar las capacidades operativas y la toma de decisiones, sin embargo, para que estas tecnologías sean eficaces, es necesario superar los problemas de interoperabilidad entre los sistemas existentes y las nuevas plataformas tecnológicas, Casale (2022) subraya que las capacidades de ciberdefensa deben ser mejoradas para proteger estas nuevas tecnologías contra amenazas externas, lo cual es esencial para garantizar la seguridad y continuidad de las operaciones militares. De hecho, los oficiales de la brigada señalaron que la falta de

ciberseguridad adecuada es un factor limitante para la implementación exitosa de las TICs, ya que sin la protección adecuada, las nuevas tecnologías no serían viables en el entorno operativo, además, la Teoría de la Aceptación de Tecnología de Davis (1989) también es crucial para entender cómo los miembros de la brigada pueden percibir la utilidad y facilidad de uso de las TICs. Si los oficiales y el personal militar no perciben las nuevas tecnologías como útiles o fáciles de usar, podrían resistirse a su adopción, lo que dificultaría la implementación de sistemas avanzados. En este sentido, la capacitación continua y la demostración práctica de la eficacia de las TICs en situaciones reales de combate son fundamentales para fomentar la aceptación de estas tecnologías y asegurar su integración exitosa en las operaciones de la brigada.

En función del Objetivo Específico 2 (OE2), los resultados obtenidos de las entrevistas, observaciones y análisis documental reflejan que la formación del personal es uno de los principales desafíos en la implementación efectiva de estas tecnologías. Las entrevistas con oficiales de la brigada destacaron que, aunque existen recursos tecnológicos a disposición, el personal no ha recibido una capacitación adecuada ni continua en el uso de estos sistemas. Un oficial señaló: “Aunque contamos con las herramientas necesarias, no siempre sabemos cómo emplearlas de manera efectiva, necesitamos más capacitación”. Este comentario resalta una problemática que limita la integración de las TICs en las operaciones de la brigada, ya que sin una capacitación adecuada, las tecnologías disponibles pierden su potencial de mejora operativa. Este hallazgo se encuentra en línea con lo indicado por Briones (2021) en su investigación sobre las capacidades de Comando y Control (C2) de la 3ra Brigada de Caballería. Briones subraya que la capacidad del sistema de C2 de la brigada está limitada por la escasez de desarrollo en las capacidades operativas necesarias para respaldar la tecnología, especialmente en lo que respecta a la capacitación del personal. Al igual que en la brigada estudiada por Briones, la 3ª Brigada Blindada enfrenta el mismo desafío: a pesar de contar con las herramientas necesarias, la falta de formación continua y especializada en el uso de estos sistemas impide que el personal utilice eficazmente las TICs en las operaciones.

Las observaciones directas realizadas durante los ejercicios de comunicaciones también confirmaron que, si bien algunos oficiales de la brigada tienen conocimientos básicos sobre el uso de las TICs, no se sienten completamente preparados para integrar estas tecnologías en un contexto de alta presión o en situaciones de guerra real. En este sentido, los problemas de conexión en zonas remotas y de alta interferencia, identificados en la Tabla 6, son exacerbados por la falta de formación en la resolución de estos desafíos tecnológicos en el campo. Por ejemplo, la falta de apoyo técnico constante y la infraestructura insuficiente en áreas de difícil acceso agravan la situación, limitando la efectividad de las TICs en estas zonas. Las entrevistas

también destacaron que la capacitación debe ser continua y no solo técnica, sino también táctica, orientada a situaciones de combate, para asegurar que el personal pueda manejar eficientemente los sistemas bajo presión.

El análisis documental también ha sido revelador en cuanto a la planificación y las políticas institucionales de formación. Los documentos revisados, como el Decreto Supremo N° 085-2023-PCM y el Decreto Supremo N° 140-2020-PCM, indican que existe una falta de alineación entre las políticas de modernización tecnológica y la capacitación del personal en el uso de nuevas tecnologías. Estos documentos resaltan la necesidad de una infraestructura adecuada y actualizada, pero también advierten sobre la insuficiencia de programas de formación especializados que capaciten a los oficiales y al personal subalterno en el uso de sistemas avanzados de C2 y en la integración de las TICs. En este sentido, Vicaña y Chafloque (2021) recalcan que la capacitación sobre el sistema de C2 debe ser continua y que debe permitir a los oficiales y soldados utilizar la tecnología para mejorar la toma de decisiones y optimizar la coordinación en tiempo real.

En términos teóricos, el Modelo de Aceptación de Tecnología (TAM) de Davis (1989) es crucial para comprender la falta de aceptación de las TICs dentro de la brigada. Según este modelo, la adopción de nuevas tecnologías depende de dos factores principales: la utilidad percibida y la facilidad de uso percibida. En este contexto, la falta de capacitación en el uso de las TICs en situaciones reales de combate podría generar una percepción negativa en cuanto a la utilidad y facilidad de uso de estas herramientas. Si los oficiales y el personal no perciben las TICs como herramientas útiles o accesibles, su disposición a adoptarlas se ve severamente afectada, por otro lado, la Teoría de la Resistencia al Cambio de Dent y Goldberg (1999) explica cómo las estructuras jerárquicas dentro de las fuerzas armadas, como en la 3ª Brigada Blindada, pueden resistirse a la adopción de nuevas tecnologías debido a la preferencia por métodos tradicionales. Este fenómeno se refleja en las entrevistas realizadas, donde algunos oficiales más experimentados expresaron dudas sobre la efectividad de las TICs en condiciones de combate, prefiriendo las metodologías de comando convencionales. Para superar esta resistencia, es esencial contar con un enfoque integral de gestión del cambio, como lo sugiere la Teoría de la Gestión del Cambio de Kotter (1996), que propone un proceso estructurado de ocho pasos para facilitar la adopción de nuevas tecnologías dentro de una organización. En este sentido, es crucial la creación de un sentido de urgencia, la formación de una coalición de líderes que apoyen la transición y la consolidación de nuevas prácticas mediante la integración de las TICs en la cultura organizacional, además, el Modelo de Capacidades Dinámicas de Teece et al. (1997) destaca la importancia de la flexibilidad organizacional y la capacidad de adaptación rápida a nuevas

tecnologías. En este caso, la brigada necesita fortalecer su capacidad de adaptación a las TICs mediante una actualización constante de las capacidades tecnológicas y la implementación de programas de formación continua, para asegurar que el personal esté preparado para enfrentar los desafíos que surgen en el campo de batalla. Según Teece et al., este enfoque permite que las organizaciones se mantengan competitivas y operativas frente a cambios rápidos en el entorno.

En función del Objetivo Específico 3 (OE3), se observa que las barreras culturales y organizacionales son elementos fundamentales que influyen de manera negativa en la integración de las tecnologías en las operaciones. Las entrevistas con oficiales de la brigada indicaron una fuerte resistencia hacia la adopción de las TICs, principalmente debido a la preferencia por los métodos tradicionales de mando y control (C2). Un entrevistado destacó que "en situaciones críticas, los sistemas tradicionales de comando y control son los que mejor conocemos y en los que confiamos, las nuevas tecnologías son vistas como algo arriesgado y complejo", esta resistencia cultural se encuentra en línea con lo propuesto por la Teoría de la Resistencia al Cambio de Dent y Goldberg (1999), que sostiene que las organizaciones jerárquicas, como las fuerzas armadas, enfrentan dificultades significativas cuando se intenta modificar sus estructuras de poder y rutinas. La introducción de nuevas tecnologías, como los sistemas automatizados de mando y control, genera una sensación de inseguridad en los oficiales de mayor antigüedad, quienes temen perder control sobre los procesos operativos. Además, la percepción de que las TICs son demasiado complejas o poco confiables en situaciones de combate es un factor adicional que fomenta la resistencia.

Las observaciones realizadas durante los ejercicios de comunicaciones corroboran esta resistencia. A pesar de las capacitaciones implementadas, los oficiales de mayor rango continuaron mostrando preferencia por métodos más tradicionales, y se evidenció una falta de disposición para cambiar los procesos establecidos. La falta de un plan claro para la transición hacia la digitalización y la falta de incentivos institucionales para fomentar este cambio se perciben como barreras importantes que refuerzan la desconfianza hacia las TICs, el Modelo de Aceptación de Tecnología (TAM) de Davis (1989) ofrece una explicación adicional sobre la resistencia observada. Según este modelo, la adopción de nuevas tecnologías depende de dos factores clave: la percepción de utilidad y la percepción de facilidad de uso. En el contexto de la 3ª Brigada Blindada, muchos oficiales no perciben las TICs como herramientas útiles para mejorar la eficiencia operativa, sino como un obstáculo adicional. La falta de familiaridad con la tecnología, sumada a la percepción de que el sistema tradicional es más sencillo y seguro, contribuye significativamente a la resistencia.

En términos de gestión del cambio, el Modelo de Gestión del Cambio de Kotter (1996) resalta la importancia de crear un sentido de urgencia y formar coaliciones de apoyo para facilitar la adopción de nuevas tecnologías. En el caso de la brigada, se debe establecer un liderazgo claro que impulse la adopción de TICs, destacando sus beneficios en términos de seguridad operativa, eficiencia en la toma de decisiones y rapidez en la comunicación. Kotter también propone que la formación de una visión compartida y la integración gradual de las TICs son esenciales para garantizar la aceptación de los cambios tecnológicos, además, el Modelo de Capacidades Dinámicas de Teece et al. (1997) puede aplicarse para abordar la necesidad de flexibilidad organizacional, según este modelo, la capacidad de una organización para adaptarse rápidamente a cambios en el entorno tecnológico es crucial para su competitividad y eficiencia operativa, en el caso de la 3ª Brigada Blindada, la adopción de TICs requiere una adaptación rápida y efectiva de las estructuras organizacionales, lo que implica no solo la actualización tecnológica, sino también un cambio en la mentalidad y la cultura de los oficiales. La brigada debe desarrollar la capacidad de integrar rápidamente las TICs a sus operaciones diarias, lo que les permitirá responder de manera más ágil a las amenazas y mejorar la eficiencia operativa.

En función del Objetivo Específico 4 (OE4), se ha identificado que la seguridad cibernética es uno de los aspectos más críticos que enfrenta la brigada en su proceso de modernización tecnológica. Durante las entrevistas realizadas a los oficiales, se destacó que “la infraestructura de ciberseguridad actual está lejos de ser suficiente para proteger nuestras comunicaciones y sistemas ante los riesgos de ciberataques”. Este comentario refleja una preocupación constante sobre las deficiencias en las capacidades de defensa cibernética, Casale (2022) subraya la importancia de la protección de las infraestructuras críticas en un contexto de creciente digitalización y conectividad en las fuerzas armadas. Según Casale, las operaciones militares se han vuelto vulnerables a amenazas cibernéticas que pueden afectar no solo las comunicaciones tácticas, sino también los sistemas de control y comando. Este enfoque es crucial para entender las dificultades de la brigada, ya que se enfrenta a desafíos similares en cuanto a la protección de datos sensibles, así como la capacidad de reaccionar ante ciberataques de alta sofisticación, las observaciones realizadas durante los ejercicios de comunicaciones también han revelado que los sistemas actuales de defensa cibernética son incapaces de detectar amenazas avanzadas en tiempo real. Las capacidades de respuesta ante ataques son limitadas, y los oficiales manifestaron la necesidad urgente de incorporar tecnologías más avanzadas para fortalecer la seguridad cibernética. Las entrevistas indicaron que “los sistemas actuales no cuentan con mecanismos de detección rápida de amenazas, y en un escenario de combate real, esta deficiencia podría comprometer toda la operación”. El Modelo de Capacidades Dinámicas de

Teece et al. (1997) ofrece un marco útil para abordar este problema, ya que subraya la necesidad de que las organizaciones sean capaces de adaptarse rápidamente a los cambios y aprovechar las oportunidades tecnológicas. En este sentido, las fuerzas armadas deben incorporar tecnologías de ciberseguridad avanzadas, como la inteligencia artificial (IA) para la detección proactiva de ciberataques, y sistemas automatizados de respuesta rápida que permitan una defensa efectiva ante amenazas emergentes. Esta flexibilidad operativa también implica una mejora en la interoperabilidad de los sistemas TICs, de manera que todos los componentes tecnológicos sean capaces de integrarse eficazmente.

En cuanto a la interoperabilidad, el Manual MACOFFAA (2019) sugieren que la falta de estandarización entre los sistemas de diferentes unidades militares puede generar barreras significativas para la comunicación y coordinación efectiva. En las entrevistas, se observó que "la diversidad de plataformas y protocolos tecnológicos en la brigada dificulta una sincronización eficiente durante las operaciones, lo que puede resultar en una toma de decisiones lenta y descoordinada". Esta falta de uniformidad en los sistemas de comunicación es un reto crucial para mejorar la interoperabilidad, y según los documentos revisados, es necesario adoptar un enfoque de estandarización progresiva para resolver este problema, en este contexto, la propuesta de solución es implementar protocolos unificados de comunicación y la integración gradual de plataformas compatibles entre diferentes unidades. Los estudios de Villarrubia (2021) sobre la adopción del 5G en el ámbito militar refuerzan la importancia de estas tecnologías emergentes, señalando que las redes de alta velocidad y baja latencia pueden mejorar la sincronización y coordinación entre unidades, optimizando la toma de decisiones y reduciendo el margen de error en el campo de batalla. Para la brigada, la implementación de tecnologías como el 5G facilitaría la transmisión de datos en tiempo real, mejorando tanto la seguridad como la eficiencia operativa.

Por otro lado, el Modelo de Aceptación de Tecnología (TAM) de Davis (1989) es relevante para la integración de estas nuevas tecnologías. Según Davis, la adopción de sistemas de TICs en las fuerzas armadas dependerá de la percepción de su utilidad y facilidad de uso. Si los oficiales perciben que las tecnologías avanzadas mejoran su capacidad para llevar a cabo las operaciones con mayor seguridad y eficacia, estarán más dispuestos a integrarlas en sus rutinas diarias. En este sentido, una estrategia clave será la capacitación continua y la sensibilización sobre los beneficios tangibles de estas nuevas tecnologías, asegurando que los miembros de la brigada las perciban como herramientas útiles en sus misiones, para mejorar la seguridad cibernética y la interoperabilidad de los sistemas TICs en la 3ª Brigada Blindada, es fundamental una actualización de las capacidades tecnológicas actuales, la integración de plataformas

estandarizadas y la implementación de tecnologías avanzadas como la inteligencia artificial y redes redundantes. Además, se debe considerar un enfoque proactivo en la formación del personal y un proceso continuo de adaptación organizacional, siguiendo el Modelo de Gestión del Cambio de Kotter (1996), que aboga por una integración estructurada y gradual de las TICs en el sistema operativo de la brigada. Estas acciones permitirán superar las barreras actuales y fortalecer la seguridad y efectividad de las operaciones en el futuro.

CONCLUSIONES

a. De acuerdo con el objetivo general: ”Analizar los principales desafíos que enfrenta la 3ª Brigada Blindada para la implementación exitosa de las TICs en sus operaciones y acciones terrestres unificadas durante el año 2025”, se han llegado a las siguientes conclusiones:

Uno de los desafíos más prominentes radica en la infraestructura tecnológica y la conectividad, especialmente en áreas remotas o de difícil acceso. La infraestructura de comunicación actual no está completamente preparada para soportar la integración de tecnologías avanzadas requeridas para las operaciones militares. La falta de redes de comunicación con la suficiente capacidad de ancho de banda y estabilidad afecta directamente la capacidad de transmitir datos de manera rápida y eficiente, lo que limita la toma de decisiones en tiempo real. Esta situación subraya la necesidad urgente de actualizar y modernizar la infraestructura tecnológica, priorizando el fortalecimiento de la conectividad y la mejora de las plataformas de comunicación para garantizar una operatividad continua y eficiente en escenarios complejos y cambiantes.

Otro desafío clave identificado es la resistencia cultural y organizacional que se observa especialmente en los niveles jerárquicos superiores de la Brigada. La estructura tradicionalmente jerárquica y la mentalidad conservadora de algunos oficiales impiden la adopción fluida de las TICs. Este tipo de resistencia es particularmente notorio entre los oficiales de mayor antigüedad, quienes se muestran escépticos ante la incorporación de nuevas tecnologías, considerando que los métodos tradicionales siguen siendo adecuados para las operaciones. En este contexto, es fundamental implementar estrategias eficaces de gestión del cambio, que no solo promuevan la sensibilización sobre los beneficios de las TICs, sino que también transformen la cultura organizacional hacia una mayor apertura a la innovación tecnológica, a través de la capacitación continua y un liderazgo comprometido con la digitalización.

La capacitación del personal militar constituye otro aspecto fundamental para la implementación exitosa de las TICs. La formación actual no cubre de manera adecuada las necesidades operativas del personal en relación con las nuevas tecnologías. Aunque se ofrece una capacitación básica sobre el uso de TICs, esta no se orienta lo suficientemente hacia la aplicación práctica de estas herramientas en escenarios operacionales reales. La Brigada necesita desarrollar programas de formación continua

y especializada, diseñados para mejorar las habilidades tácticas de los operativos en el uso de tecnologías avanzadas, como los sistemas de comando y control (C2) y las plataformas de análisis de datos en tiempo real. Además, la capacitación debe adaptarse a los distintos niveles jerárquicos, asegurando que cada miembro del personal reciba la formación necesaria según su rol dentro de la Brigada.

b. De acuerdo con el objetivo específico 1 (OE1): “Identificar las limitaciones tecnológicas e infraestructurales (hardware, software y conectividad) que afectan la implementación de las TICs en las operaciones de la 3ª Brigada Blindada”, se han llegado a las siguientes conclusiones:

Limitaciones en la Infraestructura Tecnológica y la Conectividad

A partir del análisis de la información recolectada a través de las entrevistas, las observaciones y el análisis documental, se concluye que la infraestructura tecnológica de la 3ª Brigada Blindada presenta deficiencias significativas en cuanto a su capacidad para soportar las TICs en condiciones operacionales reales. La falta de conectividad adecuada, particularmente en las zonas más alejadas o de difícil acceso, es una de las principales barreras para la implementación de las tecnologías de la información y las comunicaciones en las operaciones terrestres. La red de comunicaciones es uno de los aspectos más afectados, pues las conexiones de alta velocidad y estabilidad son limitadas en territorios de difícil acceso, lo que impide la transmisión en tiempo real de datos cruciales para la toma de decisiones durante las operaciones. Este obstáculo afecta directamente la capacidad de la Brigada para cumplir con su misión en tiempo y forma, ya que no puede obtener la información necesaria de manera eficiente.

La infraestructura tecnológica obsoleta, tanto en términos de hardware como de software, representa otro desafío considerable. La Brigada depende de equipos y plataformas de comunicaciones tradicionales que no son capaces de integrar las TICs avanzadas necesarias para realizar operaciones conjuntas o para mejorar la capacidad de respuesta ante amenazas. Como señala el marco teórico de la investigación, la transformación digital en contextos militares depende de una infraestructura que permita no solo la implementación, sino también la adaptación y evolución de los sistemas tecnológicos conforme a las necesidades.

El análisis de redes semánticas, como se muestra en la figura de la tesis, resalta cómo las limitaciones tecnológicas están interrelacionadas con las barreras de infraestructura y conectividad. Las redes semánticas desarrolladas permiten visualizar la conexión entre la infraestructura de TICs, los sistemas de comunicación y la capacidad de la Brigada para llevar a cabo sus misiones en entornos de alta exigencia. Por ejemplo, los términos como “falta de conectividad”, “infraestructura obsoleta” y

“dificultades operativas” aparecen frecuentemente vinculados, lo que resalta cómo estas limitaciones estructurales afectan la eficacia operativa de las TICs.

Compatibilidad de los Sistemas Antiguos con las Nuevas Tecnologías

Otro aspecto crítico identificado en el análisis es la incompatibilidad entre los sistemas tecnológicos antiguos y las nuevas tecnologías TIC. A pesar de los esfuerzos por modernizar algunos aspectos de la infraestructura, la falta de integración de plataformas de software y hardware antiguos con los nuevos modelos tecnológicos es una limitante directa para la operabilidad de las TICs en las operaciones. Según el marco teórico sobre interoperabilidad, las fuerzas armadas deben desarrollar sistemas capaces de interactuar y compartir información sin barreras, lo que no se está logrando debido a la coexistencia de tecnologías heterogéneas dentro de la Brigada. Las plataformas de comunicación antiguas no están optimizadas para integrar las nuevas herramientas de análisis de datos, inteligencia artificial o comunicación en tiempo real que las TICs requieren, lo que restringe el desempeño estratégico de la Brigada.

Como lo menciona teoría de la motivación y la expectativa (Vroom, 1964), la organización debe desarrollar la capacidad de adaptarse rápidamente a los cambios tecnológicos y realizar ajustes en sus sistemas para garantizar una respuesta rápida y efectiva. En este caso, la incapacidad para integrar los sistemas antiguos con los nuevos refleja una falta de flexibilidad organizacional que obstaculiza la adaptación a las TICs avanzadas.

El análisis de triangulación integrada, donde se combinan las entrevistas con los documentos y las observaciones, refuerza esta conclusión. Se observa que las interacciones entre los sistemas antiguos y nuevos generan disruptivas en la comunicación y las operaciones, lo que ralentiza las decisiones tácticas y las acciones conjuntas entre diferentes unidades. La incompatibilidad también resalta la necesidad de un enfoque estratégico para la modernización progresiva de los sistemas, que contemple la actualización de los equipos sin interrumpir las operaciones diarias.

Necesidad de Mejorar la Infraestructura y Conectividad para la Implementación Eficaz de las TICs

Finalmente, se concluye que la infraestructura y la conectividad son áreas clave que deben mejorarse para garantizar la implementación exitosa de las TICs. La evolución hacia un modelo militar digitalizado depende de la creación de una infraestructura flexible y expansiva que no solo sea capaz de soportar la integración de las TICs, sino que también permita su actualización constante a medida que surgen nuevas tecnologías. Esto implica no solo la modernización de equipos tecnológicos y redes de comunicación, sino también la creación de plataformas adaptables que puedan integrarse con nuevas tecnologías emergentes.

El análisis semántico, basado en los datos triangulados, muestra que la falta de conectividad y la infraestructura insuficiente afectan la coordinación entre unidades y el flujo de información durante las operaciones. De este modo, se destaca que el desarrollo de una infraestructura sólida es imprescindible para garantizar el uso adecuado de las TICs, especialmente en situaciones críticas donde la interoperabilidad entre plataformas y la transmisión de información rápida son fundamentales para el éxito de las operaciones.

c. De acuerdo con el objetivo específico 2 (OE2): “Evaluar el nivel de capacitación y preparación (conocimiento y habilidades) del personal militar en el uso eficaz de las TICs durante las operaciones y acciones terrestres”, se han llegado a las siguientes conclusiones:

Brechas en la Capacitación y Preparación del Personal

En el análisis realizado, se concluye que la capacitación del personal militar de la 3ª Brigada Blindada en el uso de TICs es insuficiente y presenta una brecha significativa en relación con los conocimientos y habilidades requeridas para el uso eficaz de estas tecnologías en las operaciones. Se ha identificado que la formación que se imparte actualmente está más orientada a aspectos generales y básicos de las TICs, pero no cubre de manera adecuada las aplicaciones prácticas de estas tecnologías en escenarios operacionales reales, como la gestión de información táctica o el uso de sistemas de comando y control (C2) en tiempo real.

El análisis de las entrevistas y observaciones reveló que el personal más joven, con menos años de servicio, tiene una mayor predisposición y facilidad para adoptar las TICs, mientras que los oficiales de mayor antigüedad muestran resistencia al cambio debido a la falta de familiaridad con las herramientas digitales avanzadas. Esta resistencia se debe en gran medida a la falta de capacitación continua y la desconfianza hacia las nuevas tecnologías, lo que genera una brecha intergeneracional en el uso de las TICs dentro de la Brigada. Según el marco teórico sobre teoría de la aceptación de la tecnología (Davis, 1989), la utilidad percibida y la facilidad de uso percibida son determinantes clave para la aceptación de las TICs en entornos operativos. En el caso de la 3ª Brigada Blindada, se observa que la percepción negativa de la utilidad de las TICs por parte de los oficiales veteranos contribuye a su resistencia hacia estas tecnologías.

Deficiencias en la Capacitación Práctica para Operaciones Reales

A pesar de que la capacitación teórica en el uso de TICs es una parte importante del proceso, el análisis revela que la capacitación práctica, que permita a los militares interactuar con escenarios reales en los que se emplean las TICs, es insuficiente. En

este sentido, el uso de simuladores y la formación en campo deben ser una prioridad para garantizar que el personal no solo tenga conocimientos sobre el funcionamiento de las herramientas tecnológicas, sino también sobre cómo aplicarlas de manera efectiva en situaciones tácticas.

El uso de simulaciones operacionales, basadas en escenarios reales de combate, podría proporcionar una experiencia más enriquecedora y útil para los soldados, permitiéndoles interactuar con las TICs en situaciones de alta presión. La teoría de la difusión de innovaciones (Rogers, 2003) sostiene que la adopción de nuevas tecnologías es más rápida y exitosa cuando las personas tienen la oportunidad de experimentar de manera directa cómo estas herramientas resuelven problemas prácticos. Esto es especialmente relevante en el contexto militar, donde la eficiencia y rapidez en la toma de decisiones son fundamentales. La integración de simuladores y la realización de entrenamientos en escenarios operacionales específicos facilitarán que el personal se familiarice con las TICs de manera directa, desarrollando las habilidades necesarias para su uso eficaz en el terreno.

Necesidad de Programas de Capacitación Continua y Adaptada a los Diversos Niveles del Personal

Como resultado del análisis de los datos, se concluye que la capacitación continua es esencial para garantizar el uso efectivo de las TICs en las operaciones. La capacitación inicial no es suficiente para que el personal se mantenga actualizado con las tecnologías emergentes y los avances en los sistemas de TICs utilizados en las operaciones militares. Por lo tanto, es necesario implementar programas de formación continua, que no solo incluyan la introducción de nuevas tecnologías, sino que también se enfoquen en la adaptación de los miembros de la Brigada a las TICs de manera progresiva.

El análisis de triangulación integrada (entrevistas, observación y documentos) muestra que la capacitación del personal debe ser diferenciada y adaptada a los distintos niveles de conocimiento y experiencia dentro de la Brigada. Los oficiales superiores requieren formación especializada en gestión de TICs a nivel estratégico, mientras que el personal subalterno necesita estar capacitado para utilizar las TICs en situaciones tácticas, con énfasis en el uso efectivo de los sistemas de comunicación y las plataformas tecnológicas en el terreno.

Una estrategia de formación escalonada es clave para garantizar que cada miembro del personal reciba la formación necesaria, según su rol y nivel jerárquico, para usar las TICs de manera efectiva en su área de trabajo específico. Además, estos programas deben incluir evaluaciones periódicas para asegurarse de que el conocimiento adquirido esté siendo aplicado correctamente durante las operaciones. La

integración de módulos de retroalimentación sobre el uso de TICs permitirá mejorar los programas de capacitación y ajustarlos a las necesidades operativas específicas de la Brigada.

Propuestas para una Capacitación Eficaz en TICs

Como parte de las propuestas para mejorar la capacitación en la Brigada, se recomienda la implementación de entrenamientos más prácticos y específicos que estén alineados con las exigencias de las operaciones reales. Las simulaciones deben incluir tanto el uso de plataformas de comunicación digital como el manejo de sistemas de comando y control (C2), y los soldados deben ser entrenados en la resolución de problemas tecnológicos en escenarios operativos complejos.

El uso de escenarios virtuales con simuladores de combate que integren TICs avanzadas (como sensores, inteligencia artificial y comunicaciones seguras) permitirá que el personal practique en un ambiente controlado que simule las condiciones del campo. Además, se sugiere incorporar capacitación interdisciplinaria, involucrando a expertos en tecnología y comunicación militar, para enseñar a los oficiales no solo sobre el manejo técnico de las herramientas, sino también sobre cómo integrar estas tecnologías en las tácticas y estrategias militares.

d. De acuerdo con el objetivo específico 3 (OE3): “Determinar las barreras organizacionales y culturales (cultura, liderazgo y procesos) que dificultan la adopción de las TICs en la 3ª Brigada Blindada”, se han llegado a las siguientes conclusiones:

Resistencia Cultural y Organizacional a la Adopción de las TICs

Uno de los principales hallazgos en el análisis realizado es la resistencia cultural y organizacional que existe dentro de la 3ª Brigada Blindada frente a la adopción de las TICs. Esta resistencia es particularmente fuerte en los niveles más altos de la Brigada, donde prevalece una estructura jerárquica rígida y tradicional, que se muestra reacia a aceptar el cambio tecnológico. Según el marco teórico sobre gestión del cambio (Kotter, 1996), la resistencia al cambio dentro de las organizaciones es un fenómeno común, especialmente cuando las tecnologías emergentes desafían las estructuras establecidas y los procedimientos tradicionales. En este caso, la falta de confianza en la capacidad de las TICs para mejorar los resultados operativos y la percepción de que las herramientas tradicionales son suficientes para la toma de decisiones en el campo de batalla son los principales factores que dificultan la adopción de estas tecnologías.

Además, la estructura jerárquica tradicional limita la flexibilidad organizacional necesaria para fomentar un cambio tecnológico rápido y efectivo. Como se menciona en la teoría de la resistencia al cambio (Dent & Goldberg, 1999), las organizaciones militares tienden a tener una estructura rígida, lo que genera que la innovación se

perciba como una amenaza a las normas establecidas. Esta rigidez impide la adopción rápida de las TICs y limita la capacidad de la Brigada para adaptarse a un entorno cada vez más digitalizado.

Falta de Liderazgo para Impulsar el Cambio hacia las TICs

Otro hallazgo importante es la falta de liderazgo claro y comprometido con la transformación digital dentro de la Brigada. El liderazgo en contextos militares es fundamental para implementar cambios estructurales, como la adopción de nuevas tecnologías. Sin embargo, el análisis realizado muestra que no existe una visión unificada por parte del liderazgo sobre la importancia de las TICs como un recurso estratégico. La falta de compromiso por parte de los líderes clave genera una falta de incentivos para que los subordinados adopten las tecnologías y las utilicen de manera efectiva en las operaciones.

En el contexto de la gestión de la innovación tecnológica, el liderazgo debe ser capaz de crear un ambiente de confianza, entusiasmo y compromiso con la tecnología, lo cual no ha sido el caso dentro de la 3ª Brigada Blindada. El liderazgo debe actuar como un catalizador para el cambio y, en este caso, no se ha dado la prioridad estratégica a la integración de las TICs dentro de las operaciones militares. Es necesario que los líderes inspiren y guíen a sus equipos hacia un futuro digital más eficiente y efectivo, creando una cultura organizacional que valore la innovación tecnológica.

El análisis de triangulación integrada mostró que la falta de liderazgo comprometido y la insuficiencia de políticas claras de adopción de TICs son factores críticos que obstaculizan su implementación. Las observaciones en el campo y las entrevistas con oficiales de alto rango reflejan que, aunque se reconoce la importancia de las TICs, no se ha definido un plan estratégico claro para su integración en las operaciones cotidianas.

Barreras en los Procesos y Estructuras Operacionales

Los procesos organizacionales establecidos dentro de la 3ª Brigada Blindada también representan una barrera significativa para la adopción de las TICs. Muchos de los procedimientos utilizados para las operaciones militares siguen siendo tradicionales y están diseñados para un entorno en el que las TICs no juegan un papel central. Estos procesos inflexibles dificultan la integración de herramientas tecnológicas avanzadas, como sistemas de comando y control digital, plataformas de análisis de datos en tiempo real y sistemas de monitoreo remoto, los cuales requieren adaptaciones en los procedimientos operacionales.

La teoría de la aceptación de tecnología (Davis, 1989), sugiere que las organizaciones deben ser capaces de redefinir sus procesos para adaptarse a las nuevas tecnologías. Sin embargo, en la 3ª Brigada Blindada, los procesos operativos

aún se basan en estrategias tradicionales, lo que limita la eficiencia y eficacia de la Brigada al no integrar las TICs en sus flujos de trabajo operacionales. A pesar de la importancia de las TICs para mejorar la coordinación y la toma de decisiones en situaciones de combate, la rigidez de los procesos organizacionales impide su implementación completa.

El análisis semántico realizado también muestra que los términos como "procesos rígidos", "falta de flexibilidad" y "procedimientos tradicionales" están estrechamente relacionados con la dificultad para integrar las TICs en las operaciones diarias. Es necesario un enfoque integral de reingeniería de procesos, que permita modernizar las estrategias operativas y alinearlas con las capacidades que ofrecen las TICs.

Necesidad de un Cambio Cultural hacia la Innovación Tecnológica

Finalmente, la cultura organizacional debe ser transformada para permitir una integración efectiva de las TICs. La actitud conservadora hacia la tecnología y la tendencia a aferrarse a métodos tradicionales operativos deben ser superadas mediante acciones concretas que fomenten un ambiente de innovación constante. El análisis muestra que una gestión proactiva del cambio, que implique el entrenamiento y la sensibilización continua sobre las ventajas de las TICs, es esencial para crear una cultura organizacional que valore la digitalización como una herramienta estratégica para mejorar las capacidades operacionales. En este caso, la Brigada debe evolucionar para convertirse en una entidad digitalizada, capaz de utilizar las TICs no solo en situaciones de combate, sino también en la gestión interna y la toma de decisiones estratégicas.

e. De acuerdo con el objetivo específico 4 (OE4): “Proponer estrategias y medidas (planes de capacitación, mejoras de infraestructura, protocolos de seguridad) para mitigar las vulnerabilidades de ciberseguridad relacionadas con la adopción de TICs y la interoperabilidad de los sistemas en las operaciones militares”, se han llegado a las siguientes conclusiones:

Necesidad de Fortalecer la Infraestructura Tecnológica y Mejorar la Conectividad

Uno de los principales hallazgos en el análisis realizado es la insuficiencia de la infraestructura tecnológica en la 3ª Brigada Blindada, lo que dificulta la integración efectiva de las TICs en las operaciones militares. En la actualidad, la infraestructura no está preparada para soportar el uso intensivo de las nuevas tecnologías, las cuales requieren mayor capacidad de procesamiento de datos, redes de comunicación más

rápidas y sistemas robustos de almacenamiento y gestión de información. Las redes de comunicación deben ser mejoradas, ya que las actuales presentan limitaciones en términos de ancho de banda, latencia y conectividad en zonas remotas, lo que afecta la transmisión en tiempo real de la información crucial para las decisiones tácticas y estratégicas en el campo de batalla.

El análisis de la infraestructura tecnológica se alinea con el modelo de capacidades dinámicas (Teece et al., 1997), que resalta la importancia de la adaptabilidad organizacional para integrar tecnologías emergentes. Este modelo subraya que las organizaciones deben desarrollar la capacidad de adaptar su infraestructura a las exigencias cambiantes del entorno. Por lo tanto, la modernización de los sistemas de comunicación, almacenamiento de datos y las plataformas operativas, debe ser vista como un imperativo para garantizar que la Brigada no solo mantenga la eficiencia operativa actual, sino que también se prepare para incorporar tecnologías futuras.

Protocolos de Seguridad Cibernética: Mitigación de Vulnerabilidades

En cuanto a ciberseguridad, el análisis muestra que es una de las mayores amenazas para la adopción de las TICs dentro de la 3ª Brigada Blindada. Las vulnerabilidades en los sistemas de TICs pueden comprometer la integridad y confidencialidad de la información sensible, lo que representa un riesgo crítico para la seguridad nacional. Las operaciones militares, que dependen cada vez más de las tecnologías digitales, son susceptibles a ciberataques que pueden desestabilizar las comunicaciones y coordinación operativa.

La ciberseguridad debe ser tratada como un componente clave en la infraestructura tecnológica, como también se menciona en la teoría de la gestión del cambio (Kotter, 1996). La implementación de un cambio exitoso en una organización debe considerar la infraestructura tecnológica como parte integral de su transformación. Según este marco, es fundamental que la Brigada cuente con protocolos claros y efectivos de ciberseguridad, para proteger los sistemas críticos de comunicación y comando.

Mejorar la Interoperabilidad de los Sistemas TICs

Otro aspecto fundamental identificado en el análisis es la interoperabilidad de los sistemas TICs, la cual es clave para la integración exitosa de las tecnologías en operaciones conjuntas, tanto a nivel nacional como con aliados internacionales. La falta de compatibilidad entre los sistemas tecnológicos de la Brigada y los de otras unidades militares, nacionales o aliadas, representa una barrera significativa.

En el marco teórico sobre interoperabilidad se menciona que las fuerzas armadas deben garantizar que sus sistemas de comunicación y plataformas

tecnológicas sean interoperables, a fin de facilitar la colaboración efectiva con otras unidades. La implementación de estándares de comunicación comunes entre los diferentes sistemas tecnológicos de las unidades es esencial para asegurar la coordinación fluida durante las operaciones.

Propuestas para la Capacitación Continua en Ciberseguridad y Uso de TICs

Una de las medidas más urgentes es la implementación de un programa de capacitación continua que permita al personal militar no solo dominar el uso de las TICs, sino también entender los riesgos y las mejores prácticas en ciberseguridad. La capacitación debe enfocarse en tres áreas clave:

- Capacitación técnica en TICs: Proporcionar formación sobre el uso de plataformas tecnológicas, incluyendo sistemas de comando y control (C2), herramientas de análisis de datos y comunicación segura.
- Capacitación en ciberseguridad: Instruir sobre los principios de protección de datos, gestión de vulnerabilidades, detección de amenazas y respuesta a incidentes cibernéticos.
- Simulaciones de ciberataques: Desarrollar ejercicios prácticos de respuesta ante incidentes cibernéticos, permitiendo que los operativos entrenen en un entorno controlado, desarrollando capacidades para reaccionar ante ciberataques en tiempo real.

El análisis de triangulación integrada revela que simulaciones realistas de ciberataques y el uso de entrenamientos interactivos deben ser una parte clave del programa de capacitación, para que el personal se familiarice con el entorno digital y los riesgos asociados a las TICs. Además, debe incluirse la capacitación en gestión de crisis cibernéticas, para garantizar que el personal esté preparado para tomar decisiones rápidas y eficaces durante un incidente de ciberseguridad.

RECOMENDACIONES

En cuanto al objetivo general (OG), se recomienda al señor General de Brigada Comandante General de la 3ª Brigada Blindada la adopción de medidas que aborden las limitaciones detectadas en términos de infraestructura tecnológica, gestión del cambio organizacional y capacitación del personal, tomando como base las siguientes medidas propuestas; en primer lugar, es esencial realizar una evaluación exhaustiva de la infraestructura de redes de la brigada, incluyendo sistemas de radiofrecuencia (RF), comunicación satelital y redes móviles (4G/5G). Este diagnóstico debe identificar áreas de cobertura deficiente y cuellos de botella en la capacidad de transmisión de datos, especialmente en zonas de alto riesgo o geografía compleja. Además, se debe considerar la implementación de Redes Definidas por Software (SDN), que permiten una gestión centralizada y adaptable de los recursos de red, optimizando el uso de ancho de banda y mejorando la resiliencia operativa, para garantizar una conectividad estable en áreas remotas o durante operaciones móviles intensivas, se propone el uso de satélites de órbita baja (LEO), como el sistema Starlink. Estos satélites ofrecen baja latencia, alta capacidad de transmisión y resiliencia frente a posibles interrupciones de redes terrestres, lo que permite mantener comunicaciones ininterrumpidas incluso en entornos de alta demanda. La implementación de sistemas de comunicación TETRA es otra medida recomendada, ya que estos sistemas garantizan comunicaciones seguras, resistentes a interferencias y a ataques electrónicos. TETRA permite la transmisión continua de voz y datos en tiempo real, lo que es crucial para la coordinación de unidades en condiciones adversas, en el ámbito de la ciberseguridad, se recomienda establecer un Sistema de Gestión de Seguridad de la Información (ISMS) conforme a estándares internacionales como ISO/IEC 27001 y el NIST Cybersecurity Framework. La adopción de encriptación avanzada (AES-256) y autenticación multifactor (MFA) para todas las plataformas de acceso remoto fortalecerá la seguridad de las comunicaciones, protegiendo los datos sensibles y las redes operacionales de accesos no autorizados, además, se sugiere la creación de un Centro de Respuesta a Incidentes Cibernéticos (CSIRT), encargado de monitorear las redes en tiempo real, utilizando herramientas de detección y prevención de intrusos (IDS/IPS). Este equipo especializado garantizará la mitigación eficaz de ciberataques y la recuperación de sistemas tras un incidente. La capacitación continua del personal en TICs y ciberseguridad es fundamental. Se debe

asegurar que todos los miembros de la brigada reciban formación en el uso de plataformas de Comando y Control (C2), gestión de inteligencia y en el uso de redes móviles de campo y sistemas TETRA. Además, los miembros clave deben obtener certificaciones internacionales en ciberseguridad, como CompTIA Security+, Certified Ethical Hacker (CEH) o Certified Information Systems Security Professional (CISSP), asegurando que cuenten con las competencias necesarias para gestionar infraestructuras críticas y responder a incidentes cibernéticos .

En cuanto al objetivo específico 1 (OE1) , se recomienda al Comandante General de la 3ª Brigada Blindada realizar una evaluación técnica exhaustiva de la infraestructura de comunicaciones existente en la brigada, con el objetivo de integrar soluciones que optimicen la transmisión de datos y la conectividad en entornos operacionales desafiantes. Asimismo seria conveniente implementar sistemas TETRA redundantes, que son adecuados para la transmisión de datos y comunicaciones de voz en tiempo real mediante el uso de la modulación digital por salto de frecuencia (FHSS) y la codificación avanzada de señal para garantizar la seguridad en las comunicaciones. Estos sistemas de comunicación troncales están diseñados para operar bajo condiciones extremas, asegurando cobertura en áreas de difícil acceso gracias a su infraestructura de cobertura celular troncalizada y la interoperabilidad con otras redes de emergencia. Además, se sugiere emplear antenas móviles de enlace satelital basadas en tecnologías LEO (Low Earth Orbit) como Starlink, que permitirán mantener una conexión de banda ancha de baja latencia para el intercambio de datos a través de redes IP avanzadas en zonas remotas. La redundancia del sistema de satélite y el uso de tecnología de encriptación de extremo a extremo (AES-256) en las comunicaciones asegurarán una alta disponibilidad y confidencialidad en las transmisiones, esencial en misiones tácticas. Asimismo, para asegurar la integridad y eficiencia de la infraestructura tecnológica, se recomienda la instalación de una red de fibra óptica fija, utilizando cables ópticos blindados que resistan las interferencias electromagnéticas (EMI) y las condiciones extremas del entorno de operaciones. La fibra óptica proporciona una alta capacidad de ancho de banda y latencia mínima, lo que facilita la transmisión de grandes volúmenes de datos a velocidades críticas para las operaciones de comando y control. La infraestructura de fibra debe incluir sistemas de conmutación automática para garantizar la conectividad continua a través de topologías redundantes que prevengan la caída de servicio por fallos en un nodo de la red, lo cual es crucial en entornos de alta exigencia como los de la brigada. La integración de estas tecnologías avanzadas permitirá no solo mejorar la fiabilidad y seguridad de las comunicaciones, sino también optimizar la gestión de datos en tiempo real para el análisis estratégico y táctico durante las misiones.

En cuanto al objetivo específico 2 (OE2), se recomienda realizar una evaluación exhaustiva de las capacidades actuales del personal en relación con las Tecnologías de la Información y las Comunicaciones (TIC), especialmente en el ámbito de la ciberseguridad y las comunicaciones de alto nivel. Para esto, se debe implementar un programa de formación avanzada que integre tanto simuladores de entornos virtuales inmersivos (VR) como sistemas de entrenamiento en red enfocados en plataformas de comando y control (C2), gestión de datos en tiempo real y comunicaciones seguras. Además, el personal deberá recibir formación práctica en la integración de protocolos de interoperabilidad como STANAG 4607, esenciales para garantizar la comunicación efectiva con fuerzas aliadas, y en el uso de sistemas de encriptación avanzada (AES-256) y VPNs militares para asegurar la confidencialidad de las comunicaciones operacionales. Para mejorar la capacitación técnica y estratégica, se recomienda establecer alianzas estratégicas con universidades locales y centros especializados. En Moquegua, la Universidad Nacional Jorge Basadre Grohmann (UNJBG), con su programa de Ingeniería de Sistemas y Telecomunicaciones, podría proporcionar un marco académico robusto para la formación en comunicaciones avanzadas y ciberseguridad. Además, la Universidad Tecnológica del Perú (UTP) ofrece programas en redes de datos y ciberseguridad, que podrían ser fundamentales para desarrollar una capacidad técnica de alto nivel. Por otro lado, la Presidencia del Consejo de Ministros (PCM), a través de su Programa de Ciberseguridad y Ciberdefensa, ofrece formación avanzada en protección de infraestructuras críticas, resiliencia cibernética y gestión de riesgos cibernéticos, con la participación de empresas privadas tecnológicas como Cisco Networking Academy, lo cual fortalecería la capacidad del personal para enfrentar amenazas cibernéticas. Este programa está diseñado para formar analistas junior en ciberseguridad y capacitar a más de 15,000 funcionarios públicos, lo que representa una oportunidad clave para mejorar las competencias del personal en defensa cibernética, alineado con las políticas de seguridad nacional.

En cuanto al objetivo específico 3 (OE3), se recomienda que la 3ª Brigada Blindada aborde de manera prioritaria las barreras culturales y la resistencia al cambio que existen en su estructura organizacional, especialmente en los niveles jerárquicos superiores. La resistencia cultural a la adopción de las TICs está fuertemente arraigada debido a la percepción de que la digitalización amenaza los procedimientos tradicionales y la jerarquía establecida. Esta resistencia se manifiesta en la desconfianza hacia las nuevas tecnologías y el temor a la obsolescencia de métodos tradicionales de toma de decisiones. Para superar esta barrera cultural, es esencial implementar un plan de sensibilización y formación continua dirigido a todo el personal de la brigada, desde los oficiales de alto rango hasta el personal operativo. Este plan debe centrarse en gestionar

el cambio cultural mediante el uso de herramientas como talleres, simuladores de escenarios y presentaciones interactivas que muestren los beneficios concretos de la adopción de las TICs, como la mejora de la coordinación operativa, la toma de decisiones rápida y precisa y la eficiencia en el despliegue de recursos durante las misiones. Además, la sensibilización debe centrarse en crear un ambiente de confianza en torno a las TICs, desmitificando su uso y mostrando sus aplicaciones reales dentro del contexto operativo de la brigada. Este proceso de cambio debe estar alineado con el Plan Nacional de Modernización de la Gestión Pública al 2030, que busca transformar la infraestructura tecnológica de las Fuerzas Armadas, impulsando la digitalización y la adaptación de las TICs a las operaciones militares. Este plan establece como una de sus prioridades la modernización de la cultura organizacional, de modo que las Fuerzas Armadas del Perú puedan integrarse de manera efectiva en un entorno tecnológico globalizado. A nivel institucional, el Plan Estratégico Sectorial Multianual (PESEM) destaca la importancia de fortalecer la cultura organizacional para fomentar el uso de tecnologías emergentes y avanzar hacia la transformación digital de las instituciones del Estado. Para facilitar esta transición, es fundamental un enfoque integral que combine el PTI (Plan de Transformación Institucional) con la visión estratégica del PESEM, implementando políticas que favorezcan un entorno flexible y abierto al cambio tecnológico. La brigada debe alinear su cultura interna con los objetivos del PESEM, que busca crear una estructura organizacional capaz de adaptarse rápidamente a los avances tecnológicos y mejorar la resiliencia institucional frente a los desafíos del siglo XXI. Es crucial que los líderes de la brigada se comprometan activamente con este proceso, actuando como agentes de cambio y fomentando un liderazgo que valore la innovación tecnológica como un activo estratégico. Esta transformación cultural será clave para la integración de las TICs en todos los niveles operacionales y permitirá que la 3ª Brigada Blindada esté mejor preparada para enfrentar los retos futuros.

En cuanto al objetivo específico 4 (OE4), se recomienda que la 3ª Brigada Blindada implemente una estrategia integral para mitigar las vulnerabilidades de ciberseguridad asociadas con la adopción de Tecnologías de la Información y Comunicación (TICs) y mejorar la interoperabilidad de sus sistemas en operaciones militares. Este plan debe abordar cuatro áreas clave: fortalecimiento de la infraestructura tecnológica, establecimiento de protocolos de seguridad cibernética, mejora de la interoperabilidad de sistemas y capacitación continua del personal. En primer lugar, es esencial modernizar la infraestructura tecnológica de la brigada para soportar el uso intensivo de las TICs. Esto implica actualizar las redes de comunicación para ofrecer mayor ancho de banda y menor latencia, mejorando la transmisión en tiempo real de información crítica. Además, se deben implementar sistemas de almacenamiento y

gestión de datos que permitan el manejo eficiente de grandes volúmenes de información operativa. La adopción de tecnologías emergentes, como redes definidas por software (SDN), también contribuirá a mejorar la flexibilidad y capacidad de la infraestructura de comunicación. En segundo lugar, la protección de la información sensible es crucial. Se deben desarrollar e implementar políticas de ciberseguridad que aborden la protección de datos, gestión de accesos y respuesta a incidentes cibernéticos, alineadas con la Política Nacional de Ciberseguridad del Perú. Es fundamental establecer un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT) para detectar, analizar y mitigar amenazas cibernéticas, garantizando una respuesta rápida y efectiva ante incidentes. Además, la implementación de soluciones de seguridad avanzadas, como sistemas de detección y prevención de intrusiones (IDS/IPS), firewalls de próxima generación y soluciones de cifrado de datos, reforzará la protección de los sistemas. En tercer lugar, la capacidad de operar conjuntamente con otras unidades y aliados depende de la compatibilidad de los sistemas. Se recomienda adoptar estándares de comunicación comunes, como los definidos en el marco Magerit, para facilitar la interoperabilidad entre diferentes sistemas y plataformas. Participar en ejercicios de interoperabilidad con otras unidades y fuerzas aliadas permitirá evaluar y mejorar la compatibilidad y eficacia operativa. El desarrollo de interfaces y puentes de comunicación también facilitará la integración de sistemas dispares, asegurando un flujo de información continuo y confiable. Por último, la formación del personal es fundamental para mantener un alto nivel de preparación. Se deben implementar programas de formación en ciberseguridad que aborden desde fundamentos de seguridad hasta técnicas avanzadas de defensa cibernética, adaptados a las necesidades del personal militar. La realización de simulaciones de ciberataques permitirá al personal enfrentar escenarios realistas, mejorando su capacidad de respuesta ante incidentes cibernéticos. Fomentar una cultura de seguridad cibernética, promoviendo buenas prácticas y hábitos seguros en el uso de TICs, es esencial para garantizar la protección de la información y la eficacia operativa de la brigada. Estas recomendaciones están alineadas con la Política Nacional de Ciberseguridad y buscan fortalecer las capacidades de la 3ª Brigada Blindada en el entorno digital, garantizando operaciones más seguras, eficientes y colaborativas.

PROPUESTA PARA ENFRENTAR LA REALIDAD PROBLEMÁTICA

Título del Aporte de Investigación:

"Propuestas para la Optimización de la Implementación de Tecnologías de la Información y Comunicación (TICs) en la 3ª Brigada Blindada"

Objetivos del Aporte de Investigación:

El presente trabajo de investigación tiene como objetivo principal proponer estrategias eficaces para la integración de las Tecnologías de la Información y Comunicación (TICs) en la 3ª Brigada Blindada, con el fin de optimizar sus capacidades operativas y defensivas. Para ello, se establecen los siguientes objetivos específicos:

- Evaluar la infraestructura tecnológica actual de la brigada, identificando debilidades y oportunidades de mejora en la conectividad y la capacidad de transmisión de datos.
- Desarrollar un marco robusto de ciberseguridad para proteger las comunicaciones y los sistemas informáticos de la brigada frente a ciberamenazas y vulnerabilidades.
- Promover la capacitación continua del personal para asegurar que los miembros de la brigada puedan manejar adecuadamente las herramientas TICs y respondan adecuadamente a situaciones de ciberseguridad.
- Facilitar la interoperabilidad entre las TICs de la brigada y otros sistemas de unidades militares nacionales e internacionales, garantizando la eficiencia en el intercambio de datos durante operaciones conjuntas.

Justificación del Aporte de Investigación:

Con el trabajo de investigación realizado, se ha podido analizar el estado actual de la infraestructura tecnológica, las capacidades de ciberseguridad y los procesos operativos de la 3ª Brigada Blindada, lo que ha permitido identificar importantes desafíos que limitan la eficiencia operativa y la seguridad en el manejo de las TICs. En este contexto, se pudo realizar una propuesta de medidas para optimizar la integración de las Tecnologías de la Información y Comunicación (TICs) en la brigada, enfocándose en la mejora de la infraestructura, el fortalecimiento de la ciberseguridad, la capacitación continua del personal y la interoperabilidad con otras unidades. Las medidas propuestas básicamente se refieren a las siguientes:

- Evaluación Integral de la Infraestructura de Redes: Realizar un diagnóstico técnico completo de las redes de comunicación existentes en la brigada, incluyendo las de radiofrecuencia (RF) y sistemas de comunicación satelital, y

realizar un análisis exhaustivo de vulnerabilidades en las redes móviles (4G/5G). Este diagnóstico debe identificar las zonas de cobertura deficiente y los cuellos de botella en la capacidad de transmisión de datos, lo cual afectaría las operaciones en zonas de alto riesgo y dificultad geográfica. La evaluación debe contemplar también los riesgos derivados de posibles ciberataques y la interferencia de guerra electrónica.

- Implementación de Redes Definidas por Software (SDN): Se recomienda la adopción de SDN (Software Defined Networks) para permitir la creación de redes adaptativas, donde la gestión centralizada de los recursos de red sea capaz de adaptarse a las condiciones operacionales dinámicas de la brigada. SDN permite un control más preciso del tráfico de datos, optimizando el uso de ancho de banda, y ofreciendo la capacidad de reconfigurar la red de acuerdo a las necesidades tácticas en tiempo real, asegurando que se mantenga una conectividad confiable bajo todas las condiciones.
- Uso de Satélites LEO (Low Earth Orbit): Para asegurar una conectividad estable en zonas alejadas o en escenarios de operaciones móviles de alta intensidad, se propone la implementación de constelaciones de satélites LEO, como Starlink. Esta tecnología de baja latencia y alta capacidad de transmisión proporcionará un ancho de banda mayor que los satélites tradicionales en órbita geoestacionaria, permitiendo a la brigada transmitir datos en tiempo real y facilitar la gestión de la inteligencia y las comunicaciones tácticas. La infraestructura satelital también proporcionará resiliencia frente a interrupciones de red terrestre y permitirá a la brigada mantener una comunicación ininterrumpida incluso en entornos de alta demanda.
- Implementación de Sistemas de Comunicación TETRA: Los sistemas TETRA (Terrestrial Trunked Radio) permiten la transmisión segura y encriptada de voz y datos en tiempo real, lo que los convierte en una solución ideal para operaciones de campo. TETRA garantiza comunicaciones resistentes a interferencias de radiofrecuencia y atacantes electrónicos. Su capacidad para mantener comunicaciones continuas bajo condiciones adversas es fundamental para la coordinación de unidades militares en tiempo real.
- Desarrollo de un Sistema de Gestión de Seguridad de la Información (ISMS): Establecer un marco integral de seguridad conforme a las mejores prácticas internacionales, como ISO/IEC 27001 y el NIST Cybersecurity Framework, con el fin de garantizar la protección continua de los sistemas críticos y la información confidencial. Este sistema debe incluir políticas de acceso seguro, gestión de

identidades y accesos (IAM), y la adopción de estrategias de defensa en profundidad que protejan todos los niveles de la infraestructura.

- Encriptación Avanzada y Autenticación Multifactor (MFA): Implementar tecnologías de encriptación avanzada como AES-256 para asegurar que las comunicaciones críticas estén protegidas de accesos no autorizados. Adicionalmente, se debe adoptar la autenticación multifactor (MFA) para todas las plataformas de acceso remoto, asegurando que solo los usuarios autorizados puedan acceder a la información sensible y a las redes operacionales.
- Creación de un Centro de Respuesta a Incidentes Cibernéticos (CSIRT): El CSIRT debe ser el principal encargado de monitorear las redes de la brigada en tiempo real, utilizando herramientas de detección de intrusos (IDS) y prevención de intrusos (IPS), junto con análisis forense digital para investigar y remediar incidentes. Este equipo especializado será clave en la mitigación de ciberataques y en la recuperación de sistemas tras incidentes de seguridad.
- Simulacros de Defensa Cibernética: Los ejercicios de ciberdefensa deben ser parte integral de la formación continua del personal. Estos simulacros deben incluir la simulación de ataques avanzados como APT (Advanced Persistent Threat), phishing dirigido y denegación de servicio distribuido (DDoS). Estos entrenamientos permitirán al personal responder de manera eficaz a incidentes reales, minimizando el impacto en la misión.
- Desarrollo de un Programa Integral de Capacitación en TICs y Ciberseguridad: El personal debe recibir formación continua en el uso de plataformas C2 (comando y control), gestión de inteligencia, y el uso de redes móviles de campo y sistemas TETRA. Además, el personal debe estar capacitado en el uso de herramientas avanzadas de ciberseguridad y en la gestión de incidentes cibernéticos.
- Certificación Internacional en Ciberseguridad: El personal clave debe recibir certificaciones profesionales como CompTIA Security+, Certified Ethical Hacker (CEH) y Certified Information Systems Security Professional (CISSP). Estas certificaciones aseguran que los miembros de la brigada cuenten con las habilidades necesarias para gestionar la seguridad de las infraestructuras críticas.
- Simulacros de Respuesta ante Ciberincidentes: Además de los ejercicios prácticos, se deben realizar simulaciones avanzadas que involucren a todo el personal en la gestión de ciberincidentes. Estos ejercicios deben ser realistas y permitir al equipo enfrentar ciberataques en tiempo real, evaluando su capacidad para responder a ataques de alta sofisticación.

- Adopción de Estándares Internacionales de Interoperabilidad: Implementar protocolos de comunicación estándares como IP, XML y C2 interoperability standards de la OTAN. Estos protocolos permiten la interacción fluida entre las plataformas tecnológicas de la brigada y las de fuerzas aliadas, garantizando una coordinación efectiva en operaciones multinacionales.
- Desarrollo de Interfaces Abiertas de Comunicación: La brigada debe desarrollar APIs abiertas que faciliten el intercambio de datos entre plataformas tecnológicas de diferentes unidades. Este enfoque promoverá la flexibilidad y adaptabilidad en las operaciones conjuntas.
- Ejercicios de Interoperabilidad Conjunta: Se deben realizar ejercicios multidominio para garantizar que los sistemas de comunicación y comando sean totalmente compatibles. Estos ejercicios deben involucrar pruebas de intercambio de datos en tiempo real y coordinación operativa durante escenarios de alta intensidad.

Tabla 7

Plan de Acción para la Optimización de la Implementación de TICs en la 3ª Brigada Blindada

Objetivo	Meta	Indicadores	Unidad de Medida	Plazo	Porcentaje de Cumplimiento (1er Año)	Porcentaje de Cumplimiento (2do Año)	Responsables
Fortalecer la infraestructura tecnológica	Evaluar y modernizar la infraestructura de redes, incluyendo SDN y satélites LEO, con el fin de mejorar la capacidad de transmisión de datos.	Informe de evaluación técnica, plan de modernización de redes y equipos implementados.	Informe de evaluación, cantidad de equipos implementados.	6 meses para evaluación, 12 meses para implementación total.	30% con evaluación de redes y plan de modernización aprobado.	70% con implementación y modernización total de la infraestructura.	Equipo de infraestructura y tecnología de la brigada. (SETEL – CMDTE CIA COM)
Desarrollar un marco integral de ciberseguridad	Implementar un ISMS conforme a ISO/IEC 27001 y NIST para proteger la infraestructura crítica.	ISMS implementado, auditorías de ciberseguridad realizadas, cantidad de sistemas protegidos.	Número de sistemas ISMS implementados, auditorías realizadas.	9 meses para implementación y auditoría de seguridad.	30% en fase de diseño e implementación inicial.	70% con el ISMS completamente implementado y auditado.	Oficial de ciberseguridad y equipo de TI.(SETEL – OFL COM GUC – CMDTE CIA COM)
Capacitar al personal en TICs y ciberseguridad	Entrenar al 100% del personal en el uso de TICs, en la gestión de plataformas de C2 y ciberseguridad, y certificar a los miembros clave.	Número de personal capacitado y con certificaciones obtenidas.	Número de empleados capacitados y certificados.	12 meses para completar la formación.	50% de personal capacitado y con formación inicial completada.	100% de personal capacitado y certificado en TICs y ciberseguridad.	Encargado de formación y recursos humanos. (SETEL – SIEDOC – SEPER)
Mejorar la interoperabilidad con otras grandes unidades	Asegurar que todos los sistemas de comunicación sean, utilizando estándares de interoperabilidad como C2.	Porcentaje de sistemas C2 interoperables, pruebas de interoperabilidad realizadas.	Porcentaje de compatibilidad entre los sistemas C2.	9 meses para cumplir con los estándares de interoperabilidad.	40% de integración en la fase inicial de interoperabilidad.	100% de interoperabilidad alcanzada con sistemas C2 totalmente integrados.	SETEL EN coordinación con SETEL de otras GUC (ejercicios de comunicaciones).

Desarrollar un sistema de gestión de seguridad de la información (ISMS)	Establecer un marco de seguridad basado en las mejores prácticas internacionales para la protección de los datos y comunicaciones críticas.	ISMS implementado, políticas de seguridad definidas, implementación de herramientas de monitoreo continuo.	Número de sistemas ISMS implementados, cantidad de herramientas de seguridad implementadas.	12 meses para implementación total del sistema ISMS.	30% de implementación inicial, políticas y herramientas definidas.	70% con ISMS implementado y operaciones de monitoreo continuo en curso.	Oficial de ciberseguridad y equipo de TI. (SETEL – CMDTE CIA COM)
Realizar simulacros de defensa cibernética	Realizar simulacros de ciberseguridad para entrenar a los miembros del equipo ante ciberataques avanzados (APT, DDoS, phishing, etc.).	Número de simulacros realizados, personal involucrado, evaluación de eficacia del simulacro.	Número de simulacros realizados, porcentaje de participación.	6 meses para iniciar simulacros, anuales para actualizaciones.	50% de simulacros iniciados, personal entrenado en ciberseguridad básica.	100% de simulacros completos y personal entrenado en ataques avanzados.	Departamento de formación y recursos humanos, Oficial de ciberseguridad. (SETEL – CMDTE CIA COM)
Implementar encriptación avanzada y autenticación multifactor (MFA)	Implementar tecnologías como AES-256 para comunicaciones seguras y MFA para acceso remoto a redes sensibles.	Número de sistemas encriptados y número de plataformas con MFA implementado.	Cantidad de sistemas encriptados, cantidad de plataformas con MFA.	6 meses para evaluar e implementar las primeras fases de encriptación.	50% de plataformas con encriptación y MFA implementados.	100% de plataformas encriptadas y con MFA en su totalidad.	Oficial de ciberseguridad y equipo de TI. (SETEL – SEICI)
Desarrollar interfaces abiertas de comunicación	Desarrollar APIs abiertas para mejorar la interoperabilidad entre plataformas TICs de las GUC y UU de la división y otras instituciones (FAP, MGP y PNP).	APIs implementadas, número de sistemas interoperables con fuerzas de las GUC y UU de la división y otras instituciones (FAP, MGP y PNP).	Número de APIs abiertas, porcentaje de interoperabilidad alcanzado.	9 meses para la creación y pruebas de las interfaces.	50% de interfaces desarrolladas y pruebas iniciales realizadas.	100% de interfaces creadas y en funcionamiento operativo.	SETEL COORDINACION CON SU EQUIVALENTE CON LAS GUC Y UU DE LA DIVISIÓN Y OTRAS INSTITUCIONES (FAP, MGP Y PNP).

Nota: La presente tabla, de elaboración propia, muestra el plan de acción considerando ocho aspectos significativos para la implementación.

REFERENCIAS BIBLIOGRÁFICAS

Alberts, D. J., Garstka, J. J., & Stein, F. P. (2016). *Network-centric warfare: Thinking about the future of land forces*. CCRP Press.

Baugh, T., & Peterson, K. (2018). *Big data and predictive analytics in military operations.* Journal of Military Informatics, 11(2), 87-102. https://doi.org/10.1109/JMI.2018.0206

Briones, G. (2021). *Capacidades del Sistema de Comando y Control de la 3ª Brigada de* Caballería en la Defensa Activa. http://repositorio.esge.edu.pe/handle/20.500.14141/688

Capdevilla, C. A. (2022). *Guerra Híbrida: Las nuevas tecnologías como instrumento de Guerra*.

p. 64. https://www.ceeriglobal.org/wp-content/uploads/2023/01/Revista-CEERI-Global-N2-1-59-75.pdf

Casale, C. G. (2022). *La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el nivel operacional*. https://cefadigital.edu.ar/bitstream/1847939/2585/1/TFI-MY%20CASALE%20-%20ECSOOMMTT%20-.pdf

Castillo, J. J., & Vásquez, F. M. (2003). *Metodología de la investigación: Guía práctica para la investigación en ciencias sociales (2nd ed.).* Editorial McGraw-Hill.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.)*. Sage Publications. https://us.sagepub.com/en-us/nam/research-design/book245215

Dent, E. B., & Goldberg, S. G. (1999). *Challenging "Resistance to Change".* The Journal of Applied Behavioral Science, 35(1), 25-41. https://doi.org/10.1177/0021886399351003

Davis, F. D. (1989*). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008

Espitia Cubillos, A., Agudelo Calderón, J., & Buitrago Suescún, Ó. (2020). *Innovaciones tecnológicas en las fuerzas militares de los países del mundo: una revisión preliminar*. Revista Científica General José María Córdova, 18(29), 213-235. http://dx.doi.org/10.21830/19006586.537

European Commission. (2003). Innovation and Technology. European Commission. https://ec.europa.eu/info/research-and-innovation_en

Franks, M., & Brown, L. (2017). *Simulation in modern military training.* Military Training Journal, 38(3), 223-239. https://doi.org/10.1016/j.mtj.2017.06.004

Fojón, Enrique (2020). *Era Digital y Fuerzas Armadas», Global Strategy Report, No 14/2020.* https://global-strategy.org/era-digital-y-fuerzas-armadas/

Fredericks, E. P., & Borenstein, N. (2018). *Interoperability challenges for the future of joint warfare: A case study of the U.S. Army and the U.S. Marine Corps.* Defense Systems Review, 17(1), 1-26. https://doi.org/10.1162/dsrv_a_00827

Huamán Baltazar, J. (2021). Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército. http://repositorio.esge.edu.pe/handle/20.500.14141/692

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education. https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Huertas, P. (2023). *La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, 2022,* p.2. https://repositorio.ucv.edu.pe/handle/20.500.12692/118434

International Organization for Standardization. (2008). *ISO/IEC 2382-01:2008 Information technology — Vocabulary — Part 1: Fundamental terms*. ISO. https://www.iso.org/standard/41542.html

Kessel, S. M. (2021). *Tactical information networks in modern warfare.* Military Communications Journal, 22(1), 45-59. https://doi.org/10.1016/j.milcom.2021.01.008

Kotter, J. P. (1996). Leading change. Harvard Business School Press. https://www.kotterinc.com/methodology/8-steps/

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Sage Publications. https://us.sagepub.com/en-us/nam/naturalistic-inquiry/book226263

Lodeiro Encina, A. (2021). *Evolución y proyecciones del uso de Big Data en Defensa.* Cuaderno de Trabajo N°9-2021, p.15. https://www.publicacionesanepe.cl/index.php/cdt/article/view/961

Mires, D. & Reyes, G. (2023). *Importancia de la inteligencia táctica militar y policial en la producción de inteligencia estratégica nacional.* Revista Académica de la escuela de Posgrado de la Policía Nacional del Perú, 3(1), 82-90. https://doi.org/10.59956/escpograpnpv3n1.8

Montes Vallejo, C. F. (2022). *Inteligencia artificial y el aprendizaje automático en la ciberseguridad*. Revista de la Universidad Piloto de Colombia, https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/13395/Inteligencia%20Artificial%20y%20el%20Aprendizaje%20Autom%C3%A1tico%20en%20la%20Ciberseguridad.pdf?sequence=1

National Institute of Standards and Technology. (2023). *Cybersecurity Framework*. NIST. https://www.nist.gov/cyberframework

Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Sage Publications. https://us.sagepub.com/en-us/nam/qualitative-research-and-evaluation-methods/book226264

Pasztor, P., & Shostak, S. (2020). *Cyber threats to U.S. military operations*. War on the Rocks. https://warontherocks.com/tag/cyber/

Quinto, C. & Picón R. (2023). *Uso de la inteligencia Artificial en el Ejército del Perú: Desafíos y Oportunidades.* Revista Peruana de Ciencia y Tecnología. Pag 7-11. https://orcid.org/0000-0001-9995-3941

Rai, A., & Upadhyay, S. (2020). *Challenges and opportunities of implementing cloud computing in the Indian Army*. International Journal of Information and Communication Technology, 16(2), 142-158. https://doi.org/10.1504/IJICT.2020.10023139

Ravera, C. M. L. (2024). *El rol y las capacidades cibernéticas de las Fuerzas Armadas de la República Argentina en el marco de los conflictos futuros* [Tesis de maestría, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas - Argentina]. https://cefadigital.edu.ar/bitstream/1847939/2657/1/TFM%2016-2024%20RAVERA.pdf

Reid, L. (2020). *Operational cybersecurity: Protecting military assets in the digital age.* Security Technology Journal, 18(3), 213-227. https://doi.org/10.1016/j.stj.2020.04.001

Rogers, E. M. (1962). *Diffusion of innovations*. Free Press. https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html

Sampieri, R. H. (2014). Metodología de la investigación (6ª ed.). McGraw-Hill. https://www.mheducation.es/

Schneider, B. (1985). *Organizational Culture and Climate*. Addison-Wesley. https://books.google.com/books/about/Organizational_Culture_and_Climate.html?id=yd8IAQAAIAAJ

Shannon, C. E., & Weaver, W. (1949). *The mathematical theory of communication*. University of Illinois Press.

Simon, H. A. (1977). *The new science of management decision*. Prentice-Hall.

Smith, M., & Peterson, K. (2019). *Overcoming organizational resistance to change: A case study of the adoption of enterprise resource planning (ERP) systems in the U.S. Army*. Journal of Information Systems Management, 30(3), 223-238. https://doi.org/10.1080/08972241.2019.1612441

Saltos Narváez, H. F. (2021). *Análisis de las nuevas tecnologías en las TIC y el mando y control (oportunidades y amenazas).* Maestría en Defensa y Seguridad. Universidad de las Fuerzas Armadas ESPE. https://repositorio.espe.edu.ec/bitstream/21000/27062/1/T-ESPE-017349.pdf

Scott, W. R. (2003). Organizations: Rational, natural, and open systems. Prentice Hall. https://www.jstor.org/stable/3339861

Slack, N., Chambers, S., & Johnston, R. (2013). *Operations Management (7th ed.)*. Pearson Education Limited.

Teece, D. J., Pisano, G., & Shuen, A. (1997). *Dynamic capabilities and strategic management.* Strategic Management Journal, 18(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199707)18:7<509::AID-SMJ882>3.0.CO;2-Z

Vega Castro, H. (2021). *Empleo de las tecnologías de información y comunicaciones en las acciones de gestión de riesgo de desastres del Agrupamiento de Comunicaciones "José Olaya", 2021.* http://repositorio.esge.edu.pe/browse?type=author&value=Vega+Castro%2C+Hugo

Vicaña, V. & Chafloque, C. (2021, agosto 30). *Propuesta de solución informática web y móvil, que automatice el control y monitoreo de las patrullas desplegadas en situación de emergencia, en entornos urbanos, utilizando georreferenciación y base de datos en tiempo real.* https://repositorioacademico.upc.edu.pe/handle/10757/657540

Villarrubia Marcelo, G. Á. (2021). *Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la Región Lima, 2018* [Tesis de maestría, Centros de Altos Estudios Nacionales]. https://repositorio.caen.edu.pe/server/api/core/bitstreams/cdccbd52-9e8f-4c82-80ff-3b5260d9b677/content

Vroom, V. H. (1964). *Work and motivation*. Wiley.

Wiener, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. MIT Press.

Wu, D., & Lee, J. (2022*). Emerging technologies and their impact on military operations.* Defense Science Journal, 72(5), 499-510. https://doi.org/10.14429/dsj.72.17139

Yataco Velásquez, Y. V. L. (2020). *Optimización de los sistemas de vigilancia de frontera terrestre y franja de frontera para actuar contra delitos fronterizos y ambientales.* https://repositorio.escuelamilitar.edu.pe/handle/EMCH/321

ANEXOS

- Anexo 1: Matriz de categorización
- Anexo 2: Validación de instrumento
- Anexo 3: Instrumento de Recolección de Información
- Anexo 4: Autorización para la recolección de Información
- Anexo 5: Consentimiento informado

Anexo 1: Matriz de categorización

PROBLEMAS	OBJETIVOS	CATEGORIAS Y SUB CATEGORÍAS	METODOLOGÍA
Problema general: ¿Cuáles son los principales desafíos que enfrenta la 3ª Brigada Blindada en la implementación exitosa de las Tecnologías de la Información y las Comunicaciones (TICs) en sus operaciones y acciones terrestres unificadas durante el año 2025? **Problemas específicos:** **1.** ¿Cuáles son las principales limitaciones tecnológicas y de infraestructura que afectan la implementación de las TICs en las operaciones de la 3ª Brigada Blindada? **2.** ¿Qué nivel de capacitación y preparación tiene el personal militar para utilizar eficazmente las TICs en las operaciones y acciones terrestres? **3.** ¿Qué barreras organizacionales y culturales están impidiendo la adopción de las TICs en la 3ª Brigada Blindada? **4.** ¿Qué estrategias y medidas se pueden implementar para superar las vulnerabilidades de ciberseguridad asociadas a la adopción de TICs y lograr la interoperabilidad de los sistemas en las operaciones militares?	**Objetivo general:** Analizar los principales desafíos que enfrenta la 3ª Brigada Blindada en la implementación exitosa de las TICs en sus operaciones y acciones terrestres unificadas durante el año 2025. **Objetivos Específicos:** **1.** Identificar las limitaciones tecnológicas e infraestructurales (hardware, software y conectividad) que afectan la implementación de las TICs en las operaciones de la 3ª Brigada Blindada. **2.** Evaluar el nivel de capacitación y preparación (conocimiento y habilidades) del personal militar en el uso eficaz de TICs durante las operaciones y acciones terrestres. **3.** Determinar las barreras organizacionales y culturales (cultura, liderazgo y procesos) que dificultan la adopción de las TICs en la 3ª Brigada Blindada. **4.** Proponer estrategias y medidas (planes de capacitación, mejoras de infraestructura, protocolos de seguridad) para mitigar las vulnerabilidades de ciberseguridad relacionadas con la adopción de TICs y la interoperabilidad de los sistemas en las operaciones militares.	**A) Desafíos en la implementación de TICS** - Implementación técnica (infraestructura, software, conectividad) - Cultura organizativa (liderazgo, procesos, cultura) - Seguridad Cibernética (vulnerabilidades, amenaza. **B) Impacto de las TICS en operaciones y acciones terrestres** - Eficiencia Operativa (tiempos de respuesta, coordinación, toma de decisiones) - Interoperabilidad (comunicación, colaboración, integración de sistemas) - Adaptación a la Innovación Tecnológica (flexibilidad, capacidad de aprendizaje, mejora continua)	**Enfoque de investigación:** Enfoque Cualitativo **Tipo de investigación:** Teórico - Empírico **Método de investigación:** Hermenéutico interpretativo **Muestra:** Diez (10) oficiales de estado mayor del grado de mayor, teniente coronel y coronel **Técnica:** Entrevista en profundidad Revisión documentaria Observación **Instrumentos:** Guía de entrevista Guía de análisis documental Guía de observación **Técnica de procesamiento y análisis de información:** Software Python y las bibliotecas NetworkX, Matplotlib y NLTK

Anexo 2. Validación de Instrumento

Anexo 2. Validación de Instrumento

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 31 de ENERO del 2025

Informe N.° 001
De: Mg. Ulises Barzola Pérez
Para: Edgar Jonathan Ortega Goyzueta

Me dirijo a Usted respetuosamente para saludarlo y agradecer la designación para la evaluación de la **Validez de Contenido** de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025"**

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (X)
b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

Mg. Nombres y Apellidos: Mg. Ulises Erick Barzola Pérez
Código ORCID : 0009 - 0003 - 0469 - 3692

Anexo 2. Validación de Instrumento

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 31 de ENERO del 2025

Informe N.° 002

De: RICARDO ALFONSO CARRILLO ESPICHÁN

Para: Joyce Paola Calizaya Maldonado

Me dirijo a Usted respetuosamente para saludarlo y agradecer la designación para la evaluación de la **Validez de Contenido** de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025"**

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (X)

b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

Mg. Nombres y Apellidos: RICARDO ALFONSO CARRILLO ESPICHÁN

Código ORCID : 0009-0000-7796-210X

Anexo 2. Validación de Instrumento

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 31 de Enero del 2025

Informe N.° 003

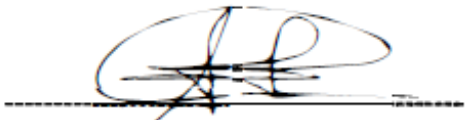
De: MARLENE EVELYN ORTIZ GUZMÁN

Para: Joyce Paola Calizaya Maldonado

Me dirijo a Usted respetuosamente para saludarlo y agradecer la designación para la evaluación de la **Validez de Contenido** de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025"**

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (X)
b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )



Mg. Nombres y Apellidos: Marlene Evelyn Ortiz Guzmán

Código ORCID : 0009-0000-1992-9491

Anexo 2. Validación de Instrumento

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 31 de Enero del 2025

Informe N.° 004

De: Javier Cesinario Mondragón

Para: Edgar Jonathan Ortega Goyzueta

Me dirijo a Usted respetuosamente para saludarlo y agradecer la designación para la evaluación de la **Validez de Contenido** de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025"**

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (X)
b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

Dr. Nombres y Apellidos: Javier Cesinario Mondragón

Código ORCID : 0009-0004-7360-4953

Anexo 2. Validación de Instrumento

PERÚ	Ministerio de Defensa	Ejército del Perú	COEDE Escuela Superior de Guerra del Ejército Escuela de Posgrado

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

Chorrillos, 31 de ENERO del 2025

Informe N.° 005

De: Jorge Rodrigo López García

Para: Edgar Jonathan Ortega Goyzueta

Me dirijo a Usted respetuosamente para saludarlo y agradecer la designación para la evaluación de la **Validez de Contenido** de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025"**

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (X)
b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

Mg. Nombres y Apellidos: JORGE RODRIGO LÓPEZ GARCÍA

Código ORCID : 0000-0002-3197-8314

Anexo 3. Instrumento de recolección de datos

GUÍA DE ENTREVISTA SEMIESTRUCTURADA

Buenos dias, me encuentro desarrollando un trabajo de investigación para obtener el grado académico de Maestro con mención en Planeamiento Estratégico y Toma de Decisiones, en la Escuela Superior de Guerra del Ejército – Escuela de Posgrado, habiendo elegido el tema titulado: **"Desafíos en la Implementación de TICs durante las operaciones y acciones terrestres unificadas en la 3ª Brigada Blindada, Moquegua, 2025".** Por lo que desarrollaré esta entrevista y desde ya le agradezco su gentil colaboración.

Teniendo en consideración su conocimiento y experiencia profesional, tenga a bien responder las siguientes preguntas:

Categorías	Sub Categorías	Preguntas
Desafíos en la Implementación de TICs	**Implementación Técnica**	1. ¿Cuáles son los principales retos técnicos que ha enfrentado la 3ra Brigada Blindada en la implementación de TICs durante operaciones y acciones terrestres unificadas?
		2. ¿Cómo se han abordado las dificultades en la integración de nuevos sistemas TIC con las plataformas tecnológicas ya existentes en la Brigada?
		3. ¿Qué mejoras técnicas podrían implementarse para optimizar el despliegue y la operatividad de TICs en escenarios de combate?
		4. ¿Cómo se han gestionado los problemas relacionados con la compatibilidad de sistemas de comunicación e información en operaciones de gran escala?
	Cultural y Organizativa	1. ¿Qué resistencias culturales y organizativas se han identificado dentro de la 3ra Brigada Blindada respecto a la adopción de TICs en las operaciones militares?
		2. ¿De qué manera la estructura organizativa actual de la Brigada ha facilitado o dificultado la implementación de TICs?
		3. ¿Cómo se ha manejado la transición hacia una cultura más orientada al uso de tecnologías avanzadas en el entorno operativo de la Brigada?
		4. ¿Qué estrategias de cambio organizacional se han empleado o podrían emplearse para mejorar la aceptación y uso de TICs entre el personal militar?
	Seguridad Cibernética	1. ¿Qué desafíos específicos de seguridad cibernética se han encontrado al integrar TICs en las operaciones y acciones terrestres de la 3ra Brigada Blindada?

Categorías	Sub Categorías	Preguntas
		2. ¿Cómo se ha preparado la Brigada para defenderse contra las amenazas cibernéticas en el contexto de la guerra moderna, y qué brechas de seguridad persisten?
		3. ¿Cuál es la capacidad actual de la Brigada para detectar, mitigar y responder a ciberataques en tiempo real durante las operaciones militares?
		4. ¿Qué medidas adicionales podrían implementarse para fortalecer la resiliencia cibernética en las operaciones de la Brigada?
Impacto de las TICs en operaciones y acciones terrestres	**Eficiencia Operativa**	1. ¿Cómo ha impactado la implementación de TICs en la eficiencia operativa de la 3ra Brigada Blindada durante las operaciones y acciones terrestres unificadas?
		2. ¿Qué áreas específicas de las operaciones militares han experimentado mejoras significativas debido a la adopción de TICs?
		3. ¿Qué desafíos han surgido en términos de eficiencia operativa tras la integración de TICs en el campo de batalla?
		4. ¿Qué indicadores de desempeño se utilizan para evaluar la eficiencia operativa después de la implementación de TICs en las operaciones de la Brigada?
	Interoperabilidad	1. ¿Cómo ha afectado la implementación de TICs a la interoperabilidad entre diferentes unidades y sistemas en las operaciones y acciones terrestres de la 3ra Brigada Blindada?
		2. ¿Qué problemas de interoperabilidad se han encontrado al integrar TICs con sistemas de armas, comunicaciones y otros equipos en el terreno?
		3. ¿Qué soluciones se han implementado o se podrían implementar para mejorar la interoperabilidad de sistemas TIC en operaciones militares conjuntas?
		4. ¿Cómo se garantiza que las TICs utilizadas en la Brigada sean compatibles y efectivas en un entorno de coalición o con fuerzas aliadas?
	Adaptación a la Innovación Tecnológica	1. ¿Cómo se ha adaptado la 3ra Brigada Blindada a las innovaciones tecnológicas recientes en el ámbito de las TICs?
		2. ¿Qué desafíos ha enfrentado la Brigada en la integración de nuevas tecnologías de TIC, y cómo se han superado?
		3. ¿Qué medidas se han tomado para asegurar una actualización continua y efectiva de las tecnologías de TIC en la Brigada?
		4. ¿Cómo evalúa la capacidad de la Brigada para mantenerse a la vanguardia de la innovación tecnológica en TICs en comparación con otras unidades militares?

Fuente: Elaboración propia.

Anexo 3. Instrumento de recolección de datos

FICHA DE ANÁLISIS DOCUMENTAL

Se seleccionó los documentos considerados de mayor relevancia para la elaboración del estudio, considerando fuentes relevantes de las bases de datos, decretos, leyes, manuales, reglamentos, directivas, entre otros. De esta forma, el análisis se centra en identificar directrices claves sobre desafíos técnicos, culturales y de ciberseguridad, además de evaluar la eficiencia e interoperabilidad de TICs en operaciones y acciones militares.

Tipo de Documento	Referencia	Tema Seleccionado
Decreto Supremo N° 085-2023-PCM: Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030	Presidencia del Consejo de Ministros. (2023). *Decreto Supremo N° 085-2023-PCM: Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030*. https://www.gob.pe/institucion/pcm/normas-legales/4471543-085-2023-pcm	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Decreto Supremo N° 009-2021-PCM: Reglamento de la Ley de Gobierno Digital	Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 009-2021-PCM: Reglamento de la Ley de Gobierno Digital*. https://www.gob.pe/institucion/pcm/normas-legales/413709-decreto-supremo-n-009-2021-pcm-reglamento-de-la-ley-de-gobierno-digital	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Ley N° 30999 - Ley de Ciberdefensa	Congreso de la República del Perú. (2020). *Ley N° 30999 - Ley de Ciberdefensa*. Diario Oficial El Peruano. https://www.elperuano.pe/NormasElperuano/Detalle.aspx?referencia=30999	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 140-2020-PCM: Política Nacional de Transformación Digital del Estado	Presidencia del Consejo de Ministros. (2020). *Decreto Supremo N° 140-2020-PCM: Política Nacional de Transformación Digital del Estado*. https://www.gob.pe/institucion/pcm/normas-legales/380269-decreto-supremo-n-140-2020-pcm-politica-nacional-de-transformacion-digital-del-estado	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Decreto Supremo N° 003-2021-PCM: Estrategia Nacional de Ciberseguridad	Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 003-2021-PCM: Estrategia Nacional de Ciberseguridad*. https://www.gob.pe/institucion/pcm/normas-legales/419222-decreto-supremo-n-003-2021-pcm-estrategia-nacional-de-ciberseguridad	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 019-2020-PCM: Estrategia Nacional de Gobierno Digital	Presidencia del Consejo de Ministros. (2020). *Decreto Supremo N° 019-2020-PCM: Estrategia Nacional de Gobierno Digital*. https://www.gob.pe/institucion/pcm/normas-legales/407442-decreto-supremo-n-019-2020-pcm-estrategia-nacional-de-gobierno-digital	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Ley N° 29571: Ley de Protección de Datos Personales	Congreso de la República del Perú. (2010). *Ley N° 29571: Ley de Protección de Datos Personales*. Diario Oficial El Peruano. https://www.gob.pe/institucion/pcm/normas-legales/29571-ley-de-proteccion-de-datos-personales	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 012-2024-PCM: Reglamento de la Ley de Ciberdefensa	Presidencia del Consejo de Ministros. (2024). *Decreto Supremo N° 012-2024-PCM: Reglamento de la Ley de Ciberdefensa*. https://www.gob.pe/institucion/pcm/normas-legales/337567-reglamento-de-la-ley-de-ciberdefensa	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 004-2020-PCM: Decreto Supremo	Presidencia del Consejo de Ministros. (2020). *Decreto Supremo N° 004-2020-PCM: Decreto Supremo sobre el Sistema de Gobierno Digital*. https://www.gob.pe/institucion/pcm/normas-legales/398018-	**Desafíos en la Implementación de TICs** (Implementación Técnica)

sobre el Sistema de Gobierno Digital	decreto-supremo-n-004-2020-pcm-decreto-supremo-sobre-el-sistema-de-gobierno-digital	
Política Nacional de Ciberseguridad	Gobierno del Perú. (2020). *Política Nacional de Ciberseguridad. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC705258316005706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf*	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Directiva N° 001-2019-PCM: Política Nacional de Transformación Digital en el Sector Público	Presidencia del Consejo de Ministros. (2019). *Directiva N° 001-2019-PCM: Política Nacional de Transformación Digital en el Sector Público*. https://www.gob.pe/institucion/pcm/normas-legales/271090-directiva-n-001-2019-pcm-politica-nacional-de-transformacion-digital-en-el-sector-publico	**Desafíos en la Implementación de TICs (Cultural y Organizativa)**
Directiva Única de Funcionamiento del Sistema de Telemática del Ejército (DUFSITELE, 2021)	Ejército del Perú. (2021). *Directiva Única de Funcionamiento del Sistema de Telemática del Ejército (DUFSITELE, 2021)*. https://www.ejercito.mil.pe/nuestroejercito/normas-y-procedimientos	**Desafíos en la Implementación de TICs** (Implementación Técnica)
MACOFFAA (Manual de Comunicaciones Operacionales de las Fuerzas Armadas del Perú, 2019)	Ejército del Perú. (2019). *MACOFFAA (Manual de Comunicaciones Operacionales de las Fuerzas Armadas del Perú, 2019)*. https://www.ejercito.mil.pe/nuestroejercito/normas-y-procedimientos	**Impacto de las TICs en Operaciones Terrestres** (Interoperabilidad)
Decreto Supremo N° 085-2023-PCM: Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030	Presidencia del Consejo de Ministros. (2023). *Decreto Supremo N° 085-2023-PCM: Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030*.	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Decreto Supremo N° 009-2021-PCM: Reglamento de la Ley de Gobierno Digital	Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 009-2021-PCM: Reglamento de la Ley de Gobierno Digital*. https://www.gob.pe/institucion/pcm/normas-legales/413709-decreto-supremo-n-009-2021-pcm-reglamento-de-la-ley-de-gobierno-digital	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Ley N° 30999 - Ley de Ciberdefensa	Congreso de la República del Perú. (2020). *Ley N° 30999 - Ley de Ciberdefensa*. Diario Oficial El Peruano. https://www.elperuano.pe/NormasElperuano/Detalle.aspx?referencia=30999	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 140-2020-PCM: Política Nacional de Transformación Digital del Estado	Presidencia del Consejo de Ministros. (2020). *Decreto Supremo N° 140-2020-PCM: Política Nacional de Transformación Digital del Estado*. https://www.gob.pe/institucion/pcm/normas-legales/380269-decreto-supremo-n-140-2020-pcm-politica-nacional-de-transformacion-digital-del-estado	**Desafíos en la Implementación de TICs** (Implementación Técnica)
Decreto Supremo N° 003-2021-PCM: Estrategia Nacional de Ciberseguridad	Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 003-2021-PCM: Estrategia Nacional de Ciberseguridad*. https://www.gob.pe/institucion/pcm/normas-legales/419222-decreto-supremo-n-003-2021-pcm-estrategia-nacional-de-ciberseguridad	**Desafíos en la Implementación de TICs** (Seguridad Cibernética)
Decreto Supremo N° 019-2020-PCM: Estrategia Nacional de Gobierno Digital	Presidencia del Consejo de Ministros. (2020). *Decreto Supremo N° 019-2020-PCM: Estrategia Nacional de Gobierno Digital*. https://www.gob.pe/institucion/pcm/normas-legales/407442-decreto-supremo-n-019-2020-pcm-estrategia-nacional-de-gobierno-digital	**Desafíos en la Implementación de TICs** (Implementación Técnica)

Anexo 3. Instrumento de recolección de datos

Guía de Observación

GUÍA DE OBSERVACIÓN CUALITATIVA			
Observación No.	01	Fecha:	15/02/2025
Lugar:	MOQUEGUA - PERÚ		
Espacio-Situación:	Ejercicio de Comunicaciones a nivel Brigada		
Aspectos Observados	Consideraciones interpretativas/Analíticas respecto al aspecto observado		
Destreza en el uso de dispositivos TIC, rapidez y precisión en operaciones; identificación y resolución de problemas técnicos.	✓ Observé que los entornos con interferencias y condiciones extremas afectan severamente la funcionalidad de las TICs. Considero necesario implementar sistemas de conmutación adaptativa y redundancia de señal en tiempo real para mitigar estas dificultades.		
Ajustes y soluciones ante dificultades técnicas en condiciones desafiantes (ruido, clima, espacio limitado).	✓ Durante la observación, noté que la falta de soporte técnico constante en campo limita la continuidad de las mejoras en coordinación en tiempo real. A pesar del uso de dispositivos portátiles y redes de alta frecuencia, esta deficiencia reduce la efectividad operativa.		
Indicadores de disposición, resistencia o aceptación hacia las TICs; grado de uso autónomo o sólo bajo instrucción.	✓ Percibí una fuerte resistencia en el personal a adoptar nuevas TICs, principalmente debido al desconocimiento de sus beneficios operativos. Recomiendo un programa de capacitación práctica basado en escenarios de combate simulados para demostrar su eficacia.		
Observación de la reacción ante la introducción de nuevas TICs, incluyendo iniciativa, entusiasmo o resistencia.	✓ Noté una disposición creciente del personal a adoptar nuevas tecnologías luego de participar en entrenamientos prácticos. Sugiero establecer un programa continuo de actualización tecnológica para mantener la competitividad de la brigada.		
Adherencia a medidas de seguridad establecidas en el uso de TICs, protección de datos sensibles y control de accesos.	✓ Identifiqué que los sistemas actuales de ciberseguridad son vulnerables a amenazas avanzadas. Propongo implementar inteligencia artificial (IA) para la detección proactiva de patrones de ataque, especialmente en redes críticas de comunicación táctica.		
Conducta y tiempo de respuesta frente a simulacros de ataques cibernéticos, y nivel de conocimiento en ciberseguridad.	✓ Se evidenció la necesidad de un enfoque proactivo en ciberseguridad. Recomiendo la integración de IA para la detección temprana de amenazas y la mejora de la infraestructura de protección de datos.		

Reducción de tiempos de respuesta y eficacia en la toma de decisiones; uso de TICs para mejorar la coordinación y ejecución de tareas.	✓ Las TICs han mejorado la coordinación en tiempo real, pero la falta de soporte técnico continuo afecta la sostenibilidad de estas mejoras. Es clave reforzar el soporte en campo para garantizar la operatividad eficiente.
Nivel de integración y cooperación entre TICs de diferentes unidades o sistemas; efectividad en la comunicación intersistemas.	✓ Observé que la interoperabilidad ha mejorado, pero la falta de estandarización genera dificultades en operaciones multinacionales. Sugiero la implementación de estándares de comunicación unificados para facilitar la colaboración con aliados.
Actitudes de apertura, disposición al aprendizaje continuo, y capacidad de adaptación frente a nuevas tecnologías.	✓ Considero que la adopción de nuevas TICs puede acelerarse mediante programas continuos de actualización y capacitación. La resistencia inicial puede ser reducida con un enfoque práctico que demuestre su utilidad operativa.
Observaciones adicionales:	✓ La implementación de sistemas de conmutación adaptativa es clave para garantizar la operatividad de las TICs en entornos hostiles. ✓ La capacitación del personal en escenarios de combate simulados facilitará la aceptación y uso eficiente de las tecnologías. ✓ La estandarización de los sistemas de comunicación contribuirá a una mejor interoperabilidad en operaciones conjuntas.
Nombre del investigador-Observador	MY COM ORTEGA GOYZUETA EDGAR JONATHAN

Guía de Observación

GUÍA DE OBSERVACIÓN CUALITATIVA			
Observación No.	02	Fecha:	15/02/2025
Lugar:	MOQUEGUA - PERÚ		
Espacio-Situación:	Ejercicio de Comunicaciones a nivel Brigada		
Aspectos Observados	Consideraciones interpretativas/Analíticas respecto al aspecto observado		
Destreza en el uso de dispositivos TIC, rapidez y precisión en operaciones; identificación y resolución de problemas técnicos.	✓ Durante la observación, noté que la infraestructura actual limita significativamente la cobertura en zonas remotas. Considero esencial una modernización tecnológica específica para estas áreas críticas, mediante la implementación de antenas de alta ganancia y redes de baja latencia.		
Ajustes y soluciones ante dificultades técnicas en condiciones desafiantes (ruido, clima, espacio limitado).	✓ Si bien las TICs han mejorado la logística y el mapeo táctico, observé que los problemas de conectividad en áreas remotas siguen afectando la rapidez en la toma de decisiones. Recomiendo la implementación de estaciones móviles de respaldo en zonas críticas para garantizar la operatividad.		
Indicadores de disposición, resistencia o aceptación hacia las TICs; grado de uso autónomo o sólo bajo instrucción.	✓ Identifiqué una resistencia moderada a la adopción de nuevas TICs, en particular a los especialistas técnicos que tienen mas de 15 años de servicio. Si bien no es abiertamente visible, hay barreras en la cadena de mando que limitan la toma de decisiones rápida. Considero que una estructura más flexible permitiría una adopción ágil de estas tecnologías.		
Observación de la reacción ante la introducción de nuevas TICs, incluyendo iniciativa, entusiasmo o resistencia.	✓ Noté que la percepción de complejidad de las TICs avanzadas hace que el cambio sea lento. Un modelo de mentoría, en el que personal experimentado guíe a los nuevos usuarios en el uso de TICs en campo, sería una estrategia adecuada para facilitar la transición.		
Adherencia a medidas de seguridad establecidas en el uso de TICs, protección de datos sensibles y control de accesos.	✓ Un aspecto preocupante que observé es la falta de un sistema de respuesta automatizada que permita detectar y mitigar ataques en tiempo real. Considero fundamental la implementación de sistemas de encriptación más robustos para garantizar la integridad de los datos en operaciones.		
Conducta y tiempo de respuesta frente a simulacros de ataques cibernéticos, y nivel de	✓ Se evidenció la necesidad de un sistema automatizado de respuesta a ciberataques. La implementación de sistemas avanzados de encriptación fortalecería la seguridad en operaciones tácticas y reduciría la vulnerabilidad ante amenazas cibernéticas.		

conocimiento en ciberseguridad.	
Reducción de tiempos de respuesta y eficacia en la toma de decisiones; uso de TICs para mejorar la coordinación y ejecución de tareas.	✓ Sugiero la modernización de la infraestructura de telecomunicaciones para mejorar la conectividad en zonas críticas. Asimismo, la implementación de estaciones móviles de respaldo optimizaría la eficiencia operativa y reduciría los tiempos de respuesta en situaciones de emergencia.
Nivel de integración y cooperación entre TICs de diferentes unidades o sistemas; efectividad en la comunicación intersistemas.	✓ He observado que los problemas de interoperabilidad se deben a la diversidad de generaciones de equipos en uso. Recomiendo una actualización progresiva de los sistemas y una capacitación cruzada para mejorar la sincronización y la comunicación entre unidades.
Actitudes de apertura, disposición al aprendizaje continuo, y capacidad de adaptación frente a nuevas tecnologías.	✓ La percepción de complejidad de las TICs avanzadas sigue siendo un obstáculo para su adopción. Propongo establecer un programa de mentoría, donde personal experimentado pueda guiar a los nuevos usuarios en el uso adecuado de estas tecnologías.
Observaciones adicionales:	✓ Considero que la modernización de la infraestructura tecnológica en zonas críticas es esencial para garantizar la continuidad de las operaciones tácticas. ✓ La implementación de sistemas de seguridad avanzados fortalecería la integridad de las operaciones en escenarios desafiantes. ✓ La interoperabilidad entre unidades podría mejorar significativamente con la implementación de un estándar de comunicación unificado y una capacitación técnica especializada.
Nombre del investigador-Observador	MY COM CALIZAYA MALDONADO JOYCE PAOLA

Anexo 4. Autorización para la Recolección de Información

PERÚ | Ministerio de Defensa | Ejército del Perú | 3ª Brigada Blindada

"Año del Bicentenario de la consolidación de nuestra independencia y de la Conmemoración de las heroicas Batallas de Junín y Ayacucho"

Moquegua, 18 de diciembre del 2024

Oficio Nº 116/3a Brig Blin/SG-3BB

Señor My Com ORTEGA GOYZUETA Edgar Jonathan. - **CHORRILLOS**
(Maestrando de la XXIII MCCMM de la ESGE-EPG)

Asunto : Respuesta a su solicitud de autorización para acceso al personal militar y uso del nombre de la 3ª Brigada Blindada para Investigación

Ref. : Solicitud Nº 001-2024/EOG del 05 de julio del 2024.

Tengo el agrado de dirigirme a usted para saludarlo cordialmente y a la vez manifestarle que, con relación al documento de la referencia, en el cual se solicitó autorización para acceder al personal militar de esta Gran Unidad con el fin de invitarlos a participar en el estudio de investigación que están realizando la señora My Com CALIZAYA MALDONADO Joyce Paola y usted señor My Com ORTEGA GOYZUETA Edgar Jonathan, para obtener el grado de Magíster en la Escuela Superior de Guerra - Escuela de Post Grado, asi como, al uso del nombre de Brigada en su referido estudio.

Al respecto, se le hace de conocimiento que dicha autorización ha sido considerada **VIABLE,** y al finalizar su estudio agradeceré remitir el informe general con los resultados de su investigación.

Hago propicia la oportunidad para reiterarle los sentimientos de mi especial consideración y deferente estima personal.

Dios Guarde a Ud.

TERCERA BRIGADA BLINDADA - COMANDANCIA GENERAL

DNI - 21627370 – A+
JULIO ULISES MORI RABANAL
General de Brigada
Comandante General de la 3a Brig Blin

DISTRIBUCION:
- Interesado..... 01
- Archivo..... 01/02

Anexo 5. Formato de Consentimiento Informado

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

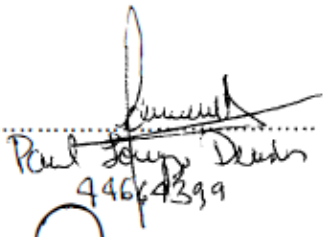
Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

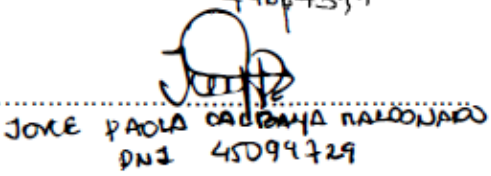
Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: .....



Investigador: Nombre y apellido, DNI y firma: .....



CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Giancarlo Uribe Acosta 43147428

Investigador: Nombre y apellido, DNI y firma:

EDGAR JONATHAN ORTEGA GOYZUETA
44635865

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Titulo de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafios operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Graciela Gomes Huaraca
DNI : 70470630

Investigador: Nombre y apellido, DNI y firma: Joyce Paola Calizaya Maldonado
DNI: 45099729

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: .....
I, [illegible] Y. DNI 41723511

Investigador: Nombre y apellido, DNI y firma: Joyce Paola Calizaya Maldonado
DNI: 45099729

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: ERNESTO HERNANDEZ MALCA DNI 44510338

Investigador: Nombre y apellido, DNI y firma: JOYCE PAOLA CALIZAYA MALDONADO
DNI 45094429

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: "***Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: .....
NICOLAS GUTIERREZ BARRERO
DNI 44742901

Investigador: Nombre y apellido, DNI y firma: .....
JOYCE PAOLA CALIZAYA MALDONADO
DNI 45099729

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: "***Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Richard Raúl Figueroa Zachilla, 43622475

Investigador: Nombre y apellido, DNI y firma:

EDGAR JONATHAN ORTEGA GOYZUETA
44635865

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

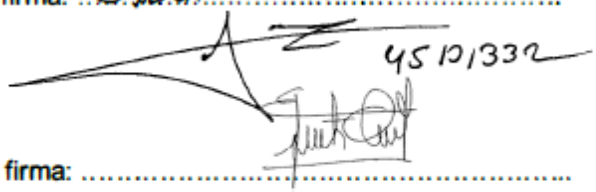
Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: "***Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Javier Richard Zuñiga Alfonte



Investigador: Nombre y apellido, DNI y firma: .....

EDGAR JONATHAN ORTEGA GOYZUETA
44635865

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: ***"Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide participar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Rodi Makol Velazco Puyo, 46316048

Investigador: Nombre y apellido, DNI y firma: .

EDGAR JONATHAN ORTEGA GOYZUETA
44635865

CONSENTIMIENTO INFORMADO

Escuela Superior de Guerra del Ejército- Escuela de Posgrado

Investigador (es): MY EP Edgar Jonathan Ortega Goyzueta
MY EP Joyce Paola Calizaya Maldonado

Título de Tesis: "***Desafíos en la implementación de TICs durante las operaciones y acciones terrestres unificadas de la 3ª Brigada Blindada, Moquegua, 2025".***

Propósito del estudio: El propósito de este estudio es analizar y evaluar los desafíos que enfrenta la 3ª Brigada Blindada en la implementación efectiva de Tecnologías de la Información y Comunicación (TICs) durante las operaciones y acciones terresres unificadas. Su ejecución permitirá identificar los desafíos operativos y organizacionales que dificultan la integración óptima de las TICs.
Procedimiento: Si usted decide pártiçipar en este estudio, se realizará lo siguiente:
La entrevista puede demorar unos 45 minutos aproximadamente, se realizarán veinticuatro (24) preguntas según la guía semiestructurada, las cuales deben ser respondidas de acuerdo a su conocimiento y experiecia profesional. Los resultados de la investigación se le entregará a usted en forma individual y se almacenará respetando la confidencialidad y el anonimato.
Riesgos: La investigación no presentará riesgo alguno para su integridad física ni emocional.
Beneficios : Considerar la relevancia social y/o institucional de la investigación.
Costos e incentivos: Usted no deberá pagar nada por la participación. Tampoco recibirá ningún incentivo económico a cambio de su participación.
Confidencialidad: Nosotros guardaremos la información de manera anónima, utilizando códigos y no con nombres. Si los resultados de este estudio son publicados, no se mostrará ninguna información que permita su identificación.
Si tiene alguna duda y necesita mayor información puede comunicarse con el My EP Edgar Ortega Goyzueta al teléfono: 988177774, o con la My EP Joyce Calizaya Maldonado al teléfono: 936298912.

CONSENTIMIENTO: Acepto voluntariamente participar en este estudio. Recibiré una copia firmada de este consentimiento.

Participante: Nombre y apellido, DNI y firma: Jacqueline García Trinidad, 44565780

Investigador: Nombre y apellido, DNI y firma: .

EDGAR JONATHAN ORTEGA GOYZUETA
44635865