-ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR LAS OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES JOSÉ OLAYA, 2023

AUTOR

Bach. Christian VELAZCO CORNELIO
0009-0001-9600-8087

Proyecto para al Grado Académico de**:**

MAGISTER EN CIENCIAS MILITARES

Con Mención en Planeamiento Estratégico y Toma de Decisiones

ASESOR

Mg. Gabriela Katherine GALLEGOS CHIARELLA
0000-0002-8241-1342

2024

Página del jurado

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 022 – 2024/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los once (11) días del mes de octubre del año dos mil veinticuatro, siendo las 0900 horas, se reunió el jurado evaluador conformado por los docentes:

❖	Doctor	GAMALIEL MANUEL GUSTAVO TALAVERA PRADO	Presidente
❖	Maestro	FERNANDO JAVIER CANAVAL RAMIREZ	Secretario
❖	Maestra	AMELBA SANDRA CALLA HERMOZA	Vocal

Designados según Resolución de Expedito para Sustentación de Tesis **N° 022-2024/SIE/DGI/ESGE-EPG** del 24 de setiembre de 2024, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR LAS OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA", 2023"**, presentado por el Bachiller **CHRISTIAN VELAZCO CORNELIO**, para optar el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones, 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 APROBADO POR EXCELENCIA

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 Planeamiento Estratégico y Toma de Decisiones.

Firmado, en Chorrillos a los once (11) días del mes de octubre del año dos mil veinticuatro.

DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO
PRESIDENTE

MG. FERNANDO JAVIER CANAVAL RAMIREZ
SECRETARIO

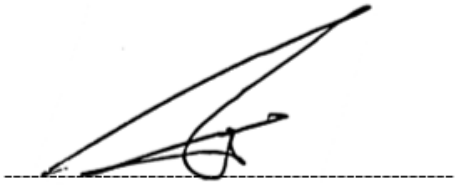
MG. AMELBA SANDRA CALLA HERMOZA
VOCAL

Autorización para publicación y uso

Autorización de Publicación y Uso

yo, Bach. Christian VELAZCO CORNELIO, a través del presente documento autorizo a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado, la publicación del texto parcial de la tesis de grado titulada: **Empleo de Equipos Remotos de Comunicaciones para Incrementar Operaciones de Protección Electrónica en el Agrupamiento de Comunicaciones José Olaya, 2023** presentada para optar el grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones, en el Repositorio Nacional de Tesis (Renati) de la Superintendencia Nacional de Educación Superior Universitaria (Sunedu), de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada, exhibida y usada también con fines académicos siempre que indique la autoría y no se podrá realizar obras derivadas de las misma.

Chorrillos, 20 de mayo de 2024



Christian VELAZCO CORNELIO

43337354

Declaración jurada de auditoría

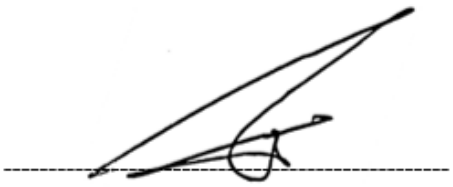
Declaración Jurada de Autoría

Mediante el presente documento, yo, Christian VELAZCO CORNELIO, identificado con Documento Nacional de Identidad N° 43337354, con domicilio real en la Calle Francisco de Zela N° 227, Villa Militar Este, del distrito de Chorrillos provincia de Lima, departamento de Lima, egresado del XXX Curso de Actualización de Egresados para optar el Grado de Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG) declaro bajo juramento que:

Soy el autor de la investigación titulada: **EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES JOSÉ OLAYA, 2023**, que presento a los 15 días del mes de junio del año 2024, ante esta institución con fines de optar al grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones.

Dicha investigación se ha desarrollado respetando los principios éticos propios, no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas y otros que corresponden al suscrito o a otro en respecto irrestricto a los derechos del autor. Declaro conocer y someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseadas, adulteraos, duplicados ni copiados. Que no he cometido fraude científico, plagio vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado y me declaro como el único responsable.



Christian VELAZCO CORNELIO

43337354

Dedicatoria

Gracias a mi esposa Ross Mery y mis hijos Carmen y Ricardo por ser mi estimulación para lograr mis metas, dándome voluntad, tenacidad y convertirme en una persona digna.

Agradecimiento

Al todo el personal de oficiales, técnicos y suboficiales que laboraron y laboran en el Cuartel “Mariano Melgar”, por su contribución y apoyo en el desarrollo del trabajo de investigación.

Índice general

Lista de tablas

Página

Lista de figuras

Resumen

Las experiencias adquiridas por los entrenamientos para guerra convencional determinaron el bajo nivel de Protección Electrónica en el empleo de los medios de comunicaciones radiales, evidenciando vulnerabilidades a las acciones de soporte y ataque electrónico que neutralizaron el apoyo de comunicaciones a las grandes unidades de combate, siendo un riesgo crítico para un conflicto bélico convencional. En ese sentido, se muestra la necesidad de incrementar la protección electrónica. Por lo tanto, el objetivo de la presente indagación fue describir el empleo de los medios remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023. Para dar cumplimiento a este objetivo, se empleó el enfoque cualitativo, de tipo teórico y empírico, con el método fenomenológico-hermenéutico. En el análisis del estudio se emplearon los instrumentos de guía de entrevista, guía de observación y análisis documental y material; la muestra de estudio utilizada fue intencional; se realizó a tres expertos en guerra electrónica y cuatro expertos en comunicaciones que laboraron y laboran en el Cuartel “Mariano Melgar”. Los resultados obtenidos fueron contar con un nuevo empleo de medios de comunicaciones de manera remota, se identificó al Enmascaramiento Electrónico como una nueva operación de protección electrónica, se requirió de un solo operador de radio para su funcionamiento y mediante la distorsión, cubierta y ocultamiento de la frecuencia del Centro de comunicaciones se protegió la información propia para no ser identificada y localizada, contribuyendo con el apoyo de comunicaciones. Llegando a la conclusión de que mendiate un empleo inédito de despliegue, integración y sincronización del material de comunicaciones disponibles en la institución, se pudo incrementar las operaciones de protección electrónica y contribuir con el apoyo de comunicaciones, proporcionado por el Agrupamiento de Comunicaciones “José Olaya”. generando un nuevo conocimiento para nuestra doctrina de guerra electrónica.

Palabras claves: *protección electrónica, enmascaramiento electrónico, apoyo de comunicaciones, operador de radio, empleo.*

Abstract

The experiences acquired through training for conventional warfare determined the low level of Electronic Protection in the use of radio communications means, evidencing vulnerabilities to electronic support and attack that neutralized communications support to large combat units, being a critical risk for a conventional war conflict. In this sense, the need to increase electronic protection is shown. Therefore, the objective of this information was to describe the use of remote communications means to increase electronic protection operations in the “José Olaya” Communications Group, 2023. To comply with this objective, the approach was used qualitative, theoretical and empirical, with the phenomenological-hermeneutic method. In the analysis of the study, the instruments of interview guide, observation guide and documentary and material analysis were used; The study sample used was intentional; three experts in electronic warfare and four communications experts who worked and worked at the “Mariano Melgar” Barracks were carried out. The results obtained were to have a new use of communications means remotely, Electronic Masking was identified as a new electronic protection operation, a single radio operator was required for its operation and through the distortion, cover and concealment of At the frequency of the Communications Center, the information was protected from being identified and located, contributing to communications support. Coming to the conclusion that through an unprecedented use of deployment, integration and synchronization of the communications material available in the institution, it was possible to increase electronic protection operations and contribute to the communications support, provided by the “José Olaya” Communications Group. generating new knowledge for our electronic warfare doctrine.

Keywords: electronic protection, electronic masking, communications support, radio operator, employment.

Capítulo I: Introducción

La Protección Electrónica (PE), como parte de la Guerra Electrónica (GE) en las operaciones, constituye un factor determinante para mantener el empleo de las plataformas de comunicaciones, así como evitar la interceptación, ubicación, perturbación y destrucción como consecuencia de las operaciones de Soporte Electrónico (SE) y Ataque Electrónico (AE) enemigos. En el ámbito internacional, por lo expresado por Vásquez (2020), en el confrontamiento naval desarrollado en Tsushima en el año de 1905, Rusia utilizó, por primera vez, acciones de Ataque Electrónico y Soporte Electrónico en contra de los buques de guerra japoneses, influyendo así en las operaciones navales y abriendo un nuevo escenario en los conflictos futuros; si Rusia hubiera aprovechado la falta de Protección Electrónica de las radios japonesas ante sus perturbaciones, otro sería el resultado de la historia de Tsushima. Según lo expresado por Prieto y Espinosa (2017), en Irak en 2003, marcaría un hito importante por la vulnerabilidad de la Protección Electrónica de su fuerza, lo que facilitaría la destrucción de su infraestructura y ubicación de sus tropas, proporcionando a la Coalición las condiciones necesarias para una posterior invasión. La coalición supo explotar bien las vulnerabilidades de las operaciones de Protección Electrónica de Irak, facilitando su ubicación, neutralización y destrucción. Para Adamy (2001), la PE refiere las medidas tomadas para proteger los sistemas de comunicación contra las amenazas planteadas por la guerra electrónica. Según Oyarzun (2022), en la guerra actual, el uso del espectro electromagnético en territorio de Ucrania fue tan deficiente por parte de las fuerzas de Rusia que obligó a los comandantes de más alto rango a concurrir al mismo frente de batalla. Esto trajo consigo que los equipos de Soporte Electrónico ucranianos y de agencias contribuyentes puedan detectar sus ubicaciones en el terreno para ser objetivos por francotiradores ucranianos. La deficiente capacidad de Protección Electrónica de los medios electrónicos rusos permitió a los ucranianos mantener las operaciones defensivas en su territorio.

En el ámbito latinoamericano, Espinoza (2014), la interceptación de las comunicaciones a las fuerzas peruanas por parte de Ecuador en la Guerra del Cenepa permitió conocer las limitaciones de la artillería peruana cuando éstas eran empleadas. La guerra del Cenepa evidenció la carencia de conocimiento y preparación en el empleo de los medios de comunicaciones. El Ejército del Perú, a pesar de contar con radios modernas, no fue eficientemente empleado por su desconocimiento.

En la institución, en el Informe de Operaciones (2013), se evidenciaron acciones de Ataque Electrónico (AE). Se llegaron a neutralizar las comunicaciones durante el uso de los medios de radio HF 6020 y VHF 9000 en los entrenamientos realizados por el Agrupamiento de Comunicaciones José Olaya, encargado de asegurar las comunicaciones en apoyo al comando y control. De continuar con esta situación, se tendría un riesgo crítico a mitigar en

la conducción de las operaciones militares. El propósito del estudio es, ante la carencia de la capacidad operativa en el material de comunicaciones, contar con nuevos procesos que generen conocimiento y permitan incrementar la capacidad de PE en las unidades de comunicaciones, de manera de contribuir con el apoyo al comando y control de las operaciones.

En esta investigación se pudo poner en práctica la teoría actual de Protección Electrónica para crear nuevos procedimientos de empleo que llenen un vacío de conocimiento sobre esta situación problemática que afectaba al campo de las comunicaciones y que sirvió de sustento para nuevos proyectos, estudios y aportes a la doctrina. En el ámbito metodológico, se tomó el enfoque cualitativo para describir un fenómeno como consecuencia del empleo de los equipos remotos de comunicaciones, se identificaron las operaciones de Protección Electrónica, se explicó la designación del personal de operadores de radio y se develó la contribución del apoyo de comunicaciones al comando y control. En lo institucional, en el marco del Plan de Empleo de la Magnitud de la Fuerza, se incrementó la capacidad de Protección Electrónica, cubriendo de esta manera la brecha con el aporte a la doctrina; se describió el empleo inédito del material de comunicaciones que cuenta actualmente la institución. En lo práctico, se ayudó a resolver una incertidumbre real y vigente de suma trascendencia, como la vulnerabilidad que se tiene al emplear los medios radiales en el campo de las comunicaciones a las operaciones de Soporte Electrónico y Ataque Electrónico, lo que limitaba el apoyo de comunicaciones proporcionado por la gran unidad del cuartel “Mariano Melgar” de Arequipa, sobre todo, en los entrenamientos y ejercicios de comunicaciones en apoyo a las operaciones para guerra convencional. En lo social, se benefició a los profesionales del arma de comunicaciones y especialidad de guerra electrónica que trabajan en Agrupamiento de Comunicaciones “José Olaya” de Arequipa y profesionales que se encuentran en unidades tipo batallón y compañías de comunicaciones, mediante la obtención de nuevos conocimientos sobre el empleo de equipos de control remoto integrados con medios de comunicaciones radiales, lo que incrementó las operaciones de Protección Electrónica.

Este estudio abarcó el territorio del departamento de Arequipa, distrito de Tiabaya, entre el personal militar especialista en guerra electrónica y de comunicaciones de la gran unidad. El tema de este estudio fue describir el funcionamiento de la integración de los equipos de control remoto de comunicaciones con equipos de radio en la gama de frecuencia de HF (alta frecuencia) y VHF (muy alta frecuencia), para incrementar las operaciones de Protección Electrónica en la gran unidad de comunicaciones en el 2023.

Esta incertidumbre a estudiar no impuso condicionamientos importantes, debido al acceso a los datos tanto a nivel de documento con los permisos solicitados al comando del Cuartel “Mariano Melgar” del distrito Tiabaya del departamento de Arequipa, así como,

cuando se realizaron las pruebas de empleo y funcionamiento en las instalaciones del mencionado cuartel y posteriormente se realizaron en el campo, también se dispuso con la financiación necesaria, el tiempo que se empleó para recopilar datos de manera presencial y que se reforzaron mediante enlaces en la plataforma informática de manera virtual.

De este contexto se desprende la investigación que se titula: Empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023, cuyo problema general es: ¿Cómo es el empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones José Olaya, 2023? Así mismo se tienen los siguientes problemas: 1. ¿Cuáles son las operaciones de protección electrónica al desarrollarse en el Agrupamiento de Comunicaciones, José Olaya, 2023? 2. ¿Cómo es la designación del personal de operadores de radio en el empleo de los equipos remotos de comunicaciones en el Agrupamiento de Comunicaciones José Olaya, 2023? 3. ¿De qué manera el incremento de las operaciones de protección electrónica contribuyen con el apoyo de comunicaciones al comando y control proporcionado por el Agrupamiento de Comunicaciones “José Olaya”, 2023?

Finalmente, el objetivo general del trabajo fue: Describir el empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones José Olaya, 2023. Con los siguientes objetivos: 1. Identificar las operaciones de protección electrónica que se desarrollan en el Agrupamiento de Comunicaciones José Olaya,2023; 2. Explicar la designación del personal de operadores de radio en el empleo de los equipos remotos de comunicaciones en el Agrupamiento de Comunicaciones José Olaya, 2023; y 3. Develar el incremento de las operaciones de protección electrónica que contribuyen con el apoyo de comunicaciones al comando y control proporcionado por el Agrupamiento de Comunicaciones José Olaya, 2023.

Para el presente capítulo se estableció los motivos claves que encajan en la investigación y los cimientos teóricos referenciales que puntualizan la presente investigación.

Se exponen los manifiestos de los antecedentes nacionales, en el cual, según Echevarría (2021), en su materia “Análisis de la situación actual de la Compañía de Guerra Electrónica de la Tercera Brigada de Comunicaciones”, se utilizó el método cualitativo, el tipo teórico-empírico y para realizar su trabajo de campo se utilizó el método hermenéutico fenomenológico mediante las técnicas de análisis, observaciones y entrevistas, etc. La finalidad de la indagación fue interpretar la situación real en la Compañía de Guerra Electrónica N° 113 y comprender la orientación y capacitación de los profesionales de la unidad en la doctrina, disponibilidad y explotación de los medios de radio, medios alámbricos y tecnología de la información en temas específicos de gestión. El proyecto de investigación se relaciona en cuanto a la carencia de equipo de guerra electrónica que padece la Compañía

de Guerra Electrónica N° 113, la operatividad en cuanto a la obsolescencia tecnológica de material de comunicaciones, así como el entrenamiento en acciones de Protección Electrónica.

Briones (2021), su tesis "Capacidades del sistema de mando y control de la 3a Brigada de Caballería en Defensa Activa, 2019" se realizó mediante un método cualitativo. La investigación pertenece al tipo de teoría empírica. El método utilizado es el método hermenéutico de edificación de la situación actual a través del entendimiento, la reflexión y la investigación continua. La finalidad de este trabajo de investigación es interpretar las posibilidades del comando y control de la 3ra Brigada de Caballería en relación a las operaciones defensivas activas en su área de operaciones asignada. Esta indagación se vincula con la pesquisa, porque aborda la situación de los equipos de radio empleados que utilizan fundamentalmente un sistema de baja frecuencia, lo que restringe el apoyo adecuado de comunicaciones. Además, no se cuenta con equipos para GE lo que hace que las comunicaciones sean suceptibles de ser interceptadas.

González (2017), en su artículo, "Empleo de Personal Especialista en Guerra Electrónica y Producción de Inteligencia de Señales en la IV División de Ejército", el estudio recomienda apoyo metodológico y regulatorio para aclarar el empleo táctico de la Guerra Electrónica para las tareas de inteligencia del Comando Especial del VRAEM. Se utilizó un desarrollo analítico minucioso basado en un bosquejo de hipótesis razonable, integrado con interpretación (hermenéutica) y juicio reflexivo. El objetivo es analizar la contribución de los expertos en guerra electrónica al desarrollo de la inteligencia de señales en un contexto de importancia teórica y práctica. Concluyó que la producción de inteligencia de señales...aumenta con la experiencia de su personal, en este caso el personal experto de GE... Además, los beneficios de formar personas en GE son claros. El proyecto de investigación se relaciona en cuanto a la necesidad de mantener en constante entrenamiento al personal especialista en Guerra Electrónica.

Arévalo (2015), en su tesis “Empleo de Radares de Vigilancia Terrestre (Rvt) en las Operaciones de Seguridad de la 3a Brigada de Caballería del Ejército del Perú-Tacna - 2014”, propone combinar los efectos del uso del radar de vigilancia terrestre con métodos y técnicas operativas durante las maniobras de seguridad dentro del presente sector asignado a la 3a Brigada de Caballería. De desarrollo supuesto deductivo y racional, acompañado de análisis y orientación reflexiva. En cuanto a los objetivos, el desarrollo cuantitativo empleado busca complementar y correlacionar recientes causas y señalizadores que permitan entender la situación verdadera del uso de los radares de vigilancia terrestre en términos de singularidades técnicas y tácticas, decepción electrónica manipulativa, operaciones y desarrollos técnicos,…Intenta aclarar las complejidades, los detalles y el entorno electromagnético. Esta indagación se vincula con la pesquisa, debido a que detalla, en

relación a sus objetivos, el empleo de material remoto para el engaño electrónico manipulativo y su conexión con las maniobras de seguridad, así como de clarificar la dificultad, la particularidad del espacio electromagnético.

Vallejos (2015), en su tesis “Efectos del Sistema de Telefonía Satelital Móvil y Apoyo de Guerra Electrónica en las Operaciones del Comando Especial del VRAEM, 2015”. Objetivo: integrar el grado de relación de los efectos del sistema de telefonía satelital móvil con el apoyo de GE en las operaciones en el CE-VRAEM. Se lleva a cabo un desarrollo supuesto deductivo y racional, integrado con un bosquejo de inducción supuesta con interpretación lógica (hermenéutica) y orientación reflexiva. Se hizo un desarrollo cuantitativo y cualitativo. Como conclusión, se ha podido asociar que un mayor uso de comunicaciones satelitales móviles permite la acción de comando y control oportuna en lugares remotos donde otros medios de comunicación no pueden establecer enlaces. Esta indagación se vincula con la pesquisa, debido a que detalla, en relación a sus objetivos, el contexto veraz de las consecuencias del enlace remoto por el satelital móvil y su conexión con la guerra electrónica para el apoyo al comando y control.

Sobre los antecedentes internacionales, Según lo expuesto por Vadell (2016), en el presente trabajo de investigación; Análisis de las Operaciones de Guerra Electrónica durante la Guerra de las Malvinas en el Teatro de Operaciones Atlántico Sur, se discute el tema de la guerra electrónica a nivel operacional y se analiza la intervención de las fuerzas armadas en el periodo de guerra con el Reino Unido,... durante la guerra entre el 7 de abril a finales del 14 de junio de 1982; todos los objetivos alcanzados se basan en una descripción de las operaciones más importantes de guerra electrónica ejecutadas por las fuerzas armadas argentinas y británicas que, según el autor, afectaron parte del territorio sur argentino. El método de investigación es exploratorio y descriptivo, utilizándose análisis bibliográficos de la Guerra de Malvinas, documentos históricos oficiales contenidos en libros de historia, así como documentos emitidos por diversas comisiones del ejército, fuerza aérea y marina, refiriéndose al despliegue de fuerzas de guerra electrónica durante el periodo de guerra. El presente trabajo se relaciona con la investigación en lo referente a la carencia de procedimientos nuevos para desarrollar operaciones de Protección Electrónica, basándose en los procedimientos pasivos que tuvieron como consecuencia la destrucción de centros de comunicaciones y sistemas de armas.

Iglesias (2015), la tesis sobre "Diseño de algoritmos de radar y guerra electrónica implementados en sistemas en tiempo real", se concentró en la indagación y la evolución de algoritmos de radar y guerra electrónica implementados en procedimientos a tiempo efectivo. La introducción de las plataformas de radio y radar en el ejército ha llevado al desarrollo de tecnología para contrarrestarlos. Los sistemas de guerra electrónica tienen como meta vigilar y asegurar el espacio electromagnético. La inteligencia electrónica es una modalidad de la

guerra electrónica, cuyas tareas son: detectar, almacenar, interpretar, clasificar y encontrar las fuentes de todas las emisiones de ondas del espectro. Esta pesquisa se relaciona con la indagación, debido a que detalla y expone temas como el control del espectro electromagnético, acciones de protección electrónica presentes en el campo de las no comunicaciones, que tienen mucha similitud en el campo de comunicaciones para las señales de radio.

Saumeth & Guaidó (2017), en su artículo, Guerra Electrónica en Suramérica, en Perú, la Marina de Guerra cuenta con una dependencia encargada en Soporte Electrónico y Ataque Electrónico italiana denominada Newton-Lambda. Junto al sistema de señuelos SCLAR, este permite detectar las emisiones de radar y comunicaciones del enemigo, localizar su origen de ser necesario, interferirlas mediante ruido de saturación o engaño, haciendo parecer, a vistas del radar atacante, una posición del buque distinta a la real. Por su parte, la Fuerza Aérea, los aviones Mig-29 y Sukhoi SU-5, cuentan con lanzadores de señuelos como protección electrónica (engaño electrónico). El presente artículo se relaciona con la investigación en cuanto a contar con capacidades de protección electrónica por medio de la saturación de radar o engaño electrónico para confundir a las capacidades de Soporte Electrónico enemigas. Así mismo, no menciona al Ejército del Perú en cuanto a capacidades de guerra electrónica.

Se tienen las bases teóricas que sustentan la investigación, en la cual se menciona como teoría general la teoría de los riesgos. Según Beck (2006), su objetivo es investigar cómo los riesgos afectan la sociedad actual. Esta teoría se centra en el análisis y las transformaciones sociales y cómo abordamos los riesgos en la sociedad moderna. Beck sostiene que los peligros en la sociedad actual no se limitan a los peligros naturales, sino que también incluyen los peligros generados por la actividad humana, como la tecnología. En este sentido, Beck argumenta que vivimos en una sociedad en la que los riesgos se han extendido a nivel mundial, se han vuelto inciertos e incontrolables y tienen un impacto general en nosotros.

La falta de certeza y la necesidad de evaluar los posibles riesgos y beneficios hacen que la toma de decisiones en sociedades en riesgo sea más complicada. Beck enfatiza que las desigualdades y los conflictos son el resultado de que diferentes grupos sociales se vean afectados de manera desigual por los riesgos. Además, señala que los sistemas de expertos e instituciones convencionales no son adecuados para gestionar estos riesgos y sugiere una democracia reflexiva que involucre a los ciudadanos en la toma de decisiones y evaluación de riesgos.

La teoría del riesgo de Ulrich Beck tiene muchas razones para ser importante. Primero, proporciona un método para evaluar los riesgos sociales actuales de la persona. Además, enfatiza que los riesgos son mundiales y que para enfrentarlos se requiere una

cooperación a nivel mundial. La teoría también incluye la individualización de los riesgos, que enfatiza que cada persona tiene la responsabilidad de tomar decisiones sobre cómo manejar los riesgos. Beck fomenta la toma de decisiones políticas efectivas para proteger a las personas en general y enfatiza el papel que juega la política en la gestión de los riesgos.

El uso de medios de comunicación remotos para mejorar las operaciones de protección electrónica se puede relacionar con los conceptos teóricos de Beck (2006) sobre cómo relacionar los peligros como resultado de la tecnología, cómo los peligros nos afectan, generando incertidumbre y cómo gestionar los peligros para proteger a las personas.

El Agrupamiento de Comunicaciones José Olaya, en las últimas décadas, por el avance de la tecnología y carencia de material y equipo, tiene el riesgo de que su tarea principal sea neutralizada (proporcionar el apoyo de comunicaciones al comando y control), lo que tendría graves consecuencias para la protección y seguridad física del personal y la conducción de las operaciones en guerra convencional (GC), por lo que la gestión del riesgo implica el empleo de los medios de comunicaciones remotos para incrementar las operaciones de protección electrónica. Esto hace que el apoyo de comunicaciones permita un comando y control (C2) adecuado, lo que limita el riesgo de ser neutralizada por acciones de ataque electrónico y, así mismo, disminuya los riesgos a ser localizados y destruidos físicamente por los sistemas de armas enemigos. Un C2 adecuado como resultado de un apoyo de comunicaciones eficiente será capaz de liderar las operaciones militares, lo que implica demostrar la naturaleza en la toma de decisiones, ya que se pueden tomar con seguridad, asumiendo riesgo o niveles de incertidumbre que pueden tener un impacto en las operaciones actuales y el planeamiento.

Teoría de alcance medio

Adamy (2001) afirma que la teoría de la GE incluye conceptos fundamentales sobre el espectro electromagnético, lo que ayuda a comprender cómo se propagan y manipulan las señales en el espectro electromagnético, lo cual es crucial para la guerra electrónica. Estos conceptos de electromagnética expresados por Adamy nos permiten comprender cómo funcionan los sistemas de comunicaciones y desarrollar contramedidas efectivas en el campo de la guerra electrónica que generen protección electrónica.

Adamy (2001) analiza la protección electrónica (PE) como una parte importante de la guerra electrónica. La PE se refiere a las medidas tomadas para proteger los sistemas de comunicación y el radar contra las amenazas planteadas por GE. Adamy enumera algunos de los temas relacionados con el ejercicio:

Análisis de vulnerabilidades: Adamy proporciona un marco para evaluar los riesgos que producen la vulnerabilidad de los sistemas propios a las amenazas de guerra electrónica. Esto implica comprender cómo el enemigo puede detectar, localizar y atacar los sistemas

propios utilizando técnicas de comunicaciones u otras formas de emisiones electromagnéticas.

Diseño de sistemas resilientes: el autor examina técnicas para hacer que los sistemas de radar y comunicaciones sean menos vulnerables a las interferencias y ataques electrónicos. La implementación de redundancias, el uso de técnicas de modulación avanzadas y la inclusión de características de seguridad en el diseño de hardware y software son algunos ejemplos de esto.

Contramedidas defensivas: Adamy habla sobre una serie de contramedidas defensivas que los sistemas pueden usar para protegerse contra las amenazas de guerra electrónica. Esto puede incluir el uso de sistemas de alerta temprana para detectar amenazas entrantes, métodos de supresión de comunicaciones para reducir la probabilidad de detección y métodos de enmascaramiento y dispersión para dificultar la localización de los propios sistemas. Gestión del espectro electromagnético. El autor destaca la importancia de una gestión eficiente del espectro electromagnético para evitar interferencias entre los propios sistemas y maximizar la eficacia del radar y las comunicaciones. Esto puede incluir asignación cuidadosa de frecuencias y planificación de operaciones en entornos de alta densidad espectral.

Además, Adamy (2001) incluye las características de los equipos de radio en su teoría de comprensión general de los sistemas de comunicación. Aunque su teoría se concentra principalmente en los principios fundamentales de la GE, también proporciona información sobre los componentes y características de los sistemas de radio utilizados en el campo de batalla. Esto es esencial para comprender cómo funcionan estos sistemas y cómo pueden afectar o manipular la GE; en este sentido se menciona como característica de los equipos la frecuencia de operación de un equipo de radio, el cual es esencial para su alcance y capacidad para comunicarse o detectar a otros equipos en el campo de batalla. Adamy habla sobre el tipo de frecuencia que debe elegir de acuerdo con el tipo de misión que tiene.

La potencia de transmisión de un equipo de radio afecta su alcance y la capacidad de superar el ruido y las interferencias en el canal de comunicación. Adamy podría explicar cómo cambia la potencia de transmisión según la distancia entre los radios y las condiciones del terreno. El ancho de banda de un equipo de radio mide la cantidad de información que puede transmitir o recibir en un período de tiempo determinado. Adamy explica cómo se calcula el ancho de banda utilizando la velocidad de transmisión requerida y la disponibilidad del espectro electromagnético. Por último, la modulación y la demodulación. Adamy explica los diferentes tipos de modulación que utilizan los equipos de radio, como los equipos de alta frecuencia (HF), modulación de fase y muy alta frecuencia (VHF) y cómo se demodulan para extraer información transmitida.

En consecuencia, los planteamientos teóricos expuestos por Adamy (2001), tienen clara relevancia y aplicación en el tema del empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones José Olaya, en lo siguiente:

Los conceptos de electromanética mencionados por Adamy son fundamentales y están relacionados con comprender cómo funcionan los medios de comunicaciones para mejorar las capacidades de protección electrónica, que es una acción de la guerra electrónica necesaria en nuestra época actual. Con el aumento del análisis de las vulnerabilidades a las acciones de SE y AE, la protección electrónica se enriquece con informes de dichas vulnerabiliades remitidos por las unidades de comunicaciones. El uso de medios de comunicaciones remotos para mejorar las operaciones de PE es parte del diseño de sistemas resilientes. Como resultado, el soporte de comunicaciones se vuelve menos vulnerable a los ataques electrónicos, ya sea a través de métodos que dificultan la localización de los propios sistemas. Esto requiere una gestión adecuada del espectro electromagnético.

Como parte de la comprensión general de la teoría mencionada por Adamy, las características de los equipos de radio que menciona se relacionan con los medios de comunicaciones remotos que se emplearán para incrementar las operaciones de Protección Electrónica. Estos medios de comunicaciones remotos cuentan con características técnicas que forman parte de las medidas de protección propias de los equipos, sumando a ello los procedimientos operacionales que realiza el operador de radio y que serán parte del propósito del estudio.

Categoría y subcategorías aprioristas

Las categorías sirven como marco teórico para la investigación cualitativa y proporcionan un fundamento científico para el proceso de investigación. Las dos categorías son apriorísticas y emergentes; durante la etapa inicial de la pesquisa, se definen las categorías apriorísticas, que se derivan del objetivo y problema del estudio y acceden al desarrollo de recolección de datos.

Tabla 1

Categorías aprioristas del estudio

Categorías	Sub Categorías
Equipos Remotos de Comunicaciones	Capacidad Operativa de Comunicaciones
	Integración Radio-alámbrica
	Designación de Operadores de Radio
Operaciones de Protección Electrónica	Sincronización de las Emisiones de Ondas
	Tipos de Operaciones de Protección Electrónca
	Contribución con el Apoyo de Comunicaciones

Bases teóricas de la categoría Equipos remotos de comunicaciones

Son medios de transmisión de información disponibles en la gran unidad de comunicaciones que utilizan ondas de radio para coordinar y controlar las operaciones militares. Estos medios abarcan una variedad de tecnologías y frecuencias que permiten la comunicación desde cortas hasta largas distancias. Asimismo, según el número empleado de medios de comunicaciones de manera simultánea, se genera una gran cantidad de energía electromagnética en las bandas de alta frecuencia (HF) y muy alta frecuencia (VHF). Estos equipos de radio pueden ser empleados de manera remota mediante la técnica de Integración Radio-alámbrica (IRA) con la Unidad de Control Remoto GRA-39 a una distancia de 3,5 km de la estación de control en la cual se encuentra el operador de radio designado, con la finalidad de permitir a los centros de comunicaciones mantener su seguridad física y electrónica, gestionando de esta manera los riesgos que genera la guerra electrónica actual sobre nuestras capacidades. Esta categoría está fundamentada en teorías científicas como la teoría del riesgo social de Beck (2001) y la teoría de la guerra electrónica de Adamy (2006). Se tienen las siguientes subcategorías: Capacidad operativa de comunicaciones, Integración radio-alámbrica y Designación de operadores de radio.

Capacidad operativa de comunicaciones

Es la disponibilidad de medios de comunicaciones que existen en la actualidad para entrar en operaciones; la gran unidad de comunicaciones no cuenta con equipos de guerra electrónica en la actividad de SE y AE. Se cuenta con material para el realizar acciones de Protección Electrónica en apoyo al comando y control de manera limitada, lo que los hace vulnerables a las acciones de Soporte y Ataque Electrónico enemigos.

Los factores para determinar la capacidad operativa de los medios de comunicaciones de una gran unidad son: La cantidad de material asignada en relación con el Cuadro de Organización y Equipo (Coeq); la operatividad del material; la obsolescencia tecnológica y el tiempo de uso en relación con el año de afectación.

Tabla 2

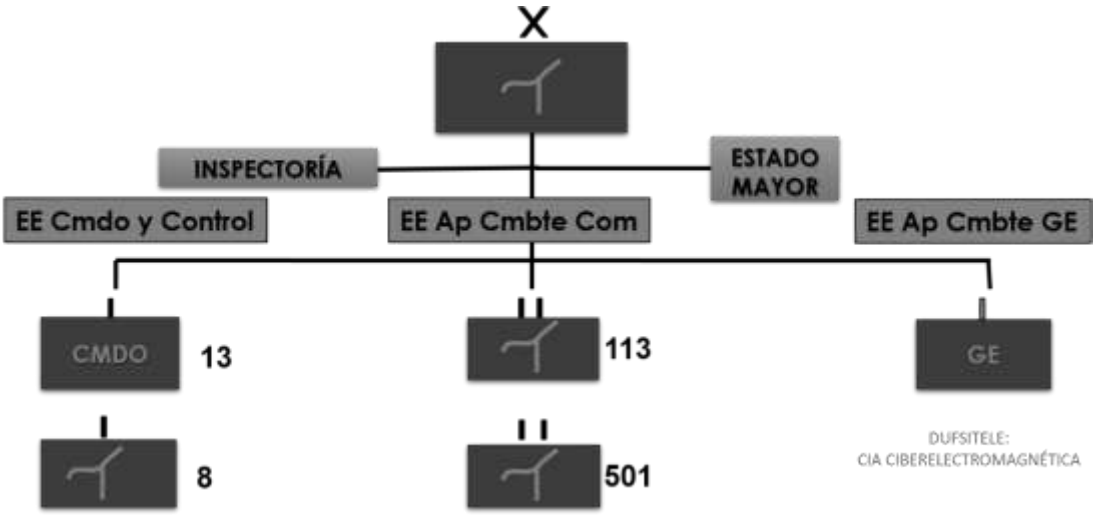
Capacidad operativa de comunicaciones

SUB FACTOR COMUNICACIONES	PUNTAJE	COEF	PUNTOS	% COM
MAT DE RADIO	33.78	03	**101.34**	**10.13%**
MAT TELEFÓNICO	16.99	04	67.97	
MAT DE SEG	0.00	02	0.00	
OTROS	60.98	01	67.98	
SUMA DE PUNTOS		10	237.29	**23.73 %**

Nota. La tabla nos muestra la situación de los equipos disponibles según la Capacidad Operativa de Comunicaciones en un 23.73%, y el material de radio en una capacidad operativa de 10.13%, siendo el 80% mínimo para entrar en operaciones. Fuente: ICO (2023).

Figura 1

Organización del Agrupamiento de Comunicaciones José Olaya.



Nota: La figura muestra a unidades de comunicaciones y guerra electrónica, las cuales no cuentan con capacidad de PE suficiente para entrar en operaciones. Fuente: Informe de Capacidad Operativa (2023).

Los equipos de comunicaciones disponibles según la capacidad operativa cuentan con características técnicas que son las particularidades técnicas de las bondades tecnológicas de los medios de comunicaciones; estas características aseguran que los sistemas de comunicaciones sean eficaces; pueden estar incluidas en la unidad de control remoto y los medios de comunicaciones por radio que se integran y emplean para incrementar las operaciones de protección electrónica. Las características más relevantes son la gama de frecuencia, el modo de emisión de la señal de radio (claro, seguro y salto de frecuencia). Potencia de salida, número de frecuencias, número de canales preestablecidos y silenciamiento; los medios disponibles son los siguientes:

Unidad de Control Remoto GRA-39

Según el Manual Técnico (1991), el AN/GRA 39, es un equipo remoto que se emplea para la integración radio-alámbrica entre la unidad de control remoto propiamente dicho, cable de campaña WD-1/TT y un transmisor-receptor de radio,… Está conformado por una unidad de control local en que se encuentra el centro de mando y una unidad de control remoto que se encuentra adjunto al equipo de radio,…cuando se conecta con una radio, el equipo remoto permite al operador transmitir y recibir comunicaciones de frecuencia de voz a través del transmisor-receptor a una distancia de hasta dos millas (3,5 kilómetros).

La Unidad de Control Remoto GRA-39 está conformada por la unidad de control local y unidad de control remoto y su alimentación es a través de baterías.

Figura 2

Equipo de control remoto AN/GRA39

Nota. Se muestra el panel frontal del Equipo de Control Remoto AN/GRA 39, en el cual se muestra al cable de interconexión que se integra a los equipos de radio. Fuente: Manual Técnico de Mantenimiento de los Equipos de Radio (1991).

Medios de comunicaciones radiales

Según lo descrito por Comunicaciones en Campaña (2007), los medios de comunicaciones cuentan con características técnicas que les permiten tener una sigularidad tecnológica para su funcionamiento y empleo en operaciones militares; dentro de estas características se encuentran los parámetros de protección que permiten realizar contramedidas electrónicas (CCME) o Protección Electrónica contra acciones de Soporte Electrónico y Ataque Electrónico enemigo.

Los medios radiales disponibles en la gran unidad de comunicaciones para incrementar las operaciones de protección electrónica, según su nomenclatura, son los siguientes:

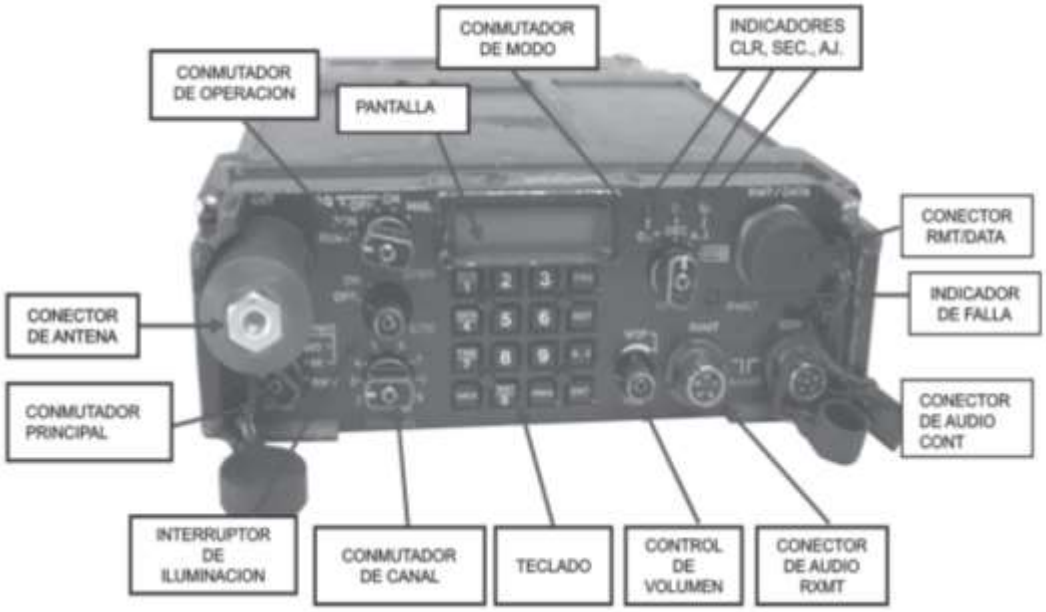
- Radio Portable de Comunicación 730 (PRC 730)
- Radio Portable de Comunicación 2200 (PRC 2200)
- Radio Portable de Comunicación 6020 (PRC 6020)
- Radio Portable de Comunicación 930 (PRC 930)
- Radio Portable de Comunicación 8020 (PRC 8020)

Radio Portable de Comunicación 730 (PRC 730)

Este equipo portátil se emplea por medio del receptor transmisor básico RT 7330; la radio de actual creación digital funciona en frecuencia modulada en un solo canal en la gama de frecuencia de VHF (Muy Alta Frecuencia) de una gama de frecuencia de 30 a 87,975 Mhz: el equipo puede tolerar el empleo de 2319 canales de radio o probables frecuencias programables de forma manual a través del panel frontal por medio del teclado a espacios de 25 Khz. La cadencia que utiliza esta radio es la FM de banda delgada; puede hacer empleo de 10 códigos de protección para el uso del Salto de Frecuencia. Tiene capacidad para un modo de transmisión por fonema y datos digitales en los modos de operación Claro, Seguro y A.J. (Salto de frecuencia), este último para operación ECCM, cuenta con una potencia de salida baja de 0.25 vatios y potencia de salida media de 4 vatios.

Figura 3

Radio Portable de Comunicación 730



Nota. La figura detalla el panel frontal de la radio PRC 730, se puede identificar al Conector de Audio Control, en él se conecta el cable de interconexión de la Unidad de Control Remoto GRA 39. Fuente: Comunicaciones en campaña (2007).

Radio Portable de Comunicación 2200 (PRC 2200)

Utiliza un transceptor RT 2001 básico, que incluye una portadora de HF fabricada en la planta de Tadiran en Israel, y un receptor/transmisor de radio portátil de banda lateral única (SSB) de HF (alta frecuencia). El PRC 2200 proporciona 285.000 canales de radio o probables frecuencias operativas en intervalos de 100 Hz y un rango de frecuencia de 1,5000 a 29,9999 MHz, incluidos parámetros de seguridad como el secreto y emisiones de A. J. (Salto de frecuencia).

Cuenta con funciones de Banda Lateral Única superior e inferior. Cuenta hasta 10 claves de cifrado independientes cubiertas. Potencia de salida de 5, 10 y 20 Watts Puede trabajar en selección de frecuencia automática y es interoperable con otros equipos en la banda HF.

Uno de los primeros equipos transmisores-receptores con tecnología digital utilizados en el conflicto del "Alto Cenepa" es esta radio. Los parámetros de seguridad de estos equipos de radio, junto con los procedimientos operacionales tácticos del operador de radio, permiten realizar acciones de Protección Electrónica excelentes, las cuales disminuyen las capacidades de soporte electrónico y ataque electrónico, brindando la seguridad física y electrónica a los órganos y medios de comunicaciones.

Figura 4

Radio Portable de Comunicación 2020.

Nota. La figura muestra el panel frontal del equipo de radio PRC 2020. Se pueden identificar los conectores de audio, en cualquiera de ellos puede ser conectado el cable de interconexión de la Unidad de Control Remoto GRA 39. Fuente: Comunicaciones en campaña (2007).

Radio Portable de Comunicación 6020 (PRC 6020)

Cuenta con cobertura de frecuencia de 1,5 a 30 Mhz, 285.000 canales con espaciado de 100 Hz, opciones: 2.850.000 canales con espaciado de 10 Hz, 100 canales preestablecidos, modos de funcionamiento, gestión de frecuencia - seguridad clara, compra de frecuencia, operación de salto de frecuencia, salto final adaptativo, transmisión de control de operación, eliminación de parámetros de emergencia, conexión automática:

Llamada automática de hasta 180 tablas, códigos de voz, transmisión de mensajes en serie (memoria flash) de hasta 1000 mensajes diferentes, omisión de frecuencia incorporada y tiene 10 claves de cifrado. Este equipo de radio, por contar con parámetros de seguridad sumado a los procedimientos operacionales tácticos realizados por el operador de radio, permite realizar acciones de Protección Electrónica óptimas que reducen las capacidades de soporte electrónico y ataque electrónico, proporcionando la seguridad física y electrónica a los órganos y medios de comunicaciones.

Figura 5

Radio Portable de Comunicación 6020

Nota. La figura muestra el panel frontal del equipo de radio PRC 6020, se pueden identificar los conectores de audio, en cualquiera de ellos puede ser conectado el cable de interconexión de la Unidad de Control Remoto GRA 39. Fuente: Comunicaciones en Campaña (2007).

Radio Portable de Comunicación 930 (PRC 930)

Emplea la gama de frecuencia de 30 a 88 Mhz (optativo 108 Mhz), intervalo de canal de 25 Khz, 2320 canales (optativo 3120), 100 canales prefijados, capacidad de radiación acoplable: Tipo portátil a la espalda: 0,25 W y 5 W, con Protección Electrónica (saltos de frecuencia) con dispositivo digital, con rebote sincrónico y ortogonal, contador de seguimiento de interferencias, escáner de canales agregado, silenciamiento selectivo de una estación de radio, receptor GPS para informes de navegación y ubicación, borrado de emergencia para parámetros sensibles; incluso si el transmisor está cerrado, existen mecanismos para evitar manipulaciones no autorizadas y cuenta con diez claves de cifrado.

Para realizar acciones de protección electrónica excelentes, que disminuyen las capacidades de soporte y ataque electrónico, el operador de radio utiliza parámetros de seguridad junto a los procedimientos operacionales tácticos; esto contribuye con mantener los enlaces de los centros de comunicaciones. Siempre y cuando estos equipos de radio se encuentran conformando parte de un sistema de comunicaciones, el empleo por sí solo tiene muchas limitaciones.

Cuenta con un mecanismo que evita el manejo no permitido a agentes externos.

Figura 6

Radio Portable de Comunicación 930

Nota. La figura muestra el panel frontal del equipo de radio PRC 930. Se pueden identificar los conectores de audio, en cualquiera de ellos puede ser conectado el cable de interconexión de la Unidad de Control Remoto GRA 39. Fuente: Comunicaciones en campaña (2007).

Radio Portable de Comunicación 8020 (PRC 8020).

Ramos (2018), en su tesis, describe que el equipo PRC-8020 es parte de la serie HF-8000. Esta versátil unidad de radio utiliza tecnologías modernas para proveer un resultado completo a las condiciones de enlace de las concurridas bandas de alta frecuencia, manteniendo al mismo tiempo una excelente simplicidad operativa incluso en las condiciones de guerra electrónica de los campos de batalla actuales. Estos equipos funcionan de 1,5 a 29,99999 MHz. Con parámetros de seguridad junto a los procedimientos operacionales tácticos del operador de radio, este equipo de radio puede realizar acciones de protección electrónica excelentes que disminuyen las capacidades de soporte y ataque electrónico, brindando así la seguridad física y electrónica a los órganos y medios de comunicaciones.

Figura 7

Radio Portable de Comunicación 8020.

Nota. La figura muestra el panel frontal del equipo de radio PRC 8020. S pueden identificar el conector de audio, en él se puede enlazar el cable de interconexión de la Unidad de Control Remoto GRA 39. Fuente: Servicio de Comunicaciones del Ejército (2023).

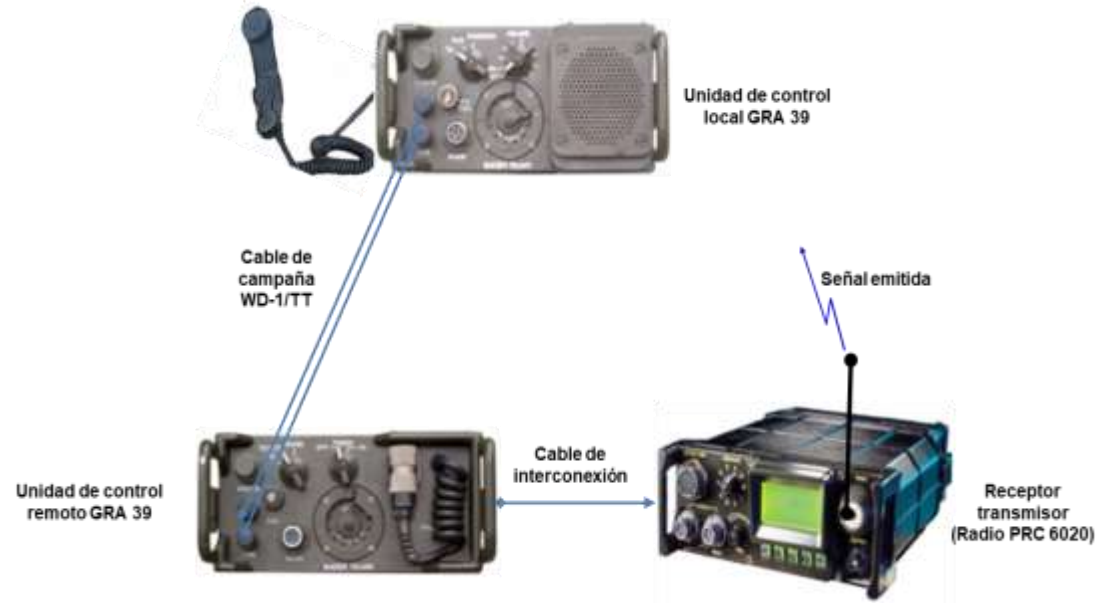
Integración Radio-Alámbrica

Esta subcategoría de los Equipos remotos de comunicaciones se define como la técnica de instalación y empleo de los medios de comunicaciones de manera remota desde el centro de comunicaciones o centro de mando a una distancia aproximada de 3.5 km. El empleo ayuda a incrementar las operaciones de Protección Electrónica, proporcionando la seguridad física al personal de operadores de radio, así como la seguridad física y electrónica al centro de comunicaciones de la gran unidad de combate contra acciones de Soporte Electrónico como radiolocalización y contra acciones de Ataque Electrónico como la perturbación.

Para la transmisión en esta técnica de empleo, requiere de equipo de Control Remoto AN/GRA 39, los cuales transmiten las señales a través de cables de campaña que se conecta a las unidades de control remoto local. Posteriormente, las señales de audio pasan por el cable de interconexión al receptor transmisor (radio), siendo emitidas al espacio electromagnético, el mismo procedimiento se realiza en cuanto se refiere a la recepción de las señales, las cuales se devuelven al control local, pasan por cable de campaña y llegan al control remoto, el cual es escuchado por el operador de radio.

Figura 8

Integración radio alámbrica



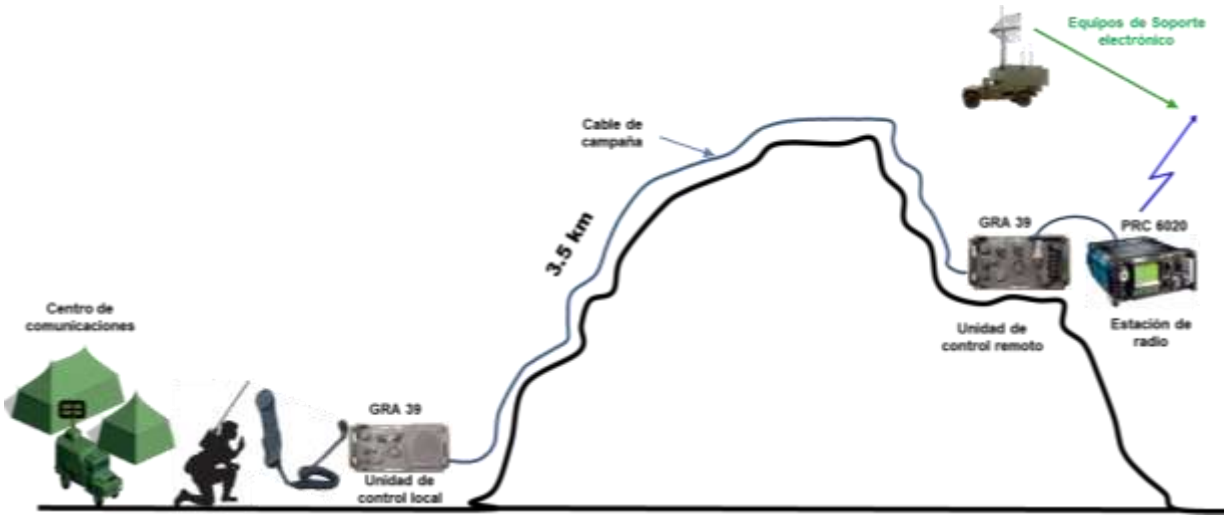
Nota. La figura permite los medios remotos de comunicaciones a través de la integración radio alámbrica del Equipo de Control Remoto GRA-39 (conformado por la Unidad de Control Local GRA 39 y Unidad de Control Remoto GRA 39), con un receptor transmisor (Radio PRC 6020).

Posicionar adecuadamente las estaciones de radio de forma remota es esencial para la seguridad. Para Guerrillacomm (2011), este equipo es un control remoto por radio, cuenta con una unidad de control local que va dentro del puesto de mando o centro de comunicaciones y en algún lugar a 3.5 km de distancia va la estación de radio conectada con la unidad de control remoto. La unidad de control remoto podrá ubicarlo en la cima de un edificio, colina o lo que sea para conseguir una altura adecuada para la antena con el fin de tener una mejor eficiencia de enlace. En operaciones, no puedes posicionar tus equipos remotos en la cima de una montaña, debido a que podrían ser vulnerables a las operaciones de guerra electrónica enemiga, como su ubicación y destrucción. Lo recomendable es

colocarlo en la parte posterior a tus fuerzas para que tengas protección. Si el enemigo descubre que estás transmitiendo desde la cima, encontrará tu señal y simplemente bombardeará esta área lejos del centro de mando. Esta ubicación es importante para que puedas mantener el centro de mando libre de acciones de Soporte Electrónico y Ataque Electrónico.

Figura 9

Despliegue y ubicación táctica de los equipos remotos de comunicaciones



Nota. La figura permite ver la ubicación posterior de los equipos remotos de comunicaciones a una distancia de 3.5 km de manera de proteger el centro de comunicaciones de la ubicación de las capacidades de Soporte Electrónico enemigo.

Designación de operadores de radio

Son los operadores de radio empleables para una adecuada distribución y gestión de la fuerza disponible, de manera que no sean mal utilizadas al ser recursos limitados y difíciles de reponer en el corto plazo, debido a su alta capacitación y entrenamiento técnico especializado en operaciones de guerra electrónica. En un enfoque sobre la gestión de recursos humanos, Chiavenato (2011), determina que, para gestionar el talento del personal, es necesario individualizar sus habilidades y potencialidades para que dichas competencias se adapten a los puestos específicos. Estos operadores de radio se designarán para operar los equipos remotos de comunicaciones durante los entrenamientos en los ejercicios de comunicaciones para guerra convencional, manteniendo así la economía de fuerzas, que se entiende como la distribución y gestión adecuadas de las fuerzas disponibles, es un principio de la guerra, según Izcue y Arriarán (2013), para evitar el mal uso de las fuerzas al tener recursos limitados y difíciles de reponer. Tolmos (2015), afirma que el líder está muy

comprometido con la evaluación y disposición adecuada de su economía de fuerzas y cree que reducir los medios de las fuerzas circunstanciales al mínimo necesario le permitirá completar la tarea encomendada.

Con base en el estudio de Ventura & Jaramillo (2014), en cuanto a los efectivos de técnicos y suboficiales, se tiene un 32.21 % (153 efectivos asignados de un total de 475 técnicos y suboficiales según el Cuadro de Organización y Equipo), de los cuales sólo el 4% (19 efectivos) son operadores de radio.

Según el Informe de Capacidad Operativa (2023), el Agrupamiento de Comunicaciones José Olaya cuenta con una cantidad de efectivos asignados de técnicos y suboficiales de 64 (13.4%) de un total de 475 efectivos, de los cuales 12 (2.5%) son operadores de radio.

Tabla 3

Cuadro de comparativo de efectivos de Tecnicos y Suboficiales al 2023

Unidades del Agrup Com José Olaya	**Personal de Técnicos y Suboficiales**		
	Cuadro de Organización y Equipo	Efectivo asignado	Operadores de radio
Cuartel General	31	27	3
Batallón de Comunicaciones Nº 113	110	10	2
Batallón de Comunicaciones N° 501	110	8	3
Compañia de Guerra Electrónica N° 113	162	6	2
Compañia de Comunicaciones Nº 8	37	7	2
Compañia de Comando Nº 13	25	6	0
TOTAL	**475 (100%)**	**64 (13.4%)**	**12 (2.5%)**

Nota. La tabla nos muestra la situación del personal de operadores de radio asignado por unidades del Agrupamiento de Comunicaciones José Olaya, con una cantidad de 12 operadores de radio. Fuente : Informe de Capacidad Operativa (2023).

Bases teóricas de la categoría Operaciones de Protección Electrónica

Esta categoría se define como el conjunto de tipos de operaciones y procedimientos operacionales (sincronización de ondas electromagnéticas) que son aplicados para contrarrestar acciones de Soporte Electrónico como la rediolocalización y acciones de Ataque Electrónico como la perturbación de manera limitar las operaciones de guerra electrónica enemigas. Según la Electronic Warfare Techniques (2023), es una operación militar que consiste en el uso de poderío electromagnético para dominar el propio espacio electromagnético y protegerlo de los ataques del adversario. También la PE es la actividad

de la guerra electrónica, que incluye tareas empleadas para dar seguridad al personal militar, establecimientos y medios de alto valor militar y vehículos militares de cualquier influencia de fuerzas amigas, neutrales u hostiles en el espectro electromagnético, que podrían perjudicar, neutralizar o destruir las capacidades operativas amigas. Esto permite al Agrup Com José Olaya proporcionar el apoyo de comunicaciones para el comando y control de las operaciones en guerra convencional. Esta categoría está fundamentada en teorías científicas como la teoría del riesgo social de Beck (2001) y la teoría de la guerra electrónica de Adamy (2006).

El Manual de Guerra Electrónica (2013) menciona que la Protección Electrónica es una de las actividades de la guerra electrónica, cuyo propósito es proteger nuestras emisiones electrónicas, asegurando el uso efectivo (activo y pasivo) del espectro electromagnético ante las acciones de GE emprendidas por el enemigo, por las propias fuerzas e interferencias no intencionadas. La Protección Electrónica tiene como objetivo impedir, negar y reducir los esfuerzos enemigos siguientes:

- La adquisición de datos sobre nuestras emisiones electrónicas a través de la Inteligencia de Señales y SE de la GE.
- Producir información o conocimiento de nuestras señales para la toma de decisiones.
- Ejecutar acciones de ataque electrónico de la GE con efectividad.

Sicronización de ondas electromagnéticas

El establecimiento de la coordinación entre la Estación de Protección y el Centro de comunicaciones para emitir ondas de radio de estilo simultáneo en un momento determinado con el fin de generar una gran cantidad de energía electromagnética constituye esta subcategoría de las Operaciones de Protección Electrónica. La sincronización, según Planeamiento de las Operaciones Terrestres (2015), es el uso de las funciones militares en maniobras militares en un momento, área y finalidad específicos para generar la más alta potencia combativa en el tiempo y área de operaciones decisivas.

Tipos de Operaciones de Protección Electrónica

Esta subcategoría se define como las diversas operaciones empleadas para contrarrestar las acciones de guerra electrónica enemigas. Según el Manual de Guerra Electrónica (2013), los tipos o acciones de Protección Electrónica son: Anti-Soporte Electrónico, que tiene por finalidad negar la búsqueda, monitoreo, localización e identificación de las plataformas de comunicaciones que emplean la energía electromagnética a través de sus equipos de Soporte Electrónico, y el Anti-Ataque Electrónico, que tiene por finalidad reducir los efectos del ataque electrónico enemigo, o los efectos colaterales del empleo del ataque electrónico por parte de nuestras fuerzas sobre sus sistemas de comando y control.

Tanto las operaciones Anti-Soporte Electrónico y Anti-Ataque Electrónico están supeditadas al empleo táctico adecuado de los procedimientos operacionales y empleo de sus recursos técnicos.

Procedimientos operacionales de Protección Electrónica.

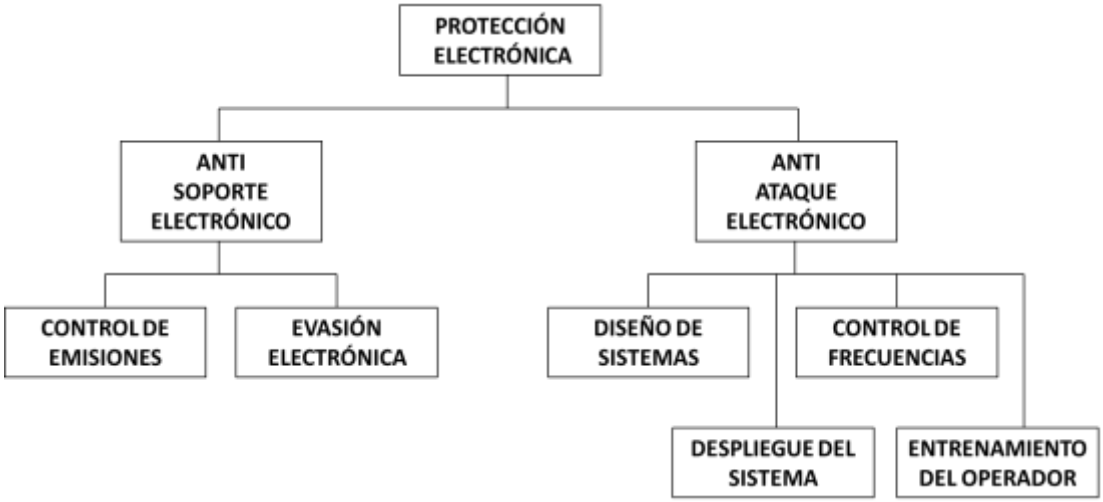
Se adoptan desde el período de paz, es decir, tienen un carácter permanente a fin de que los operadores obtengan la destreza adecuada y se constituyan en factores de resistencia ante el esfuerzo de la GE enemiga. Los procedimientos operacionales pueden ser: Anti-SE, se tiene al entrenamiento al operador; previsión de procedimientos de operación, previsión de sistemas redundantes y uniformes, alteración en el padrón o rutina de las emisiones, utilización de códigos, control de la potencia, despliegue de los medios y uso de antena direccional. El Anti-AE, es un procedimiento que consiste en seguir operando bajo la acción de la perturbación como el cambio de puesto retransmisor, cambiar el modo de operación, uso de rutas alternas, cambiar la polarización de la antena o usar antena direccional, cambiar frecuencia y cambiar terminal.

Recursos técnicos o parámetros de seguridad.

El avance de la electrónica permite que las plataformas de comunicaciones dispongan permanentemente de mayores capacidades de protección. Algunas tecnologías de Protección Electrónica para los sistemas de comunicaciones son: Espectro extendido, transmisión por salvas, mezclador de voz, secreto, criptografía, salto de frecuencia y control automático de potencia (Potencia adaptativa).

Figura 10

Tipos de operaciones de Protección Electrónica (acciones de PE)



Nota. La figura muestra los dos tipos considerados como acciones de Protección Electrónica, Anti-SE y Anti-AE, con sus respectivas modalidades para hacer frente a las operaciones de guerra electrónica. Fuente: Doctrina General de Guerra Electrónica (2005).

Enmascaramiento electrónico.

Por lo descrito en el Electronic Warfare Techniques (2023), en sus definiciones, considera que es la emisión moderada de energía electromagnética en la gama de frecuencias empleadas por las estaciones de radio de nuestras fuerzas, con la finalidad de cuidar nuestras señales de radio y plataformas de comunicaciones contra el empleo de operaciones de Soporte y Ataque Electrónico enemigo, midiendo su búsqueda de la información, sin disminuir notablemente el funcionamiento de nuestras estaciones.

Contribución con el apoyo de comunicaciones

Concepto de apoyo de comunicaciones de la Gran Unidad.

Según el Informe de Capacidad Operativa (2023), la gran unidad de comunicaciones proporciona apoyo de combate de comunicaciones y guerra electrónica limitado, al despliegue y preservación de la fuerza, a las operaciones ofensivas y defensivas,… para facilitar el comando y control de las operaciones,… con la finalidad de permitir que al Componente Terrestre cumpla su misión.

El "apoyo de comunicaciones" en un contexto militar se refiere a todos los recursos, infraestructuras, y actividades necesarias para garantizar que las unidades militares puedan comunicarse de manera efectiva durante operaciones. Esto es crucial para la coordinación, comando y control de las operaciones militares. Como expresa Colom (2017), el término "comando y control" se refiere a lo que debe lograrse mediante la implementación e integración de sistemas de comunicaciones que permitan el enlace desde el nivel estratégico al táctico, lo que permite una ventaja en la obtención de información y en el proceso de toma de decisiones, esto representa una ganancia significativa para la fuerza que pueda maximizar esta capacidad.

Importancia del apoyo de comunicaciones

El apoyo de comunicaciones es vital para el éxito de las operaciones militares, ya que permite la toma de decisiones informada, permite proporcionar información en tiempo real a los comandantes; coordinación eficiente, permite asegurar que todas las unidades trabajen de manera sincronizada y respuesta rápida, permite facilitar una respuesta ágil a los cambios en el campo de batalla o situaciones de emergencia.

El apoyo de comunicaciones es una función crítica en las operaciones militares, permite que la información fluya de manera segura y eficiente sin interrupciones entre las unidades, proporcionando la infraestructura necesaria para la toma de decisiones y la coordinación efectiva de las operaciones.

Definición de términos

El Manual de Empleo ME 11-221. (2013) Guerra Electrónica, define lo siguiente:

Ataque Electrónico (AE). Es la actividad de GE que tiene el propósito de negar o disminuir el empleo seguro del espacio electromagnético del adversario, así como destrozar, anular o disminuir su posibilidad de operación en la guerra, utilizando para ello energía electromagnética propia o por medio del guiado de misiles. Se divide en AE destructivo y AE no destructivo (perturbación y engaño electrónico).

Campo de comunicaciones y no comunicaciones. El primero es la parte del espectro en que operan los equipos utilizados para el tránsito de informaciones (radiotransmisores y receptores en general), y el segundo es la parte del espectro en que operan los equipos utilizados para producir informaciones, como los radares de vigilancia; sensores remotos; sistemas electrónicos de guiado de misiles.

Centro de comunicaciones (Cecom). Instalación responsable de recibir y transmitir mensajes. Generalmente incorpora personal y medios para su funcionamiento. Es la que se encarga de la administración de las redes de radiotácticas, así como redes alámbricas, mensajeros, etc. Son objetivos de alto valor para la guerra electrónica del adversario.

Chaff. Son pequeñas fibras de aluminio que, al ser lanzadas al aire, generan una nube o cortina electromagnética, la cual refleja las ondas de radar, considerada como una contramedida de radar debido a su capacidad de perturbar, saturar y abrumar la pantalla de radar, el objetivo de esta acción es ocultar temporalmente la nave.

Comando y Control (C2). Es el ejercicio del mando de las fuerzas por parte de un comandante nombrado apropiadamente para cumplir un objetivo. Durante las operaciones, los comandantes utilizan el mando y control para integrar otras funciones de la guerra y sincronizar su propia fuerza en el momento, el espacio y el objetivo.

Espectro electromagnético. También llamado espacio o entorno electromagnético…, es la dimensión empleada por los equipos de comunicaciones y no comunicaciones y, en común, cualquier otro transmisor que emita señales de ondas.

Energía electromagnética. Es la energía existente en la onda de radio, que se difunde en el ambiente electromagnético, capaz de inducir un campo eléctrico y magnético en la antena de recepción.

Engaño electrónico o decepción electrónica. Son operaciones de radiación deliberada, reradiación, cambio, impregnación, intensificación o rebote de la potencia electromagnética; de tal manera que intenta confundir o desconcertar al adversario en el análisis los datos recepcionados por sus plataformas de comunicaciones o no comunicaciones.

Frecuencia protegida. Nuestras fuerzas tácticas las utilizan para satisfacer necesidades operativas específicas. El comandante táctico de más alto escalón las nombró para supervisar la interferencia causada por nuestras acciones de perturbación y engaño electrónico.

Guerra Electrónica (GE). Es el conjunto de acciones con objetivo de afianzar el uso real de las radiaciones electromagnéticas amigas; al mismo tiempo, busca impedir, dificultar, destruir o explotar las emisiones enemigas. Es dividida en tres actividades: Soporte Electrónico (SE), Ataque Electrónico (AE) y Protección Electrónica (PE).

Inteligencia de Comunicaciones. Parte de la Inteligencia de Señales, cuyo producto es el resultante de la colección, interceptación, monitoreo y análisis de emisiones de los equipos de comunicaciones del oponente, como los radiotransmisores y receptores en general. Tiene por objetivo crear la base de datos de los emisores de comunicaciones del oponente, asociándolos a sistemas de armas.

Inteligencia electrónica. También conocida como inteligencia de No comunicaciones, es la actividad de colección y procesamiento técnico de informaciones derivadas de radiaciones electromagnéticas, excluidas aquellas destinadas a las comunicaciones.

Localización electrónica. Es el proceso de determinación por medios electrónicos de la ubicación de una fuente emisora de energía electromagnética. Es acción de SE.

Monitoreo. Es el acto de escuchar las comunicaciones propias o del enemigo. La primera es realizada con la finalidad de conservar y/o mejorar las medidas de PE, la segunda es para obtener informaciones del oponente.

Perturbación. Es la radiación o reradiación intencionada de la potencia electromagnética, con la finalidad de impedir u obstaculizar el empleo de los dispositivos, medios radiales o electrónicos, sean amigos o enemigos. Es un Ataque Electrónico no destructivo.

Protección Electrónica (PE). División (actividad) de GE que tiene por misión asegurar la utilización eficiente del espectro electromagnético por nuestras fuerzas, no importando si el oponente tiene o no equipos de GE.

Radar. Es un dispositivo electrónico que permite, por medio del manejo de las características del empleo de equipos de radio, detectar la presencia de objetos, determinar su distancia, dirección, velocidad y altura, y reconocer algunas de sus características.

Salto de Frecuencia (AJ). Técnica de espectro extendido que consiste en hacer que la frecuencia del transmisor cambie dentro de una banda ancha según una secuencia pseudo aleatoria codificada.

Soporte Electrónico (SE). División de la GE que consiste en la obtención de datos del oponente a partir de la adquisición de sus señales electromagnéticas. Tiene la finalidad de interceptar e identificar esas emisiones y localizar sus fuentes emisoras con el objetivo de realizar el reconocimiento inmediato de la amenaza. Realiza las mismas acciones de

obtención de información, localización electrónica, interpretación y emisión que la Inteligencia de Señales.

Técnica de triangulación. Es la capacidad de acceder a triángulos a través de la intersección como mínimo de tres direcciones marcadas sobre una carta, con finalidad de levantar áreas probables de localización de la fuente emisora.

Parámetros de seguridad. Son los programas de seguridad ya instalados en los equipos de radio que requieren de técnicas especializadas del operador para ser modificadas o reprogramadas en el equipo antes de emplearse.

Destrucción física. Es la destrucción del emisor receptor o estación de radio a través de la emisión de ondas que queman los circuitos de las radios o la destrucción por medio de las coordinaciones con los sistemas de armas del adversario.

Destrucción electrónica. Es cuando, a través de la acción del Ataque Electrónico, no se pueda emplear el equipo de radio o que se emplee de la manera que deseamos para favorecer a nuestras intenciones tácticas.

Perturbación de radar. Es disminuir temporalmente la efectividad del equipo electrónico enemigo, ya sea bloqueando o sobresaturando el receptor con una señal potente. Es afectar los sistemas de seguimiento, rastreo o escucha, enviando señales de ondas que tiendan a confundir dichos sistemas.

Otros términos:

Agrupamiento de Comunicaciones José Olaya (Agrup Com "JO"). Gran Unidad de Combate de Comunicaciones, creada en el año 2009 como 3ra Brigada de Comunicaciones, posteriormente se le denominó el año 2017 como Agrupamiento de Comunicaciones "José Olaya" encarga de proporcionar el apoyo de comunicaciones a las operaciones que realiza la División Costa y División Sierra. (Manual de Operaciones y Funciones).

Apoyo de Comunicaciones. Es la que proporciona el Agrupamiento de Comunicaciones "José Olaya" relacionado con combate de comunicaciones y guerra electrónica limitada, al despliegue y preservación de la fuerza, con orden, en la zona de combate, para ayudar el comando y control de la fuerza, ... (Informe de Capacidad Operativa 2023).

Cable de Campaña WD-1/TT. Es el cable de uso militar que se emplea en instalaciones de integración radio-alámbrica y medios de comunicación alámbricos para enlazar a dos operadores de teléfono de campaña a una distancia máxima de 35 km, (MTE 11-200: Características Técnicas de Material de Comunicaciones en uso en el Ejército).

Concepto de capacidades. Es la metodología empleada para determinar el diseño de una fuerza que haga frente a las amenazas identificadas, así como determinar las brechas que impiden o dificultan el diseño de la fuerza. (Plan de Empleo y Magnitud de la Fuerza 2023-DIPLANE).

Control Remoto AN/GRA 39. Es la unidad de control remoto que se emplea para la integración radio-alámbrica, … cuando se conecta con una radio, la unidad de control remoto permite al operador transmitir y recibir comunicaciones de frecuencia de voz a través de la radio a una distancia de hasta 3,5 kilómetros (Manual Técnico).

Capacidad operativa de comunicaciones. Es un subfactor de la capacidad operativa del factor de logística, expresado en porcentaje de operatividad de los equipos y material de comunicaciones. Los factores para determinar la capacidad operativa de una gran unidad son la cantidad de material asignada en relación con el Cuadro de Organización y Equipo (Coeq), la operatividad del material, obsolescencia tecnológica y tiempo de uso en relación con el año de afectación. (Directiva N° 007/07.10.01/H-2/OPPE).

Enmascaramiento electrónico. Es la emisión moderada de la potencia electromagnética en la gama de frecuencias empleadas por las estaciones de radio propias, con la finalidad de cuidar nuestras señales de radio y plataformas de comunicaciones contra el empleo de Soporte y Ataque Electrónico enemigo, midiendo su búsqueda de la información, sin disminuir notablemente el funcionamiento de nuestras estaciones de radio. Electronic Warfare Techniques, ATP 3-12.3).

Economía de fuerzas. Se trata de la adecuada distribución y gestión de las fuerzas disponibles para que no sean mal utilizadas al ser recursos limitados y difíciles de reponer en el corto plazo. Izcue & Arriarán (2013).

Modo secreto. Es el modo de emisión de radio en el que la señal emitida sale codificada hasta llegar al receptor (MTE 11-200 Características Técnicas del Material de Comunicaciones en uso en el Ejército).

Sincronización. Es el agrupamiento de tareas militares en un determinado momento, área decisiva y finalidad para producir la más alta potencia combativa (ME 1-134 Planeamiento de las Operaciones Terrestres).

Radio-alámbrica. Proceso de integración de los medios de alámbricas con los medios radiales, lo que permite comunicaciones entre dos estaciones de radio separadas más allá del alcance normal (ME 11-2 Empleo del Batallón de Comunicaciones).

Riesgo critico. Cuando existe la posibilidad de que una actividad altere los resultados, se debe considerar que existe un riesgo. También señala que un evento o incidente crítico se considera cuando puede causar daño a personas, equipos y/o materiales, así como detener las operaciones o la producción. Phiipe (2008).

Capítulo II: Materiales y Métodos

La pesquisa realizada se basó en el enfoque cualitativo, debido a que se indaga conocer nuevos conceptos sobre el empleo de los equipos remotos de comunicaciones para incrementar las operaciones de Protección Electrónica como consecuencias de las experiencias de los especialistas en comunicaciones y guerra electrónica en los entrenamientos para guerra convencional. El enfoque cualitativo, según Hernandez y Sampieri (2018), dirige y profundiza el fenómeno de estudio, investigando la información desde la perspectiva de los participantes en relación con el conocimiento y las experiencias.

El tipo de la investigación fue de naturaleza teórica-empírica. Esto se debió a que se examinara el tema en cuestión desde la perspectiva de la teoría del tema de estudio que existe actualmente. En consecuencia, se realizó un análisis de la realidad empírica al mismo tiempo que se examinaba el contexto teórico. Vargas (2011), afirma que las preguntas, los objetos de estudio y los ámbitos de estudio determinan el tipo de investigación a realizar. La investigación teórico-empírica es un tipo de investigación que explora primero la estructura categorial y empírica de una realidad específica y luego la lleva a una discusión con varios autores teóricos.

El método de la investigación fue fenomenológico-hermenéutico; se basó en las experiencias de los especialistas en comunicaciones y guerra electrónica en el fenómeno estudiado y reveló los componentes comunes de esas experiencias. Según Creswell (2013), esto se traduce en un enfoque para pesquisar la incógnita que inserta entrar en el campo de la percepción de los integrantes; observar cómo se percatan, perviven y desdoblan el fenómeno; y buscar la acepción de las experiencias de los integrantes.

El objeto de estudio constituye lo que se va a investigar y que permite conocer la problemática que va a ser analizada. En relación al objeto de estudio. Izcara (2014), sostiene que un objeto de estudio más específico, que se centra en un aspecto o situación concreta, permite un enfoque más general. Finalmente, el tema de investigación debe ser significativo, es decir, debe ser relevante para la disciplina y contribuir al crecimiento del conocimiento.

En el desarrollo del estudio, fue describir, identificar, explicar y develar nuevos procedimientos para el empleo de la integración raidoalámbrica de diversos equipos de comunicaciones radiales y que estos nuevos procedimientos puedan impedir acciones de SE y AE, de manera de incrementar las operaciones de Protección Electrónica en el Agrup Com José Olaya.

La muestra de estudio utilizada fue intencional; en primer lugar, se tomó una muestra homogénea a 03 expertos en guerra electrónica y 04 expertos en comunicaciones que laboraron y laboran en el Agrup Com José Olaya, desde el año 2013 al año 2023, para conocer su opinión sobre el empleo de medios remotos de comunicaciones para incrementar las operaciones de protección electrónica, así como sus experiencias y conocimientos para

solucionar o proponer cambios a la vulnerabilidad actual de las comunicaciones ante las actividades de SE y AE del enemigo, y en segundo lugar, se incluyó a personal de operadores de radio que laboran actualmente en la gran unidad, quienes apoyaron con la realización del empleo y operaciones de los medios de control e integración radio alámbrica. Según Creswell (2013), la investigación cualitativa no busca generalizar resultados a una población amplia, sino profundizar en contextos específicos y significativos subjetivos.

Criterios de inclusión: personal de comunicaciones que laboró y labora en el Cuartel Mariano Melgar, personal con experiencia en los entrenamientos de guerra convencional del 2013 al 2023 y que tengan conocimiento en guerra electrónica y comunicaciones.

Criterios de exclusión, personal de comunicaciones que no laboró en el Cuartel Mariano Melgar y personal que no sean especialistas en guerra electrónica y comunicaciones.

El ámbito seleccionado para realizar el procedimiento desarrollado fueron las instalaciones del cuartel “Mariano Melgar”, tomándose los criterios de disponibilidad del material y equipo, disponibilidad de personal, operadores de radio y especialistas en guerra electrónica y comunicaciones. Estas instalaciones son de la gran unidad donde se detectó el problema a investigar.

Las técnicas e instrumentos de recolección de datos, previo a la aplicación de las técnicas e instrumentos, se solicitó la autorización obteniendo el permiso respectivo; se realizaron las coordinaciones para la aplicación de los instrumentos con el Comando de la gran unidad y personal responsable del material y equipo en el mes de octubre del 2023; así como se dio una explicación al personal entrevistado sobre la naturaleza del estudio y los objetivos a llegar. Las técnicas e instrumentos de recolección de datos fueron diversos, a los cuales se accedió para procesar parte de las informaciones que se utilizaron en las instalaciones del cuartel “Mariano Melgar” de Arequipa. Según Barrantes (2002), la investigación cualitativa puede realizarse a través de la observación y la información de documentos, así como entrevistando a las partes involucradas en los hechos o fenómenos.

La entrevista. Esta técnica tuvo como instrumento la Guía de Entrevista no estructurada con 10 preguntas (05 preguntas para cada categoría y subcategoría) en forma de interrogantes abiertas y contestaciones de personal de oficiales especialistas en guerra electrónica y comunicaciones que laboran y laboraron en la gran unidad de comunicaciones; dicho instrumento fue validado por expertos; en las entrevistas, a través de una conversación con los entrevistados, se recopiló la información tomando aspectos sobre sus experiencias en los entrenamientos y ejercicios de comunicaciones para guerra convencional a partir del año 2013 al 2023, así como sus opiniones, conocimientos y sensaciones sobre los procedimientos nuevos de empleo de equipos remotos de comunicaciones y de cómo estos procedimientos incrementaron las capacidades de PE que contribuyeron con el apoyo de comunicaciones al comando y control.

La observación. En el empleo, la Guía de la Observación no se restringió en solo ver el uso y procedimientos del empleo de los materiales y equipos de las unidades de control remoto y medios de comunicaciones radiales, sino también el empleo de otros sentidos, como el de escuchar de manera clara sin perturbaciones las señales de radio del Cecom, las cuales fueron enmascaradas electrónicamente. También se tuvo como objetivo el observar y comprender la designación del personal de operadores de radio que operaron en la estación de protección, y seleccionar los especialistas de guerra electrónica y comunicaciones que participaron en el nuevo procedimiento de empleo de los medios de comunicaciones que actualmente cuenta la institución; Identificar los tipos de operaciones de protección electrónica resultantes del nuevo procedimiento y develar que el incremento de la Protección Electrónica contribuye con el apoyo de comunicaciones.

El análisis de documentos y materiales. Se realizaron a través de la herramienta de Ficha de Análisis Documental; fueron de origen muy valioso para asistir y entender este fenómeno específico de la indagación. Ayudó a comprender el contexto del ambiente, las experiencias o situaciones que tienen lugar en él.

Tabla 4

Técnicas e instrumentos aplicados con finalidad a emplear.

Técnicas	**Instrumentos**	**Finalidad**
Entrevista	Guía de entrevista	Se recopiló información de expertos en GE y comunicaciones sobre sus experiencias en la actividad de PE y de qué manera ésta se pueda incrementar.
Observación	Guía de observación	Se describió, identificó, explicó y develó de manera directa, a través de la observación del estudio a realizar sobre el empleo de medios de control remoto y medios de radio de manera de incrementar la capacidad de PE.
Análisis Documental	Ficha de Análisis Documental	Se tuvo un fuente certera y quedó como antecedente de opinión, relacionado a PE en el campo de las no comunicaciones y que ésta sirvió como base para el campo de las comunicaciones.

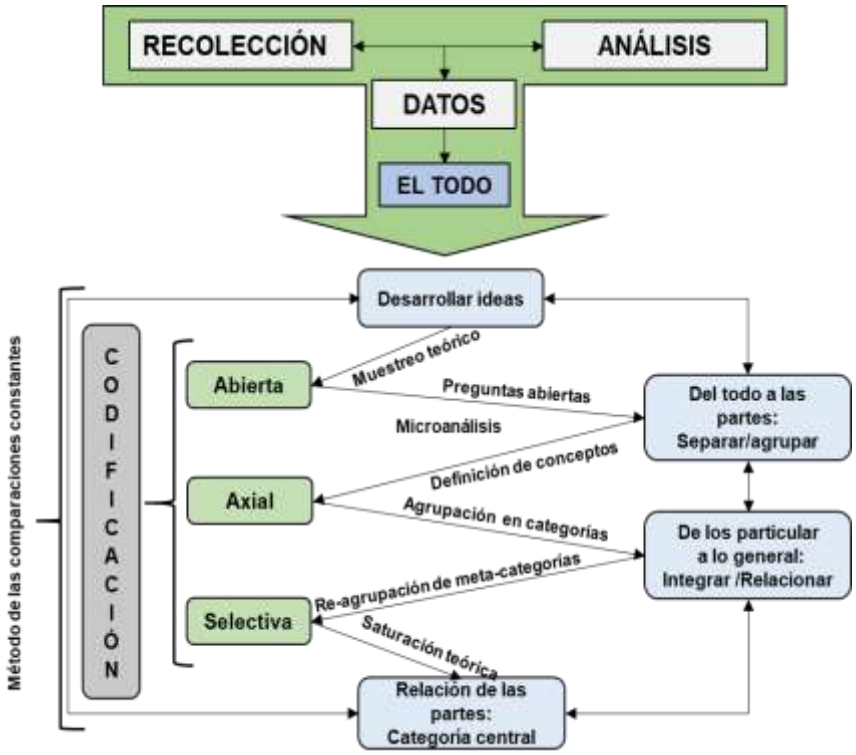
El rigor científico del desarrollo de la indagación tuvo una intención de desarrollar un trabajo de alta calidad, cumpliendo con el rigor del método de investigación. La validez de los instrumentos fue evaluada mediante juicio de expertos; en este sentido, se demostró el control de calidad de la puesta en conocimiento científica, a partir de los criterios basados en el método triangular. La credibilidad o validez interna se percibió en la connotación completa e intensa de la experiencia de los especialistas en guerra electrónica y comunicaciones, especialmente en relación con la propuesta del problema. Se utilizó la observación continua, triangulación y validación de los participantes. La aplicabilidad de los resultados no se generalizó a la población general, ya que este no era el objetivo de este estudio cualitativo,

pero el personal de oficiales, técnicos y suboficiales de la especialidad de comunicaciones y guerra electrónica que laboran en las unidades de comunicaciones puede aplicar los resultados durante sus entrenamientos para guerra convencional. La investigación fue consistente. Se evitó la inestabilidad mediante la realización de descripciones minuciosas de los entrevistados y participantes del procedimiento estudiado; se emplearon apuntes de campo, guías de entrevistas y documentos de referencia; la confirmabilidad se realizó mediante las entrevistas, observación, análisis de documentos y triangulación para evitar que los descubrimientos no estén inclinados por el entusiasmo, beneficio y puntos de vista propios.

Para la técnica de procesamiento y análisis de datos, se extrajeron conclusiones de la observación, análisis documentario y entrevistas, cuya redacción de las preguntas se compararon en categorías y subcategorías; se formularon las preguntas sobre qué, quién, cómo, cuándo, dónde, por qué y qué permite desarrollar la categoría de acuerdo a sus características; se buscaron sus condiciones conceptuales y estructura teórica. El material se organizó y analizó, utilizando el análisis de forma tradicional para comprender e interpretar datos cualitativos. Para Arispe et al. (2016), sobresale que en la mayoría de los estudios de análisis de datos cualitativos, los procesos de análisis, codificación y categorización son comunes. Esto se conoce como análisis de texto cualitativo.

Figura 11

Método de recolección y análisis de datos



Fuente: Arispe et al.(2016). La Investigación Científica.

Capítulo III: Resultados

3.1 Recolección de datos

El proceso para la obtención de los datos se realizó mediante las técnicas de entrevista, observación y análisis documental y material. Según Arispe et al (2020), los métodos cualitativos consideran diferentes tipos de recopilación de datos para comprender una realidad particular, incluidas entrevistas, documentos, observaciones y dibujos/fotos/películas.

Entrevistas

Se empleó como instrumento la Guía de entrevista no estructurada con diez (10) preguntas abiertas, cinco (5) para la categoría (Equipos remotos de comunicaciones) y subcategorías (Capacidad operativa de comunicaciones, Integración radio-alámbrica y Designación de operadores de radio) y cinco (5) para la categoría (Operaciones de protección electrónica) y subcategorías (Sincronización en la propagación de ondas, Tipos de operaciones de protección electrónica y Contribución con el apoyo de comunicaciones), la entrevista se realizó a siete (7) oficiales con el perfil de especialistas en guerra electrónica y en comunicaciones; contar con la experiencia y conocimientos en ejecutar ejercicios de comunicaciones para guerra convencional; así mismo, haber laborado y/o seguir laborando en el Cuartel “Mariano Melgar” desde el año 2013 al 2023. La entrevista a los oficiales, previa coordinación e inducción del tema a investigar, se realizó en octubre del 2023 de manera presencial y remota.

Observación

Se empleó como instrumento la guía de observación del empleo de los medios remotos de comunicaciones con 10 aspectos a evaluar relacionados con el procedimiento de empleo. En la observación de campo, aparte de los elementos de muestreo, se consideró lo siguiente:

- El entorno fue en las instalaciones del Cuartel “Mariano Melgar” de Arequipa.
- Los grupos fueron: el personal operadores de radio (técnicos y suboficiales) y el personal especialistas en guerra electrónica y comunicaciones (oficiales) con experiencias desde el año 2013 al 2023 en los entrenamientos para guerra convencional, dicho personal fue preparado para su participación en el empleo de los equipos remotos de comunicaciones. Las actividades actuales que realizan los participantes son de planeamiento y asesoramiento en el Estado Mayor, así como jefes de almacén de radios de las unidades del Agrupamiento de Comunicaciones Jose´Olaya.
- Los materiales y equipos a utilizar fueron:
    - Una (1) Unidad de Control Local GRA 39, ocho (8) unidades de control remoto GRA 39 y 1800m de cable de campaña.

- Ocho (8) equipos de radio (02 PRC 2200, 02 PRC 6020, 02 PRC 930, 01 PRC 730, 01 PRC 8020), 01 equipo de radio (VRC 6200) del Cecom de la gran unidad, uno (1) equipo de radio (VRC 6200) del Cecom de la III División de Ejército; así mismo, se emplearon dos (2) radios en alta frecuencia (HF) y muy alta frecuencia (VHF) para la verificación de la transmisión y 48 baterías BA30 (pilas).
- Equipo del proyecto de Soporte Electrónico (Interceptación y Localización).

- Los especialistas de comunicaciones y guerra electrónica que participaron en la observación fueron cuatro (4), de los cuales dos (2) fueron comandantes de unidad de la Compañía de Guerra Electrónica N° 113, uno (1) fue Ejecutivo del Batallón de Comunicaciones N° 113 y uno (1) fue Ejecutivo y Cmdte. de Unidad de la Compañía de Comunicaciones N° 8 del Cuartel Mariano Melgar.

La clase de observación que se desarrolló fue natural, participativa y estructurada y el papel de los observadores fue variado para impedir sesgos propios y contar con diferentes opiniones; los observadores participaron libremente, anotando diversos aspectos percibidos. Se consideraron los componentes esenciales de la técnica de observación:

Análisis documental.

Se utilizó la herramienta de la Ficha de Análisis Documental, por medio del cual se ordenó el material, registrándose cuatro (4) documentos literarios nacionales y tres (3) documentos literarios internacionales, asi como uno (1) material audiovisual, de manera de contar con un sustento teórico relacionado con las categorías y subcategorías, así como sobre las experiencias documentadas en los entrenamientos para guerra convencional realizados por la gran unidad y que fueron los cimientos para el problema a estudiar.

3.2 Organización de los datos

Entrevistas.

Se recopilaron las respuestas de los tres (3) especialistas en guerra electrónica y de los cuatro (4) especialistas de comunicaciones, transcribiendo las respuestas de las guías de entrevistas a una matriz en Word para su explotación, respetando en todo momento el principio de confidencialidad.

El criterio utilizado para la organización de los datos fue en referencia a las respuestas de los entrevistados relacionadas con las categorías de la investigación, posteriormente se organizó por orden secuencial de respuestas, codificándolas para que en relación con los patrones y temas se pueda identificar la similitud o diferencias sobre las experiencias, conocimientos y sensaciones de los entrevistados.

Tabla 5

Organización de datos en base a la entrevista - Equipos remotos de comunicaciones

Categoría	Sub categoría	Pregunta	Entrevistado	Patrones	Respuestas
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	Como oficial de comunicaciones durante su permanencia en el Agrup Com "JO", ¿ha tenido alguna experiencia sobre interferencias o perturbaciones en el empleo de los medios de comunicaciones de su unidad?	Entrevistado 1	Experiencia en el trabajo	Permanencia en el BCOM N° 113 y Agrup Com "JO", experiencia de COM y GE en el año 2013, fuerte perturbación de nuestros medios de C2 en las bandas de HF y VHF, crearon una zona de silencio por un espacio de tres horas.
			Entrevistado 2		Sí, en el año 2013 como ejecutivo de la CIA COM N° 08 y en el año 2014 como Comandante de Unidad, durante los entrenamientos para guerra convencional (GC), los medios radioeléctricos de HF y VHF fueron perturbados y/o interferidos por agentes externos.
			Entrevistado 3	Entrenamiento en Guerra Convencional (GC)	Sí, año del 2018 al 2020 como Cmdte de Unidad de la CIA G. ELECT N° 113 en los entrenamientos para guerra convencional, en el empleo de radios de campaña.
			Entrevistado 4		Si, año 2013 como Jefe de la Sección Inteligencia de Comunicaciones de la CIA G. ELECT N° 113, durante los ejercicios para guerra convencional (GC) , empleo de radios militares en (VRC 6200, PRC 6020 y PRC 930 y VRC 980).
			Entrevistado 5	Unidades de Comunicaciones	Sí, año 2013 y 2014 como S-3 de la CIA G ELECT N° 113 durante los entrenamientos para guerra convencional, empleo de medios de COM radioeléctricos y alámbricos con sus respectivos recursos técnicos anti soporte electrónico y anti ataque electrónico.
			Entrevistado 6		Sí, año 2013 como Ejecutivo y Jefe de Instrucción y Entrenamiento del BCOM N° 113, durante los entrenamientos para GC, empleo medios radioeléctricos en HF y VHF.
			Entrevistado 7		Si, año 2018 como Ejecutivo y Jefe de Instrucción y Entrenamiento S-3 del BCOM N° 113, ocurrieron interferencias de radios en los entrenamientos para guerra convencional.
		Teniendo conocimiento sobre la tecnología avanzada dispuesta en los sistemas de SE y AE en los conflictos y guerras actuales en el 2023. ¿Considera usted necesario la generación de nuevas propuestas o iniciativas que permitan optimizar el material de Com con que cuenta la institución?	Entrevistado 1	Iniciativas	Tener una visión estratégica, desarrollar nuevas propuestas o iniciativas y optimizar la implementación de dichos sistemas.
			Entrevistado 2		Sí, es necesario contar con propuestas nuevas con el material disponible. No se dispone de una adecuada PE, lo que limita la realización de las actividades SE, así como AE.
			Entrevistado 3		Es muy necesario, porque no contamos con equipos de PE que puedan hacer frente a las operaciones de soporte electrónico y ataque electrónico.
			Entrevistado 4	Nuevas propuestas	Por supuesto, esto es muy necesario; es importante considerar nuevas propuestas para optimizar los materiales de comunicaciones, por el crecimiento de la guerra electrónica enemiga especialmente en la localización y la interferencia electrónica.
			Entrevistado 5	Carencia	Sí, es necesario. Las iniciativas que deben construirse deben realizarse en base a las capacidades actuales del equipo, entrenamiento del operador y propuestas adicionales que busquen contribuir a la maniobra táctica, buscando mantener el comando y control.
			Entrevistado 6		Sí es muy necesario contar con tecnologías de comunicaciones modernas de última generación, no contamos con equipos y/o medios de PE para hacer frente en SE y AE.
			Entrevistado 7		Es muy necesario, en la actualidad no contamos con medios de PE; no puedes hacer frente a las nuevas capacidades electrónicas modernas del SE y AE.

Capacidad operativa de comunicaciones	Teniendo en consideración a las operaciones de PE ¿Conoce usted si las características técnicas que disponen los equipos remotos de Com, son vulnerables a las operaciones de Soporte Electrónico y Ataque Electrónico?	Entrevistado 1	Vulnerabilidad Perturbación Capacidades de PE	Dispositivo electrónico es vulnerable a los AE; las características que poseen nuestros radios definidos por Software no son suficientes para proteger las emisiones radioeléctricas y la seguridad física de los sistemas de comunicaciones
		Entrevistado 2		Si bien las características de equipos de radios que contamos actualmente son vulnerables a las acciones de GE enemiga, estos no son suficientes para proteger las emisiones radioeléctricas y seguridad física de los sistemas de comunicaciones.
		Entrevistado 3		Se cuenta, pero estos no son suficientes para proteger las emisiones y la seguridad física en los centros de comunicaciones y operadores de radio.
		Entrevistado 4		Se tienen, pero no son suficientes para proteger las emisiones de ondas de radio y mucho menos proteger la seguridad física de los centros de comunicaciones y sus operadores.
		Entrevistado 5		Los equipos remotos de comunicaciones son vulnerables a las operaciones de GE si no son bien empleados técnica y tácticamente.
		Entrevistado 6		Sí cuentan , pero estos no son suficientes para proteger las comunicaciones o enlaces, así como la integridad seguridad física de los centro de comunicaciones y personal.
		Entrevistado 7		Se tienen pero no son suficientes para proteger las emisiones y seguridad física de los Puestos de Comando y su personal de apoyo de comunicaciones.
Integración radio-alámbrica	Considera usted, ¿Cuál es el la finalidad de empleo de los equipos remotos de comunicaciones en las operaciones de Protección Electrónica?	Entrevistado 1	Seguridad Física y Electrónica Radio Localización Sistemas de armas Centro de comunicaciones Operación remota Unidad de control remoto	La finalidad, proteger al elemento más valioso, el factor humano, y lograr la supervivencia de nuestros sistemas.
		Entrevistado 2		La finalidad es operar los equipos de radio a distancia. La emisión de la señal electrónica se propague lo más lejos de las medios empleados, proporcione seguridad a los mismos, minimizando las acciones de radiolocalización y destrucción por los sistemas de armas.
		Entrevistado 3		El propósito de su uso es controlar remotamente equipos de radio para evitar operaciones de radiolocalización y la posterior destrucción de los sistemas de armas enemigos.
		Entrevistado 4		La finalidad de controlar de forma remota equipos de radio utilizando el GRA 39, garantizar la seguridad contra operaciones de localización electrónica y la destrucción por los sistemas de armas enemigos guiados electrónicamente.
		Entrevistado 5		La finalidad del empleo de los equipos remotos, es proteger a los puestos de comando y centro de comunicaciones de la localización electrónica y del AE destructivo y no destructivo.
		Entrevistado 6		La finalidad es que, por medio del empleo de los equipos GRA 39, se puedan operar de manera remota equipos de radio a distancia, proporcionar seguridad contra las acciones de radiolocalización y destrucción por los sistemas de armas enemigos, y 2do, crear confusión al enemigo.
		Entrevistado 7		La finalidad, se pueda operar a distancia las estaciones de radio y proporcionar seguridad contra las acciones de radiolocalización y destrucción por los sistemas de armas enemigos.

Designación de operadores de radio	La institución dentro de las especialidades técnicas contempla personal especialista en la operación de radios, ¿Considera usted que la designación del personal especialista como operadores de radio para el empleo de los medios remotos de comunicaciones, es igual a la designación de personal de operadores de radio para los centros de comunicaciones?	Entrevistado 1	Instrucción de GE Conocimiento Capacitación Operación de las estaciones Unidad de control remoto Diversidad de empleo	No es lo mismo; sus funciones son diferentes: el operador de comunicaciones opera sus equipos en una estación fija o móvil emitiendo señales en un pequeño ancho de banda; los operadores de radios a control remoto requieren de habilidades para operar diversos sistemas a la vez.
		Entrevistado 2		No es lo mismo; un operador de radio puede emplear con un solo equipo de control remoto diferentes estaciones de radios de manera simultánea. Los operadores de radio del Cecom están designados para emplear una estación de radio por cada red.
		Entrevistado 3		La diferencia es que los operadores de radio pueden utilizar una unidad GRA 39 e integrarlas simultáneamente en diferentes estaciones de radio; en el centro de comunicaciones los operadores de radio se asignan individualmente a cada estación de radio.
		Entrevistado 4		Se diferencia, los operadores de radio pueden controlar diferentes estaciones de radio simultáneamente; los operadores de radio en un centro de comunicaciones son asignados individualmente para controlar cada estación de la red.
		Entrevistado 5		No, el personal que debe operar estos equipos remotos debe contar con una mayor capacitación en el despliegue táctico y recursos técnicos del equipo, con la finalidad de poder lograr un empleo eficiente.
		Entrevistado 6		No es lo mismo; un operador de radio puede emplear con un solo equipo de control remoto diferentes estaciones de radios de manera simultánea, los operadores de radio del centro de comunicaciones del BCOM N° 113 estaban designados de manera individual cada estación de radio.
		Entrevistado 7		No es lo mismo; un operador de radio puede emplear con un solo equipo de control remoto diferentes estaciones de radios al mismo tiempo. Los operadores de radio del centro de comunicaciones, están designados de uno por cada red radio.

Nota. La matriz muestra el criterio lógico (codificación abierta) para organizar las respuestas de los entrevistados, relacionados con las preguntas de la Guía de entrevista, basándose en la categoría Equipos remotos de comunicaciones y sus subcategorías que guardan relación con los patrones, las cuales se han extraído de la lectura temática de la información registrada, de manera de identificar la similitud o diferencias sobre las experiencias, conocimientos y sensaciones de los entrevistados.

Tabla 6

Organización de los datos base a la entrevista - Operaciones de protección electrónica.

Categoría	Sub categoría	Pregunta	Entrevistado	Patrones	Respuestas
Operaciones de Protección Electrónica	Sincronización de la propagación de ondas	En base a su experiencia, considera que, ¿La sincronización de las comunicaciones es uno de los factores importantes para las operaciones de enmascaramiento electrónico como parte de la Protección Electrónica?	Entrevistado 1	Importancia	Es muy importante; permite proteger nuestras operaciones; es una gran herramienta para la seguridad de las maniobras, así como de dificultar al enemigo en su accionar de SE.
			Entrevistado 2		Sí que es muy importante, es una manera de enmascarar electrónicamente la señal protegida; permite contar con una adecuada PE y desorientar las acciones de guerra electrónica sobre la real fuente electromagnética a identificar.
			Entrevistado 3	Modalidad de protección	Sí, es importante. Es el blindaje electrónico de las emisiones protegidas al transmitir energía electromagnética al mismo tiempo que el centro de comunicaciones lo que podría provocar la desorientación del sistema de guerra electrónica enemigo.
			Entrevistado 4		Sí es muy importante, porque se vio la emisión de energía electromagnética simultáneamente con las estaciones del Cecom. Pudo cubrir electrónicamente la frecuencia real, por la cual se realizan los enlaces para ejercer el comando y control.
			Entrevistado 5	Señal protegida	Sí, es muy importante, es un método para proteger electrónicamente la transmisión del Cecom, causando que el sistema de guerra electrónica del enemigo se desoriente y no pueda identificar y encontrar la correcta fuente electromagnética.
			Entrevistado 6	Simultáneo	Sí, es muy importante porque se irradian múltiples señales de radio en paralelo a la señal protegida; esta es una forma de cubrir la transmisión de señales prioritarias a través de las cuales se realizan las comunicaciones para respaldar el comando y control.
			Entrevistado 7	Desorientación	Sí, es muy importante radiar energía electromagnética simultáneamente en tiempo y espacio con las del Cecom. Estas señales cubren electrónicamente la señal protegida, lo que provoca desorientación a los sistemas de guerra electrónica.
	Tipos de operaciones de protección electrónicas	En el tiempo que participó en los entrenamientos para operaciones de guerra convencional. ¿Qué operaciones de Protección Electrónica pudo identificar para contribuir con el apoyo de comunicaciones al Comando y Control proporcionado por el Agrupamiento de Comunicaciones “José Olaya”?	Entrevistado 1	Enmascaramiento electrónico	Programar los equipos en seguridad y parámetros Anti perturbación, un solo equipo de control remoto, operaron de manera simultánea, emitiendo señales al mismo tiempo en el apoyo de comunicaciones.
			Entrevistado 2		Parámetro de seguridad, Anti perturbación (A.J.), de manera de evitar la interceptación y análisis de las emisiones, enmascaramiento permitió reducir las acciones de GE.
			Entrevistado 3	Parámetros de seguridad	Parámetros de seguridad para evitar la interceptación y análisis de transmisiones cubrieron las señal real, identificando una nueva acción anti AE y anti SE lo que pudo evitar perturbaciones en las señales.
			Entrevistado 4	Procedimientos operacionales	Parámetros de seguridad para evitar interceptaciones y análisis de emisiones. Al conectar las radios a la unidad de control remoto GRA 39, se pudo identificar operaciones contra las perturbaciones y contra la radiogoniometría.
			Entrevistado 5	Instalación remota	Realizaron operaciones de PE a través de los recursos técnicos de las radios, con procedimientos operacionales, enmascaramiento electrónico para evitar que la señal protegida sea localizada y perturbada.
			Entrevistado 6	Radiación simultánea	Estas radiaciones de energía electromagnéticas permitieron cubrir la señal del centro de comunicaciones, evitando perturbaciones que pudieran neutralizar las señales.
			Entrevistado 7		Parámetros de seguridad en función de sus características técnicas, medidas de PE para evitar análisis de emisiones, actividades anti-perturbación y anti-localización, ocultar señales verdaderas.

Contribución con el apoyo de comunicaciones	En base a su experiencia ¿Cómo describiría el aporte para mantener el enlace de las comunicaciones en apoyo al comando y control proporcionado por el Agrupamiento de Comunicaciones “José Olaya” en los entrenamientos para operaciones de guerra convencional?	Entrevistado 1		Fue muy buena porque puso a prueba el ingenio e innovación de los oficiales de comunicaciones, dado que se trabajó con equipos no tan sofisticados empleando el radio móvil para nuestro planeamiento
		Entrevistado 2		Cubriendo las emisiones del centro de comunicaciones, se contribuyó a mantener los enlaces entre las grandes unidades, permitiendo que se cumpla con la misión de proporcionar el apoyo de comunicaciones a la fuerza.
		Entrevistado 3		Ayudó a mantener las comunicaciones entre las grandes unidades durante todo el ejercicio.
		Entrevistado 4		Contribuyó a mantener los enlaces entre las grandes unidades durante toda la programación de entrenamiento.
		Entrevistado 5	Mantener enlaces	Se realizaron actividades anti-localización electrónica para neutralizar las actividades de ataque electrónico del enemigo.
		Entrevistado 6		Con cubrir las emisiones del Cecom del BCOM N° 113, esto contribuyó a mantener las comunicaciones del PC con las demás brigadas durante el apoyo al comando y control.
		Entrevistado 7		Contribuyó a mantener los enlaces con los puestos de comando de todas las grades unidades.
	¿Que opinión tendría Ud., sobre las consecuencias o efectos de no implementar procedimientos nuevos para incrementar las operaciones de Protección Electrónica en la Institución?	Entrevistado 1	Grandes unidades.	Pondríamos en riesgo nuestro sistema de comando y control y por ende la supervivencia de nuestros puestos de comando.
		Entrevistado 2		No contar con medios de última generación que dispongan capacidades de PE que sea soporte de las operaciones defensivas, llevaría una gran vulnerabilidad defensiva.
		Entrevistado 3	Innovación	Nuestras fuerzas estarán en una enorme desventaja táctica y en riesgo las operaciones.
		Entrevistado 4		No contar con las capacidades de PE en la conducción de las operaciones defensivas. Esto nos llevará a la destrucción inminente y total de nuestra fuerza.
		Entrevistado 5	Nivel de eficiencia	No se lograría proteger. Se pondría en riesgo el apoyo al comando y control del componente terrestre, ante la evidente ventaja tecnológica del adversario.
		Entrevistado 6	Riesgo crítco	No contar con capacidades de PE suficientes para el apoyo a las operaciones defensivas y/o ofensivas; esto tendría como consecuencia una destrucción inminente de nuestra fuerza.
		Entrevistado 7		No contar con eficaces operaciones de PE en las operaciones defensivas generaría un riesgo crítico, seríamos parte de una vulnerabilidad crítica a explotar por el enemigo.
	Con los medios de comunicaciones disponibles que cuenta nuestra institución, desde su punto de vista ¿Cuál cree que es el nivel de eficiencia, alto, medio o bajo de las operaciones de Protección Electrónica?	Entrevistado 1	Capacidades de PE.	Nuestro nivel de eficiencia es limitada.
		Entrevistado 2	Tecnología	Nivel de eficiencia es bajo, teniendo en consideración que el avance de la tecnología hace que los ejércitos modernos cuenten con capacidades operacionales eficientes para entrar en conflicto.
		Entrevistado 3		Los niveles de eficiencia son bajos en vista de que los equipos no brindan una capacidad de protección electrónica.
		Entrevistado 4		Medio/bajo por la experiencia y consideraciones antes mencionadas.
		Entrevistado 5		Bajo es el nivel debido a la ventaja tecnológica del adversario en operaciones de guerra electrónica.
		Entrevistado 6		Bajo porque seguimos con las mismas capacidades de hace diez (10) años; no disponemos con medios de guerra electrónica, ni mucho menos con sistemas o plataformas de comunicaciones como sistemas integrados.
		Entrevistado 7		El nivel de eficiencia es bajo. El desarrollo de nuevas tecnologías para la interceptación o perturbación de señales es incesante, tanto así, que genera una brecha tecnológica que no puede cubrirse sólo con el compromiso.

Nota. La matriz muestra el criterio lógico (codificación abierta) para organizar las respuestas de los entrevistados a las preguntas de la Guía de entrevista, basándose en la categoría Operaciones de protección electrónica y sus subcategorías que guardan relación con los patrones, los cuales se han extraído de la lectura temática de la información registrada de manera de identificar la similitud o diferencias sobre las experiencias, conocimientos y sensaciones de los entrevistados.

Observación.

Se recopilaron las anotaciones como resultado de las observaciones de tres (3) especialistas en guerra electrónica, incluido el investigador y uno (1) especialista de comunicaciones, transcribiendo, digitalizando y centralizando las respuestas de las guías de observación a una matriz en Word, respetando en todo momento el principio de confidencialidad.

El criterio lógico empleado para la organización de los datos fue relacionar los aspectos a evaluar de cada oficial especialista que participó como observador con las categorías y subcategorías del estudio.

Tabla 7

Organización de los datos en base a la observación - Equipos remotos de comunicaciones.

Categoría	Sub categoría	Aspecto por evaluar	Observador	Patrones	Respuestas
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	Los medios de comunicaciones se encuentran operativos y están programados	Observador 1 (Investigador)	Programación	Se programaron ocho (08) radios en diferentes modalidades de emisión, así como la operatividad de la unidad de control remoto.
			Observador 2	Recursos Técnicos	Las radios se programaron en Claro Secreto y Salto de Frecuencia, así como la operatividad de la Unidad GRA 39.
			Observador 3	Operatividad	Inicialmente probaron la operatividad de las radios, baterías, antenas, parámetros de Seguridad y Salto de Frencuencia (AJ).
			Observador 4		Se verificó que las radios y GRA 39 estén operativas, probando su enlace con el Cecom en diferentes modalidades de seguridad.
		Se realizó el nuevo procedimiento de despliegue, instalación e integración de los medios de comunicaciones.	Observador 1 (Investigador)	Nuevo procedimiento	Es nuevo, se empleó una estación local GRA 39, conectadas a 08 unidades de control remoto del GRA 39 por medio del cable de campaña, integrándose cada estación de radio.
			Observador 2		Se instaló una estación local y 08 unidades de control remoto del GRA 39 por cable de campaña, integrándose a las 08 estaciones de radio.
			Observador 3	Integración del GRA 39 y 08 estaciones de radio	Inicia desde la instalación de unidades de control local, conectadas por medio del cable de campaña a 08 unidades de control remoto, posteriormente, éstas se integran a las 08 estaciones de radio.
			Observador 4		Nuevo, se procedió con la instalación de una unidad de control local, se conectó 08 líneas de cable de campaña, cada línea a una unidad de control remoto y estas unidades se integraron a las 08 estaciones de radio
		Las unidades de control remoto y unidad local del equipo GRA 39 se interconectan con las estaciones de radio a distancia	Observador 1 (Investigador)	Instalación remota	Se realizó el ejercicio de una estación a 500 m, posteriormente a 200 y 300 m aproximadamente.
			Observador 2		Se instaló una estación a 500 m de distancia y después a 200 y 300 m.
			Observador 3		De manera de probar la conexión, se operó una radio a 500 m y para el ejercicio fue a 200 y 300m.
			Observador 4		Se interconectaron de 200 a 500 m de distancia.
		Las emisiones de ondas son emitidas de manera simultánea en las diferentes estaciones de radio cuando son operados remotamente con los parámetros programados.	Observador 1 (Investigador)	Señal simultánea Recepción de la señal	Se encuentran operando simultáneamente, sin novedad. Se comprobó la recepción de la señal, así como la señal del Cecom.
			Observador 2		Las señales de los equipos salen en un 5 x 5 con los parámetros de seguridad de manera simultanea.
			Observador 3		Salen simultáneamente y se verificó con una radio la recepción y se pudo interconectar con cada una de las estaciones. El Cecom lo hizo con la III DE.
			Observador 4		Todas las radios están operando simultáneamente sin novedad. Se pudo comprobar la recepción de las señales.

Integración radio-alámbrica	El personal que operan las estaciones de radio, conocen la finalidad de empleo del material.	Observador 1 (Investigador)	Estaciones radio	Si conoce la finalidad de ejercicio.
		Observador 2	Enlace remoto	Los operadores saben las ventajas de este modo de empleo de las radios
		Observador 3	Procedimiento operacional	Conocen su finalidad de dar seguridad física y electrónica.
		Observador 4	Seguridad física y electrónica	Cuenta con conocimientos de guerra electrónica.
Designación de operadores de radios	Son más de 2 los operadores que integra la estación de protección electrónica,	Observador 1 (Investigador)	Un operador de radio Instrucción de guerra electrónica	Sólo se empleó un operador de radio capacitado en Guerra Electrónica para empleos remotos de las 8 estaciones.
		Observador 2		Se tuvieon previsiones de designar a dos operadores, pero solo fue necesario uno.
		Observador 3		Un solo operador de radio a través de la Unidad de control local GRA 39 opera las 8 radios.
		Observador 4		Se emplea solo un operador de radio.

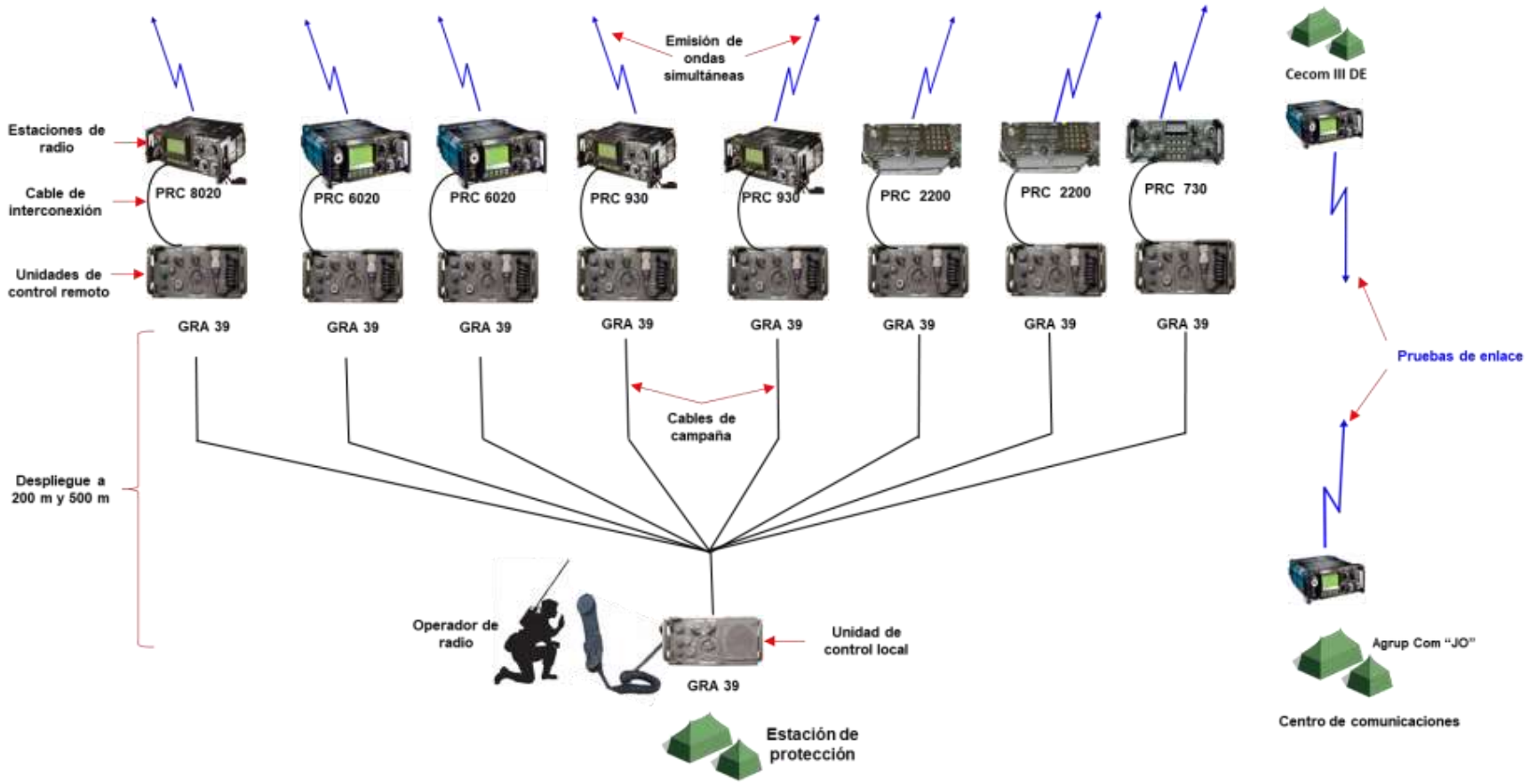
Tabla 8

*Organización de los datos en base a la observación - Operaciones de Protección Electrónica***.**

Categoría	Sub categoría	Aspecto por evaluar	Observador	Patrones	Respuestas
Operaciones de Protección Electrónica	Sincronización de la propagación de ondas	Existe sincronización en las emisiones de radio entre la estación del CECOM del Agrup Com "JO" con las estaciones de radio operadas de manera remota.	Observador 1 (Investigador)	Entrenamiento con el Centro de comunicaciones.	Después de varios ensayos se logró la sincronización.
			Observador 2		Si había sincronización de las emisiones de radio con el centro de comunicaciones, se tuvo que entrenar.
			Observador 3	Emisiones de ondas	Si existe sincronización en las transmisión de la señales de la estación de protección con el centro de comunicaciones.
			Observador 4	Estaciones de radio	Después de varios ejercicios, sí existe sincronización de las señales emitidas por las radios y la señal del centro de comunicaciones.
	Tipos de operaciones de protección electrónicas	Identifica operaciones de Protección Electrónica, que tipos según su observación.	Observador 1 (Investigador)	Enmascaramiento electrónico.	Se observó operaciones de protección electrónica de tipo, enmascaramiento.
			Observador 2		Se identificó un Enmascaramiento electrónico.
			Observador 3	Recursos Técnicos	Se generó acciones Anti Soporte Electrónico; Anti Ataque Electrónico, así como Enmascaramiento electrónico.
			Observador 4		Se protegió la señal del centro de comunicaciones con acciones Anti Localización y Anti Perturbación.
	Contribución con el apoyo de comunicaciones	Las señales de radio de la estación del Centro de Comunicaciones del Agrup Com "JO" están interferidas o perturbadas.	Observador 1 (Investigador)	Interferencia y Perturbación	No hay ningún tipo de interferencia externa ni de las propias emisiones de ondas.
			Observador 2		No hay perturbación.
			Observador 3		Las señales están sin novedad.
			Observador 4		No hay interferencia exterior ni de las propias estaciones de radio.
		Se pudo mantener las comunicaciones entre el Centro de comunicaciones del Agrup Com y el Cecom de la III DE.	Observador 1 (Investigador)	Centro de Comunicaciones	Se mantiene durante la transmisión.
			Observador 2		Existe enlace entre los centros de comunicaciones.
			Observador 3	Mantener enlaces.	La señal del centro de comunicaciones se escuchó durante todo el ejercicio.
			Observador 4		El Centro de Comunicaciones se pudo enlazar durante la prueba.

Figura 12

Esquema del proceso de integración realizado en la observación.



*Nota***.** La figura muestra a un operador de radio manejando a una Unidad de Control Local GRA 39, la cual se integra a través de cables de campaña a ocho (8) unidades de Control Remoto GRA 39, interconectadas a ocho (8) estaciones de radio para emitir ondas electromagnéticas simultáneas y se muestran pruebas de enlace entre los Centros de Comunicaciones (Cecom).

Análisis documentario.

Esta técnica se desarrolló para saber los aspectos teóricos, antecedentes, experiencias documentadas que contribuyeron a proponer las categorías y subcategorías que están referenciadas en el marco teórico del presente estudio. En relación con esto, el análisis documental atendió los puntos de vista lógicos para la organización de los datos siguientes:

Tabla 9

Organización del contenido del análisis documental - Equipos de remotos de comunicaciones

Categorías	Material/ Documento Referencia	Temas	Contenido
Equipos remotos de comunicaciones	Manual Técnico Unidad de Control GRA 39 (1991)	- Unidad de Control GRA 39 - Integración radio-alámbrica	El AN/GRA-39 se utiliza junto con un receptor-transmisor de radio para ampliar la capacidad de interfaz de la radio. Cuando se conecta con una radio, el AN/GRA-39 permite al operador transmitir y recibir comunicaciones de frecuencia de voz a través de la radio a una distancia de hasta dos millas (3,3 kilómetros) de la radio. Integración radio-alámbrica: Transmisión: Las señales de voz y la señal de 3.900 Hz son transmitidas a través del cable de campaña a la unidad de control local que controla la parte del transmisor del aparato de radio. Recepción: Las señales de audio del receptor de radio se devuelven al control remoto a través de la unidad de control local y cable de campaña.
	Manual Comunicaciones en Campaña (2007)	- Medios de comunicación militar	Características técnicas de los equipos de comunicación VHF, Radio PRC 730 y Radio PRC 930; equipos de comunicación HF, Radio PRC 2200, Radio PRC 6020 y Radio PRC 8020, cuentan con capacidades para transmitir en modo Seguro y Salto de Frecuencia.(PE)

	Video Introducción al Set de Control Remoto por radio GRA-39 Guerrillacomm (2011)	-Unidad de Control GRA 39 -Instalación de las estaciones remotas de radio.	Este equipo es un control remoto por radio, cuenta con una unidad local que va dentro del puesto de mando y en algún lugar a 3.5km de distancia va la estación de radio conectada con la unidad remota. En operaciones, no puedes posicionar tus equipos remotos en la cima de una montaña, debido a que podrían ser vulnerables a las operaciones de Guerra Electrónica enemigas, como su ubicación y destrucción, lo recomendable es colocarlo en la parte posterior a tus fuerzas para que tengas protección, si el enemigo descubre que estás transmitiendo desde la sima, encontrará tu señal y simplemente bombardeará esta área, lejos del centro de mando, esta ubicación es importante para que puedas mantener el centro de mando libre de acciones de Soporte y Ataque Electrónico.
	Informe de operaciones Informe (2014)	- Empleo de medios de comunicaciones disponibles. - Acciones de perturbación durante el ejercicio.	Recomendar sobre el mejor el empleo de medios disponibles como sistemas de radio y equipos de control remoto GRA 39, de manera de no ser objeto de acciones de GE de Negro. Durante las coordinaciones en Claro y posteriormente en Secreto con los centros de comunicaciones de las fuerzas, se pudieron apreciar perturbaciones de tipo zumbido en periodos regulares de 5 a 10 min. El día 21 de 0800hrs a 1400hrs se desarrolló el ejercicio en el terreno, el apoyo de comunicaciones fue a través del sistema monocanal HF Secreto, en donde no se pudieron determinar acciones efectivas de perturbación. Se debe de intensificar el entrenamiento sobre las acciones del operador de radio en caso éste sea perturbado (qué debe de hacer).

Nota. La matriz muestra el criterio lógico para organizar los temas, basándose en la categoría de Equipos remotos de comunicaciones y sus subcategorías, guardando relación con los manuales, informes de operaciones y videos.

Tabla 10

Organización del contenido del análisis documental- Operaciones de protección electrónica

Categorías	Material/ Documento Referencia	Temas	Contenido
Operaciones de Protección Electrónica	Publicación Electronic Warfare Techniques (2023)	- Protección Electrónica	Los equipos de comunicaciones electromagnéticas tienen funciones integradas que se utilizan para mitigar las amenazas, como el ataque electromagnético, soporte electromagnético.
		- Enmascaramiento electrónico (Masking Electromagnétic)	Para la planificación de protección electromagnética, el G-6 considera: Gestión del espectro, ... Enmascaramiento electromagnético, …. El enmascaramiento electromagnético es la radiación controlada de energía electromagnética sobre frecuencias amigas de manera que se protejan las emisiones de comunicaciones amigas y sistemas electrónicos contra medidas/señales de apoyo electromagnético del enemigo, sin degradar significativamente el funcionamiento de los sistemas amigos. El enmascaramiento electromagnético disfraza, distorsiona o manipula radiación de señales electromagnéticas amigables, para ocultar información crítica o presentar percepciones falsas de amenaza. El enmascaramiento electromagnético es un componente esencial del engaño militar, seguridad de operaciones y seguridad de señales.
	Manual de empleo Guerra Electrónica (2013)	- Acciones de Protección Electrónica	Las acciones de protección electrónica se clasifican en Anti-Soporte Electrónico y Anti-Ataque Electrónico.
		- Procedimientos operacionales de Protección Electrónica	Tanto para las acciones Anti-ES como Anti-EA, es necesario adoptar las siguientes acciones: 1) Gerenciamiento, …2) Recursos Técnicos, consiste en la utilización de los dispositivos de protección electrónica existentes en los sistemas de C2 que resguardan de las acciones de GE enemigas: Salto de frecuencia, Seguridad, …3) Procedimientos Operacionales,... Anti SE, a) entrenamiento del operador, despliegue de medios,… Anti AE, …Empleo de un puesto retransmisor, …
	Manual de empleo Planeamiento de Operaciones Terrestres (2015)	Sincronización	Implica organizar operaciones militares en el tiempo, el espacio y el propósito para garantizar la máxima efectividad del combate en el momento y lugar cruciales. Un aspecto clave en el planeamiento es la sincronización, que no es más que ordenar las acciones en tiempo, espacio y propósito, para generar el máximo esfuerzo o potencia de combate en el punto y tiempo decisivo. En el entrelazado de la maniobra, las relaciones horizontales son clave para la conciencia y la comprensión situacional; así como para la sincronización; Conops Fase I: Intención, …Sincronización (empleo operacional del tiempo: inicio y fin).

	Informe de operaciones Informe (2014)	- Tarea Cubierta Electrónica - Conclusiones del informe.	La tarea que se desarrolló en el día D (22 de Nov de 0800hrs a 1400hrs) consistió en emitir señales simultáneas en intervalos de 10 y 15 min, mediante dos (02) equipos de radio HF en SEC y Claro, así como en dos (02) equipos de radio VHF en SEC y AJ. Esta acción posiblemente haya causado mayor análisis de flujo, teniendo como resultado que las capacidades de Negro no hayan podido identificar la frecuencia de trabajo del Cte, por lo que no pudieron realizar acciones de Ataque Electrónico de perturbación. El empleo de equipos de radio que realicen emisiones falsas y cubran las emisiones reales, permiten distraer las capacidades de análisis de G Elect del Negro, dándonos mayor tiempo en mantener el Comando y Control de nuestras fuerzas.
	Publicación Análisis de las operaciones de Guerra Electrónica durante la Guerra de las Malvinas en el TOAS Vadell (2016)	-Procedimientos de operaciones -Protección Electrónica	En cuanto a las fuerzas armadas, es importante resaltar que la mayoría de las actividades propuestas son pasivas, pero otras innovadoras, como las utilizadas por los operadores de radares de la FAA en Puerto Rico, Argentina, son reveladoras. Acercarse cada vez. Se las arreglaron para evitar destruir el radar simplemente encendiéndolo y apagándolo unas cuantas veces mientras los aviones volaban hacia ellos. Específicamente, la confrontación requiere medidas de PE dirigidas a las capacidades de GE del enemigo para minimizar tales ataques, pero esto no se reflejó de manera efectiva o adecuada a lo largo de la campaña. En el caso del Reino Unido, casi todos los británicos que utilizan equipos de radio en todos los niveles cuentan con equipos de cifrado para garantizar comunicaciones seguras. Durante la planificación e implementación de la campaña TOAS, no se anticiparon objeciones al uso del espectro electromagnético y sus niveles de protección de conducción, desde el nivel operativo hasta el táctico.

Nota. La matriz muestra el criterio lógico para organizar los temas, basándose en la categoría de Operaciones de protección electrónica y sus subcategorías, guardando relación con los manuales, informes de operaciones y videos.

3.3 Definición de categorías

La codificación axial implica identificar las categorías más importantes (las más mencionadas) en el planteamiento del problema y agrupar categorías similares en temas. La codificación selectiva... implica esencialmente identificar categorías o temas principales que explican un fenómeno o problema. Hernández y Mendoza (2018).

Tabla 11

Agrupación de temas y patrones por categorías de la entrevista.

Categoría	Subcategorías	Temas agrupados	Patrones
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	Experiencia en el trabajo	Entrenamiento el Guerra C. Unidades de comunicaciones Nuevas propuestas
		Capacidades de Protección Electrónica	Perturbación e interferencia Vulnerabilidad electrónica
	Integración radio-alámbrica	Seguridad física y electrónica	Radiolocalización Sistemas de armas
		Operación remota de radios	Centro de comunicaciones Unidad de control remoto
	Designación de operadores de radio	Instrucción de GE	Conocimientos Capacitación
		Operación de estaciones	Unidad de control remoto Diversidad de operación Un operador de radio
Operaciones de protección electrónica	Sincronización de la propagación de ondas	Importancia	Modalidad de protección
		Señal real protegida	Radiación simultánea Desorientación
	Tipos de operaciones de Protección Electrónica	Enmascaramiento electrónico	Recursos técnicos Señal protegida
		Procedimientos operacionales	Instalación remota Radiación simultanea
	Contribución con el apoyo de comunicaciones	Mantener enlaces	Grandes unidades Innovación
		Nivel de eficiencia	Tecnología Capacidades de PE Riesgo Vulnerabilidad electrónica

Tabla 12

Codificación axial de la entrevista - Equipos remotos de comunicaciones

Categorías	Sub categoría	Texto codificado
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	1. Experiencia de haber trabajado en las unidades del Agrup Com “JO”, sobre todo en el Batallón de Comunicaciones N° 113, Compañía de Comunicaciones N° 8 y Compañía de Guerra Electrónica N° 113 y en haber participado en los entrenamientos para guerra convencional (GC). 2. Se tuvo perturbación o interferencia que afectaron los equipos de radio empleados por el centro de comunicaciones. 3. Es necesario contar con nuevas propuestas, iniciativas o procedimientos, optimizando el material de comunicaciones actual, debido a que no contamos con equipos adecuados de Protección Electrónica que puedan hacer frente al avance del Soporte Electrónico y Ataque Electrónico. 4. Los medios remotos de comunicaciones cuentan con capacidades de protección electrónica; sin embargo, estos siguen siendo vulnerables a las operaciones de guerra electrónica, no son suficientes para proteger las emisiones de radio ni la seguridad física del centro de comunicaciones y su personal.
	Integración radio-alámbrica	1. La finalidad es de proteger electrónica y físicamente las estaciones de radio que operan en el centro de comunicaciones. 2. Operar las estaciones de radio de los centros de comunicaciones de manera remota o a distancia por medio de las unidades de control remoto GRA 39. 3. Proporcionar y garantizar seguridad contra acciones de radiolocalización y posteriormente destrucción física por los sistemas de armas enemigos.
	Designación de operadores de radio	1. Son diferentes las funciones del operador de comunicaciones. Los operadores de radio a control remoto requieren habilidades, mayores capacitaciones y conocimientos de guerra electrónica en el despliegue táctico y de operar diversos sistemas a la vez. 2. No es lo mismo; un operador de radio de los equipos de control remoto, puede operar varias estaciones de radio en un mismo momento o de manera simultánea, empleando para las unidades de control remoto GRA 39, mientras que los operadores de radio de los centros de comunicaciones son designados individualmente para cada estación o control de red.

Tabla 13

Codificación axial de la entrevista- Operaciones de protección electrónica

Categorías	Sub categoría	Texto codificado
Operaciones de Protección Electrónica	Sincronización de la propagación de ondas	1. Es muy importante¸permite proteger nuestras operaciones es una nueva forma, herramienta y método de enmascarar electrónicamente la transmisión de las señales. 2. Emitir o radiar energía electrónica simultáneamente en tiempo y espacio con el centro de comunicaciones permite enmascarar o cubrir electrónicamente la fuente real o frecuencia protegida para apoyar y ejercer el comando y control. 3. Cubrir la señal real, provoca desorientación a los sistemas de guerra electrónica, así como incapacidad de identificar y localizar la correcta fuente electromagnéticas para ser perturbadas y destruidas.
	Tipos de operaciones de Protección Electrónica	1. El tipo de operaciones de PE, fue mediante el empleo de redes de engaño o redes fantasma. 2. La programación de los parámetros de seguridad en las estaciones de radio mediante la modalidad en modo secreto a través de tablas de seguridad y parámetros anti perturbación, así como el empleo de la IOC, códigos flash y mensajes preestablecidos. 3. Mediante un solo equipo de control remoto GRA 39, se emitieron radiaciones de energía electromagnética de manera simultánea y remota que son procedimientos operacionales del operador, así como la seguridad física del Cecom y su personal. 4. Una nueva acción Anti Soporte Electrónico y Anti Ataque Electrónico, fue el Enmascaramiento electrónico que permitió reducir las acciones de guerra electrónica, cubriendo la señal protegida evitando su interferencia, localización, análisis y perturbación que afecten el apoyo de comunicaciones.
	Contribución con el apoyo de comunicaciones	1. Fue muy buena porque puso a prueba el ingenio e innovación de los oficiales de comunicaciones, dado que se trabajó con equipos no tan sofisticados. 2. Cubrir las emisiones del centro de comunicaciones contribuyó a mantener los enlaces entre los puestos de comando de las grandes unidades durante el entrenamiento para operaciones de guerra convencional, manteniendo el apoyo de comunicaciones al comando y control. 3. No contar con capacidades de Protección Electrónica genera una vulnerabilidad crítica, siendo un riesgo crítico para el apoyo del comando y control de la fuerza durante las operaciones defensivas. Esto tendría como consecuencia una desventaja táctica y destrucción inminente de nuestra fuerza. 4. Teniendo en consideración el avance y desarrollo de nuevas tecnologías en operaciones de interceptación o perturbación de señales, los ejércitos modernos cuentan con capacidades operacionales eficientes. 5. Nosotros no contamos con capacidades de Protección Electrónica, lo que genera una brecha tecnológica desde hace 10 años, ni mucho menos con sistemas de comunicaciones integrados, por lo que nuestro nivel de eficiencia de Protección Electrónica es limitado y bajo.

Tabla 14

Codificación selectiva de la entrevista - sub categorías de Equipos remotos de comunicaciones

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. Experiencia de haber trabajado en las unidades del Agrup Com “JO”, sobre todo en el Batallón de Comunicaciones N° 113, Compañía de Comunicaciones N° 8 y Compañía de Guerra Electrónica N° 113 y participado en los entrenamientos para guerra convencional. 2. Se tuvo perturbación o interferencia que afectaron los equipos de radio empleados por el centro de comunicaciones. 3. Es necesario contar con nuevas propuestas, iniciativas o procedimientos, optimizando el material de comunicaciones actual, debido a que no contamos con equipos adecuados de Protección Electrónica que puedan hacer frente al avance del Soporte Electrónico y Ataque Electrónico. 4. Los medios remotos de comunicaciones cuentan con capacidades de Protección Electrónica; sin embargo, estos siguen siendo vulnerables a las operaciones de guerra electrónica; no son suficientes para proteger las emisiones de radio ni la seguridad física del centro de comunicaciones y su personal.	**Capacidad operativa de comunicaciones** Experiencia en el trabajo. - Entrenamiento en GC. - UU de comunicaciones. - Nuevas propuestas Capacidades de PE - Vulnerabilidad electrónica - Perturbación e interferencia	Las experiencias en los entrenamientos para guerra convencional visualizaron que el empleo de radios con capacidades de PE son vulnerables a la perturbación electrónica, por lo que se requiere de nuevas propuestas de empleo del material de comunicaciones.	Las experiencias en los entrenamientos para GC visualizaron que el empleo de radios con capacidades de PE son vulnerables a la perturbación electrónica, por lo que se requiere de nuevas propuestas de empleo del material que reduzcan esta vulnerabilidad. Por ende, designar a un operador de radio instruido en GE para operar las radios de manera remota y diversa incrementa la protección física y electrónica del Centro de Comunicaciones contra la localización, perturbación y posible destrucción por las armas enemigas.
1. La finalidad es proteger electrónica y físicamente las estaciones de radio que operan en el centro de comunicaciones, garantizando la seguridad contra acciones de radiolocalización y posteriormente destrucción física por los sistemas de armas enemigos. 2. Operar las estaciones de radio de manera remota o a distancia por medio de las unidades de control remoto GRA 39 para proteger los centros de comunicaciones.	**Integración radio-alámbrica** Seguridad física y electrónica. - Radiolocalización - Sistema de armas Operación remota de radios - Centro de comunicaciones - Unidad de control remoto	La seguridad física y electrónica del centro de comunicaciones se obtiene mediante la operación remota de las estaciones de radio.	
1. Son diferentes las funciones del operador de comunicaciones; los operadores de radio a control remoto requieren habilidades, mayores capacitaciones y conocimientos de guerra electrónica en el despliegue táctico y para operar diversos sistemas a la vez. 2. No es lo mismo: un operador de radio de los equipos de control remoto puede operar varias estaciones de radio en un mismo momento, empleando las unidades de control remoto GRA 39, mientras que los operadores de radio del centro de comunicaciones son designados individualmente para cada estación o control de red.	**Designación de operadores de radio** Instrucción de GE - Conocimiento - Capacitación Un operador de radio - Operación de las estaciones - Unidad de control remoto - Diversidad de operación	Un operador de radio requiere de mayor instrucción, conocimiento y capacitación para realizar diversos tipos de operaciones de las estaciones de radio de manera remota y simultánea.	

Tabla 15

Codificación selectiva de la entrevista- sub categorías de Operaciones de protección electrónica

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. Es muy importante; permite proteger nuestras operaciones; es una nueva forma, herramienta y método de enmascarar electrónicamente la transmisión de las señales. 2. Emitir o radiar energía electrónica simultáneamente en tiempo y espacio con el centro de comunicaciones permite enmascarar o cubrir electrónicamente la fuente real o frecuencia protegida para apoyar y ejercer el comando y control. 3. Cubrir la señal real provoca desorientación a los sistemas de guerra electrónica, así como incapacidad de identificar y localizar la correcta fuente electromagnética para ser perturbadas y destruidas.	**Sincronización de la propagación de ondas** Importancia - Modalidad de protección Señal protegida - Radiación simultánea - Desorientación al SE y AE	La importancia de establecer la sincronización como una nueva modalidad de radiación de la energía de manera simultánea con el Cecom permite cubrir la señal protegida, causando desorientación a la localización y perturbación enemiga.	La importancia de establecer la sincronización como una nueva modalidad de radiación accedió a identificar al Enmascaramiento electrónico como un tipo de operación de PE para la señal del centro de comunicaciones, causando desorientación a las capacidades de localización y perturbación enemigas. Esta innovación permitió mantener los enlaces entre las grandes unidades; sin embargo, nuestro nivel de PE es muy limitado por el avance de la tecnología. No implementarlo o incrementarlo generaría una vulnerabilidad, siendo un riesgo crítico que afectaría el apoyo de comunicaciones a las operaciones en guerra convencional.
1. El tipo de operaciones de PE fue mediante el empleo de redes de engaño o redes fantasma. 2. La programación de los parámetros de seguridad antiperturbación y Anti SE en las estaciones de radio fue mediante la modalidad de secreto, así como empleo de códigos flash y mensajes preestablecidos. 3. Mediante un solo equipo de Control Remoto GRA 39, se emitieron radiaciones de energía electromagnética de manera simultánea y remota. Estas actividades son procedimientos operacionales del operador, así como la seguridad física del Cecom y su personal. 4. Una nueva acción contra el SE y AE fue el Enmascaramiento Electrónico, que permitió reducir las acciones de GE, cubriendo la señal protegida evitando su interferencia, localización y perturbación que afecten el apoyo de comunicaciones.	**Tipos de operaciones de Protección Electrónica** Enmascaramiento Electrónico -Parámetros de Seguridad - Señal protegida. Procedimientos operacionales - Instalación remota - Radiación simultánea	El empleo de los parámetros de seguridad y procedimientos operacionales para una instalación remota con radiaciones simultáneas permitió identificar un enmascaramiento electrónico para la señal protegida.	
1. Fue muy buena porque puso a prueba el ingenio e innovación de los oficiales de Com dado que se trabajó con equipos no tan sofisticados. 2. Cubrir las emisiones del Cecom contribuyó a mantener los enlaces entre los puestos de comando de las grandes unidades durante el entrenamiento para operaciones de guerra convencional, manteniendo el apoyo de comunicaciones al comando y control. 3. No contar con capacidades de PE genera una vulnerabilidad crítica, siendo un riesgo crítico para apoyo del comando y control de la fuerza durante las operaciones defensivas, esto tendría como consecuencia una desventaja táctica y destrucción inminente de nuestra fuerza. 4. Teniendo en consideración el avance y desarrollo de nuevas tecnologías en operaciones de interceptación o perturbación de señales, los ejércitos modernos cuentan con capacidades operacionales eficientes. 5. Nosotros no contamos con capacidades de PE, lo que genera una brecha tecnológica desde hace tiempo, por lo que nuestro nivel de eficiencia de PE es limitado y bajo.	**Contribución con el apoyo de comunicaciones** Mantener enlaces - Grandes unidades. - Innovación Nivel de eficiencia - Capacidades de PE - Tecnología - Riesgo crítico - Vulnerabilidad electrónica	Mantener los enlaces entre las grandes unidades se debió a la innovación; sin embargo, el nivel de eficiencia de las capacidades de PE por el avance de la tecnología es muy limitado; no aumentarlo generaría una vulnerabilidad, siendo un riesgo crítico que afectaría el apoyo de comunicaciones a las operaciones en guerra convencional.	

Tabla 16

Agrupación de temas y patrones por categorías de la observación.

Categorías	Subcategorías	Temas agrupados	Patrones
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	Nuevo procedimiento	Instalación remota Integración del GRA 39 y 08 estaciones de radio. Operatividad
		Señal simultánea	Programación Recursos Técnicos Recepción de la señal
	Integración radio-alámbrica	Estaciones radio	Enlace remoto Procedimiento operacional Seguridad física y electrónica
	Designación de operadores de radio	Un operador de radio	Instrucción de GE
Operaciones de protección electrónica	Sincronización de la propagación de ondas	Entrenamiento con el Centro de comunicaciones	Emisiones de ondas simultaneas Estaciones de radio
	Tipos de operaciones de Protección Electrónica	Enmascaramiento electrónico	Recursos Técnicos
	Contribución con el apoyo de comunicaciones	Mantener enlaces	Ejercicio de Comunicaciones Interferencia Centro de Comunicaciones

Tabla 17

Codificación axial la observación-Operaciones de protección electrónica

Categorías	Sub categoría	Texto codificado
Operaciones de Protección Electrónica	Sincronización de la propagación de ondas	1. Existe sincronización de las emisiones de ondas de la estación de protección con las emisiones de ondas del centro de comunicaciones. 2. El entrenamiento de los operadores contribuye a lograr que la sincronización sea efectiva en un mismo momento y espacio.
	Tipos de operaciones de Protección Electrónica	Se observó que la operación de Protección Electrónica fue del tipo Enmascaramiento electrónico, que incluye acciones anti soporte y ataque electrónico (perturbación).
	Contribución con el apoyo de comunicaciones	Las señales de radio entre los centros de comunicaciones del Agrup Com y III División de Ejército se mantuvieron fluidas durante todo el ejercicio, no hubo perturbación e interferencia.

Tabla 18

Codificación axial de la observación- Equipos remotos de comunicaciones

Categorías	Sub categoría	Texto codificado
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	1. Se probaron la operatividad de las radios y unidades de control remoto; posteriormente se programaron las radios con diferentes modalidades de emisión, en especial secreto y salto de frecuencia. 2. El procedimiento es nuevo, porque se procedió con la instalación de una unidad de control local del GRA 39, a esta se conectaron 08 líneas de cable de campaña; cada línea se conecta a una unidad de control remoto del GRA 39 y estas unidades posteriormente se integran a las 08 estaciones de radio. 3. De manera de probar la integración radioalámbrica, se instalan los equipos a diferentes distancias, entre 200 y 500 m aproximadamente. 4. Se verificó el funcionamiento de la estación del centro de comunicaciones con el Cuartel General de la III División de Ejército y el funcionamiento de las estaciones remotas y de manera simultánea, comprobando la recepción de sus emisiones por 02 radios programadas con los mismos parámetros y gama de frecuencia.
	Integración radio-alámbrica	Los operadores de radio designados conocen la finalidad del emplear las estaciones a distancia, como un procedimiento operacional de PE que da seguridad física y electrónica.
	Designación de operadores de radio	Solo fue necesario un operador de radio con instrucción y capacitación de guerra electrónica para el empleo remoto y simultáneo de las 8 estaciones de radio.

Tabla 19

Codificación selectiva de la observación de las subcategorías - Equipos remotos de comunicaciones

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. Se probaron la operatividad de las radios y unidades de control remoto, posteriormente se programaron las radios con diferentes modalidades de emisión, en especial secreto y salto de frecuencia. 2. Nuevo procedimiento porque se procedió con la instalación de una unidad de Control Local del GRA 39, a esta se conectaron 08 líneas de cable de campaña, cada línea se conecta a una unidad de control remoto del GRA 39 y estas unidades posteriormente se integran a las 08 estaciones de radio. 3. De manera de probar la integración radioalámbrica, se instalaron los equipos en diferentes distancias, entre 200 y 500 m aproximadamente. 4. Se verificó el funcionamiento de la estación del Cecom con el Cuartel General de la III División de Ejército y el funcionamiento de las estaciones remotas con sus emisiones de manera simultánea, comprobando la recepción de sus emisiones por 02 radios programadas con los mismos parámetros y gama de frecuencia.	**Capacidad operativa de comunicaciones** Nuevo procedimiento - Instalación remota - Integración del GRA 39 y 08 estaciones de radio. - Operatividad Señal simultánea - Recepción de señal. - Recursos Técnicos - Programación	El nuevo procedimiento de integración del equipo GRA 39 con las 08 estaciones de radio y su instalación remota a diferentes distancias implica la verificación de la operatividad, emisión simultánea y recepción de la señal de las diversas estaciones de radio con su adecuada programación de recursos técnicos.	El nuevo procedimiento de integración del equipo GRA 39 con las 08 estaciones de radio y su instalación remota a diferentes distancias, por medio del cable de campaña, requiere de un operador de radio capacitado en guerra electrónica, para la verificación de la operatividad, emisión y recepción de la señal simultánea de diversas estaciones de radio con su adecuada programación de recursos técnicos, con el propósito de proporcionar seguridad física y electrónica al centro de comunicaciones.
Los operadores de radio designados conocen la finalidad del emplear las estaciones a distancia, como un procedimiento operacional de PE que da seguridad física y electrónica.	**Integración radio-alámbrica** Estaciones de radio - Enlace remoto - Procedimiento operacional - Seguridad física y electrónica	Emplear las estaciones mediante un enlace remoto es un procedimiento operacional que da seguridad física y electrónica.	
Solo fue necesario un operador de radio con instrucción y capacitación de Guerra Electrónica para el empleo remoto y simultánea de las 8 estaciones de radio.	**Designación de operadores de radio** Un operador de radio - Instrucción de GE	La operación de las estaciones de radio la realizó un solo operador de radio capacitado en guerra electrónica.	

Tabla 20

Codificación selectiva de la observación de las subcategorías – Operaciones de protección electrónica

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. Existe sincronización de las emisiones de ondas de la estación de protección con las emisiones de ondas del centro de comunicaciones. 2. El entrenamiento de los operadores contribuye a lograr que la sincronización sea efectiva en un mismo momento y espacio.	**Sincronización de la propagación de ondas** Entrenamiento con el Cecom. - Emisiones de ondas	El entrenamiento contribuye a la sincronización de las emisiones de ondas con las del centro de comunicaciones.	El entrenamiento en los ejercicios de comunicaciones contribuye a que las estaciones de radio puedan emitir sus ondas seguras de forma simultánea con las del Centro de comunicaciones, generando un enmascaramiento electrónico de la señal protegida, reduciendo la interferencia o perturbación y contribuyendo a mantener los enlaces de los centros de comunicaciones.
Se observó que la operación de Protección Electrónica fue del tipo Enmascaramiento Electrónico, que incluye acciones anti-soporte y ataque electrónico (perturbación).	**Tipos de operaciones de Protección Electrónica** Enmascaramiento electrónico. - Parámetros de seguridad	El enmascaramiento electrónico es un tipo de operación de Protección Electrónica de la señal verdadera que incluye el uso de parámetros de seguridad.	
Las señales de radio entre los centros de comunicaciones del Agrup Com y III División de Ejército se mantuvieron fluidas durante todo el ejercicio, no hubo perturbación e interferencia.	**Contribución con el apoyo de comunicaciones** Mantener enlaces. - Ejercicio de comunicaciones - Interferencia y Perturbación - Centro de comunicaciones	Durante el ejercicio se mantienen los enlaces entre los centros de comunicaciones, sin acciones de perturbación e interferencia.	

Tabla 21

Agrupación de temas y patrones por categorías del Análisis documental y material.

Categorías	Subcategorías	Temas agrupados	Patrones
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	Integración	Distancia
		Ejercicios de comunicaciones	Recursos Técnicos Perturbación
	Integración radio-alámbrica	Despliegue	Estaciones de radio Instalación remota
		Operación remota	Acciones de GE
	Designación de operadores de radio	Entrenamiento	Operador de radio Perturbación
Operaciones de protección electrónica	Sincronización de la propagación	Planeamiento	Máxima potencia Coordinaciones Tiempo decisivo
	Tipos de operaciones de Protección Electrónica	Enmascaramiento electrónico	Recursos Técnicos Seguridad electrónica
		Disfrazar y distorsionar	Radicaciones Señal real protegida
	Contribución con el apoyo de comunicaciones	Ejercicio de comunicaciones	Distracción Mantener los enlaces Perturbación
		Innovación	Proteger Desventaja

Tabla 22

Codificación axial del análisis documental - Equipos remotos de comunicaciones

Categorías	Sub categoría	Texto codificado
Equipos remotos de comunicaciones	Capacidad operativa de comunicaciones	1. El equipo GRA 39, permite al operador de comunicaciones transmitir y recibir comunicaciones a través de la radio a distancia por medio del cable de campaña. 2. Todas las radios empleadas cuentan con capacidades de transmisión en modo Seguro y Salto de Frecuencia. 3. Durante las coordinaciones y el ejercicio en el terreno, se pudieron determinar acciones efectivas de perturbación.
	Integración radio-alámbrica	1. En operaciones, lo recomendable es operar los equipos remotos en la parte posterior a tus fuerzas para que tengan protección. 2. La ubicación de la estación remota es importante para mantener el Centro de Mando libre de acciones de Soporte y Ataque Electrónico. 3. Hacer un mejor empleo de los medios remotos disponibles de manera de no ser objeto de acciones de guerra electrónica enemigas. 4. Procedimientos de operaciones para acciones de Anti-Soporte Electrónico se tiene el despliegue de medios y para acciones de Anti-Ataque Electrónico, se incluye el empleo de un puesto retransmisor.
	Designación de operadores de radio	1. Intensificar el entrenamiento sobre las acciones del operador de radio en caso de que sea perturbado. 2. Procedimientos operacionales dentro de las acciones de Anti-Soporte Electrónico, se encuentra incluido el entrenamiento del operador.

Tabla 23

Codificación axial del análisis documental- Operaciones de protección electrónica

Categorías	Sub categoría	Texto codificado
Operaciones de Protección Electrónica	Sincronización de la propagación de ondas	1. Disposición de las operaciones militares en el tiempo, el espacio y el objetivo para maximizar la efectividad del combate en el momento y lugar cruciales. 2. Un aspecto clave en el concepto de las operaciones y el planeamiento es la sincronización, para generar el máximo esfuerzo o potencia de combate en el punto y tiempo decisivo. 3. En el entrelazado de la maniobra, las relaciones horizontales son clave para la conciencia y la comprensión situacional; así como para la sincronización.
	Tipos de operaciones de Protección Electrónica	1. El enmascaramiento electromagnético es la radiación controlada de energía electromagnética sobre frecuencias amigas, de manera que se protejan las emisiones de comunicaciones amigas. 2. Para la planificación de protección electromagnética, el G-6 (Oficial de telemática) considera: Gestión del espectro del enmascaramiento electromagnético. 3. El enmascaramiento electromagnético disfraza, distorsiona o manipula radiación de señales electromagnéticas amigables, para ocultar información crítica o presentar percepciones falsas de amenaza. 4. Tanto para las acciones Anti-ES como Anti-EA es necesario adoptar el empleo de los recursos técnicos, que consiste en la utilización de los dispositivos de PE existentes en los sistemas de comando y control como el modo Seguro y Santo de frecuencia.
	Contribución con el apoyo de comunicaciones	1. La tarea que se desarrolló consistió en emitir señales simultáneas en intervalos mediante cuatro equipos de radio de alta frecuencia (HF) y muy alta frecuencia (VHF) en Secreto y Claro. 2. El empleo de equipos de radio con emisiones falsas que cubran las emisiones reales, permite distraer las capacidades de análisis de guerra electrónica de Negro, dándonos mayor tiempo para mantener el comando y control de nuestras fuerzas. 3. Esta acción posiblemente haya causado mayor análisis de flujo, contribuyendo a que las capacidades de Negro no hayan podido identificar la frecuencia de trabajo del Componente Terrestre y no poder realizar acciones de Ataque Electrónico de perturbación. 4. Es importante destacar que algunas acciones planteadas fueron innovadoras, como las que empleaba el personal de operadores del radar en Puerto Argentino. De esta manera consiguieron exitosamente evitar su destrucción. 5. Planear el empleo y la protección del medio electromagnético contribuye a usar acciones de PE, lo que da una ventaja bélica a diferencia de no planearlas y emplearlas, reflejándose durante una confrontación, en donde una fuerza está destinada a ser dominada en todos los niveles de la conducción de una guerra.

Tabla 24

Codificación selectiva del análisis documental-Equipos remotos de comunicaciones

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. El equipo de control remoto GRA 39, permite al operador de comunicaciones transmitir y recibir comunicaciones a través de la radio a distancia por medio del cable de campaña. 2. Todas las radios empleadas cuentan con capacidades de transmisión en modo seguro y salto de frecuencia 3. Durante las coordinaciones y el ejercicio en el terreno, se pudieron determinar acciones efectivas de perturbación.	**Capacidad operativa de comunicaciones** Integración - Distancia Ejercicio de comunicaciones - Recursos técnicos - Perturbación	En el ejercicio de comunicaciones se determinaron acciones de perturbación a radios programadas con recursos técnicos, por lo que tuvieron que ser integradas al Equipo Remoto GRA 39 y operar a distancia.	El entrenamiento del operador de radio en los ejercicios de comunicaciones contribuye en la integración de los medios de comunicaciones con los recursos técnicos programados, accediendo a un adecuado despliegue e instalación a distancia, lo que permite proporcionar seguridad y protección al Centro de Comunicaciones de acciones de guerra electrónica enemigas.
1. En operaciones, lo recomendable es operar los equipos remotos en la parte posterior a tus fuerzas para que tengan protección. 2. La ubicación de la estación remota es importante para mantener el Centro de Mando libre de acciones de Soporte y Ataque Electrónico. 3. Hacer un mejor empleo de los medios remotos disponibles de manera de no ser objeto de acciones de guerra electrónica enemigas. 4. Dentro de los procedimientos operacionales para acciones de Anti Soporte Electrónico se tiene el despliegue de medios y para acciones de Anti Ataque Electrónico se incluye el empleo de un puesto retransmisor.	**Integración radio-alámbrica** Despliegue - Estaciones de radio - Instalación remota Operación remota - Acciones de GE	Un adecuado despliegue e instalación remota de las estaciones de radio bien ubicadas permite una operación remota que proporciona seguridad para el Cecom contra acciones de guerra electrónica.	
1. Intensificar el entrenamiento sobre las acciones del operador de radio, en caso sea perturbado. **2.** Los procedimientos operacionales dentro las acciones de Anti Soporte Electrónico, se encuentra incluido el entrenamiento del operador.	**Designación de operadores de radio** Entrenamiento - Operador de radio - Perturbación	El operador de radio requiere de entrenamiento para hacer frente a acciones de perturbación.	

Tabla 25

Codificación selectiva del análisis documental- Operaciones de protección electrónica

Texto codificado	Sub categoría	Categoría emergente	Síntesis integral
1. Disposición de las operaciones militares en el tiempo, el espacio y el objetivo para maximizar la efectividad del combate en el momento y lugar cruciales. 2. Un aspecto clave en el concepto de las operaciones y el planeamiento es la sincronización, para generar el máximo esfuerzo o potencia de combate en el punto y tiempo decisivo. 3. En el entrelazado de la maniobra, las relaciones horizontales son clave para la conciencia y la comprensión situacional; así como para la sincronización.	**Sincronización de la propagación de ondas** Planeamiento - Máxima potencia. - Coordinaciones - Tiempo decisivo	En el planeamiento, la coordinación es clave para la sincronización, y generar la máxima potencia en un momento decisivo..	La innovación permite obtener nuevas operaciones de PE, como el enmascaramiento electrónico, que a través de la coordinación de las emisiones con el centro de comunicaciones, ejerce una máxima potencia electromagnética en un tiempo decisivo, disfrazando y distorsionando las radiaciones amigas, para ocultar la información, distrayendo y limitando las acciones de SE y AE enemigos, como la perturbación, y limitar así estas desventajas durante las operaciones militares, a fin de contribuir en mantener los enlaces y proteger el comando y control.
1. El enmascaramiento electromagnético es la radiación controlada de energía electromagnética sobre frecuencias amigas de manera que se protejan las emisiones de comunicaciones amigas. 2. Para la planificación de protección electromagnética, el G-6 (oficial de telemática) considera: Gestión del espectro. Enmascaramiento electromagnético. 3. El enmascaramiento electromagnético disfraza, distorsiona o manipula radiación de señales electromagnéticas amigables, para ocultar información crítica o presentar percepciones falsas de amenaza. 4. Para todas las acciones Anti-ES y Anti-EA es necesario adoptar el empleo de los recursos técnicos (Seguro y Salto de Frecuencia), que consiste en la utilización de los dispositivos de PE existentes en los sistemas de comando y control.	**Tipos de operaciones de Protección Electrónica** Enmascaramiento electrónico. - Recursos Técnicos - Seguridad Disfrazar y distorsionar - Radiaciones - Señal protegida	El Enmascaramiento electrónico adopta recursos técnicos para la seguridad de las comunicaciones disfrazando y distorsionando radiaciones amigas para ocultar información a las acciones de SE y AE.	
1. La tarea que se desarrolló consistió en emitir señales simultáneas en intervalos, mediante cuatro equipos de radio HF y VHF en Secreto y Claro. 2. El empleo de equipos de radio con emisiones falsas que cubran las emisiones reales, permite distraer las capacidades de análisis de GE de Negro, dándonos mayor tiempo en mantener el comando y control de nuestras fuerzas. 3. Esta acción posiblemente haya causado mayor análisis de flujo, contribuyendo a que las capacidades de Negro no hayan podido identificar la frecuencia de trabajo del Componente Terrestre y no poder realizar acciones de Ataque Electrónico de perturbación. 4. Es importante destacar que algunas acciones planteadas fueron innovadoras, como las que empleaba el personal de operadores del radar en Puerto Argentino. De esta manera consiguieron exitosamente evitar su destrucción. 5. Planear el empleo y la protección del medio electromagnético contribuye a usar acciones de PE, lo que da una ventaja bélica a diferencia de no planearlas y emplearlas, en donde una fuerza está destinada a ser dominada en todos los niveles de la conducción de una guerra.	**Contribución con el apoyo de comunicaciones** Ejercicio e comunicaciones - Distracción - Mantener enlaces - Perturbación Innovación - Proteger - Desventaja	La innovación permite proteger nuestras emisiones y distraer las capacidades de GE enemigas, de manera de limitar las desventajas como la perturbación durante el ejercicio de comunicaciones, contribuyendo a mantener los enlaces y proteger el comando y control.	

3.4 Soporte de categorías

Tabla 26

Matris de soporte de patrones.

Categorías	Sub categorías	Patrones	Descripción
Equipos remotos de Comunicaciones	Capacidad operativa de comunicaciones	Experiencia en el trabajo	Son los diferentes eventos en relación con el conocimiento práctico relacionado con el planeamiento, entrenamiento y ejecución del empleo de comunicaciones y GE en las unidades de comunicaciones y guerra electrónica.
		Entrenamiento en GC	Es el empleo táctico de las diferentes unidades de comunicaciones y guerra electrónica en apoyo a las unidades de maniobra en operaciones militares para guerra convencional.
		UU de comunicaciones	Son las diferentes compañías y batallones de comunicaciones y compañía de guerra electrónica, orgánicos del Agrupamiento de Comunicaciones José Olaya.
		Nuevas propuestas	Son las nuevas ideas e iniciativas de empleo del material de comunicaciones que se pueden ofrecer para mejorar e incrementar las capacidades de Protección Electrónica.
		Nuevo procedimiento	Es el procedimiento inédito de interconexión e integración de los equipos remotos de comunicaciones.
		Vulnerabilidad	Es la fragilidad o incapacidad de resistencia de los medios de comunicaciones con recursos técnicos a las diferentes amenazas de las operaciones de Ataque Electrónico y Soporte Electrónico.
		Perturbación	Es el uso de la energía electromagnética deliberada y planeada por parte de medios enemigos de Ataque Electrónicos no destructivos, con la finalidad de degradar o neutralizar las comunicaciones de los centros de comunicaciones.
		Capacidades de Protección Electrónica	Son los medios, personal y procedimientos que se emplean por parte de nuestras unidades de comunicaciones para reducir, negar e impedir acciones de Soporte Electrónico y acciones de Ataque Electrónico enemigas.
		Operatividad	Es la capacidad de funcionamiento de los equipos de comunicaciones de manera de ser utilizados por los operadores de comunicaciones y guerra electrónica.
		Integración	Es la interconexión de los equipos de radio a través del cable de campaña y cable de integración con los medios de Control Remoto del GRA 39, de manera de ser operados como un solo sistema.
		Programación	Es la introducción de diferentes datos en los equipos de radio en relación con sus características técnicas y recursos técnicos propios, de manera de emitir señales de radio en modo Seguro y Salto de Frecuencia, así como potencia de salida, etc.
		Distancia	Es la instalación de las estaciones de radio en diversos espacios o separaciones del centro de comunicaciones o de la estación de protección.
		Recursos técnicos	Son los diferentes parámetros (Secreto y Salto de Frecuencia) de seguridad que cuenta cada equipo de radio, de modo tal que la señal electromagnética limite las acciones de SE y AE enemigo.

	Integración radio-alambrica	Seguridad física y Electrónica.	Es la certeza o el convencimiento de que los centros de comunicaciones no sean objetos de ataques por los sistemas de armas, Fuerzas Especiales o Aviación, así como por acciones de SE y AE enemigos.
		Radiolocalización	Es una acción de Soporte Electrónico que consiste en la ubicación física de la estación de radio por donde se emiten las comunicaciones.
		Sistemas de armas	Son los sistemas que, mediante el uso de la información proporcionada por los medios de Soporte Electrónico tienen la capacidad de atacar objetivos (Centros de Comunicaciones) para destruirlos.
		Centro de Comunicación	Instalación responsable del recibimiento y transmisión de mensajes. Generalmente incorpora personal y medios para su funcionamiento.
		Operación remota de radios	Es la operación de las diferentes estaciones radio de manera remota a distancias distintas para la emisión de ondas simultáneas, para lo cual se requiere una unidad de control remoto GRA 39.
		UU de control remoto	Medio de comunicación denominado GRA 39 que, integrado por medio del cable de campaña con varias estaciones de radio, permite la transmisión a distancia del centro de comunicaciones.
		Estaciones de radio	Equipos de comunicaciones radiales de diferentes características técnicas que son integrados a la unidad de Control Remoto GRA 39.
		Recepción de señal	Es la comprobación de la señal electromagnética emitida simultáneamente por la operación remota de las estaciones de radio.
		Emisión simultánea	Es la radiación de ondas electromagnéticas de manera simultánea por diversas estaciones de radio, integradas y operadas a control remoto.
		Despliegue	Es el planeamiento, desplazamiento e instalación de los medios de comunicaciones remotos.
	Designación de operadores de radio	Instrucción de Guerra Electrónica	Es la formación del personal de operadores de radio en temas relacionados con comunicaciones y protección electrónica de manera de generar el conocimiento de los mismos.
		Conocimientos	Es la capacidad de observar, identificar y analizar la información obtenida de Protección Electrónica y de comunicaciones de manera de poder emplearla en los entrenamientos para Guerra Convencional.
		Capacitación	Es el conocimiento de temas específicos de Protección Electrónica que requieren los operadores de radio para poder operar las estaciones de radio de manera remota.
		Operación de estaciones	Es el empleo de los equipos de comunicaciones radiales de diferentes características técnicas.

		Diversidad de operación	Diferencia en la operación de una estación de radio de un centro de comunicaciones con la operación de diversas estaciones de radio de manera simultánea y remota desde una estación de protección.
		Un operador de radio	Es el único personal militar designado que es especialista en el manejo, programación y operación de los equipos de radio, con conocimientos de acciones de Protección Electrónica.
		Entrenamiento	Es la aplicación de la instrucción de la operación de los equipos de radio y unidad de control remoto para ser empleados en los ejercicios de comunicaciones y cubierta electrónica.
Operaciones de Protección Electrónica	Sincronización de las emisiones de ondas	Importancia	Es la trascendencia de las emisiones electromagnéticas de manera remota, al transmitirse al mismo tiempo con las emisiones del centro de comunicaciones.
		Modalidad de protección	Es la nueva manera o forma de proteger las emisiones electromagnéticas como consecuencia de la transmisión simultánea por diferentes equipos de radio.
		Señal protegida	Es la señal de radio del centro de comunicaciones, la cual está protegida de la radiolocalización y/o perturbación por el empleo remoto de las estaciones de radio.
		Radiación de ondas simultánea	Son las emisiones de onda que se emiten al mismo tiempo por las diferentes estaciones de radio operadas de manera remota.
		Desorientación	Es la confusión en los analistas de guerra electrónica enemigos, para la radiolocalización o perturbación de la señal protegida como consecuencia de las emisiones de ondas de radio simultáneas.
		Entrenamiento con el Cecom	Es el empleo constante de los equipos de radio de manera remota con los del Cecom, de manera que la capacidad de sincronización de las emisiones cumpla su propósito.
		Estaciones de radio	Son los diferentes equipos de radio desplegados e instalados a diferentes distancias y que se encuentran funcionando de manera remota y simultánea.
		Planeamiento	Es la consideración de importancia de la sincronización en las diferentes fases del concepto de las operaciones.
		Máxima potencia	Es la cantidad de emisiones de energía electromagnética emitidas en un mismo momento para causar confusión en las estaciones de guerra electrónica enemigas.
		Coordinaciones	Son las diversas actividades que se realizan con el centro de comunicaciones, para que sus emisiones de radio salgan de manera simultánea con las estaciones de radio remotas.
		Tiempo decisivo	Momento determinado para radiación de energía electromagnética, con el propósito de causar desorientación a las estaciones de guerra electrónica enemigas.

	Tipos de operaciones de Protección Electrónica.	Enmascaramiento electrónico	Es la radiación controlada de energía electromagnética sobre frecuencias amigables de manera que serán protegidas, con la finalidad de disfrazar o distorsionar la radiación de señales amigables, para ocultar información crítica.
		Recursos técnicos	Son los diferentes parámetros (Secreto y Salto de Frecuencia) de seguridad con que cuenta cada equipo de radio, de manera que la emisión electromagnética limite las acciones de SE y AE enemigos.
		Procedimientos operacionales	Son las diferentes formas de empleo (Despliegue, Instalación, Programación, etc.) de los equipos de radio a través de los operadores de radio, para evitar acciones de guerra electrónica.
		Radiación de ondas simultánea	Son las emisiones de onda que se emiten al mismo tiempo por las diferentes estaciones de radio operadas de manera remota.
		Instalación remota	Es el despliegue e instalación de las estaciones de radio a diferentes distancias entre estaciones y estas con la unidad de control remoto.
		Disfrazar y distorsionar	Camuflar y desnaturalizar la señal protegida del Cecom por medio del enmascaramiento electrónico de las señales de radio, para que no sea identificada por los sistemas de guerra electrónica enemigos.
		Señal real protegida	Es la señal de radio del Centro de Comunicaciones, la cual es protegida para ocultar su información de la radiolocalización y/o perturbación por el empleo remoto de las estaciones de radio.
	Contribución con el apoyo de comunicaciones	Mantener enlaces	Capacidad de dar continuidad a las comunicaciones realizadas por el Cecom, ante acciones de Ataque Electrónico enemigo.
		Grandes unidades	Son las brigadas y agrupamientos bajo el comando y control de la División de Ejército que participan en los entrenamientos para guerra convencional.
		Innovación	Es la aplicación de nuevas prácticas en el empleo del material de comunicaciones disponible en la institución con la finalidad de incrementar la capacidad de PE.
		Nivel de eficiencia	Es la capacidad de eficiencia de los medios de PE de los sistemas de comunicaciones ante las capacidades de AE y SE enemigos.
		Tecnología	Es el avance y el desarrollo de nuevos procesos en operaciones de interceptación y perturbación de señales los que minimizan la tecnología actual de nuestros sistemas de comunicaciones en PE.
		Capacidades de PE	Son los medios, personal y procedimientos que se emplean por las unidades de comunicaciones para reducir, negar, impedir acciones de SE y acciones de AE enemigos.
		Ejercicios	Entrenamiento y empleo del material de comunicaciones para guerra convencional.
		Distracción	Es la desviación de la atención de las acciones de SE y AE enemigos a las emisiones de las estaciones remotas, dándonos mayor tiempo en mantener el comando y control de la fuerza.
		Riesgo crítico	Es la probabilidad crítica de que se materialice la neutralización del apoyo de comunicaciones al comando y control en las operaciones.
		Interferencias	Es la intromisión de las comunicaciones del Cecom por medios de acciones de ataque electrónico.
		Vulnerabilidad	Es la fragilidad o incapacidad de resistencia de los medios de comunicaciones con recursos técnicos a las diferentes amenazas de las operaciones de Ataque Electrónico y Soporte Electrónico.

Tabla 27

Soporte de categoría- Equipo remotos de comunicaciones

Categoría	Guía de Entrevista	Guía de Observación	Revisión documental	Resumen conclusivo
Equipos remotos de comunicaciones	Las experiencias en los entrenamientos para guerra convencional visualizaron que el empleo de radios con capacidades de Protección Electrónica son vulnerables a la perturbación electrónica. Por lo que se requiere de nuevas propuestas de empleo del material que reduzcan esta vulnerabilidad. Por ende, operar las radios de manera remota y diferente por un operador de radio instruido en Guerra Electrónica incrementa la protección física y electrónica del centro de comunicaciones contra la localización, perturbación y posible destrucción por las armas enemigas.	El nuevo procedimiento de integración del equipo GRA 39 con las 08 estaciones de radio y su instalación remota a diferentes distancias, a través del cable de campaña, requiere de un operador de radio capacitado en guerra electrónica, para la verificación de la operatividad, emisión y recepción de la señal simultánea de diversas estaciones de radio con su adecuada programación de recursos técnicos con el propósito de dar seguridad física y electrónica al centro de comunicaciones. .	El entrenamiento del operador de radio en los ejercicios de comunicaciones contribuye a la integración de los medios de comunicaciones con los recursos técnicos programados, accediendo a un adecuado despliegue e instalación a distancia, lo que permite proporcionar seguridad y protección al centro de comunicaciones de acciones de guerra electrónica enemigas.	Las experiencias en los entrenamientos para guerra convencional determinaron que la capacitación del operador de radio en el empleo de los equipos remotos de comunicaciones es un procedimiento nuevo que abarca el despliegue, instalación e integración de varias estaciones de radio y unidades de control remoto debidamente programadas con sus recursos técnicos, para emitir señales simultáneas, con la finalidad de proporcionar seguridad física y electrónica al centro de comunicaciones.

Tabla 28

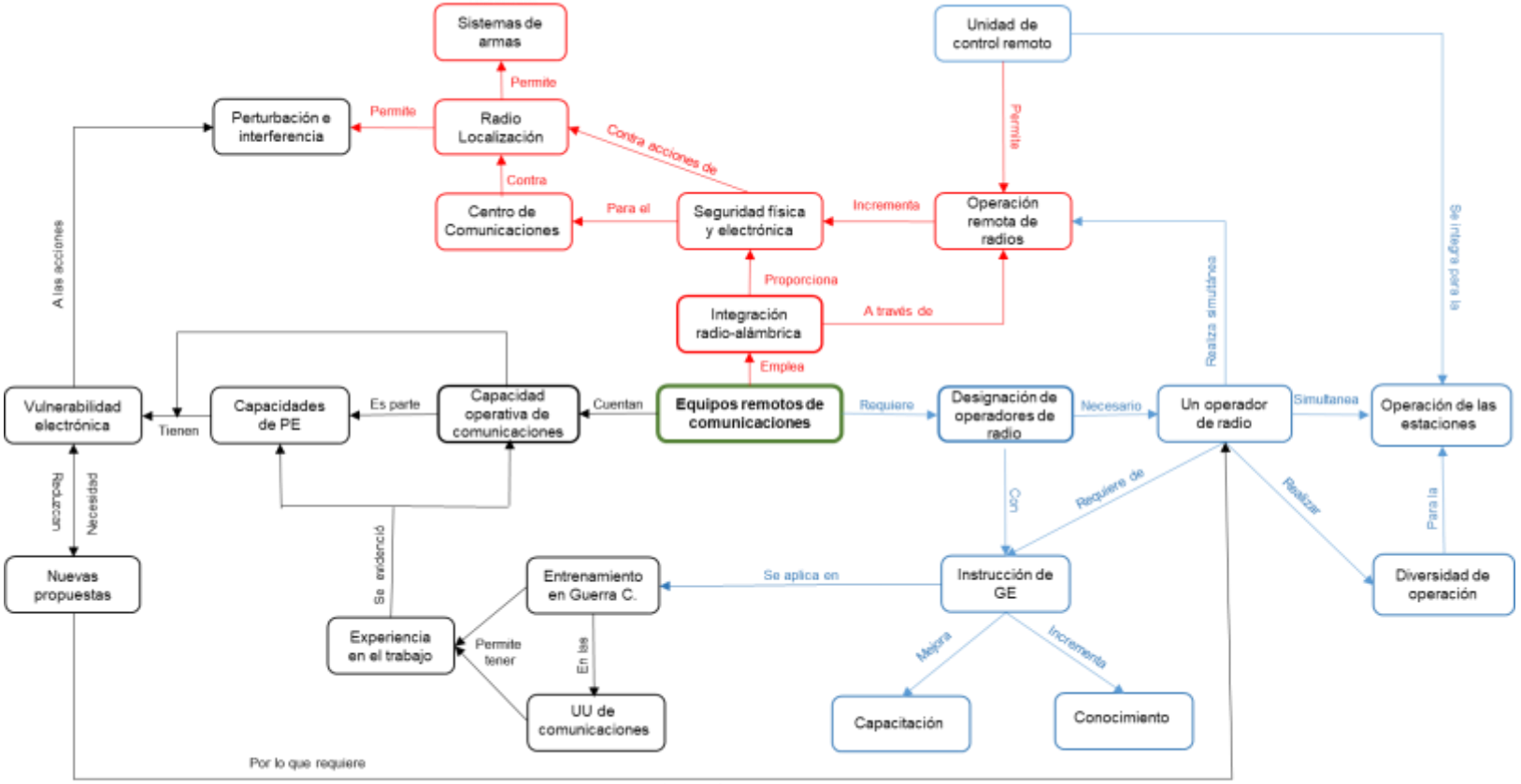
Soporte de categoría- Operaciones de protección electrónica

Categoría	Guía de Entrevista	Guía de Observación	Revisión documental	Resumen conclusivo
Operaciones de protección electrónica	La importancia de establecer la sincronización como una nueva modalidad de radiación accedió a identificar al Enmascaramiento electrónico como un tipo de operación de PE para la señal del centro de comunicaciones, causando desorientación a las capacidades de localización y perturbación enemigas. Esta innovación permitió mantener los enlaces entre las grandes unidades; sin embargo, nuestro nivel de PE es muy limitado por el avance de la tecnología. No implementarlo o incrementarlo generaría una vulnerabilidad, siendo un riesgo crítico que afectaría el apoyo de comunicaciones a las operaciones en guerra convencional.	El entrenamiento es efectivo para que las estaciones de radio propaguen ondas seguras de manera simultánea con las del centro de comunicaciones, generando un enmascaramiento electrónico de la señal protegida, reduciendo la interferencia o perturbación, contribuyendo a mantener los enlaces de los centros de comunicaciones.	La innovación permite obtener nuevas operaciones de PE, como el Enmascaramiento electrónico, que a través de la coordinación de las emisiones con el centro de comunicaciones, ejerce una máxima potencia electromagnética en un tiempo decisivo, disfrazando y distorsionando las radiaciones amigas para ocultar la información, distrayendo y limitando las acciones de SE y AE enemigos, como la perturbación, y limitar así éstas las desventajas durante las operaciones militares y contribuir en mantener los enlaces y proteger el comando y control.	El bajo nivel y las limitaciones exigen mayor entrenamiento con el centro de comunicaciones, de manera de generar innovaciones en el empleo de las operaciones de Protección Electrónica. Accediendo así a identificar al enmascaramiento electrónico como un nuevo tipo de operación que se sincroniza con las emisiones del centro de comunicaciones para distraer y desorientar las acciones de Soporte Electrónico y Ataque Electrónico enemigo, gestionándose el riesgo crítico que contribuye a mantener el apoyo de comunicaciones.

3.5 Red semántica

Figura 13

Red semántica de la entrevista- Equipos remotos de comunicaciones.



Nota. Los colores de las flechas y óvalos están relacionados a las subcategorías: Capacidad operativa de comunicaciones (negro), Integración radio-alámbrica (rojo) y la Designación de operadores de radio (azul).

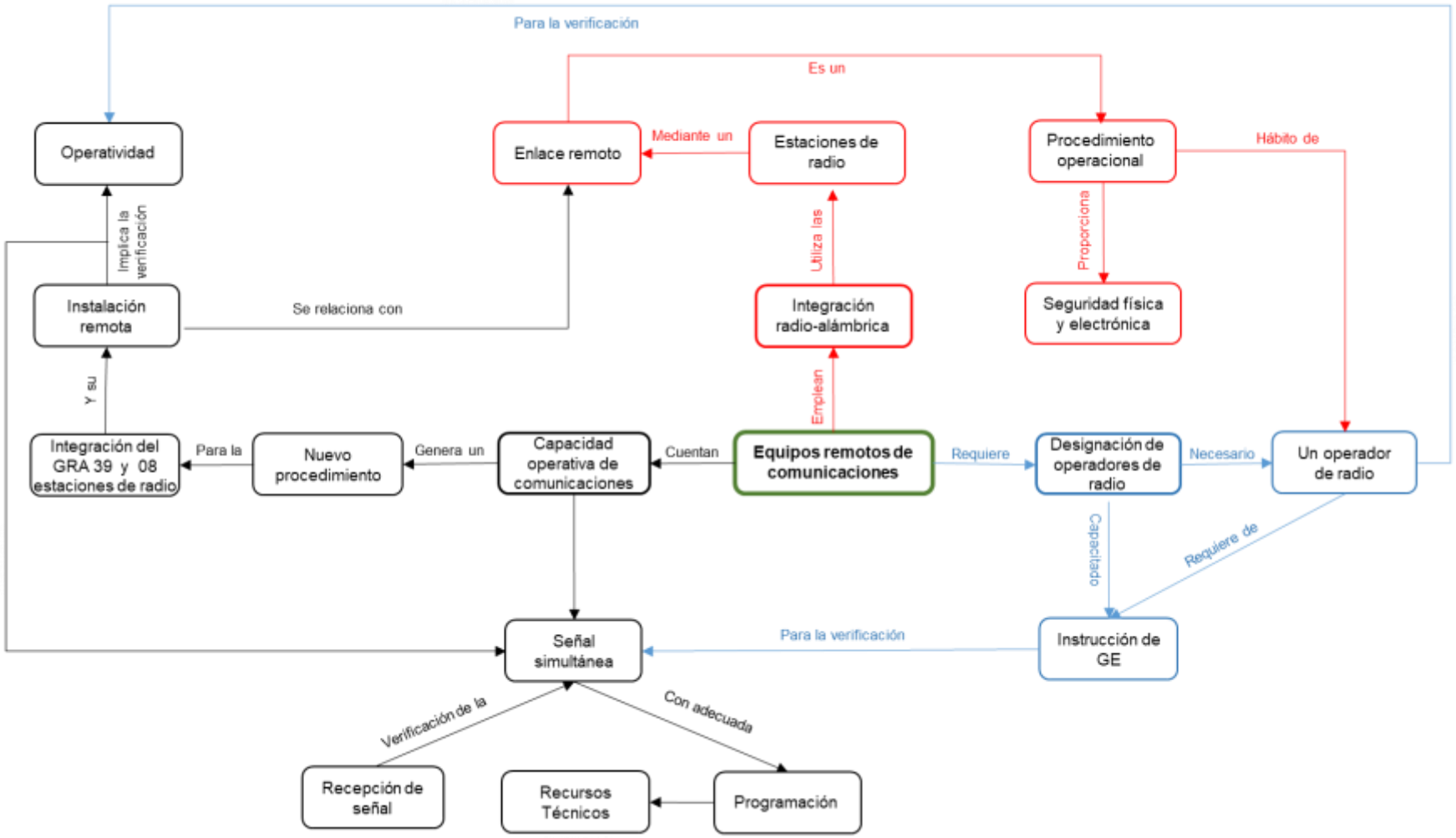
Según la red semántica de entrevistas, establece que la categoría Equipos remotos de comunicaciones se encuentra asociada con la integración radio-alámbrica, capacidad operativa de comunicaciones y la designación de operadores de radio para su empleo; estos conceptos están relacionados con los temas y patrones. En el contexto de estudio destacan temas como la experiencia que se obtuvo mediante la labor prestada en las unidades de comunicaciones del Agrup Com “JO” y los entrenamientos en guerra convencional. Dicha experiencia visualizó que las capacidades de Protección Electrónica, incluyen a la capacidad operativa de comunicaciones y éstas cuentan con vulnerabilidades electrónicas, siendo necesario hacer nuevas propuestas de empleo de los Equipos remotos de comunicaciones para que reduzcan estas vulnerabilidades a las acciones de perturbación e interferencia enemiga.

Como se mencionó anteriormente, el empleo de los Equipos remotos de comunicaciones será mediante la explotación inicial de sus peculiaridades técnicas, de manera que, a través de la unidad de control remoto, se puedan operar de forma remota los equipos de radio. Esta integración radio alámbrica tiene la finalidad de proporcionar la seguridad física y electrónica al centro de comunicaciones contra la radiolocalización, perturbación y evitar la posterior destrucción física por los sistemas de armas enemigos.

Para la designación de operadores de radio, en el empleo de los Equipos remotos de comunicaciones, se requiere que el personal de operadores cuenten con la instrucción de guerra electrónica, la cual es aplicada en el entrenamiento para guerra convencional, de manera que mejoren su capacitación e incrementen sus conocimientos. En esta nueva propuesta, se comprende que solo se requiere de un operador de radio debidamente instruido para realizar esta diversa operación como resultado de la integración de la Unidad de control remoto con las estaciones de radio para su operación remota y simultánea.

Figura 14

Red semántica de la observación-Equipos remotos de comunicaciones.

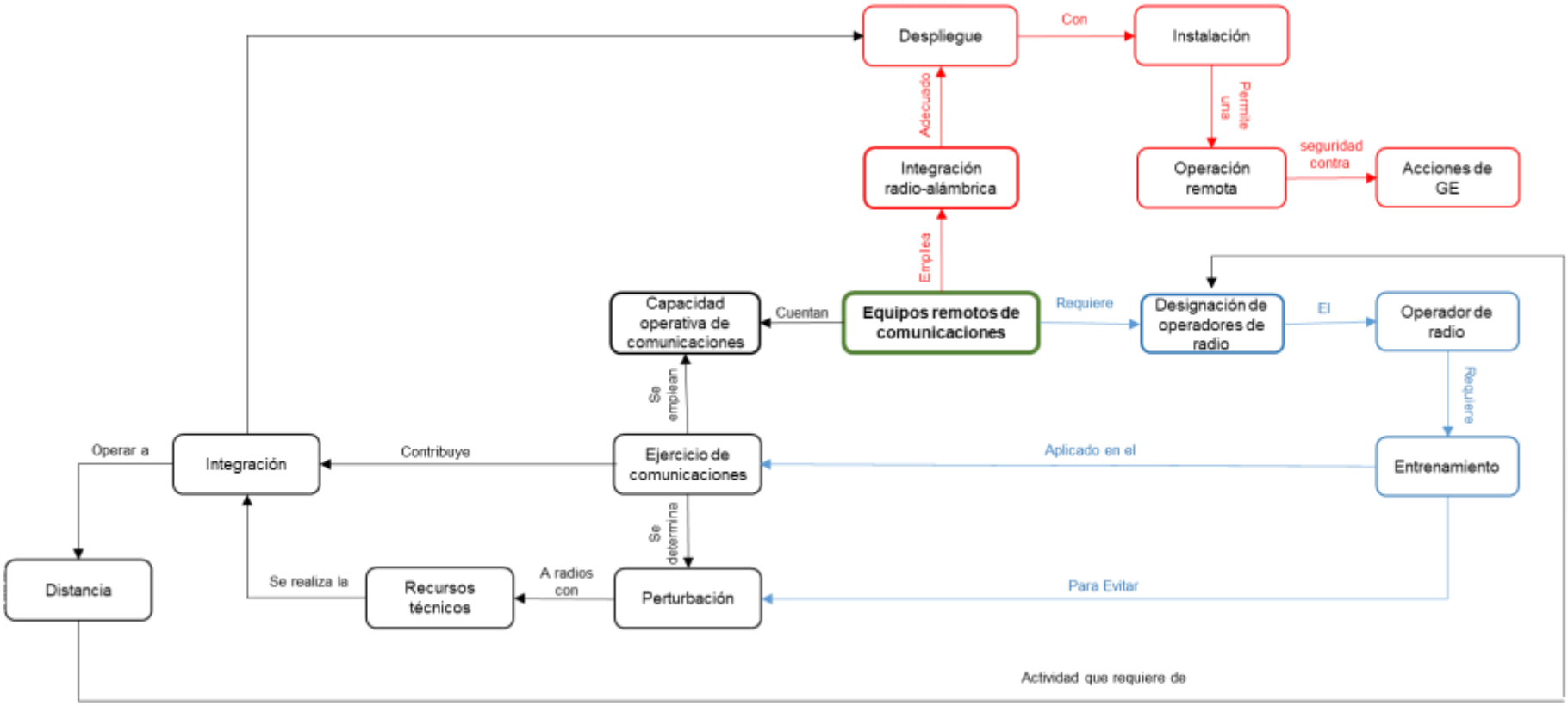


La red semántica de la observación demuestra que la categoría Equipos remotos de comunicaciones se relaciona con tener capacidad operativa, las cuales, a través de su explotación, generan un nuevo procedimiento de empleo de los equipos de comunicaciones. Este procedimiento se realiza por medio de la integración de la Unidad de Control Remoto GRA N° 39 y ocho (8) estaciones diversas de radio, además de su instalación remota por conducto del cable de campaña desplegado a diferentes distancias de la Estación de Protección. Esta práctica involucra las actividades de verificación de la operatividad, programación de los recursos técnicos, verificación de las emisiones y recepción de las señales de las ocho (8) estaciones de radio de forma simultánea.

Para el cumplimiento de estas actividades, se procede con la designación de los operadores de radio, demostrando que, para el empleo de los equipos remotos de comunicaciones, se comprenda que solo se requiere un operador de radio debidamente instruido y capacitado en guerra electrónica, cuya integración radio-alámbrica se relaciona con el uso de las estaciones de radio a través de un enlace remoto, procedimiento operacional hábito de los operadores de radio, para proporcionar la seguridad física y electrónica al centro de comunicaciones.

Figura 15

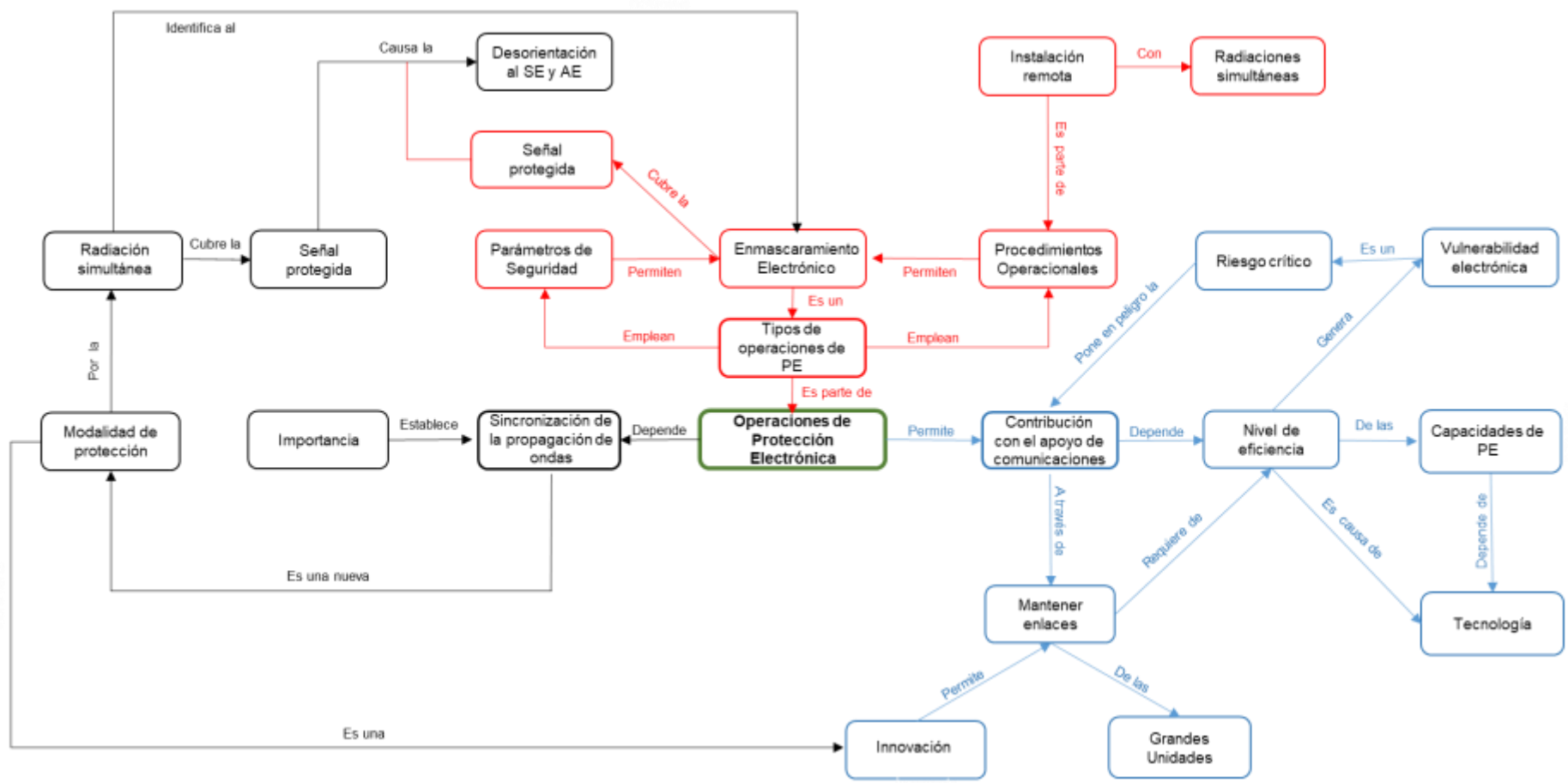
Red semántica del análisis documental y material- Equipos remotos de comunicaciones.



La red semántica del instrumento de análisis documental demuestra que el tema del entrenamiento documentado en guerra convencional y del soporte teórico en el concepto general de la categoría Equipos remotos de comunicaciones cuenta con una capacidad operativa las cuales son empleadas en el ejercicio de comunicaciones y que, a pesar de ello, se determinan acciones de perturbación a estaciones de radios programadas con sus recursos técnicos. Como consecuencia de esta acción de Ataque Electrónico, se tuvo que integrar las estaciones de radio con la Unidad de Control Remoto GRA 39 con la finalidad de operar a distancia. Para esta actividad, la designación entre el personal de operadores de radio, se procede sólo con el personal que tiene entrenamiento en guerra electrónica, de manera de hacer frente a las acciones de perturbación. Asimismo, este entrenamiento aplicado en el ejercicio de comunicaciones generó la necesidad del empleo de equipos remotos a través de la integración de los medios de comunicaciones, accediendo a un adecuado despliegue e instalación de las estaciones de radio debidamente ubicadas a una distancia que permita una operación remota con el fin de proporcionar seguridad y protección al centro de comunicaciones contra acciones de guerra electrónica enemigas.

Figura 16

Red semántica de la entrevista – Operaciones de Protección Electrónica.



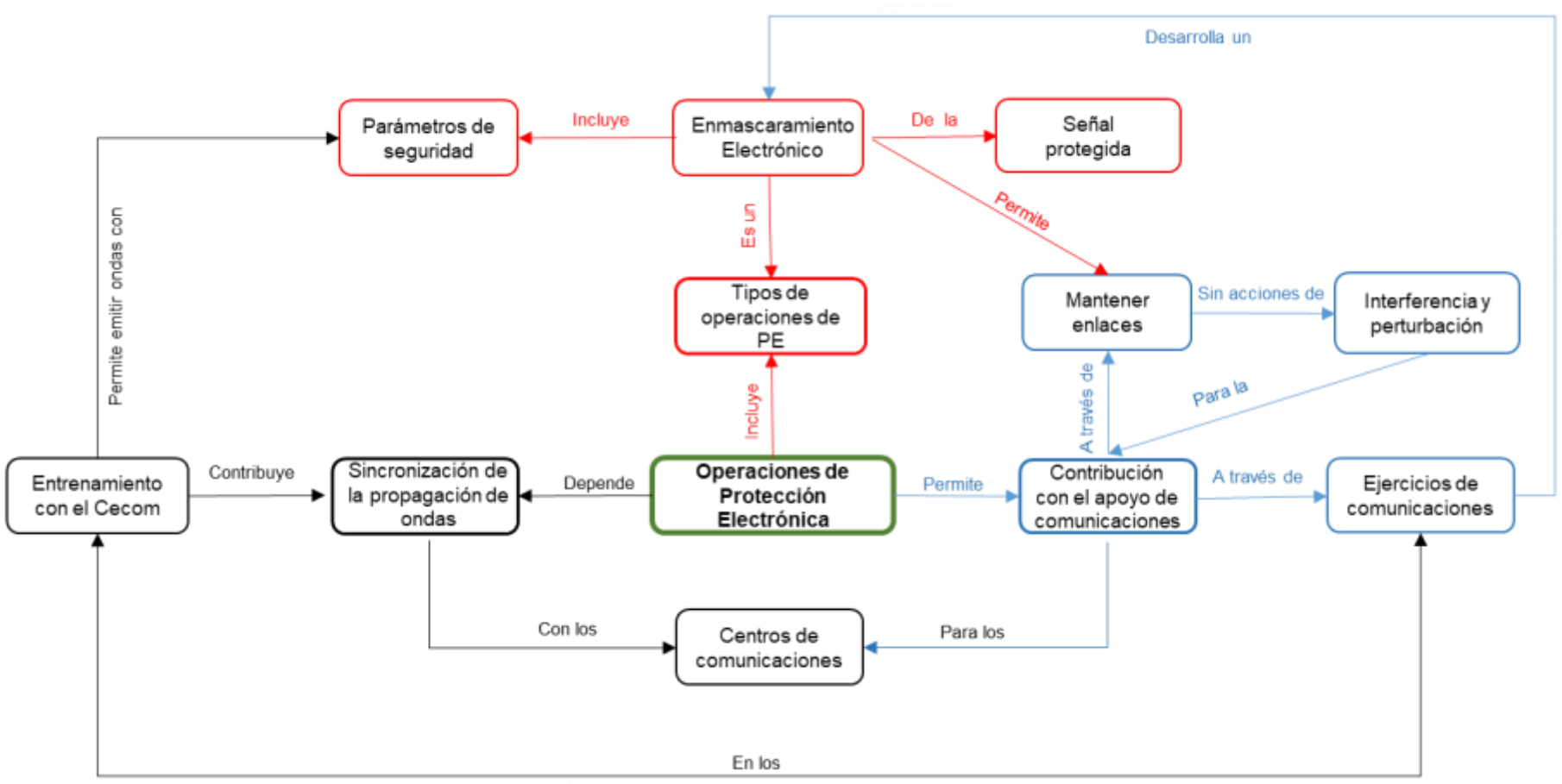
La red semántica establece que la categoría Operaciones de protección electrónica se relaciona por su dependencia de la sincronización de emisiones de ondas, incluye tipos de operaciones de Protección Electrónica y permite la contribución al apoyo de comunicaciones. Los conceptos están relacionados con los temas y patrones. En el contexto del estudio, en particular, resaltan el tema de importancia en su relación con establecer la sincronización como una nueva modalidad o herramienta para la protección electrónica; esto se debe a la radiación simultánea de las estaciones de radio que cubren la señal protegida del Centro de comunicaciones. Este vínculo causa la desorientación a las capacidades de Soporte Electrónico y Ataque Electrónico enemigo.

Por lo expresado anteriormente, debido al patrón de la radiación simultánea de la Estación de Protección con la radiación del Centro de Comunicaciones, origina la relación con el tema de Enmascaramiento Electrónico que, debido al empleo de los parámetros de seguridad y los procedimientos operacionales (instalación remota), permiten que este tipo de operación sea identificado como una operación de la Protección Electrónica, en vista de que su vínculo con cubrir la señal protegida causa desorientación a las capacidades de Soporte y Ataque Electrónico enemigas.

Se ha demostrado que la sincronización de la propagación de ondas está relacionada con el tema de identificar el tipo de operación de Protección Electrónica y que de esta relación de conceptos se incrementan las operaciones de seguridad, vinculándose a la contribución al apoyo de comunicaciones. En particular, en el tema de la nueva modalidad de protección, que es una innovación que accede a mantener los enlaces de las Grandes Unidades, sin embargo, esta contribución depende del nivel de eficiencia de las capacidades de Protección Electrónica que, como consecuencia del avance de la tecnología, se encuentra en un nivel bajo. No incrementarlo generaría vulnerabilidades electrónicas, siendo un riesgo crítico que pondría en peligro el apoyo de las comunicaciones a las operaciones.

Figura 17

Red semántica de la observación – Operaciones de Protección Electrónica.



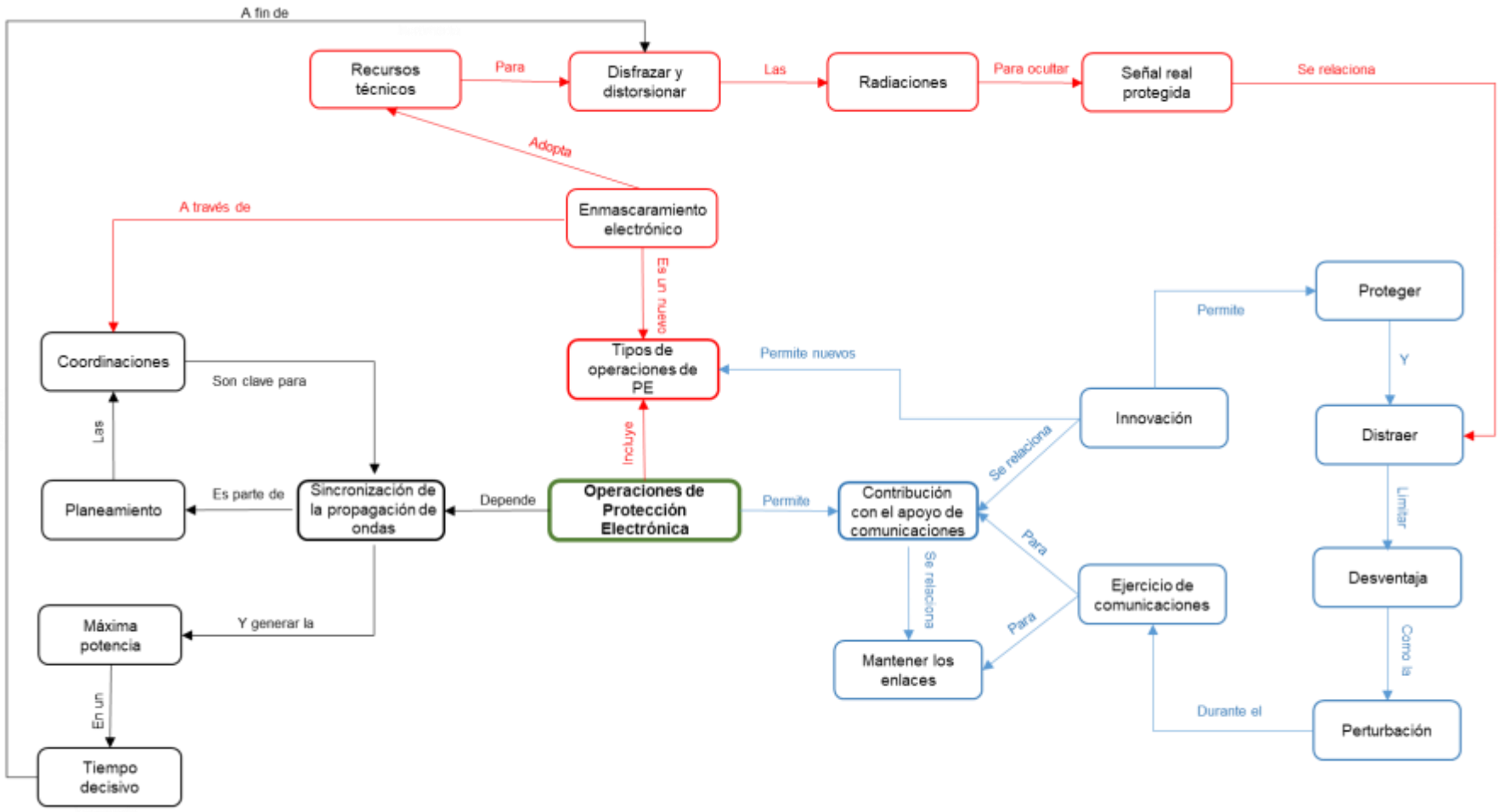
La red semántica del instrumento de la observación establece que la categoría de Operaciones de protección electrónica se relaciona por su dependencia de la sincronización de emisiones de ondas, así como por incluir a los tipos de operaciones de Protección Electrónica y permitir la contribución con el apoyo de comunicaciones. Estos conceptos se encuentran relacionados con los temas y patrones.

En el contexto desarrollado, se argumenta que el entrenamiento de la Estación de Protección, en coordinación con el Centro de Comunicaciones para ejecutar los ejercicios de enlace para operaciones, contribuye a que las estaciones de radio funcionen de manera remota y que éstas puedan emitir ondas de radio seguras de forma simultánea y ulteriormente sincronizadas.

Esta actividad inicia el desarrollo de un tipo de operación de Protección Electrónica que incluye el uso de parámetros de seguridad, identificado como Enmascaramiento Electrónico de la señal protegida. La operación nueva resultante del ejercicio de comunicaciones incrementa las capacidades de Operaciones de Protección Electrónica, lo que permite mantener los enlaces de las grandes unidades y reducir las acciones de guerra electrónica enemigas como la interferencia y perturbación, contribuyendo con el apoyo de comunicaciones al Comando y Control proporcionado por el Agrup Com José Olaya.

Figura 18

Red semántica del análisis documental – Operaciones de Protección Electrónica.



La red semántica del instrumento de análisis del documental demuestra que el soporte teórico en el concepto general de la categoría, Operaciones de protección electrónica, evidencia su dependencia a la sincronización de emisiones de ondas, inclusión de los tipos de operaciones de Protección Electrónica y la contribución al apoyo de comunicaciones; estos conceptos están relacionados con los temas y patrones; en el contexto desarrollado, se demuestra que la innovación permite obtener nuevos tipos de operaciones de Protección Electrónica, como es el caso del Enmascaramiento Electrónico que, a través de las coordinaciones realizadas de la Estación de Protección con el Centro de Comunicaciones para realizar las emisiones simultáneas de radio, determina la clave para la sincronización que se establece en el planeamiento de las operaciones y, de esta forma, genera la máxima potencia de la energía electromagnética en un tiempo decisivo en las operaciones. Esta acción distorsiona y disfraza las radiaciones amigas con el propósito de ocultar la información contenida, así como de distraer y limitar las desventajas ante las acciones de Soporte Electrónico y Ataque Electrónico enemigos, como la perturbación.

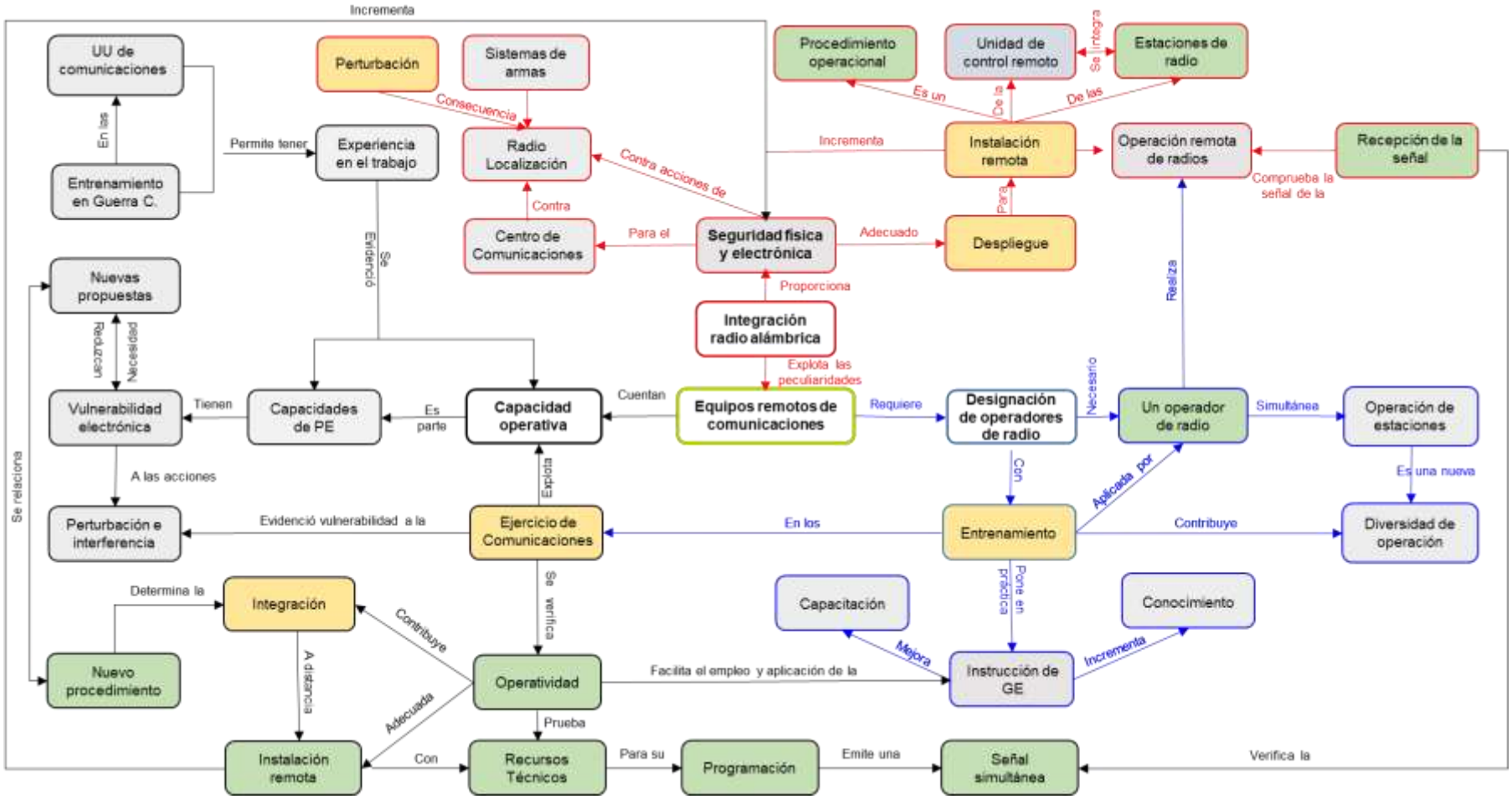
Todo lo señalado anteriormente incrementa las operaciones de Protección Electrónica que se realizan en un ejercicio de comunicaciones, operaciones que son el apoyo para mantener los enlaces del Centro de Comunicaciones, contribuyendo así con el apoyo de comunicaciones al Comando y Control.

3.6 Triangulación

Según Vargas (2011), la triangulación puede confirmar el contenido de una técnica con el contenido de otra. Por lo tanto, se destaca la importancia de este paso. Para este estudio, se utilizó un esbozo con una parte descriptiva y tablas de doble entrada para triangular cada categoría.

Figura 19

Triangulación de red semántica - Categoría Equipos remotos de comunicaciones.



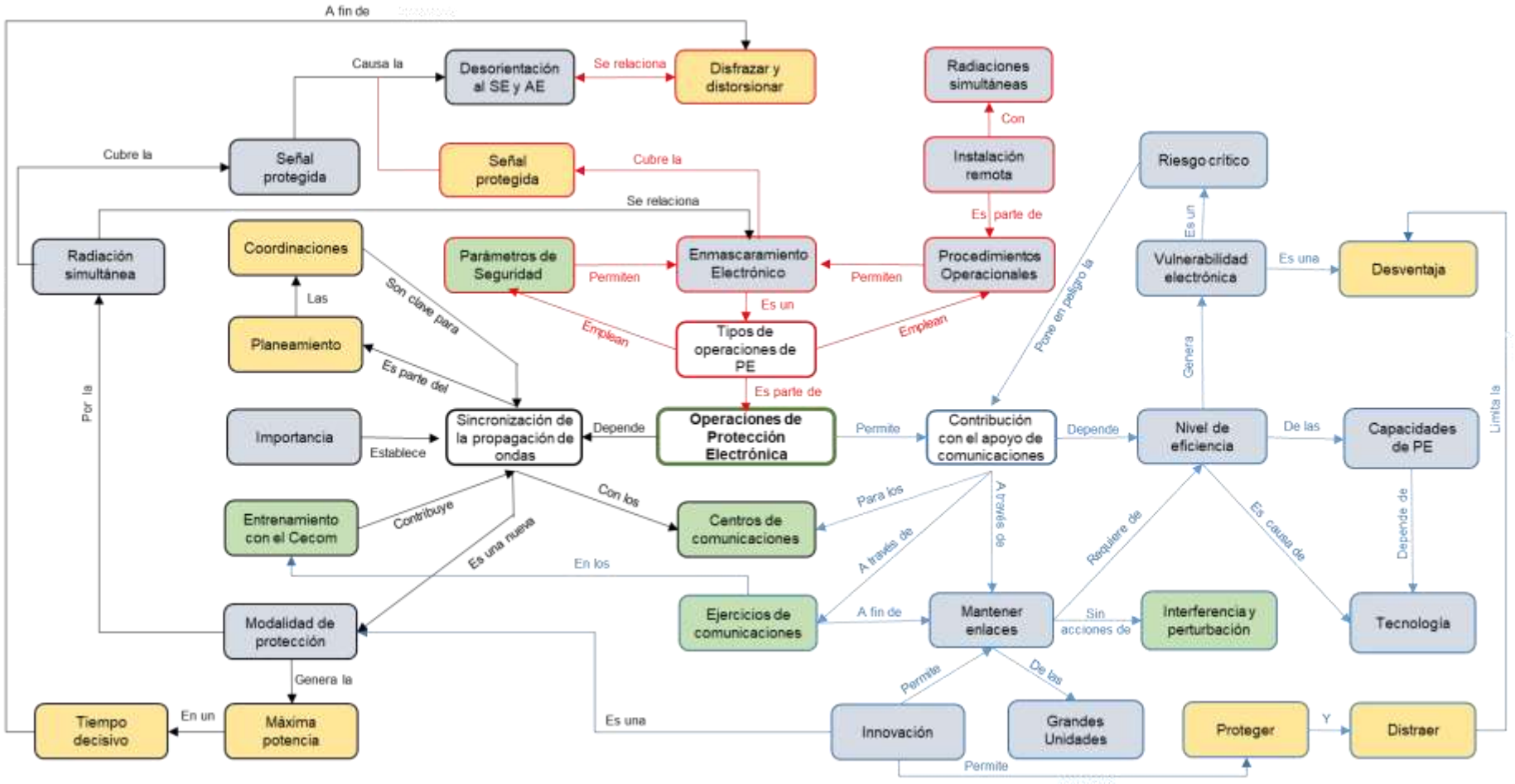
Nota. Los colores de los óvalos están relacionados con los instrumentos de la investigación: Entrevista (gris), Observación (verde) y Análisis documental (anaranjado) y las flechas con las subcategorías.

En la triangulación se reúnen los tres instrumentos empleados en la investigación, en los cuales se demuestra la relación y complemento de los temas y patrones de la categoría: Equipos remotos de comunicaciones y sus subcategorías. Se tiene en consideración que los temas asociados prueban que el empleo de equipos remotos de comunicaciones es una nueva propuesta con procedimientos inéditos, como la integración de la Unidad de control remoto GRA 39 con diferentes estaciones de radio programadas con sus recursos técnicos propios; su despliegue adecuado que involucra su instalación a diferentes distancias de la estación de protección para ser operada de manera remota y generar señales simultáneas de radio, las cuales son verificadas mediante la recepción de sus señales; en este nuevo procedimiento se indica la finalidad de su empleo, como la seguridad física y electrónica del Centro de comunicaciones contra las acciones de Soporte Electrónico, como la radiolocalización que trae como consecuencias acciones de Ataque Electrónico, como la perturbación o destrucción por los sistemas de armas enemigos. Se argumenta que, para la operación de este nuevo empleo de equipos remotos de comunicaciones, se designa a un solo operador de radio, el cual debe contar con entrenamiento e instrucción en guerra electrónica, que le permita contar con conocimientos y estar capacitado de manera de poder adecuarse a esta diversidad de operación.

Se revela que esta nueva propuesta es una necesidad que nace de la experiencia de haber laborado y seguir laborando en las unidades de comunicaciones, en donde se realizan prácticas de enlace a través de los ejercicios de comunicaciones como parte de los entrenamientos para guerra convencional, en el cual se visualizan vulnerabilidades electrónicas que requieren ser minimizadas o reducidas, como la perturbación de los equipos de radios con las capacidades de Protección Electrónica.

Figura 20

Triangulación de red semántica - Categoría Operaciones de protección electrónica.



En la triangulación se reúnen los tres instrumentos empleados en la investigación, en los cuales se demuestra la relación y complemento de los temas y patrones de la categoría Operaciones de protección electrónica y sus subcategorías. Se tiene en consideración que los temas asociados prueban que el entrenamiento en los ejercicios de comunicaciones contribuye a determinar la importancia del desarrollo de la sincronización de la propagación de ondas como una nueva modalidad de protección, al sincronizar, previa coordinación, las radiaciones simultáneas de las estaciones de radio con las radiaciones de radio del Centro de Comunicaciones. Aplicar la máxima potencia de energía en un tiempo decisivo; este evento que involucra el empleo de parámetros de seguridad y procedimientos operacionales (instalación remota) es identificado como una operación de Enmascaramiento Electrónico, siendo una nueva operación de Protección Electrónica para la señal protegida del Centro de Comunicaciones. Este tipo de operación disfraza y distorsiona la señal amiga, causando desorientación a las acciones de Soporte y Ataque Electrónico enemigos. Este incremento de las operaciones PE es una innovación que accede a mantener los enlaces de las grandes unidades sin acciones de perturbación, contribuyendo así con el apoyo de comunicaciones al Comando y Control. Sin embargo, nuestro nivel de eficiencia a causa del avance tecnológico de las capacidades de PE es bajo; no aumentarlo genera vulnerabilidad electrónica que es un riesgo crítico para el apoyo de comunicaciones a las operaciones de Guerra Convencional.

Tabla 29

Triangulación de subcategorías- Equipos remotos de comunicaciones.

Sub Categorías	Guía de Entrevista	Guía de Observación	Revisión documental	Resumen conclusivo
SC1 Capacidad operativa de comunicaciones	Las experiencias en los entrenamientos para guerra convencional visualizaron que el empleo de radios con capacidades de Protección Electrónica, son vulnerables a la perturbación electrónica, por lo que se requiere de nuevas propuestas de empleo del material de comunicaciones.	El nuevo procedimiento de integración del equipo GRA 39 con las 08 estaciones de radio y su instalación remota a diferentes distancias, implica la verificación de la operatividad, emisión simultánea y recepción de la señal de las estaciones de radio con su adecuada programación de recursos técnicos.	En el ejercicio de comunicaciones se determinó acciones de perturbación a radios programadas con recursos técnicos, por lo que tuvieron que ser integradas al equipo remoto GRA 39 y operar a distancia.	Las experiencias en los entrenamientos de los ejercicios de comunicaciones determinaron acciones de perturbación electrónica a estaciones de radio, lo que generó nuevos procedimientos de empleo en la integración e instalación remota de los equipos de comunicaciones que, debidamente programados con sus recursos técnicos, emiten señales simultáneas de radio.
SC2 Integración radio-alábrica	La seguridad física y electrónica del centro de comunicaciones se obtiene mediante la operación remota de las estaciones de radio.	Emplear las estaciones mediante un enlace remoto es un procedimiento operacional que da seguridad física y electrónica.	Un adecuado despliegue e instalación de las estaciones de radio bien ubicadas, permite una operación remota que proporciona seguridad para el centro de comunicaciones contra acciones de guerra electrónica.	El adecuado despliegue y procedimiento operacional de los equipos remotos de comunicaciones permite proporcionar la seguridad física y electrónica al centro de comunicaciones de acciones de Soporte y Ataque Electrónicos enemigos.
SC3 Designación de personal de operadores	Un operador de radio requiere de mayor instrucción, conocimiento y capacitación para realizar diversos tipos de operación de las estaciones de manera remota y simultánea.	La operación de las estaciones de radio la realizó un solo operador de radio capacitado en guerra electrónica.	El operador de radio requiere de entrenamiento para hacer frente a acciones de perturbación.	La capacitación e instrucción en guerra electrónica son indispensables para que un operador de radio pueda realizar diversos empleos de los equipos remotos de comunicaciones.

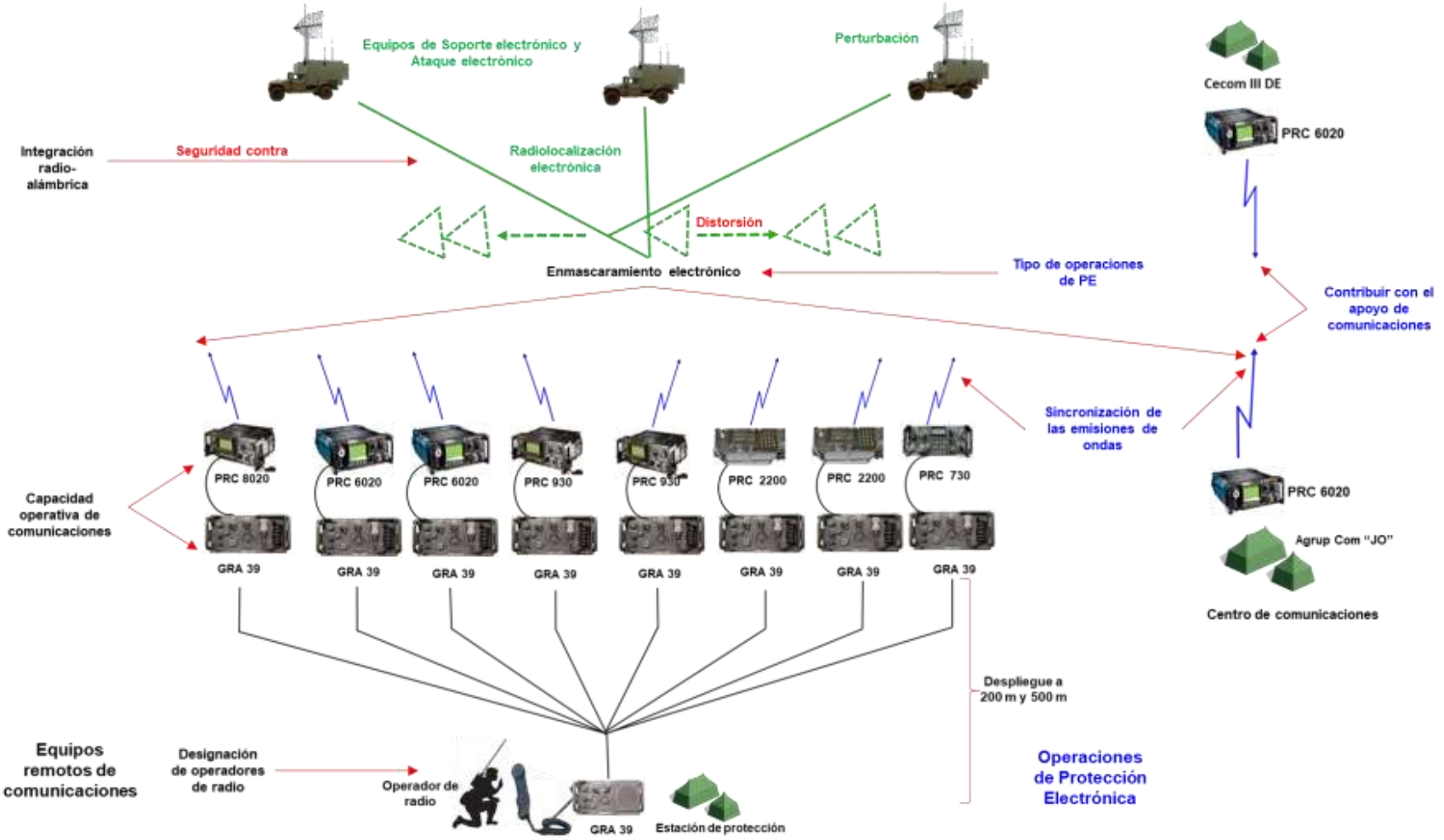
Tabla 30

Triangulación de subcategorías - Operaciones de protección electrónica

Sub Categorías	Guía de Entrevista	Guía de Observación	Revisión documental	Resumen conclusivo
SC4 Sincronización de emisiones de onda	La importancia de establecer la sincronización como una nueva modalidad en la radiación de la energía de manera simultánea con el Cecom permite cubrir la señal protegida del centro de comunicaciones, causando desorientación a la localización y perturbación enemiga.	El entrenamiento contribuye a la sincronización de emisiones de ondas con las del centro de comunicaciones.	En el planeamiento, la coordinación es clave para la sincronización, generando así la máxima potencia en un momento decisivo.	El planeamiento y el entrenamiento establecen la importancia de la sincronización en la radiación de ondas de energía de las estaciones de radio remotas con las radiaciones del centro de comunicaciones, generando la máxima potencia en un momento determinado, cubriendo así la señal o frecuencia protegida, causando desorientación a las capacidades de guerra electrónica enemigas.
SC5 Tipos de operaciones de Protección Electrónica	El empleo de los parámetros de seguridad y procedimientos operacionales para una instalación remota con radiaciones simultáneas, permitió identificar un enmascaramiento electrónico para la señal protegida.	El Enmascaramiento electrónico es un tipo de operación de Protección Electrónica.	El enmascaramiento electrónico adopta recursos técnicos para la seguridad de las comunicaciones, disfrazando y distorsionando radiaciones amigas para ocultar información a las acciones de SE y AE.	El empleo de los recursos técnicos y procedimientos operacionales en el nuevo procedimiento de despliegue, instalación e integración remota con radiaciones sincronizadas, identificaron al Enmascaramiento electrónico como un tipo de operación de PE que disfraza las radicaciones amigas contra las acciones de Soporte y Ataque Electrónico.
SC6 Contribución con el apoyo de comunicaciones	Mantener los enlaces entre las grandes unidades se debió a la innovación. Sin embargo, el nivel de eficiencia de las capacidades de Protección Electrónica por el avance de la tecnología es muy limitado, no aumentarlo generaría un incremento de la vulnerabilidad, siendo un riesgo crítico para el apoyo de comunicaciones a las operaciones.	Durante el ejercicio se mantienen los enlaces entre los centros de comunicaciones.	La innovación permitió proteger nuestras emisiones, limitando las desventajas como la perturbación e interferencia durante el ejercicio de comunicaciones, contribuyendo en mantener los enlaces y proteger el comando y control.	La innovación, a pesar de nuestro nivel limitado de Protección Electrónica, accedió a proteger las emisiones durante el ejercicio de los centros de comunicaciones, limitando las desventajas ante las acciones de localización y perturbación enemiga, gestionando el riego y contribuyendo así con el apoyo de comunicaciones a las grandes unidades.

Figura 21

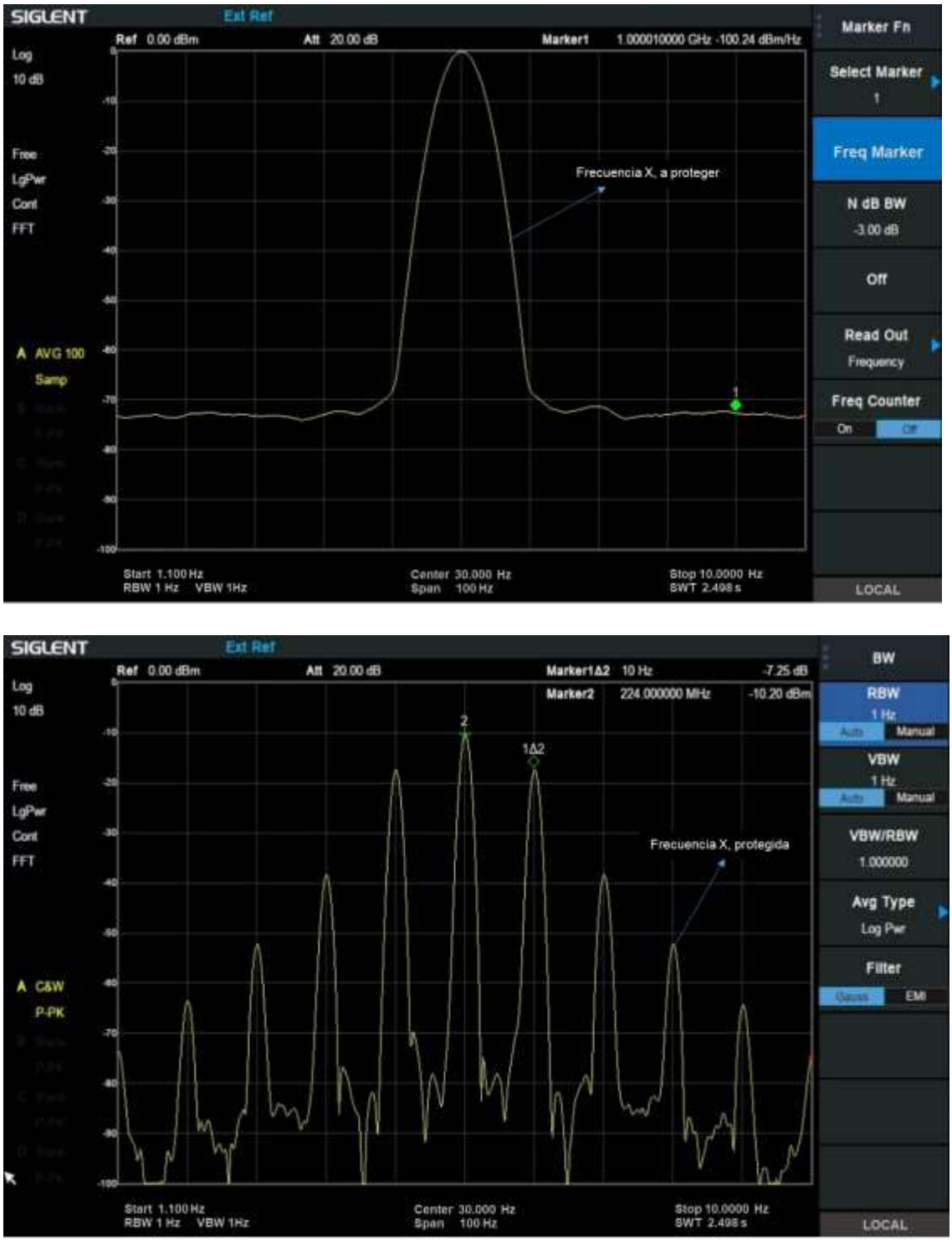
Esquema general del empleo de los Equipos remotos de comunicaciones para incrementar Operaciones de protección electrónica



*Nota***.** La figura muestra las representaciones de las categorías: Equipos de remotos de comunicaciones y las Operaciones de protección electrónica con sus respectivas subcategorías.

Figura 22

Enmascaramiento electrónico de la frecuencia del Centro de comunicaciones



Nota. La figura muestra un ejemplo de enmascaramiento de la frecuencia protegida del Centro de Comunicaciones, sincronizada con ocho señales simultáneas de la estación de protección. Fuente: Analizador de espectro SVA1015X.

Capítulo IV: Discusión de resultados

4.1 Discusión

El objetivo N° 1, identificar las operaciones de Protección Electrónica que se desarrollan en el Agrupamiento de Comunicaciones “José Olaya”, 2023. De conformidad con las respuestas adquiridas en los instrumentos aplicados, se pudo identificar a la acción de Enmascaramiento Electrónico como una nueva operación de Protección Electrónica en la gran unidad de comunicaciones como resultado del uso de los recursos técnicos de las estaciones de radio y aplicación de procedimientos operacionales en el nuevo desarrollo de despliegue, instalación e integración remota de los medios de comunicaciones disponibles que, al ser operados de manera simultánea, generaron radiaciones electromagnéticas mutuas, las cuales al encontrarse en sincronización con las emisiones del Centro de comunicaciones, cubrieron y saturaron de señales del monitor de localización electrónica; distorsionando y protegiendo la señal real o frecuencia única por la cual se realiza el enlace con las grandes unidades y unidades de la División de Ejército contra las acciones de radiolocalización y la perturbación. Coincidiendo con Adamy (2001), para dificultar la localización de los propios sistemas, las contramedidas defensivas incluyen técnicas de supresión de comunicaciones y técnicas de enmascaramiento y dispersión. Como se define en Electronic Warfare Techniques (2013), el Enmascaramiento Electrónico se refiere al control de la radiación de energía electromagnética en frecuencias amigables, disfrazando, distorsionando o manipulando las señales electromagnéticas amigables, para ocultar información clave o crear una falsa impresión de una amenaza. Los resultados obtenidos concuerdan con Arévalo (2015), quien confirmó que los radares de vigilancia terrestre también deben diseñarse para funcionar como medios de PE, y que deben resalizar operaciones de engaño electrónico como parte del subsistema de guerra electrónica. También con lo planteado por Saumeth & Guaidó (2017), la Marina de Guerra del Perú cuenta con capacidades de interferencia mediante ruido de saturación y engaño, haciendo parecer, a vistas del radar atacante, una posición del buque distinta a la real. Los antecedentes y las coincidencias de la presente investigación guardan relación en cuanto a confundir y engañar a las capacidades de Soporte Electrónico enemigo, acciones que, como resultado del nuevo procedimiento de empleo, permitieron identificar al Enmascaramiento Electrónico como una nueva operación de las operaciones de Protección Electrónica realizadas en el Agrup Com “JO”, incrementando así las capacidades militares en la institución.

El objetivo N° 2, explicar la designación del personal de operadores de radio en el empleo de los equipos remotos de comunicaciones en el Agrupamiento de Comunicaciones José Olaya, 2023. Por los resultados obtenidos en las entrevistas, se explica que, para la designación del personal de operadores de radio, se requiere que el personal cuente con la

instrucción de Guerra Electrónica, de manera que estén capacitados con los conocimientos técnicos correspondientes; entendiéndose por medio de la observación que, para el cumplimiento de las actividades del nuevo procedimiento de empleo de equipos remotos de comunicaciones, sólo se requiere de un operador de radio, debidamente instruido y capacitado en Protección Electrónica, de manera que pueda aplicar un procedimiento operacional mediante enlaces remotos de estaciones de radio; coincidiendo con lo dicho por Chiavenato (2011), donde determina que, para gestionar el talento del personal, es necesario individualizar sus habilidades y potencialidades para que dichas competencias se adapten a los puestos específicos. Asimismo, por la cantidad de operadores designados para el manejo de varias estaciones de radio, se emplea el principio de economía de fuerzas. Como lo mencionan Izcue & Arriarán (2013), la economía de fuerzas trata de la adecuada distribución y gestión de las fuerzas disponibles para que no sean mal utilizadas al ser recursos limitados y difíciles de reemplazar. Por tanto, no será necesario requerir de un efectivo mayor de personal de operadores especialistas, no afectando la capacidad operativa del personal de operadores de radio. Concordando con lo estudiado por Ventura & Jaramillo (2014), en donde encontraron que en relación a la capacidad operativa de personal de técnicos y suboficiales sólo el 4 % (19 efectivos) son operadores de radio capacitados en guerra electrónica y, según el Informe de Capacidad operativa (2023), se cuenta con 2.5% (12 efectivos) de operadores de radio. Los resultados obtenidos concuerdan con la investigación de Gonzales (2017) en mantener la instrucción y entrenamiento del personal de operadores de la CIA. G. Elect. N° 113 en actividades de Soporte Electrónico para acciones de radiolocalización electrónica. Los antecedentes y las coincidencias de la presente investigación evidenciaron la importancia de explicar la designación del personal de operadores de radio en relación con la economía de fuerzas y la trascendencia de encontrarse debidamente capacitado con la instrucción precisa en guerra electrónica para el nuevo empleo de medios de comunicaciones disponibles en el Agrup Com “JO”.

El objetivo N° 3, develar el incremento de las operaciones de protección electrónica, contribuyen con el apoyo de comunicaciones al comando y control proporcionado por el Agrupamiento de Comunicaciones José Olaya, 2023. Según la guía de entrevista, el nivel actual de las capacidades de PE es bajo debido al avance tecnológico y, de no mejorarse, incrementaría la vulnerabilidad electrónica que es un riesgo crítico para el apoyo de las comunicaciones al comando y control. Sin embargo, mediante la observación se verificó que, como resultado del nuevo procedimiento de empleo de los medios remotos de comunicaciones, la sincronización de ondas de los equipos de radio de la Estación de Protección con las ondas de radio del Centro de Comunicaciones del Agrup Com “JO”, dio como resultado una nueva operación, identificada como Enmascaramiento Electrónico; esta nueva operación originó desorientación y distracción de las señales amigas a la

radiolocalización y perturbación, incrementando así las capacidades de las operaciones de Protección Electrónica, lo que accedió a gestionar el riesgo crítico, accediendo a mantener los enlaces del Centro de Comunicaciones del Agrup Com “JO” con el Centro de Comunicaciones de la III División de Ejército, de manera continua, contribuyendo así con el apoyo de comunicaciones al Comando y Control y, por consiguiente, la seguridad física de los sistemas de enlace y personal. Coincidiendo con Beck (2006), en el cual sostiene que los riesgos incluyen tanto la actividad humana como la tecnología. Este resultado está en línea con Vadell (2016), en donde menciona que, ante la carencia de capacidades de PE y empleo de procedimientos pasivos que generaron la destrucción de los centros de comunicaciones, se implementó un nuevo procedimiento que consistía en apagar los radares, negando así su ubicación y posterior destrucción, manteniendo el comando y control de la alerta temprana. Así como menciona Vallejos (2015), respecto a los objetivos relacionados con la teoría, se intentó esclarecer la complejidad, el detalle y el ambiente electromagnético, respondiendo a una fortaleza de la acción de comando y control al permitir el dominio del espacio electromagnético. Los antecedentes y las coincidencias de la presente investigación, guardan relación en cuanto a las iniciativas de empleo de medios de comunicaciones que, como consecuencia, incrementaron las capacidades de Protección Electrónica, accediendo a mantener la seguridad de los medios electrónicos, personal y el apoyo de comunicaciones al comando y control.

Cómo resultado en el objetivo general: describir el empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones José Olaya, 2023. La guía de entrevista resaltó la experiencia obtenida de los especialistas en determinar que, por la carencia de medios de GE, el bajo nivel de PE y el avance de la tecnología, se realizó un nuevo empleo de los medios de comunicaciones disponibles en la institución, corroborado mediante la observación de que, a través de la explotación de la capacidad operativa de los medios de comunicaciones, se realizó la integración de una Unidad de Control Local GRA 39 a diferentes distancias de la Estación de Protección con diferentes estaciones de radio para ser operadas de manera remota y generar señales simultáneas de radio de forma tal que estén sincronizadas con las emisiones del Centro de Comunicaciones; este nuevo empleo, generó un enmascaramiento electrónico y para su funcionamiento se designó a un operador de radio, con la finalidad de proporcionar la seguridad física y electrónica al Centro de Comunicaciones contra los riesgos que generan las acciones de radiolocalización y perturbación electrónica; como lo señala Adamy (2001), la PE son medidas tomadas para proteger los propios sistemas de comunicación contra las amenazas planteadas por la GE; de igual forma, menciona Guerrillacomm (2011), en operaciones, no puedes posicionar tus equipos remotos en la cima de una montaña, debido a que podrían ser vulnerables a las operaciones de Guerra

Electrónica enemigas como su ubicación y destrucción. En el análisis de los resultados obtenidos, ante la carencia de equipos de SE y AE propios, se incrementaron las capacidades de Protección Electrónica, concordando con la investigación por Echeverría (2021), que concluye que el estado actual de disponibilidad y operatividad del material de comunicaciones que padece la Compañía de Guerra Electrónica N° 113 del Agrupamiento de Comunicaciones José Olaya en el tema de comando y control es insuficiente. Los antecedentes y las coincidencias de la presente investigación evidenciaron la necesidad de un nuevo empleo de medios de comunicaciones disponibles en el Agrup Com “JO” para incrementar las capacidades de PE en la institución.

4.2 Conclusiónes

En cuanto al primer objetivo, identificar las operaciones de protección electrónica que se desarrollan en el Agrupamiento de Comunicacionses “José Olaya”, como conclusión de los resultados obtenidos en las entrevistas, observación y análisis documental, se identificó la acción de Enmascaramiento Electrónico como una nueva operación de Protección Electrónica, porque, debido a la nueva modalidad de las emisiones electrónicas de manera simultánea y sincronizada con las emisiones del centro de comunicaciones, se distorcionó y cubrió las frecuencias, protegiendo y ocultando información propia para no ser analizada. El producto del análisis documental, en el cual se describe la teoría que sustenta esta operación y que no es empleada en nuestra doctrina, ayudó a relacionar e identificarla como una operación de Protección Electrónica. Asimismo, lo demostrado mediante la observación en trabajo de campo permitió relacionar los nuevos procedimientos de protección electrónica con el Enmascaramiento Electrónico. Lo más difícil de identificar la operación de protección electrónica fueron los constantes ensayos de los ejercicios de enlace, lo que demandó mayor tiempo de entrenamientos y coordinaciones a fin de llegar a la sincronización en tiempo y espacio de las emisiones de los equipos de radio de la Estación de Protección con las emisiones de radio del Centro de Comunicaciones, retrasando la obtención de datos. Para solucionar estos problemas de sincronización, se tiene que impulsar el entrenamiento y ejercicios de comunicaciones con los medios disponibles con los que cuenta la unidad, así como incluir en la doctrina institucional estos nuevos conocimientos, de manera que formen parte de los programas de instrucción para el personal militar del arma de comunicaciones y especialistas en guerra electrónica.

El segundo objetivo, explicar la designación del personal en el empleo de los medios remotos de comunicaciones, se concluye que como resultado del análisis de los obtenidos en los instrumentos, se requirió de sólo un operador de radio debidamente capacitado para emplear este nuevo procedimiento por medio de un equipo de Control Remoto GRA 39 integradas con ocho equipos de radio de manera simultánea. Esta designación no afectó la capacidad operativa de personal de la gran unidad y no será necesario requerir mayor efectivo

de operadores de radio. La predisposición y colaboración del personal de oficiales, técnicos y suboficiales del arma de comunicaciones en ejecutar este nuevo procedimiento de empleo para incrementar las operaciones de Protección Electrónica, fue primordial para explicar la designación de personal, porque se pudo demostrar en la observación la experiencia de los oficiales como producto de su entrenamiento. Lo más difícil de explicar la designación del personal de operadores de radio fue encontrar entre los operadores de radio personal con conocimiento y capacitación en guerra electrónica, puesto que se carece de este personal especializado en el Agrupamiento de Comunicaciones José Olaya, por el motivo de que ya no se desarrolla el Curso de Guerra Electrónica en la Escuela de Comunicaciones del Ejército. Para dar solución a este problema se tiene que gestionar y retomar la especialización de operadores de radio en guerra electrónica o que se incluyan estos conocimientos en los programas de instrucción de los diplomados de capacitación del nivel básico y avanzado de técnicos y suboficiales.

En el objetivo tercero, develer el incremento de las operaciones de protección electrónica contribuye con el apoyo de comunicaciones al comando y control. Se concluye que, como producto obtenido de los instrumentos de estudio, mediante las acciones de cobertura y distorsión de la señal propia se pudo gestionar el riesgo crítico, manteniendo el enlace que proporcionaba el centro de comunicaciones de la gran unidad con el centro de comunicaciones de la III División de Ejército, sin presentar discontinuidad y neutralización por acciones de perturbación de agentes externos o interferencias por las emisiones propias. Lo que más ayudó a develar el incremento de las operaciones, fue la gran cantidad de energía electromagnética emitida por la Estación de Protección de manera simultánea, a través de diversos equipos de radio con parámetros de seguridad debidamente programados en salto de frecuencia y secreto, dificultanddo el análisis sobre la real frecuencia a identificar. Lo más difícil en develar el incremento de las operaciones fue el de no poder contar con equipos más complejos de interceptación y radiolocalización de señales, porque no se pudo constatar el tiempo efectivo de distorsión y encubrimiento de la señal protegida. Para solucionar este problema de equipos de interceptación, se puede gestionar ante el Ministerio de Comunicaciones la asignación temporal de estos medios. Teniendo en cuenta estos puntos, será necesario investigar más a fondo, a fin de determinar el tiempo de distorsión y encubrimiento de las emisiones amigas para este nuevo proceso de empleo. Así como, es necesario investigar la contribución al apoyo de comunicaciones con una mayor cantidad de Estaciones de Protección, de manera de formular nuevos procedimientos que permitan una mejor capacidad de PE y mantener en un mayor tiempo las comunicaciones en apoyo al comando y control.

En conclusión general, en el objetivo de describir el empleo de los equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el

Agrupamiento de Comunicaciones “José Olaya”, destaca la demostración del nuevo proceso de instalación, integración e interconexión de una unidad de Control Remoto GRA 39 con varias estaciones de radio, porque dieron como resultado emisiones simultáneas de energía electromagnética que, al ser sincronizadas con las emisiones de radio del Centro de Comunicaciones, dieron como producto al enmascaramiento electrónico, accediendo a contribuir con el apoyo de comunicaciones a las grandes unidades, beneficiando al personal que trabaja en el Agrup Com “JO” y demás profesionales mediante la obtención de nuevos conocimientos. La observación realizada por el personal especialista en guerra electrónica y comunicaciones en las instalaciones del cuartel “Mariano Melgar” de Arequipa fue fundamental para describir este inédito empleo, porque se demostró que mediante la designación de un solo operador para el empleo de diversos medios de comunicaciones disponibles en la institución se pueden incrementar las operaciones de protección electrónica , ratificando lo expresado en las entrevistas a los expertos, quienes tuvieron experiencias sobre el bajo nivel de las capacidades de PE en los sistemas de comunicaciones durante los entrenamientos en guerra convencional. Lo más difícil de la descripción de empleo fueron los constantes ensayos de sincronización en los ejercicios de comunicaciones, porque llevaron a la investigación a un mayor tiempo en la obtención de datos y solventar el abastecimiento de baterías para las unidades de control remoto y local. Para dar solución a este problema, se tienen que gestionar ante el Batallón de Mantenimiento y Abastecimiento N° 511 y Centro de Ciencia y Tecnología del Ejército, proyectos de estudio que generen baterías que accedan a ampliar la operatividad de las unidades de Control Remoto GRA 39.

4.3 Recomendaciones

La Sección de Instrucción, Entrenamiento y Doctrina del Estado Mayor del Agrupamiento de Comunicaciones “José Olaya”, formule el proyecto de modificación del Manual de Empleo 11-221 “Guerra Electrónica” y el Manual de Empleo 11-16 “Doctrina General de Guerra Electrónica”, considerando el aporte conceptual de la acción de Enmascaramiento Electrónico como una nueva operación de protección electrónica en nuestra doctrina. Así mismo, se deben considerar las implicancias en la capacidad operativa de la Instrucción y Entrenamiento en cuanto al incremento de las operaciones de protección electrónica como un factor a considerar como parte de los ejercicios de comunicaciones de la gran unidad. Que la Sección Logística del Estado Mayor gestione ante el Servicio de Comunicaciones del Ejército la redistribución del material de comunicaciones de última generación, teniendo prioridad el Agrupamiento de Comunicaciones “José Olaya”, a fin de impulsar esta nueva modalidad de empleo del material y equipo.

La Escuela de Comunicaciones del Ejército gestione ante la Dirección General de Doctrina y Educación del Ejército la reactivación del Curso de Especialidad de Guerra Electrónica para el personal de técnicos y suboficiales de la especialidad de Operadores de

Radio y Mecánicos de Radio, así como incluir en los diplomados programas de actualización con los nuevos aportes a la doctrina y conceptos de la nueva operación de protección electrónica. Agregando a los anteriores, la Sección Personal del Estado Mayor del Agrupamiento de Comunicaciones “José Olaya” gestione ante el Comando de Personal del Ejército el incremento de operadores de radio de manera de incrementar el efectivo de personal y capacitar en el nuevo procedimiento de empleo de medios de comunicaciones remotos.

La Dirección de Planeamiento del Ejército impulse la formulación del Proyecto de Guerra Electrónica ante el Comité Especial Técnico Operativo (CETO) responsable, a fin de viabilizar su compra según lo programado en el Plan de Inversiones, de manera de contar con equipos modernos de soporte electrónico que puedan determinar el tiempo real de distorsión y encubrimiento de las emisiones amigas por el nuevo procedimiento de empleo de los medios de comunicaciones que incrementan las operaciones de protección electrónica. Así mismo, con base en los beneficios obtenidos, se recomienda que el personal especialista en guerra electrónica y comunicaciones de la institución realice investigaciones con una mayor cantidad de estaciones de protección, de manera de solucionar con mayor efectividad la vulnerabilidad electrónica; que acceda a asegurar y mantener el apoyo de comunicaciones proporcionado por el Agrupamiento de Comunicaciones “José Olaya” al comando y control.

La Sección de Planes y Operaciones del Estado Mayor del Agrupamiento de Comunicaciones “José Olaya” disponga a la Compañía de Guerra Electrónica N° 113, ponga en práctica el nuevo procedimiento de empleo de los medios de comunicaciones remotos a fin de incrementar las operaciones de protección electrónica durante los entrenamientos de los ejercicios de comunicaciones para guerra convencional, con la finalidad de explotar en las mejores condiciones los nuevos conocimientos de esta nueva capacidad que permite contribuir con el apoyo de comunicaciones al comando y control de la III División de Ejército. Asimismo, la Sección Logística del Estado Mayor deberá gestionar ante el Servicio de Comunicaciones del Ejército y ante el Centro de Ciencia y Tecnología del Ejército la formulación de proyectos de investigación que generen una mayor operatividad y tiempo de funcionamiento a las unidades de control remoto GRA 39.

Referencias

Adamy, D. (2001). *EW 101: A First Course in Electronic Warfare*. Editorial: Artech House Publisher.

Arispe, C., Yandal, J., Guerrero, M., Rivera, O., Acuña, L. y Arellano, C. (2020). *La investigación científica.* Editorial. Universidad Internacional de Ecuador.

Arévalo, A. (2015). *Empleo de Radares de Vigilancia Terrestre (Rvt) en las Operaciones de Seguridad de la 3ra Brigada de Caballería del Ejército del Perú – Tacna - 2014* [Tesis de maestría, Escuela Superior de Guerra del Ejército]. https://renati.sunedu.gob.pe /handle /sunedu/3305473.

Barrantes, R. (2002). *Investigación. Un camino al conocimiento. Un enfoque cualitativo y cuantitativo.* Editorial. Universidad Estatal a distancia.

Beck, U. (2006). La sociedad del riesgo global. https://www.sigloxxieditores.com/libro/la-sociedad-del-riesgo-global_17637/.

Briones, B. (2021). *Capacidades del Sistema de Comando y Control de la 3a Brigada de Caballería en la Defensa Activa* [Tesis de Maestría, Escuela Superior de Guerra del Ejército]. https://renati.sunedu.gob.pe/handle/sunedu/3304954.

Características Técnicas de Material de Comunicaciones en uso en el Ejército. (2004). Ejército del Perú. Manual de Empleo MTE 11-200.

Centro de Escritura Javeriano. (2020). *Normas APA, séptima edición*. Pontificia Universidad Javeriana, seccional Cali. https://www2.javerianacali.edu.co/centro-escritura/recursos/manual-de-normas-apa-séptima-edicion#gsc.tab=0%C2%A0

Chiavenato, I. (2011). *Administración de recursos humanos. El capital humano de las organizaciones*. Mc Graw Hill.

Colom, G. (2017). Una revisión del Planeamiento de la Defensa por Capacidades en España. *Papeles de Europa, 47,* 47-68. http://dx.doi.org/10.5209/PADE.56334.

Comunicaciones en Campaña. (2007). Fuerzas militares de Colombia. Ejército Nacional. Manual EJC. 4-32

Creswell, J. W. (2013). *Investigación Cualitativa y Diseño Investigativo: Elección entre cinco enfoques.* Londres: Sage 2013.

Doctrina General de Telemática. (2004). Ministerio de Defensa. Ejército del Perú. Manual de Empleo 11-1.

Doctrina General de Guerra Electrónica. (2005) Ministerio de Defensa. Ejército peruano. Manual de Empleo 11-16 EP.

Echevarría, M. (2021). *Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de Comunicaciones.* [Tesis de maestría, Escuela Superior de Guerra del Ejército]. https://renati.sunedu.gob.pe/handle/sunedu/3305192

Echazu, L. (2022). *La Silenciosa Guerra Electrónica*. Editor, Ciudad Autónoma de Buenos Aires. https://www.youtube.com/watch?v=bn3do9NVipU

Empleo de Comunicaciones para todas las Armas. (2000). Ministerio de Defensa. Ejército peruano. Manual de Empleo 11-9.

Espinoza, C. (2017). *Apuntes de un Conflicto, Cenepa 1195.* Edición Jorge Martinez

Electronic Warfare Techniques. (2023). *Técnicas de Guerra Electromagnéticas* ATP 3-12.3 https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37298-ATP_3-12.3-000-WEB-1.pdf

Gonzales. G. (2017). *Empleo de Personal Especialista en Guerra Electrónica y Producción de Inteligencia de Señales en la IV División de Ejército [*Tesis de maestría, Escuela Superior de Guerra del Ejército]. https://renati.sunedu.gob.pe/handle/sunedu/3305407

Gutierrez, C. (2006). *El conflicto de Irak II.* Editorial Nipo.

Guerra Electrónica (2013). Ministerio de Defensa. Ejército peruano. Manual de Empleo 11-221 EP.

Guerrillacomm. (2011, 05 de agosto). *Introducción al set de control remoto por radio excedentes A/N GRA-39* [video]. You Tube. https://www.youtube.com/watch?v=REoJr31iSeg&t=9s

Hernández, S. y Mendoza (2018). *Metodología de la Investigación*. Editorial. McGraw-Hill Interamericana Editores.

Informe de la Compañía de Guerra Electrónica (2014). *Perturbación en los equipos de radio HF 6020 y VHF 9000 durante la maniobra en el terreno*. Agrupamiento de Comunicaciones “José Olaya”.

Informe de Capacidad Operativa (2023). *Capacidad Operativa de Comunicaciones.* Sección Logística y Personal, Agrupamiento de Comunicaciones “José Olaya”-Tiabaya.

Iglesias, M. (2015). *Diseño de algoritmos de guerra electrónica y radar para su implementación en sistemas en tiempo rea*l [Tesis de doctorado, E.T.S.I. Telecomunicación UPM]. https://doi.org/10.20868/UPM.thesis.35022.

Izcara, P. (2014). Manual de Investigación Cualitativa. México, D.F: Fontamara.

Izcue, C. & Arriaran, F. A. (2013). *Apuntes sobre estrategia* operacional. Editor, División de Publicaciones de la Escuela Superior de Guerra Naval.

https://repositorio.esup.edu.pe/bitstream/20.500.12927/157/1/Apuntes%20de%20Estrat%C3%A9gia%20Operacional.

Manual Técnico. (1991). *Manual de Soporte Directo de Mantenimiento para control y ajuste del grupo de radio* AN/GRA-39, AN/GRA-39A, AN/GRA-39B y AN/GRA-39C

Marcos, V. (2021, 16 enero). *Mundo de la aviación, Contramedidas Flares, Chaff y electrónica* [Video]. You Tube. https://www.youtube.com/watch?v=kJcswLtwQfs

Martil, I. (2023). *Radar en la historia del siglo XX.* Editorial Guillermo Escolar

Nyquist, H. (13-17 de febrero de 1928). *Certain topics in telegraph transmission theory.* Teorema del muestreo.

Perez, J. (2022). *Sincronización, definición y concepto.* https://definición.de/sincronizacion/

Pillpe, C. (2018). *Gestión de riesgos críticos de seguridad y salud ocupacional en minería subterránea*. [Tesis de Maestría. Universidad Científica del Sur. Lima].

Plan de Empleo y Magnitud de la Fueza.2023. Dirección de Planeamiento. Ejército del Perú

Planeamiento de Operaciones Terrestres (2015). Ejército del Perú. Manual de Empleo 1-134

Prieto, G. y Espinoza, J. (2017). *La Semilla de Odio. De la invasión de Irak al surgimiento del ISIS.* Editorial DEBATE.

Saumeth, E. & Guaidó, J. (2017) *Guerra Electrónica en Suramérica.* Tecnología Militar-TECMIL- N° 1 P. 80. https://monch.com/ebooks/tecnologia-militar/2017/01/mobile/index.html#p=80

Shannon, C. (1949). *Communication in the presence of noise.* Teorema del muestreo.

Tolmos, Y. (2015). *Clausewitz, concepto, historia y realidad.* Editorial Prinley, S.R.L https://www.esffaa.edu.pe/wp-content/uploads/2020/10/LIBRO-CLAUSEWITZ-2015.pdf.

Vallejos, R. (2015). *Efectos del Sistema de Telefonía Satelital Móvil y Apoyo de Guerra Electrónica en las Operaciones del Comando Especial del Valle de los Ríos Apurímac, Ene y Mantaro, 2015* [Tesis de maestría, Escuela Superior de Guerra del Ejército]. https://renati.sunedu.gob.pe/handle/sunedu/3305050.

Vasquez, J. (2020). *Guerra Ruso Japonesa 1904-1905.* Editorial Galland Book.

Vadell, F. (2016). *Análisis de las Operaciones de Guerra Electrónica durante la Guerra de las Malvinas en el Teatro de Operaciones Atlántico Sur.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Argentina. http://www.cefadigital.edu.ar/bitstream/1847939/901/1/TFI%20342016%20VADELL.pdf

Ventura, D. & Jaramillo, C. (2014). *Sistema de comunicaciones y la capacidad operativa de la 3ra Brig Com, 2014* [Tesis de maestría, Escuela Superior de Guerra].

Vargas, X. (2011). *Cómo hacer investigación cualitativa. Edición Etxeta,SC.* Mexico.

ANEXOS

ANEXO 1

MATRIZ DE CONSISTENCIA

ANEXO 1 MATRIZ DE CONSISTENCIA

Título: Empleo de equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023.

Preguntas de Investigación	Objetivos	Teorías	Categorías	Subcategorías	Metodología	Análisis de datos
¿Cómo es el empleo de los equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023? ¿Cuáles son las operaciones de protección electrónica a desarrollarse en el Agrupamiento de Comunicaciones “José Olaya”, 2023? ¿Cómo es la designación del personal de operadores de radio en el empleo de equipos remotos de comunicaciones en las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023? ¿De qué manera el incremento de las operaciones de protección electrónica contribuye con el apoyo de comunicaciones al comando y control proporcionado por el Agrupamiento de Comunicaciones “José Olaya”, 2023?	Describir el empleo de los equipos remotos de comunicaciones para incrementar las operaciones de protección electrónica en el Agrupamiento de Comunicaciones “José Olaya”, 2023. Identificar las operaciones de protección electrónica que se desarrollan en el Agrupamiento de Comunicaciones “José Olaya”,2023. Explicar la designación del personal de operadores de radio en el empleo de equipos remotos de comunicaciones en el Agrupamiento de Comunicaciones “José Olaya”, 2023. Develar el incremento de las operaciones de protección electrónica contribuye con el apoyo de comunicaciones al comando y control proporcionado por el Agrupamiento de Comunicaciones “José Olaya”, 2023.	Teoría del riesgo social Beck (2001), los conceptos sobre cómo relacionar los riesgos como resultado de la tecnología, cómo los riesgos nos afectan y cómo gestionar los riesgos para proteger a las personas, se relacionaron con el uso de los medios de comunicación remotos para incrementar las operaciones de protección electrónica, debido al riesgo de que el apoyo de comunicaciones sea neutralizado. La teoría de la guerra electrónica de Adamy (2006), tiene clara relevancia y aplicación en el tema del empleo de equipos remotos de comunicaciones y las operaciones de PE en comprender cómo funcionan los medios de comunicaciones para mejorar las capacidades de PE y que, como resultado, la capacidad de comunicaciones se vuelva menos vulnerable a los AE.	Equipos remotos de comunicaciones Operaciones de Protección Electrónica	• Capacidad operatva de comunicaciones. • Integración radio-alámbrica. • Designación de Operadores de radio • Sincronización en la propagación de ondas. • Tipos de operaciones de protección electrónica. • Contribución con el apoyo de comunicaciones	**Enfoque:** Cualitativo **Tipo:** Teórico-empírico **Método:** Fenomenológico-hermenéutico **Población:** Personal militar especialista en Guerra Electrónica y Comunicaciones **Muestra** 04 Oficiales de comunicaciones 03 Oficiales especializados en Guerra Electrónica	**Técnicas:** • Entrevistas • Observación • Análisis documental **Instrumentos:** • Guía de entrevista • Guía de observación • Ficha de análisis documental y material **Técnica de análisis de datos:** Los datos se procesaron de forma manual o artesanal.

ANEXO 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA (NO ESTRUCTURADA)

Entrevista al Señor ……. jefe de …… Mi Corone,l buenos días, me encuentro desarrollando un trabajo de investigación de tesis para obtener el grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones en la Escuela Superior de Guerra del Ejército-Escuela de Postgrado, habiendo elegido el tema titulado (**Empleo de Equipo Remotos de Comunicaciones para Incrementar las Operaciones de Protección Electrónica en el Agrupamiento de Comunicaciones "José Olaya", 2023**). Desde ya le agradezco su colaboración.

Mi ……:

1. Como oficial de comunicaciones durante su permanencia en el Agrupamiento de Comunicaciones "José Olaya", ¿ha tenido alguna experiencia sobre interferencias o perturbaciones en el empleo de los medios de su unidad?

Rpta.- ……..

2. Teniendo conocimiento sobre la tecnología avanzada dispuesta en los sistemas de Soporte y Ataque Electrónico en los conflictos y guerras actuales en el 2023. ¿considera usted que es necesario contar con nuevas iniciativas sobre el empleo del material de comunicaciones que cuenta la institución?

Rpta.- ……..

3. Teniendo en consideración a las operaciones de Protección Electrónica, ¿conoce usted si las características técnicas de las que disponen los equipos remotos de comunicaciones son vulnerables a las operaciones de Soporte Electrónico y Ataque Electrónico?

Rpta.- ……..

4. Considera usted, ¿cuál es la finalidad de empleo de los equipos remotos de comunicaciones en las operaciones de Protección Electrónica?

Rpta.- ……..

5. La institución dentro de las especialidades técnicas contempla personal especialista en operación de radios, ¿considera usted que la designación del personal especialista como operadores de radio para el empleo de los medios remotos de comunicaciones, es igual a la designación de personal de operadores de radio para los centros de comunicaciones?

Rpta.- ……..

6. En base a su experiencia, considera que, ¿la sincronización de las comunicaciones es uno de los factores importantes para las operaciones de enmascaramiento electrónico como parte de la Protección Electrónica?

Rpta.- ……..

7. En el tiempo que participó en los entrenamientos para operaciones de guerra convencional, ¿qué operaciones de Protección Electrónica se pudieron identificar para contribuir con el apoyo de comunicaciones al Comando y Control proporcionado por el Agrupamiento de Comunicaciones “José Olaya”?

Rpta.- ……..

8. Base a su experiencia, ¿cómo describiría el aporte a mantener el enlace en apoyo al comando y control proporcionado por el Agrupamiento de Comunicaciones “José Olaya” en los entrenamientos para operaciones de guerra convencional?

Rpta.- ……..

9. ¿Que opinión tendría Ud. sobre las consecuencias o efectos de no implementar procedimientos nuevos para incrementar las operaciones de Protección Electrónica en la Institución?

Rpta.- ……..

10. Con los medios de comunicaciones disponibles con que cuenta nuestra institución, desde su punto de vista, ¿cuál cree que es nivel de eficiencia, alto, medio o bajo de las operaciones de Protección Electrónica?

Rpta.-……

FICHA DE ANÁLISIS DOCUMENTAL

Se seleccionaron los documentos considerados de mayor relevancia para la elaboración del estudio de la base de datos de repositorios académicos, Google Académico y fuentes primarias, tales como libros, tesis de investigación y revistas electrónicas especializadas. De esta forma, los documentos claves que cumplieron a cabalidad con los criterios establecidos en las fases del estudio, y que dieron sustento al estudio conceptual, son los que se describen a continuación:

Tipo de documento	País	Referencia	Temas
Manual de empleo	Perú	Guerra Electrónica (2013)	- Protección Electrónica - Acciones de PE - Procedimientos operacionales de PE
Manual de empleo	Perú	Doctrina General de Guerra Electrónica (2005)	- Protección Electrónica
Publicación	Estados Unidos	Electronic Warfare Techniques (2023)	- Protección Electrónica - Enmascaramiento electrónico
Manual Técnico	Estados Unidos	Unidad de Control GRA 39 (1991)	- Unidad de Control GRA 39 - Integración radio alámbrica
Manual de empleo	Perú	Planeamiento de Operaciones Terrestres (2015)	- Sincronización
Informe de operaciones	Perú	Informe (2014)	- Perturbación - Protección electrónica
Manual	Colombia	Comunicaciones en Campaña (2007)	- Medios de comunicaciones radiales
Video	Estados Unidos	Guerrillacomm (2011)	- Introducción al set de control remoto por radio A/N GRA-39
Artículo de investigación	Argentina	Vadell (2016)	- Procedimientos de operaciones Protección Electrónica

GUIA DE OBSERVACIÓN DEL "EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR LAS OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA", 2023.

N°	ASPECTOS A EVALUAR	SI	NO	OBSERVACIONES
1	¿Los medios de comunicaciones se encuentran operativos y están programados?	X		Se probaron la operatividad de las radios y unidades de control remoto; posteriormente se programaron las radios con diferentes modalidades de emisión en especial secreto y salto de frecuencia
2	¿Se realizó el nuevo procedimiento de despliegue, instalación e integración de los medios de comunicaciones?	X		Se procedió con la instalación de una unidad de control local del GRA 39, a esta se conectaron 08 líneas de cable de campaña, cada línea se conecta a una unidad de control remoto del GRA 39 y estas unidades posteriormente se integran a las 08 estaciones de radio.
3	¿Las unidades de control remoto y unidad local del equipo GRA 39 se interconectan con las estaciones de radio a distancia?	X		De manera de probar la integración radio alámbrica, se instalaron los equipos a diferentes distancias, entre 200 a 500m aproximadamente.
4	¿Las emisiones de ondas son emitidas de manera simultánea en las diferentes estaciones de radio cuando son operadas remotamente con los parámetros programados?	X		Se verificó el funcionamiento de la estación del Cecom con el Cuartel General de la III División de Ejército y el funcionamiento de las estaciones remotas con sus emisiones de manera simultánea, comprobando la recepción de sus emisiones por dos radios programadas con los mismo parámetros y gama de frecuencia.
5	¿El personal que opera las estaciones de radio, conoce la finalidad de empleo del material?	X		Los operadores de radio designados conocen la finalidad de emplear las estaciones a distancia como un procedimiento operacional de Protección Electrónica que da seguridad física y electrónica.
6	¿Son más de dos los operadores que integra la estación de protección electrónica?		X	Solo fue necesario un operador de radio con instrucción y capacitación de Guerra Electrónica para el empleo remoto y simultáneo de las 8 estaciones de radio.
7	¿Existe sincronización en las emisiones de radio entre la estación del Centro de comunicaciones del Agrup Com "José Olaya" con las estaciones de radio operadas de manera remota?	X		Existe sincronización de las emisiones de ondas de la estación de protección con las emisiones de ondas del centro de comunicaciones.

8	¿Identifica operaciones de Protección Electrónica, qué tipos según su observación?	X		Se observó que la operación de Protección Electrónica fue del tipo enmascaramiento electrónico, que incluye acciones anti-soporte y ataque electrónico (perturbación).
9	¿Las señales de radio de la estación del Centro de Comunicaciones del Agrupamiento Comunicaciones “José Olaya” es interferidas o perturbadas?		X	Durante el ejercicio de comunicaciones no hubo perturbación e interferencia.
10	¿Se pudieron mantener las comunicaciones entre el Centro de Comunicaciones del Agrupamiento de Comunicaciones “José Olaya” y el Cecom de la III DE?	X		Las señales de radio entre los centros de comunicaciones de la gran unidad y III División de Ejército se mantuvieron fluidas durante todo el ejercicio.

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN:EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES JOSÉ OLAYA,2023.

II. **DATOS DEL EXPERTO:**

a. Apellidos y nombres : Vega Castro Hugo Edwin
b. Grado académico-profesión : Magister
c. D.N.I. : 09933373
d. N° de teléfono : 988037956
e. Lugar y fecha : Lima 25 octubre 2023
f. Firma

II. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : Christian Velazco Cornelio
b. Institución a la que pertenece : Dirección de Planeamiento del Ejército
c. Método de investigación : Cualitativo
d. Tipo de entrevista : Entrevista no estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: 0 a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta, número de entrevistas.	1
03	Estructuración	Guía de entrevista: Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistadoTema propios: Aspectos que interesen	0.8
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitoria.	1
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armonizacon las experiencias que esperan ser revaloradas en el cuestionario.	0.7
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de lasvariables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conoceren el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	1
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos queayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultadosde la entrevista y analizarlos /interpretarlos.	1

VII. RESULTADO DE VALORACIÓN: 95 %.

V. OPINIÓN DE APLICACIÓN

APLICABLE PARA LA GUIA DE ENTREVISTA DEL TESISTA

Aspectos para la valoración

- Validada por TRES expertos, con grado académico demaestro/doctor.
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales queterminen en cero o en cinco. Ejemplo: 0.60; 0.75

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN: EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES JOSÉ OLAYA,2023.

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : Medina Diaz Ronald Jesús
b. Grado académico-profesión : Magister
c. D.N.I. : 29652045
d. N° de teléfono : 944434952
e. Lugar y fecha : Lima 24 octubre 2023
f. Firma :

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a. Autor(es) del instrumento : Christian Velazco Cornelio
b. Institución a la que pertenece : Dirección de Planeamiento del Ejército
c. Método de investigación : Cualitativo
d. Tipo de entrevista : Entrevista no estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: 0 a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta, número de entrevistas.	0.6
03	Estructuración	Guía de entrevista: Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistadoTema propios: Aspectos que interesen	1
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitoria.	1
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armonizacon las experiencias que esperan ser revaloradas en el cuestionario.	1
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de lasvariables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conoceren el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	1
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos queayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultadosde la entrevista y analizarlos /interpretarlos.	1

IV. RESULTADO DE VALORACIÓN: 96%.

V. OPINIÓN DE APLICACIÓN

Aplicable para la guía de entrevista del tesista.

Aspectos para la valoración

- Validada por TRES expertos, con grado académico demaestro/doctor.
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales queterminen en cero o en cinco. Ejemplo: 0.60; 0.75

VALIDACIÓN DE GUÍA DE ENTREVISTA POR EXPERTO

TÍTULO DE LA INVESTIGACIÓN: EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES JOSÉ OLAYA,2023.

III. DATOS DEL EXPERTO:

a.	Apellidos y nombres	: Rivera Schreiber Hernán Enrique
b.	Grado académico-profesión	: Magister
c.	D.N.I.	: 43328983
d.	N° de teléfono	: 996549818
e.	Lugar y fecha	: Arequipa, 26 octubre 2023
f.	Firma	:

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN (entrevista)

a.	Autor(es) del instrumento	: Christian Velazco Cornelio
b.	Institución a la que pertenece	: Dirección de Planeamiento del Ejército
c.	Método de investigación	: Cualitativo
d.	Tipo de entrevista	: Entrevista no estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: 0 a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta, número de entrevistas.	1
03	Estructuración	Guía de entrevista: Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios: Aspectos que interesen	0.9
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitoria.	1
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	0.8
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	0.7
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	1

X. RESULTADO DE VALORACIÓN: 94 %

V. OPINIÓN DE APLICACIÓN

El instrumento es aplicable.

Aspectos para la valoración

- Validada por TRES expertos, con grado académico demaestro/doctor.
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales queterminen en cero o en cinco. Ejemplo: 0.60; 0.75

ANEXO 4

COMPROMISO ÉTICO

DECLARACIÓN DE COMPROMISO ÉTICO

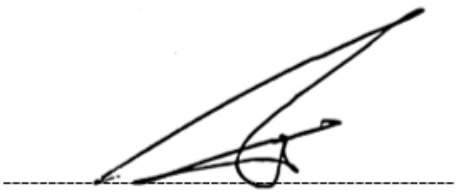
El presente trabajo de investigación titulado: **Empleo de Equipos Remotos de Comunicaciones para Incrementar Operaciones de Protección Electrónica en el Agrupamiento de Comunicaciones José Olaya, 2023.**

Se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación en Ciencias Militares promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado.

En vista de lo anterior:

Yo Bach. Christian Velazco Cornelio egresado de la Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado esta investigación siguiendo las instrucciones brindadas por el Departamento de Gestión de la Investigación, desde la elaboración del marco referencial y recolección de la información, hasta el análisis de datos y elaboración del informe final.

En tal sentido la información contenida en el presente documento es producto de mi trabajo personal, apegándome a la legislación sobre propiedad intelectual, sin haber incurrido en falsificación de la información o cualquier tipo de fraude, por lo cual me someto al marco legal y normativo vigente relacionado a dicha responsabilidad, así como a las normas disciplinarias establecidas en la ESGE-EPG.



Christian VELAZCO CORNELIO

43337354

ANEXO 5

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

PERÚ | Ministerio de Defensa | Ejército del Perú | Estado Mayor General del Ejército | Dirección de Planeamiento del Ejército

"Año de la unidad, la paz y el desarrollo"

San Borja, 14 de agosto de 2023.

Oficio N° 211/H-1.a.3/06.00

Señor General de Brigada
Hernán Enrique RIVERA SCHERIBER
Comandante General del Agrupamiento de Comunicaciones "José Olaya". –**Arequipa**

Asunto : Solicita brindar facilidades a personal que se indica

Ref. : a. Reglamento para la obtención del grado académico de Maestro en Ciencias Militares.
b. Reglamento de investigación de la ESGE-EPG.

Tengo el honor de dirigirme a usted, para manifestarle que, en relación a los documentos de la referencia, se le solicita respetuosamente se digne disponer a quién corresponda, brindar las facilidades para el levantamiento de datos e informaciones al Crl EP Christian VELAZCO CORNELIO, oficial I Maestría de Ciencias Militares y que actualmente se encuentra laborando en la Dirección de Planeamiento del Ejército, que realiza la investigación titulada: **EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR LAS OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA", 2023.**

Agradeciendo de antemano por las facilidades brindadas, en espera del acuse de recibo correspondiente, es propicia la oportunidad para expresarle los sentimientos de mi especial consideración y deferente estima.

Dios guarde a usted.

ESTADO MAYOR GENERAL DEL EJÉRCITO – DIRECCIÓN DE PLANEAMIENTO DEL EJÉRCITO

O - 300014072 - O+
RICARDO Aníbal BENAVIDES FEBRES
General de Brigada
Director de Planeamiento del Ejército

Distribución
- III DE/Agrup Com "JO"....01
- Archivo.....01/02

DIRECCIÓN DE PLANEAMIENTO DEL EJÉRCITO
RECIBIDO
S-00048078-10-O+
LINDA A. DIAZ HUAYTA
S02 EP
FECHA 21/8/23

PERÚ | Ministerio de Defensa | Ejército del Perú | III División de Ejército

"Año de la unidad, la paz y el desarrollo"

Tiabaya, 18 de agosto de 2023.

Oficio N° /Secretaría/Agrup Com

Señor General de Brigada
Ricardo Aníbal BENAVIDES FEBRES
Director de Planeamiento del Ejército. –**San Borja**

Asunto : Autorización de acceso a las instalaciones y levantamiento de información.

Ref. : Oficio N° 211/H-1.a.3/06.00 del 14 agosto 2023

Tengo el agrado de dirigirme a usted, para manifestarle que, en relación a los documentos de la referencia, este comando autoriza y brinda las facilidades de acceso a las instalaciones y el levantamiento de datos e informaciones al Crl EP Christian VELAZCO CORNELIO, oficial I Maestría de Ciencias Militares y que actualmente se encuentra laborando como oficial de Estado Mayor en la Dirección de Planeamiento del Ejército, que realiza la investigación titulada: **EMPLEO DE EQUIPOS REMOTOS DE COMUNICACIONES PARA INCREMENTAR LAS OPERACIONES DE PROTECCIÓN ELECTRÓNICA EN EL AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA", 2023.**

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

Dios guarde a usted.

AGRUP COM "JOSÉ OLAYA" - COMANDANCIA -

O – 223918775 – O +
HERNÁN ENRIQUE RIVERA SCHERIBER
General de Brigada
Comandante General del Agrup Com "José Olaya"

Distribución
- JEMGE/DIPLANE.....01
- Archivo.....01/02

EJÉRCITO DEL PERÚ
III DIVISIÓN DE EJÉRCITO
AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA"
OFICINA PLANES
RECIBIDO
FECHA 18 AGO. 2023 HORA 14:01

ANEXO 6

HOJA DE DATOS PERSONALES

HOJA DE DATOS PERSONALES

GRADO: CORONEL

NOMBRES: Christian

APELLIDOS:Velazco Cornelio

EMAIL: ChristianVelazco1177@gmail.com y cvelazcoc@esge.edu.pe

DIRECCIÓN: Calle Franciscon de Zela 227- Villa Militar Este- Chorrillos

CELULAR: 955504059

FIRMA:

ANEXO 7

APORTE DE INVESTIGACIÓN

DESARROLLO DEL APORTE DOCTRINARIO

1. Definición del Enmascaramiento Electrónico

El término de Enmascaramiento Electrónico, según la doctrina norteamericana descrita en el Electronic Warfare Techniques (2023) es la emisión moderada de energía electromagnética en la gama de frecuencias empleadas por las estaciones de radio de nuestras fuerzas, con la finalidad de cuidar nuestras señales de radio y plataformas de comunicaciones contra el empleo de operaciones de Soporte y Ataque Electrónico enemigo, sin disminuir notablemente el funcionamiento de nuestras estaciones.

El Enmascaramiento Electrónico disfraza, distorsiona o manipula radiación de señales electromagnéticas amigables, para ocultar información crítica o presentar percepciones falsas de amenaza. ATP 3-12.3.

2. Definición del Enmascaramiento Electrónico (EnmElec) para nuestra doctrina

El Enmascaramiento Electrónico es la emisión de una gran cantidad de energía electromagnética de diferentes estaciones de radio en distintas gamas de frecuencia, potencia y emisión de forma simultánea para ser sincronizadas con las emisiones de las estaciones de radio de los centros de comunicaciones o estaciones de radio de nuestras fuerzas, con la finalidad de disfrazar y distorsionar la frecuencia protegida cubriendo información crítica, de manera de contribuir con el apoyo de comunicaciones al comando y control de las operaciones.

El EnmElec disminuye el riesgo de acciones de SE como la radiolocalización, así como las acciones de AE como la perturbación, proporcionando seguridad física y electrónica a los medios y órganos de comunicaciones.

3. Equipos de comunicaciones remotos empleados

Los equipos de radios son los siguientes:

a. Unidad de Control Remoto GRA 39

b. Cable de Campaña WD-1/TT

c. Equipo de radio PRC 930

d. Equipo de radio PRC 2200

e. Equipo de radio PRC 6020

f. Equipo de radio PRC 8000

g. Equipo de radio PRC 730

h. Bateras BA 30

Se emplearon para el EnmElec. las siguientes cantidades de material y equipo:

Material/Equipo	Cantidad	Material/Equipo	Cantidad
Radio HF PRC 2200	02	Radio VHF PRC 730	02
Radio HF PRC 6020	01	Radio VHF PRC 930	01
Radio HF PRC 8000	01	Unidad Control Local GRA 39	01
Bateria BA 30	108	Unidad Control Remoto GRA 39	08
Equipo de interceptación	01	Cable de Campaña WD-1/TT	1600m

4. Procedimiento de empleo de los medios de comunicaciones

El procedimiento de empleo se realizó en las instalaciones del Agrup Com “JO”, del Cuartel Mariano Melgar del Distrito de Tiabaya, Departamento de Arequipa, de la siguiente manera:

a. Verificación de la operatividad de los equipos de radio y unidades de control remoto.

b. Programación de los equipos de radio con parámetros de seguridad.

- Banda de frecuencia igual a los equipos de radio a cubrir.
- Tipo de emisión en secreto y salto de frecuencia.
- Potencia de salida media y alta.

c. Verificación de la transmisión y recepción de la señal.

d. Instalación de la Estación de Protección en la cual irá la Unidad de Control Local GRA 39 y el operador de radio.

e. Conexión de los 08 cables de campaña a la unidad de control local.

f. Se procede al despliegue de las 08 unidades de Control Remoto GRA 39 con las 08 estaciones de radio a 200m de la estación de protección y 50m entre estaciones (en operaciones dependerá de la distancia a considerar para la seguridad del Cecom).

g. Conexión de los 08 cables de campaña a las unidades de Control Remoto GRA 39, y posteriormente se interconectan con el cable de interconexión a las 08 estaciones de radio.

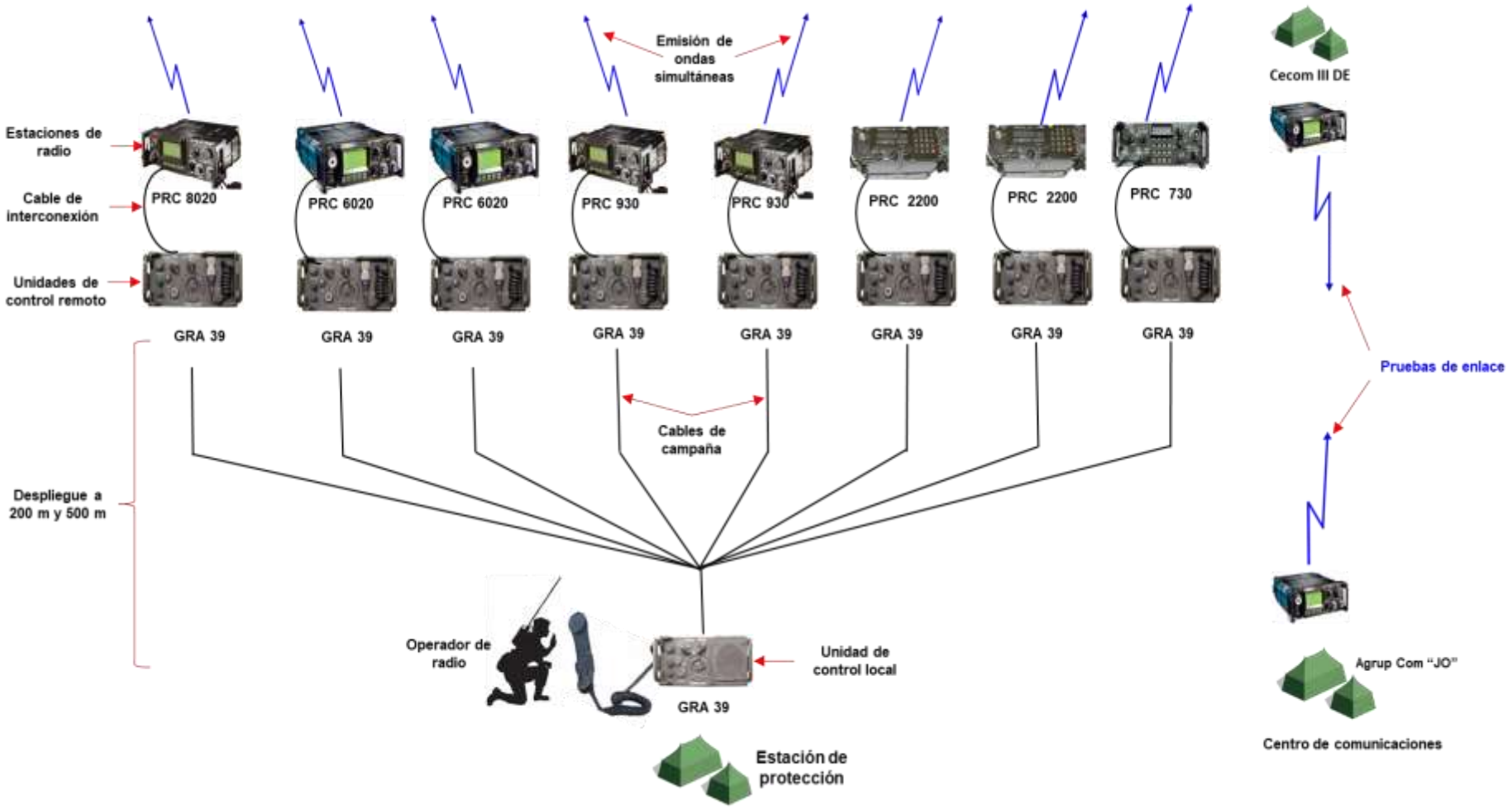
h. Se encienden las estaciones de radio y se procede a ser operadas de manera remota y simultánea a través del operador de radio que se encuentra en la Estación de Protección.

I Se procede a realizar ejercicios de enlace del Centro de Comunicaciones de la Gran Unidad con una o varias estaciones de otras grandes unidades.

j. Se procede a la instalación de la estación de interceptación.

Imagen 1

Esquema del proceso de integración de los equipos de comunicaciones manera remota

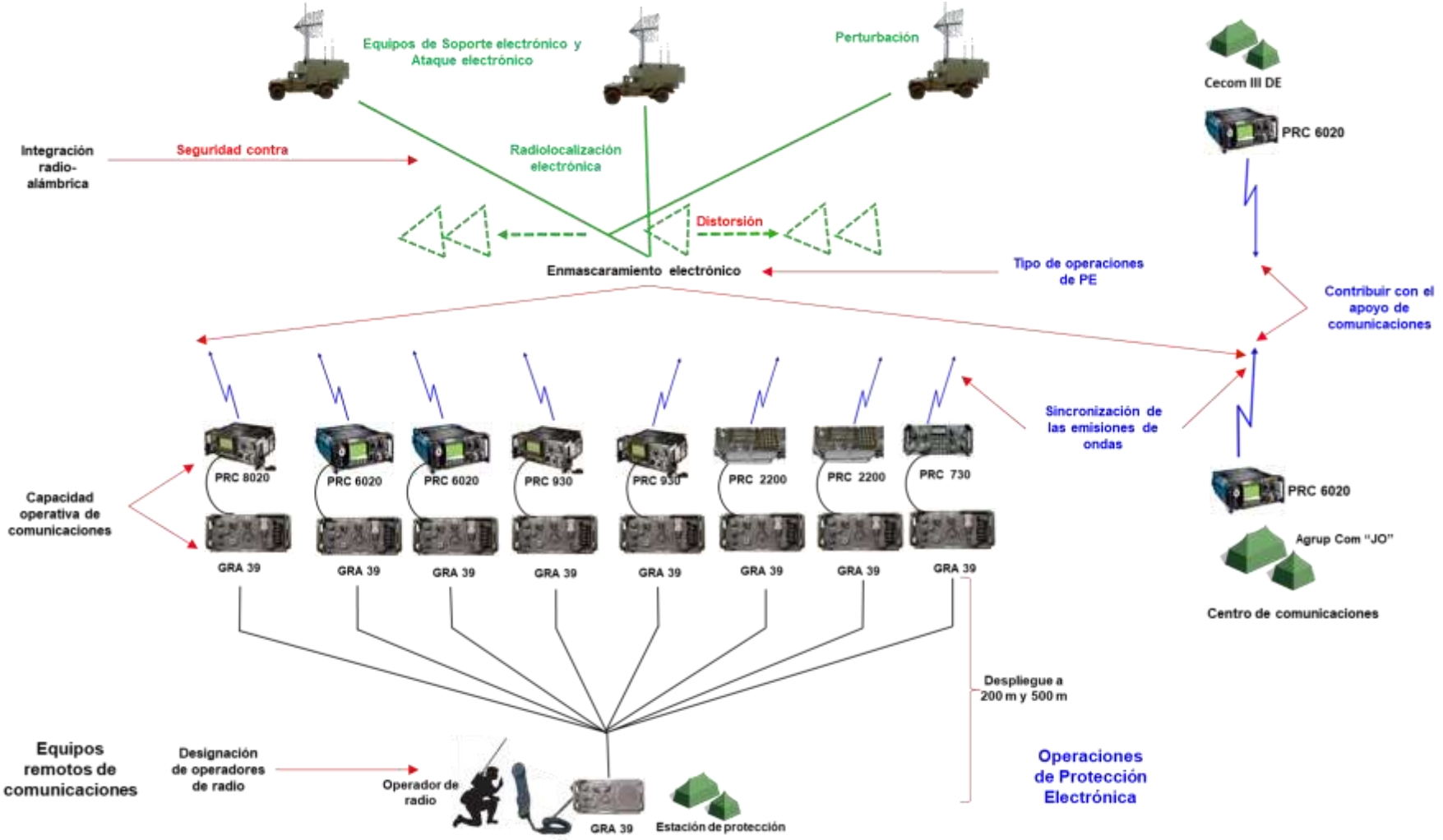


5. Procedimiento del Enmascaramiento Electrónico al apoyo de las comunicaciones

a. Inicio de las coordinaciones con el Centro de Comunicaciones de la gran unidad para determinar los horarios de reporte y/o reporte por orden del jefe de operaciones.
b. Se procede a los ejercicios de sincronización de las emisiones de la Estación de Protección con las emisiones del Centro de Comunicaciones.
c. Se verifica si la señal del Cecom es monitoreada por la estación de interceptación.
d. Se procede al Enmascaramiento Electrónico de la señal del centro de comunicaciones.
e. Se verifica si el monitor de la estación de interceptación logra visualizar la señal protegida; se logra ver la distorsión o enmascaramiento de la señal.
f. Se verifica si la señal del Cecom mantiene su flujo de información.

Imagen 2

Esquema general del empleo de los Equipos remotos de comunicaciones para incrementar las Operaciones de protección electrónica



6. Propuesta de inclusión en el Manual de Empleo de Guerra Electrónica. ME 11-221

Capítulo 6

Protección Electrónica (PE)

Sección I

Consideraciones Generales

6.2 Clasificación

e. El Enmascaramiento Electrónico, incluye acciones de Anti SE como Anti AE, así como las acciones nombradas en el párrafo “d”.

6.3 Fundamentos

e. La acción de EnmElec se realiza en operaciones, y requiere de gran entrenamiento, coordinación de manera de lograr la sincronización con las emisiones de los Cecom**,** con la finalidad de buscar el efecto deseado.

Sección III

Procedimientos Operacionales de Protección Electrónica

6.9 Consideraciones

c. Los procedimientos operacionales pueden ser:

3) Enmascaramiento Electrónico

6.10 Entrenamiento del operador

e. Entrenamiento en el empleo del Enmascaramiento Electrónico.

6.19 Enmascaramiento Electrónico

Anexo 1. Simbolos y Abreviaturas

a. Simbolos

2. Acciones e instalaciones de GE

Estación de Protección Electrónica  EnmElt

a. Abreviatura

Enmascaramiento Electrónico	EnmElt
Estación de Protección Electrónica	EPElt

Anexo 3. Lista de verificación de Protección Electrónica

1. Lista de verificación del Estado Mayor

r. ¿Se ha realizado instrucción y entrenamiento del Enmascaramiento Electrónico?

2. Lista de verificación de comunicaciones

a. ¿Emplean los operadores apropiadamente la Protección Electrónica? Como las que se menciona a continuación:

6) Sincronización de las emisiones de la EPElt con las emisiones del Cecom.

d. ¿Se ha establecido la cantidad de medios radiales para el EnmElt?

3. Lista de verificación de los operadores

j. ¿Conocen los operadores los procedimientos para realizar el EnmElt?

ANEXO 8

REPORTE DE SIMILITUD DE TURNITIN

turnitin **Identificación de reporte de similitud:** oid:12350:378164130

NOMBRE DEL TRABAJO
IFI- BACH. CH VELAZCO C (2).docx

AUTOR
VELAZCO CORNELIO

RECUENTO DE PALABRAS
38249 Words

RECUENTO DE CARACTERES
218680 Characters

RECUENTO DE PÁGINAS
146 Pages

TAMAÑO DEL ARCHIVO
18.3MB

FECHA DE ENTREGA
Sep 4, 2024 9:34 AM GMT-5

FECHA DEL INFORME
Sep 4, 2024 9:36 AM GMT-5

7% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 6% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 4% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado