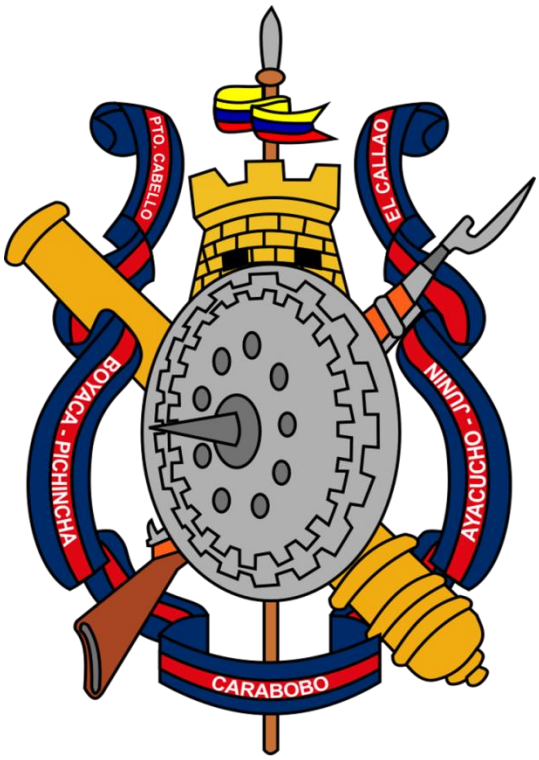
EJB-MT-004

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
FUERZA ARMADA NACIONAL BOLIVARIANA
EJÉRCITO BOLIVARIANO



DOCTRINA MILITAR BOLIVARIANA
(SUB-TAREA TERRESTRE)

MANUAL DE COMUNICACIONES DEL EJÉRCITO BOLIVARIANO

Caracas, 09 de febrero del 2026

Elaborado por el Grupo de Trabajo Organización y Doctrina de la Dirección de Apresto Operacional del Ejército Bolivariano y aprobado por la Sub-tarea “Terrestre”.

NO CLASIFICADO

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
FUERZA ARMADA NACIONAL BOLIVARIANA
EJÉRCITO BOLIVARIANO

DEL : MG. Comandante General del Ejército Bolivariano.
ASUNTO: Manual de Comunicaciones del Ejército Bolivariano

I. PROPÓSITO:

El objetivo de este manual es proporcionar un método o modelo de empleo de las Comunicaciones militares del Ejército Bolivariano en el marco de las 2da, 5ta y 6ta. Líneas estratégicas del Comandante en Jefe de la Fuerza Armada Nacional Bolivariana.

II. VIGENCIA:

Esta publicación entrará en vigencia a partir de la fecha de su promulgación y tendrá un lapso de aplicación de tres (03) años para su primera revisión.

III. DISTRIBUCIÓN:

Efectúese de acuerdo con la lista de distribución.

IV. INSTRUCCIONES ESPECIALES:

A. Las observaciones y aportes a este documento deberán enviarse por escrito al Comité de Doctrina del Ejército Bolivariano, para el análisis, revisión, modificación y publicación.
B. Este manual deja sin efecto cualquier otro documento que coliden con lo establecido en este.

Caracas, 11 de febrero del 2026.

JOHAN ALEXANDER HERNÁNDEZ LÁREZ
MAYOR GENERAL
COMANDANTE GENERAL DEL EJÉRCITO BOLIVARIANO

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

ÍNDICE

PÁG.

CARTA DE PROMULGACIÓN……..... 01

INTRODUCCIÓN……..... 01

CAPÍTULO I. DOCTRINA DE LAS COMUNICACIONES TÁCTICAS……..... 05

SECCIÓN A. GENERALIDADES……..... 05

1. Definición de términos…… 05
2. Responsabilidad por el establecimiento y mantenimiento de las comunicaciones…… 05
   a. Responsabilidad de comando…… 05
   b. Superior a subordinado…… 05
   c. Apoyante a apoyada…… 06
   d. Reforzante a reforzada…… 06
   e. Comunicaciones laterales……... 06
   f. Apoyo común de las comunicaciones…… 06
3. Principios de las comunicaciones…… 07
   a. Generalidades…….. 07
   b. Uso restringido…….. 07
   c. Medios apropiados……... 07
   d. Flexibilidad…… 07
   e. Dispersión……. 08
   f. Simplicidad operacional…….. 08
   g. Medios orgánicos……. 08
   h. Seguridad…….. 09
4. Medios de comunicaciones…… 09
   a. Consideraciones básicas…… 09
   b. Mensajeros…… 10
   c. Clases de mensajeros……. 11

d. Empleo de los mensajeros…….. 11
5. Comunicaciones visuales…….. 12
a. Banderas…… 12
b. Luces…….. 13
c. Pirotécnica…… 13
d. Paineles……. 14
6. Comunicaciones acústicas…… 14
7 Comunicaciones por radio y alambre…… 15
8. Comunicaciones por radio…….. 15
a. Capacidades y limitaciones……. 16
b. Características del radio…….. 16
c. Seguridad…….. 17
d. Capacidad de manejo de los mensajes en una red…… 18
e. Control remoto…….. 18
f. Integración radio-alámbrica (IRA)…….. 18
g. Radio silencio…… 19
h. Retransmisiones……... 20
9. Comunicaciones alámbricas…….. 20
a. Alcance…….. 21
b. Tiempo requerido para su instalación…… 21
c. Empleo……... 22
d. Sistemas de radio relevo……. 22
10. Comunicaciones pictóricas y audiovisuales…… 23
a. Fotografía…….. 23
b. Fax…….. 23
c. Televisión……..... 23
d. Empleo……..... 24
11. Dispositivos auxiliares……. 25

CAPÍTULO II. SEGURIDAD DE LAS COMUNICACIONES…… 27
SECCIÓN A. PROTECCIÓN DE LAS COMUNICACIONES……. 27
1. Responsabilidad…….. 27
2. Niveles de responsabilidad…… 27
a. Alto mando y liderazgo……. 27
b. Departamentos y unidades especializadas…….. 28
c. Todo el personal militar…… 28
d. Principios fundamentales…… 29
e. Componentes de la seguridad de las comunicaciones…….. 29
f. Medios y protocolos de comunicación seguros…… 30
g. Amenazas a la seguridad de las comunicaciones…… 30
3. Importancia de la seguridad de las comunicaciones militares….. 31
SECCIÓN B. CLASIFICACIÓN DE SEGURIDAD…….. 31
1. Políticas básicas…….. 31
2. Responsabilidad de la clasificación…….. 32
3. Propósito de la clasificación……... 32
4. Designación de clasificación…….. 33
5. Autoridades clasificadoras……. 35
a. Clasificación…….. 35
b. Reclasificación…….. 36
6. Acceso…….. 36
7. Otorgamiento del acceso…… 37
8. Registro de acceso…….. 40
9. Acceso de emergencia…… 41
10. Autorización para acceso limitado……. 42
SECCIÓN C. SEGURIDAD FÍSICA…….. 43
1. Normas de control y clasificación…….. 44
2. Material secreto, confidencial y reservado……... 45

3. Papeles de trabajo, cintas de máquinas de escribir, diskettes…. 46
4. Requerimientos de seguridad para el almacenaje de publicaciones……..... 47
5. Seguridad física de las ayudas criptográficas……. 47
6. Seguridad física de equipos de comunicaciones e informática… 48
SECCIÓN D. SEGURIDAD DE TRANSMISIÓN …….. 49
1. Definición…….. 49
2. Principios generales…… 49
3. Seguridad de radio…….. 51
4. Política de emisiones…….. 52
5. Responsabilidades para la elaboración del plan de control de emisión…….. 55
SECCIÓN E. SEGURIDAD CRIPTOGRÁFICA…….. 55
1. Definición…….. 55
2 Criptograma……. 55
3. Principios generales…… 56
4. Clasificación apropiada…….. 58
5. Redacción…… 58
6. Selección del sistema criptográfico…….. 60
7. Criptografía…….. 60
8. Parafraseado…… 62
CAPÍTULO III. SEGURIDAD INFORMÁTICA…… 64
SECCIÓN A. SEGURIDAD INFORMÁTICA…… 64
1. Modelo de seguridad informática para la FANB……. 64
2. Organización…… 66
3. Análisis y gestión de riesgos……. 68
4. Política de seguridad…….. 70
5. Auditoría y control de seguridad…… 71
6. Plan de contingencia…….. 72
7. Seguridad de red extremo a extremo…… 73

8. Seguridad física y lógica…… 75
SECCIÓN B. VIOLACIONES DE SEGURIDAD…… 77
1. Generalidades…… 77
2. Compromiso…… 77
3. Otras violaciones de seguridad…… 78
4. Medidas disciplinarias…… 78
CAPITULO IV. COMUNICACIONES SATELITALES…….. 81
SECCIÓN A. GENERALIDADES…… 81
1. Componentes principales…….. 81
2. Funcionamiento básico…….. 81
3. Características clave……... 81
4. ¿Cómo funcionan las comunicaciones satelitales?..... 82
5. Definición de términos…… 83
6. Beneficios de la comunicación satelital…… 85
7. Tipos de satélites…… 85
8. Consideraciones básicas de seguridad …….. 87
9. Uso de la comunicación satelital para la defensa integral de la nación…… 88
CAPITULO V. EQUIPOS Y SISTEMAS DE COMUNICACIONES …….. 92
SECCIÓN A. ANTENAS DE CAMPAÑA, LA IMPROVISACIÓN ES EL TRABAJO DE CAMPO…… 92
1. Expediente de campaña…… 92
2. Carta de referencia rápida, longitud de antenas…… 94
3. Tipos de antenas …… 95
SECCIÓN B. MICROTELEFONOS…….. 111
1. Mantenimiento…… 111
2. Procedimiento…… 111
a. Prueba cable resortado…… 112
b. Conexión de la toma de audio…… 112
3. Mantenimiento de la carcasa…… 113

4 Prueba PTT…….. 114
SECCIÓN C. EQUIPOS Y SISTEMAS DE COMUNICACIONES…… 115
1. AN-PRC 660 UV…….. 115
2. Características principales……. 115
3 Radio vehicular VRC-240 UV……. 121
4. Componentes principales…….. 122
5. Radio transmisor receptor UV-9R……. 127
6. Descripción…….. 127
7. Características, funciones e instalación…….. 127
8. Precauciones generales de seguridad en la operación y mantenimiento de los equipos……... 133
9. Especificaciones del radio Motorola PRO-7100……. 134
10. Mantenimiento preventivo…….. 135
11. Radio transmisor receptor radio quansheng UV – K5…….. 137
12. Características principales……..... 137
13. Radio transmisor receptor EP-450…… 147
14. Introducción, alcance, descripción general……. 147
15. ICOM IC-A110…….. 157
16. Características, instalación, mantenimiento y operación…….. 158
17. Motorola PRO-5100…… 164
18. Características, instalación, mantenimiento y operación…….. 164
19. Sistema trasportable de comunicaciones N° 3 “Agraz”…… 170
20. Características, instalación, mantenimiento y operación…….. 171
21. Sistema de comunicaciones de alta movilidad “D&R Atanasio Girardot”…… 181
22. Características, instalación, mantenimiento y operación…….. 182
23. Sistema de comunicaciones móvil “TONY” 186
24. Características, instalación, mantenimiento y operación…….. 186
25. Sistema de comunicaciones integrado “SICOIN ESEQUIBO”… 192
26. Características, instalación, mantenimiento y operación…….. 193

CAPITULO VI. COMUNICACIONES AUDIOVISUALES…….. 202

SECCIÓN A. COMUNICACIONES PIROTÉCNICAS AUDIOVISUALES……. 202

1. Elementos clave…….. 202
2. Comunicaciones multimedia o digital…….. 203
3. Fotografía y video…… 204
4. Televisión y streaming…… 204
5. Instantaneidad y cobertura……. 205
6. Empleo táctico y estratégico……. 207

CAPITULO VII. FUNDAMENTOS Y MEDIOS DE LAS COMUNICACIONES ALÁMBRICAS……. 208

SECCIÓN A. SONIDO Y TELEFONÍA…….. 208

1. Naturaleza del sonido…… 208
2. Ondas sonoras……. 209
3. Características de las ondas sonoras…….. 210
4. Armónicos…… 212
4. Características del sonido…….. 213
5. Frecuencias de las voces……... 215

SECCIÓN B. PROBLEMA BÁSICO DE LA TELEFONÍA. CIRCUITO TELEFÓNICO SIMPLE. MESA DE CONMUTACIÓN…… 214

1. Problema básico de la telefonía…… 215
2. Sistema telefónico…….. 217
3. Oficina telefónica…… 218

SECCIÓN C. CLASIFICACIÓN DE LOS SISTEMAS TELEFÓNICOS. SISTEMA TELEFÓNICO MANUAL. SISTEMA DE BATERÍA LOCAL Y BATERÍA COMÚN. SISTEMA TELEFÓNICO AUTOMÁTICO. COMPARACIÓN DE LOS SISTEMAS TELEFÓNICOS…… 218

1. Clasificación de los sistemas telefónicos…… 219
2. Sistema telefónico Manual…… 219
3. Sistema de batería local……. 219
4. Sistema de batería común…….. 220
5. Sistema telefónico automático…….. 223

6. Comparación de los sistemas telefónicos…… 223

7. Sistemas telefónicos automáticos……. 224

SECCIÓN D. CIRCUITOS DE UNA MESA DE CONMUTACIÓN DE UN SISTEMA DE BATERÍA LOCAL. OPERACIÓN DE UNA MESA DE CONMUTACIÓN. FUNCIÓN DE LOS JACK. CIRCUITOS DE UNA MESA DE CONMUTACIÓN DE UN SISTEMA DE BATERÍA COMÚN……. 225

1. Circuitos de línea…… 225

2. Circuitos troncales…… 225

3. Circuitos de cordón…… 225

4. Circuitos comunes…….. 226

5. Operación de una mesa de conmutación de batería local……. 227

6. Los Jack de la mesa le conmutación…… 228

7. Lámpara piloto……. 231

8. Circuito conmutador del generador…….. 232

SECCIÓN E. MEDIOS ALÁMBRICOS DE CAMPAÑA…….. 233

1. Características generales de todo alambre de campana……. 233

2. Alambre de campaña WD-1/TT……. 234

3. Empalme de campana…… 234

4. Equipos de tendido y recuperación…….. 235

5. Bobinas de repetición……. 236

6. EJE RL-27…… 237

7. Amarre del alambre de campaña……..... 240

8. Atadura de nudo y lazo…… 241

9. Teléfonos de campaña…… 242

10. Teléfono de campaña TA-312/PT……. 245

11. Teléfono de campaña TA-427 BD……... 246

12. Teléfono de campaña TA-427 BR……. 247

13. Central telefónica SB-993…….. 250

14. Central telefónica manual SB-86/P…….. 251

15. Central telefónica de campaña SB-22/PT…… 253

16. Tipos de centrales telefónicas administrativas…… 260
17. Como está estructurada una central telefónica…….. 262
18. Herramientas básicas para trabajar en la telefonía…… 266
19. Código de colores fibra óptica…….. 266
CAPÍTULO VIII. SEGURIDAD DE LAS COMUNICACIONES Y CIBERDEFENSA…… 274
SECCIÓN A. MARCO DOCTRINAL DE LA CIBERSEGURIDAD…….. 274
1. Alcance y definición……. 274
2. El ciberespacio como dominio de guerra…… 275
3. Los tres pilares de la seguridad de comunicaciones……. 275
4. Principios de mínimo privilegio…….. 276
5. Segmentación y arquitectura de confianza cero…… 277
6. Protección del tráfico y detección de intrusiones…… 278
7. Gestión de la configuración y vulnerabilidades…….. 278
8. Seguridad lógica de los terminales…….. 279
9. Control de medios extraíbles……. 280
10. Inteligencia artificial (IA) como habilitador operacional…… 281
11. IA para la gestión dinámica del espectro electromagnético……. 281
12. IA en ciberseguridad, defensa predictiva…… 282
13. Respuesta y continuidad operacional cibernética……. 283
14. Recuperación de desastres y respaldo de información crítica…. 283
15. Deberes del operador ante la sospecha de intrusión…… 284
CAPITULO IX. COMUNICACIONES ALTERNATIVAS…… 287
1. Generalidades……. 287
1. Tipos de comunicaciones militares……... 287
2. Importancia de las comunicaciones alternativas…… 288
SECCIÓN A. LAS COMUNICACIONES MILITARES ALTERNATIVAS……. 289
1. Tipos y tecnologías……. 289
2. Importancias…… 290

3. Desafíos……..…... 290
SECCIÓN B. LAS COMUNICACIONES MILITARES ALTERNATIVAS…… 290
1. Términos prácticos…… 291
2. Importancia de las comunicaciones militares alternativas..…… 291
3. Ejemplos y tipos de comunicaciones militares alternativas …… 291
4. Por alcance…….…… 292
5. Por contexto operacional…….…..... 292
6. Factores a considerar al diseñar las comunicaciones militares alternativas…..…….. 293
7. Desafíos y limitaciones…..……. 294
SECCIÓN C. ESTACIÓN DE RADIO COMUNITARIAS…… 295
1. Marco histórico…...…….…… 295
2. Conceptos básicos……...…… 298
3. Características……. 301
SECCIÓN D. RADIOAFICIONADO...……..…… 302
1. Definición…….……. 302
2. Tipos de permisos……..……. 304
3. Aspectos claves ……. 304
4. Operación de las operaciones de radioaficionados…..……. 305
5. Distintivos de llamadas…….……. 307
6. Eventos especiales……..……. 308
7. Inspecciones……..…….. 309
8. Sanciones……..……. 309
CAPÍTULO X. ASPECTOS FUNDAMENTALES DE OPERACIONES ELECTROMAGNÉTICAS…….. 312
SECCIÓN A. CONCEPTO DE OPERACIONES ELECTROMAGNÉTICAS……. 312
1. División para su aplicación…..……..……. 312
2. Tipos de interferencias……..…… 313
3. Ejemplos de interferencias…..…….. 313
4. Supresión de defensas aéreas enemigas ……..... 314

5. Objetivos de la operación…….…….. 314
5. Origen y desarrollo.……...…….. 315
7. Ejemplos históricos…..……..…….. 315
8. Guerra de los navegadores (tecnológicos)……...…….. 316
9. Importancias estratégicas de la guerra de navegación…...…….. 317
10. Vulnerabilidades y amenazas……..……...…….. 318
11. Pulso electromagnético…..……..……. 319
12. Protección electromagnética……...……. 323
13. Medidas de defensa……..……. 325
14. Guerra electrónica y defensa……...…...……. 330
15. Dependencia del adversario en la exploración radioelectrónica……..……..…….. 331
CAPÍTULO XI. VEHÍCULOS NO TRIPULADOS…….. 334
SECCIÓN A. AÉREOS, TERRESTRES Y MARÍTIMOS…… 334
1. Generalidades……..……..……. 334
2. Vehículos aéreos no tripulados……...……. 339
3. Empleo de los vehículos aéreos no tripulados…….. 343
4. Operaciones electromagnéticas…….. 345
5. Vehículos terrestres no tripulados…..…….. 348
6. Empleo de los vehículos terrestres no tripulados ……..... 350
7. Vehículos marítimos no tripulados……..…….. 351
CAPÍTULO XII. SISTEMA DEFENSIVO TERRITORIAL……..... 356
SECCIÓN A. GENERALIDADES…….. 356
1. Conceptos y alcances……..……..……. 356
2. Estructura de mando y control…….……...…….. 356
3. Componentes claves……..……..……. 357
4. Trinomio estratégico C3 comando, control y comunicaciones.…….……..……. 357
5. Rol del oficial de comunicaciones…..……..……. 358

6. Comunicaciones con la población y cuerpo de reserva (el tejido social)…….....…… 360
7. Guerra psicológica y de la información…….. 361
8. Desafíos y vulnerabilidades del sistema……..……..…… 362
9. Ejemplos prácticos de su empleo……..……..……. 363
SECCIÓN B. COMUNICACIÓN POR SEÑALES VISUALES……. 372
1. Comunicación por señales visuales ……..…… 372
2. Introducción…….……. 372
3. Justificación ……..……..…….. 373
4. Señales de brazos y manos…….. 374
CAPÍTULO XIII. CENTROS DE COMUNICACIONES ……..... 378
SECCIÓN A. GENERALIDADES ……. 378
1. Propósito……..……..…… 379
2. Responsabilidades……..……..……..…… 379
3. Normas generales.…….……..……... 379
4. Marco legal.……..…….....…..... 380
5. Empleo de los centros de comunicaciones..……..... 383
6. Alcance……. 384
7. Centro general de tecnología de información y las comunicaciones ……. 385
8. Centro local TIC……. 386
9. Sub - centro local TIC…….. 387
10. Procedimientos de los centros de comunicaciones…….. 388
11. Normas de los centros de comunicaciones……. 389
REFERENCIAS BIBLIOGRÁFICAS……..... 397

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

NTRODUCCIÓN

La República Bolivariana de Venezuela, es irrevocablemente libre e independiente y tiene como derechos irrenunciables la independencia, la libertad, la soberanía, la inmunidad, la integridad territorial y la autodeterminación nacional, según lo establecido en su Carta Magna (Art. N° 1), en consecuencia, existe un máximo órgano encargado de planificar, programar dirigir, ejecutar y controlar todas las estrategias operacionales necesarias para el cumplimiento de los derechos de la Nación anteriormente mencionados, el cual es el Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana (CEOFANB).

En nuestro país, en los últimos años han ocurrido algunos cambios revolucionarios y drásticos observados en la nueva realidad política, social, económica y militar, que afronta al ser blanco de interés del Imperio Norteamericano y de algunos de sus aliados en el mundo donde con bloqueos y sanciones, guerra mediática, entre otras amenazas impiden el desarrollo normal de nuestra Nación, es allí donde el rol de la Fuerza Armada Nacional Bolivariana es vital para el desarrollo integral de la nación y la Seguridad de la Nación, esto muy bien se puede observar en nuestra Constitución de la República Bolivariana de Venezuela donde nos habla en su artículo N° 326, la seguridad de la Nación se fundamenta en la corresponsabilidad entre el Estado y la sociedad, y en el artículo N° 328, donde nos habla sobre las tareas y misiones de la FANB, garantizando la Independencia y soberanía de la Nación y asegurar la integridad del espacio geográfico, mediante la defensa militar, la cooperación en el mantenimiento del orden interno y la participación activa en el desarrollo nacional, aunado a todas las Leyes y Reglamentos que nos dictan los deberes y derechos y los Planes del Estado para librar cualquier conflicto armado.

Las Comunicaciones Militares han jugado un papel muy importante en las guerras. Proveen los medios para la transmisión de información obtenida del reconocimiento y otras unidades en contacto con el enemigo y también los medios para ejercer el comando mediante el envío de órdenes e instrucciones del

comandante a sus subordinados. Comprende todos los medios para transmitir mensajes, órdenes y reportes tanto en el terreno, el aire, el mar y entre un Puesto de Comando e instalaciones distantes y barcos.

El Oficial de Comunicaciones emplea los sistemas modernos de comunicaciones y hace uso de las herramientas de HF, VHF, UHF, Comunicaciones Satelitales (SATCOM) y aprovecha las capacidades únicas que ofrecen cada una de ellas para cumplir sus requerimientos.

¿Qué desafíos les esperan a los equipos de comunicaciones tácticos militares en el siglo XXI?. La respuesta a esto puede encontrarse mirando observando los cambios que han surgido en el campo de batalla moderno. Durante la Guerra del Golfo, fuimos testigos del dramático incremento en el ritmo operativo del campo de batalla. Las comunicaciones de comando y control se perdieron mientras las fuerzas militares se movían rápidamente a través del abierto escenario del desierto, sobrepasando los sistemas de comunicaciones militares convencionales. El incremento en el flujo de información demanda el uso de comunicaciones de datos en lugar de las comunicaciones de voz, con una red siempre creciente de ancho de banda. La información crítica del campo de batalla debe fluir de forma horizontal y vertical, impulsando la necesidad de una red de tráfico entre redes tácticas.

Surge también la imperiosa necesidad del conocimiento situacional, o sea conocer la ubicación precisa de los recursos y personal militares. Mientras el tamaño de las fuerzas se reduce por los recortes en el gasto militar, el conocimiento situacional exacto es la clave para mantener un nivel dominante de fuerza letal. En el futuro, el conocimiento situacional se convertirá en la tarea de fondo de la estructura de comunicaciones de comando y control. La información de ubicación física será anexada con seguridad a todo el tráfico de voz y datos y encaminada hacia un punto de recolección de conocimiento situacional, de modo que los mandos militares puedan planificar y llevar a cabo una campaña exitosa.

Desde sus inicios, las radiocomunicaciones utilizaron el código Morse para las comunicaciones. A través del tiempo, se desarrollaron técnicas mejoradas para la transmisión de datos tomando en consideración la variabilidad del medio y el gran incremento de la velocidad a la cual ocurre la transmisión de datos sobre un enlace de radio. A medida que fue pasando el tiempo, se fue olvidando el uso de técnicas de transmisión y ya no se enseñan a nuestro personal, haciéndonos aún más vulnerables a ser interferidos y quedarnos sin comunicaciones efectivas, es por ello que se hace imperioso volver a retomar estas metodologías para hacerle frente a las adversidades que puedan afectar el flujo de comunicaciones.

La información aquí presentada es susceptible de mejoras y de modificaciones que conlleven a hacer este manual lo más actualizado posible. En este sentido, cualquier sugerencia que sirva para incrementar la calidad del mismo será bien recibida en la Dirección de Tecnología de la información y las comunicaciones del Ejército Bolivariano.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO I

DOCTRINA DE LAS COMUNICACIONES TÁCTICAS.

SECCIÓN A

1. DEFINICIÓN DE TÉRMINOS.

El término de comunicaciones tácticas corresponde aquellos sistemas y medios de comunicaciones que sirven a los elementos del Ejército de operaciones, ellos son empleados desde los comandos del Teatro del Ejército hasta los niveles más bajos de las Unidades de Combate, de las Unidades de Apoyo de Combate y Unidades de Apoyo de Servicio, están sujetas a las mismas prerrogativas locales como se aplica el comando, control y apoyo de todas las operaciones de combate. Ellos son generalmente de corto alcance. Las comunicaciones tácticas, normalmente emplean equipos portátiles, transportables o móviles, orgánicos de las unidades que operan.

2. RESPONSABILIDAD POR EL ESTABLECIMIENTO Y MANTENIMIENTO DE LAS COMUNICACIONES.

a. Responsabilidad de Comando.

El comandante es responsable personalmente por las comunicaciones de su unidad, sin embargo, es el personal de comunicaciones orgánico quien cumple con el establecimiento, operación y mantenimiento del sistema de comunicaciones.

b. Superior a Subordinado.

El comandante de un escalón superior o una unidad superior es responsable por el establecimiento y mantenimiento de las comunicaciones hacia una unidad de un escalón inferior a una unidad subordinada. Una unidad agregada es considerada subordinada al

comando al cual está agregada, con respecto a establecer la responsabilidad por las comunicaciones.

c. Apoyante a Apoyada.

El comandante de una unidad que apoya es responsable por el establecimiento y mantenimiento de las comunicaciones hacia la unidad apoyada.

d. Reforzante a Reforzada.

Una unidad que tiene una misión de refuerzo es responsable por el establecimiento y mantenimiento de las comunicaciones hacia la unidad que está siendo reforzada.

e. Comunicaciones Laterales.

La responsabilidad por el establecimiento de las comunicaciones entre unidades adyacentes puede ser fijada por el comandante próximo superior o puede ser establecida en el Procedimiento Operativo Vigente (P. O. V.).

En la ausencia de órdenes específicas para fijar la responsabilidad, el comandante de la unidad de la izquierda es responsable por el establecimiento de las comunicaciones con la unidad a la derecha.

f. Apoyo Común de las Comunicaciones.

Las tropas de comunicaciones son responsables por instalar y operar las comunicaciones de uso común para las Unidades de Combate, Apoyo de Combate y Unidades de Apoyo de Servicio. Tales comunicaciones complementarán, pero no duplicarán las capacidades orgánicas de comunicaciones de las unidades y serán de acuerdo con los requisitos tácticos, administrativos y logísticos de las unidades. Los centros de comunicaciones en los sistemas de comunicaciones tácticos, son normalmente responsables por establecer y mantener todas las facilidades de extensión, desde el centro de las unidades en la vecindad.

3. PRINCIPIOS DE LAS COMUNICACIONES.

a. Generalidades.

Los principios básicos aplicables a las comunicaciones son derivados de los principios fundamentales de la guerra. La extensión, hasta donde cualquier principio puede ser aplicable, variará con la situación táctica y el juicio del comandante.

b. Uso Restringido.

Los medios de comunicaciones de la unidad son para el uso exclusivo del comandante y aquel personal que él designe. El empleo de tales medios es mantenido al mínimo de acuerdo con la misión u objeto del comandante, la aplicación de este principio no es para fomentar una actitud conservadora hacia el empleo total de los medios disponibles, sino para desanimar el uso de tales medios en propósitos diferentes. Ellos existen como un instrumento del comandante y su estado mayor y no como una conveniencia general para el comando.

c. Medios Apropiados.

Ciertos medios de comunicaciones son más efectivos que otros, bajo circunstancias dadas. La selección del medio más apropiados es hecha, tomando en consideración factores tales como: urgencia operacional, tiempo de instalación, tiempo de transmisión, susceptibilidad a la acción del enemigo, confiabilidad y costo en los recursos. El control es comprometido cuando se depende de unos pocos medios y es fortalecido cuando la confianza es dispersa en una variedad de medios. En la selección del medio más apropiado, la principal consideración es siempre la urgencia del requerimiento operacional.

d. Flexibilidad.

Los medios de comunicaciones y el sistema para su empleo deben ser flexible y capaz de soportar el grado de refuerzo, al que pueda estar sujeto razonablemente al comando, en tiempo de guerra. La amplia dispersión de las unidades con sus habilidades para movimientos

rápidos, requiere un sistema de comunicaciones flexible que pueda ajustarse rápidamente a los cambios en la misión, situación táctica y operaciones diversas.

e. Dispersión.

Las facilidades de comunicaciones están ubicadas y desplegadas de una manera, que proporcione al enemigo un objetivo no beneficioso y un mínimo de información de orden de batalla. Las unidades tácticas se despliegan de acuerdo con sus misiones y la amenaza hostil. Así, las facilidades de comunicaciones se dispersan de acuerdo con las unidades que sirven. Alguna concentración de las facilidades de comunicaciones en los escalones del comando, puede aumentar el control operacional; sin embargo, las grandes concentraciones son evitadas, debido a que ellas aumentan el problema de interferencia mutua y la probabilidad de detección por parte del enemigo.

f. Simplicidad Operacional.

Sin tomar en cuenta la complejidad técnica interna, los sistemas de comunicaciones y equipos deben ser simples operacionalmente. El incremento en la complejidad de los sistemas de comunicaciones y equipos, requiere énfasis en la simplificación de los procedimientos operacionales. De otro modo, se encontrarán retardos en la adquisición e intercambio de información y un alto requerimiento de entrenamiento será impuesto al personal operativo.

g. Medios Orgánicos.

Los medios de comunicaciones de las unidades de combate, apoyo de combate de las brigadas y unidades tácticas, son generalmente orgánicos. Las comunicaciones de la división, comandos superiores y las organizaciones de combate de apoyo de servicio de tamaños comparables, son normalmente proporcionadas por un sistema de usuarios comunes, instalado y operado por unidades de comunicaciones. Esto incluye las comunicaciones internas de los varios escalones del comando respectivo, así como las facilidades de interconexión. A las

unidades se les proporciona las capacidades de comunicaciones por las tablas de organización y equipos que las gobiernan.

De modo, que hasta donde sea práctico, los medios de comunicaciones se hacen orgánicos a los niveles sucesivos del comando, en vez de ser mantenidos en el comando superior para una asignación subsecuente o ser agregados a un escalón inferior del comando. La aplicación de este principio no es alterada por la presencia de cualquier tipo de sistema de comunicaciones de usuario común. En realidad, los medios orgánicos de las unidades más pequeñas y los sistemas de comunicaciones en los niveles superiores, deben ser completamente compatibles para su integración como una sola entidad.

h. Seguridad.

La máxima seguridad de las comunicaciones es obtenida mediante el empleo de cualquier protección, de acuerdo con los requerimientos operacionales. La seguridad efectiva depende de un balance apropiado, entre los controles de seguridad y la urgencia operacional. La seguridad estricta debe ser observada en todo momento en las situaciones estáticas mientras que, en las fluidas las situaciones de combate el relajamiento de la seguridad puede ser forzado por las condiciones. En una situación de combate, el comandante decide, si la urgencia de enviar una información clasificada en texto claro, sobre-pesa el valor de la información para el enemigo. El comandante no permite el relajamiento de las medidas de seguridad, donde tal acción pueda resultar, en el comprometimiento de los planes de un comandante superior o de un sistema criptográfico, fuera de su comando inmediato.

4**.** MEDIOS DE COMUNICACIONES.

a. Consideraciones Básicas.

Los medios de comunicaciones de una unidad pueden estar constituidos por ópticos, acústicos, radio, alambre, gráficos, audio-visuales, mensajeros, etc. Depende normalmente del personal, equipo y

transporte, proporcionado sus tablas de organización y equipo. Los medios tienen capacidades y limitaciones diferentes y consecuencialmente, son empleados para complementarse unos con otros, de modo que se ponga una dependencia excesiva en el uso de un solo medio. De esta manera, la confiabilidad de un sistema de comunicaciones es incrementada grandemente.

Generalmente los medios empleados en cualquier situación táctica, son aquellos que proporcionen la máxima confiabilidad, seguridad y rapidez con un mínimo de esfuerzo y material. El grado de énfasis que se dé a cualquiera de estas cualidades principales de comunicaciones, varia continuamente en relación con las otras, bajo las variadas situaciones y condiciones.

La confiabilidad en las comunicaciones: Es aquella probabilidad de un dispositivo de comunicaciones, que ejecuta su misión adecuadamente bajo las condiciones operativas que se esperan encontrar, en una variedad de situaciones tácticas y no tácticas. Para asegurar confiabilidad en las comunicaciones tácticas, tiene que haber un adecuado planeamiento para minimizar las interrupciones.

La seguridad de comunicaciones: Incluye cripto-seguridad, seguridad física y seguridad de transmisión.

La rapidez en las comunicaciones: Es esencial para poner las informaciones o instrucciones requeridas en posesión de la agencia apropiada, para permitirle tomar la acción en el menor tiempo posible. La velocidad es lograda por la acción en el menor tiempo posible. La velocidad es altamente deseable, pero no necesariamente como para sacrificar la confiabilidad o la seguridad.

b. Mensajeros.

El mensajero es el medio de comunicaciones confiable y está disponible a todas las unidades. Es el método más efectivo para la transmisión y entrega de mensajes largos y artículos voluminosos. La eficiencia de la comunicación por mensajero depende de la selección y

entrenamiento de los mensajeros. Es flexible y confiable, su velocidad depende del modo de desplazamiento, de la situación táctica, del terreno y de la transitabilidad de las rutas.

Los mensajeros tienen algunas limitaciones, son vulnerables en las áreas adelantadas y no permiten la conversación de persona a persona.

c. Clases de Mensajeros.

Los mensajeros están clasificados generalmente, como mensajeros a horario y mensajeros especiales, así como también de acuerdo con su modo de transporte (p. ej., mensajero motorizado a horario, mensajero aéreo especial, mensajero a pie a horario, etc). Los mensajeros horarios son utilizados cuando las ubicaciones no cambian frecuentemente y la cantidad de tráfico justifica una rutina programada. Los mensajeros especiales son utilizados siempre que se requieran para entregar mensajes que requieren una acción más rápida o manejo especial.

d. Empleo de los Mensajeros.

Los mensajeros son orientados sobre la ruta, velocidad de desplazamiento, ubicación de los puntos de entrega y si debe esperarse una respuesta. Los mensajeros muy importantes pueden ser enviados por más de una ruta y/o por mensajes dobles. Los mensajeros dobles son usados normalmente cuando las condiciones del combate son extremadamente peligrosas y cuando haya dudas acerca de que un mensajero alcance exitosamente su destino. Ellos deben mantenerse a la vista uno de otro, pero lo suficientemente separados para evitar una destrucción simultánea o captura.

Un reconocimiento previo de las rutas propuestas de los mensajeros, debe ser hecho cuando sea práctico, para asegurar que son utilizables durante el día y durante la noche. Puestos de relevo de mensajeros pueden ser establecidos, cuando los mensajeros son llevados frecuentemente entre los mismos puntos o unidades, y la distancia, el terreno difícil y la actividad hostil, así lo justifica.

Clase de Mensajero	Promedio de viaje (en Km/h)	
	Diurno	Nocturno
Mensajero a pie.	5 o 8	2 o 4
Mensajero Motorizado.	60 o 80	30 o 50
Mensajero Aéreo.	130 o más	130 o más

Tabla 1 Promedio de Viaje en (Km/h).

5. COMUNICACIONES VISUALES.

Las comunicaciones visuales son un medio disponible a todas las unidades. Estas comunicaciones son hechas por banderas, luces, artificios pirotécnicos, paineles, señales de brazo y mano y otros medios visuales, pre-arreglados tales como maniobra de aviones etc. Ellas son apropiadas para transmitir rápidamente mensajes pre-arreglados sobre cortas distancias, así como para reconocimientos e identificación de fuerzas amigas. Las señales visuales son mal entendidas fácilmente, son muy vulnerables a la intercepción, y el enemigo puede usar similares para propósitos de engaños y confusión. Su uso es restringido durante periodos de poca visibilidad o cuando no están disponibles ubicaciones de líneas de vistas y pueden ser prohibidas por razones de seguridad. Sin embargo, ellas no pueden ser interceptadas de la misma manera que las comunicaciones por radio o teléfonos y son de valor para algunos usos de control especial y reconocimiento, particularmente durante los periodos de radio silencio.

a. Banderas.

Los mensajes pueden ser enviados por señales de banderas mediante el uso de señales pre-establecidas, el alfabeto de semáforos u ondeando representaciones de los caracteres del Código Internacional Morse. En adición donde se empleen vehículos anfibios del ejército o lanchas de desembarcos en cruces de ríos u operaciones de costa a costa, pueden usarse banderas de código internacional o banderas especiales de la marina.

b. Luces.

Aunque las luces para propósitos de comunicaciones no son usualmente un artículo de la TOE; existen varios tipos disponibles. Ellas pueden ser usadas para enviar mensajes pre-arreglados, tales como la identidad de unidades amigas, basadas en el significado dado en el I.O. C. de la unidad o como lo prescriba el comandante. Los mensajes en código internacional Morse pueden ser transmitidos por luces. Dispositivos infrarrojos, tales como filtros infrarrojos y pantallas direccionales, también son empleados para señales y como ayudas para aterrizaje y reunión en las operaciones aerotransportadas y anfibias. Tales medios son particularmente útiles para incrementar la seguridad durante la oscuridad y cuando las condiciones atmosféricas impiden el uso de otros medios visuales.

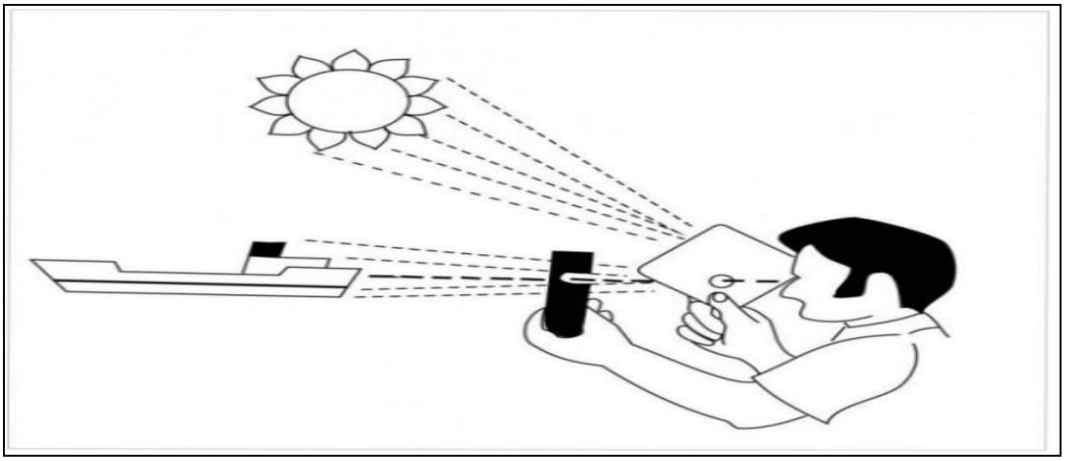


Figura N° 1. Luces Dispositivos Infrarrojos

c. Pirotécnica.

La pirotécnica, incluyendo el humo, está disponible en varios colores y tipos. Los significados de ciertas señales son dados en el I.O.C de la unidad. Usualmente las señales son incluidas para identificación de unidades amigas, control de fuego, marcación de objetivos y para reportar las ubicaciones. La transmisión y recepción de las señales pirotécnicas, son pre-planeadas, para asegurar su efectividad. La

pirotécnica puede ser usada para las comunicaciones dentro y entre las unidades terrestres y barcos fuera de la costa. El principal valor de las señales pirotécnicas reposa en la velocidad con la cual puede ser transmitidas cierta información a un gran número de tropas y unidades aisladas.

d. Paineles.

Se disponen de dos tipos generales de paineles para las comunicaciones con aviones, los paineles de marca y de identificación y para la trasmisión de mensajes. Los paineles de marca y de identificación son hechos en colores claros fluorescentes. Ellos pueden ser usados para marcar posiciones y para identificar unidades como amigas. Juegos de paineles blancos y negros para la transmisión de mensajes son preparados para ser usados sobre fondos claros u oscuros respectivamente. Estos son usados para transmitir mensajes breves o para identificar una unidad en particular. Esto se realiza utilizando el sistema de paineles combinados y el código de reconocimiento del I. O. C de la unidad.

6. COMUNICACIONES ACÚSTICAS.

Las comunicaciones acústicas están tipificadas por dispositivos simples tales como pitos, sirenas, campanas, amplificadores de voz y dispositivos explosivos. El principal valor de las señales acústicas es atraer la atención, transmitir mensajes pre-arreglados y para propagar alarmas. Mensajes en código Morse pueden ser enviados por señales acústicas. Sin embargo, como cualquier mensaje enviado por este medio debe mantenerse cortos y simples para evitar confusiones o malentendidos. Las señales acústicas son satisfactorias solamente para distancias cortas y su efectividad es grandemente reducida por el ruido de la batalla y por la dirección del viento. Ellas son vulnerables a la interceptación enemiga, por lo tanto, su uso puede ser restringido por razones de seguridad.

7. COMUNICACIONES POR RADIO Y ALAMBRE.

Radio y Alambre denotan aquellos medios de comunicaciones eléctricas - electrónicas, por medio de las cuales se pueden enviar comunicaciones a través del espacio y conductores alámbricos respectivamente. Como medios complementarios, radio y alambre pueden ser usados en combinación con uno o con otro considerado el medio principal para una aplicación en particular o pueden también ser usados separadamente. Cada uno tiene sus ventajas y desventajas, y ninguno debe ser considerado como un medio principal total. Excepto para las redes de radio a voz en los escalones inferiores, los circuitos de radio y alambre son terminados generalmente en dispositivos terminales idénticos o compatibles que permitan el uso de los dos medios para apoyarse mutuamente y como elementos complementarios de un sistema de comunicaciones integrados. Los dispositivos terminales pueden incluir teléfono, teletipo, fax, televisión y procesadores de datos.

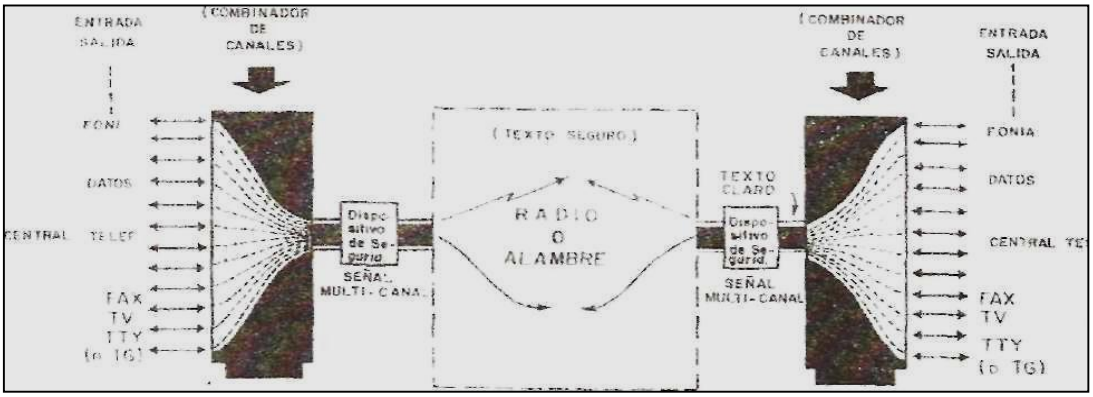


Figura N° 2. Circuitos de Radio y Alambre

8. COMUNICACIONES POR RADIO.

El radio es empleado extensivamente como un medio de comunicación dentro del Ejército. El alcance del radio empleado varía, desde los equipos de alta-potencia de radio y teletipo, radio-telegrafía (CW) o equipos de voz, en niveles desde los comandos de un conflicto o teatro de la guerra, hacia abajo, hasta los comandos de los batallones de combate (maniobra), hasta los

equipos de baja- potencia a voz, usados por los comandantes de escuadra y comandantes de tanques.

a. Capacidades y Limitaciones.

Dentro de las principales capacidades de las comunicaciones por radio, está su rapidez de instalación y establecimiento de las comunicaciones, su habilidad para interconectar escalones tácticos separados por grandes distancias y obstáculos (P. ej. terreno y el enemigo) y la alta calidad de comunicaciones que pueden ser proporcionadas. Sin embargo, el radio este sujeto a las interferencias producidas por las estáticas, interferencia intencional y por otras estaciones de radio. Su confiabilidad depende grandemente en la habilidad de los operadores y la naturaleza del terreno, las condiciones atmosféricas y las características de los equipos de radio. Estos factores juntos con la situación táctica, dictan el empleo del radio. Para ser capaz de operar juntos los equipos de radio deben tener una frecuencia común o que pueda solaparse, ser del mismo tipo de modulación, transmitir y recibir el mismo tipo de señal; y el equipo más potente debe ser mantenido dentro del alcance del equipo más débil.

b. Características del Radio.

Todos los equipos de radio se caracterizan generalmente por su banda de frecuencias y por su modulación, el equipo del Ejército casi exclusivamente utiliza las bandas de alta frecuencia (HF), muy alta frecuencia (VHF), o ultra alta frecuencia (UHF). Los tipos de modulación incluyen voz en amplitud modulada (AM), voz en frecuencia modulada (FM), banda lateral única (SSB), radiotelegrafía (CW), y Tetra. Para una descripción completa de un tipo específico de radio ó red es necesario usar una combinación de los términos anteriores o abreviaturas tales como UHF/AM, HF, HF/SSB, VHF/FM, UHF/FM, etc. Sin embargo, donde sean necesarias menos descripciones específicas, solamente la identificación de la banda de frecuencia será a menudo suficiente y es más precisa que la sola identificación del medio de modulación. Esto es

porque las capacidades de alcance (distancia) están más directamente relacionadas con las frecuencias que el tipo de modulación; VHF y UHF están generalmente limitados a trayectorias de línea de vista, mientras que HF puede operar sobre distancias mucho mayores. Por lo tanto, cuando una identificación completa tal como VHF/FM no se usa, los equipos de radio o redes son categorizadas como HF, VHF, o UHF en vez de FM, AM o SSB.

c. Seguridad.

El radio es probablemente el menos seguro de los medios de comunicaciones. Siempre debe asumirse que la intercepción enemiga toma lugar cada vez que un transmisor de radio es puesto en operación. Por lo tanto, la seguridad del radio es una consideración constante. El enemigo obtiene información conociendo meramente que radio están operando. Su análisis del número de radios en operación, el volumen de tráfico o la ubicación de los equipos son particularmente de valor. Las transmisiones de radio pueden ser restringidas o prohibidas por razones de seguridad. Las medidas importantes para la defensa contra la obtención de inteligencia por parte del enemigo son:

El Radio Silencio, Radioescucha, Criptografía. y el uso de transmisores con las técnicas modernas de salto de frecuencia, transmisión por paquetes y la simulación de redes de comunicación. Las comunicaciones tácticas pueden ser aseguradas posteriormente mediante el empleo de cripto-sistemas "en línea" y "fuera de línea". Los mensajes transmitidos por radio son criptografiados, como sea requerido por contenido. Después de que todos los factores hayan sido considerados cuidadosamente se pueden tomar las decisiones para prohibir las comunicaciones por radio en texto claro (las comunicaciones por radio no son prohibidas cuando la necesidad de ellas sobrepasa el valor de la información que el enemigo pueda ganar). Consecuentemente, los radios no son silenciados, en las unidades que están en contacto con el enemigo.

d. Capacidad de manejo de los mensajes en una red.

La velocidad y capacidad de manejo de los mensajes en una red de radio es incrementada mediante el entrenamiento de todo el personal en el procedimiento radiotelefónico, con la disciplina de red y entrenando al personal de usuarios en la escritura de mensajes. Cuando sea posible, los mensajes deben ser presentados por escrito antes de ser transmitidos.

e. Control Remoto.

Mediante el uso de ciertos tipos de equipos de control remoto, un operador de radio puede estar ubicado a una distancia segura del equipo que opera. Otras unidades de control remoto conectan un equipo de radio a una central telefónica a través de teléfonos. Este método de interconexión es llamado integración radio-alambre (IRA) y se detalla a continuación:

f. Integración Radio-Alámbrica (IRA).

Las facilidades de integración radio alámbricas permiten al comandante y a su estado mayor y algún otro personal designado que está equipado con radios VHF/FM, hacer contacto con los elementos del comando a través del sistema de conexión telefónica mientras esté ausente del puesto de comando. Las facilidades de integración radio alámbrica están normalmente disponibles en cada comando o centro de comunicaciones principal. Estos sistemas móviles están interconectados en base a "presione para hablar" (PTT) a través de la estación de IRA en el comando o centro de comunicaciones y de allí al sistema de comunicaciones principal, mediante un dispositivo de conexión desde la estación de IRA hacia la central telefónica principal. Los procedimientos de operación para las estaciones de IRA, deben ser cubiertos adecuadamente en los P.O.V, IPC e IOC para una estandarización y entendimiento por parte de todos los operadores, así como los usuarios.

Usos más importantes de la Integración Radio-Alámbrica:

1) Comunicaciones de emergencia entre una estación de radio VHF móvil y una unidad que tenga acceso sistema telefónico.
2) Comunicaciones entre dos estaciones VHF, ampliamente separadas, que están más allí del alcance normal de cualquiera de los dos radios.
3) Comunicaciones a voz desde las unidades móviles en las áreas adelantadas, hacia las unidades ubicadas en la retaguardia.
4) Contacto con aviones de vuelo a baja altura, por elementos de control de vuelo que tengan acceso a enlaces multicanales del sistema de comunicaciones sobre el terreno.
5) Establecimiento inicial (antes de que las facilidades multicanales están operativas) del servicio telefónico entre los centros de comunicaciones.
6) Suplementar las comunicaciones entre los oficiales de enlace aéreos y los controladores aéreos adelantados.
7) Contacto entre los comandos subordinados y superiores durante el desplazamiento.
8) Conexión entre dos centrales telefónicas, para servir de puente en una ruptura de una línea alámbrica.
9) Comunicaciones durante un cruce de río.

g. Radio Silencio:

Es llamado así, al período especificado por un comandante, durante el cual los transmisores y receptores de todos los equipos de radio usados para las comunicaciones dentro del comando se mantienen apagados y no operan excepto durante emergencias descritas específicamente en órdenes. Cuando los receptores de radio, son permitidos permanecer en operación, para servir de monitores en las frecuencias de la red y los transmisores son apagados, la condición es denominada Radioescucha.

h. Retransmisiones:

El término retransmisión se aplica a un método de extender el alcance de una red de radio o circuito, a través del uso de una estación intermedia, la cual en una dirección y retransmite en otra. Esto no debe ser confundido con radio relevo. La retransmisión puede ser automática, a través del uso del equipo apropiado, en cuyo caso debe ser usada una frecuencia diferente en cada dirección desde el punto de retransmisión. Cuando no está disponible el equipo automático, puede ser usada la repetición manual de los mensajes por el operador de la estación de retransmisión. Las estaciones de retransmisión pueden ser situadas sobre terrenos elevados escogidos para una cobertura óptima del área o cuando sea requerido por las circunstancias, pueden ser instaladas en aviones.

9. COMUNICACIONES ALÁMBRICAS.

El alambre es uno de los medios de comunicaciones más seguros. Incluye el uso de alambre de campaña, equipos de tendido y recuperación de alambre, cable, teléfonos operados por baterías y de sonido reforzado, centrales telefónicas, teletipos, multiplexadores y otros equipos asociados o terminales. Ellos permiten la conversación de persona a persona con operación de interrupción (capacidad de interrumpir la conversación). Las comunicaciones alámbricas son más seguras que las de radio, pero la seguridad de las informaciones clasificadas nunca es asegurada, cuando son transmitidas en texto claro sobre círculos alámbricos. La decisión de establecer comunicaciones alámbricas depende de la necesidad de ellas, del tipo disponible para instalarlas y usarlas, y de la capacidad para mantenerlas. También deben ser considerados el suministro del alambre en mano, el reabastecimiento que se espera y las necesidades futuras. Las comunicaciones alámbricas pueden ser usadas en la mayoría de los terrenos y situaciones tácticas.

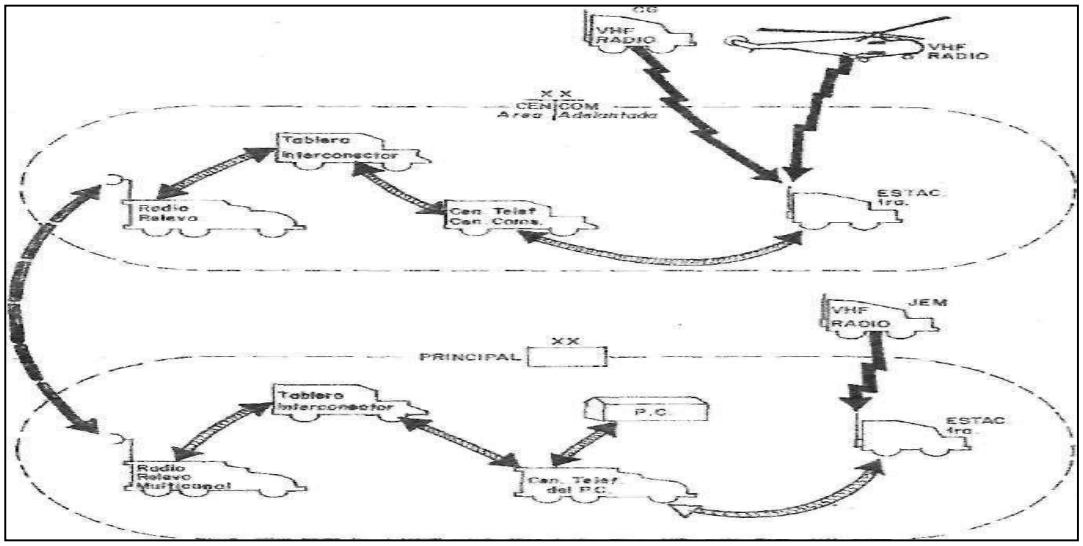


Figura N° 3. Radio relevo

a. Alcance.

El alcance de las comunicaciones alámbricas varía, dependiendo principalmente de las condiciones atmosféricas y las condiciones del alambre (p. ej., alambre húmedo empalmes pobres y aislamiento dañado). Los alcances de los circuitos alámbricos pueden ser extendido mediante el uso de repetidores, ya sean atendidos o no atendidos. Para propósitos de planeamiento, el alcance de los circuitos de alambre de campaña usando teléfonos operados por baterías, es desde 22 a 35 kilómetros. Usando teléfonos de sonido reforzado, el alcance es reducido de 5 a 16 kilómetros.

b. Tiempo requerido para su instalación.

Toma más tiempo instalar comunicaciones alámbricas que cualquier otro medio. El tiempo requerido depende principalmente de la longitud de la línea de alambre y el método de tenderla (vehículo terrestre, vehículo aéreo, llevado por Hombre). Al estimar el tiempo requerido también es necesario considerar el número de hombres disponibles, su entrenamiento, el tipo de terreno, las rutas, las condiciones atmosféricas y la visibilidad.

c. Empleo.

El alambre es empleado tácticamente, principalmente para interconectar unidades ubicadas de manera cercana, tales como: Dentro de un puesto de comando y entre los terminales de radio-relevo y las centrales de interconexión. Grandes tipos de circuitos alámbricos (troncales) entre los centros de comunicaciones y los comandos, son instalados para complementar (o como reserva para) sistema de radio y radio-relevo, cuando el tiempo, el personal y el equipo está disponible. Mediante el uso de varios dispositivos múltiples, es posible transmitir simultáneamente más de un mensaje sobre un solo circuito. En combate, los circuitos alámbricos comerciales existentes pueden ser reparados y utilizados beneficiosamente, si el tiempo lo permite. Las comunicaciones alámbricas son especialmente confiables y deseables en las operaciones defensivas desde la movilidad está limitada y hay tiempo disponible para su instalación y mantenimiento.

d. Sistemas de radio relevo.

Los sistemas de radio relevo también conocidos como radio-enlace, multicanal proporcionan circuitos comparables al alambre o cable por medio de equipos de radio y multiplexadores altamente direccionales, de modulación en fase, tiempo, división de frecuencia en VHF o UHF. Los multiplexadores, los cuales se usan también en cable, proporcionan canales telefónicos múltiples sobre un solo sistema de radio relevo. Un sistema completo que se extiende por una distancia de varios cientos de kilómetros puede ser construido de una combinación de radio relevo y secciones de cable, aun cuando cada sección de radio-relevo o enlace está limitada al enlace de línea de vista. Los sistemas multicanales son empleados para proveer comunicaciones al ejército de operaciones. Divisiones y Brigadas que lo componen con una capacidad que varía de 16 a 64 canales. Mientras el radio-relevo tiene la ventaja de una instalación más rápida con menos personal que alambre o cable, es

susceptible a interferencias de otros sistemas de radio y a la intercepción o interferencia intencional por parte del enemigo.

10. COMUNICACIONES PICTÓRICAS Y AUDIOVISUALES.

Los medios pictóricos y audio-visuales detectan, exhiben, registran o transmiten una representación precisa de cualquier escena u objeto. La fotografía, el FAX y la televisión son los principales medios pictóricos y audiovisuales, éstos son empleados para complementarse unos con otros.

a. Fotografía.

Los métodos convencionales de fotografía táctica son los siguientes. Fotografía fija y Fotografía móvil. Los dispositivos fotográficos más comunes están diseñados para registrar representaciones permanentes sobre película, papel o placas electrostáticas. Los registros fotográficos ofrecen la ventaja de reproducción de páginas múltiples. La fotografía proporciona un método de registrar con precisión y permanentemente, información y eventos para apoyar y extender las observaciones visuales.

b. El Fax.

La capacidad de los medios pictóricos ha sido aumentada por el desarrollo del FAX y la televisión. Estos dispositivos representan una fusión de la función de la fotografía y la transmisión electrónica. Los instrumentos de FAX usados sobre circuitos de radio o alambre, transmiten material pictórico fijo, tales como mapas, diagramas y documentos. En las estaciones receptoras, el material es reproducido en forma impresa permanente. Su uso, sin embargo, requiere el empleo de Circuitos que pueden ser requeridos más urgentemente para otros usos de comunicaciones.

c. Televisión.

La televisión proporciona una transmisión instantánea sobre radio o alambre, de sujetos fijos o móviles. la velocidad de la cobertura de la televisión sobrepasa a la fotografía y puede ser usada donde haya la

necesidad de una exhibición instantánea, visual y acústica de una situación táctica cambiante en un punto distante.

d. Empleo.

El uso táctico más importante de los medios de comunicaciones pictóricas y audio-visuales, descritos anteriormente está relacionado conjuntamente con las actividades de inteligencia estratégica, operacional y técnica. A través de la interpretación de fotografías aéreas y terrestres, ya sean fijas o móviles, puede ser extractada información de extrema importancia, en relación con la disposición del enemigo, material y otras actividades. Los sistemas de televisión que cubren las actividades de reconocimiento en áreas adelantadas (Ej. sistema tv instalados en vehículos de reconocimiento aéreo no tripulados) pueden exhibir a los comandantes de las unidades de combate ubicados a una distancia considerable, las operaciones en progreso, vistas instantáneas del campo de batalla, situación del enemigo, etc. Para proporcionar la inteligencia necesaria con el fin de facilitar la toma de decisiones precisas y oportunas. Otras aplicaciones importantes de los medios pictóricos y audio-visuales incluyen:

1) Fotografía de operaciones psicológicas para la diseminación de propaganda.
2) Registros operacionales para ser usados como registros gráficos de las operaciones y organizaciones militares en las áreas de combate y retaguardia.
3) Diseminación de apreciables informaciones públicas y de tropas.
4) Otras que incluyen entrenamiento, identificación personal, aplicaciones legales y médicas.

11. DISPOSITIVOS AUXILIARES.

Los dispositivos que son empleados como adjuntos a los medios de comunicaciones son clasificados como dispositivos auxiliares. Ellos incluyen dispositivos procesadores de datos capaces de correlacionar y almacenar información a altas velocidades, repetidores para extender el alcance de los circuitos de comunicaciones, multiplexadores (p. ej. terminales multicanales), que incrementen la capacidad de canales de un circuito dado y otros instrumentos que incrementan las capacidades de las facilidades de comunicaciones.

Figura N° 4. Auxiliares de Comunicación

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO II

SEGURIDAD DE LAS COMUNICACIONES

SECCIÓN A

PROTECCIÓN DE LAS COMUNICACIONES

1. RESPONSABILIDAD.

El comandante y los jefes de comunicaciones son responsables de mantener la seguridad de las comunicaciones. En adición al mantenimiento de la Seguridad de las Comunicaciones dentro de su propio Comando, es su deber informar las violaciones de la seguridad de las comunicaciones al comandante de la unidad o establecimiento donde se cometiera y al comando superior de quien depende administrativamente y operacionalmente, tan pronto sea posible tomando en consideración los requerimientos de silencio de radio.

La protección de las comunicaciones militares es una responsabilidad compartida, que recae en múltiples niveles dentro de la fuerza armada. La cadena de mando, los departamentos de tecnología y comunicaciones, y cada miembro del personal militar tienen un papel crucial en asegurar la confidencialidad, integridad y disponibilidad de la información.

2. NIVELES DE RESPONSABILIDAD.

a. Alto mando y liderazgo.

1) Creación de políticas: Los altos mandos establecen la estrategia general de seguridad de las comunicaciones (COMSEC) y las políticas que rigen su uso.

2) Supervisión: Son responsables de supervisar la implementación de estas políticas y de asegurar que se apliquen adecuadamente en todas las unidades.

3) Toma de decisiones: Se encargan de tomar decisiones rápidas y estratégicas basadas en información precisa y segura, lo que depende directamente de la calidad de las comunicaciones.

b. Departamentos y unidades especializadas.

1) Implementación técnica: Organismos como el Centro de Comunicaciones (CECOM) en algunos países o la Dirección de Tecnología de la Información y las Comunicaciones (DTIC) en el Ejército Bolivariano, son responsables de la infraestructura tecnológica, la encriptación y la ciberseguridad.
2) Auditoría y control: Auditan los sistemas para garantizar su eficiencia y efectividad, y evalúan las políticas para resguardar la confidencialidad y la disponibilidad de los datos.
3) Capacitación: Imparten formación especializada al personal para el uso correcto de los equipos y protocolos de comunicación segura.

c. Oficiales y personal de comunicaciones.

1) Mantenimiento: Se encargan del mantenimiento y operación de los equipos de comunicación, desde radios tácticas hasta sistemas satelitales.
2) Gestión en el terreno: Aseguran que las comunicaciones se realicen de acuerdo con los procedimientos operativos estándar y las técnicas de transmisión segura, especialmente en entornos hostiles.
3) Todo el personal militar.
    a) Cumplimiento de protocolos: Todos los miembros de las fuerzas armadas son responsables de cumplir estrictamente con los protocolos de seguridad de las comunicaciones, como el uso del alfabeto fonético o el manejo de material clasificado.
    b) Manejo de equipos: Deben asegurarse de que sus equipos de comunicación no sean utilizados por personal no autorizado y reportar cualquier incidencia o violación de seguridad.

La seguridad de las comunicaciones militares, es un conjunto de medidas multidisciplinares para proteger las telecomunicaciones y la información sensible que se transmite. Su propósito principal es negar al adversario el acceso a información vital y asegurar la autenticidad, integridad y disponibilidad de las comunicaciones propias.

d. Principios fundamentales: La seguridad de las comunicaciones militares se basa en los mismos principios de la seguridad de la información:
   1) Confidencialidad: Asegurar que la información solo sea accesible para el personal autorizado. Esto se logra mediante técnicas como el cifrado de extremo a extremo.
   2) Integridad: Garantizar que la información no haya sido alterada o manipulada durante su transmisión. Los sistemas deben poder detectar cualquier cambio no autorizado.
   3) Disponibilidad: Asegurar que los sistemas de comunicación estén operativos y sean accesibles para el personal autorizado cuando se necesiten, incluso en entornos degradados por guerra electrónica.
   4) Autenticidad: Confirmar la identidad de los interlocutores y la veracidad de la información, evitando la suplantación de identidad.

e. Componentes de la seguridad de las comunicaciones.

   Para lograr estos principios, se estructura en cuatro elementos principales:
   1) Seguridad criptográfica: Es la protección de la información mediante el uso de algoritmos y técnicas de cifrado. Su objetivo es hacer que los mensajes sean ininteligibles para cualquiera que no posea la clave de descifrado.
   2) Seguridad de las transmisiones: Se centra en la protección de las señales de comunicación para evitar su interceptación, interferencia o análisis. Busca dificultar que el adversario obtenga información del tráfico, incluso si no puede descifrar los mensajes.
   3) Seguridad de las emisiones: se ocupa de proteger contra el espionaje de las emisiones electromagnéticas inadvertidas (radiación de los

equipos). Busca impedir que un adversario analice estas emisiones para obtener información sensible.

4) Seguridad física: Es la protección de los equipos de comunicación, materiales criptográficos y la infraestructura de comunicaciones contra el acceso no autorizado, sabotajes y daños. Esto incluye el control de acceso a áreas seguras, el almacenamiento adecuado de los dispositivos y la protección de los cables.

f. Medios y protocolos de comunicación seguros.

Para garantizar la seguridad de las comunicaciones militares, la fuerza armada utiliza una variedad de medios y protocolos especializados:

1) Radios tácticos: Utilizan saltos de frecuencia y cifrado para asegurar las comunicaciones en el campo de batalla, con diferentes alcances y bandas.
2) Comunicaciones satelitales: Permiten la transmisión de voz, datos y video de forma segura a larga distancia, vital para el comando y control global.
3) Sistemas de mensajería cifrada: Aplicaciones y dispositivos que permiten el intercambio de mensajes de forma segura.
4) Alfabeto fonético: Permite deletrear palabras clave de manera clara y sin ambigüedades por radio, crucial en situaciones de alta tensión.
5) Señales de mano y brazos: Se utilizan para la comunicación sigilosa en operaciones especiales y de reconocimiento, donde el silencio es crucial.

g. Amenazas a la seguridad de las comunicaciones.

La seguridad de las comunicaciones militares debe ser robusta para enfrentar diversas amenazas:

1) Guerra electrónica: Busca degradar o interrumpir los sistemas de comunicación del adversario mediante interferencias o engaños.
2) Interceptación y espionaje: El adversario intenta escuchar o grabar las comunicaciones para obtener inteligencia.

3) Ciberataques: Los ataques cibernéticos pueden comprometer sistemas de información críticos, robando datos o interrumpiendo las operaciones.
4) Manipulación (spoofing): El adversario intenta hacerse pasar por una fuente autorizada para enviar información falsa.
5) Fallas técnicas o humanas: Errores en la operación de los equipos o en los protocolos de seguridad pueden comprometer la confidencialidad.

3. IMPORTANCIA DE LA SEGURIDAD DE LAS COMUNICACIONES MILITARES

La seguridad de las comunicaciones militares es crítica para el éxito de cualquier operación. Permite a las fuerzas militares coordinarse eficazmente, mantener el comando y control, y reaccionar rápidamente a las amenazas. La falta de seguridad puede llevar a la pérdida de vidas, el fracaso de la misión y la exposición de información sensible al enemigo.

SECCIÓN B

CLASIFICACIÓN DE SEGURIDAD

1. POLÍTICA BÁSICA.

Es política de la Fuerza Armada Bolivariana dar a conocer al público tanta información de sus actividades como sea posible, en contraposición con la necesidad de proteger la Seguridad Nacional; así mismo, la información será clasificada de acuerdo con este principio básico.

La innecesaria e indebida asignación de clasificación de seguridad debe ser evitada. Si existe alguna duda sobre el grado adecuado de clasificación que debe colocarse a un documento resguárdelo como si tuviese colocado como mínimo “CONFIDENCIAL” y espere el asesoramiento de una Autoridad de Clasificación.

2. RESPONSABILIDAD DE LA CLASIFICACIÓN.

   a. El Jefe Militar de la Fuerza Armada Bolivariana tendrá la máxima responsabilidad de determinar las medidas generales de seguridad para las informaciones, documentos y materiales clasificados; tal cual está establecido en el “REGLAMENTO PARA LA CLASIFICACIÓN, SEGURIDAD Y MANEJO DE LAS INFORMACIONES, DOCUMENTO Y MATERIALES CLASIFICADOS DE LA FUERZA ARMADA NACIONAL BOLIVARIANA”. Las medidas generales de seguridad serán ejecutadas y controladas por los comandantes de Unidades o Jefes de Establecimientos y Dependencias de la Fuerza Armada Bolivariana, constituidas en custodios principales, pudiendo realizar estas medidas a través del oficial de control de seguridad o de quien ejerza función como tal; este último tendrá igualmente carácter de custodio.
   b. Los comandantes son responsables de la clasificación apropiada de los mensajes originados dentro de sus jurisdicciones. Esta función puede ser delegada a subordinados, pero, la autoridad delegante no es relevada de la responsabilidad de la clasificación apropiada.
   c. A una respuesta o referencia de un mensaje clasificado, le puede ser asignada una clasificación más baja cuando el contenido del texto la respuesta no revele información que podría comprometer al documento inicial y el asunto que trata.

3. PROPÓSITO DE LA CLASIFICACIÓN.

   a. El propósito principal de la clasificación es el de imponer restricciones en el manejo de los documentos y en la diseminación de la información contenida. Las clasificaciones altas pierden su significado cuando se usan excesivamente.
   b. La clasificación de los mensajes debe recibir especial consideración por parte del promotor. Se deben evitar las clasificaciones demasiadas altas o bajas.
   c. El grado de seguridad criptográfica dada a un mensaje está gobernando

por la clasificación de seguridad.

d. La clasificación de seguridad podrá ser asignada por personal profesional autorizado de los centros de comunicaciones.

4. DESIGNACIÓN DE CLASIFICACIÓN.

La información que requiere protección contra la revelación no autorizada, en interés de la Seguridad Nacional o de la Fuerza Armada Bolivariana se clasificará en tres categorías:

a. SECRETO: La clasificación SECRETO, se asignará a las informaciones, documentos y materiales clasificados que requieran el más alto grado de protección y cuyo conocimiento y divulgación por parte de personas no autorizadas, causen graves daños a la Nación Venezolana y a su Fuerza Armada Bolivariana. Tendrán esta clasificación:

1) Los planes y documentos derivados de los tratados suscritos por el estado venezolano.
2) Los documentos de suma importancia sobre convenios de la Fuerza Armada Bolivariana.
3) Los planes operacionales de defensa y los de áreas estratégicas vitales a la defensa del Continente Americano, que afecten la seguridad de la Nación.
4) Las informaciones que se refieren a estrategias nacionales, métodos técnicos o tácticas especializadas que se pueden aplicar en determinadas operaciones, así como también la composición e identidad de las Unidades que se pretendan utilizar para llevarlas a cabo.
5) Las informaciones de los métodos y resultados del sistema de inteligencia y contrainteligencia, y abastecimiento de materiales incluyendo cantidades específicas, ubicación y reservas.
6) Los planes generales o específicos para la defensa nacional.
7) En tiempo de conflicto, la información específica que revela la ubicación capacidad y estado de preparación de la Fuerza Armada

Bolivariana; o de con las cuales el estado venezolano haya suscrito convenios.

8) Todas aquellas informaciones, claves criptográficas, material de combate, fuerzas, métodos, tácticas, estado de entrenamiento, reservas y otros datos del probable agresor o de nuestra propia fuerza; que sean de interés para la planificación y desarrollo de las operaciones.
9) Las informaciones sobre cantidades específicas de reservas de materiales estratégicos.
10) La información militar que contengan datos relativos a las necesidades de adquisición y utilización de equipos y sistemas de armas.
11) Las informaciones militares que contengan fotografías aéreas, cartas o cualquier otro dato acerca de instalaciones o construcciones militares y en general todo documento o material que por su naturaleza puedan afectar las relaciones internacionales del país en general o de las naciones con las cuales éste haya suscrito acuerdos de defensa en particular.
12) Las informaciones que se refieran al estado de operatividad de equipos y reportes de capacidad combativa.

b. CONFIDENCIAL: La clasificación CONFIDENCIAL se asignará a las informaciones, documentos y materiales cuyo conocimiento y divulgación o personas no autorizadas, causen daños a la Nación Venezolana o a su Fuerza Armada Nacional. Tendrán está clasificación:

1) Las informaciones militares que contengan datos relativos a la celebración de contratos para la adquisición de equipos y sistemas de armas, órdenes de compras y requisiciones.
2) La asignación de frecuencias, cambio de estas y señales de llamada de radio de significado especial.
3) La información que indique parcialmente la identidad, composición de nuestras unidades, cantidad de equipos específicos; sí como las

partes operacionales y de orden de batalla que sean de importancia para el probable agresor.

4) Historial de Personal

c. RESERVADO: La clasificación RESERVADO se asignará a las informaciones, documentos y materiales que deben ser mantenidos fuera del alcance de personas no autorizadas. Tendrán esta clasificación:

1) Los programas, directivas de trabajo, conferencias, informes, reglamentos y manuales que por su naturaleza estén clasificados en esta categoría.

d. NO CLASIFICADO: Se marcará NO CLASIFICADO toda información cuya divulgación dentro de la institución no afecta los intereses de la nación ni de su Fuerza Armada y toda documentación concerniente al manejo de personal, por lo que no adquiere ningún tipo de clasificación.

5. AUTORIDADES CLASIFICADORAS.

Están facultadas para clasificar las informaciones documentos y materiales de la Fuerza Armada Nacional Bolivariana:

a. El Ministro del Poder Popular para la Defensa, Viceministros y Directores.
b. El Comandante Estratégico Operacional de la Fuerza Armada Nacional Bolivariana.
c. El Inspector General de la Fuerza Armada Nacional Bolivariana.
d. El Jefe del Estado Mayor Conjunto y los Directores Conjuntos.
e. Los Comandantes Generales de cada Componente, su Estado Mayor y oficiales hasta nivel Director.
f. Los Comandantes de Regiones, Zonas y Áreas de Defensa Integral; su Estado Mayor y oficiales hasta nivel Director.
g. Los Comandantes de Unidades Superiores y Tácticas, Dependencias y Establecimientos de la Fuerza Armada Bolivariana.

6. CLASIFICACIÓN.

a. A la información, documentos y materiales clasificados, se les asignará la clasificación más acorde y compatible con la información requerida, a

fin de evitar la sobre o sub-clasificación.

b. Los documentos serán clasificados conforme a su propio contenido y de acuerdo a la relación que tengan con otros documentos

c. La clasificación de un legajo de documentos físicamente unidos o encuadernados, debe ser igual a la del documento de más alta clasificación del conjunto. Cuando un documento sea separado del legajo o agrupación, este será manejado de acuerdo con su propia clasificación.

d. Toda comunicación que acompañe un documento o material clasificado debe tener la misma clasificación.

e. La información y documentos no clasificados, que hagan referencia a materias de seguridad y defensa, no deben contener extracto de la información clasificada.

7. RECLASIFICACIÓN.

a. La reclasificación es la asignación de una nueva “CLASIFICACIÓN” como consecuencia del cambio de los factores que determinen su clasificación original.

b. Las autoridades clasificadoras, harán del conocimiento al oficial encargado de la Seguridad de Comunicaciones de la dependencia respectiva, la clasificación, a fin que éste ejecute los cambios respectivos.

c. De ser necesario, las autoridades clasificadoras indicarán en el propio documento, la reclasificación a llevarse a efecto en una fecha determinada.

d. En todo documento o material a reclasificarse, se tachará el sello de la clasificación original y se sellará nuevamente como “RECLASIFICADO SECRETO”, “RECLASIFICADO CONFIDENCIAL” o “RECLASIFICADO RESERVADO”.

8. ACCESO.

a. Por acceso se entiende la facultad que tiene determinada persona para utilizar, elaborar, leer o manipular material clasificado.

b. La política del “ACCESO” está basada en el principio simple de control

de circulación y control del acceso a la información clasificada. El conocimiento o posesión de información clasificada está permitido solamente a individuos cuyas funciones oficiales requieren el acceso a ella, en interés de promover la seguridad, solamente si ha sido clasificado como “ELEGIBLE PARA ACCESO”.

c. Nadie podrá tener acceso a información clasificada, basándose en el rango, posición o nivel de seguridad. La responsabilidad final para determinar si una persona, por sus funciones oficiales, requiere tener acceso a un elemento o ítem de información clasificada (“LA NECESIDAD DE CONOCER”), recae en el Comandante y en el individuo que tiene autorizada la posesión, conocimiento y control de la información involucrada; y no sobre el probable receptor, únicamente podrán tener acceso a información clasificada el individuo que ha sido clasificado como “ELEGIBLE PARA ACCESO”.

d. Estos principios son igualmente aplicables si los posibles receptores son:
   1) Comandos de Otros Componentes
   2) Organismos Oficiales
   3) Organismos Privados
   4) Contratistas
   5) Autoridades Extranjeras.

e. Los Comandantes, deben asegurarse que el personal que se encuentre bajo su jurisdicción, tenga debido conocimiento de la Doctrina de Seguridad, que se encuentra contenida en el Manual de Seguridad de las Comunicaciones (MAN-CO-FANB-003) antes de conceder el acceso a información clasificada.

9. OTORGAMIENTO DEL ACCESO.

a. La autoridad para conceder el acceso a información clasificada es el comandante, quien es el responsable por la seguridad de la información y material clasificado que se encuentre en su comando. Un comandante puede conceder el acceso a información clasificada a aquel individuo que

tiene una necesidad de conocerla, que tiene la adecuada clasificación de seguridad y sobre quien no existe ningún dato de que pueda revelarla.

b. La autoridad de un comandante para conceder el acceso a información clasificada está sujeta a las siguientes restricciones:

1) Los inmigrantes no deben tener acceso a información de inteligencia extranjera, a material clasificado más alto o igual que “RESERVADO” y a información de criptografía, sin la autorización previa de la autoridad competente u originador del documento.
2) Los empleados de contratistas no deben tener acceso a las áreas restringidas, a la información criptográfica y a la inteligencia de comunicaciones.
3) Aquellos individuos que tengan autorizado “ACCESO LIMITADO”, expedido por el Estado Mayor del Comando Estratégico Operacional, Componente o Región de Defensa Integral, lo tendrán solamente sobre aquella información o material clasificado específicamente autorizado.
4) El otorgamiento de acceso a representantes de gobiernos extranjeros, incluyendo personal contemplado en el intercambio de cursos, será estrictamente limitado a aquella información y material clasificado necesario para el cumplimiento de los objetivos trazados por la Fuerza Armada Bolivariana.
5) El personal civil que trabaja en la Fuerza Armada Bolivariana podrá tener acceso a información clasificada, siempre y cuando las funciones que desempeña lo requieran y que haya cumplido los requisitos establecidos en el “INSTRUCTIVO PARA LA CALIFICACIÓN INDIVIDUAL DEL PERSONAL CON ACCESO A MATERIAL CLASIFICADO” (INS-IT-FANB-0012).
6) Los pasos a seguirse en el otorgamiento de acceso a un miembro de un comando son:
    a) Determinar el nivel de acceso requerido para el cumplimiento de sus funciones oficiales.

b) Verifique el registro individual oficial y determine si tiene la apropiada clasificación de seguridad (si no la tiene, tome las acciones apropiadas establecidas en el Manual de Seguridad de las Comunicaciones).
c) Revise los registros disponibles en el comando de degradación de información.
d) Si el individuo tiene la apropiada clasificación y no degrada la información, conceda el acceso y regístrelo.
e) Proceda a informar a la persona involucrada, mediante una comunicación oficial, informándole sobre el nivel de acceso que le ha sido concedido, así como, que material está autorizado para manejar; advirtiéndole de la responsabilidad que comparte y de las consecuencias que le acarrearía su revelación.
f) Como el otorgamiento del “ACCESO” es responsabilidad del comando, éste determina automáticamente cuando el individuo es transferido, separado del cargo o dado de baja del componente. También finaliza cuando vence el período establecido, si es denegado o si es renovada por órdenes supriores.
g) Cuando se tiene información desfavorable de una persona que le ha sido autorizado el acceso, el comandante podrá decidir si lo restringe o suspende. La restricción o suspensión de acceso por esta circunstancia, podrá ser usada como una medida preventiva y temporal hasta que la situación surgida haya sido aclarada.
h) Cuando se haya comprobado el acceso de una persona a información no autorizada y la misma pudiera traer consecuencias perjudiciales a intereses de la institución, el Comando deberá notificar a la Dirección de Inteligencia del Comando Estratégico Operacional o del Componente, quien asumirá el estudio y control de la situación.

10. REGISTRO DE ACCESO.

a. Todo otorgamiento de “ACCESO” a información y material clasificado, debe ser debidamente registrada en el “LIBRO DE REGISTRO DE OTORGAMIENTO DE ACCESO” que para los efectos debe ser llevado en todos los comandos.

b. Las autorizaciones de acceso deben ser firmadas por el comandante o autoridad en quien se le ha delegado esta función.

c. No es necesario registrar a los comandantes, excepto para aquella infamación o material clasificado que no requiera que el acceso haya sido formalmente concedido.

d. El Comandante Estratégico Operacional y su Estado Mayor, los Comandantes Generales de Componentes y su Estado Mayor, así como los Comandantes de Regiones de Defensa Integral y su Estado Mayor, tendrán acceso a toda información y material clasificado, motivo por el cual no serán asentados en los libros de registro de correspondientes.

e. A los efectos de conceder el acceso a la información clasificada para determinar los diferentes niveles, se debe dar estricto cumplimiento a lo establecido en el INSTRUCTIVO PARA LA CALIFICACIÓN INDIVIDUAL CON ACCESO A MATERIAL CLASIFICADO (INS-IT-FANB-0012), el cual, una vez en poder de la Dirección de Inteligencia del Comando Estratégico Operacional o del Componente, servirá para efectuar las investigaciones de rigor, y la posterior emisión de la información sobre el individuo que pasará a formar parte del “REGISTRO INDIVIDUAL”

f. La Dirección de Inteligencia del Comando Estratégico Operacional y de cada Componente, llevará un registro individual de todas aquellas personas a quienes se le ha llevado INS-IT-FANB-0012, y mantendrá informado a los comandos a quienes pertenecen sobre cualquier dato favorable o desfavorable que se tenga de ellas.

g. Todos los comandos llevarán un registro individual de las personas a quienes se le ha concedido o no el acceso, e incluirán en él toda aquella información que se reciba de la Dirección de la inteligencia del Comando

Estratégico Operacional, del Componente o cualquier otro organismo del Estado.

h. Cuando la persona sea transferida a otro comando, se deberá enviar el Registro Individual y un informe de su gestión anexo, el cual, servirá el comandante para el otorgamiento del acceso a esa persona, en su jurisdicción.

11. ACCESO DE EMERGENCIA.

a. Cuando un individuo requiere acceso a la información clasificada y las investigaciones de seguridad no han sido concluidas, el comandante puede autorizar “ACCESO DE EMERGENCIA”.

1) Los procedimientos necesarios de investigación de inteligencia tienen que ser iniciados.
2) La espera de la finalización de la investigación de inteligencia puede causar un retardo crucial en el adiestramiento o asignación de personal.
3) Otros procedimientos de investigación no deben ser utilizados.
4) Los registros inmediatamente disponibles deben ser revisados y determinar si el individuo es elegible para el acceso requerido.

b. Este tipo de acceso no será concedido, bajo ninguna circunstancia:

1) Personas extranjeras sin importar el cargo que ocupen del país.
2) A civiles asignados a posiciones críticas.
3) A cualquier persona para que la finalización de las investigaciones sea un requisito.

c. Los comandantes deben llevar un libro de registro especial para asentar los otorgamientos del “ACCESO DE EMERGENCIA”, debiendo escribir las razones que lo originaron.

d. El otorgamiento del acceso de emergencia puede constituir un olvido de la solicitud de la investigación a la persona, motivo por el cual, los comandantes deben seguir su inicio y llevar un registro de las solicitudes.

12. AUTORIZACIÓN PARA ACCESO LIMITADO.

a. Cuando un Comandante considere que debe, en interés de la seguridad nacional, conceder acceso a información clasificada, de la cual es responsable, a una persona que no es una autoridad oficial o gubernamental o dicho de otra manera, no elegible por razones de seguridad física; hará requerimiento al Comandante Estratégico Operacional, Comandante de Componente o Región de Defensa Integral o a los integrantes del Estado Mayor de los comandos antes indicados para la concesión de una “AUTORIZACIÓN PARA ACCESO LIMITADO”.

b. El requerimiento debe ser hecho por escrito, debiéndose hacer una detallada exposición de los motivos que la originan, la clasificación, naturaleza y objeto de la información y período de tiempo durante el cual se necesita la autorización. Acompañe la solicitud con todos los datos de la persona que requiere la autorización, con el fin de iniciar de inmediato la investigación de inteligencia.

c. Los Comandantes e integrantes del Estado Mayor no aceptarán solicitudes cursadas directamente por las personas interesadas. Estas deberán ser hechas por el Comandante de la Unidad o Dependencia que haya determinado la necesidad, quien asumirá la responsabilidad por el adoctrinamiento de la persona afectada del acceso al que ha sido autorizado y el adoctrinamiento al final del período autorizado sobre las consecuencias que traería la revelación de la información, la persona con autorización para acceso limitado, no podrá solicitar acceso a publicaciones con mayor clasificación de seguridad que la establecida por el Comandante o integrante del Estado Mayor haya autorizado. En caso de así requerirlo, se procederá con una nueva solicitud de autorización.

d. El acceso será autorizado por el Comandante o integrante del Estado Mayor, sólo para el propósito y la información clasificada especificada indicada en la solicitud. La autorización será efectiva por el periodo de tiempo necesario y generalmente no mayor de dos años. La custodia

física del material clasificado, no debe ser concedida.

SECCIÓN C

SEGURIDAD FÍSICA

1. DEFINICIÓN.

Seguridad física, es el componente de Seguridad de Comunicaciones que resulta de todas las medidas necesarias para salvaguardar equipo, material y documentos clasificados del acceso a personas no autorizadas. La seguridad física se obtiene cuando los métodos establecidos y procedimientos establecidos son llevados a cabo eficientemente. Esto impone el manejo por parte de todos los interesados, el almacenaje apropiado del equipo y material cundo no está en uso, y cuando sea necesario, su destrucción.

2. SEGURIDAD FÍSICA EN LOS ASUNTOS CLASIFICADOS.

a. El mantenimiento de la seguridad física asegura la protección máxima del material clasificado desde la fecha de producción hasta su destrucción. Las informaciones, documentos etc., deberán ser guardados en sitios que ofrezcan un máximo grado de seguridad, protegiéndolas contra robo, espionaje, observación, fotografía, reproducción, copia y cualquier otra forma de difusión. Las siguientes prácticas deben adoptarse para garantizar la seguridad física.

1) Manejo Cuidadoso
2) Almacenaje Protegido
3) Contabilidad Exacta
4) Destrucción completa cuando sea necesario

b. Los desperdicios de las canastas de basura, aun cuando estén en forma de pedazos arrugados, puedan plancharse y juntarse en tal forma que aparecen los caracteres legibles y las impresiones correctas. Las huellas invertidas de los papeles secantes y carbón, pueden leerse con facilidad,

lo que está escrito en documentos incinerados también se pueden leer.

c. Cuando se incinera material clasificado, hay que observarlo hasta que se convierta en ceniza, lo cual se debe esparcir tanto como sea posible, Las hojas sueltas de papel que han pertenecido a libros, son difíciles de quemares completamente; por lo cual, deben ser rotas en pedazos pequeños con anticipación hay que tener cuidado que las porciones aún no completamente incineradas sean llevadas por el viento.

d. Cada combinación de la caja fuerte o archivadores usados para el almacenaje de material clasificado contendrá un registro de la última fecha que fue cambiada la combinación. Las combinaciones serán cambiadas por lo menos cada seis meses, o cuando las combinaciones hayan sido conocidas por personas no autorizadas o por cambio del custodio. Los nombres, direcciones y número telefónicos de las oficinas o habitaciones del personal responsable que debe ser notificado en caso de encontrarse una caja fuerte abierta, se encontrará dentro de esta: igualmente deberá encontrarse en caja fuerte o archivador una lista de las personas que conocen combinaciones de la misma. Las combinaciones de las cajas fuertes deberán ser mantenidas en un archivo localizado en algún lugar seguro, que permita su acceso a las personas autorizadas en cualquier emergencia.

3. NORMAS DE CONTROL Y CLASIFICACIÓN.

a. A la información y al material clasificado debe proporcionársele un grado de control adecuado de acuerdo a la clasificación asignada.

b. La contabilidad y el control sirven para:

1) Limitar la diseminación de la información.

2) Prevenir las reproducciones innecesarias.

3) Determinar la oficina o personal normalmente responsable por la seguridad del material.

4) Determinar los poseedores, así ellos pueden ser notificado de cambios que se realicen a la publicación o a su clasificación.

c. En el caso de la información secreta es también importante mantener un registro de quienes han tenido la información y de quienes la han visto.

d. Resulta sumamente difícil proveer una contabilidad y control de toda la información clasificada. Sin embargo, con un buen proceso de administración del tiempo, del dinero y del personal que labora en el Sistema de Comunicaciones, se puede garantizar a los tres (3) niveles de clasificación de seguridad un alto grado de confiabilidad en la contabilidad y control de las publicaciones y documentos.

e. Se deben implementar medidas en los comandos, para asegurar que al material que ingrese por los medios de correo le sea debidamente controlada su recepción y se pueda formalizar que el acceso al material clasificada recibido, sea plenamente restringido.

4. MATERIAL SECRETO, CONFIDENCIAL Y RESERVADO.

a. Los comandos, asistidos por los oficiales designados para el control del material clasificado son responsables para la revisión y mantenimiento de los registros de contabilidad y por la distribución de este material.

b. Todas las copias del material al cual se le haya asignado esta clasificación, deben tener asignado su respectivo número de registro y el mismo deberá colocársele en cada una de sus páginas. Este número de registro será el asignado de acuerdo a la lista de distribución de la publicación.

c. En aquellos casos en los cuales sea autorizada la distribución de copia adicionales, deberá incluirse en el expediente de la publicación, copia de la comunicación mediante la cual se autoriza su reproducción y agregársele en la lista de distribución los números de registro de las copias con sus respectivos destinatarios y anexarse al expediente los recibos de entre de publicaciones debidamente firmados.

d. Al recibirse una publicación con esta e custodio de la misma deberá chequear minuciosamente su contenido verificar que todas las páginas estén completas. De igual manera deberá procederse cuando se reciban

cambios a la misma publicación, y las páginas sustituidas deberán ser destruidas de inmediato de acuerdo lo establecido en este manual para tal procedimiento.

e. La retención de los documentos debe mantenerse al mínimo, por lo cual esta documentación, tan pronto haya cesado su vigencia, debe ser destruida.

f. Las copias en lenguaje llano de los mensajes criptografiados y los criptogramas de los mensajes clasificados se archivarán por separado. Las copias de los mensajes indicados como parafraseados se les darán las facilidades más seguras de archivo de acuerdo a las directivas vigentes.

5. PAPELES DE TRABAJO, CINTAS DE MÁQUINAS DE ESCRIBIR, DISKETTES**.**

a. Los papeles de trabajo son material utilizado mientras se prepara una publicación, documento o mensaje; cuando se ha concluido la elaboración de la publicación, y su contenido es clasificado, éstos papeles de trabajo llevarán la misma clasificación que le correspondería a la publicación elaborada.

b. Como mínimo los papeles de trabajo serán:

1) Fechados al elaborarse
2) Marcados en cada página con la clasificación más elevada de cualquier información que ellos contengan.
3) Protegidos de acuerdo al grado de clasificación asignada.
4) Destruidos por medios autorizados, cuando no se requieran por largo tiempo.

c. El acceso a las áreas donde se manejan papeles de trabajo con material de clasificación secreto, estará restringido al personal no autorizado y se deberán tomar las medidas adecuadas para impedir la revelación de información clasificada.

d. Las notas clasificadas de curso de entrenamiento o de una conferencia,

deben ser considerada como papeles de trabajo, con las mismas condiciones de seguridad impuestas a éstas.

e. Medidas similares de seguridad deben tomarse con las cintas de maquinarias de escribir o impresoras una vez terminadas, así como también con los Diskettes cuando contienen información clasificada impresa.

6. REQUERIMIENTOS DE SEGURIDAD PARA EL ALMACENAJE DE PUBLICACIONES.

a. Las publicaciones secretas, deberán ser guardadas en sitios que ofrezcan la máxima seguridad de las mismas.

b. Los documentos y materiales clasificados “Secreto”, se mantendrán guardados en cajas fuertes con cerraduras de combinación.

c. Los documentos y materiales clasificados “Confidencial” y “Reservado”, se mantendrán guardados en archivos normales que posean como mínimo e con seguridad de combinación o cerraduras.

d. La combinación de las cajas fuertes, gabinetes o archivos de metal será protegida, colocándola en sobre dobles, debidamente lacrados y guardados en sitio seguro.

e. El conocimiento que se tenga de una combinación será limitado al personal integrante de la junta Criptográfica respectiva.

7. SEGURIDAD FÍSICA DE LAS AYUDAS CRIPTOGRÁFICAS.

a. Las ayudas criptográficas, y los textos descriptografiados, de los mensajes deber merecer mayor cuidado que los asuntos clasificados en general por las siguientes razones:

1) Los equipos de comunicaciones sufren rápida y radicalmente, cambios y mejoras, por eso es conveniente, que personas no autorizadas puedan percatarse del estado de los equipos.

2) Las personas no autorizadas que obtengan información del estado de los equipos de comunicaciones y su operación, estarán capacitados para desarrollar cualquier contramedida efectiva contra

nuestros dispositivos y métodos.

b. Solamente el siguiente personal puede tener acceso a los locales donde se encuentren equipos de comunicaciones.
   1) El personal que labora en las áreas de comunicaciones por necesidades de trabajo.
   2) El personal civil que tenga que efectuar trabajos autorizados dentro de los compartimientos de comunicaciones, y que tengan clasificación de seguridad.
   3) Los oficiales de la Fuerza Armada Bolivariana, que por razones de sus deberes y con autorización del Director de Comunicaciones de la Fuerza Armada Bolivariana, visiten los Centros de Comunicaciones.
   4) El comandante y segundo comandante de la Unidad.

c. El personal “NO AUTORIZADO” no debe tener acceso a los locales de comunicaciones, y en particular, aquel personal que lleve máquinas fotográficas, video, cámaras o grabadoras de sonido.

8. SEGURIDAD FÍSICA DE EQUIPOS DE COMUNICACIONES E INFORMÁTICA.

   a. Las áreas de trabajo de comunicaciones, deben considerarse como reservadas y no se debe permitir el acceso a personal no autorizado. A tal efecto se deben colocar avisos con la firma del comandante de Unidad donde se indique la prohibición de acceso y la lista con el personal autorizado.

   b. Los cuartos de servidores, concentradores, cableado, centrales telefónicas, salas de medios solo se podrán utilizar por el personal de comunicaciones calificado para operar los equipos y debidamente autorizado por el comandante de Unidad y Jefe de Comunicaciones. Estos locales deben poseer medidas de protección para evitar el acceso de personal no autorizado (paredes de concreto con una sola puerta de acceso de metal con cerradura, si posee ventanas estas deben tener rejas de seguridad); así como, medios de seguridad industrial para

proteger la integridad de los equipos y sistemas que allí se operan (Sistemas antincendios, reguladores, UPS, sistemas de puesta a tierra, para-rayos, piso con cubierta aislante, etc.).

c. El administrador de redes, debe preparar un apropiado sistema de claves de acceso para los servidores, y administrador de usuarios; debiendo mantener en caja de seguridad una copia del mismo para su uso por parte del Jefe de Comunicaciones en caso de ser necesario.

d. Se debe establecer una política de respaldo de la información que se mantiene en los servidores y bases de datos.

SECCIÓN D

SEGURIDAD DE TRANSMISIÓN

1. DEFINICIÓN.

Es el componente de la Seguridad de las Comunicaciones que resulta de todas las medidas diseñadas para proteger las transmisiones, de la intercepción no autorizada, el análisis y la decepción. La seguridad relativa de un medio de transmisión sobre otro varía con las circunstancias.

2. PRINCIPIOS GENERALES.

a. La seguridad de transmisión se inicia desde el momento de la planificación, en cada IOC/IPC y en los anexos de comunicaciones de cada ejercicio u operación, se deben considerar redes de comunicaciones principales y alternas en las bandas de frecuencia UHF, VHF, HF y satelitales; así como, redes alámbricas y redes de datos, métodos para señales visuales y sonoras, y sistema de correo; de tal manera que con el uso apropiado de cada una de estas redes se contribuya a la seguridad. Así tenemos que el correo, las redes alámbricas, las señales visuales y sonoras brindan el mayor nivel de seguridad, pero solo pueden ser usadas a corta distancia, luego en función a las características técnicas que limitan el alcance de los

equipos de radio y las características del área geográfica donde se esté operando, deberán usarse las redes en UHF, VHF y finalmente las de HF para comunicaciones a mayores distancias.

b. La seguridad de transmisión implica la selección del método de transmisión que dará a un mensaje la necesaria velocidad y certeza de entrega, con el mínimo de exposición a la intercepción no autorizada. El uso de los métodos menos expuesto, tiende a reducir la cantidad de tráfico a disposición del interceptor para estudio analítico. Pero, el envío de un mensaje por correo u otro medio aparentemente no expuesto no asegura contra la intersección, pues existe el peligro del robo.

c. El uso del radio puede revelar la posición de una estación transmisora, a un interceptor enemigo equipado con radiogoniómetro, es por ello que los mensajes deben ser claros y cortos.

d. Es necesario un alto nivel de disciplina y entrenamiento en radio por las siguientes razones:

   1) Las transmisiones no autorizadas o innecesarias aumentan la oportunidad a los radiogoniómetros enemigos.
   2) La confusión de indicativos de llamada conduce a comprometerlos.
   3) Si una unidad rompe el silencio de radio sin autorización puede comprometer el resultado completo de una operación.
   4) La conversación no oficial entre los radioperadores y las transmisiones no autorizadas, pueden revelar indicativos de llamada e información clasificada.
   5) El uso de procedimientos no autorizados conduce al desarrollo de hábitos personales o peculiaridades de un circuito, que puede servir para identificar una estación o un circuito, aun cuando cambie conjuntamente la frecuencia e indicativos de llamadas.
   6) Los ajustes incorrectos de transmisores y receptores conducen al uso de excesiva potencia de transmisión y frecuentes repeticiones proporcionando así, grandes oportunidades para la intercepción y radiogoniometría enemiga.

7) El uso de frecuencias no autorizadas pueden revelar información clasificada ayudando así a la intercepción enemiga.

3. SEGURIDAD DE RADIO.

a. Cada vez que sea necesario usar la emisión de radio de largo alcance en la transmisión de mensajes, se deben observar siempre las siguientes precauciones:

1) Mientras sea posible, debe usarse los métodos “I” Interceptado y “F” Radiodifusión, para el tráfico prefiriéndolos al método “R” Recibido. Se debe hacer la combinación debida en las antenas y potencias de transmisión pero que se asegure una buena calidad de recepción.

2) Los mensajes deben ser transmitidos usando aquellos circuitos que no impliquen el uso de muchas retransmisiones para llegar a sus destinatarios.

3) El tráfico que se transmita para el adiestramiento del radio operadores debe ser redactado con anterioridad para ese objeto, no usando jamás despachos, auténticos de los archivos.

4) Siempre que las bondades de los equipos lo permitan, deberá protegerse la transmisión encriptando la voz, usando saltos de frecuencia con el empleo de criptógrafos en línea.

6) Todo mensaje que se transmita debe ser criptografiada o ser cifrado con un pre-arreglado.

7) La transmisión por finía no debe ser excesiva, variando diariamente las frecuencias.

b. Se puede mantener la disciplina del circuito y evitar los errores comunes, usado operadores bien adiestrados. Esta regla es importante para todos los sistemas de comunicaciones, desde el punto de vista de la eficiencia y de la calidad. Es particularmente importante en los circuitos de radio de largo alcance, donde la seguridad requiere una consideración especial. Las siguientes reglas básicas son esenciales en la seguridad de transmisión y deben ser cumplidas estrictamente en todas las redes y

circuitos de radio.

1) No se hará ninguna transmisión, que no haya sido autorizada por la autoridad competente.
2) Las siguientes prácticas están estrictamente prohibidas:
    a) Violación del silencio de radio
    b) Conversación no oficial entre radioperadores
    c) Uso indebido de indicativos de llamada
    d) Transmitir en una red dirigida sin permiso
    e) Transmitir el nombre del operador
    f) Uso no autorizado del lenguaje llano
    g) Uso de signos y frases de procedimientos no autorizados
    h) Lenguaje profano, indecente u obsceno
    i) Uso de abreviaturas no autorizadas oficialmente
    j) Uso de excesiva potencia en transmisión
    k) Uso de frecuencias no autorizadas
    l) Uso indebido de frecuencias coordinadas para transmisiones no oficiales.
    m) No usar diariamente las mismas frecuencias por fonía.
3) Las siguientes prácticas deben evitarse:
    a) Empleo de excesivo tiempo en sintonizar, cambiar frecuencia o ajustes en el equipo.
    b) Transmitir a velocidades superiores a la capacidad de los operadores que reciben.

4. POLÍTICA DE EMISIONES

a. El radio es potencialmente el sistema menos seguro de los medios de comunicaciones de la Fuerza Armada bolivariana. Debe suponerse que cada transmisión va a ser interceptada. De esta manera el enemigo, no solo tiene oportunidad de obtener información usando el criptoanálisis, sino que puede estar capacitado para localizar nuestras unidades transmisoras empleando radiogoniómetros o equipos similares; usando

técnicas receptivas puede hacer que nuestras comunicaciones se confundan, y se interrumpan, el volumen y tipo de tráfico puede hacer deducciones con relación a la potencia e intenciones de nuestras fuerzas. Por tal razón La Política de Emisiones de la Fuerza Armada Bolivariana es de Discreción, tratando de reducir al mínimo el empleo de los medios radioeléctricos.

b. A pesar de esto el radio permanece irremplazable como medio primario de comunicaciones militares. Es rápido y eficiente y la mayoría de las veces es el único de mantener contacto entre las unidades móviles y los puestos de comando ubicados a grandes distancias. Pero debe recalcarse la necesidad de su uso adecuado e inteligente satisfactorio. A tal efecto solo se usará:
   1) En caso de Necesidad. El radio deberá ser empleado solamente cuando sea esencial para las operaciones, y cuando los elementos del planeamiento y la capacidad de otros medios de comunicaciones no sean suficientes.
   2) Requerimientos mínimos. Las comunicaciones por radio serán restringidas al mínimo requerido para el cumplimiento de la misión o tarea asignada.
   3) Autorización. Ninguna transmisión de radio deberá hacerse si no ha sido autorizado por la autoridad correspondiente.

c. El Comando en todos los escalones, puede, durante un determinado período, imponer el siguiente político de emisión, para los medios electro-magnéticos:
   1) De Silencio. En el régimen de silencio, las estaciones no están autorizadas a transmitir; pero, sin embargo, se deben dedicar a la escucha permanente.
   2) De Discreción. En el régimen de discreción, la transmisión está autorizada, pero sólo para el caso de comunicaciones urgentes e importantes para las operaciones.
   3) De Libertad. En el régimen de libertad no existe restricción alguna

para el tráfico.

d. Consideraciones para la Formulación de la Política de Emisión (PE).

1) La Política de Emisión no sólo abarca todo el espectro electromagnético sino también las emisiones acústicas y su elección está fuertemente ligada con cualquier Plan de Cobertura o de Engaño requerido, frente a la luz de la capacidad de vigilancia total del adversario.

2) La Política de Emisión debe apoyar al objetivo de la misión en todos sus puntos y para la formulación de una política se deben tomar en cuenta las siguientes consideraciones:

a) La pérdida o ganancia operacional proveniente del uso de cada emisor.

b) El riesgo de interceptación.

c) El valor del adversario y su capacidad para usar la información que pueda obtener de la interceptación.

d) La necesidad de restringir ciertas emisiones de manera de mejorar la eficiencia de los propios equipos de interceptación.

3) Una forma útil de llegar a la formulación de una PE es hacer una lista con todos los emisores de la fuerza, y revisarla preguntándose si necesita realmente o no emitir con ese equipo (incluyendo otros emisores sónicos). El objetivo sería obligar a que el adversario trabaje muy duro para conseguir cada parte de la información que pueda recoger. Luego, la política sería la de examinar su consistencia en todos los aspectos. Inevitablemente la política termina como una serie de compromisos y es raro que puedan justificarse los argumentos de "todo encendido" o de "todo apagado". Lo que, es más, raramente es suficiente una sola política de emisión y se debe permitir la flexibilidad y cambios a medida que se desarrolla la situación.

4) El método mediante el cual se implementa la política de emisión se conoce como el Plan de Control de Emisión (Plan CONEM) y es

generalmente promulgada con los planes CONEM

5. RESPONSABILIDADES PARA LA ELABORACIÓN DEL PLAN CONEM.

a. El Comandante Estratégico Operacional a través del director de Comunicaciones de la Fuerza Armada Nacional Bolivariana, establecerá en las Instrucciones Permanentes de Comunicaciones (I.P.C) la Política de Emisiones y en la Publicación Complementaria (I.O.C), el Plan de Control de Emisiones de acuerdo a la situación táctica que se presente durante el desarrollo de las operaciones.

b. Cada comandante de Región de Estratégica de Defensa Integral y comandante de Componente, debe prever en sus IPC e IOC un Plan de Control de Emisiones.

SECCIÓN E

SEGURIDAD CRIPTOGRÁFICA

1. DEFINICIÓN.

Seguridad Criptográfica es el componente de la seguridad de las comunicaciones que resulta de la provisión de sistemas de seguridad con la finalidad de negar información de alto valor y clasificación a personal no autorizado. En general estos sistemas deberán ser lo suficientemente flexibles y de alta velocidad.

2. CRIPTOGRAMA.

Es una versión, en clave, del texto en lenguaje claro de una comunicación. La comunicación resultante es escrita en un texto ininteligible o en códigos especiales establecidos periódicamente con un significado específico y no el texto mismo del criptograma.

3. PRINCIPIOS GENERALES.

a. Una persona no autorizada que intercepte mensajes criptografiados y que es capaz de asociar este tráfico con hechos conocidos, estará capacitada para comenzar un trabajo para descubrir las claves y/o códigos de los sistemas criptográficos empleados. Por esto, es necesario evitar, tanto como sea practicable la relación entre el tráfico criptografiado y cualquier cosa que sea conocida por los extraños. Todas las reglas de seguridad criptográfica están basadas en este principio. Se ha hecho esfuerzo para proporcionar ayudas criptográficas diseñadas para ocultar tanto como sea posible, la relación que hay entre los textos criptografiados de los mensajes, y las claves inalterables de los mensajes que se cursen en lenguaje llano. En adición, las claves se cambian y se renuevan con suficiente frecuencia como para reducir al mínimo la posibilidad de conocimiento por los extraños. El sistema más complicado de ayuda criptográfica no podrá proporcionar una completa seguridad, si se le emplea con demasiada frecuencia, en tal sentido se deben tomar las máximas medidas de protección para negar al enemigo toda posibilidad de interceptación de nuestras transmisiones.

b. La seguridad criptográfica resulta de disponer de seguros sistemas criptográficos, técnicamente efectivos y de usarlos adecuadamente. Las claves y códigos, autorizados, si son bien empleados proporcionar seguridad, impidiendo su explotación y uso por parte del enemigo. Cada sistema de clave o código ve acompañado de instrucciones que se aplican específicamente a tal sistema. Ninguna persona debe ser autorizada para emplear un sistema criptográfico hasta que no haya recibido el adiestramiento teórico y práctico correspondiente y esté debidamente familiarizado con las instrucciones generales y específicas que lo regulan.

c. Todos los mensajes clasificados que deban ser transmitidos por medios electrónicos cuando exista el peligro de la interceptación enemiga o por personas no autorizadas, deben ser cifrados a excepción de aquellos

mensajes que requieran de una transmisión en forma inmediata, a saber:

1) Mensajes Operacionales: Los cuales pueden transmitirse en lenguaje claro o códigos abreviados, como información clasificada de inmediata explotación y que pudiendo ser interceptada por el enemigo no tenga influencia en el desarrollo de la operación, debido al poco tiempo que se dispone para tomar una determinada acción. Este tipo de mensaje deberá ser autorizado por el comandante.
2) Unidades Pequeñas: En situaciones de movimiento rápido los comandantes de Unidades pequeñas, pueden autorizar su envío en texto claro de aquellos mensajes que indiquen acciones inmediatas. Los mensajes de clasificación Secretos a ser transmitidos por medios eléctricos y/o electrónicos jamás puede ir el texto en lenguaje claro.
3) Los criptogramas deben ser mensajes concisos y claros; los mensajes extensos atentan contra la seguridad, rapidez y la fidelidad, por la mayor probabilidad de cometer errores en su elaboración y deben llevar el menor número posible de destinatarios.

b. Los requisitos de seguridad criptográfica son:

1) Requisitos de Producción.
2) Proporcionar sistemas criptográficos de alta seguridad.
3) Proveer un número suficiente de canales criptográficos que permita una distribución razonable del tráfico.
4) Cambiar frecuenten ente los componentes físicos, códigos y/o arreglos Operacionales internos y externos para minimizar le posibilidad de descodificación.

c. Requisitos de operación.

1) Clasificar apropiadamente los mensajes.
2) Redactar cuidadosamente los mensajes.
3) Escoger la ayuda criptográfica apropiada.
4) Criptografíar con cuidado y exactitud.

4. CLASIFICACIÓN APROPIADA.

a. Una apropiada clasificación se requiere:

1) Para la mejor distribución del tráfico.

2) Para evitar la relación que pudiera existir entre dos sistemas, como resultado de mensajes del mismo contenido, pero con diferentes clasificaciones.

3) Para evitar el que los sistemas informantes sean recargados con asuntos que no son importantes y altamente clasificados, el criptoanalista enemigo estará recibiendo gran cantidad de material de nuestros sistemas y aprovechando la oportunidad para resolver esos sistemas. Por otra parte, la tendencia hacia una clasificación muy baja sirve al enemigo para recibir información fácil de mensajes transmitidos.

b. Una vez que un mensaje clasificado ha sido manipulado en un canal especifico, ese mensaje no podrá ser nuevamente clasificado más bajo, aun cuando la información deje de ser materia clasificada.

c. Si en una de las etapas de la transmisión de un mensaje, una autoridad superior del trayecto nota que es necesaria una clasificación mayor o menor del mensaje, estará autorizada a hacer la reclasificación del mensaje, pero sólo con clasificación mayor.

5. REDACCIÓN

Una redacción cuidadosa para evitar fraseología estereotipada, redundancia y repeticiones excesivas, impide que el criptoanalista interceptor, utilice métodos estadísticos de solución que depende de la frecuencia probable en el uso de métodos habituales de expresión. Estos son los sistemas más fructíferos para el ataque criptoanalítico. Sin embargo, no hay que olvidar que el uso de palabras no comunes y modos de expresión no usuales, cuando son exagerados pueden llegar a obscurecer el significado del mensaje. El principio básico consiste en evitar hábitos.

a. El texto criptografiado y el texto en lenguaje llano de un mensaje, nunca

deben estar juntos. El texto de un mensaje debe ser íntegramente criptografiado o íntegramente en lenguaje llano.

b. El texto de los mensajes criptografiados deben tener diez grupos de columna en sentido horizontal y el número de grupos de todo el contenido del texto no debe ser mayor de 200 grupos, excepto los criptografiados por sistemas electrónicos, que no tiene límites por ser una ayuda criptográfica de avanzada tecnología.

c. Los siguientes hábitos de redacción son peligrosos y no recomendables:
   1) Comenzar habitualmente el mensaje con el nombre de la autoridad promotora o destinataria.
   2) Comenzar habitualmente el mensaje con expresiones como las siguientes: RESPUESTA SOLICITADA, SE ENVÍAN INSTRUCCIONES, AUTORIDAD, DENEGADO, INFORMADO etc.
   3) Terminar los mensajes habitualmente con la fecha.

d. Los mensajes criptografiados no deben contener informaciones literales de periódicos, conversaciones telefónicas, exposiciones de conversaciones personales, publicaciones, otros mensajes cursados en lenguaje llano o cualquier otra forma de comunicación no criptografiada. Si fuera necesario insertar un párrafo conocido dentro de un despacho criptografiado, la materia insertada debe ser previamente parafraseada.

e. No se debe copiar el texto íntegro de un mensaje criptografiado o una parte de éste en otra clase de comunicación oral o escrita. La información contenida en un mensaje criptografiado y que debe ser incluida en otra comunicación seré previamente parafraseada, sin mencionar el mensaje que dio origen y que de otra manera sería identificado.

f. Un mensaje que ha sido transmitido criptografiado en una clave no debe ser criptografiado textualmente en otra clave.

g. Los Oficiales de Comunicaciones cuando noten que la redacción de un mensaje no se ha hecho de acuerdo con los principios de seguridad, o cuando observen una mala práctica de las comunicaciones, sugerirán al promotor los cambios necesarios. Si esto no es practicable porque

significaría demora, el mensaje será transmitido sin alteración, con excepción de que el oficial de comunicaciones puede hacer pequeños cambios simples que no afecten el significado. El oficial de comunicaciones debe evitar cualquier posibilidad de que se obscurezca o tergiverse el pensamiento del promotor.

6. SELECCIÓN DEL SISTEMA CRIPTOGRÁFICO.
   a. Es importante efectuar la selección de la ayuda criptográfica a usarse, cuando se manipulan varias clases de mensajes. Es tan importante como la clasificación apropiada, por las mismas razones. Los canales criptográficos de la Armada están subdivididos para proporcionar la máxima protección a la mayoría de las claves, en caso de que una cayera en poder del enemigo. El principio es aislar el daño.
   b. Las siguientes reglas son de aplicación general para la selección de la ayuda criptográfica en un mensaje en particular.
      1) Los mensajes clasificados normalmente deben emplea) los canales criptográficos establecidos para cada clasificación en particular.
      2) Los sistemas diseñados y prescritos para usos especiales solo deberán ser usados para esos propósitos.
      3) Normalmente un mensaje clasificado debe emplear el canal criptográfico apropiado como para tener la más limitada distribución que cubra todas las direcciones del preámbulo en él.

7. CRIPTOGRAFÍA.
   a. Los criptoanalistas consiguen la mayor parte de sus éxitos, valiéndose de los errores cometidos en el uso de los códigos y las claves. Por esto, es de gran importancia criptografíar con propiedad y exactitud. Cada paso del método prescrito al usar un sistema está designado para prevenir tales errores o para proveer protección contra alguna forma particular de ataque analítico. El operador de un sistema criptográfico debe conocer las reglas aplicables a ese sistema y las estrictamente inherentes.

b. Las reglas detalladas para el uso de las varias ayudas criptográficas están contenidas en las instrucciones individuales que acompañan a cada una.

c. Para proteger la debilidad criptográfica de los mensajes criptografiados debido a la fácil identificación de las palabras comunes, (fraseología estereotipada) usualmente empleadas al principio y al final del texto, se establecen los métodos siguientes para ser usados desde Confidencial hasta la más alta clasificación de seguridad.

1) Bisección: Consiste en dividir el texto en lenguaje llano, en dos segmentos desiguales, añadiéndole un grupo de cinco (5) consonantes iguales que no sean X ni Z, que sirve de separador entre los dos segmentos. El principio del texto, que está siempre después del grupo separador de las cinco consonantes, se coloca indistintamente en cualquier lugar de la bisección, cuidando siempre de no ponérselo nunca al comienzo, en la parte media o al final del texto.

2) Rellenado: Consiste en la adición de una o más palabras colocadas al comienzo o final del texto de un mensaje, para disfrazar la fraseología estereotipada que se ha usado. El rellenado se emplea también para variar la longitud de los mensajes de rutina criptografiados, transmitidos a intervalos frecuentes. El uso innecesario del rellenado ocasiona pérdida de tiempo en criptografíar, transmitir y descriptografiar.

d. Uno de los problemas de comunicaciones, al usar bisección o rellenado, es conocer qué palabras o frases son estereotipadas. La experiencia ha demostrado que la mayoría de los mensajes empiezan con una de las siguientes palabras: ESTISUIN (**Estimole sus instrucciones**), RESU (**Referente a su**), ESTINF (**Estimole informar**), SURAD (**Referente a su radiograma**), PACOFI (**Para conocimiento y fines**), ESTIREBRE (**Estimole remitir a la brevedad**), REMI (**Referente a mi**), MIRAD (**Hacer referencia a radiograma escrito por promotor**), ACURE

(**Acuse de recibido**). Esta lista de palabras provee un excelente punto de partida para determinar qué palabras son típicamente estereotipadas. Cualquier palabra puede convertirse en estereotipada, en una o más áreas, si el promotor la usa continuamente, como primera o última palabra en el texto de sus mensajes.

e. Se debe evitar el uso de las palabras o frases estereotipadas al comienzo o fin del texto, en los mensajes criptografiados.

8. PARAFRASEADO.

Es un compromiso entre los requisitos de seguridad y la conveniencia, pero debe ser hecho con gran cuidado y con una completa apreciación de sus posibilidades y limitaciones. El parafraseado debe cumplir los siguientes requisitos.

a. La versión parafraseada debe tener el mismo significado que la versión original, y debe ser igualmente clara.
b. Deben sustituirse tanto como sea practicable, los sinónimos y las expresiones de este género.
c. Se debe alterar el orden de las oraciones y frases o se pueden recombinar.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO III

SECCIÓN A

SEGURIDAD INFORMÁTICA

1. MODELO DE SEGURIDAD INFORMÁTICA PARA LA FANB.

El Modelo de Seguridad Informática para la FANB, está formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Estas capas son:

a. Organización
b. Análisis y Gestión de Riesgos
c. Política de seguridad de la organización.
d. Sistema de Auditoría.
e. Sistemas de seguridad a nivel de RED de Área Amplia.
f. Sistemas de detección de intrusos (Redes Locales).
g. Plan de respuesta a incidentes (Plan de Contingencia).
h. Pruebas de Penetración.
    1) Este modelo está orientado a lograr la autenticidad, confidencialidad, integridad y disponibilidad de los datos y debe abarcar todas las capas del MODELO ISO/OSI.
    2) La Confidencialidad es la condición que asegura que la información no puede estar disponible o ser descubierta por o para personas, entidades o procesos. La confidencialidad a menudo se relaciona con la intimidad cuando se refiere a personas físicas. La confidencialidad de los datos exige medidas específicas también en su eliminación o de los soportes en los que hubieran estado almacenados.
    3) La Norma ISO 7498-2 también la define como: Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados.

4) La integridad es la condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. La integridad está ligada a la fiabilidad funcional del sistema de información, a su eficacia para cumplir las funciones para las que fue creado.
5) La Norma ISO 7498-2, también la define como: Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado.
6) La Disponibilidad es el grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información.
7) La Norma ISO 7498-2, también la define como: Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada.
8) Se ha de tener en cuenta que en la disponibilidad intervienen múltiples aspectos: Unas adecuadas instalaciones y equipamiento físico, un adecuado dimensionamiento de la plataforma tecnológica que permita hacer frente a escenarios variables de carga de trabajo, o posibles fallos, procedimientos de explotación y de mantenimiento, protección contra código dañino y frente a intentos de intrusión o ataques de denegación de servicio, así como procedimientos relativos a la gestión de la información que pueda almacenarse cifrada o codificada que garanticen la gestión de claves. La eliminación de errores de codificación y la adopción de estándares y especificaciones públicas de programación pueden facilitar el control de la aplicación (software libre).
9) La autenticación se refiere a la capacidad de verificar que un usuario, convenientemente identificado, que accede a un sistema o aplicación

es quien dice ser; o que un usuario que ha generado un documento o información es quien dice ser.

10) La identificación de los usuarios y la verificación de la autenticidad de la misma es un requisito previo a la autorización del acceso a los recursos del sistema. Es conveniente apuntar que el proceso de autenticación de la identidad de las personas lleva asociado, de forma implícita, la manifestación de la voluntad de la misma, que se extiende a todas y a cada una de las operaciones que realice a partir de haberse identificado y autenticado su identidad, hasta que, mediante una acción bien determinada, por ejemplo, desconectándose de la sesión de trabajo, manifiesta su voluntad de no continuar.
11) Según la Norma ISO 7498-2 la autenticación se define como: Servicio de seguridad que se puede referir al origen de los datos o a una entidad homóloga. Garantiza que el origen de datos, o entidad homóloga, son quienes afirman ser.
12) Para este servicio se pueden usar métodos de autenticación fuerte o autenticación simple, en función del nivel de clasificación de la información y el nivel de acceso que posee el usuario.
13) Autenticación fuerte: Autenticación basada en la utilización de técnicas de criptografía asimétrica y en el uso de certificados electrónicos. También suele referirse a la combinación de algo que el usuario posee (por ejemplo, una tarjeta electrónica) con algo que el usuario conoce (como las claves conocidas como "PIN").
14) Autenticación simple: Autenticación basada en mecanismos tradicionales de usuario y contraseña.

2. ORGANIZACIÓN.

a. La Dirección de Comunicaciones de la FANB, a través de la División de Informática será la encargada de establecer las políticas de seguridad y sistema de auditoria, aplicables a la Fuerza Armada Nacional Bolivariana.

b. Las Direcciones de Comunicaciones de Componentes y REDI, deben incluir en sus estructuras los elementos que permitan implementar estas políticas.

c. Básicamente esa estructura será la encargada de administrar la seguridad informática en su área de responsabilidad.

d. Las tareas de administración de seguridad se pueden agrupar en tres grandes áreas:

   1) Autenticación: Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

   2) Autorización: Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

   3) Auditoría: Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

e. La organización debe definir y documentar las funciones y obligaciones del personal, en particular en relación con el acceso y utilización de los sistemas de información y, en particular, en relación con el acceso a los datos de carácter personal. Definir las responsabilidades relacionadas con la seguridad en cada puesto de trabajo, debiendo aplicar el principio de segregación de funciones.

f. Otra tarea del área de seguridad es dar a conocer al personal las medidas de seguridad que afecten al desarrollo de sus funciones y que en su caso deban aplicar, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

g. Para lograr la seguridad se deben emplear algunos de los métodos de protección que se indican a continuación:

   Sistemas de detección de intrusos: Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o

eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

1) Sistemas orientados a conexión de red: monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.
2) Sistemas de análisis de vulnerabilidades: Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
3) Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.
4) Sistemas de protección a la privacidad de la información: Herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

3. ANÁLISIS Y GESTIÓN DE RIESGOS.

a. El proceso de análisis y gestión de riesgos constituye la tarea primera y a la vez esencial de toda actuación organizada en materia de seguridad. Permite conocer de manera rigurosa el estado de seguridad y determinar

la valoración del riesgo. Es adecuado en las fases y actividades de carácter general (gestión global y política de seguridad con la implicación de la dirección) y en las de carácter específico de un determinado sistema de información (planificación, organización, implantación de salvaguardas, sensibilización, operación y mantenimiento).

b. El análisis y la gestión de los riesgos tiene como objetivo proporcionar evidencias racionales que permitan tomar decisiones acerca de la seguridad imprescindible para que las organizaciones puedan cumplir su misión.

c. El análisis de los riesgos: Identificación de las amenazas que acechan a los activos (componentes pertenecientes o relacionados con el sistema de información) y determinación de la vulnerabilidad de los activos ante esas amenazas. Con lo anterior se estima el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización a partir del cual se calcula el riesgo que se corre.

d. La Gestión de los riesgos: Selección e implantación de las medidas de seguridad o 'salvaguardas' adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

e. Identificación de activos a proteger: Se debe realizar y mantener un inventario de los activos a proteger (información, equipamiento del sistema, soportes e información, otros equipos - climatización, alimentación, etc.).

f. Para cada activo se debe identificar a su propietario, así como su valor e importancia en términos cuantitativos o cualitativos, en función de los requisitos de autenticidad, integridad, confidencialidad y disponibilidad que le son aplicables. Esta información es crucial, pues facilita el análisis y gestión de riesgos y, por tanto, sirve, para determinar las medidas de seguridad proporcionadas.

h. La identificación de amenazas requiere conocer los tipos de ataques, el

tipo de acceso, la forma operacional y los objetivos del atacante.

i. Las consecuencias de los ataques se podrían clasificar en:
    1) Corrupción de Datos: La información que no contenía defectos pasa a tenerlos.
    2) Deterioro de la Calidad de Servicio: Servicios que deberían estar disponibles no lo están.
    3) Desvíos: Los datos llegan a destinos a los que no deberían llegar.

4. POLÍTICA DE SEGURIDAD.
    a. La Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema.
    b. Es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.
    c. La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; ante todo, una política de seguridad es una forma de comunicarse con los usuarios, siempre hay que tener en cuenta que la seguridad comienza y termina con personas.
    d. Finalmente, por política de seguridad se entiende el conjunto de normas, reglas y prácticas, que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de una organización.
    e. Contenido de la política de seguridad:
        1) Objeto del documento.
        2) Ámbito de aplicación de la política de seguridad.
        3) Recursos protegidos.
        4) Funciones y obligaciones del personal.

5) Normas, procedimientos, reglas, estándares y medidas para garantizar
6) La autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.
7) Identificación, autenticación y control de accesos
8) Gestión de incidencias de seguridad.
9) Gestión de soportes y copias de respaldo.
10) Acceso a través de redes.
11) Contingencias y continuidad del servicio.
12) Controles periódicos de verificación del cumplimiento.

f. Estas Políticas deben contener como anexos:
1) Documentos de notificación y normas de creación de ficheros o de la aplicación para el ejercicio de potestades.
2) Descripción de la aplicación y del sistema informático.
3) Descripción de la estructura de ficheros o bases de datos.
4) Entorno del sistema operativo y de comunicaciones.
5) Descripción de locales y equipamientos.
6) Análisis y gestión de riesgos.
7) Descripción de las funciones y obligaciones del personal.
Personal autorizado para acceder al fichero/aplicación.
8) Procedimientos de control de accesos y perfiles de usuarios.
9) Gestión de soportes de información.
10) Gestión de copias de respaldo y recuperación.
11) Procedimientos de notificación y gestión de incidencias.
12) Plan de contingencias.
13) Auditorias y controles periódicos.

5. AUDITORIA Y CONTROL DE SEGURIDAD

a. Es el proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que

se compara la evidencia.

A tal efecto, la Dirección de Comunicaciones de la FANB, elaborará una guía de inspección y verificación de seguridad de los sistemas informáticos para ser utilizado en los procesos de auditoria a los Comandos de Componentes y REDI.

b. La Dirección de Comunicaciones de la FANB, elaborará un Plan de Auditorias de Seguridad a ser aplicado a las unidades de la Fuerza Armada Bolivariana.

6. PLAN DE CONTINGENCIAS.

a. El plan de contingencias es la forma detallada en que la organización debe reaccionar para asegurar que las aplicaciones sigan activas ante determinados eventos, accidentales o deliberados.

b. La elaboración de un plan de contingencias debe tener en cuenta aspectos tales como la magnitud del riesgo de la aplicación afectada, incluyendo las interdependencias con otras aplicaciones; así como las prioridades de los distintos elementos de la aplicación, considerando el valor que cada elemento supone para la organización.

c. El análisis y gestión de riesgos genera información sobre las posibles consecuencias de distintos tipos de eventos de carácter accidental o deliberado (desastres, ataques y fallos de la aplicación e de interrupciones del servicio). El plan de contingencias se desarrolla para garantizar la continuidad de la aplicación dentro de un determinado intervalo de tiempo. Este plan debe ser mantenido a lo largo de la vida de la aplicación, y además se deberá formar al personal en su puesta en marcha.

d. La gestión de la continuidad debe incluir los controles para identificar y reducir riesgos, limitar las consecuencias de incidentes y garantizar la recuperación de las operaciones principales en un intervalo de tiempo aceptable.

7. SEGURIDAD DE RED EXTREMO A EXTREMO.

a. La Recomendación X.805 del UIT-T, “Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo”, define una arquitectura de seguridad de red para proveer seguridad de red de extremo a extremo. Esta arquitectura puede ser aplicada a varios tipos de redes en las que la seguridad de extremo a extremo es una preocupación y es independiente de la tecnología subyacente de la red. Esta Recomendación define los elementos arquitectónicos generales relacionados con la seguridad que son necesarios para proveer seguridad de extremo a extremo. El objetivo de esta Recomendación es servir como base para desarrollar Recomendaciones detalladas para seguridad de red de extremo a extremo.

b. La arquitectura aborda preocupaciones de seguridad para la administración, control y uso de la infraestructura, servicios y aplicaciones de la red. Provee una perspectiva exhaustiva, descendente, de extremo a extremo, de seguridad de red y puede ser aplicada a elementos, servicios y aplicaciones de red para detectar, predecir y corregir vulnerabilidades de seguridad.

c. La arquitectura de seguridad lógicamente divide un conjunto complejo de características relacionadas a la seguridad de red de extremo a extremo en componentes arquitectónicos separados. Esta separación permite un enfoque sistemático de la seguridad de extremo a extremo que puede ser usado para planificar nuevas soluciones de seguridad al igual que para determinar la seguridad de las redes existentes. Se abordan tres componentes arquitectónicos: Dimensiones de seguridad, niveles de seguridad y planos de seguridad.

d. Dimensiones de Seguridad. Una dimensión de seguridad es un conjunto de medidas diseñadas para abordar un aspecto particular de seguridad de red. Esta Recomendación X.805 identifica ocho de estos conjuntos que protegen contra todas las principales amenazas de seguridad. Las dimensiones de seguridad son:

1) Control de acceso
2) Autenticación
3) No repudio
4) Confidencialidad de la información
5) Seguridad de la comunicación
6) Integridad de la información
7) Disponibilidad
8) Privacidad

e. Niveles de Seguridad. Para proveer una solución de seguridad de extremo a extremo, las dimensiones de seguridad deben ser aplicadas a una jerarquía de equipo de red y agrupamientos de instalaciones, a las que nos referimos como niveles de seguridad. La Recomendación X.805 define tres niveles de seguridad:
   1) Nivel de Seguridad de la Infraestructura
   2) Nivel de Seguridad de los Servicios
   3) Nivel de Seguridad de las Aplicaciones

f. Los niveles de seguridad son una serie de factores que permiten soluciones de redes seguras: El nivel de la infraestructura habilita al nivel de los servicios y el nivel de los servicios habilita al nivel de las aplicaciones. Los niveles de seguridad identifican los lugares donde la seguridad debe ser abordada en productos y soluciones, proveyendo una perspectiva secuencial de seguridad de red.

g. Planos de Seguridad. Un plano de seguridad es un cierto tipo de actividad de red protegida por dimensiones de seguridad. La Recomendación X.805 define tres planos de seguridad para representar los tres tipos de actividades protegidas que tienen lugar en una red. Los planos de seguridad son:
   1) Plano de Administración
   2) Plano de Control
   3) Plano del Usuario Final

h. Estos planos de seguridad abordan necesidades de seguridad

específicas asociadas con actividades de administración de la red, control de red o señalización de actividades y actividades del usuario final, respectivamente.

i. La arquitectura de seguridad descrita en la Recomendación X.805 puede ser usada para guiar el desarrollo de definiciones de políticas de seguridad exhaustivas, planes de respuesta a incidentes y de recuperación y arquitecturas de tecnología, tomando en consideración cada dimensión de seguridad en cada nivel y plano de seguridad durante la fase de definición y planificación. La arquitectura de seguridad también puede ser usada como la base de una evaluación de seguridad que examinaría cómo la implementación del programa de seguridad aborda las dimensiones, niveles y planos de seguridad, a medida que se expiden políticas y procedimientos y se despliega la tecnología.

8. SEGURIDAD FÍSICA Y LÓGICA.

a. Para los efectos de planificación y aplicación de medidas tendientes a elevar el nivel de seguridad informática, se establecen dos subgrupos, la seguridad física y la seguridad lógica.

b. La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial o secreta. Se refiere a los controles y mecanismos de seguridad dentro y alrededor de los Centro de Cómputo; así como, los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

c. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

d. Las principales amenazas que se prevén en la seguridad física son:

1) Desastres naturales, incendios accidentales tormentas e inundaciones.

2) Amenazas ocasionadas por el hombre.
3) Disturbios, sabotajes internos y externos deliberados.

e. Para asegurar la seguridad física de los sistemas informáticos se hace necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

e. Para protegerlos se debe tener en cuenta que:

1) La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
2) Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
3) Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

g. La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

h. Los objetivos que se plantean serán:

1) Restringir el acceso a los programas y archivos.
2) Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3) Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4) Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5) Que la información recibida sea la misma que ha sido transmitida.
6) Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7) Que se disponga de pasos alternativos de emergencia para la

transmisión de información.

SECCIÓN B

VIOLACIONES DE SEGURIDAD

1. GENERALIDADES.
   a. Existen dos tipos de violaciones de seguridad; una es el denominado compromiso o posible compromiso de información clasificada y el otro ocurre cuando son violadas las normas de seguridad, pero no existe compromiso.
   b. Todo el personal de la Fuerza Armada Bolivariana está en la obligación de notificar de inmediato a su comando cuando se entere por cualquier medio de alguna violación de seguridad de material clasificado, independientemente de grado, condición, empleo u oficio dentro de la organización.

2. COMPROMISO.
   a. Es la situación que se presenta cuando personas no autorizadas obtienen información clasificada contenida en determinada publicación o base de datos; en este caso se dice, que la información contenida en esa publicación se halla en condición de compromiso.
   b. El compromiso de una publicación o base de datos se confirma cuando existen evidencias de que la información en ella contenida, ha sido puesta en el conocimiento de personas no autorizadas.
   c. El compromiso de información clasificada representa una amenaza para la seguridad de la Nación de sus Fuerzas Armadas.
   d. La seriedad de esta amenaza debe ser determinada y tomarse de inmediato las acciones para negar o minimizar los efectos adversos a ser causados por, este compromiso.

3. OTRAS VIOLACIONES DE SEGURIDAD.

Obviamente el compromiso representa la amenaza más grande para la seguridad de la Nación o de la Fuerza Armada Nacional Bolivariana, pero todas las demás violaciones de seguridad deben ser tratadas seriamente porque ellos demuestran que existe una fuga de información o brechas en los sistemas o regulaciones de seguridad de comunicaciones. Por esta razón, cada una de las violaciones de seguridad deben ser investigadas exhaustivamente para determinar las causas que la motivaron, debiéndose aplicar los correctivos necesarios para esta situación, además de la determinación de las sanciones respectivas en caso de negligencia por los responsables del manejo de esa información o publicación.

4. MEDIDAS DISCIPLINARIAS.

a. Todo Comando de Unidad o Dependencia de la Fuerza Armada Nacional Bolivariana en el cual se manejan publicaciones, información o material clasificado establecerá y mantendrá un programa activo de educación en los aspectos concernientes a la políticas y procedimientos de seguridad, el cual será impartido a todo el personal que por el cargo que ocupe o por su grado, tenga acceso autorizado a información clasificada.

b. El propósito de esta instrucción en asuntos de seguridad es:

1) Asegurar que todo el personal con acceso a la información y material clasificado entienda qué es “Información y material clasificado” y porque y como protegerla de personal no autorizado.

2) Advertir al personal la necesidad de su protección por los efectos adversos para la seguridad nacional, resultantes de la obtención de esta información por personas no autorizadas.

3) Informar al personal sobre las técnicas empleadas por las agencias de inteligencia de los demás países para obtener información clasificada y su responsabilidad en cuanto al reporte de cualquier intento detectado.

4) Advertir al personal sobre las acciones disciplinarias y penales por

ver comprometido en asuntos de espionaje.

5) Advertir al personal el peligro que ocurre cuando se discuten o tratan asuntos clasificado por teléfono o por cualquier otro medio susceptible a intercepción por personas no autorizadas.
6) Advertir al personal sobre las acciones disciplinarias o penales que resultan de la negligencia comprobada en el caso del manejo de la información clasificada.
7) Advertir a los supervisores sobre la necesidad de mantener una evaluación continua del personal seleccionado para acceso al material clasificado o para desempeñar cargo en áreas donde se utilice este tipo de material.
8) Advertir al personal sobre el riesgo que implica retirar material clasificado y utilízalo fuera de áreas con seguridad adecuada.
9) Informar al personal sobre la necesidad de notificar cualquier conocimiento de ciudadanos extranjeros en áreas restringidas de información clasificada.

c. Cualquier brecha de seguridad debe ser inmediatamente informada.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPITULO IV

COMUNICACIONES SATÉLITALES

1. GENERALIDADES

Las comunicaciones satelitales son el uso de satélites en órbita para transmitir señales de forma inalámbrica, actuando como repetidores en el espacio para conectar puntos en la Tierra. Permiten la transmisión de voz, datos y video a través de largas distancias, incluso en áreas remotas, y son vitales para servicios como la telefonía satelital, Internet de banda ancha, televisión y comunicaciones móviles.

a. Componentes principales.
   1) Segmento espacial: El satélite en sí mismo, que actúa como un repetidor en el espacio y está equipado con antenas y transpondedores.
   2) Segmento terrestre: Incluye las estaciones terrenas con sus antenas para enviar y recibir señales, así como el equipo auxiliar necesario en los puntos de origen y destino.

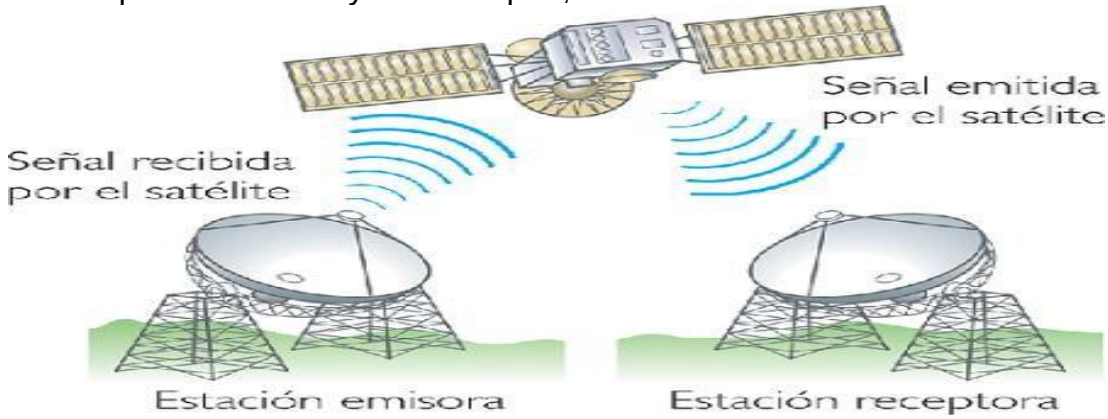
b. Funcionamiento básico.
   1) Enlace de subida: Una estación terrena transmite una señal de radiofrecuencia a un satélite.
   2) Procesamiento en el satélite: El satélite recibe la señal, la amplifica, cambia su frecuencia y la prepara para ser retransmitida.
   3) Enlace de bajada: El satélite reenvía la señal procesada a una o varias estaciones terrenas en la Tierra.

c. Características clave.
   1) Alcance global: Permite la comunicación en cualquier lugar del planeta, haciendo irrelevante la distancia física.
   2) Conectividad en zonas remotas: Es una solución esencial para lugares sin acceso a infraestructura terrestre como fibra óptica o torres de telefonía celular.

3) Estabilidad y capacidad: Utiliza señales de radiofrecuencia de alta calidad que resultan en conexiones estables y capacidad para manejar diversos tipos de tráfico de información.
4) Frecuencia: Opera en diferentes bandas de frecuencia (como C, Ku y Ka) para la transmisión y recepción, lo que permite una mayor eficiencia y separación de las señales.
5) Estas bandas que usan los satélites trabajan en los siguientes rangos de frecuencias, la banda C estándar abarca de 3,7 a 4,2 GHz.; la banda Ku para satélites es aproximadamente de 12 a 18 GHz. y la banda Ka para satélites es de 26.5 a 40 GHz.
6) Tipos de servicios y aplicaciones.
7) Servicios: Los satélites proporcionan telecomunicaciones, radiodifusión y comunicaciones de datos.
8) Aplicaciones: Se aplican en servicios como la televisión satelital, telefonía satelital, acceso a internet satelital y en la industria de defensa, entre otras.
9) Radiodifusión: Televisión y radio satelital.
10) Otras industrias: Soporte para operaciones en el sector marítimo, minero y de petróleo y gas en ubicaciones remotas.
11) Defensa y seguridad: Comunicaciones seguras y resilientes para fuerzas armadas.

d. ¿Cómo funcionan las Comunicaciones Satelitales?

El propio satélite actúa como canal de comunicación entre un dispositivo emisor y otro receptor, difundiendo información a través de



ondas electromagnéticas. En la práctica, las antenas en tierra se utilizan para enviar señales al satélite, que a su vez las transmite a otra antena en una ubicación diferente. La comunicación se divide en dos fases principales: Un "enlace ascendente" donde la señal viaja de la Tierra al satélite, y un "enlace descendente" donde el satélite la envía de vuelta a estaciones en la Tierra. También se dice que la comunicación puede ser unidireccional, cuando la señal se envía de un dispositivo a otro en una sola dirección o de manera bidireccional, intercambiando señales en direcciones opuestas entre dispositivos.

e. Pasos del proceso.
    1) Enlace ascendente (Uplink): Una estación terrestre envía una señal de radio a un satélite en órbita. El satélite, que está equipado con un transpondedor, recibe esta señal.
    2) Procesamiento en el satélite: El transpondedor del satélite amplifica la señal recibida, que puede haber perdido potencia en su viaje a través de la atmósfera.
    3) Enlace descendente (Downlink): El satélite vuelve a transmitir la señal amplificada a la Tierra, enviándola a otra estación terrestre, un área de recepción más amplia o múltiples receptores simultáneamente.

2. DEFINICIÓN DE TÉRMINOS.
    a. Artificial: Algo que no es natural, sino hecho por el ser humano o con un propósito.
    b. Bélico: Es un adjetivo que se refiere a todo lo relacionado con la guerra.
    c. Cartografía: Es la ciencia y el arte de hacer, estudiar y analizar mapas.
    d. Cobertura: Cantidad o porcentaje abarcado por una cosa o una actividad.
    e. Comunicación: Es el proceso de transmitir y recibir mensajes, ideas e información entre dos o más personas a través de un código común. Es

fundamental para la sociedad, ya que permite establecer relaciones, compartir conocimientos y organizarse.

f. Conectividad: Es la capacidad de dispositivos, sistemas o personas para comunicarse e intercambiar información entre sí, ya sea a través de medios físicos (cables, fibra óptica) o digitales (inalámbricos, internet).

g. Geoestacionaria: Es una órbita circular sobre el ecuador de la Tierra, a una altitud de aproximadamente 35,786 km, en la que un satélite se mantiene inmóvil respecto a un punto en la superficie terrestre porque su período orbital coincide con la rotación de la Tierra.

h. Investigación: Es un proceso sistemático, creativo y metódico de indagación para aumentar el conocimiento, resolver problemas o explicar fenómenos.

i. Microsatélites: Son satélites pequeños (entre 10 y 100 kg) que se utilizan para una amplia gama de aplicaciones, incluyendo la transmisión de datos y la comunicación.

j. Minisatélites: Son satélites pequeños, generalmente con un peso de entre 100 y 500 kg, que se usan para tareas como teledetección y telecomunicaciones.

k. Nanosatélites: Es cualquier satélite que pese menos de 10 kilos.

l. Navegación: Es el proceso de determinar la posición y el rumbo para viajar de un lugar a otro, ya sea físicamente (marítima, terrestre, aérea o espacial) o virtualmente (navegación web)

m. Observación: Es la acción de examinar atentamente un fenómeno, hecho o caso para recopilar información y registrarla para su posterior análisis.

n. Órbita: Se refiere a la trayectoria curva que un cuerpo describe al moverse alrededor de otro (como la de un planeta alrededor del Sol) o a la cuenca del ojo en la anatomía.

o. Remoto: Sumamente distante o lejano, en el espacio o en el tiempo.

p. Repetidor: Es un dispositivo que recibe una señal débil, la amplifica o regenera, y la retransmite para extender el alcance de la comunicación.

q. Satélite: El satélite recibe, amplifica, cambia la frecuencia de la señal y la retransmite. Su carga útil incluye antenas y repetidores.

3. BENEFICIOS DE LA COMUNICACIÓN SATÉLITAL**.**

a. Cobertura global: Permite que las organizaciones y las personas se comuniquen en cualquier parte del mundo, incluso en áreas remotas donde la infraestructura terrestre es escasa o inexistente. Esto hace que la comunicación por satélite sea una opción atractiva para empresas que operan en varios países o que necesitan mantener una comunicación ininterrumpida.

b. Calidad: La comunicación por satélite utiliza señales de radio de alta frecuencia para transmitir datos, lo que generalmente da como resultado una conexión más estable. También es superior en términos de velocidad y capacidad, lo que la hace apta para soportar varios tipos de tráfico de informaciones.

c. Confiabilidad: Uno de los principales diferenciales de la comunicación vía satélite es la seguridad, ya que los datos están encriptados y protegidos contra posibles violaciones de la privacidad. Además, es menos susceptible a interferencias electromagnéticas y de otro tipo, lo que da como resultado una conexión más confiable.

d. Flexibilidad: Permite a las empresas ser flexibles en sus operaciones, posibilitando la comunicación en áreas remotas y en situaciones de emergencia. Además, la configuración es sencilla, por lo que es una alternativa interesante para empresas que necesitan una solución práctica y ágil.

4. TIPOS DE SATÉLITES.

Los satélites se clasifican principalmente en naturales (como la Luna) y artificiales, que son máquinas creadas por el ser humano. Los satélites artificiales pueden subdividirse según su órbita (baja, media, geoestacionaria), su tamaño (minisatélites, microsatélites, nanosatélites) y su función (observación, comunicación, navegación).

a. Según su origen:
    1) Satélites naturales: Cuerpos celestes que orbitan alrededor de un planeta. El ejemplo más conocido es la Luna, que órbita la Tierra, aunque hay cientos más en el sistema solar.
    2) Satélites artificiales: Máquinas construidas por humanos, lanzadas al espacio y puestas en órbita para realizar diversas tareas, como la comunicación, la observación de la Tierra, la meteorología o la investigación científica.
b. Según su órbita:
    1) Órbita terrestre baja (LEO): Satélites que orbitan a altitudes de hasta 2,000 km.
    2) Órbita terrestre media (MEO): Satélites a una altitud intermedia entre la órbita baja y la geoestacionaria.
    3) Órbita geoestacionaria (GEO): Se encuentran a unos 36,000 km sobre el ecuador. Giran a la misma velocidad que la Tierra, por lo que parecen estar fijos en un punto sobre la superficie terrestre.
c. Según su tamaño y masa
    1) Minisatélites: Masa entre 100 y 500 kg.
    2) Microsatélites: Masa entre 10 y 100 kg.
    3) Nanosatélites: Masa entre 1 y 10 kg.
    4) Picosatélites: Masa entre 0.1 y 1 kg.
d. Según su función
    1) Satélites de observación: Utilizados para la observación terrestre, el monitoreo del clima, la cartografía y la vigilancia.
    2) Satélites de comunicación: Se emplean para retransmitir señales de televisión, telefonía y datos.
    3) Satélites de navegación: Proporcionan servicios de posicionamiento global, como el GPS.
    4) Satélites de investigación: Llevan a cabo experimentos y estudios en el espacio, como la Estación Espacial Internacional.

5. CONSIDERACIONES BÁSICAS DE SEGURIDAD EN LAS COMUNICACIONES SATÉLITALES.

Las consideraciones básicas de seguridad en las comunicaciones Satelitales incluyen el cifrado robusto de datos (como AES), la protección contra ciberataques en estaciones terrestres y satélites, el uso de autenticación y control de acceso para proteger la información, y la gestión segura del hardware y software, incluyendo la planificación de contingencias y mantenimientos.

a. Consideraciones técnicas:
    1) Cifrado de datos: Es fundamental implementar protocolos de cifrado avanzado como el AES para proteger los datos en tránsito y en reposo contra accesos no autorizados.
    2) Criptografía: Utilizar técnicas como RSA y Diffie-Hellman, además de la criptografía cuántica, puede crear comunicaciones prácticamente invulnerables.
    3) Ciberseguridad del sistema: Proteger tanto el satélite como las estaciones terrestres mediante firewalls, sistemas de detección de intrusos y monitoreo constante del tráfico.
    4) Segmentación de redes: Dividir la red en segmentos más pequeños para limitar el impacto de una brecha de seguridad.
b. Consideraciones de infraestructura física y operativa.
    1) Seguridad física: Proteger físicamente el equipo de tierra, como antenas y centros de datos, contra el sabotaje y el acceso no autorizado.
    2) Gestión de hardware y software: Asegurar la integridad del software de operación, implementar un mantenimiento preventivo y tener planes de contingencia para fallas de hardware y cortes de energía.
    3) Actualizaciones regulares: Mantener el software de los dispositivos y la aplicación emparejada actualizada para protegerse contra vulnerabilidades conocidas.
c. Consideraciones de uso y acceso.

1) Autenticación: Implementar métodos de autenticación robustos para verificar la identidad de los usuarios y dispositivos que acceden a la red.
2) Control de acceso: Definir claramente quién tiene permiso para acceder a ciertos datos o funciones del sistema.
3) Contraseñas seguras: Utilizar contraseñas fuertes y únicas para el acceso a cuentas y dispositivos.

d. Consideraciones de operación diaria.

1) Uso de dispositivos de forma segura: Emparejar el dispositivo con la aplicación correcta y sincronizar las actualizaciones antes de usarlo, especialmente en exteriores o en zonas de alta actividad.
2) Prueba de funcionamiento: Realizar pruebas antes de un viaje importante para confirmar que el dispositivo y el plan de suscripción están funcionando correctamente.
3) Entorno de comunicación: Buscar un lugar tranquilo y con señal fuerte para evitar el ruido de fondo que puede afectar la claridad de la comunicación, especialmente en llamadas.

6. USO DE LA COMUNICACIÓN SATÉLITAL PARA LA DEFENSA INTEGRAL DE LA NACIÓN.

Las comunicaciones satelitales son cruciales en conflictos armados para la vigilancia, el mando y el control, y la logística, ya que proporcionan conectividad en áreas remotas o destruidas. Sin embargo, también son un objetivo estratégico susceptible a ataques, como interferencias electrónicas, ciberataques y destrucción física. La importancia de estas tecnologías ha llevado a inversiones en sistemas de defensa más seguros y resilientes, como comunicaciones encriptadas y defensas contra la guerra electrónica.

a. Funciones clave en conflictos

1) Inteligencia y reconocimiento: Los satélites proporcionan imágenes y datos para identificar objetivos y monitorear el movimiento de las fuerzas enemigas.

2) Mando y control: Permiten la comunicación segura y en tiempo real entre las unidades militares, sin importar su ubicación, lo que es vital para coordinar operaciones.
3) Navegación: Apoyan sistemas de navegación y geolocalización para la precisión de misiles, drones y otros vehículos.
4) Logística: Facilitan la comunicación para la gestión de suministros y la coordinación de operaciones logísticas. Respuesta a desastres: Son fundamentales para la comunicación en zonas de desastre o conflicto donde la infraestructura terrestre ha sido dañada.

b. Vulnerabilidades y amenazas
1) Guerra electrónica: Los satélites y sus estaciones terrestres pueden ser blancos de interferencias (Jamming) para bloquear o distorsionar las comunicaciones.
2) Ciberataques: Los sistemas satelitales son vulnerables a ciberataques que pueden interrumpir o alterar las señales, como ocurrió en un ciberataque en Europa en 2022.
3) Intercepción de datos: Las señales no encriptadas son susceptibles de ser interceptadas, lo que expone información clasificada, como se demostró en investigaciones recientes.
4) Ataques físicos: Los satélites de comunicaciones son objetivos militares potenciales. Su destrucción podría paralizar servicios críticos y afectar operaciones militares.

c. Contramedidas y desarrollo:
1) Sistemas encriptados: Se utilizan sistemas de comunicación encriptados para proteger los datos transmitidos.
2) Resiliencia: Se están desarrollando tecnologías para hacer los satélites más resistentes, como la capacidad de desplegar satélites de reemplazo rápidamente.
3) Maniobrabilidad: Algunos satélites pueden mover sus órbitas para evadir amenazas, aunque esto reduce su vida útil.

4) Neutralización de interferencias: Se desarrollan técnicas para detectar y localizar inhibidores (Jammers) y para mantener la funcionalidad de los sistemas bajo interferencia.
5) Sistemas autónomos: La investigación se dirige hacia armas con mayor autonomía que no dependen de una conexión satelital constante.

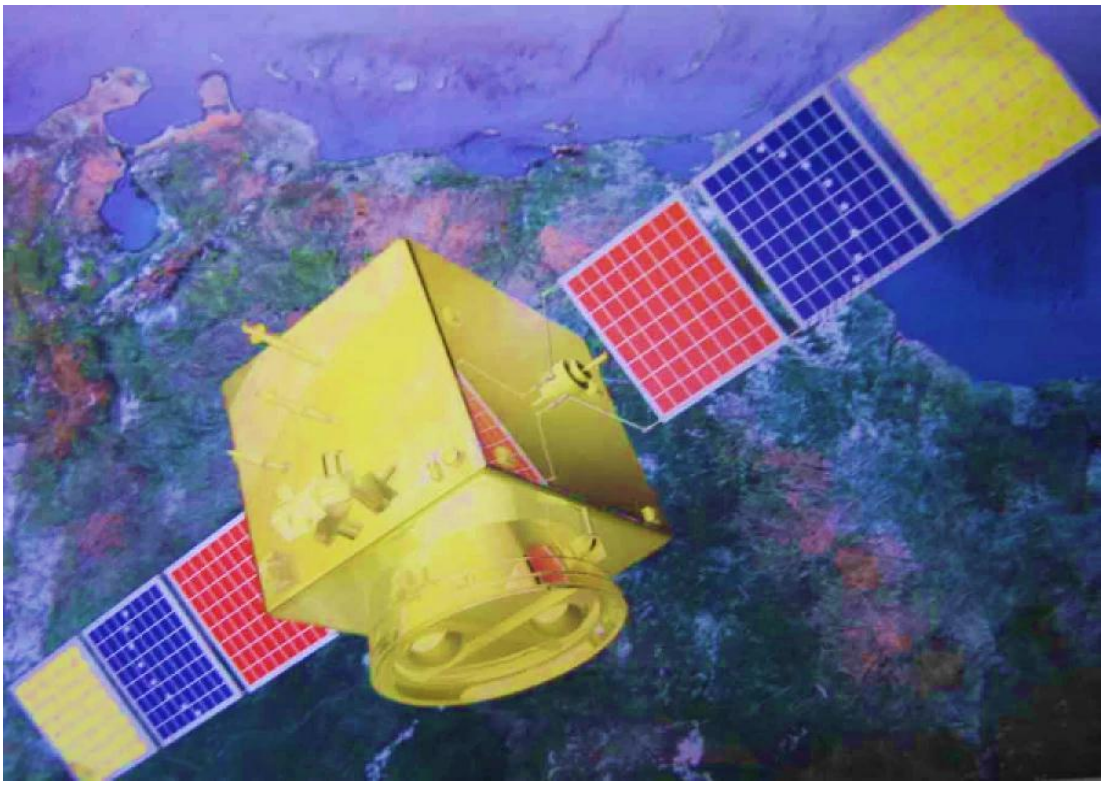


Figura N° 1. Empleo de los satélites para las operaciones Militares

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO V

ANTENAS DE CAMPAÑA

SECCIÓN A

LA IMPROVISACIÓN ES EL TRABAJO DE CAMPO

ANTENAS
(EXPEDIENTES DE CAMAPAÑA)

QUE ES UNA ANTENA?
Una Antena puede definirse como un conductor o sistema de conductores (alambres, cables, aluminio, cobre, bronce, etc.) o dispositivos de cualquier clase, destinados a radiar o recibir energía electromagnética.

QUE ES UNA ONDA DE RADIO O LONGITUD DE ONDA?
Es la distancia que atraviesa la onda en cierto período de tiempo (para completar un ciclo o Hertz) en un segundo, se expresa con la letra griega λ.

RELACION ENTRE LONGITUD DE ONDA λ, FRECUENCIA F Y VELOCIDAD DE PROPAGACION V.

Fórmula $\lambda = \frac{V}{F}$ se expresa en metros

- En el espacio libre la velocidad de las ondas electromagnéticas, usa una constante C, constante de propagación 300.000 Km/seg = 3×10^5 m/seg.

LONGITUD DE ONDA (en metros) (Espacio libre)

$La = \frac{300.000.000 \text{ m/seg}}{\text{Frec. Hertz}}$ $la = \frac{300.000}{\text{Frec. Khz}}$ $la = \frac{300}{\text{Frec. Mhz}}$

- La velocidad depende de las características del medio, la longitud de onda no es la misma para los diferentes medios.

LEY
A MAYOR FRECUENCIA MENOR SERA LA LONGITUD DE ONDA.

TIPOS DE ANTENAS

- Vertical.
- Horizontal.

PATRON DE RADIACIÓN

- Omnidireccional.
- Bidireccional.
- Unidireccional

CARACTERÍSTICAS DE LA PROPAGACIÓN Y PATRON DE RADIACIÓN.

- Frecuencia de trabajo
- Tipo de modulación.
- Características del terreno
- Polarización de las Antenas
- Longitud de del Recorrido
- Estado de la atmósfera
- Tipos de Antenas

CALCULOS DE LONGITUD DE ANTENA EN:

Metro	= 300 / F(MHz)	=	285 / F(MHz)
Pie	= 984 / F(MHz)	=	934,8 / F(MHz)
Pulgada	= 11.812 / F(MHz)	=	11.221,4 / F(MHz)

ANTENAS DE ½ ONDA

Metro	= 150 / F(MHz)	=	142,5 / F(MHz)
Pie	= 492 / F(MHz)	=	467,4 / F(MHz)
Pulgada	= 5.906 / F(MHz)	=	5.610,7 / F(MHz)

ANTENAS DE ¼ ONDA

Metro	= 75 / F(MHz)	=	71,25 / F(MHz)
Pie	= 246 / F(MHz)	=	233,7 / F(MHz)
Pulgada	= 2.953 / F(MHz)	=	2.805,35 / F(MHz)

FACTOR "K" PARA LONGITUDES DE ANTENAS

Factor "K" o constante de corrección.

0,96 = Frecuencias inferiores a 3 MHz.
0,95 = Frecuencias de 3 a 30 MHz
0,94 = Frecuencias superiores a 30 MHz

CONVERSIONES:

1 MTS = 39,37 Pulgada = 3,28 Pies

CARTA DE REFERENCIA RAPIDA, LONGITUD DE ANTENAS HF- VHF- UHF EN MTS

(FRECUENCIAS MILITARES)

LONGITUD DE ANTENA HF/AM				LONGITUD DE ANTENA VHF/FM				LONGITUD DE ANTENA VHF/AM (AVIACION)				LONGITUD DE ANTENA UHF/AM				MULTICANAL UHF-TRC/1645			
FREQ. (MHz)	1/4 ONDA	1/2 ONDA	1 ONDA	FREQ. (MHz)	1/4 ONDA	1/2 ONDA	1 ONDA	FREQ. (MHz)	1/4 ONDA	1/2 ONDA	1 ONDA	FREQ. (MHz)	1/4 ONDA	1/2 ONDA	1 ONDA	FREQ. (MHz)	1/4 ONDA	1/2 ONDA	1 ONDA
2	35,6	71,2	142,5	30	2,3	4,7	9,5	100	0,712	1,425	2,85	225	0,31	0,63	1,26	610	0,11	0,23	0,46
3	23,7	47,5	95	33	2,1	4,3	8,6	105	0,678	1,357	2,714	230	0,30	0,61	1,28	620	0,11	0,22	0,45
4	17,8	35,6	75,25	35	2,0	4,0	8,1	110	0,647	1,295	2,590	235	0,30	0,60	1,21	630	0,11	0,22	0,45
5	14,2	28,5	57	37	1,9	3,8	7,7	115	0,619	1,239	2,478	240	0,29	0,59	1,18	640	0,11	0,22	0,44
6	11,8	23,7	47,5	40	1,7	3,5	7,1	120	0,593	1,187	2,375	245	0,29	0,58	1,16	650	0,10	0,21	0,43
7	10,1	20,3	40,7	43	1,6	3,3	6,6	125	0,57	1,14	2,28	250	0,28	0,57	1,14	670	0,10	0,21	0,42
8	8,9	17,8	35,6	45	1,5	3,1	6,3	128	0,55	1,11	2,22	255	0,27	0,55	1,11	700	0,10	0,20	0,40
9	7,9	15,8	31,6	48	1,4	2,9	5,9	130	0,54	1,09	2,19	260	0,27	0,54	1,09	720	0,90	0,19	0,39
10	7,1	14,2	28,5	50	1,4	2,8	5,7	133	0,53	1,07	2,14	265	0,26	0,53	1,07	740	0,90	0,19	0,38
11	6,4	12,9	25,9	55	1,2	2,5	5,1	135	0,52	1,05	2,11	270	0,26	0,52	1,05	760	0,90	0,18	0,37
12	5,9	11,8	23,7	57	0,2	2,5	5,0	138	0,51	1,0	2,06	275	0,25	0,51	1,03	780	0,90	0,18	0,36
13	5,4	10,9	21,9	60	1,1	2,3	4,7	140	0,50	1,01	2,03	280	0,25	0,50	1,01	800	0,08	0,17	0,35
14	5,0	10,1	20,3	65	1,0	2,1	4,3	143	0,498	0,996	1,993	285	0,25	0,50	1,00	820	0,08	0,17	0,34
15	4,7	9,5	19,0	68	1,0	2,0	4,1	145	0,491	0,98	1,96	290	0,24	0,49	0,98	840	0,08	0,16	0,33
16	4,4	8,9	17,8	70	1,0	2,0	4,0	148	0,481	0,96	1,92	300	0,23	0,47	0,95	860	0,08	0,16	0,33
17	4,1	8,3	16,7	75	0,9	1,9	3,8	150	0,475	0,95	1,90	320	0,22	0,44	0,89	880	0,08	0,16	0,32
18	3,9	7,9	15,8	80	0,8	1,7	3,5	153	0,46	0,93	1,86	340	0,20	0,41	0,83	900	0,07	0,15	0,31
19	3,7	7,5	15,0	85	0,8	1,6	3,3	155	0,459	0,91	1,83	360	0,19	0,39	0,79	920	0,07	0,15	0,30
20	3,5	7,1	14,2	90	0,7	1,5	3,1	157	0,453	0,90	1,81	380	0,18	0,37	0,75	940	0,07	0,15	0,30
21	3,3	6,7	13,5					160	0,44	0,89	1,78	400	0,17	0,35	0,71	960	0,07	0,14	0,20
22	3,2	6,4	12,9																
23	3,0	6,1	12,3																
24	2,9	5,9	11,8																
25	2,8	5,7	11,4																
26	2,7	5,4	10,9																
27	2,6	5,2	10,5																
28	2,5	5,0	10,1																
29	2,4	4,9	9,8																

CALCULOS DE ANTENAS

1.- $\frac{\lambda}{2}$ = La: $\frac{\text{C Kms/seg x 0,95}}{\text{F(MHz)}} = \frac{285}{\text{F(MHz)}} \div 2 = \frac{142,5}{\text{F(MHz)}}$ = mts

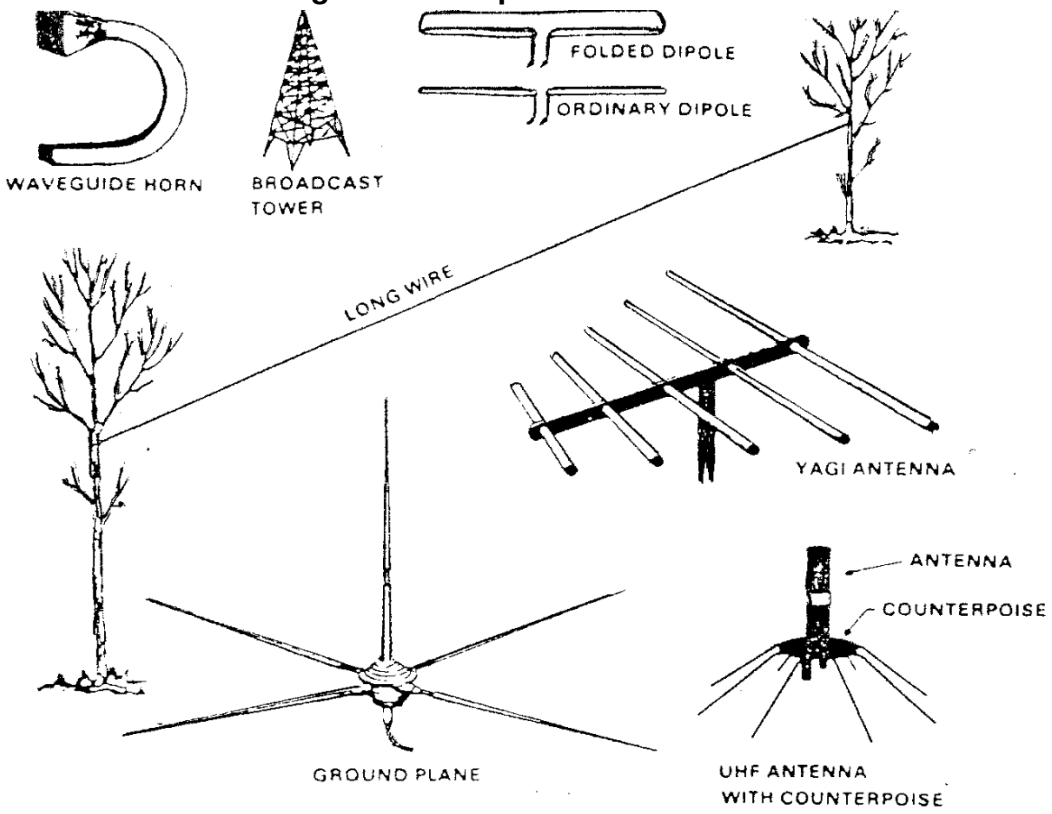
2.- $\frac{\lambda}{4}$ = La: $\frac{\text{C Kms/seg x 0,95}}{\text{F(MHz)}} = \frac{285}{\text{F(MHz)}} \div 2 = \frac{142,5}{\text{F(MHz)}} \div 2 = \frac{71,25}{\text{F(MHz)}}$ = mts

Oscar Rafael Alvarez Nieves
M.T.S. (Ej.)

Figura N° 2 Carta de Referencia

CELDAR

Figura N° 3. Tipos de Antena



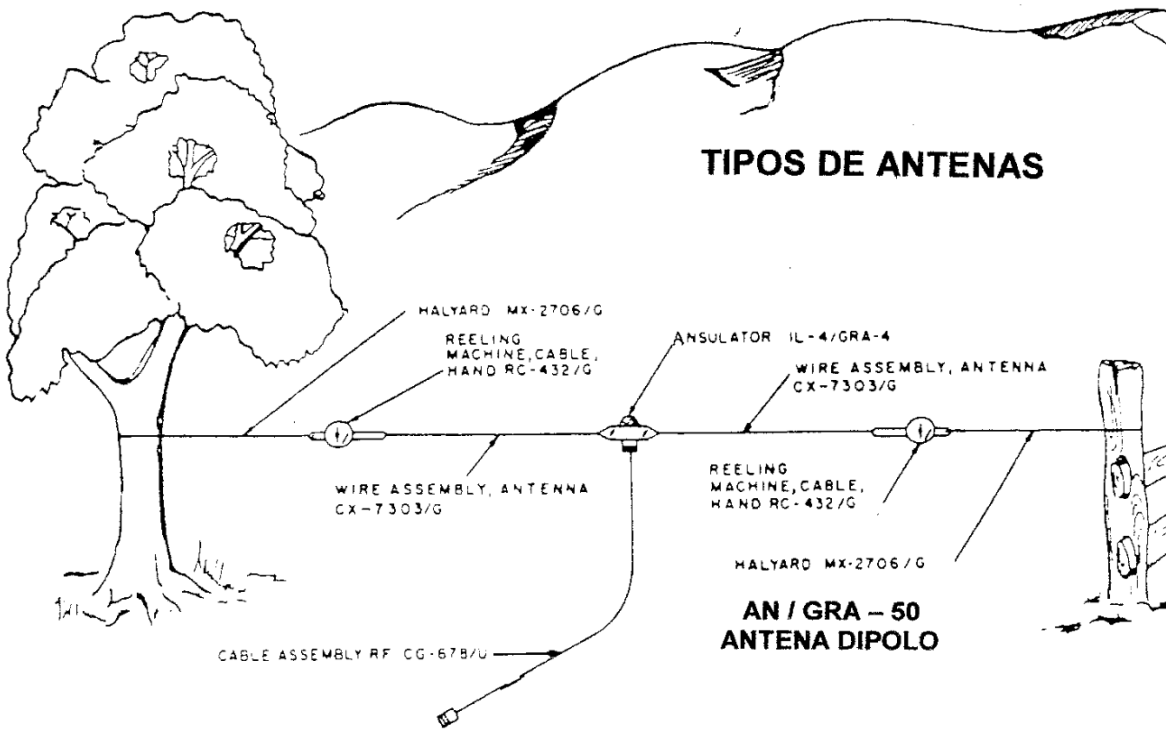
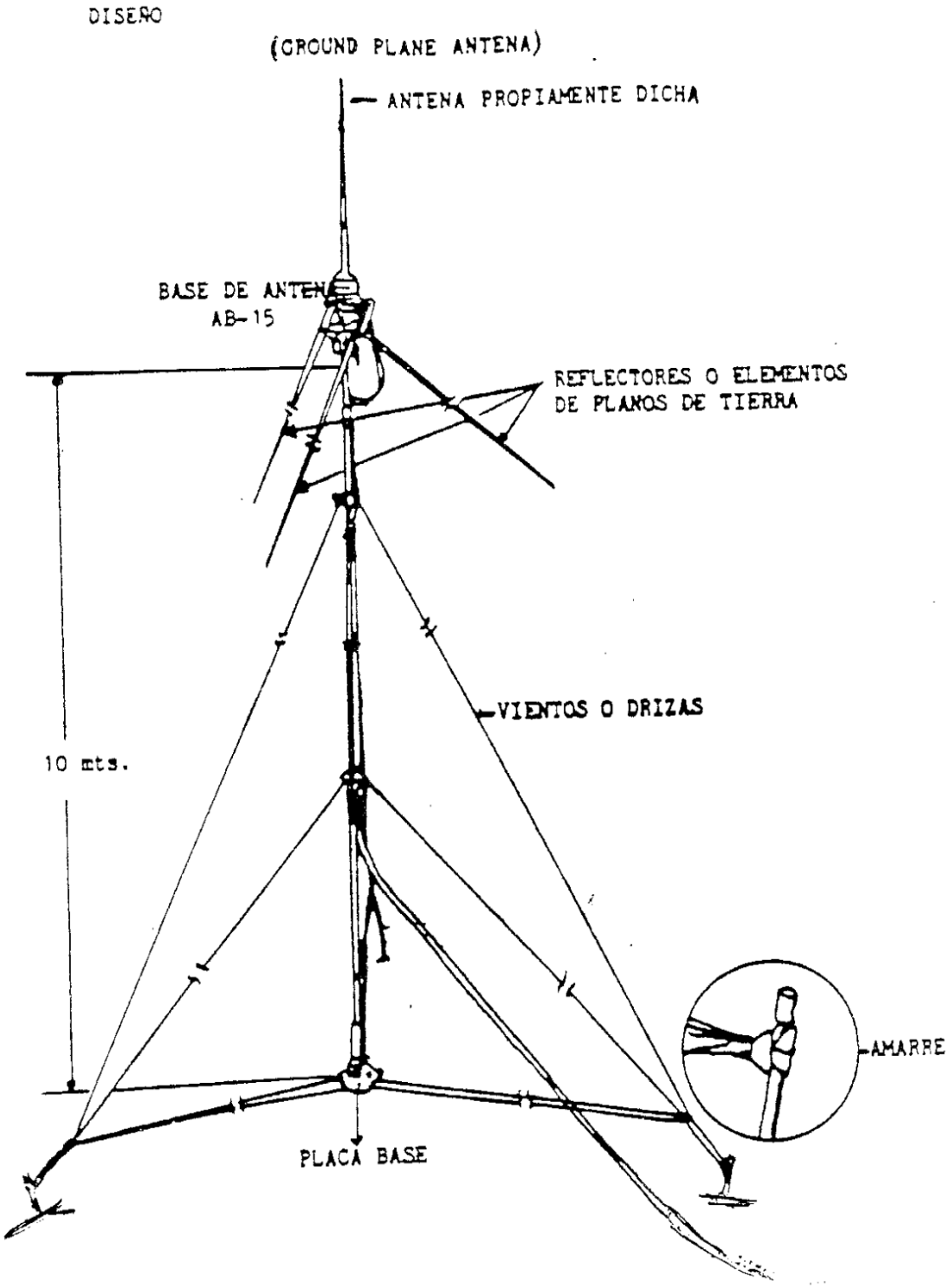
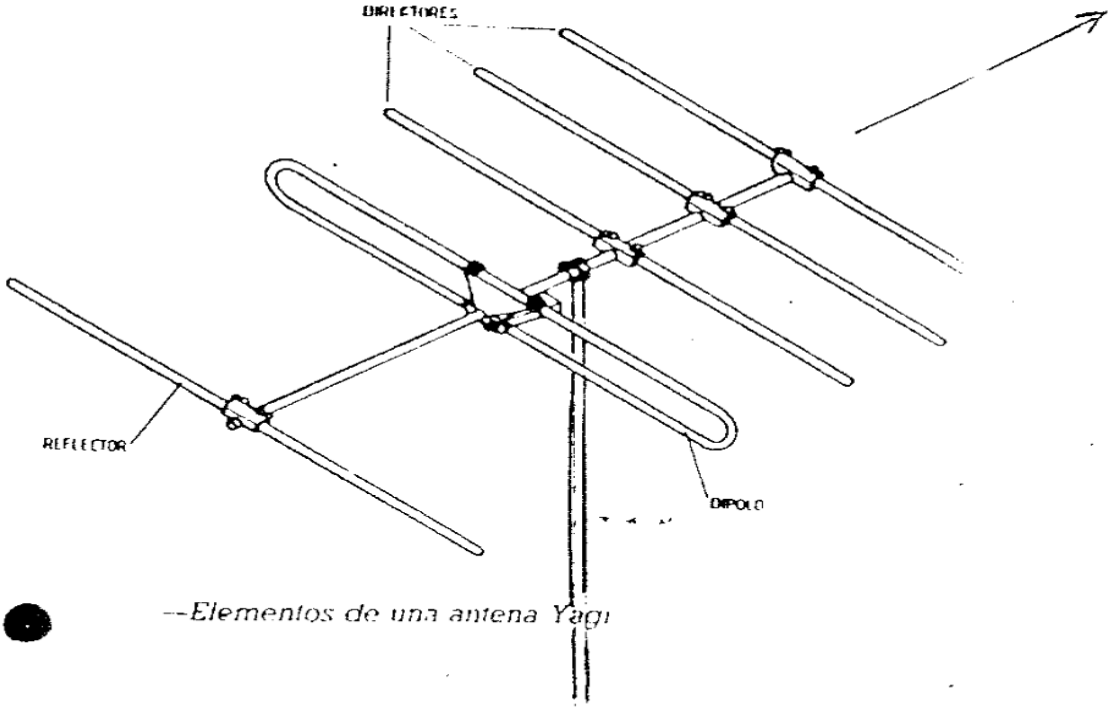


Figura N° 4. Antena RC-292



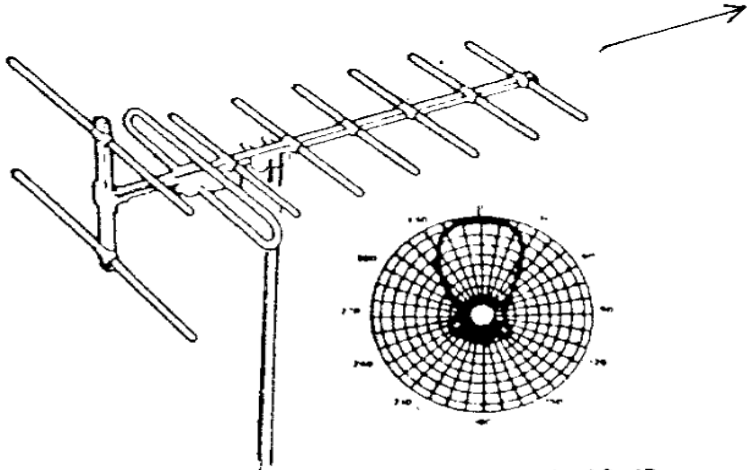
ANTENA RC – 292
(GROUND-PLANE)

Figura N° 5. Antena Tipo Yagi



--Elementos de una antena Yagi

TIPOS DE YAGI



—Antena bicanal para la banda III, ganancia 10 dB

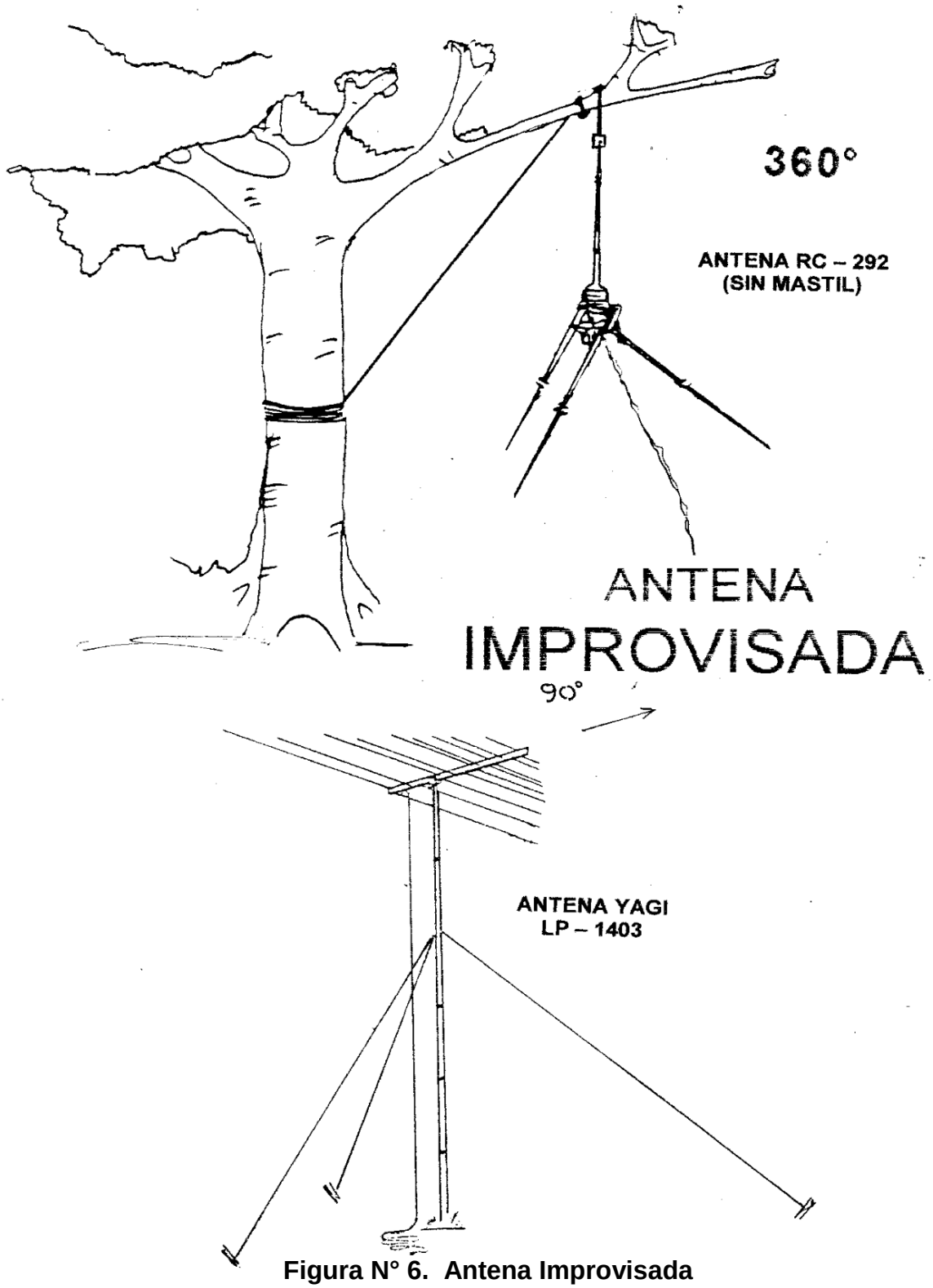
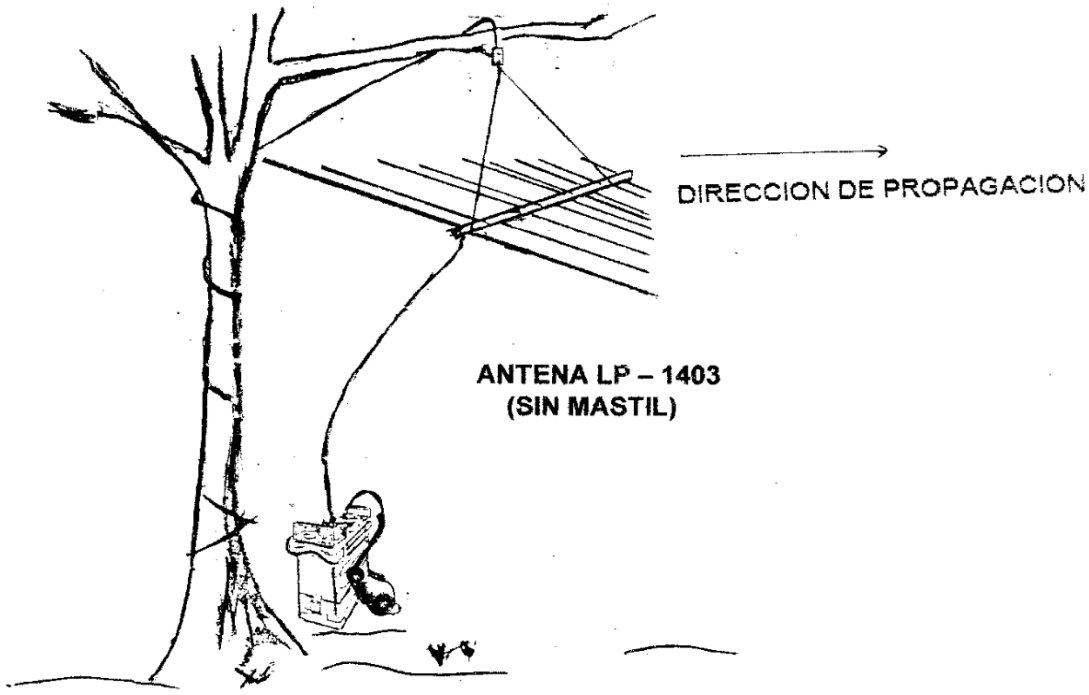


Figura N° 6. Antena Improvisada

Figura N° 7. Antena Horizontal



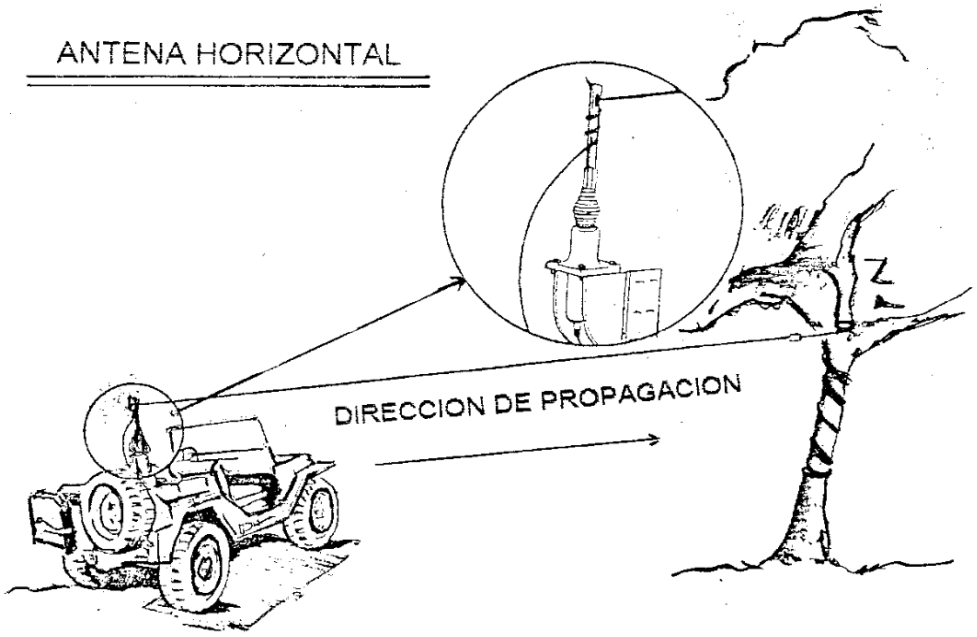
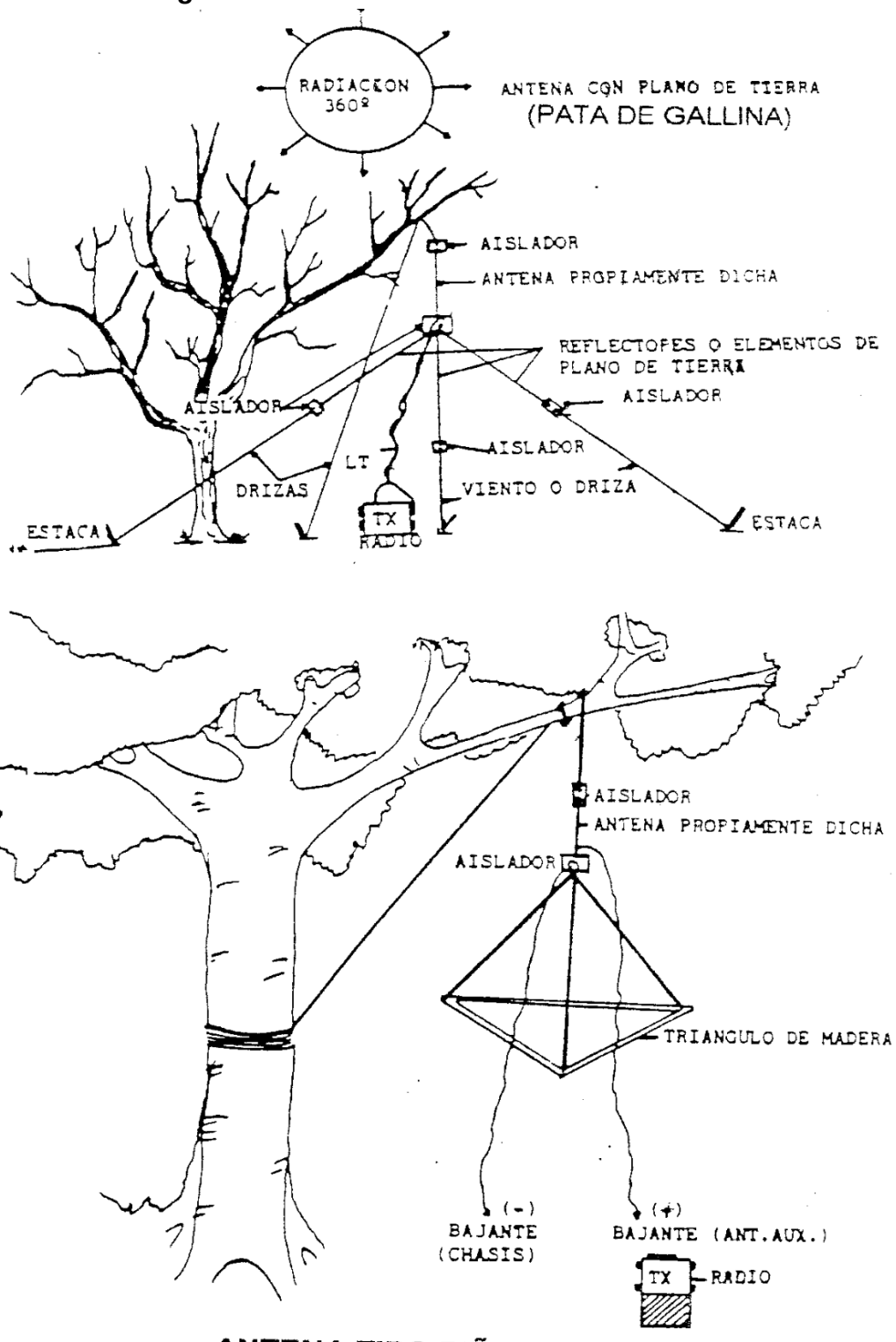


Figura N° 8. Antena Pata de Gallina



ANTENA TIPO PIÑATA

Figura N° 9. Antena Globo

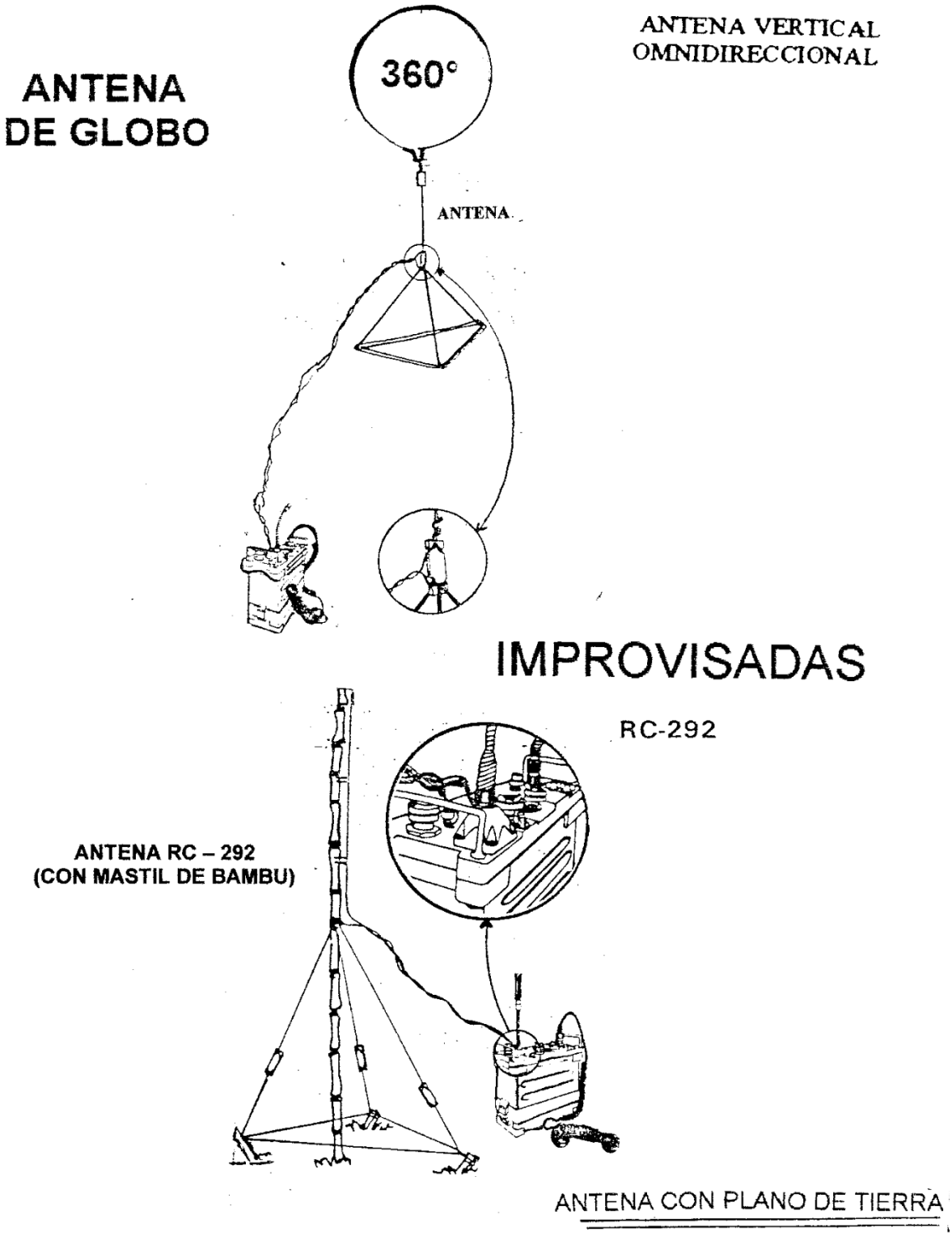
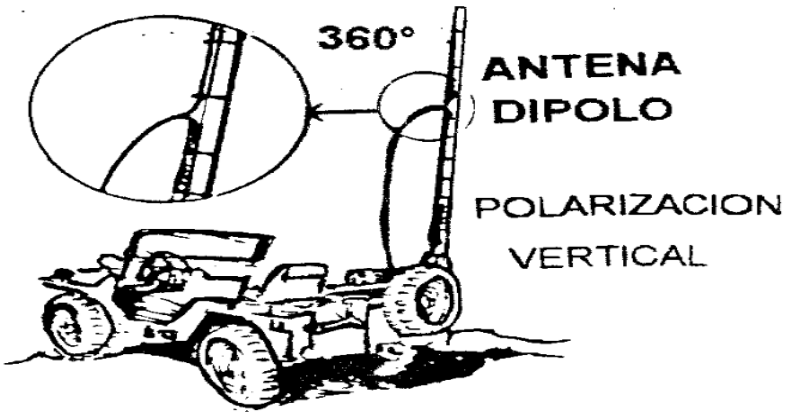
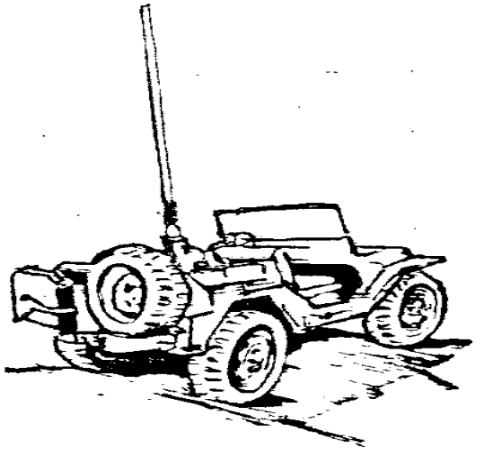
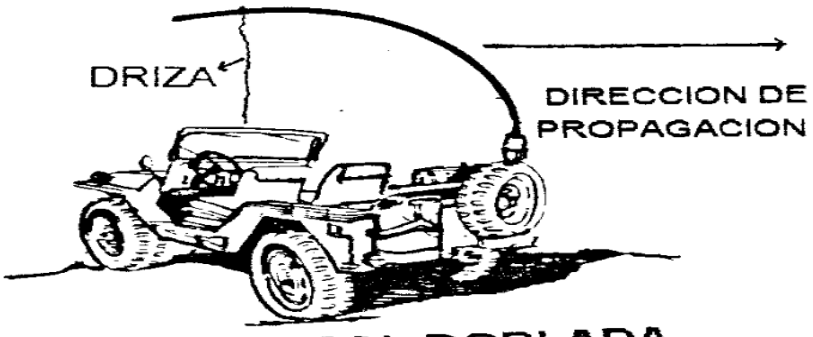


Figura N° 10. Antena Dipolo





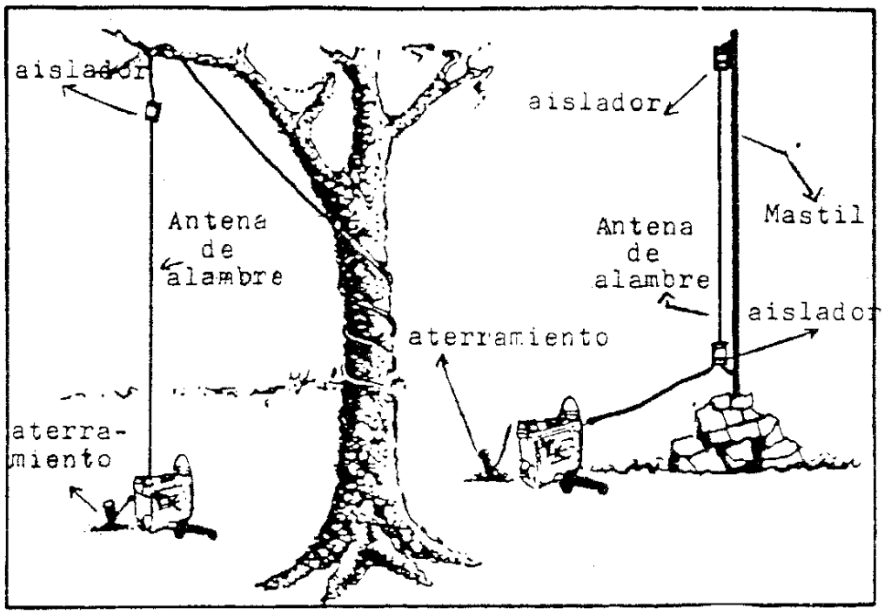
ANTENA VERTICAL
(VEHICULAR)



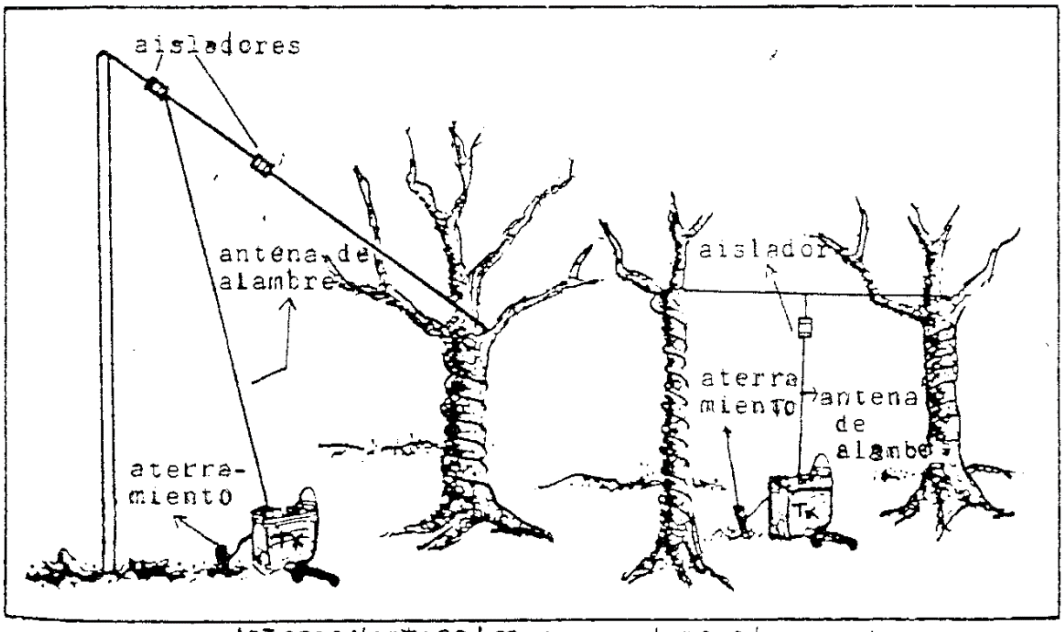
ANTENA VERTICAL DOBLADA

Figura N° 11. Antena Verticales

ANTENAS VERTICALES

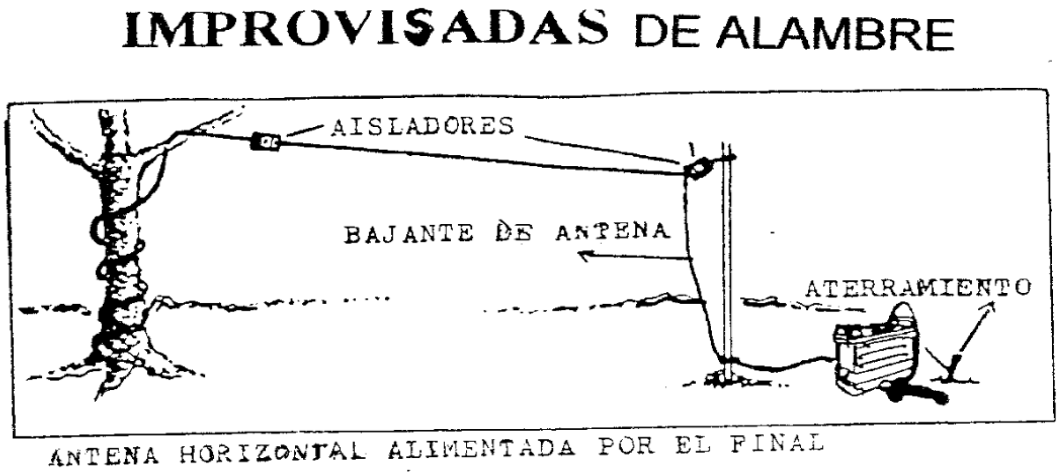


Antena vertical de alambre(soportadas por mastil)



Antenas Verticales por medios adicionales

Figura N° 12. Improvisada de Alambre



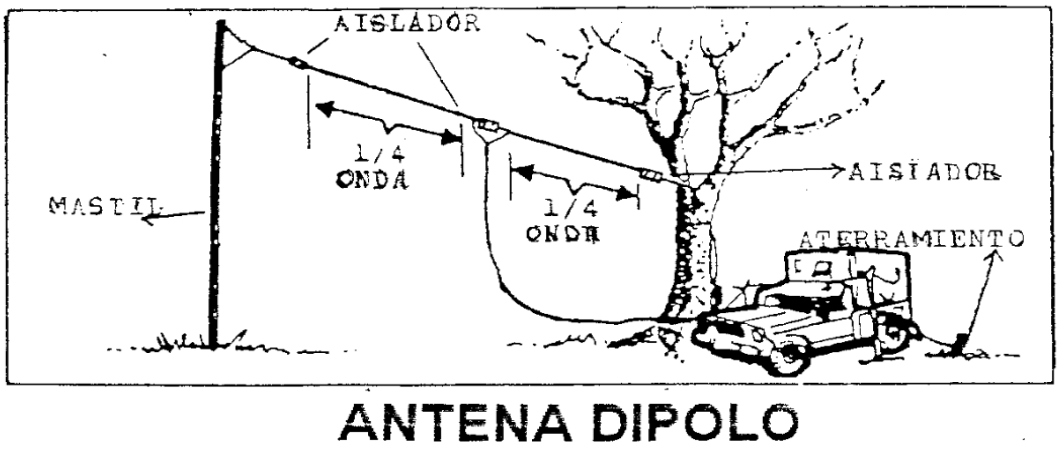
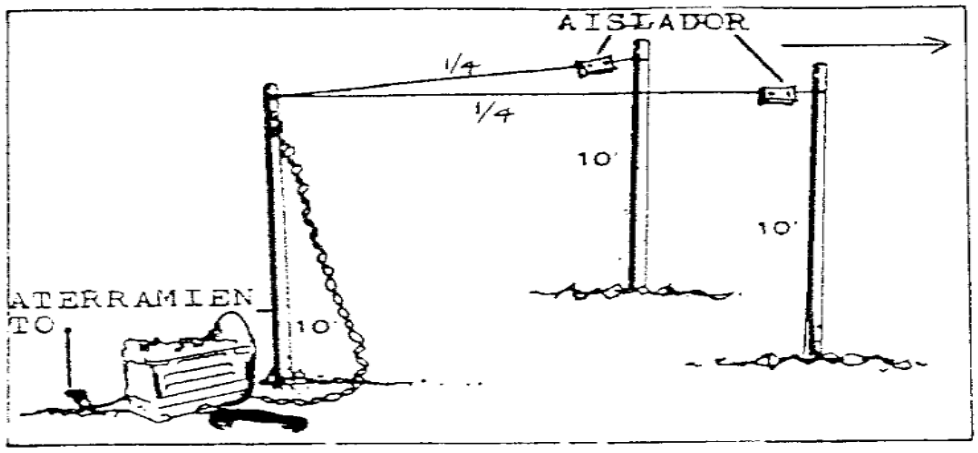
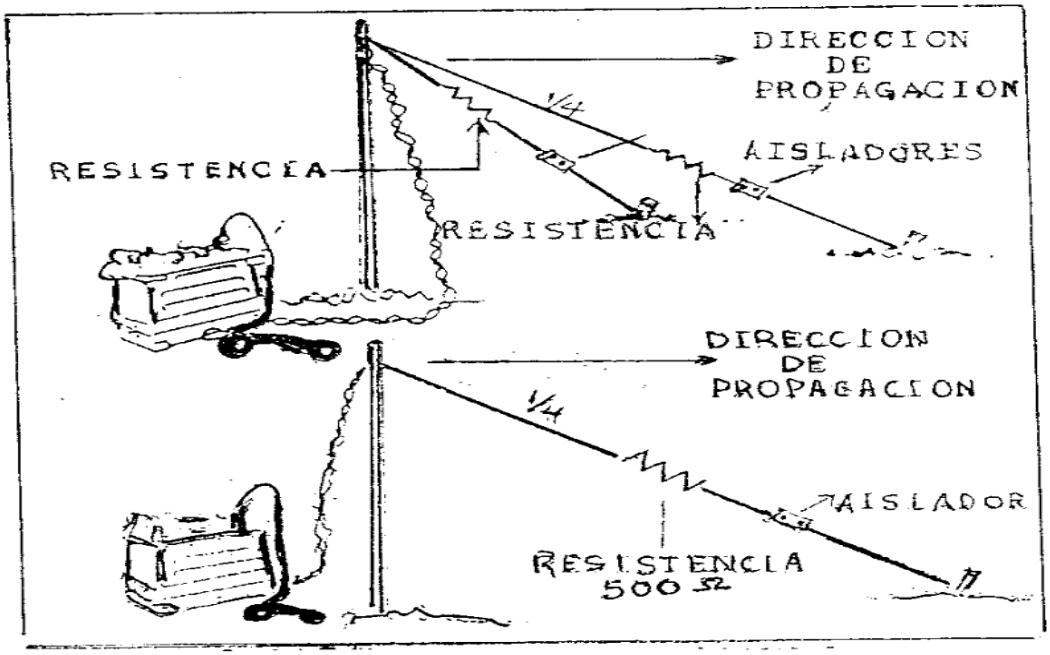


Figura N° 13. Antena Tipo "V"

ANTENAS TIPO "V"



ANTENA TIPO "V"



TIPO "V" INCLINADA

Figura N° 14. Antena Patrulla

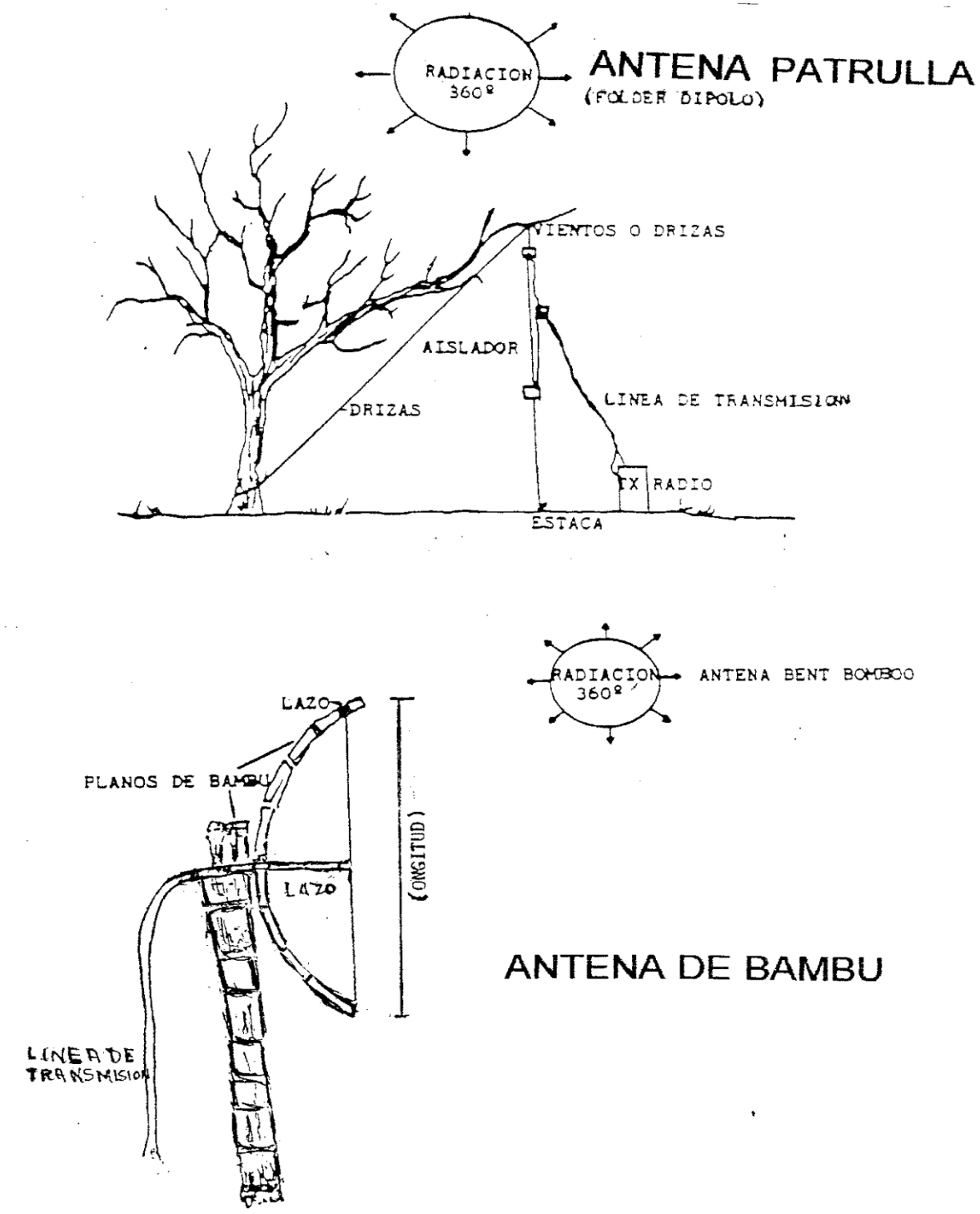


Figura N° 15. Antena de 1/2 Onda Rómbica

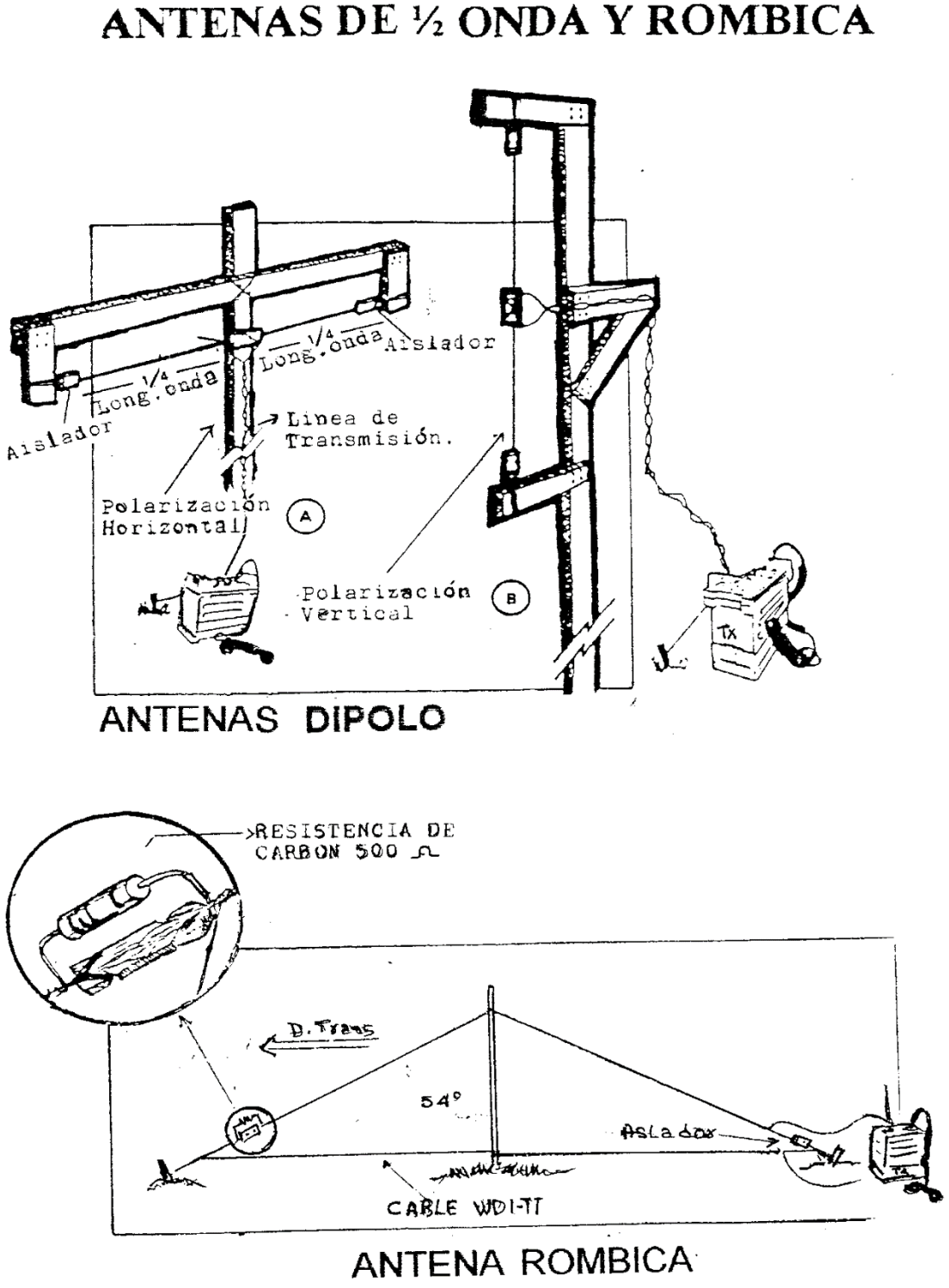
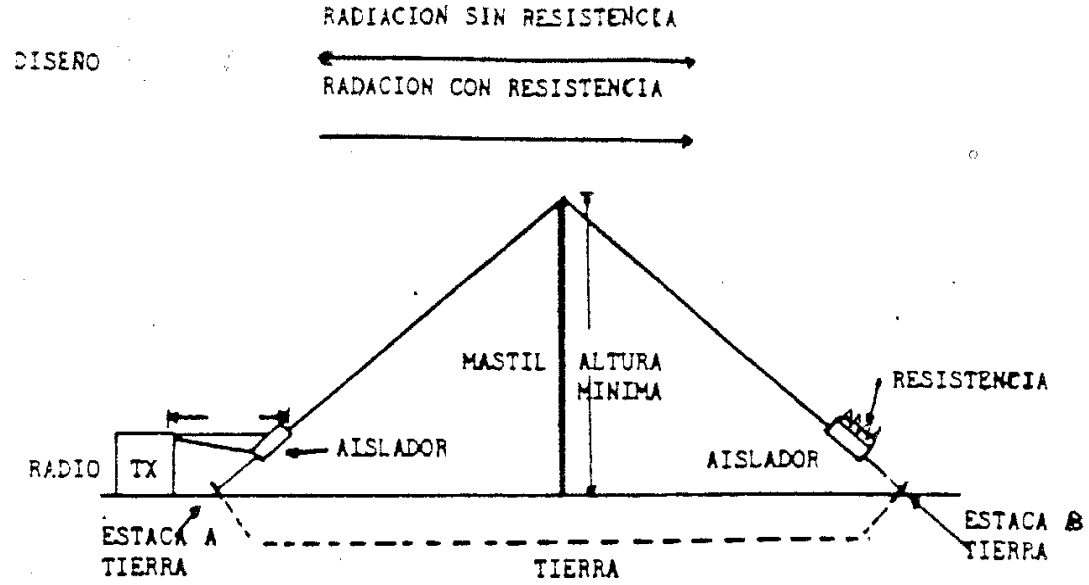
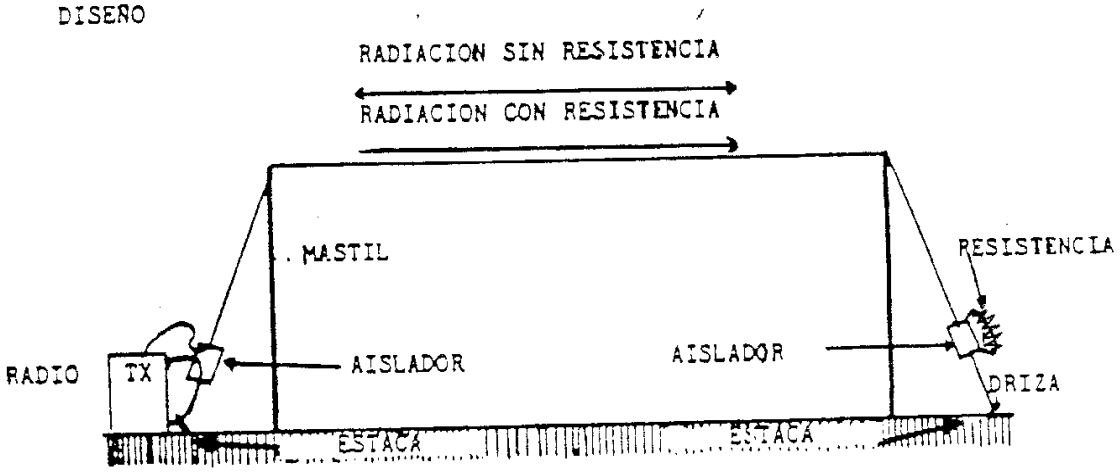


Figura N° 16. Antena Media Rómbica



ANTENA MEDIA ROMBICA



ANTENA HORIZONTAL

Figura N° 17. Antena Subterránea

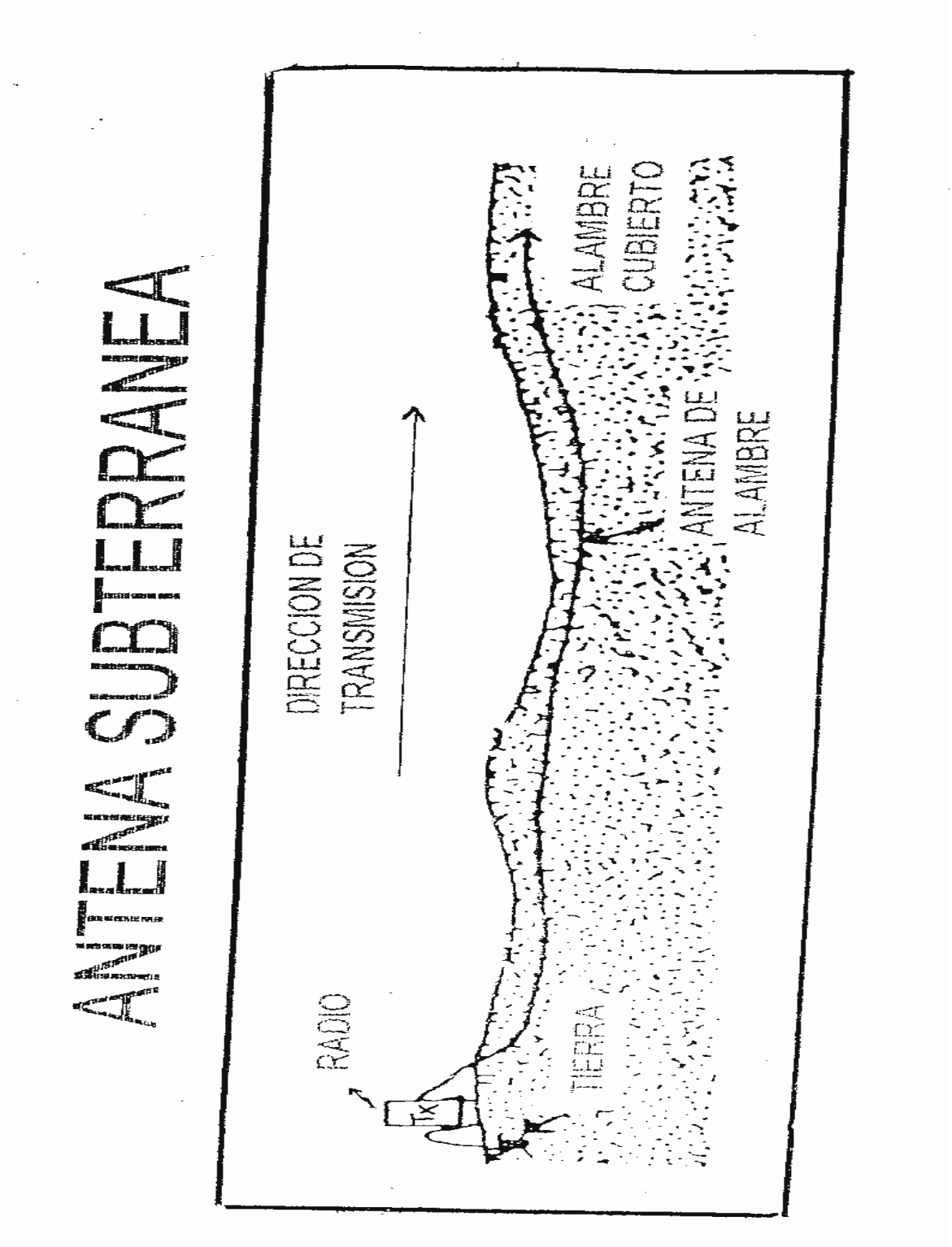
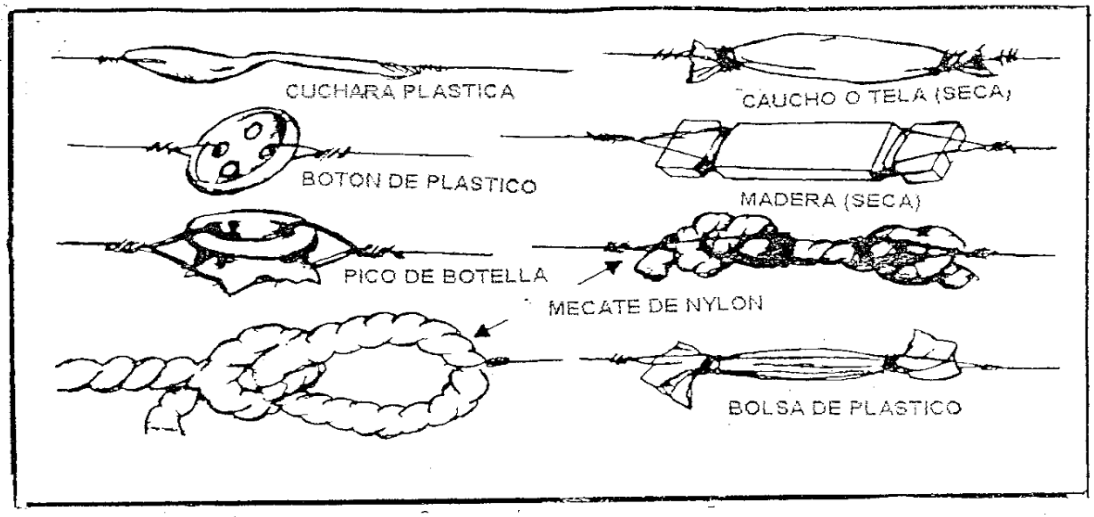


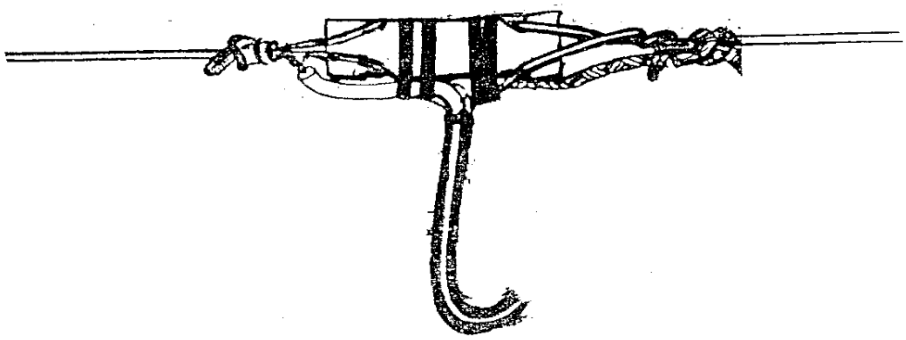
Figura N° 18. Aisladores Improvisados

AISLADORES IMPROVISADOS



METALES CONDUCTORES

- ORO
- PLATA
- ALUMINIO
- COBRE
- BRONCE
- HIERRO



AMARRADURAS DE UNA
ANTENA DIPOLO IMPROVISADA

Oscar Rafael Alvar
M.T.S. (Ej.)

SECCIÓN B

MICROTELÉFONOS

1. MANTENIMIENTO.

Para el mantenimiento de este equipo se requiere de un multímetro con el fin de facilitar la reparación en cualquier terreno.

2. PROCEDIMIENTO.

a. Prueba capsulas.

Con el multímetro verifique las cápsulas colocando las dos puntas de prueba en sus pines, si pita están buenas condiciones, al pitar hace referencia al termino de continuidad, que significa que hay enlace físico entre un punto y otro en algunos multímetros para hacer esta prueba es necesario colocar la perilla en la posición que tiene un símbolo similar a de lo contrario no está en buen estado.

Figura N° 23. Microteléfono

b. Prueba cable resortado.
   1) Verifique la continuidad de cada uno de los hilos del cable resortado colocando una punta a cada extremo estirando el cable con la ayuda de otra persona para garantizar su estado interno. Si pita esta bueno, de lo contrario no.
   2) Verifique que los filamentos de cada hilo estén haciendo buen contacto con las terminales porque en ocasiones no lo hacen, desarme y vuelva a colocar las terminales si es necesario.
   3) Vuelva a medir continuidad antes de instalar el cable.
   4) Si presenta cortadas cerca de la toma de audio o la carcasa corte totalmente y ármelo de nuevo, no coloque cinta, esto es una solución pasajera.

c. Conexión de la toma de audio.
   1) Los hilos deben quedar de un centímetro (1 cm.) de largo con el fin de evitar que quede flojo el cable a la toma de audio.
   2) El hilo negro va unido con la maya.
   3) Cada Terminal debe hacer un buen contacto con los filamentos.
   4) Evite que la Terminal quede floja dentro de la cavidad del conector, entre más asegurado quede, mejor.
   5) El orden de los cables dentro del conector es:

      A = TIERRA + MAYA

      B = BLANCO

      C = VERDE

      D = ROJO

      E = NO CONECTADO

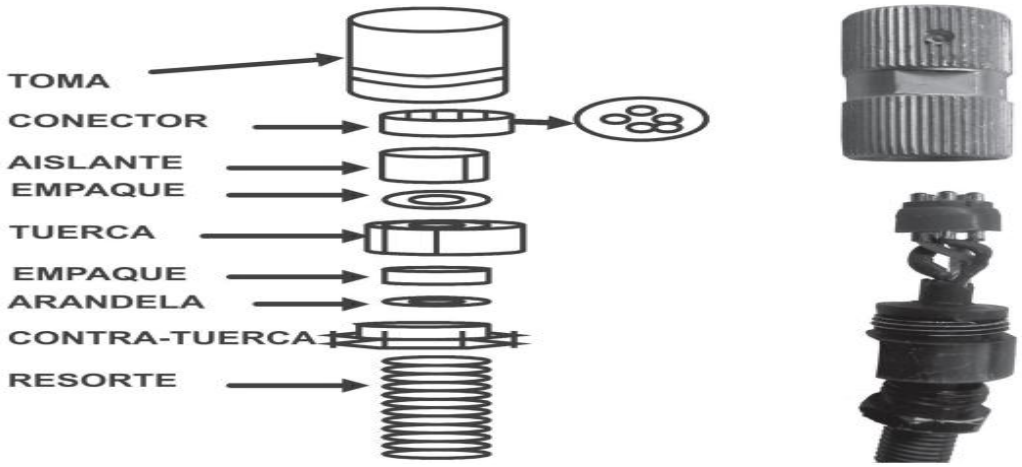


Figura N° 19. Conexión de la toma de audio

5) Coloque todas y cada una de las partes de la toma U-229/U en el orden que se indica en la figura anterior. Evite que el cable gire cuando este asegurando las tuercas, utilice pinzas.

6) Si es necesario retire el cable reportado de la carcasa con el fin de cortar las partes averiadas, luego coloque los terminales en cada hilo y la abrazadera que es la encargada de sujetar el cable a la carcasa. Los hilos deben ser de 5cm de largo aprox., para la conexión al PTT.

7) Si el cable está muy averiado cambie por otro nuevo.

3. MANTENIMIENTO DE LA CARCASA

Verificar que los contactos no estén oxidados, si es así se debe cambiar el contenido por un pedazo de maya del mismo cable resortado con el fin de garantizar el contacto de los pines de las cápsulas; no es recomendable usar esponjilla ya que esta se oxida rápidamente. La única causa de dar de baja una carcasa es que se encuentre partida.

4. PRUEBA PTT

PASO 1:

Teniendo el PTT desconectado y con el multímetro se mide así:

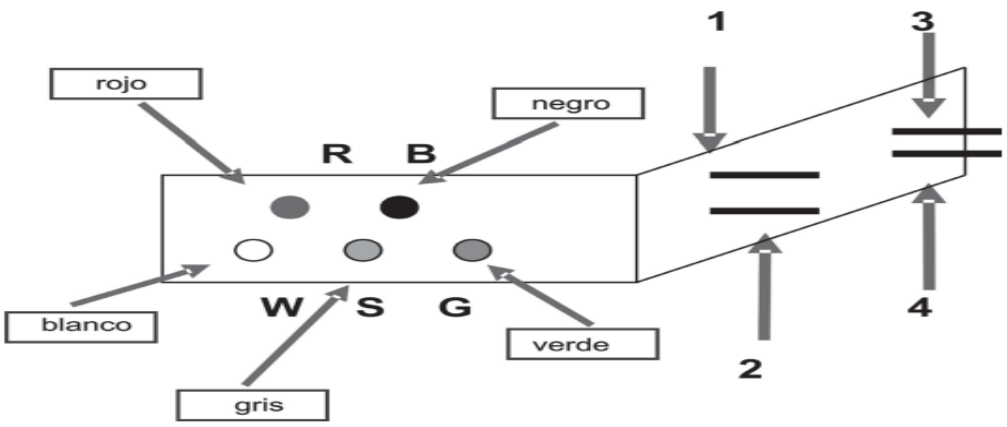


Figura N° 20. Prueba PTT

Colocamos un cable del multímetro en el pin R y el otro cable en el Pin 1 cuando obturamos debe sonar un pito, cuando soltamos no debe sonar de lo contrario esta averiado 65.

PASO 2:

Colocamos un cable del multímetro en el pin G y el otro cable en el Pin 4 cuando obturamos debe sonar un pito, cuando soltamos no debe sonar, de lo contrario esta malo.

5. CONEXIÓN DEL PTT

En la figura 6.9 los colores de los puntos son los mismos colores de los hilos y van conectados en ese orden e identificados por las siguientes letras:

R = CABLE ROJO

B = CABLE NEGRO

W = CABLE BLANCO

S = MAYA

G = CABLE VERDE

Es necesario colocar una cinta o el plástico aislante en la base del PTT con el fin de evitar un corto entre las terminales 1 a 4. Así mismo aislar la malla. Luego coloque el caucho protector, la lámina y asegure los tornillos.

6. INSTALACIÓN DE LAS CÁPSULAS

Cada cápsula se debe instalar con su respectivo empaque y protector, si no tiene el empaque puede reemplazarlo por un caucho muy similar con el fin de asegurarla bien y evitar un mal funcionamiento.

AN-PRC 660 UV.

El AN/PRC-660 UV es un transceptor portátil de radio de banda dual que opera en las frecuencias UHF y VHF, a diferencia del modelo original AN/PRC-660 que solo operaba en UHF. Fue desarrollado por Tadirán en 1984 como sucesor del AN/PRC-660 para incluir el uso en la banda VHF del aire. Este modelo más moderno permite la comunicación tanto en el aire (aire-tierra) como en tierra (tierra-tierra), y también puede operar como baliza o en modo de relevo.

7. CARACTERÍSTICAS PRINCIPALES:

- **Banda de frecuencia:** Opera en los rangos de 116-156 MHz y 225-400 MHz (VHF y UHF).
- **Funcionalidad:** Puede usarse para comunicaciones de voz en tierra-aire y tierra-tierra, y como baliza o para retransmisión.
- **Sucesión:** Es el sucesor del modelo original AN/PRC-660, que solo utilizaba la banda UHF.
- **Fabricante:** Fue desarrollado por Tadirán en Tel Aviv.

- **Diseño:** Comparte una carcasa y arnés similares a los del AN/PRC-25 y AN/PRC-77, lo que facilita su integración.

Figura N° 21. AN-PRC 660 UV

Transceptor RT-6241TG: Esta es la unidad de radio principal que se usa de forma portátil.

Arnés (ST-138): Un arnés de transporte que permite al operador llevar la radio en la espalda, similar al del PRC-25 o PRC-77.

Batería: El sistema funciona con una batería recargable, como la SK 660 Li (de 28 V y 7 Ah), y se puede cargar a través de una fuente de alimentación de 22 a 38 V CC.

8. ANTENAS:

   Antena de látigo (AT-6600 T): Utilizada para las comunicaciones tácticas de corto a medio alcance.

   Antena AT-803/VRC: Parte de las configuraciones vehiculares (VRC-240T), pero también puede ser utilizada por la versión portátil.

9. AUDIO:

   a. Auricular (H-189/GR): El dispositivo de audio estándar para la comunicación de voz.
   b. Micrófono (M-80/GR): Un micrófono de mano que se puede usar en lugar del auricular.

c. Auriculares con micrófono (H-161A/U): Un juego de auriculares que se incluye en el equipo para operaciones manos libres.

Figura N° 22. Accesorios

10. FALLAS MAS COMUNES EN EL AN/PRC-660T:

    Posibles causas:

    a. Control de encendido en posición incorrecta.
    b. Control de volumen en mínimo.
    c. Receptáculo del micro teléfono H-189 malo.
    d. Batería deficiente.
    e. No hay ruido de fondo.

11. ACCIÓN A TOMAR:

    a. Control de encendido en "ON".
    b. Control de volumen a mediana escala.
    c. Reemplazar el H-189.
    d. Cambiar de receptáculo al H-l 89.
    e. Reemplazar la batería.

12. NO HAY RECEPCIÓN:

    Posibles causas:

    a. H-189 malo.
    b. Batería deficiente.
    c. Antena conectada incorrectamente.
    d. Receptáculo del H-189 malo.

13. ACCIÓN A TOMAR:

    a. Reemplazar H-189.
    b. Reemplazar batería.
    c. Verificar la posición correcta de la antena.
    d. Cambiar de receptáculo el H-189.

14. NO HAY TRANSMISIÓN:

    Posibles causas:

    a. Batería deficiente.
    b. Amena conectada incorrectamente.
    c. H-189 malo.
    d. Receptáculo del H-189 malo.
    e. Swich en posición incorrecta.

15. ACCIÓN A TOMAR:

    a. Reemplazar batería.
    b. Verificar posición correcta de la antena.
    c. Reemplazar H-189.
    d. Cambiar de receptáculo el H-189.
    e. Coloca» el control en la posición adecuada.

16. MANTENIMIENTO PREVENTIVO:

    Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de

comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.
b. Instalar el equipo en un lugar apropiado para su adecuada operación.
c. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.
d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc., con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.
e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.
f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.
g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:
   1) Cables de tensión conectados incorrectamente (Inversión de polaridad).
   2) Clavijas gastadas, rotas o desconectadas.
   3) Conectores de los cables de las antenas sueltos.
   Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los micro teléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.
b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.
c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.
d. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: Agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.
f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

RADIO VEHICULAR VRC-240 UV

El VRC-240 UV es un conjunto de radio militar móvil de banda aérea superior que se utiliza para comunicaciones de tierra a aire y de tierra a tierra. Puede funcionar como una estación baliza o de retransmisión.

Figura N° 23. Radio Vehicular VRC-240 UV

17. COMPONENTES PRINCIPÁLES:
    a. Radio mochila AN/PRC-660T: El transmisor-receptor principal.
    b. Amplificador/Fuente de alimentación AM-2411TG: Proporciona energía y amplifica la salida de la radio mochila hasta 16 vatios.
    c. Soporte MT-1029: Conecta el equipo a una fuente de alimentación móvil.
18. CARACTERÍSTICAS:
    a. Rango de frecuencia: 225 a 399,950 MHz, con 3500 canales.
    b. Modo: Amplitud modulada (AM).
    c. Operación remota: Se puede controlar hasta a 15 metros de distancia con el control C 2410 T
    d. Transceptor (RT-6241TG): La unidad principal de radio que opera en las bandas de HF y VHF. Para la versión móvil, esta unidad portátil se integra en el resto del sistema.
    e. Amplificador/fuente de alimentación (AM-2411TG): Este componente amplifica la señal de la radio a una potencia de 16 W. También actúa como una fuente de alimentación, convirtiendo el voltaje del vehículo (22-35V CC) para alimentar tanto la radio como el propio amplificador.
    f. Montaje (MT-1029): Se trata de un chasis de montaje que sujeta el transceptor portátil (RT-6241TG) y el amplificador/fuente de alimentación (AM-2411TG), permitiendo la instalación en un vehículo.
    g. Unidad de control remoto (C-2410TG): Una caja de control que permite manejar la radio desde una distancia de hasta 15 metros. Esta unidad tiene memoria para almacenar canales pre-programados.
19. CABLES:
    a. Cable de interconexión (CX 4723): Conecta el transceptor y el amplificador.
    b. Cable de control remoto (CX 2421 T): Permite conectar la unidad de control remoto a la radio.
    c. Cable de antena (CG 1127/U): Conecta la salida del amplificador a la antena vehicular.

Figura N° 24. AN-WRC

20. ANTENAS:
    a. El sistema utiliza antenas vehiculares, como la AT-803/VR.
    b. Accesorios de audio:
    c. Auricular (H-189/GR): Un auricular estándar militar para comunicación de voz.
    d. Micrófono (M-80/GR): Un micrófono manual que se puede usar en lugar del auricular.

    Altavoz (LS-454/U): Un altavoz externo que puede conectarse al sistema.

21. FALLAS MAS COMUNES EN EL AN-WRC-240T:

    Fallas:

    No hay ruido en la corneta.

    Posibles causas:

    Fase del sistema alimentación, CX-4720.

22. ACCIÓN A TOMAR:
    a. Reemplazar baterías. Revisar sistema eléctrico del vehículo.
    b. Colocar el positivo (rojo-blanco) y negativo (negro-verde) a la batería.
    c. No hay ruido en la corneta:

    Posibles causas:

    a. Switch de la corneta en posición OFF.
    b. Desconectado o pines doblados del conector CX-4723.

c. Colocarlo en "ON".

d. Reemplazar en caso de pines doblados y colocarlos en los receptáculos posteriores del AM-241 IT.

No recibe:

Posibles causas:

a. Conector CG-1127/U ACCIÓN A TOMAR:

b. Reemplazar conector CG -1127 AJ

No transmite:

Posibles causas:

a. Fuera de posición o en mal estado.

b. Otras (Ver fallas más comunes en el PRC-660).

Acción a tomar:

a. Colocarlo en la salida del RT-6241 y entrada del AM-2411.

23. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.
b. Instalar el equipo en un lugar apropiado para su adecuada operación.
c. Usar un paño limpio y seco para remover el polvo y la humedad de los micro teléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando

así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los micro teléfonos y altoparlantes.

d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

   1). Cables de tensión conectados incorrectamente (inversión de polaridad).

   2). Clavijas gastadas, rotas o desconectadas.

   3). Conectores de los cables de las antenas sueltos.

   4). Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Los altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo.

Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.
b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.
c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.
d. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.
e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.
f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

RADIO TRANSMISOR RECEPTOR RADIO UV 9R

a. Descripción:

El radio Baofeng UV-9R (o sus variantes Plus/Pro) es una radio portátil de doble banda (VHF/UHF) y resistente al agua y al polvo con certificación IP67 o similar. Sus características incluyen múltiples canales, VOX (manos libres), linterna LED, y un diseño robusto ideal para actividades al aire libre, seguridad y entornos húmedos. Ofrece comunicación confiable en largas distancias, con potencias de transmisión y rangos de alcance variables según el modelo específico.

b. Características y funciones:

1) Transceptor portátil de doble-banda con menú de funciones de visualización en la pantalla "LCD"
2) Con codificación DTMF • Batería de Ion- Litio de alta capacidad • Receptor de radio comercial en FM (65 MHz - 108 MHz)
3) Incorpora 105 códigos "DCS" y 50 códigos de privacidad «CTCSS» programables • Función «VOX» (transmisión activada por voz)

c. Función de alarma

1) Hasta 128 canales en memoria
2) Posibilidad de seleccionar Banda Ancha (Wide) o Estrecha (Narrow)
3) Posibilidad de seleccionar alta potencia o baja potencia de transmisión (5W/ 1W)
4) Iluminación de la pantalla y teclado programable
5) Función pitido “beep” en el teclado
6) Escucha dual/ recepción dual
7) Posibilidad de seleccionar los pasos de frecuencia de 2.5 /5/6.25/10/12.5/25 kHz

8) Posibilidad de seleccionar los pasos de frecuencia de 2.5 /5/6.25/10/12.5/25 kHz
9) Función "OFF/SET" (desplazamiento de la frecuencia de acceso del repetidor)
10) Función de ahorro de batería “SAVE”
11) Tiempo de transmisión “TOT” programable
12) Selección de Modo Escáner
13) Función de bloqueo de canal ocupado “BCLO”
14) Escáner de recepción CTCSS/ DCS integrado
15) Luz flash tipo LED integrada • Programable por PC
16) Nivel del Umbral "Silenciador" ajustable desde 0 a 9
17) Operación en bandas cruzadas “Cross/band”
18) Tono de fin de transmisión
19) Tecla de bloqueo integrada

24. DESEMPAQUETADO Y COMPROBACIÓN DEL EQUIPO

Desembale cuidadosamente el transceptor. Recomendamos que identifique los elementos que aparecen a continuación antes de desechar el material de embalaje. Si alguno de los elementos no está o han está dañado durante el envío, póngase en contacto con su distribuidor inmediatamente.

25. INSTALACIÓN DE ACCESORIOS ES INSTALACIÓN DE LA ANTENA.

Instalar la antena como indica la imagen y girarla en el sentido de las agujas del reloj hasta que no se pueda roscar.

26. INSTALACIÓN DEL CLIP DE CINTURÓN

Si lo necesita, instale el clip de cinturón en la parte trasera de la carcasa de la batería como se muestra en la imagen.

27. INSTALACIÓN DE LOS MICROAURICULARES EXTERNOS

Enchufar el “Jack” del microauricular externo de altavoz y micro “SP & MIC” en el aparato como indica la figura.

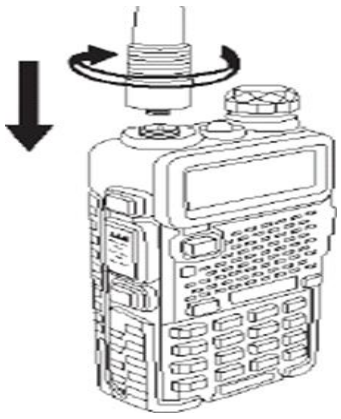
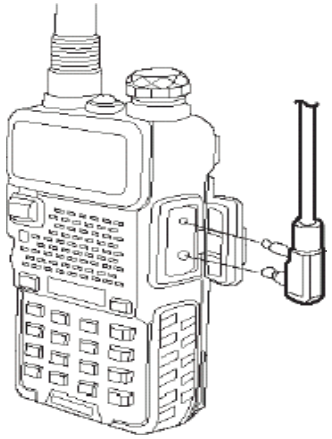


Figura N°25. Radio UV

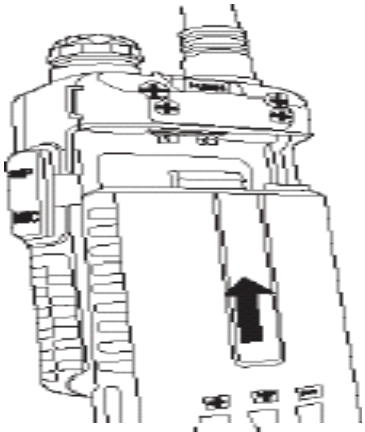
28. INSTALACIÓN DE LA BATERÍA

a. Al colocar la batería, asegúrese de que la batería esté paralela y en contacto con el chasis de aluminio. El fondo de la batería debe estar de 1 a 2 centímetros por debajo de la parte inferior del cuerpo de la radio.

b. Alinee la batería con los rieles de guía sobre el chasis de aluminio y deslícela hacia arriba hasta que se oiga un “click”.



Cuando la batería se alinee con el aparato, se bloquea automáticamente.

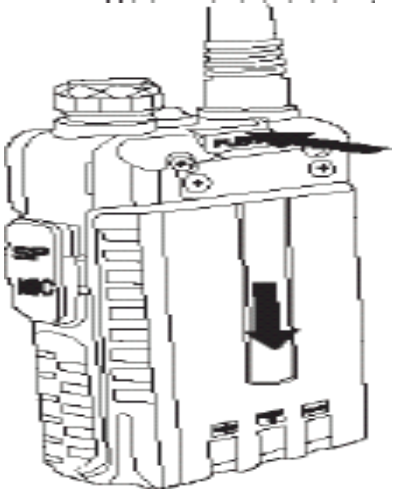


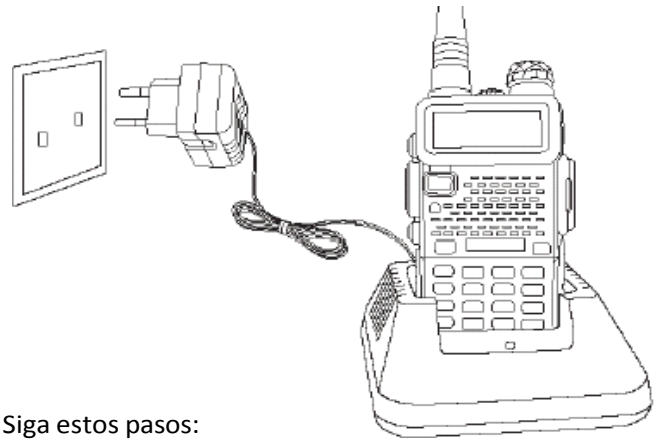
29. DESINSTALACIÓN DE LA BATERÍA

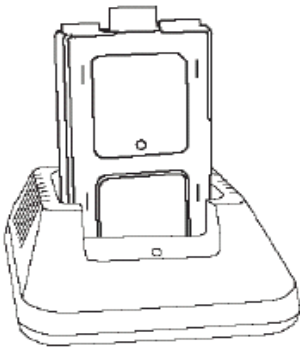
a. Apagar la radio antes de retirar la batería.

b. Presione el pestillo de la batería, en la parte superior del aparato, en la dirección indicada por la flecha.

c. Deslice hacia abajo la batería hasta que sobresalga aproximadamente 1 a 2 centímetros y luego retirarla cuerpo de la radio.







Siga estos pasos:

30. INFORMACIÓN DE LAS BATERÍAS

Uso inicial

Las baterías nuevas vienen descargadas completamente de fábrica. Cargar una batería nueva durante 5 horas antes del uso inicial. La capacidad máxima de la batería y el rendimiento se consigue después de tres ciclos completos de carga/ descarga. Si usted nota que la batería está baja, por favor recargue la batería.

31. TECLADO NUMÉRICO:

Usarlo para introducir la información para programar la lista de radio y los CTCSS no estándares.

En el modo transmisión, presione el teclado numérico para enviar las señales de código (el código debe ser introducido mediante el software del PC).

32. TONO 1750 Hz PARA ACCEDER A LOS REPETIDORES:

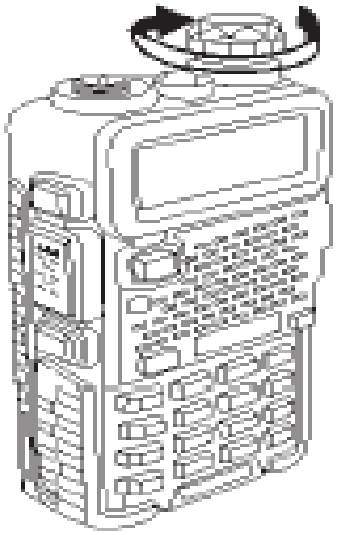
El usuario puede establecer comunicaciones de larga distancia a través de un repetidor de radio aficionados que se activa después de recibir un tono de 1750

Hz. Presione y sostenga el [PTT] y, a continuación, pulse el botón de [BAND] para transmitir un tono 1750 Hz.

33. OPERACIONES BÁSICAS:

Encendido – apagado (On- Off) / control de volumen:

Asegúrese de que la antena y la batería están instalados correctamente y la batería está cargada.



Gire la perilla en sentido horario para encender la radio y gire la perilla completamente a la izquierda hasta oír un 'clic' para apagar la radio. Gire la perilla en sentido horario para aumentar el volumen, o en sentido anti-horario para disminuir el volumen.

34. SELECCIONAR UNA FRECUENCIA O CANAL:

Pulse la tecla [▲] o [▼] para seleccionar la frecuencia/ canal deseado. La pantalla muestra la frecuencia / canal seleccionado. Pulse y mantenga pulsada la tecla [▲] o [▼] para llevar la frecuencia hacia arriba o hacia abajo rápidamente.

35. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de

los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.
b. Instalar el equipo en un lugar apropiado para su adecuada operación.
c. Usar un paño limpio y seco para remover el polvo y la humedad de los micro teléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los micro teléfonos y altoparlantes.
d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.
e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.
f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.
g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.
h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:
   1) Cables de tensión conectados incorrectamente (inversión de polaridad).
   2) Clavijas gastadas, rotas o desconectadas.
   3) Conectores de los cables de las antenas sueltos.

4) Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Los altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

36. LAS SIGUIENTES SON LAS PRECAUCIONES GENERALES DE SEGURIDAD EN LA OPERACIÓN Y MANTENIMIENTO DE LOS EQUIPOS:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

d. En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

g. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

RADIO MOTOROLA PRO 7100

a. Frecuencias de operación: VHF 136-174 MHZ UHF 403-470 / 450-527 MHZ
b. Potencia de operación: 25-45 VATIOS VHF / 25-40 VATIOS UHF
c. Capacidad de canales: 128 CANALES VHF 136-174MHZ, UHF403-470MHZ Y450-527MHZ
d. Push-To-Talk (PTT-ID) permite identificar quien está transmitiendo
e. Llamada selectiva permite a usuarios o grupos específico
f. Altavoz ubicado en la parte frontal del radio
g. Microteléfonos, armn4025
h. Pantalla de catorce caracteres alfa numérico
i. Espacio entre canales 12,5/20/25khz
j. Potencia de salida en VHF 45 W en UHF 40 W
k. Llamada de alerta
l. Llamada selectiva de voz (envío y recepción)

Figura N° 26. Motorola Pro 7100

37. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.
b. Instalar el equipo en un lugar apropiado para su adecuada operación.
c. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.
d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. Con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.
e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.
f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

   1) Cables de tensión conectados incorrectamente (inversión de polaridad).
   2) Clavijas gastadas, rotas o desconectadas.
   3) Conectores de los cables de las antenas sueltos.
   4) Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

i. Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

   1) Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.
   2) Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.
   3) Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.
   4) En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

5) En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.
6) En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.
7) Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

RADIO TRANSMISOR RECEPTOR RADIO QUANSHENG UV – K5

Descripción:

La Quansheng UV-K5 es una radio bidireccional de doble banda (VHF/UHF) de bajo costo y gran versatilidad, ideal para radioaficionados, seguridad y actividades al aire libre. Ofrece comunicación de largo alcance con 200 canales, una potencia de 5W, batería recargable de larga duración y carga por USB-C. Entre sus funciones se incluyen VOX, alerta de emergencia, receptor meteorológico NOAA, frecuencímetro, DTMF y la capacidad de copiar frecuencias de otras radios.

38. CARACTERÍSTICAS PRINCIPALES:

a. 200 canales Intercomunicador de banda cruzada.
b. Tono de llamada de 1750 HZ
c. Programa en el sitio.
d. Alerta de emergencia
e. Radio FM

f. Pantalla LCD
g. Mensaje de voz
h. Interruptor de recordatorio
i. Visualización múltiple de número de canal/frecuencia de canal/nombre de canal

39. ANCHO DE BANDA ANCHO/ESTRECHO

Asunto	cantidad
Radio portátil	1
Antenas	1
Li-ion	1
Cargador de batería	1
Pinza de cinturón	1
Manual de usuario	1

j. Conjunto de dirección de frecuencia compensada y replicación de radio inalámbrica
k. Nivel de silenciamiento ajustable y escaneo múltiple CTCSS/DCS Matar/Revivir a distancia
l. Bloqueo de teclado
m. Luz de fondo
n. PC Programable
o. Bloqueo de canal ocupado
p. VOX
q. Operación de vigilancia dual
r. Temporizador de tiempo de espera

s. Seleccionar llama da DTMF (llamada ú nica, llamada de grupo, llamada a todos)
t. Tiempo de apagado automático de retroiluminación selectivo
u. Búsqueda automática de señalización y frecuencia de varios pasos
v. Canal de llamada de una tecla

40. ACCESORIOS ESTÁNDAR

Teclado

Tecla PTT (Tecla de transmisión)

1) Tecla de conmutación de transmisión/recepción. Presione "PTT" para transmitir y hablar al micrófono. Suelte "PTT" para recibir.

Tecla de función programable y su función

2) Función inicial

3) Tecla lateral 1: presiónela durante un breve período de tiempo para activar la función Monitor. Presiónelo durante mucho tiempo para encender 1750 Hz. Tecla lateral 2: presiónela durante un breve período de tiempo para encender la luz Jack. Presiónelo durante mucho tiempo para encender la alarma.

Tecla del teclado

Tecla Menú/Confirmar: MENU

a. En la página principal, presione brevemente para ingresar al menú, elija el menú elemento y presione la tecla MENU para confirmar el parámetro.

b. Mantenga presionada esta tecla para ingresar al último

elemento de configuración.

c. Bajo la función DTMF, significa una palabra clave.

Tecla Salir/Borrar: SALIR

a. En el estado de edición, presione brevemente para salir y llegar al menú superior; manténgalo presionado para salir y volver a la página principal.

b. En el estado de entrada, presiónelo para borrar la información de entrada.

c. Bajo la función DTMF, significa palabra de código D.

Tecla Arriba:

Mover hacia arriba

Bajo la función DTMF, significa palabra de código B.

Tecla abajo:

a. Mover hacia abajo.

Especificaciones

Tabla 2 RADIO TRANSMISOR RECEPTOR RADIO QUANSHENG UV – K5

Especificaciones generales	
Canal:	200
Cantidad de canales de radio	20
Canal NOAA:	10

Estabilidad de frecuencia:	± 1ppm
Modo de modulación:	FM: 11 K Φ F3 E (12.5 KHz), 16 K Φ F3 E (25 KHz)
Dimensión:	115 mm X 60 mm X 37.5 mm
Peso:	234 g
Temperatura de funcionamiento:	-20 ℃ + 60 ℃
Impedancia	50Ω

RECEPCIÓN	
Sensibilidad:	
FM (12dB SINAD)	F1(50∽76) -121dBm F2(108∽135.9975) -121dBm F3(136∽173.9975) -123dBm F4(174∽349.9975) -123dBm F5(350∽399.9975) -123dBm F6(400∽469.9975) -123dBm F7(470∽599.9975) -121dBm
WFM (20dB SINAD)	WFM (76∽108) -110dBm
AM (10dB S/N)	F2(108∽135.9975) -113dBm

Frecuencia de audio:	≥0.5W
Distorsión de audio:	≤10%

TRANSMISIÓN:

Banda de transmisión de la versión FCC

Frecuencia: UHF420∽450MHz/VHF144∽148MHz

Banda de transmisión de la versión CE

Frecuencia: UHF430∽440MHz/VHF144∽146MHz

banda de transmisión versión

Figura 27 RADIO TRANSMISOR RECEPTOR RADIO QUANSHENG UV – K5

Potencia de salida:	≤5W	≤5W
Corriente de emisión:	≤1.5A	≤1.5A
Desviación de frecuencia máxima:	≤5 KHz (25 KHz), ≤2.5 KHz (12.5 KHz)	≤5 KHz (25 KHz), ≤2.5 KHz (12.5 KHz)
Distorsión de modulación:	≤5%	≤5%
Poder perdido:	≤7.5uW	≤7.5uW
Potencia del canal adyacente:	70 dB (25 KHz), 60 dB (12.5 kHz)	70 dB (25 KHz), 60 dB (12.5 kHz)
Modulación residual:	40dB	40dB

Frecuencia: UHF400⌣470MHz/VHF136⌣17

Figura 28 RADIO TRANSMISOR RECEPTOR RADIO QUANSHENG UV – K5

Mantenimiento Preventivo:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

1. Inspeccionar que el equipo este completo con todos sus accesorios.

2. Instalar el equipo en un lugar apropiado para su adecuada operación.

3. Usar un paño limpio y seco para remover el polvo y la humedad de los micro teléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así

la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los micro teléfonos y altoparlantes.

4. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. Con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

5. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

6. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

7. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

8. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

    a. Cables de tensión conectados incorrectamente (inversión de polaridad).

    b. Clavijas gastadas, rotas o desconectadas.

c. Conectores de los cables de las antenas sueltos.

d. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los micro teléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

1. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

2. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

3. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

4. En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

5. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre

éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

6. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

7. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

RADIO TRANSMISOR RECEPTOR EP-450

1. INTRODUCCIÓN Y ALCANCE

Este manual proporciona la información técnica y los procedimientos operativos necesarios para la correcta instalación, configuración y uso del radio móvil VHF FM EP-450. Está dirigido a técnicos y usuarios finales que operen el equipo en aplicaciones de radiocomunicación móvil terrestre, tales como seguridad, transporte, industria y servicios.

2. DESCRIPCIÓN GENERAL DEL EQUIPO

El EP-450 es un radio de comunicaciones móvil profesional de banda VHF, diseñado y fabricado por Entel Chile. Es un equipo robusto y confiable, concebido para operar en vehículos, proporcionando comunicaciones de voz claras y eficaces en un entorno de trabajo exigente.

Principales Características Operativas:

a. Comunicaciones Móviles: Diseñado específicamente para instalación en vehículos, operando en la banda VHF (136-174 MHz).

b. Robustez y Durabilidad: Construcción metálica y estándares de fabricación que garantizan su operación en condiciones adversas de temperatura, vibración y humedad.

c. Funcionalidad y Flexibilidad: Cuenta con múltiples canales programables, funciones de exploración (Scan) y opciones de tonos squelch (CTCSS/DCS) para una operación flexible en redes compartidas.

d. Audio de Alta Potencia: Altavoz interno de 5W que garantiza un audio nítido incluso en entornos ruidosos.

3. CARACTERÍSTICAS TÉCNICAS DETALLADAS

3.1. Especificaciones de Radiofrecuencia (RF)

Parámetro	Especificación
Banda de Frecuencia	136 - 174 MHz (VHF)
Número de Canales	16 canales (estándar, expandible vía software)
Potencia de Salida (RF)	Alta: 25W / 30W (según versión), Baja: 1-5W (programable)

Parámetro	Especificación
Sensibilidad del Receptor	Mejor de 0.25 µV para 12 dB SINAD
Selectividad	Mejor de 70 Db
Inmunidad a Interferencias	Mejor de 70 dB
Espurios y Armónicos	Mejor de 65 dB (60 dB típico)

3.2. Especificaciones Generales

Parámetro	Especificación
Tipo de Emisión	16K0F3E (FM)
Fuente de Alimentación	13.8 V DC (negativo a masa). Tolerancia: ±15%
Consumo de Corriente	En recepción:~0.8ª En transmisión (MAX Potencia): ~7.5 A
Sistema de Tonos Squelch	CTCSS (38 tonos estándar), DCS (Códigos Digitales)

3.3. Especificaciones de Audio

Parámetro	Especificación
Potencia de Audio (Altavoz Int.)	5 W (máxima) con <10% de distorsión
Respuesta en Frecuencia (Audio)	300 - 3000 Hz
Conectores	Micrófono: Conector de 4 pines Altavoz externo: Conector de 2 pines

3.4. Especificaciones Mecánicas y Ambientales

Parámetro	Especificación
Dimensiones (A x P x H)	Aprox. 160 mm x 155 mm x 45 mm (sin protuberancias)
Peso	Aprox. 1.3 kg
Temperatura de Operación	-30°C a +60°C
Temperatura de Almacenamiento	-40°C a +80°C
Grado de Protección (IP)	IP54 (Protegido contra polvo y salpicaduras de agua)

4. CONFIGURACIÓN Y PARTES PRINCIPALES

1. Unidad Principal (Transceptor):

    a. Panel Frontal: Contiene el control de volumen/encendido, perilla selectora

    b. De canales, botones de funciones, LED indicador de estado y altavoz.

    c. Parte Superior: Conector para micrófono.

    d. Parte Posterior: Conectores para alimentación, antena, altavoz externo e interfaz de programación.

    e. Micrófono: Con cable, con pulsador PTT (Presionar Para Hablar) y posiblemente botones para funciones adicionales (como exploración o cambio de potencia).

    f. Cable de Alimentación: Con fusible integrado para protección.

    a. Soporte de Montaje: Brazo y base para fijación en el vehículo.

5. PROCEDIMIENTOS BÁSICOS DE OPERACIÓN

    a. Instalación y Encendido:

        1. Conecte el cable de alimentación a una fuente de 13.8V DC del vehículo (generalmente directamente a la batería, con fusible).

        2. Conecte la antena VHF firmemente al conector correspondiente en la parte posterior del radio.

3. Conecte el micrófono al conector frontal.

4. Gire la perilla de VOLUMEN/ENCENDIDO en sentido horario para encender el equipo. Se escuchará un clic y el display se encenderá.

b. Operación básica en un canal:

1) Seleccionar Canal: Gire el selector de canales para elegir el canal preprogramado deseado.

2) Ajustar Volumen: Gire la perilla exterior (VOLUMEN) hasta un nivel de audio confortable.

3) Ajustar Squelch: Gire la perilla interior (SQUELCH) hasta el punto donde el ruido de fondo se silencie y solo se abra al recibir una señal válida.

4) Para Transmitir: Mantenga presionado el pulsador PTT en el micrófono y hable claramente a una distancia normal (2-5 cm). El LED en el panel frontal se encenderá en color ROJO.

5) Para Recibir: Suelte el PTT. El LED volverá a verde o se apagará, indicando que el radio está en modo de recepción.

c. Funciones adicionales comunes:

1) Cambio de Potencia: Algunos canales pueden estar programados para permitir el cambio entre Alta y Baja potencia, generalmente mediante un botón en el micrófono o en el panel.

2) Exploración (Scan): Presionar el botón de SCAN (si está programado) hará que el radio barra secuencialmente los canales en busca de actividad.

6. MANTENIMIENTO PREVENTIVO Y RECOMENDACIONES

a. Limpieza: Limpie el exterior del radio con un paño seco o ligeramente humedecido con agua y un detergente suave. No utilice disolventes o productos abrasivos.

b. Ventilación: Asegúrese de que las rejillas de ventilación del radio no estén obstruidas para evitar sobrecalentamiento.

c. Conexiones: Periódicamente, verifique que los conectores de alimentación y antena estén firmemente ajustados. Una conexión de antena suelta puede dañar el radio.

d. Fusible: Si el radio no enciende, verifique el estado del fusible en el cable de alimentación.

e. Antena: NUNCA active el transmisor sin tener la antena correctamente conectada. Esto puede causar daños graves e irreversibles en la etapa final de transmisión.

f. Programación: La configuración de frecuencias, tonos y funciones debe ser realizada por un técnico calificado utilizando el software y cable de programación específicos para el modelo EP-450.

Mantenimiento Preventivo:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

1. Inspeccionar que el equipo este completo con todos sus accesorios.

2. Instalar el equipo en un lugar apropiado para su adecuada operación.

3. Usar un paño limpio y seco para remover el polvo y la humedad de los

4. microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

5. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc.., con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

6. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

7. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

8. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

9. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

    1) Cables de tensión conectados incorrectamente (inversión de polaridad).

    2) Clavijas gastadas, rotas o desconectadas.

    3) Conectores de los cables de las antenas sueltos.

4) Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

1. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

2. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

3. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

1. En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

2. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc, ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la

herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

3. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

4. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

ICOM IC-A110

El receptor ICOM IC-A110 es un dispositivo de radiocomunicación diseñado para su uso en aviones. Con un diseño compacto y ligero, este receptor proporciona una comunicación clara y confiable en el aire. El IC-A110 utiliza tecnología de radiofrecuencia avanzada para ofrecer un rendimiento excepcional en términos de recepción y transmisión de señales. Con una potencia de salida de hasta 36 vatios, este receptor garantiza una comunicación clara incluso en condiciones adversas. El IC-A110 cuenta con una pantalla LCD fácil de leer que muestra información importante como la frecuencia, el canal y el estado de la batería. También incluye una función de escaneo que permite la exploración rápida de diferentes frecuencias para encontrar las más utilizadas en el entorno aéreo. Este receptor está diseñado para ser fácil de instalar y utilizar. Viene con un conjunto completo de accesorios, incluyendo un soporte de montaje y un micrófono de mano. La interfaz de usuario intuitiva permite una operación sencilla, incluso para aquellos que no están familiarizados con los equipos de radiocomunicación. En términos de durabilidad, el IC-A110 está construido con materiales de alta calidad que garantizan su resistencia y confiabilidad a largo plazo. Cumple con los estándares industriales más exigentes y está diseñado para soportar condiciones extremas en el entorno aéreo. En

resumen, el receptor ICOM IC-A110 es una opción confiable y eficiente para la comunicación aérea. Con su diseño compacto, características avanzadas y facilidad de uso, este receptor es una opción popular entre los pilotos y operadores aéreos en Venezuela.

Características

General

•Cobertura de frecuencia: 118 a 136,975 MHz
• Espaciado de canales :25 kHz o 25/8.33 kHz
• Modo: AM (6K00A3E)
•Número de canales de memoria: 20
•Fuente de alimentación aceptable: 13,75V o 27,5V CC (tierra negativa) Selección automática
• Rango de temperatura utilizable :–30℃ a +60ðo
•Estabilidad de frecuencia: ±5ppm
•Consumo de corriente
(a 13,75 V CC): Tx 5 A (máx.)
Receta médica 4 A (en OFF máx.)
0,5 A (en modo de espera)

Transmisor

•Potencia de salida: 36 W (energía) típico

9 W (portadora) típica

•Modulación: Modulación de última etapa

•Limitación de modulación :70 a 100 %

•Distorsión armónica de audio: Menos del 10 %

(con una modulación del 85%)

•Relación entre zumbido y ruido: Más de 40 dB

• Emisiones espurias: –16dBm o menos

• Impedancia de la antena: Estándar 50Oh con ROE

Receptor

•Sistema de recepción: Doble conversión

superheterodino

• Frecuencias intermedias: 1º 38,85 MHz

2º 450 kHz

•Sensibilidad

(en6dB Relación señal/ruido: Menos de 1 µV (pd)

•Sensibilidad del silenciador: Menos de 0,35 µV (pd)

(en el umbral)

•Selectividad

Espaciado entre canales de 25 kHz: Más de ±8 kHz (a–6 dB)

Menos de ±17 kHz (a–40 dB)

Menos de ±25 kHz (a–60 dB)

8.33* espaciado de canales en kHz Más de ±2,778 kHz (a–6 dB)

Menos de ±7,37 kHz (a–60 dB)

•Respuesta espuria rechazada, Más de 74 dBµ

• Potencia de salida de audio: Más de 10 W (a 13,75 V CC)

con 8Oh carga 60 % MOD. 10% (distorsión)

Tono lateral Más de 100 mW (con 500Oh

carga 60% MOD. 10 % distorsión)

•Zumbido y ruido: Más de 25 dB

• Impedancia de salida de audio: Ext. SP 8Oh

Tono lateral 500Oh

Accesorios

1. Micrófono

2. Soporte para micrófono 1 un juego

3. Cable de micrófono

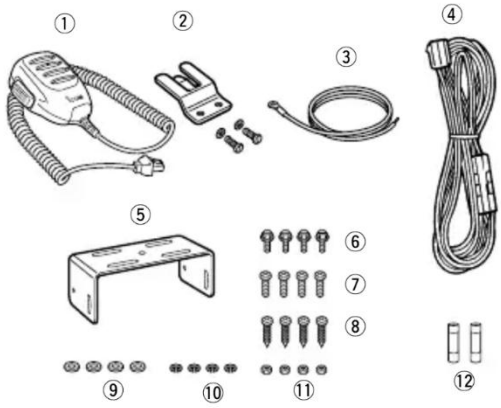
4. Cable de alimentación de CC (OPC-344)

5. Soporte de montaje

6. 4 pernos de Soporte

7. 4 tornillos de Montaje (M5 x 12)

8. 4 tornillos autorroscantes (M5 x 20)



9. 4 arandelas planas

10. 4 arandelas elásticas

11. 4 tuercas

12. 2 fusibles (10 A)

Mantenimiento Preventivo:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

1. Inspeccionar que el equipo este completo con todos sus accesorios.

2. Instalar el equipo en un lugar apropiado para su adecuada operación.

3. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

4. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc., con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

5. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

6. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

7. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

8. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también

puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

a. Cables de tensión conectados incorrectamente (Inversión de polaridad).

b. Clavijas gastadas, rotas o desconectadas.

c. Conectores de los cables de las antenas sueltos.

d. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

9. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

10. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

11. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

12. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

MOTOROLA PRO-5100

El Motorola PRO-5100 VHF es una radio móvil analógica profesional con 64 canales, pantalla alfanumérica de 14 caracteres y funciones de señalización MDC como PTT-ID y Llamada Selectiva. Está diseñado para comunicaciones eficientes y seguras en sectores como seguridad, transporte y construcción, ofreciendo robustez y claridad de audio incluso en entornos ruidosos.

Características

• 64 canales convencionales

• 15 zonas troncalizadas con 16 grupos de conversación cada una.

• Identificación de Llamada PTT-ID (envío / recepción)

• Alerta de Llamada (envío / recepción)

• Llamada Selectiva de Voz (envío / recepción)

• Verificación del Radio (envío / recepción)

• Inhibición Selectiva del Radio (recepción)

• Emergencia (envío)

• Señalización Quik-Call II (envío / recepción)

• Zonificación • Monitoreo • Rastreo con Doble Prioridad

• Pantalla de 14 Caracteres Alfanuméricos

• Bloqueo de Canal Ocupado

• Limitador de Tiempo de Transmisión

• Eliminación de Canal no Deseado

• Botones Intercambiables

• CSQ / PL / DPL / Inv-DPL

• Puerto para Tarjetas Opcionales

Accesorios

a. Alimentación:

1) Cables de alimentación para radio móvil.

2) Cargadores de vehículo para la batería.

b. Audio:

1) Micrófonos tipo altavoz.

2) Micrófonos con teclado.

3) Auriculares.

c. Programación y Conexión:

1) Cables de programación USB FTDI, como el RKN4081, para conectar la radio a un ordenador.

d. Componentes del Radio:

1) Baterías.

2) Antenas.

3) Caras frontales completas.

4) Perillas del interruptor de volumen.

5) Clips de sujeción.

Mantenimiento Preventivo:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

1. Inspeccionar que el equipo este completo con todos sus accesorios.

2. Instalar el equipo en un lugar apropiado para su adecuada operación.

3. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

4. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc., con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las

mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

5. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

6. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

7. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

8. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:
   a. Cables de tensión conectados incorrectamente (Inversión de polaridad).

   b. Clavijas gastadas, rotas o desconectadas.

   c. Conectores de los cables de las antenas sueltos.

   d. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar

primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

1. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.
2. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

3. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

4. En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.
5. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc, ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.
6. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

7. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando

excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

SISTEMA TRASPORTABLE DE COMUNICACIONES N° 3 “CAP. JUAN DE DIOS AGRAZ”

DESCRIPCIÓN GENERAL

EL SISTEMA TRASPORTABLE DE COMUNICACIONES N° 3 “CAP. JUAN DE DIOS AGRAZ” es un vehículo no motorizado, diseñado para establecer comunicaciones entre diferentes puntos, ya sea HF.UHF.VHF TACTICO Y ADMINISTRATIVO, como también Comunicaciones Satelitales, este contiene además comunicaciones aire tierra y punto de circuito cerrado para la seguridad del mismo, también puede ser operado con un repetidor administrativo usado un radio como estación base y radios portátiles para las operaciones de comando y control del sistema defensivo territorial.

Figura N° 29
STC N° 3 AGRAZ.

STC. N° 3 ¨AGRAZ¨

El STC N° 3 está equipado con sistema de alimentación múltiple, es decir, que puede ser alimentado con corriente alterna procedente de la red pública AC 110V, así como de un banco de baterías internas alimentadas por dos (02) paneles solares y corriente alterna, así mismo, posee un generador portátil el cual se encuentra dentro del STC-III. Cuando el STC-III esta alimentado por la red pública de corriente alterna un cargador de baterías se encarga de que las mismas se mantengan completamente cargadas

CARGADOR DE BATERÍAS NEWMA PT 40 PC

Si durante la operación con corriente alterna, ocurriera una interrupción en la red de alimentación de corriente alterna, el STC-III “CAP. JUAN DE DIOS AGRAZ” continuará su operación sin interrupción alguna debido a que la alimentación será transferida, de forma automática, al banco de baterías, mediante un sistema de transferencia de energía

SISTEMA DE ALIMENTACIÓN PANEL SOLAR

Igualmente, si el STC debe ser operado en un lugar donde no esté disponible una red de corriente alterna, el mismo puede ser operado con la alimentación de las baterías. En este tipo de situaciones un equipo de inversor DC/AC 12V A 110V se encargará de suministrar corriente alterna para disponer de ella en las diferentes tomas situadas en el STC-III.

Durante el tiempo que se esté usando este banco de baterías las misma estarán siendo cargadas, poniendo en funcionamiento dos paneles solares.

1. PROCEDIMIENTOS DE ENCENDIDO DEL SISTEMA TRASPORTABLE DE COMUNICACIONES III “CAP JUAN DE DIOS AGRAZ”

   a. Debe dirigirse a la PUERTA “C” y tomar la extensión eléctrica con conectores amarillos colocada en la parte de arriba.
   b. Conectar la extensión eléctrica a una toma de corriente de 110v en la cual debe verificar con un multímetro que la misma sea de 110 voltios y no de 220 voltios y la otra punta de la extensión al sistema trasportable de comunicaciones a la TOMA PRINCIPAL.

c. Chequear que los equipos estén apagados luego dirigirse a la BREKERA PRINCIPAL y pasar el switch a modo ON.

d. Dirigirse al frente del S.T.C. III y pasar el switch de la REGLETA “A” a modo ON.

e. Pasar el switch de la REGLETA “B” a modo ON.

2. FUENTE DE PODER NEUMAR Y MODULO DE CONTROL DE FUNCIÓN NEUMAR PFM-400

a. Pasar el switch de la REGLETA “C” a modo ON.
b. pasar el switch de la FUENTE DC ubicada en la parte de arriba de la REGLETA “A” a modo ON.
c. dirigirse a la parte de atrás del S.T.C. III y abrir la PUERTA “B” y presione el botón de la fuente y banco de baterías de 24V del radio Marca Manpack.

d. Dirigirse a la PUERTA “A” frente el S.T.C. III y Presione el botón de encendido durante diez (10) segundo del radio VHF MANPACK- MR9560

e. Dirigirse en la parte de debajo de radio MR-9560 y gire la perilla de volumen del radio HF BARRET-950 para su encendido.

f. Presionar el botón rojo de encendido de la radio base tetra MTM-5400 el cual se encuentra en la parte de arriba del radio MANPCK-VHF MR9560.

g. Dirigirse frente el RADIO BASE PRO-5100 y presione la perilla de volumen durante diez (05) segundos para su encendido.

h. debajo de la radio base PRO-5100 se encuentra el radio VRC-240 VHF y UHF El cual tiene su fuente de alimentación de bajo de la etiqueta donde puede ver el nombre del radio Pase la perilla de encendido a modo ON.

i. Encienda el DVR y monitor de circuito cerrado al lado derecho de la Radio base PRO-5100

j. Diríjase a la parte de arriba del STC-III y conecte las antenas

k. Abrir la puerta D. y Bajar la planta eléctrica los dos bancos de madera los cuales no pueden mojarse,

PANEL SWICHT DE DISTRIBUCIÓN DE ENERGÍA

3. PROCEDIMIENTOS DE APAGADO DEL SISTEMA TRASPORTABLE DE COMUNICACIONES III **:**

Se debe seguir las siguientes instrucciones para el apagado del sistema es inportante resguardar todo el material de antenas y micros de los equipos los cuales debe reguardar en el gabetero principal del sistema.

a. Pase la perilla de encendido a modo OFF de la fuente del radio VRC-240 VHF-UHF.

b. Pase la perilla de encendido a modo OFF del radio VRC-240 VHF-UHF.

c. Presionar la perilla de volumen de la RADIO BASE PRO-5100 para su apagado.

d. Presionar el botón rojo en la RADIO BASE TETRA hasta que visualice que se apague.
e. Pasar el Switch de la FUENTE DC ubicada en la parte de arriba al lado derecho de la radio base tetra a modo OFF.

f. Presione el botón de encendido durante diez (05) segundos del radio VHF MANPACK- MR9560 se encuentra debajo de la radio base tetra MTM-5400.

g. Dirigirse en la parte de debajo de radio MR-9560 y gire la perilla del radio BARRET-950 HF

h. dirigirse a la parte de atrás del S.T.C. 2 y abrir la PUERTA “B” y presione el botón de la fuente y banco de baterías de 24V de los radios Marca Manpack Para su apagado

i. Pasar el switch de la REGLETA “C” a modo OFF.

j. Pasar el switch de la REGLETA “B” a modo OFF.

k. pasar el switch de la REGLETA “A” a modo OFF.

l. Chequear que los equipos estén apagados en su totalidad luego dirigirse a la BREKERA PRINCIPAL y pasar el switch a modo OFF.

m. Desconectar la extensión eléctrica de la toma principal del S.T.C. 2 y de la toma de corriente de 110v.

n. Dirigirse a la PUERTA “C” y guardar la extensión eléctrica con conectores amarillo y negro en la parte de arriba.

o. Abrir la puerta D y Guardar la planta eléctrica
p. Debe resguardar en la parte de arriba las antenas de cada radio pasando revista de la antena de la radio base tetra la cual por su pequeño tamaño puede extraviarse o ser olvidada en el terreno.

q. Se debe asegurar después de cerrar el sistema con llaves y pasar su seguro nuevamente pasando revista que no abra ninguna de las puertas.

4. OPERACIÓN DE ALIMENTACIÓN CON BATERÍAS

a. Active el conmutador de baterías

b. Active el conmutador 1 del panel de distribución 1

c. Active conmutador 1 y 2 del panel de distribución 2

d. Verifique que la lámpara indicadora DC este iluminado.

e. Si se requiere de alimentación de corriente alterna, situé el interruptor del inversor en posición de encendido

f. Verifique que la lámpara indicadora AC INTERNA esta iluminada

g. Nota: una vez terminada la operación, apague el interruptor del inversor y desactive el conmutador de las baterías.

5. OPERACIÓN CON EL GENERADOR PORTÁTIL

a. Encienda el generador.

b. Gire la válvula de combustible de combustible que se encuentra debajo del tanque a la posición ON.
c. Mueva la palanca de control del ahogador totalmente hacia la derecha.
d. Encienda el generador tirado lentamente de la cuerda del arrancador hasta sentir una resistencia. Luego tire de la cuerda rápidamente para vencer la compresión para arrancar el motor.

e. Mueva lentamente la palanca de control del ahogador totalmente hacia la izquierda a medida que el motor se caliente.

f. Con el generador en funcionamiento se suministra energía a las tomas de corriente.

6. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.

b. Instalar el equipo en un lugar apropiado para su adecuada operación.

c. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

i. Cables de tensión conectados incorrectamente (Inversión de polaridad).

j. Clavijas gastadas, rotas o desconectadas.
k. Conectores de los cables de las antenas sueltos.

l. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

d. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: Agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

SISTEMA DE COMUNICACIONES DE ALTA MOVILIDAD “D&R ATANASIO GIRARDOT.

EL SISTEMA DE COMUNICACIONES DE ALTA MOVILIDAD “ATANASIO GIRARDOT”, consta de 2 equipos de radio que operan en la banda de frecuencia VHF administrativo que actúan como un sistema repetidor a través de un dúplex que permite, la operatividad de ambos equipos con una sola antena, este sistema consta de 2 tipos de fuente de alimentación la primera, a través de un inversor de corriente de 110v a 12v también puede ser alimentado desde su vehículo de transporte tipo moto con alimentación de 12v.

Es un dispositivo de telecomunicaciones de alta frecuencia (VHF: Very High Frequency, típicamente de 136 a 174 MHz para uso comercial/privado) diseñado para extender significativamente el alcance y la cobertura de un sistema de radio bidireccional, como los utilizados por organismos gubernamentales, empresas de seguridad, servicios de emergencia o grandes corporaciones (uso administrativo).

Sus características se centran en la confiabilidad, el rendimiento continuo (ciclo de trabajo alto) y la capacidad de integración en redes de comunicación complejas.

CARACTERÍSTICAS PRINCIPALES.

Las características clave de un repetidor VHF administrativo se pueden agrupar en aspectos de radiofrecuencia (RF), operación y capacidad de red.

1. ACCESORIOS:

a. 02 radios Motorola VHF

b. Antena 02 Dipolos VHF

c. Inversor 12v-110v

d. Fuente de poder 110v-12v.

e. 02 radios EP-450 VHF

f. Duplexor de Antena

2. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.

b. Instalar el equipo en un lugar apropiado para su adecuada operación.

c. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

i. Cables de tensión conectados incorrectamente (inversión de polaridad).

j. Clavijas gastadas, rotas o desconectadas.

k. Conectores de los cables de las antenas sueltos.

l. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

d. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: Agua dulce, agua

destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.
g. Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

SISTEMA DE COMUNICACIONES MÓVIL

“TONY”

1. DESCRIPCIÓN GENERAL

El Sistema de Comunicaciones Móvil ‘‘TONY’’, consta de 04 equipos de radio que operan en las bandas de frecuencia HF (Barret 5020),VHF (Motorola Pro5100-Administrativo),UHF (Motorola Em-200-Administrativo), Tetra(Motorola Mtm 5400), que actúan como un Puesto de Comando de Comunicaciones Móvil a través de 4 tramos de mástil desarmable/armable permite la operatividad de los equipos con sus antenas de una manera rápida y eficaz, este sistema consta de 1 tipo de fuente de alimentación a través de corriente de 110v a una fuente de poder estabilizada de 12v.

2. CARACTERÍSTICAS TÉCNICAS:

Este sistema de comunicación moderno es multibanda/multiequipos, para asegurar la interoperabilidad en las operaciones militares.

3. BANDAS DE FRECUENCIA Y PROPAGACIÓN

Cada banda de frecuencia tiene usos específicos debido a sus características de propagación:

Banda	Rango de Frecuencias (Aprox.)
HF (Alta Frecuencia)	3 — 30 MHz
VHF (Muy Alta Frecuencia)	30 — 300 MHz
UHF (Ultra Alta Frecuencia)	300 MHz – 3 GHz
TETRA (Terrestrial Trunked Radio)	Generalmente en bandas UHF (380 — 470 MHz).

4. MODOS DE OPERACIÓN Y SEGURIDAD

Los equipos modernos, especialmente las Radios TETRA, soportan múltiples modos de operación y altos niveles de seguridad:

5. MODOS DE OPERACIÓN COMUNES

Voz y Datos: Analógico (AM/FM) y Digital.

Multimodo: CW, AM, FM, SSB, C4FM, PSK31, RTTY.

Troncalizado (TMO): Uso de una infraestructura de red (como en TETRA).

Directo (DMO): Comunicación directa entre terminales sin infraestructura.

Salto de Frecuencia (ECCM): Mecanismo contra contramedidas electrónicas para evitar la interferencia y la detección.

ALE (Automatic Link Establishment): Utilizado en HF para establecer automáticamente el mejor enlace de comunicación.

Cifrado de Extremo a Extremo (E2EE): Fundamental en comunicaciones militares y TETRA.

6. POTENCIA Y ROBUSTEZ: La potencia de salida (TX) varía enormemente según la configuración (portátil, mochila o vehicular/base) y la banda de frecuencia

Configuración / Banda	Potencia de Salida (Ejemplos Típicos)
TETRA Portátil (UHF)	Clase 3L (1.8 W) o Clase 4 (1 W).
VHF Portátil/Mochila (Tácticas)	5 W (portátil), 25 W (mochila), 50 W (móvil/ base).
HF/VHF/UHF Multibanda (Vehicular)	HF: 5 — 100 W. VHF/UHF: 5 — 50 W. SATCOM de UHF: 5, 20, 50 W.
HF/VHF/UHF Multibanda (Amateur/Comercial)	HF: 100 W. VHF/UHF: 50 W.

1. ACCESORIOS

- Radio Barret HF
- Microtelefono
- Antena Dipolo
- Radio Motorola TETRA
- - Microtelefono
- Antena látigo
- GPS
- Radio Motorola UHF
- Microtelefono
- Antena Dipolo UHF
- Radio Motorola VHF
- Microtelefono
- Antena Vehicular
- Interfaz de transmisión de imagen
- 02 radios EP-450 UHF
- 02 radios EP-450 UHF

2. MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

a. Inspeccionar que el equipo este completo con todos sus accesorios.

b. Instalar el equipo en un lugar apropiado para su adecuada operación.

c. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

d. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc. con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.
e. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

f. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.
g. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

h. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:

1) Cables de tensión conectados incorrectamente (Inversión de polaridad).

2) Clavijas gastadas, rotas o desconectadas.
3) Conectores de los cables de las antenas sueltos.

4) Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.

b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

d. En la ejecución de las tareas de limpieza: Eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

e. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.

f. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

SICOIN

Sistema de Comunicaciones Integrado "ESEQUIBO"

Es un sistema comunicaciones móvil que incorpora equipos de transmisión y recepción de señales de radio en HF, VHF y UHF. Su versatilidad y eficiencia en el terreno lo hacen útil para operaciones en entornos inhóspitos y aquellas donde se requiera gran movilidad. Con capacidad de alimentación por corriente alterna, directa y por panel solar con banco de baterías provisto es capaz de mantener las comunicaciones en cualquier parte del territorio nacional.

Capacidades:

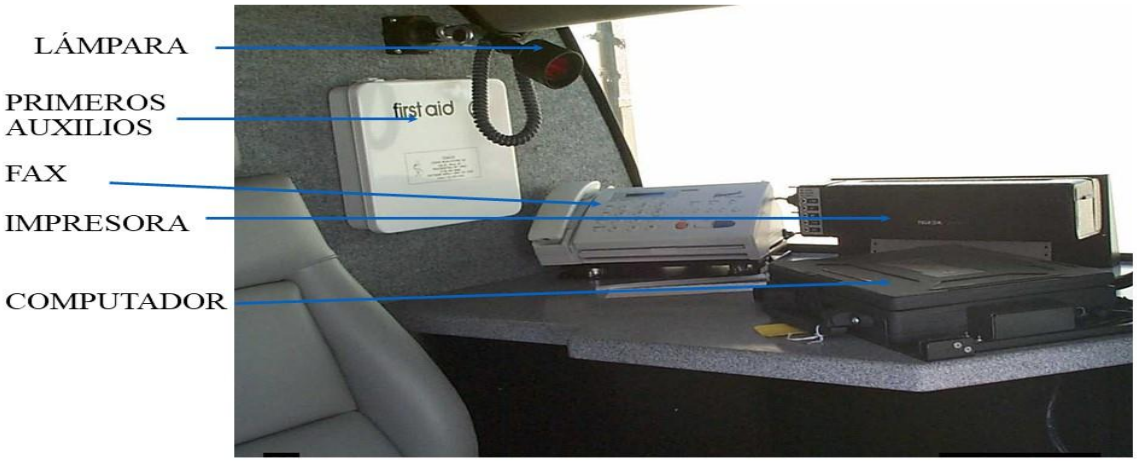
1) Establecer enlaces de comunicaciones en la banda de frecuencia HF, VHF y UHF.

2) Redundancia en conexión de energía eléctrica: Red pública, planta eléctrica y sistema de energía fotovoltaica.

3) Integración de equipos de comunicaciones.

Accesorios:

Radio Motorola Tetra MTM-5400 Serial: 938TPA1199



Compuesto por:

A. Altavoz

B. Micro

C. Antena

D. Base de antena

E. Línea de trasmisión CS23 LOW LOSS de (05) metros para señal de

F. Línea de trasmisión RG174U de seis (06) metros para señal de GPS

G. Cable de alimentación rojo y negro de 2.5 metros

RADIO MOTOROLA PRO-5100

Compuesto por:

A. Micro serial

B. Antena vehicular de VHF látigo

C. Línea de trasmisión de tres metros (03) RG223 con base de Antena y

conector (TNC)

D. Cable de alimentación rojo y negro un (01) metro conectado a la

fuente Astron.

RADIO BARRETT 950 HF

Compuesto por:

A. Micro

B. Parlante

C. Cable de alimentación

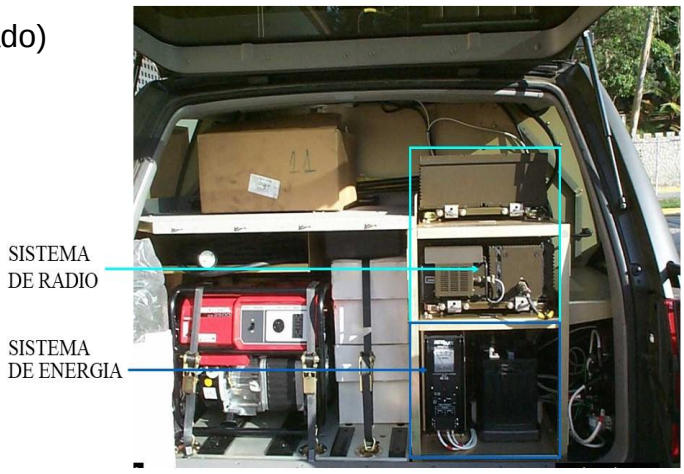
D. Cable DV9 conectado del radio al panel frontal

E. Panel Frontal

F. Cable de audio que va conectado del frontal al parlante

G. Antena Dipolo HF (8 metros de cada lado)

H. Bajante de antena RG58 de antena HF



MATRIZ DE AUDIO ACU-1000

Compuesto por:

A. Cable de alimentación

B. Cable de interfaz de audio para radio Motorola TETRA MTM5400

C. Cable de interfaz de audio para radio Aire-Tierra RF-AM 2411

D. Micro teléfono

Radio TADIRAN RT-7330 (S) VHF

Compuesto por:

A. Micro Serial:

B. Antena látigo de dos (02) secciones

C. Base de antena VHF

D. Bajante de antena

EQUIPO DE RADIO AIRE-TIERRA ICOM VHF:

Compuesto por:

A. Micro

B. Antena de Radio ICOM

C. Bajante de antena con conector BNC de 6 metros.

Fuente de alimentación de 12 voltios

Compuesto por:

A. Con cable de alimentación

Sistema de Energía de Panel Solar

Compuesto por:

A. Controlador de carga de 12V,24V y 48V

Cargador de batería RM2033 con cable de alimentación

Panel de distribución De Energía 12v

Cable de alimentación

Cable de Alimentación de 110v

INVERSOR DE ENERGIA 12V-110V

Regleta 110v

LLAVES DEL VEHÍCULO Y DE TAPA DE LA GASOLINA

MANTENIMIENTO PREVENTIVO:

Deberá ser realizado por los operadores y usuarios del equipo antes y después de su empleo; los equipos y accesorios de comunicaciones mientras permanezcan en los depósitos deberán ser examinados por el almacenista de comunicaciones de la unidad a intervalos regulares, con el fin de evitar averías y/o daños en los mismos por acción del tiempo y otros agentes.

Las distintas tareas que se requieren en la ejecución de este tipo de mantenimiento para cada equipo en particular, estará indicado en el manual técnico respectivo del mismo, pero en general el mantenimiento preventivo de los equipos y accesorios de comunicaciones abarcaran las siguientes actividades:

1. Inspeccionar que el equipo este completo con todos sus accesorios.

2. Instalar el equipo en un lugar apropiado para su adecuada operación.

3. Usar un paño limpio y seco para remover el polvo y la humedad de los microteléfonos, altoparlantes, antenas y partes metálicas de los equipos evitando así la corrosión y/u oxidación; así mismo emplear un cepillo pequeño para la limpieza de los conectores de los microteléfonos y altoparlantes.

4. Examinar minuciosamente todas las partes accesibles del equipo como conectores de alimentación, fusibles, conectores de antenas, etc., con el fin de tener la seguridad que al ser instalados funcionen normalmente. Es necesario tener en cuenta que al reponer un fusible se debe reemplazar por uno de las mismas características, ya que, al no usar un fusible apropiado u otro elemento en su reemplazo, puede causar serias averías y/o daños a los módulos internos de los equipos.

5. Verificar que todas las perillas estén fijadas a los ejes de control, ya que por lo general se encuentran ajustadas por medio de pequeños tornillos de sujeción, que por efecto del empleo del equipo y los movimientos terminan aflojándose y perdiéndose.

6. Inspeccionar que los estuches y bolsas de accesorios no se encuentren rotos, evitando así la perdida de elementos y accesorios.

7. Verificar que las baterías no tengan polvo, corrosión, sulfatación, y conexiones flojas, ya que le restan capacidad de operabilidad y pueden producir daños en los equipos.

8. Antes de operar el radio, el operador o usuario debe inspeccionarlo en busca de desperfectos; esto economizara tiempo de reparación y además también puede evitar una falla adicional. Generalmente las fallas de muchos equipos son causadas por los siguientes descuidos:
   a. Cables de tensión conectados incorrectamente (inversión de polaridad).

b. Clavijas gastadas, rotas o desconectadas.

c. Conectores de los cables de las antenas sueltos.

d. Conectores de audio sucios o húmedos, los cuales no permiten una adecuada conexión con los microteléfonos o altoparlantes.

Altos voltajes pueden ser necesarios en la operación de aparatos de radio, por lo tanto, los operadores, usuarios y personal de mantenimiento deben examinar primero el manual del equipo en busca de cualquier advertencia antes de operarlo. Puede ocasionar LA MUERTE EN CONTACTO si el personal de operación y mantenimiento no observa las precauciones de seguridad al respecto.

Las siguientes son las precauciones generales de seguridad en la operación y mantenimiento de los equipos:

a. Tener especial cuidado de no tocar conexiones de alta tensión o alto voltaje.
b. Evitar entrar en contacto con líneas de transmisión y antenas tipo vehicular que tengan voltaje de radiofrecuencia.

c. Cuando se desarme un equipo de radio para efectuar su reparación se debe tener la seguridad de haber desconectado la fuente de energía y que los condensadores de alto voltaje no estén puestos en corto circuito.

9. En la ejecución de las tareas de limpieza: eliminar polvo, suciedad, exceso de lubricantes y en general todo agente extraño al equipo; se deben emplear normalmente algunos de los siguientes elementos: Agua dulce, agua destilada, alcohol isopropílico, aspiradora, sopladora de aire, pinceles, cepillos, esponjas, gamuzas, estopas o trapos, limpia contactos.

10. En la acción de llevar a la posición correcta las piezas que se unen entre sí por tuercas, tornillos, pasadores, correas, flejes, etc., ajustando o ejerciendo sobre éstos una presión adecuada, se debe observar el empleo correcto de la herramienta adecuada en cada caso y no ajustar excesivamente, ya que hay riesgo de cortar el tornillo, inutilizar la rosca o dañar las piezas en ajuste.
11. En la lubricación de partes, se deben emplear sustancias grasas, aceite y otros lubricantes minerales con el fin de proteger de agentes atmosféricos los equipos y accesorios.

Si bien es cierto que los equipos de comunicaciones requieren poco empleo de lubricantes, cada vez que se haga necesario su uso, se hará evitando excesos y la aplicación de lugares que no corresponda, ya que facilita la fijación de polvo y arena.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPITULO VI

COMUNICACIONES AUDIOVISUALES

SECCIÓN A

1. COMUNICACIONES PICTÓRICAS Y AUDIOVISUALES:

Son un sistema de comunicación visual que utiliza imágenes, símbolos y elementos gráficos para transmitir ideas, emociones y mensajes. Se basan en el lenguaje visual, que puede incluir pintura, fotografía, diagramas y otros medios artísticos, y funcionan como un medio para expresar y compartir información de forma rápida, directa y, en ocasiones, universal.

a. Elementos clave:

1) Imágenes y símbolos:

Utiliza imágenes, signos e iconos para representar conceptos de manera sencilla y clara, como se ve en el diseño gráfico.

2) Lenguaje visual:

Se apoya en elementos como líneas, formas, colores y texturas para evocar emociones y transmitir mensajes.

3) Medio de expresión:

La pintura, el dibujo, la escultura, la fotografía y el cine son ejemplos de medios que utilizan elementos visuales para comunicar ideas.

4) Emisor y receptor:

El artista es el emisor que crea el mensaje a través de su obra, y el espectador es el receptor que interpreta el mensaje.

b. Características principales:

1) Directa y rápida: Transmite mensajes de manera más directa y rápida que el lenguaje verbal.

2) Potencialmente universal: Puede trascender barreras de idioma, aunque la interpretación cultural sigue siendo un factor importante.

3) Emocional y sensorial: Puede conectar directamente con las emociones del espectador a través de sus colores, formas y composiciones.

4) Permanente: Mientras la obra exista, se mantiene como un medio de comunicación silencioso y duradero
5) Generalidades: Convergencia Digital y Multimedia.

c. Las comunicaciones pictóricas y audiovisuales hoy se conocen como: Comunicaciones Multimedia o Digitales.

1) Definición Actual: Son la transmisión o el registro de información que combina múltiples formas de contenido (texto, imagen, audio y video) de manera digital.

2) Medios Actualizados: La fotografía digital, el video digital, el streaming, las videoconferencias y las plataformas de mensajería multimedia son los principales medios. La transmisión electrónica es ahora sinónimo de redes IP (Internet Protocol) de alta velocidad.

d. Fotografía y Video: La Imagen Digital

La fotografía y el video (antes fotografía móvil) han evolucionado completamente al ámbito digital, ofreciendo inmediatez y versatilidad.

1) Digitalización: Las cámaras (incluyendo las de Smartphones) capturan imágenes como datos binarios (píxeles), almacenándolas en memorias flash y permitiendo la visualización y distribución instantánea.

2) Ventajas Modernas:

a) Metadatos: Cada imagen o video registra automáticamente información crucial (ubicación GPS, hora, tipo de dispositivo).

b) Procesamiento: El software per la edición, el análisis automatizado (Ej. reconocimiento facial u óptico de caracteres) y la reproducción de copias ilimitadas sin pérdida de calidad.

c) Tecnologías Avanzadas: Se integra con la fotogrametría (creación de modelos 3D a partir de imágenes) y la visión artificial.

2. El FAX: Obsoleto y Modernizado

El sistema de FAX tradicional (analógico, sobre línea telefónica) es un medio en gran parte obsoleto para la transmisión de mapas y diagramas.

a. Sustitución: Ha sido reemplazado por el correo electrónico con archivos adjuntos (PDF, JPEG) y plataformas de intercambio de archivos en la nube (como Google Drive o Dropbox), que ofrecen mayor calidad, velocidad y seguridad en la transmisión.

b. FAX Digital (e-Fax): Su funcionalidad persiste en el ámbito legal y médico a través de servicios de FAX por Internet, que envían y reciben documentos como archivos adjuntos de correo electrónico, manteniendo la formalidad del facsímil sin necesidad de una línea de teléfono dedicada.

c. Televisión y Streaming: Transmisión Instantánea de Contenido Audiovisual la televisión ha sido transformada por la tecnología de streaming y las redes IP, llevando la transmisión de video a cualquier dispositivo.

d. Instantaneidad y Cobertura: La transmisión es ahora global y móvil. El uso de cámaras IP, drones con capacidad de transmisión en vivo (FPV/First-Person View) y satélites permite el streaming en tiempo real de situaciones tácticas a través de internet con baja latencia.

3. VENTAJAS MODERNAS:

a. Interactividad: Permite la comunicación bidireccional inmediata (Ej. videoconferencias tácticas).

b. Alta Definición: El video en 4K o superior proporciona un nivel de detalle mucho mayor para el análisis.

c. Almacenamiento en la Nube: Las grabaciones de video vigilancia o reconocimiento se almacenan de forma segura y accesible remotamente.

4. EMPLEO TÁCTICO Y ESTRATÉGICO: INTEGRACIÓN DE SISTEMAS

El uso de estos medios se centra en la fusión de datos y la inteligencia en tiempo real para lograr el Dominio de la Información.

Tabla N° 3 sensores multiespectrales

Aplicación Original (Militar/Estratégica)	Adaptación y Tecnologías Modernas
Inteligencia (Fotografía Aérea/Terrestre)	**Sensores Multi-espectrales y Satelitales** (ópticos, infrarrojos, SAR). El análisis se realiza con **Inteligencia Artificial (IA)** para detección automática de objetos, clasificación y geo-localización precisa.
Reconocimiento con TV (UAVs)	**Drones y Sistemas de Video en Red (IP)**. El video en vivo se integra directamente a **Sistemas de Información Geográfica (SIG)** para superponer datos, rutas, y posiciones del enemigo en un mapa digital interactivo.
Operaciones Psicológicas (Propaganda)	**Guerra de la Información** y **Operaciones de Influencia**. Uso de deepfakes, micro-segmentación de contenido audiovisual en redes sociales y difusión masiva a través de plataformas de video streaming para manipular narrativas.
Registros Operacionales	**"Bodycams" y Dashcams** digitales para grabación de eventos. Los registros se almacenan en bases de datos seguras y etiquetadas para auditoría (blockchain o cifrado robusto).
Entrenamiento	**Realidad Virtual (RV) y Realidad Aumentada (RA)**. Se usan videos y simulaciones inmersivas para el entrenamiento de personal, ofreciendo escenarios realistas y feedback inmediato sobre decisiones.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPITULO VII

FUNDAMENTOS Y MEDIOS DE LAS COMUNICACIONES ALÁMBRICAS

SECCIÓN A

SONIDO Y TELEFONÍA, NATURALEZA DEL SONIDO. ONDAS SONORAS. CARACTERÍSTICAS DE LAS ONDAS SONORAS. ARMÓNICOS, CARACTERÍSTICAS DEL SONIDO. FRECUENCIAS DE LAS VOCES

1. SONIDO Y TELEFONÍA:

Antes de que se inventara el teléfono, la voz humana sólo podía ser transmitida hasta donde lo permitiera la potencia de garganta del que hablaba y de la sensibilidad del oído del oyente.

Con el megáfono se conseguía llevar el sonido a distancias un poco mayores, pero sólo con la aparición del teléfono, se consiguió llevar la voz humana hasta distancias verdaderamente importantes.

2. NATURALEZA DEL SONIDO:

a. El sonido puede definirse como la sensación causada en el sistema nervioso, por la vibración de las delicadas membranas del oído.

b. La vibración de un cuerpo rígido o semirrígido, produce ondas sonoras, las cuales son transmitidas a través del aire, hasta nuestros oídos.

c. En el vacío, no es posible transmitir sonidos, porque no existe medio de comunicación. En efecto si tomamos un reloj despertador y lo colocamos debajo de una campana de vidrio, oiremos el sonido del despertador, aunque en forma atenuada. Si luego, hacemos el vacío en la campana, cuando suene el despertador, este sonido no llegará a nuestros oídos, por carecer del medio de comunicación, que en el caso anterior era el aire.

d. Así que la transmisión del sonido siempre requiere un medio. No ocurre lo mismo con la luz y la electricidad, las cuales pueden transmitirse a través del vacío. El sonido puede transmitirse a través de cualquier medio (sólido o líquido).

e. Así, puede oírse el ruido de un tren, presionando la oreja al riel. También los indios americanos gozaban de una merecida reputación, por su habilidad en descubrir la presencia de caballería, presionando la oreja al suelo.

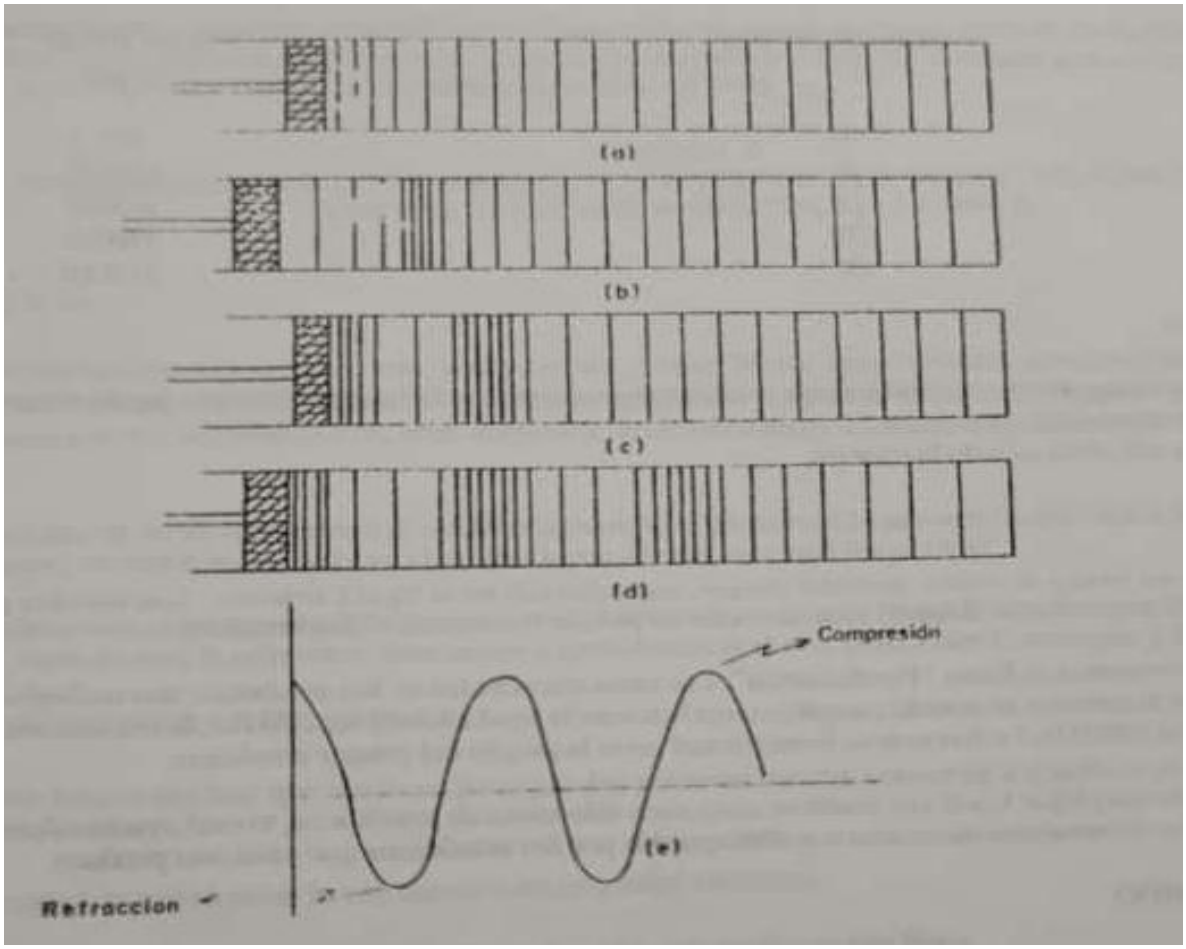
3. ONDAS SONORAS:

El movimiento de las moléculas de aire cercanas a un cuerpo que vibra, produce ondas sonoras, las cuales se dispersan en los 360° alrededor de la fuente de vibración.

Cuando un cuerpo vibra, él produce compresiones y refacciones sucesivas de moléculas de aire. La onda sonora viaja a través del aire, produciendo un movimiento de las moléculas en forma de acordeón, cuando la compresión, ellas se condensan, cuando hay la rarefacción ellas se dispersan. Así, las moléculas de aire permanecen en su lugar, pero transmiten el movimiento a las moléculas vecinas.

La figura siguiente enseña un embolo colocado al extremo de un tubo lleno de una sustancia comprensible. En la fig. las capas de moléculas están igualmente espaciadas, cuando la sustancia está en reposo. Si se empuja el émbolo, éste comprime las moléculas más cercanas. Estas capas a su vez comprimirán otras capas más alejadas del émbolo y se transmite un impulso de compresión a lo largo del tubo. Si el émbolo es sacado del tubo rápidamente, las capas de moléculas cercanas se dilatan, produciendo un impulso de rarefacción que también se propaga a través del tubo. Si el émbolo oscila hacia atrás y hacia adelante, se producirá una cadena de impulsos de compresión y rarefacción, según se muestra en la figura. En la misma forma, se produce la transmisión de ondas sonoras a través del aire u otro medio cualquiera.

En la figura representamos la compresión relativa que se produce a través del tubo, según nos índica la figura. Podemos notar que la compresión de moléculas va



de máxima condensación a cero, y de cero a máxima rarefacción, para luego volver al punto cero y de allí nuevamente al punto de máxima condensación. De tal forma que la onda sonora, semejante a la de la figura, puede representarse por medio de una curva senoidal o cosenoidal como la representa en la figura

4.- CARACTERÍSTICAS DE LAS ONDAS SONORAS

En la curva senoidal que nos representa la onda sonora, podemos distinguir los siguientes elementos:

a. CICLO

Es la colección completa de todos los valores de la onda {positivos y negativos).

b. PERIODO (T)

Es el tiempo T que se requiere para completar un ciclo,

c. FRECUENCIA (F)

Es el número de ciclos que se producen en un segundo La unidad de frecuencia es el ciclo por segundo o hertz, cuyos múltiplos más usados son:

El Kilohertz K Hz= 103 HZ

El Megahertz, M Hz= 106 HZ

d. AMPLITUD

El máximo valor ele la onda, medido desde el eje de los ceros.

f. Velocidad de la onda sonora.

Una onda sonora para ir de un lugar a otro, necesita de un tiempo definido para hacerlo. Cuando dos personas conversan, la distancia entre una y otra están corta, que el tiempo requerido para la onda hacer su requerido es prácticamente despreciable. Sin embargo, cuando la distancia es apreciable, como en un stadium, se pueden apreciar ciertas perturbaciones.

La velocidad del sonido incrementa con el crecimiento de la temperatura. Ella también dependerá del medio, por el cual será la velocidad de la onda, mientras más denso sea el medio por el cual ella viaja o se desplaza.

A continuación, se dan unos ejemplos de velocidad del sonido, en diferentes medios y a diferentes temperaturas.

MEDIO	TEMPERATURAS o C	VELOCIDAD m\seg
Aire	0	331,3
Hidrógeno	0	1286,0
Agua	15	1450,0
Aluminio	20	**5100,0**
Hierro	20	5130,0

f. Longitud de onda

La longitud de onda es la distancia entre sucesivas condensaciones o sucesivas rarefacciones. También pueden definirse como

la distancia que se cubre en un ciclo.

Esta longitud puede ser calculada usando la relación

5.- ARMÓNICOS.

La mayoría de los sonidos no tienen la forma senoidal simple, representada en la figura anterior. Los sonidos generalmente están compuestos de varios sonidos simples, cada uno con su propia frecuencia y amplitud.

La componente de más baja frecuencia se llama "Fundamental". Las otras frecuencias de los armónicos son múltiplos enteros de la frecuencia de la fundamental. Si tenemos un sonido complejo cuya frecuencia fundamental sea 500 Hz, la frecuencia del tercer armónico es 1500 Hz. la del quinto 2500 Hz. la frecuencia fundamental sería la propia del primer armónico.

Los sonidos de voz son sonidos complejos. Cada voz contiene conjuntos diferentes de armónicos, lo cual ayuda a distinguir las voces de las personas. También los instrumentos musicales son distinguidos por los armónicos que cada uno produce.

6.- CARACTERÍSTICAS DEL SONIDO

Los sonidos provocados por voces o por instrumentos, tienen tres propiedades de que lo identifican: el tono, la intensidad y la calidad o timbre.

a. El Tono

El tono está determinado por la frecuencia más alta del sonido; cuanto más alta la frecuencia tanto más alto es el tono. Así la voz de un soprano es de un tono más alto que la de un bajo.

El sonido más bajo que el oído humano puede detectar es 20 HZ y el más alto de cerca de 20.000 Hz.

b. Intensidad del Sonido.

La intensidad depende de la amplitud de vibración de la fuente, la cual determina la amplitud de la onda sonora y el oído. Si la distancia es constante y el medio uniforme, la intensidad del sonido dependerá solamente de la amplitud de la vibración de la frente sonora, La intensidad puede medirse en vatios por centímetro cuadrado. Así el sonido promedio en la calle es de 10-9 vatios/cm 2 y en una casa de habitación corriente de 10-13 vatios/cm 2.

c. Calidad o timbre del sonido

1) Esta característica es vital para cl reconocimiento de voces y sonidos.

2) El timbre de un sonido está determinado por el número de armónicos presente y por sus intensidades respectivas.

3) Ello nos permite diferenciar el sonido de un violín del de una flauta o permite a una madre diferenciar el llanto de su hijo del llanto del hijo de su vecina.

7.- FRECUENCIA DE LAS VOCES.

Este es uno de los factores más importantes en el diseño y construcción de líneas y equipos telefónicos. Los sonidos normales de voz contienen frecuencias fundamentales entre 100 y 300 Hertz. Los armónicos contendidos en estos sonidos extienden la gama de frecuencia a aproximadamente 5000 Hz. Los hombres generalmente tienen voces con frecuencias fundamentales y armónicas más bajas que las mujeres y los niños. La frecuencia fundamental es mayor cuando se canta que cuando se habla y será mayor en un soprano que en un bajo.

Debido a la amplia gama de frecuencias contenidas en instrumentos y voces, los circuitos telefónicos presentan un diseño más complicado y deben ser construidos, atendiendo a rígidas especificaciones, que lógicamente incrementan los costos.

Para la transmisión de conversaciones ordinarias se ha encontrado, que un suficiente grado de inteligibilidad es conseguido si los circuitos telefónicos se proyectan para transmitir frecuencias entre los 200 y 2700 Hz. Mediante un audiómetro se puede determinar, como el oído humano es más sensible a las frecuencias cerca a los 2000 Hz.

SECCIÓN B

PROBLEMA BÁSICO DE LA TELEFONÍA. CIRCUITO TELEFÓNICO SIMPLE. MESA DE CONMUTACIÓN.

Central Telefónica. Oficina Telefónica.

1. INTRODUCCIÓN

Después de varias experiencias tales como las de Ampere, Gauss, Weber y muchos otros, para conseguir la transmisión de señales por medio de electricidad,

en 1835 Samuel Morse, tuvo el gran mérito de ser el primero en imaginar y construir un rudimentario aparato, que vino a servir al público nueve (09) años después, con el cual realizó un enlace telegráfico entre las ciudades de Baltimore y Washington.

Luego en el año de 1850, fue lanzado al canal de la mancha el primer cable submarino, que unía a Inglaterra con Holanda. Este duró poco tiempo, siendo lanzado otro, en el mismo lugar, el cual funcionó hasta 1930.

La telefonía tuvo su origen en el teléfono experimental del profesor alemán Philip Reisz, pero este fue creado por el italiano Antonio Meucci, quien en 1854 construyó su primer prototipo, aunque no formalizó su patente por dificultades económicas, el cual más tarde fue patentado por Alexander Graham Bell, realizándose la primera conversación a gran distancia el año 1876, entre Cambrigde y Boston.

En el año 2002 Antonio Meucci fue reconocido por su contribución en el desarrollo del teléfono, cuando la cámara de representante de EE.UU. Aprobó una resolución en la que le atribuyen la patente por su trabajo en el año 1871.

2.- PROBLEMA BÁSICO DE LA TELEFONÍA

El problema básico que hay que resolver, para que dos personas puedan conversar a través de un circuito telefónico, se puede resumir en tres puntos:

a.- Necesidad de transformar la voz humana en una señal eléctrica.

b.- Transportar esa señal eléctrica de uno a otro punto, por medio de una línea.

c- Transformar la señal eléctrica, en el sitio de recepción, en sonidos audibles.

3.- CIRCUITO TELEFÓNICO SIMPLE

En la figura siguiente presentamos un circuito telefónico elemental. Una persona que desee hablar desde la estación A, accionará el generador manual, el cual envía una señal a la estación B, para hacer sonar la campana o timbre. Una persona puede recibir la llamada en B, y establecer la conversación, transmitiendo a través del transmisor (I) y recibiendo por el receptor (R).

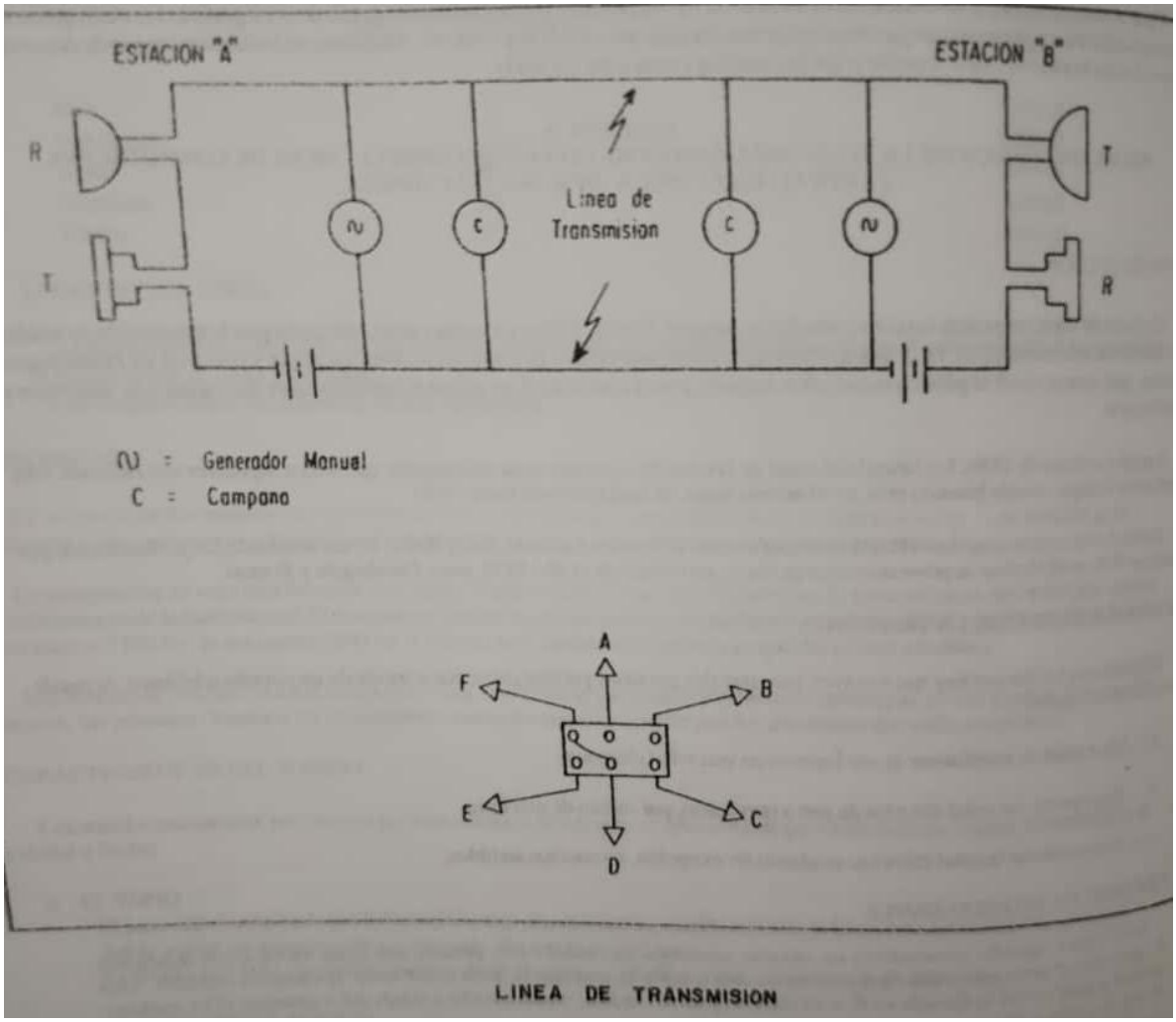
4.- MESA DE CONMUTACIÓN

Un sistema telefónico puede estar constituido por cientos o miles de teléfonos. Para intercomunicarlos a todos entre sí directamente, se requeriría de un par telefónico por cada teléfono. De tal forma que a cada estación llegarían cientos o miles de pares, tanto como teléfonos tuviere el sistema. Esto haría prácticamente imposible su funcionamiento. La solución adoptada es muy simple, y consiste en un tablero a donde llegan los pares telefónicos que enlazan cada una de las estaciones a este centro de conmutación.

En la figura representamos un sistema de seis teléfonos. Todas las líneas llegan al tablero de conmutación, donde se hacen las conexiones solicitadas por los abonados. En el ejemplo de la figura, se encuentran ligadas las estaciones D y F. Las conexiones pueden hacerse por medio de operadores o en forma automática. El panel se presenta en forma de mesa y se llama mesa de conmutación.

5.- CENTRAL TELEFÓNICA

Las oficinas donde se encuentran las mesas de conmutación y otros equipos necesarios, se llama oficina central telefónica. Los requerimientos del servicio determinarán la capacidad de la mesa de conmutación y el tráfico (número de conexiones en un determinado tiempo) determina el número de operadores que atienden las mesas.



6. SISTEMA TELEFÓNICO

Un sistema telefónico consiste de un número de estaciones conectadas por líneas a la oficina central, para que cualquier teléfono puedan ser conectados para establecer una conversación. El sistema puede tener cientos o miles de teléfonos y una o varias centrales. Un sistema incluye:

a.- Las estaciones individuales (teléfonos).

b.-Equipo de planta externa para conectar cada teléfono a la central y para interconectar diversas centrales.

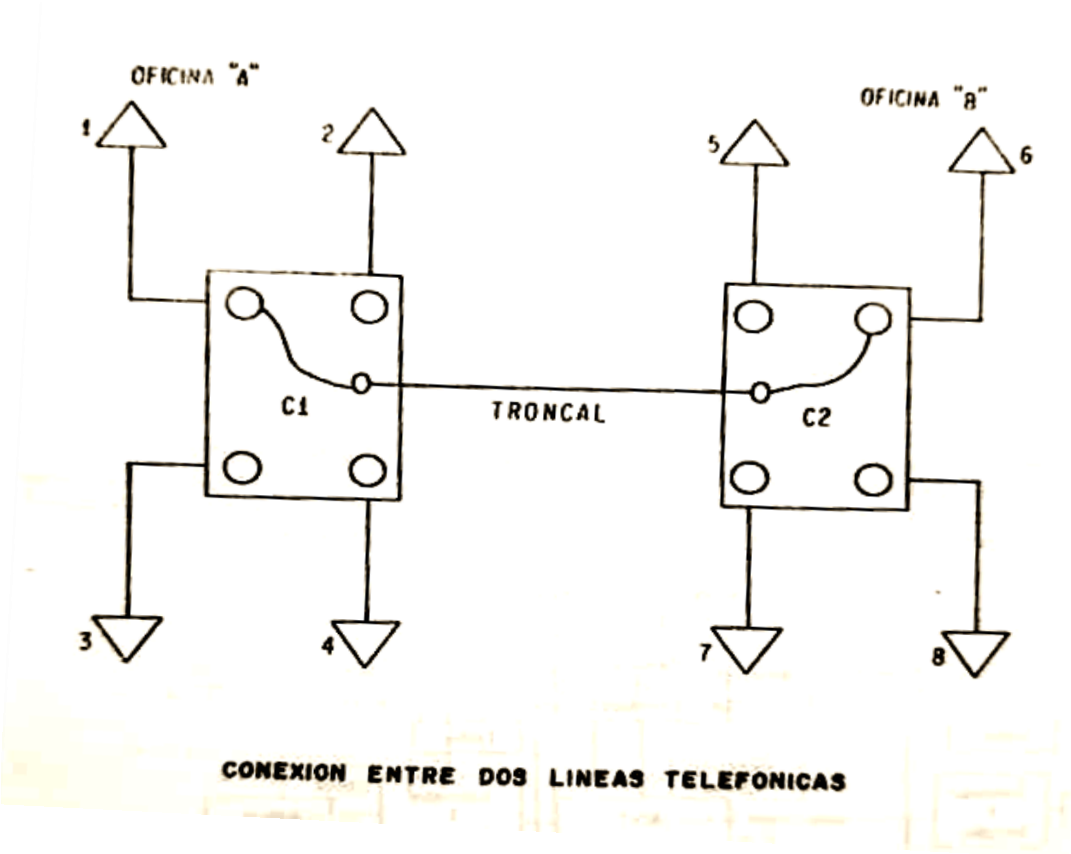
c.- Equipo de la oficina central para conectar las estaciones y las mesas operadoras.

7.- OFICINA TELEFÓNICA

Un sistema telefónico el cual provee las comunicaciones dentro de un área determinada, se llama oficina telefónica. Ella puede tener una o más centrales, dependiendo de las necesidades de tráfico.

La figura siguiente representaría una oficina telefónica.

La conexión entre estaciones telefónicas, servidas por diferentes oficinas telefónicas, se establece a través de líneas llamadas "troncales".



CONEXION ENTRE DOS LINEAS TELEFONICAS

SECCIÓN C

CLASIFICACIÓN DE LOS SISTEMAS TELEFÓNICOS. SISTEMA TELEFÓNICO MANUAL. SISTEMA DE BATERÍA LOCAL Y BATERÍA COMÚN. SISTEMA TELEFÓNICO AUTOMÁTICO. COMPARACIÓN DE LOS SISTEMAS TELEFÓNICOS.

1. CLASIFICACIÓN DE LOS SISTEMAS TELEFÓNICOS

Los sistemas telefónicos son clasificados de acuerdo al método de conmutación usado, en sistemas manuales y sistemas automáticos. Como lo indica su nombre, en los sistemas manuales la conexión entre estaciones se hace manualmente, por medio de operadores, y en el sistema automático por medio de mecanismos electromecánicos, sin el servicio de operadores.

2. SISTEMA TELEFÓNICO MANUAL

La mayoría de los sistemas telefónicos militares son sistemas manuales. Ellos pueden clasificarse de acuerdo con las fuentes de energía eléctrica suministrada a los transmisores, en sistemas de batería local y sistemas de batería común.

a. Sistema de batería local

En estos sistemas, las fuentes de energía eléctrica para los transmisores y aparatos de señalización son incluidos en los equipos telefónicos, localizados en cada estación. El término local significa que la fuente de energía eléctrica,

es una parte de la estación telefónica. Una batería local suministra la corriente para el circuito transmisor y un generador de mano o magneto

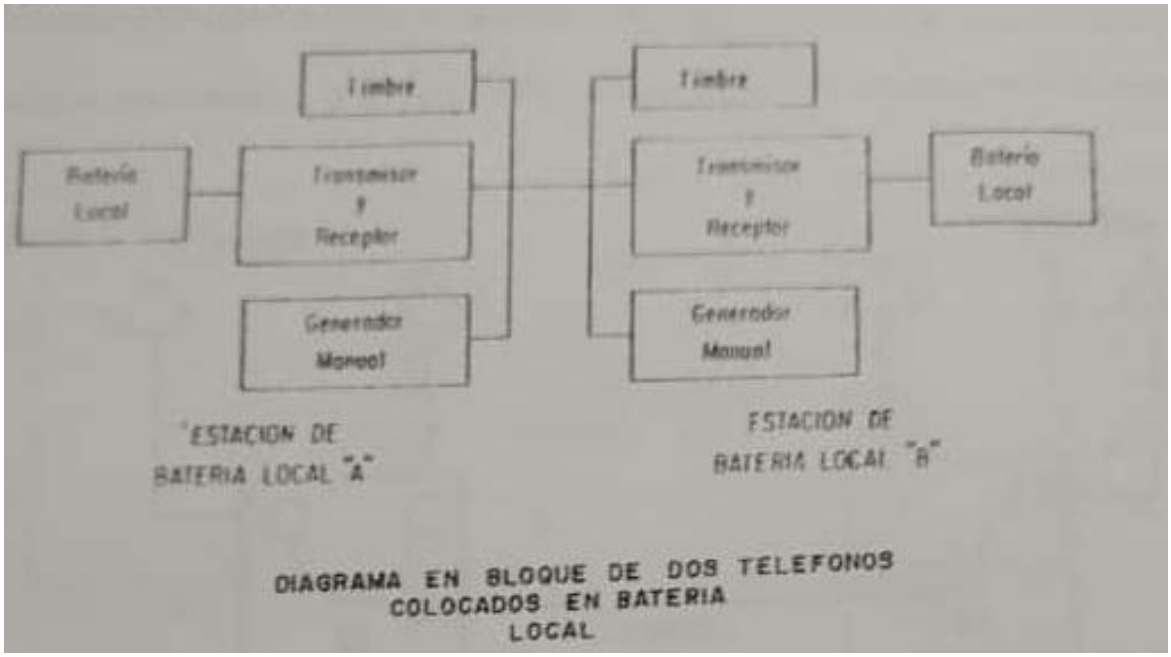
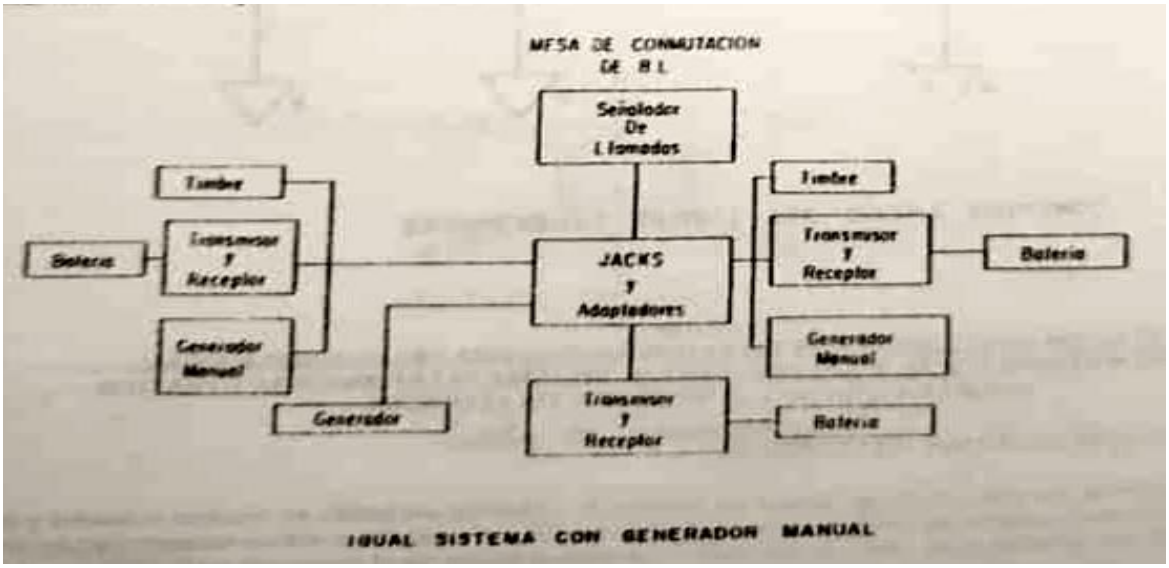


DIAGRAMA EN BLOQUE DE DOS TELEFONOS COLOCADOS EN BATERIA LOCAL

suministra la corriente para, señalización. El diagrama en bloque de la Figura muestra como dos teléfonos de batería local son conectados directamente uno al otro.

Notamos que además de las estaciones, la mesa de conmutación también está dotada de su batería local. También notamos, que en el tablero de conmutación hay una señal de llamada, la cual consiste de una persiana la



IGUAL SISTEMA CON GENERADOR MANUAL

cual cae y llama la atención del operador cuando el usuario de una estación de B.L, envía señales con su generador manual. Generalmente cuando la persiana cae, una señal audible se producirá en la mesa de conmutación.

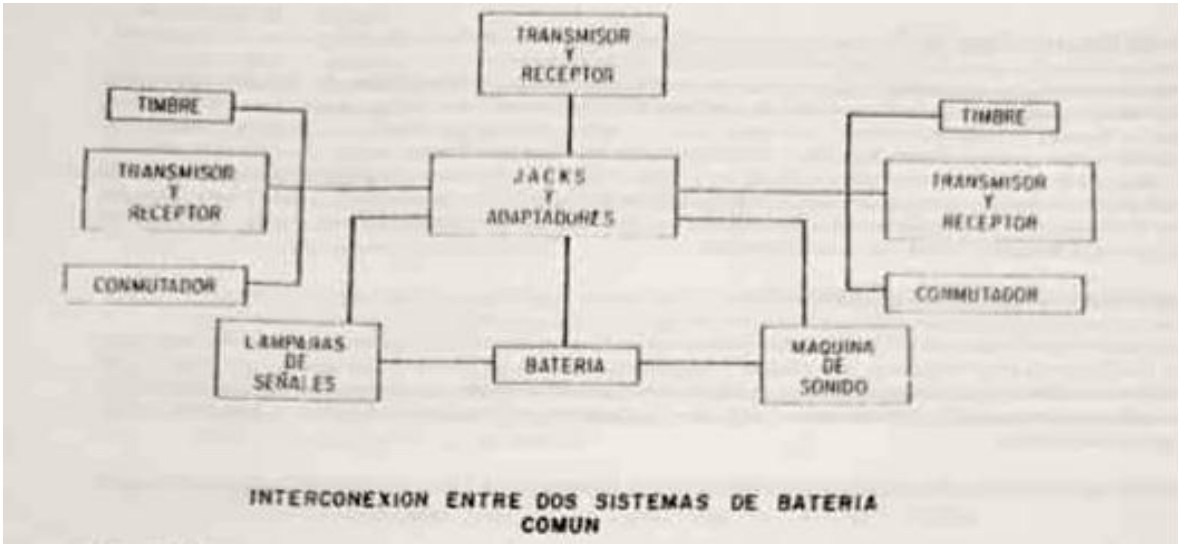
b. Sistema de batería común

En este sistema, las fuentes de energía eléctrica son colocadas en la oficina central; o sea, que todas las estaciones obtienen la energía para transmisión y señalización de una fuente común.

Una fuente primaria de energía tal como un generador y una batería de acumuladores en la oficina central, suministran la corriente para los transmisores y también la corriente para las lámparas de señales de la mesa de conmutación, una máquina de sonido suministra la corriente para los timbres de todas las estaciones telefónicas.

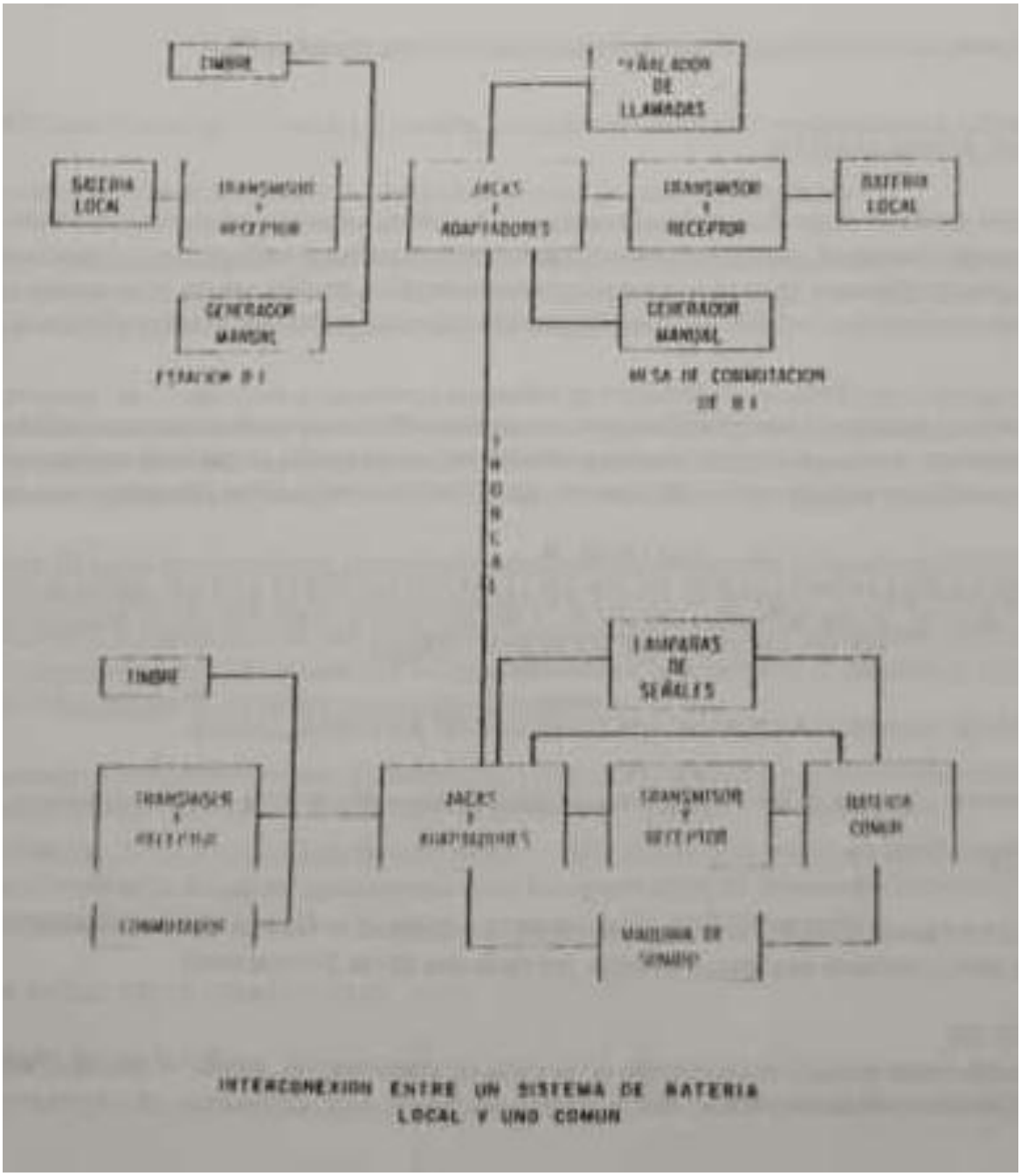
La figura muestra dos teléfonos de batería común conectados a una mesa de conmutación, también de batería común.

En esta figura vemos que no hay baterías en los equipos telefónicos y que el medio de señalización de la mesa operadora está compuesta por lámparas las



INTERCONEXION ENTRE DOS SISTEMAS DE BATERIA COMUN

cuales encienden cuando se levanta el receptor de cualquiera de los equipos telefónicos de las estaciones. No existe, por tanto, la ventanilla o persiana del



INTERCONEXION ENTRE UN SISTEMA DE BATERIA LOCAL Y UNO COMUN

sistema de batería local.

Un sistema de batería local puede ser interconectado con un sistema de batería común, y permitir así una conversación desde una estación conectada a una central

de batería local, con otra conectada a una central de batería común, como se muestra en la figura

3. SISTEMA TELEFÓNICO AUTOMÁTICO.

El sistema telefónico automático es aquel en que las conexiones entre teléfonos se hacen, sin intervención de operadores, por medio de un mecanismo electromecánico. Este mecanismo se controla mediante el dial o disco, adicionado al equipo telefónico de la estación, desde donde se hace la llamada Al operar el dial se envían impulsos a la central, por medio de la línea. Allí los pulsos controlan el equipo de conmutación el cual automáticamente hace interconexión entre las dos estaciones. Por medios electromecánicos, todas las operaciones efectuadas por el operador, en una central manual, son realizadas automáticamente en una central automática: conecta las líneas de las estaciones que llaman con las de las estaciones llamadas; determina si la línea está ocupada; y si no lo está, alerta por medio de un timbre al teléfono llamado; transmite una señal al teléfono que está llamando si el llamado está ocupado; desconecta las dos líneas (el que llama y el llamado), cuando los usuarios cuelgan.

4. COMPARACIÓN DE LOS SISTEMAS TELEFÓNICOS

a. Los sistemas telefónicos usados por el Ejercito deben proveer un buen servicio telefónico, en muchos tipos de condiciones operativas. Cada sistema tiene ventajas y desventajas, y bajo ciertas condiciones provee mejor servicio que otros. De allí que cada sistema telefónico tenga un importante lugar en las comunicaciones militares. En general los sistemas automáticos son menos usados que los manuales para operaciones móviles y usualmente son instalados solamente en dependencias que funciones permanentemente.

b.- Los sistemas telefónicos militares de campaña, generalmente son un sistema manual. Ellos pueden ser de batería local o batería común.

c- Un sistema militar de campaña, de batería local permite instalar en forma rápida, el alambre aislado o cable para sus líneas y usa equipos fuertes y portátiles en su central.

d- El sistema telefónico manual de batería común, es usado más frecuentemente para servir un gran número de usuarios localizados en un área pequeña. Ella tiene numerosos refinamientos no encontrados en el simple sistema de batería local, el cual hace posible y más eficiente y rápido manejo de llamadas. Debido a estos refinamientos, una central con batería común, requiere más tiempo para su instalación y mayor atención en su mantenimiento.

Los sistemas de baterías común son utilizados en el Ejército en los cuarteles e instalaciones fijas.

5. SISTEMAS TELEFÓNICOS AUTOMÁTICOS.

Son también de batería común, mediante el uso de conmutación automática, elimina los errores inherentes a la condición humana, producidos en las mesas de conmutación manual. Una central automática envuelve un cableado intrincado y un equipo muy complejo. Su instalación requiere mucho tiempo (meses) y es costosa; su mantenimiento también resulta costoso, pero cuando ella recibe un mantenimiento adecuado, provee un manejo más rápido y seguro del pesado tráfico telefónico, (en comparación con los sistemas de conmutación manual).

Para proveer mayor flexibilidad para operaciones militares, prácticamente todas las mesas de conmutación de batería común son diseñadas para permitir

conexiones con mesas de conmutación y teléfono de batería loca. Las mesas de conmutación de batería local más grandes, permiten las conexiones con las mesas de conmutación de batería común, tanto manuales como automáticas.

SECCIÓN D

CIRCUITOS DE UNA MESA DE CONMUTACIÓN DE UN SISTEMA DE BATERÍA LOCAL. OPERACIÓN DE UNA MESA DE CONMUTACIÓN. FUNCIÓN DE LOS JACK. CIRCUITOS DE UNA MESA DE CONMUTACIÓN DE UN SISTEMA DE BATERÍA COMÚN.

1. CIRCUÍTOS DE UNA MESA DE CONMUTACIÓN DE UN SISTEMA DE BATERÍA LOCAL.

Estos pueden ser clasificados en: circuitos de línea, circuitos troncales, circuitos de cordón y circuitos comunes.

a. Circuitos De Línea

La línea de cada estación telefónica es conectada a un circuito de línea individual de la mesa de conmutación. Así, una mesa con 20 circuitos de línea, tiene conectada una línea telefónica por cada una de las 20 estaciones.

b. Circuitos Troncales

El circuito troncal, o simplemente troncal, es un circuito de la mesa de conmutación, similar al circuito de línea. Él está conectado a la tronca de otra mesa de conmutación.

c- Circuitos de Cordón

Son circuitos usados en interconectar dos circuitos de línea, dos circuitos troncales o una línea y una troncal. El número de circuitos de cordón de una mesa de conmutación depende del tráfico telefónico que ella maneja. El tráfico es determinado por el número de llamadas telefónicas que se hacen de las estaciones telefónicas servidas por la mesa de conmutación y el promedio de duración de estas llamadas. Las mesas de conmutación generalmente tienen muchos menos circuitos de cordón que circuitos de línea, dependiendo del tipo de mesa.

d. Circuitos Comunes

Son circuitos usados con los circuitos de línea o con los circuitos de cordón o con ambos a la vez. Los principales circuitos comunes son cuatro:

1) El circuito telefónico del operador, que permite a éste hablar con cualquiera de las estaciones. Este circuito puede ser conectado, por medio de un conmutador, a cualquiera de los circuitos de cordón, luego él es común a todos estos circuitos.

2) El circuito de llamada, el cual permito al operador alertar por medio de una señal (timbre) a la estación llamada. Al igual que el circuito telefónico del operador, él puede ser conectado a cualquiera de los circuitos de cordón, mediante la operación de un conmutador.

3) El circuito de supervisión, el cual permite, a la estación que está llamando, informar al operador cuando la conversación ha terminado. Él también es común a todos los circuitos de cordón.

4) El circuito de alarma nocturna, el cual hace que una campana o timbre suene cuando se hace una llamada y de esta manera alertar al operador. Este circuito generalmente se usa cuando el tráfico es muy ligero y el operador no está atendiendo permanentemente.

2. OPERACIÓN DE UNA MESA DE CONMUTACIÓN DE BATERÍA LOCAL.

La operación de una mesa de conmutación para completar una llamada telefónica entre dos estaciones, es explicada a continuación;

Esta mesa tiene seis (06) líneas telefónicas y tres (03) circuito de cordón. Todos los circuitos están señalados en el gráfico, en forma de bloques. Supongamos que una persona de la estación A, desea llamar a otra persona en la estación D.

a. La persona en A gira el generador de mano del teléfono. Este provee una señal de llamada de 20 Hz, la cual va, a través de la línea, hasta la mesa de conmutación. Esta señal opera el circuito de línea y hace que la persiana indicadora caiga. Esta es una indicación visual para el operador de que la estación A está llamando.

b. Cuando la persiana cae, el operador selecciona el adaptador de respuesta de uno de los tres (03) circuitos de cordón y lo inserta en el circuito de Jack de la estación A y coloca la persiana en su posición original. El operador acciona luego el conmutador del circuito de cordón seleccionado, en la posición de escucha (hacia arrite). Este conecta el circuito telefónico del operador al circuito de cordón y permite a éste hablar con la estación que hace la llamada y preguntar por el número del teléfono llamado.

c. Luego el operador toma el adaptador de llamada del mismo circuito de cordón utilizado para recibir la llamada de A, y lo inserta luego en el circuito de Jack de la estación llamada (D). luego, el operador acciona el conmutador a la posición de llamada (hacia abajo). Este conecta el circuito llamado circuito de cordón, luego el operador gira la manivela del generador de la mesa y proporciona una señal, a través de la línea, que alerta a la persona en la estación D. Luego el operador acciona el conmutador a la posición de escucha y espera que D conteste.

d. Cuando D contesta, el operador restaura el conmutador a la posición normal y la conexión queda establecida. Cuando este termine, cualquiera de las personas en A o D, gira la manivela del generador de su teléfono.

Esto provee una señal de 20 Hz a través de la línea telefónica y del circuito del cordón al circuito de supervisión, ocasionando la caída de la persiana o ventanilla, lo que indica al operador que la conversación ha terminado. El operador procede a remover los adaptadores de respuesta y llamada de los Jacta y restaura la persiana en su posición normal.

3. LOS JACK DE LA MESA LE CONMUTACIÓN

a- Función del Jack

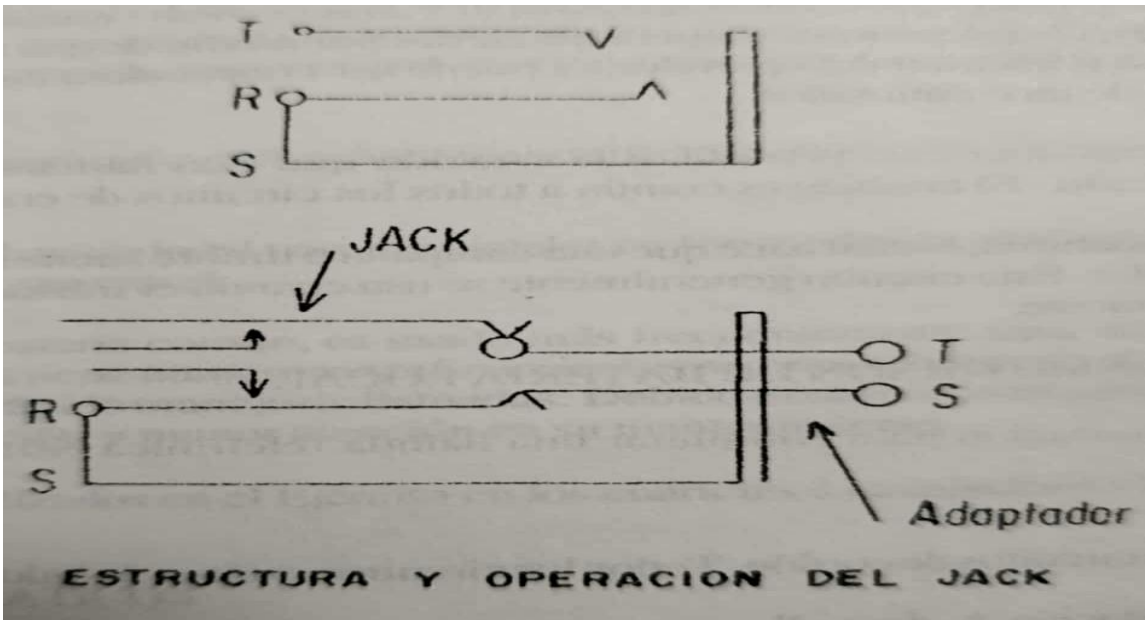
El Jack es el conector de conmutación para el circuito de línea. Cada circuito de línea es conectado a un Jack, montado en el tablero de la mesa de conmutación. El Jack está diseñado para ser usado con el adaptador o clavija del circuito de cordón; juntos forman el conector.

b. Estructura y Operación del Jack

La figura muestra un Jack de un sistema de batería local, representado por su símbolo.

El Jack tiene dos muelles, el muelle de punta y el muelle de timbre. Cada muelle opera un contacto y la manga provee un tercer contacto. Los nombres de punta, timbre y manga, son los mismos que tienen las partes de los adaptadores, con los cuales los elementos del Jack hacen contacto cuando el adaptador es insertado en el Jack.

Los Jack de batería local requieren solo dos puntos de contacto, el de punta y el de timbre; los contactos de timbre y el de manga generalmente se dejan conectados permanentemente.



ESTRUCTURA Y OPERACION DEL JACK

Cuando el adaptador es insertado en el Jack, los muelles son apartados de su posición normal y se abren los contactos, tal como indica la fig.

4. FUNCIONAMIENTO DE LA MESA DE CONMUTACIÓN DE BATERÍA COMÚN.

En general el funcionamiento de la mesa de conmutación de un sistema de batería común es bastante parecido al de una mesa de un sistema de batería local, por lo tanto, no haremos un estudio especial para ese sistema A continuación se hace un análisis de los circuitos de señalización del sistema de batería común, los cuales se difieren bastante de los análogos en el sistema de balería local.

5. CIRCUITOS DE SEÑALIZACIÓN EN UN SISTEMA DE BATERÍA COMÚN

a- Circuito de línea con lámparas en serie.

El circuito de línea debe proveer, además de la conexión entre la estación y la mesa de conmutación, un sistema de señalización para avisar al operador cuando llega una llamada a la mesa o cuando ésta ha terminado. Esta señal se establece por medios de unas lámparas en serie el circuito telefónico. Cuando el micro teléfono es retirado del gancho, unos contactos se cierran automáticamente, completando un circuito en serie, que una la batería comunal circuito de la lámpara. Esta se enciende, indicando al operador que una estación desea hacer una llamada. Cuando el operador hace le contacto, insertando a Jack correspondiente, se abre el circuito de la lámpara, la cual se apaga.

b- Señales de Supervisión

El término supervisión puede considerarse como lodo aquello que el operador debe realizar, entre la señal original de 3a estación que llama y la restauración de la mesa de conmutación a su condición original. Para que el operador haga las operaciones necesarias para el momento indicado, se requiere que éste sepa cuando un usuario desea hacer una llamada, si el

teléfono llamado ha contestado, sr un usuario desea hablar con el operador y cuando cualquiera de los abonados tiene su teléfono descolgado.

Las lámparas de línea, las cuales informan al operador de una llamada, se apagan tan pronto como el adaptador es conectado por el operador. En este instante, un equipo adicional de señales, llamadas lámparas supervisoras entran en servicio.

Estas lámparas señalan al operador cuando cualquiera de las personas conectadas, coloca su receptor en el gancho o cuando la persona llamada levanta el receptor para contestar. Cuando las personas tienen descolgados su micro teléfono, ¡as lámparas asociadas a sus líneas permanecen apagadas, al terminar la conversación y colgar, estas luces vuelven a encenderse, informando así al operador que puede retirar los adaptadores, o sea deshacer la conexión.

c- Circuitos Auxiliares

1) Lámpara piloto:

debido a que el operador puede estar desatento, y puede no notar la señal de llamada instantáneamente, para llevar con mayor seguridad la señal de llamada al operador, un circuito de lámpara piloto es incluido en la mesa de conmutación. La lámpara piloto es mucho mayor que las lámparas de línea y ella está situada estratégicamente en el panel frontal de la mesa operadora.

2) Supervisor piloto:

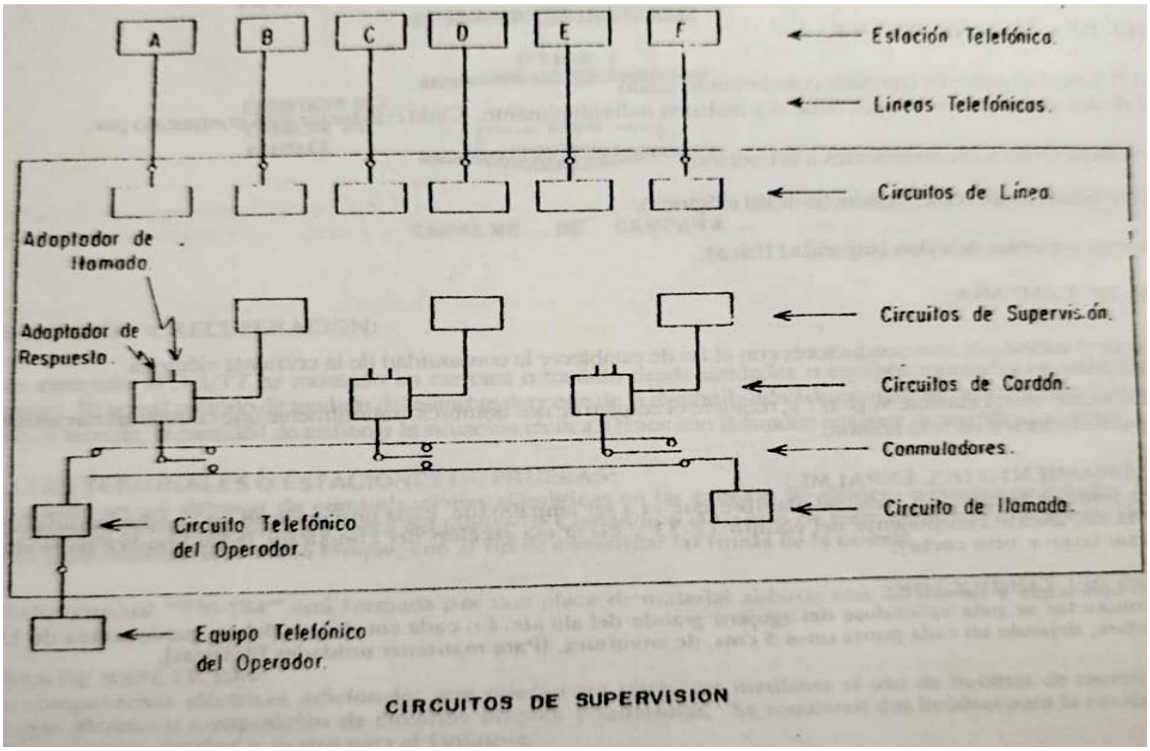
Este circuito está asociado con las lámparas supervisoras, de fa misma manera como la lámpara piloto lo está con las lámparas de línea. AI igual que la lámpara

piloto este circuito es usado para dar al operador una señal adicional, durante períodos en que él puede no notar las lámparas supervisoras. La señal usada en el circuito supervisor piloto es también una lámpara y ella está situada cerca de la lámpara de línea piloto.

3) Alarma nocturna

Esta es usada para dotar al operador con una señal audible, en conjunción con el piloto de línea y el piloto de supervisión. Este circuito es usado para atraer la atención del operador, durante intervalos cuando él puede estar fuera de su posición en ia mesa de conmutación, pero suficientemente cerca para oír la campana o timbre. Esta señal puede ser mantenida fuera de su posición en la mesa de conmutación, pero suficiente-mente cerca para oír la campana o timbre. Esta señal puede ser mantenida fuera de operación, mediante un conmutador.

4) Circuito conmutador del generador: Este es un conmutador que permite el cambio rápido del generador de máquina para el generador de mano,



CIRCUITOS DE SUPERVISION

el cual puede ser utilizado en los sistemas de baterías común en casos de emergencia.

5) Circuito de corte de batería:

En muchos casos no es necesario, operar una mesa de conmutación el día entero, especialmente en el caso de pequeñas centrales. En tales casos existe un conmutador que desconecta la batería, cuando la mesa no está en uso.

6) Circuito de alarma de fusible:

Este es usado para informar al operador de la mesa de conmutación cuando se ha quemado un fusible. El consiste de una lámpara y un timbre. El operador puede desconectar el timbre de alarma por medio de un conmutador. La lámpara permanece encendida hasta que el problema es corregido y un nuevo fusible es colocado.

SECCIÓN E

MEDIOS ALÁMBRICOS DE CAMPAÑA

1. GENERALIDADES:

Los medios alámbricos, son aquellos que necesitan una conexión física a los equipos, mediante conductores metálicos de distintos tipos. Su empico comprende el uso de: Alambre, Equipos de tendido y recuperación, teléfonos, centrales y demás equinos complementarios.

2. CARACTERÍSTICAS GENERALES DE TODO ALAMBRE DE CAMPANA:

a. La flexibilidad en los alambres de campana se consigue mediante la flexibilidad de los elementos que componen ese alambre en particular

b. Resistencia a la tracción se consigue con el empleo de filásticas de acero.

c. Buena conductibilidad se consigue mediante el empleo de filásticas de cobre.

d. Aislamiento contra agentes exteriores se consigue mediante el uso de capas de aisladores tales como: Plásticos., goma, nylon, etc

3. ALAMBRE DE CAMPAÑA WD-1/TT:

El WD-1/TT es el alambre de campaña comúnmente usado.

Consiste de dos conductores torcidos entre sí y aislados individualmente. Cada conductor está compuesto por:

a. Tres filásticas de acero (resistentes a la tracción).

b. Cuatro filásticas de cobre (conductibilidad eléctrica)

c. Una capa o camisa de nylon (seguridad física).

4. EMPALME DE CAMPANA:

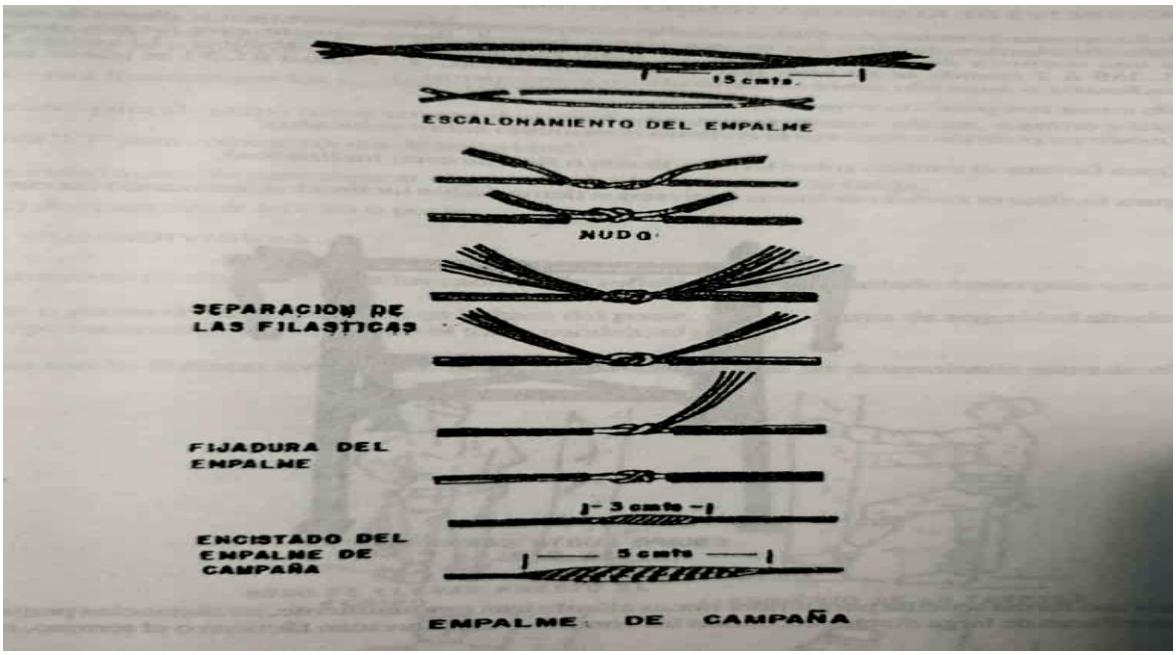
Empalmar es el método de unir conductores con el fin de establecer la continuidad de la corriente eléctrica.

El empalme usado con el alambre WD-l /TT, requiere el empleo de dos hombres, naturalmente que cuando las circunstancias la requieran se puede reducir a un solo hombre.

a. Escalonamiento del empalme:

Cada hombre prepara un lado del alambre que va a ser empalmado, cada uno mide en un conductor una longitud igual a la del alicate componente del equipo TE-33 y corta esa sección de conductor (cada hombre tiene ahora un conductor largo y otro corto).

b. Pelado del conductor:



El conductor se pela valiéndose del agujero grande del alicate. En cada conductor deben quedar cerca de 15 cms. de peladura, dejando en cada punta unos 5 cms. de envoltura. (Para mantener unidades filásticas).

5. EQUIPOS DE TENDIDO Y RECUPERACIÓN:

Es alambre de campana WD-l/TT es montado en carretes o tendido desde unidades o equipos montados en vehículos o transportados a mano. El actual método de tendido del alambre depende de la disponibilidad de equipo, las condiciones de las vías de comunicaciones y terreno, la cantidad de tráfico y la situación táctica. (Estos son llamados equipos de tendido de líneas).

a. Regletas terminales o estaciones de pruebas:

Son usadas en los sistemas de comunicaciones alámbricas en las cabezas de alambre o puntos de prueba. Una regleta termina siempre se colocará cerca del puesto de Comando o el Centro de mensaje de manera que las líneas entrantes sean reunidas en un solo bloque, con el fin de consolidar las líneas de la central.

La regleta terminal "TM-184" está formada por una placa de material aislante con 28 bornes y capacidad de 7 líneas.

b. Bobinas de repetición:

Son componentes eléctricos adicionales que pueden ser obtenidas mediante el uso de bobinas de repetición para mayor alcance y composición de circuitos simplex y fantasmas. Se requieren dos bobinas para la construcción de un circuito simplex y cuatro para el fantasma.

La bobina de repetición "C-161" es una caja metálica con un transformador de audio en una relación (1:1), provista de* cinco terminales del tipo tornillo para las conexiones necesarias.

6. EQUIPOS PORTA CARRETES DE RECOGER Y TENDER ALAMBRE:

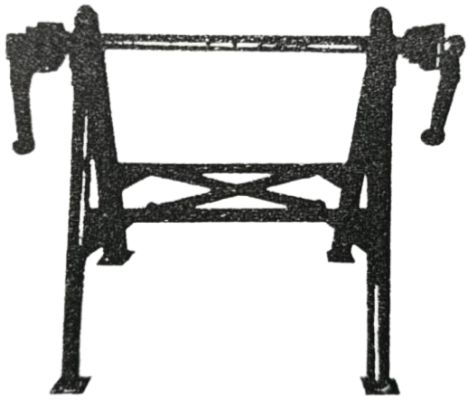
Porta carretes RL-31, es una armazón portátil o caballete, de peso relativamente ligero, diseñado para facilitar la recolección y tendido de alambre, de campo o en pares en forma manual. Lleva cojinete para recibir el eje de acero, el cual está provisto de una manivela desmontable, tiene un freno manual sujeto al caballete. El equipo RL-31 puede recibir un carrete RL-159 y, cuando se tienden las líneas telegráficas, el equipo RL-31 se puede operar desde el suelo en posición estacionaria o montado sobre un vehículo en movimiento.

El equipo RL-31 puede tomar tres posiciones que son:

a. Como caballete (usado en posición estacionaria en tierra o montado sobre vehículo).

b. Como carretilla (para facilitar el tendido sobre terrenos llanos o ligeramente inclinados).

c. Como parihuela (para facilitar el tendido de líneas en terrenos demasiados inclinados, utilizando las correas de transporte).

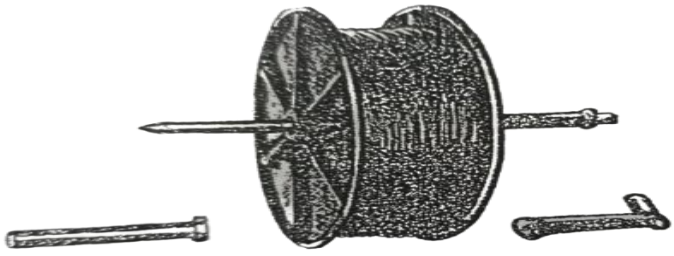


EQUIPO PORTA CARRETE DE CABLE

7. EJE RL-27:

Este equipo proporciona una forma sencilla para tender líneas alámbricas manualmente, en distancias pequeñas de líneas locales. Se puede utilizar para tender líneas de larga distancia cuando las condiciones, bien sean tácticas o el terreno, no permitan el empleo de otro equipo.

El eje consiste de una barra de acero de 60 cms. de largo, con dos manubrios estriados, uno de los cuales está permanentemente fijo a la barra; el otro manubrio se puede desmontar y es así como permite la colocación de un carrete RL-159 en



EJE RL - 27

el eje de acero. El eje está provisto de cojinetes de rodillo que permiten libre movimiento del mango. Este porta-carrete requiere un mínimo de

dos hombres, uno de cada lado para tender o recoger el alambre (ver dibujo).32.-

8. TÉCNICA PARA TREPAR POSTES:

Un correcto mantenimiento y servicio de las líneas de campaña, es una misión fundamental de comunicaciones, la cual consume esfuerzo y tiempo por parte de todo el personal de comunicaciones, cuando se hacen instalaciones de líneas aéreas, la misión es más fácil de cumplir cuando se emplea el equipo para trepar postes.

El equipo de trepar está formado por los siguientes elementos:

a. Cinturón de cuero para el cuerpo (tiene compartimientos para destornillador, alicate, martillo y teipe).

b. Dos aros forma "D" para colocar correa de seguridad,

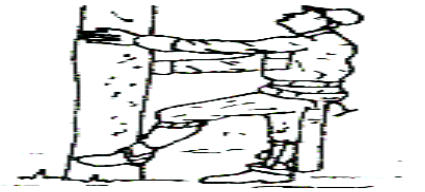
c. Correa de seguridad ajustable para abrazar el poste o el árbol y reducir la fatiga. d.- Trepadoras (2) dos para trepar árboles o postes.

9. AJUSTE PARA EL USO INDIVIDUAL:

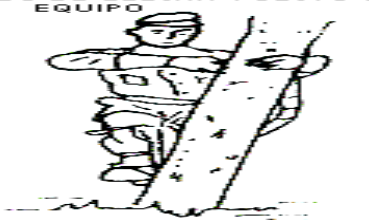
a. El cinturón de cuero es usado encima de las caderas, lo suficientemente ajustado como para que no exista deslizamiento.

b. clave tres punías o garras de las trepadoras en la base del poste-, pase la correa de seguridad alrededor de éste y asegúrela. Descanse el cuerpo hacia atrás manteniendo el torso paralelo al poste.

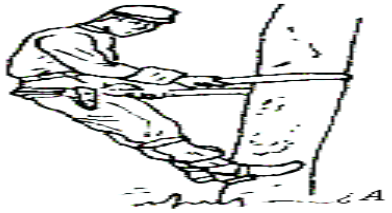
MODO DE LLEVAR PUESTO EL EQUIPO



COMIENZO DE LA TREPADA



TRANSFERENCIA DE LA CUERDA DE TRABAJO



POSICIÓN DE TRABAJO

c. Las trepadoras son dé distintas longitudes. La medida correcta debe ser determinada antes de efectuar algún trabajo.

10. MANTENIMIENTO DE LAS TREPADORAS.

a. Inspeccionarla cuidadosamente antes de emplearla, para percatarse de si está defectuosa, sustituirla si lo estuviese.

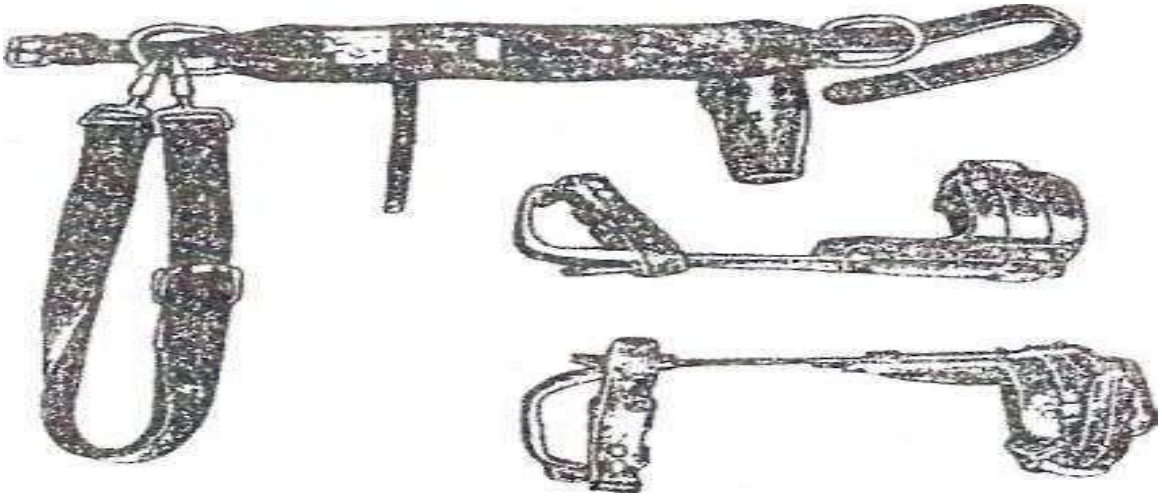
b. Las garras de las trepadoras deben mantenerse siempre libres de moho y afiladas.

c. Las partes de cuero se deben mantener siempre limpias y suaves (se usa jabón natural para su limpieza).

d. Las trepadoras no deben estar en el mismo compartimiento con las correas ya que pueden dañarse.

11. AMARRE DEL ALAMBRE DE CAMPAÑA:

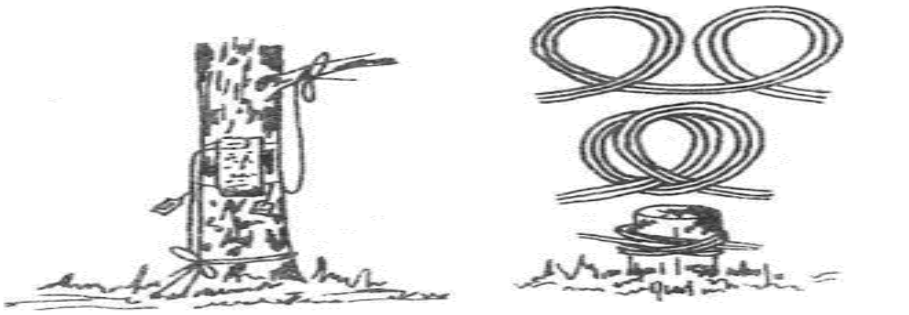
Los amarres o ataduras del alambre de campaña WD-1/TT son usados para sostener el alambre en su lugar apropiado y aliviar la tensión de línea sobre los puntos terminales del equipo. El alambre deberá asegurarse por una atadura a un árbol, postes u otros soportes, antes de conectarse a un equipo o bornes, las líneas deberán atarse cada 100 metros o menos si así se requiere.



a. Lazo escurridor:

Cuando el alambre está atado a un soporte que quede por encima del equipo por conectar, debe utilizarse este tipo de lazo (Ver dibujo 40-A) con el fin de evitar el escurrimiento del agua sobre el equipo.

b. Nudo de ballestrinque o de doble cotes:



A
LAZO ESCURRIDOR

B
NUDO DE BALLESTRINQUE

AMARRES DEL ALAMBRE DE CAMPAÑA

Para hacer esta atadura, haga dos lazos al alambre, coloque el lazo a la derecha sobre el lazo de la izquierda sin voltearlo. Luego coloque ambos lazos sobre el objeto al cual se va a atar y apriételo.

c. Atadura de nudo y lazo.

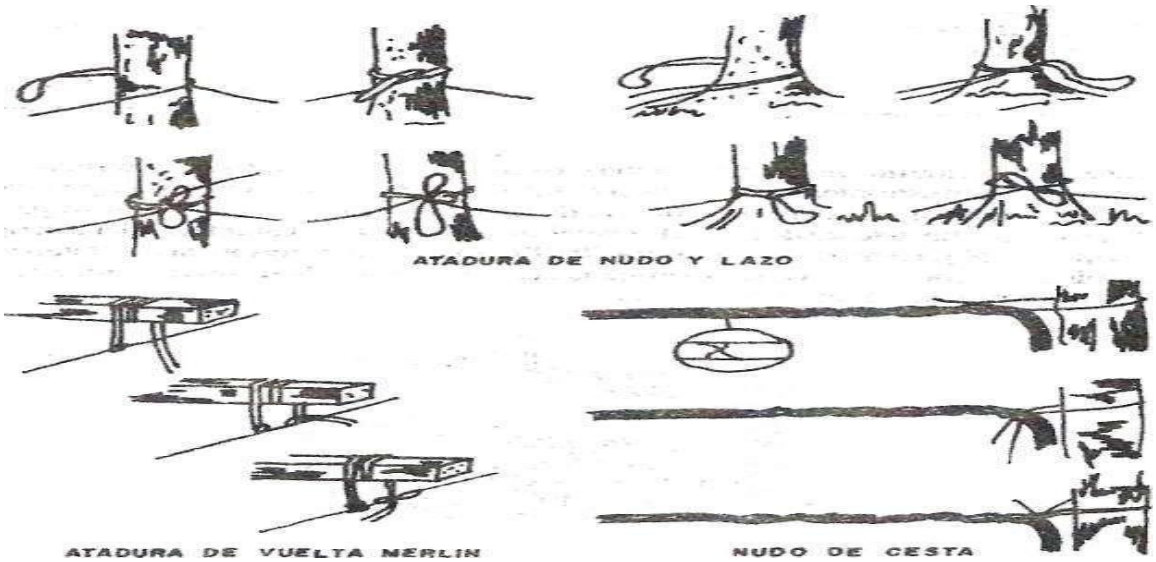
Primero, el frente del objeto del lado del cual se va a tender la línea. Dejar el alambre flojo para hacer un seno que dé la vuelta al objeto y para un virtual nudo durante un recorrido de 60 metros de largo. Si durante la hechura del amarre, el mayor esfuerzo se ejerce en la parte fija, colocar el seno alrededor del objeto en dirección del cabo de labor y continuado hasta el frente en la parte que va hacia la parte fija. Pasar el seno por debajo y luego pasarlo por encima de la parte fija y del cabo de labor formado así, la abertura de frente en forma de V, como lo muestra el gráfico.

d. Atadura de vuelta culebra o merlín

Se emplea para sostener una línea alámbrica de campaña en una viga, cruceta u otros soportes. Para hacer esta atadura, tomar un pedazo de MERLÍN que, al doblarlo, desde la posición de sustentación del cordón, dé

dos vueltas alrededor del soporte y vuelta hacia abajo otra vez (hacia el alambre con un soporte de 10 metros para atarle. Inserte los extremos por el lado formado en la mitad del MERLÍN y ajustarlo bien alrededor del cordón; pasar el Merlín doble dos veces alrededor del soporte y devolver al hombre.

e. Nudo de cesta.



Se usa para sostén y tensión en árboles o postes. Se hace amarrando una chinela al conductor hasta llegar al poste, luego se hace una atadura de tensión al árbol.

12. TELEFONOS DE CAMPAÑA:

El uso frecuente del teléfono por parte del personal militar, es ya causa lógica para que nos tengamos que mantener familiarizados con estos equipos. La eficiencia que nos pueda prestar este equipo depende de varios factores que debemos tener siempre presentes:

a. El tipo de construcción de líneas.

b. Tipos de equipos a usar.

c. Condiciones climáticas.

d. Adiestramiento del personal.

Existen tres tipos de servicios diferentes en las comunicaciones telefónicas, los cuales han sido denominados: sistemas alámbricos de campaña:

1) Batería local (BL).

2) Batería común (BC).

3) Señal de llamada batería común (SBC).

1). BATERÍA LOCAL(BL).

En este sistema, la energía eléctrica o fuente de poder para transmitir es suministrada por las baterías internas o externas de cada teléfono o central telefónica y para llamadas es suministrada por un generador manual o magneto.

2). BATERÍA COMÚN (BC).

Es el sistema en el cual la energía eléctrica para transmisión y para llamadas es suministrada por una fuente de poder que es común a todas las estaciones y que generalmente se encuentra en la central telefónica.

3). SEÑAL DE LLAMADA EN BATERÍA COMÚN (CBS).

En este sistema la energía eléctrica para la transmisión proviene de la batería de cada teléfono, pero la energía para las llamadas se origina en una fuente común a todas las estaciones.

13. TELÉFONO DE CAMPAÑA TA 1/PT:

El teléfono TA 1/PT (ver dibujo) es un equipo de sonido reforzado diseñado especialmente para ser usado en las áreas cercanas al enemigo o también como teléfono de prueba de línea.

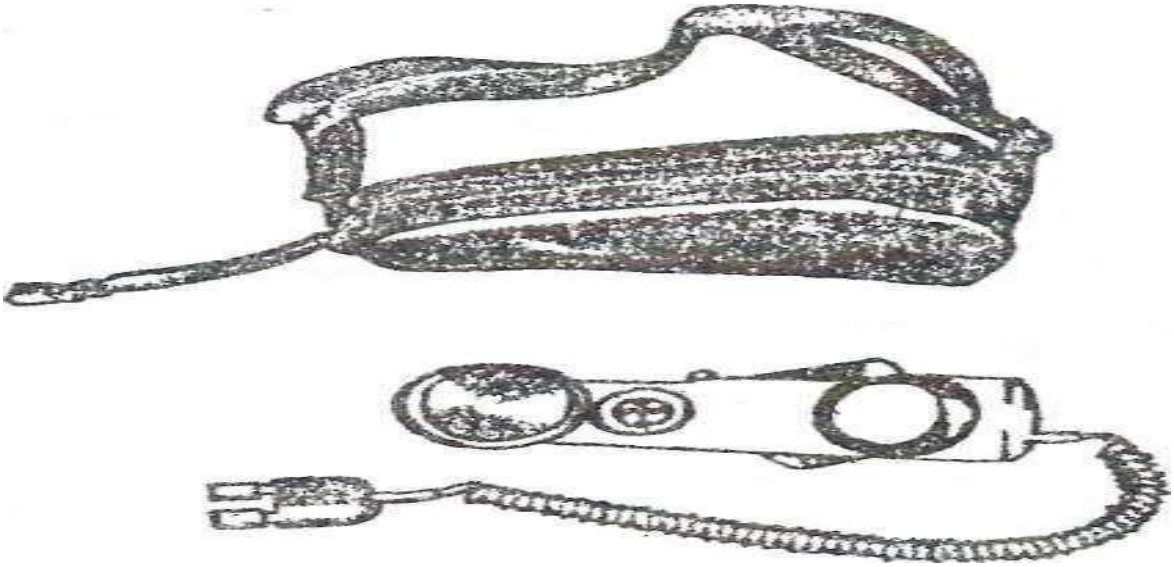
Este teléfono puede ser usado para las comunicaciones con cualquier otro teléfono o central telefónica de campaña en el sistema de batería local (BL), tiene un alcance de transmisión de 6 a 16 Kms. aproximado, su peso es de 1,5 Kg.

a. Descripción:

El teléfono está diseñado en forma de micro teléfono con un transmisor y receptor y un interruptor del circuito (PTT) presione para hablar. En la parte opuesta de este interruptor, se encuentra una palanca que hace rotar un generador (G) el cual está ubicado dentro del micro teléfono y genera una corriente alterna de (15 a 20 voltios). En la parte central se encuentra un dispositivo en forma de reloj para la señal de llamada visual, al producirse la llamada, se llena la figura con una placa de color blanco que luego desaparece al presionar el interruptor (PTT). En la parte inferior está ubicado el control de volumen de la señal de llamada audible, marcado OFF LOUD. Completa el equipo, un cable de dos conductores que terminan en un par de terminales del tipo de resortes para su conexión a la línea.

14. TELÉFONO DE CAMPAÑA TA-312/PT:

El teléfono TA-312/PT (ver dibujo) es un equipo impermeable de campaña y se puede emplear en sistemas de batería local (BL), llamada de batería común



(CBS) o sistema de batería común (CB). El teléfono pesa aproximadamente 4,50 Kgs. El alcance de transmisión del teléfono empleado con alambre de campaña WD 1/TT es de 24 a 35 Kms., dependiendo de las condiciones del alambre. El teléfono TA-312/PT puede ser operado con el micro teléfono del teléfono propiamente dicho o con un micro teléfono de casco auxiliar.

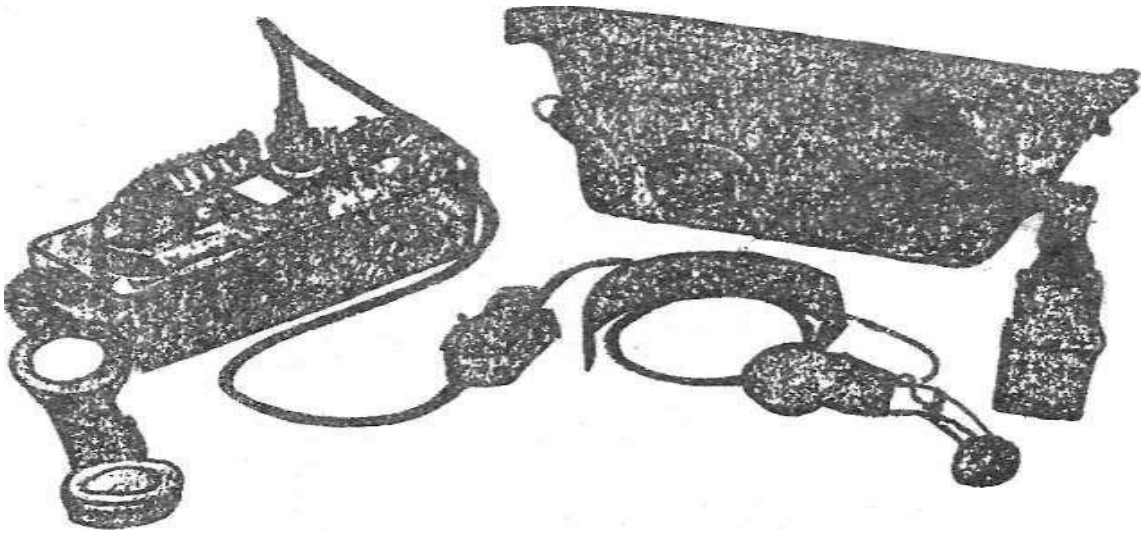
a. Componentes:

1) Estuche CY-1277/PT del teléfono. El estuche de lona incluye una correa que está adherida con sujetadores rápidos o argollas, en las extremidades del estuche.

2) Conjunto de caja y tablero que contienen todos los controles de operación.

3) Micro-teléfono H-60/PT.

4) Equipo adicional (2) baterías BA-30 para la operación de un microteléfono de casco H-144/U.



15. TELÉFONO DE CAMPAÑA TA-427 BD

a. Descripción

El TA-427 BD es un aparato telefónico versátil de diseño moderno que puede operar en todo tipo de condiciones, tanto en interiores como exteriores. El equipo incluye en su diseño un extenso uso de componentes eléctricos, tales como mic1ro-fono electromagnético con un amplificador. El modelo TA-427 BD está diseñado para operar en redes telefónicas civiles con método de discado por pulsos.

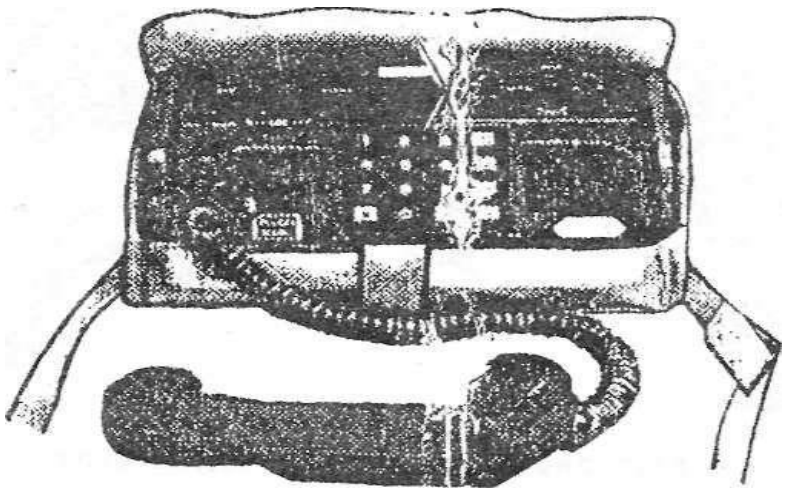
b. Características técnicas:

Banda de frecuencia:	300 a 3400 Hz
Impedancia:	600 Ohmios.
Consumo de corriente:	7 mA (típ.)

Modos de operación: Batería Central (CB)

c. Componentes externos:

COMPONENTE	FUNCIÓN
(a) BORNES DE LÍNEA:	CONEXIÓN PARA LOS CABLES DE LÍNEA TELEFÓNICA
(b) ZUMBADOR:	SEÑALIZADOR DE LLAMADAS
(c) LED INDICADOR:	CENTELLEA CUANDO SE RECIBE UNA LLAMADA
(d) CONTROL DE VOLUMEN:	CONTROLA EL VOLUMEN DEL ZUMBADOR.



16. TELÉFONO DE CAMPANA TA-427

a. Operación

b. Efectuando llamadas:

1) Levante el microteléfono y escuche el tono de discado.
2) Marque el número solicitado presionando las teclas adecuadas.
3) Mientras esté hablando presione el interruptor PTT y deje de presionarlo cuando esté escuchando.
4) Al finalizar la conversación, devuelva el microteléfono y verifique que esté bien colocado en su cuna.

c. Recibiendo llamadas:

1) Al recibir una llamada suena el zumbador y centellea el LED.
2) Regule el volumen del zumbador mediante su control VOLUME.
3) Para responder, levante el microteléfono de su soporte.
4) Al finalizar la conversación, devuelva el microteléfono a su cuna.

17. TELÉFONO DE CAMPAÑA TA-427 BR.

a. Descripción:

El TA-427 BR es un aparato telefónico de diseño moderno que puede operar en todo tipo de condiciones. Es un equipo de características idénticas al equipo telefónico TA-427 BD, con la diferencia que el modelo BR está diseñado para ser usado en sistemas telefónicos de campaña. El teléfono de campaña TA-427 modelo BR incorpora un generador de llamada de baja frecuencia y alto voltaje para líneas telefónicas de uso militar.

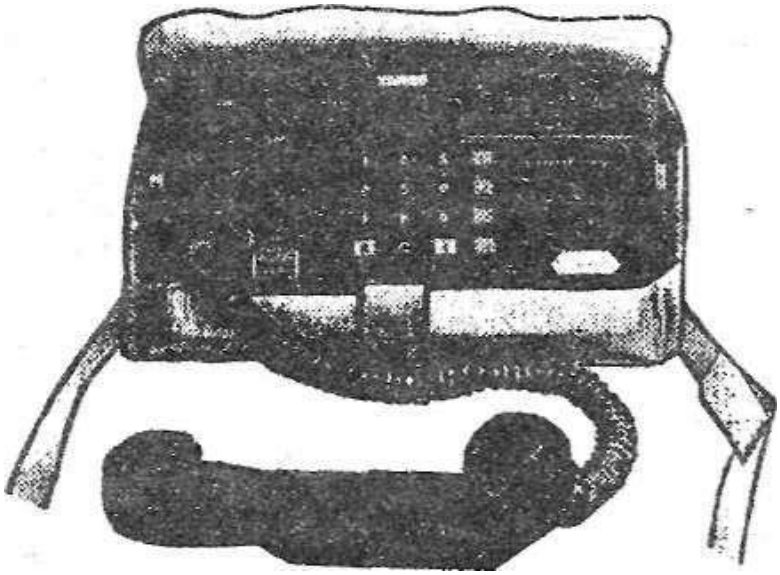
b. Características técnicas:

Iguales a los del modelo BD, salvo las especificadas a continuación:

Fuente de alimentación: Tres baterías BA-30 (1,5 V X 3).

Modos de operación: LB, CB Y CBS."

Impedancia de entrada: 290 Ohmios, en modos CB y CBS.



c. Componentes externos:

1) Selector De Modo: Selecciona El Modo De Operación: Lb, Cb O Cbs. Existe En El Selector Una Ranura Que Apunta Hacia El Modo Elegido. El Modo De Operación Se Cambia Girando El Selector Con Un Pequeño Destornillador.

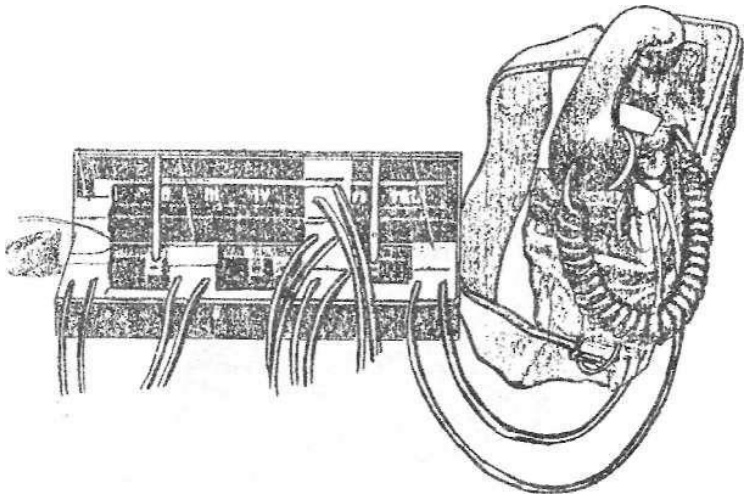
2) Botón De Llamada: Este Botón Se Encuentra Ubicado En El Panel. Se Presiona Para Llamar A Un Abonado O A La Central Telefónica.

CENTRALES TELEFÓNICAS

a. CENTRAL TELEFÓNICA SB-993/GT

Provee comunicaciones para seis circuitos, líneas telefónicas de batería local. Estas líneas pueden ser interconectadas, bien sea de tipo punto a punto, o como una llamada conmutada (a). La señal de llamada es provista por una lámpara incandescente que se halla al lado derecho de cada vibrador. La central telefónica SB-993/GT está dotada de seis vibradores numerados, los primeros seis de izquierda a derecha y el séptimo marcado TEL, que usa el teléfono del operador.

CENTRAL TELEFÓNICA SB 993



a. DESCRIPCIÓN

(1) La central telefónica SB-993/GT consiste en una funda CY-2589/GT, un estuche porta-adaptadores MT-2156/GT y siete adaptadores U-184/GT.

(2) La funda CY-2589/GT está forrada de lona, es usada para proteger y guardar el estuche porta-adaptadores.

(3) El estuche porta-adaptadores MT-2156/GT como su nombre lo indica, es usado para montar siete adaptadores U-184/GT, siete Jacks en la base del estuche, sujetan a los adaptadores en posición vertical durante la operación. Dos porta-cubiertas mantienen la tapa o cubierta del estuche abierta durante la operación.

(4) El adaptador U-184/GT es una combinación de Jacks y clavijas montadas en un pequeño cuerpo cuadrado de un material plástico transparente. Una resistencia de 50 K y una lámpara incandescente de 1/25 vatios están montados cerca a través del par de Jacks y las clavijas y sellados dentro del cuerpo transparente.

(5) La fuente de poder de la SB-993/GT no usa ningún tipo de batería. El operador de la central se vale de un teléfono cualquiera para las necesidades de marcación o hablar con otro teléfono.

CENTRAL TELEFÓNICA MANUAL SB-86/P

a. GENERALIDADES. (Ver figura)

Es una central telefónica de batería local, tipo campaña de funcionamiento normal. Se proporcionan facilidades para seleccionar la transmisión de batería común o magneto de cada circuito. Dos de los circuitos se pueden emplear como troncales con una central de batería común de nivel.

b. COMPONENTES Y ACCESORIOS PRINCIPALES:

1. Sección SB 248/P, central telefónica y manual (sección de clavijas).
2. Conjunto de transmisión TA 207/P de central (sección Jacks de enchufes).
3. Fuente de poder PP 998/G 24 V (C).
4. Cubierta exterior (estuche).
5. Micrófono. Casco teléfono H-91/U.
6. Placa de registro
7. Cable de tres conductores (6 pies).
8. Cable de dos conductores (6 pies).

9. Bolsa de lona (para piezas de repuestos).

c. EQUIPOS ADICIONALES:

1. Cuatro baterías BA-30 de 1 1/2 VCD.

2. Diez baterías BA-200/U de 6 1/2 VCD.

d. CAPACIDADES DE LINEAS:

3. Treinta circuitos, empleando 1 sección de Jacks de campo.

4. Sesenta circuitos, empleando 2 secciones de Jacks de campo.

e. CIRCUITOS DE CORDONES TELEFÓNICOS Y DISTANCIA DE OPERACIÓN:

(1) Dieciséis.

(2) Transmisión de magneto 5 K y 22 millas o 35 Kms. de distancia.

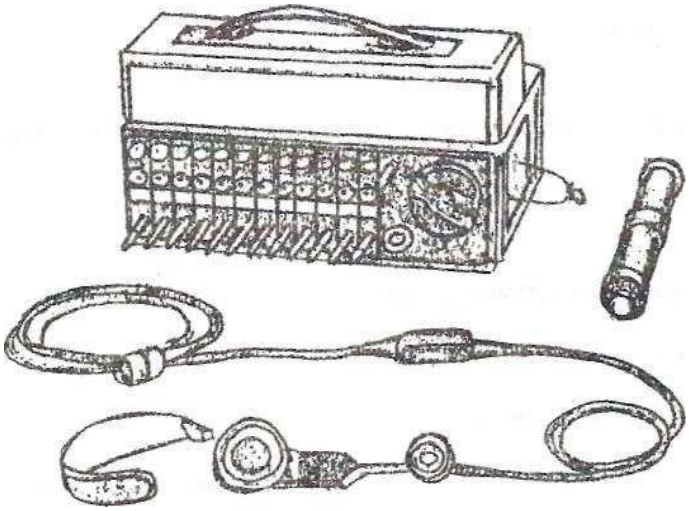
(3) Línea de transmisión batería común 2 K y 4,5 millas o 7,5 Kms. de distancia.

f. CENTRAL TELEFÓNICA DE CAMPAÑA SB-22/PT:

a. DESCRIPCIÓN:

Es una central de 12 líneas, magnéticas, monocordio, de campaña, empleada para intercomunicar líneas de batería local y equipos telegráficos de frecuencia radiotelefónica (F-RT).

Se puede interconectar con el Grupo de Control Remoto GRA-990 ó con el Sistema de Radio-teléfono Multicanal TRC-645.



CENTRAL TELEFÓNICA SB-22 PT

Es pequeña, liviana y no requiere montura especial para su funcionamiento, todo equipo intercomunicador asociado con cada línea, está montado en un envase de metal, el cual está enchufado en la central telefónica, este envase se llama UNIDAD TELEFÓNICA (TA 221/TT).

a. COMPONENTES, ACCESORIOS Y CAPACIDAD

1. Unidad telefónica TA 221/TT (12 unidades).
2. Unidad telefónica del operador TA 222/TT (1 unidad)
3. Fuente de poder (4) baterías BA 30 (para teléfono del operador y señales).
4. Porta baterías.
5. Micro-teléfono - casco telefónico.
6. Estuche de accesorios.
7. Varilla de metal (para unir al tablero con la tierra).
8. Capacidad 12 líneas.

9. Peso 13,6 Kgs. aproximado.

(1) UNIDAD TELEFÓNICA:

1. Cordón y clavijas retráctil.
2. Un enchufe indicador de llamada.
3. Plaquita de identificación.

(2) UNIDAD DEL OPERADOR:

1. Cordón y clavija.
2. Equipo de timbre.
3. Equipo de alarma.
4. Receptáculo de micro-teléfono - casco telefónico.

(3) TABLERO TERMINAL:

Es un tablero plástico laminado, equipado por un lado con dos hileras de 17 bornes y por el otro lado con cuatro hileras de enchufe.

a. INSTALACIÓN

1. La SB-22 no tiene patas para apoyarse, así que se debe colocar en el suelo, expediente de campaña o mesa.
2. Conecte a tierra el tablero con una estaca conveniente.
3. Conecte la línea de alambre con el borne terminal y anote la identificación del circuito en la tarjeta de identificación.
4. Instale las baterías en la caja para baterías y vea que la caja esté conectada correctamente (con su polaridad).

5. Quite el microteléfono - casco telefónico de la cubierta delantera de la central telefónica y conecte con el receptáculo correcto de la unidad del operador.

6. Conecte el cable de alimentación del timbre externo, si existe, al borne terminal.

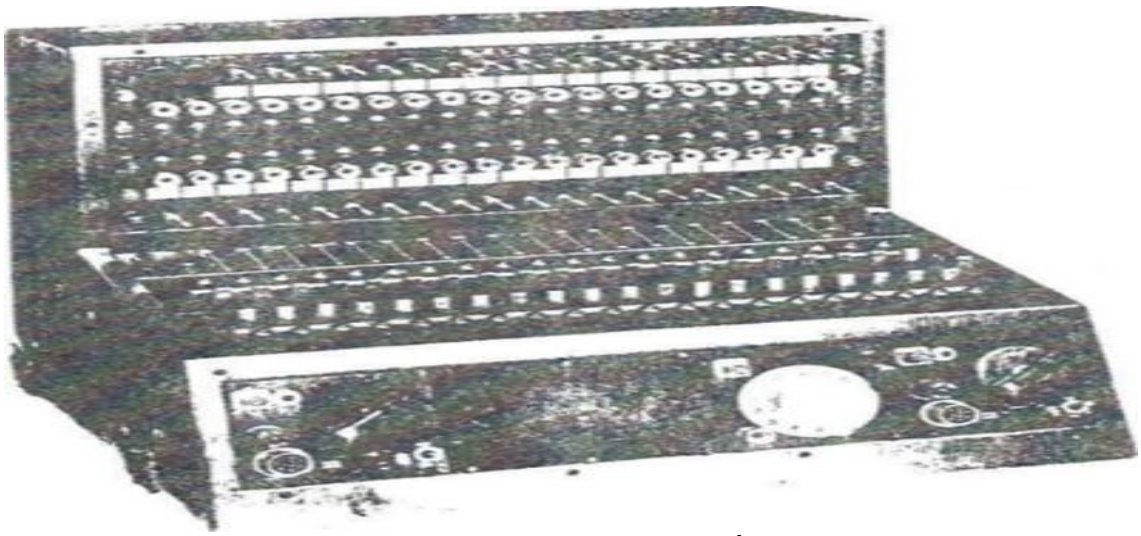
CENTRAL TELEFÓNICA SB-42a.

a. DESCRIPCIÓN

La SB-42 es una central telefónica tipo militar, que puede ser usada para interconexión de las redes de magneto, líneas de discar ligadas a la central automática y una troncal fácil conectada a la central normal.

Las unidades básicas (tiras y paquetes de operadores) de la SB-42 son las mismas a las utilizadas por la central SB 22PT, por eso es que existe una total compatibilidad con los otros equipos militares existentes.

Todas las unidades son del tipo módulos enchufables y fácil mantenimiento.



La SB-42 contiene 40 paquetes o terminales de líneas, los cuales pueden ser divididos en las proporciones deseadas entre el magneto y el grupo de líneas automáticas, además, las características del panel contienen el DIAL SWITCH

(accesorio opcional sustituto de la SB-22PT y dos grupos de operadores para añadir mayor confiabilidad.

Una característica alumbró nica en la lámpara de llama al lado del Switch individual, los switches sirven para responder y llamar a los suscriptores y para la intervención del operador.

CENTRAL TELEFÓNICA – SB – 42

Están provistas dos facilidades para la conexión de los cables a la SB-42, bornes y conectores multipin.

Ambos están instalados en la cubierta del panel trasero del gabinete del tablero de control.

El panel puede ser operado desde cualquier fuente de poder externa de 24 voltios D.C., similar a la utilizada por la SB 22PT, o desde las tres baterías secas de 3 voltios D.C. ubicadas anteriormente. Las líneas son protegidas por descargadores contra rayo o fusibles de voltaje. Son provistas de una iluminación del panel y una lámpara de prueba.

b. CARACTERÍSTICAS TÉCNICAS

CAPACIDAD:

40 líneas (automáticas o magneto).

02 grupos o paquetes de operadores en paralelo.

01 dial switch.

20 watios 25 Hz.

Unidad de discado (con sistema alambrado).

FUENTE DE PODER:

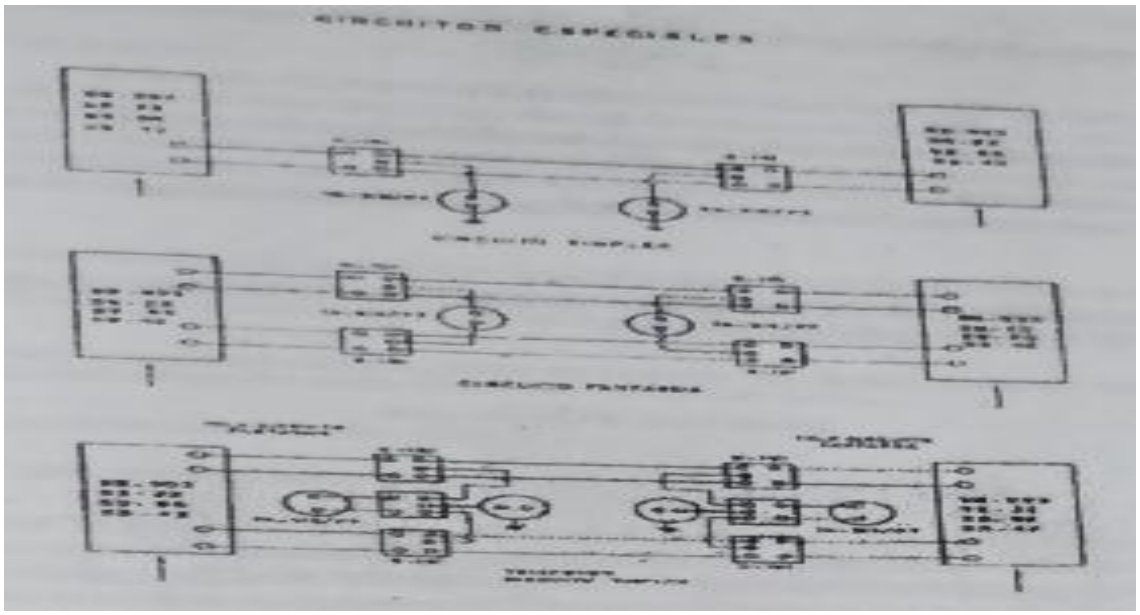
24 volt. D.C. interno (sin lámparas de llamadas).

SEÑALAMIENTO:

Señal de líneas mecánicas y señal lumínica en lámparas individuales de llamadas.

PESO: 45 Kgs

40. CIRCUITOS ESPECIALES DE ALAMBRE DE CAMPAÑA, CIRCUITOS



SIMPLEX Y FANTASMAS SIMPLEX.

1. INTRODUCCIÓN:

Estos circuitos son construidos para proveer canales de comunicación adicionales. Un conocimiento exacto de las construcciones de estos circuitos por parte del personal de comunicaciones es esencial para el buen funcionamiento de los sistemas alámbricos de campaña.

2. BOBINAS DE REPETICIÓN:

La bobina de repetición es el componente más usado en este tipo de circuitos, está compuesta por un transformador de audio en una relación (1:1) provista de dos arrollados sobre el núcleo de hierro dulce, uno de estos

arrollados es tocado por una conexión en su centro eléctrico. Cada bobina está compuesta de 5 terminales o bornes, 3 a un lado y 2 en el otro. El lado donde están los terminales está conectado a los terminales exteriores situados en lado de 3 terminales marcados "LINE" (línea). El terminal central está conectado al terminal marcado "PT". El terminal marcado "GND" no tiene conexión eléctrica.

3. CIRCUITO SIMPLEX:

   Un circuito simplex puede ser definido como circuito de retorno por tierra, superpuesto en un circuito metálico mediante el uso de dos bobinas de repetición.

4. VENTAJAS DEL CIRCUITO SIMPLEX:
   a. Evitar sobrecarga de tráfico en los circuitos metálicos.
   b. Ahorrar tiempo y alambre.
   c. Asegura un canal de comunicación, aunque exista corto circuito un conductor abierto en el circuito metálico.

5. CIRCUITOS FANTASMAS:

   Es un canal adicional de comunicación superpuesta en dos circuitos metálicos existentes por medio de 4 bobinas de repetición.

6. USO DE LOS CIRCUITOS FANTASMAS:

   a. Los circuitos metálicos deben ser balanceados (igual longitud e igual resistencia) ya que de otra forma se producirían interferencias.

   b. El circuito fantasma puede ser usado para canales de teletipo cuando no existen posibilidades de un buen contacto con tierra.

   c. Puede ser usado para proveer un canal adicional entre dos puestos de comando.

   d. Puede o no ser controlado por el operador de la central telefónica.

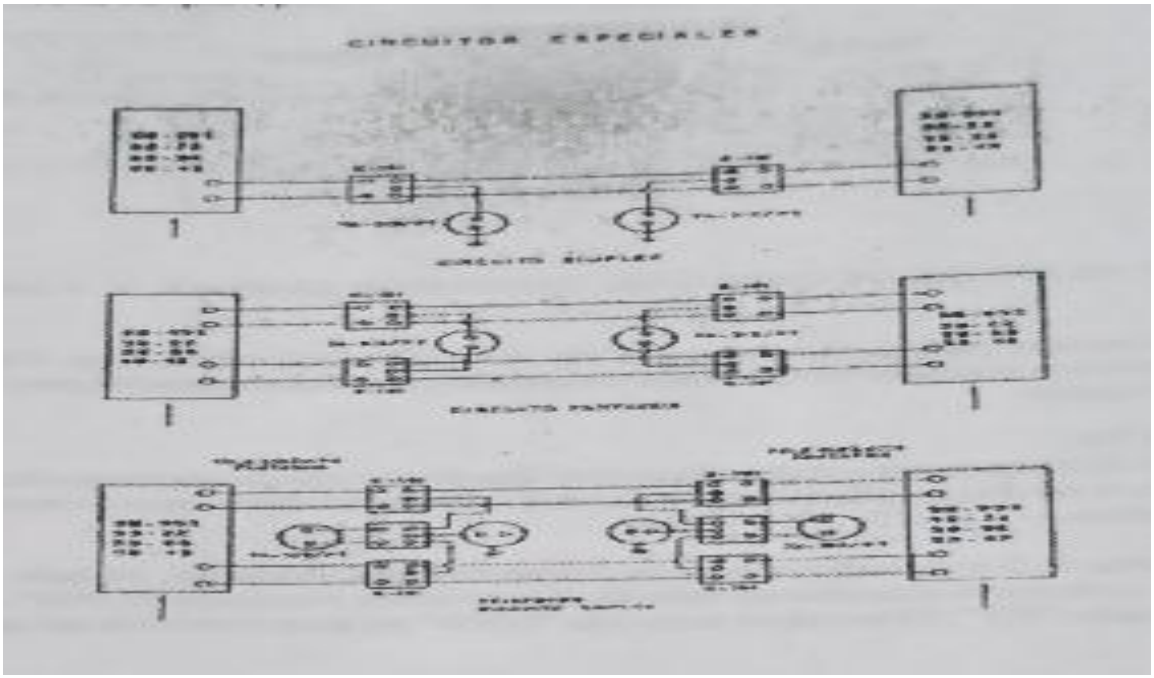
7. CIRCUITOS FANTASMAS SIMPLEX:

Es un circuito de retorno por tierra superpuesto a otro circuito fantasma ya existente.

USO

a. Un circuito fantasma, puede llegar a ser fantasma-simplex, usando bobinas de repetición extras. Seis bobinas se requieren para formar un circuito fantasma-simplex.

b. Solamente un circuito simplex, puede ser usado con cada circuito fantasma, para una conexión de retorno por tierra.



8. CENTRAL TELEFÓNICA

En los primeros teléfonos, la corriente estaba generada por una batería. El circuito local tenía, además de la batería y el transmisor, un arrollamiento de transformador, que recibe el nombre de bobina de inducción; el otro arrollamiento, conectado a la línea, elevaba el voltaje de la onda sonora. Las conexiones entre teléfonos eran de tipo manual, a cargo de operadores que trabajaban en centralitas ubicadas en las oficinas centrales de conmutación o centralitas.

9. TIPOS DE CENTRALES TELEFÓNICAS ADMINISTRATIVAS

La Centrales Telefónicas Análogas.

La Central Telefónica Digital.

Centrales Telefónicas híbrida.

Centrales Telefónicas IP.

10. CENTRALES TELEFÓNICAS ANÁLOGAS.

Un teléfono convencional que transmite los datos de voz al convertirlos en pulsos electrónicos. La telefonía analógica lleva décadas entre nosotros, y depende exclusivamente de líneas de teléfono de hilo de cobre y conexiones RJ-11.

11. LA CENTRAL TELEFÓNICA DIGITAL.

Usa Internet para enviar sus datos de llamadas telefónicas digitales a un servidor externo; y una vez allí esos datos digitales viajan a otro sistema telefónico digital, o se vuelven a convertir en datos analógicos, si es que se desea llamar a un teléfono fijo de red conmutada.

12. CENTRALES TELEFÓNICAS HÍBRIDA.

La centralita híbrida, es capaz de soportar diferentes tecnologías de transmisión e interfaces telefónicas. Por lo tanto, la centralita híbrida puede

conectarse a las redes telefónicas públicas mediante una interfaz móvil o mediante Voz sobre IP.

13. CENTRALES TELEFÓNICAS IP.

En el caso de la telefonía IP la señal telefónica se transmite al puerto de enlace: si la señal de entrada no es digital, hay que digitalizarla; luego los datos se comprimen, se dividen en paquetes y se transmiten al punto de destino utilizando el protocolo TCP / IP.

14. COMO ESTA ESTRUCTURADA UNA CENTRAL TELEFONICA

Armario de distribución Primario (ADP).

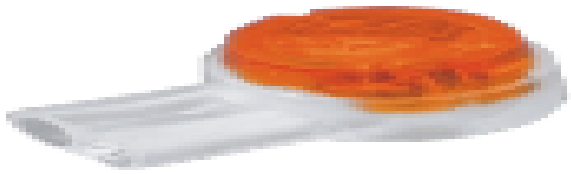
Armario de Distribución Secundaria (ADS).

Un FXB (Feed Exchange Box). Caja de Distribución

Principal (CDP) o Tablero Principal.

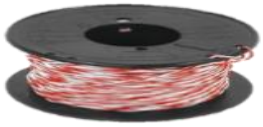
15. HERRAMIENTAS BÁSICAS PARA TRABAJAR EN LA TELEFONÍA.

Es un conector cuya función es empalmar dos cables para conseguir una unión perfecta y sin interferencias entre ambos (la misma función la cumple la roseta de empalme, pero ésta es una opción mucho más económica que se debe usar sólo en interiores).



16. CABLE JUMPER TELEFÓNICO.

Es un cable telefónico de cobre sirve para construir las rutas en los Armarios.



17. CABLE DE PAR TRENZADO: Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado.

18. QUE ES EL CÓDIGO DE COLORES

Es un código de colores usado para identificar inequívocamente un conductor en un cableado de Telecomunicaciones para uso en interiores, conocido como cableado estructurado. El aislante de cada conductor es coloreado, el primer color es elegido grupo de cinco colores y el otro color de un segundo grupo, ofreciendo 25 combinaciones de dos colores.

a. COLORES PRIMARIOS

Los colores primarios o colores primitivos son aquellos colores que no pueden ser obtenidos mediante la mezcla de otros tonos o colores.

Blanco, Rojo, Negro, Amarillo, Violeta o Morado.

b. COLORES SEGUNDARIOS.

Se llaman colores secundarios a aquellos que se obtienen al mezclar dos colores primarios. Reciben ese nombre justamente porque derivan de los colores primarios.

Azul, Naranja, Verde, Marrón, Cris.

Identificación de pares

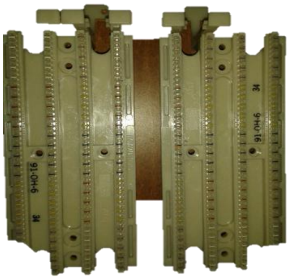
Par	Color 1		Color 2	
1		Blanco		Azul
2		Blanco		Naranja
3		Blanco		Verde
4		Blanco		Marrón
5		Blanco		Gris
6		Rojo		Azul
7		Rojo		Naranja
8		Rojo		Verde
9		Rojo		Marrón
10		Rojo		Gris
11		Negro		Azul
12		Negro		Naranja
13		Negro		Verde
14		Negro		Marrón
15		Negro		Gris
16		Amarillo		Azul
17		Amarillo		Naranja
18		Amarillo		Verde
19		Amarillo		Marrón
20		Amarillo		Gris
21		Violeta		Azul
22		Violeta		Naranja
23		Violeta		Verde
24		Violeta		Marrón
25		Violeta		Gris

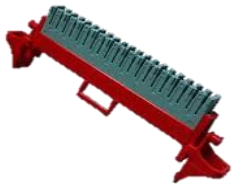
1. MANGA DE EMPALME.

Es un componente de empalme utilizado para mejorar la protección o el posicionamiento de soporte de empalmes de telefonía. Pueden ir aéreas o

SUBTERRÁNEAS.

2. REGLETA TELEFÓNICA





TESTER	MICRO TELEFONO	GENERADOR DE TONO

PINZA	ALICATE DE CORTE	DESTORNILLADORES DE PALA Y ESTRIA.

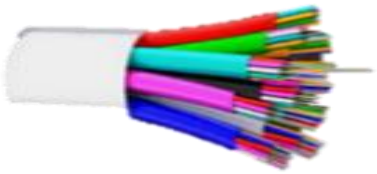
3. HERRAMIENTAS BÁSICAS PARA TRABAJAR EN LA TELEFONÍA.

4. CÓDIGO DE COLORES FIBRA ÓPTICA

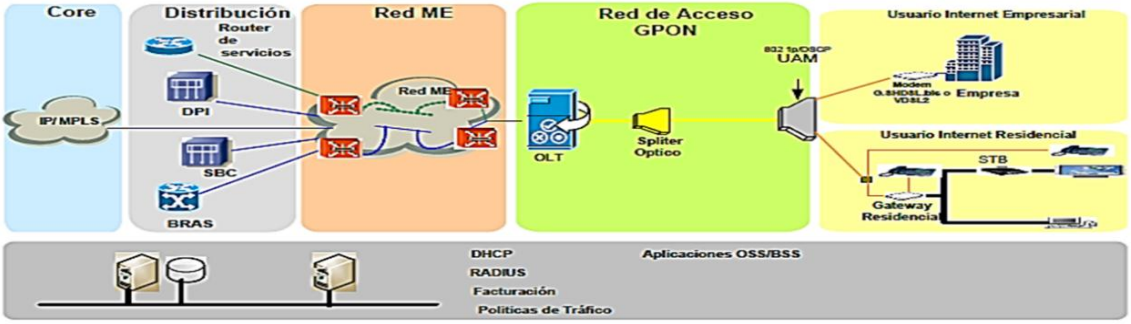
La codificación por color de la fibra es una técnica que garantiza la identificación clara de cada hebra y una mecanización adecuada. Esta técnica cumple con las normas TIA-598C, que dictan cómo se organizan los marcadores y los tubos de protección en las hebras. Sin esta norma, las redes de fibra tendrían dificultades para reconectar los cables, lo que implicaría costosos ciclos de reparación y pérdida de tiempo.

	1 = AZUL
	2 = NARANJA
	3 = VERDE
	4 = MARRON
	5 = GRIS
	6 = BLANCO
	7 = ROJO
	8 = NEGRO
	9 = AMARILLO
	10 = VIOLETA
	11 = ROSA
	12 = CELESTE

5. CABLE DE FIBRA OPTICA: es un cable de red que contiene hilos de fibra de vidrio dentro de una carcasa aislada. Están diseñados para redes de datos y telecomunicaciones de larga distancia y alto rendimiento.



a. **¿QUÉ ES GPON?** Redes Ópticas Pasivas en Gigabit (Gigabit Passive Optical Network), ITU G.984.X. Es una tecnología de acceso de telecomunicaciones que permite alcanzar altas velocidades de transmisión y recepción de datos



b. **Aspectos Generales de Gpon:** La Terminación de Línea Óptica (OLT, optical line termination): es el elemento que proporciona la interfaz del

lado a la red de la OAN (redes ópticas activas), y está conectada a una o varias ODN (red de distribución óptica)

MA5600T

ZTE ZXA10 C300

Huawei MA5608T

Los equipos terminales son los encargados de trasladar la información desde los formatos encapsulados e interfaces utilizados en la red PON a los requeridos por el usuario. Son conocidos ONT (optical network terminal) u ONU (optical network unit). El primero de los términos es más aplicado a las unidades para usuarios domésticos y el ultimo para usuarios comerciales.

c. Arquitectura de Tecnología GPON

GPON: Gigabit-capable Passive Optical Network (Red óptica pasiva con capacidad Gigabit)

PON es acrónimo para Passive Optical Network (Red óptica pasiva)

Arquitectura de red punto a multipunto:

Optical Line Terminal (OLT). (Terminal de línea óptica)

Optical Network Unit (ONU). (Unidad de red óptica)

Optical Distribution Network (ODN). (Red de distribución óptica)

Optical Access Network (OAN). (Red de acceso óptico)

ELEMENTOS DE LA RED

Elementos Pasivos:

FXB (Caja de Distribución Principal): Contiene las líneas telefónicas en un edificio

d. ODF (Distribuidor de Fibra Central)

Dispositivo que permite conexión entre OLT y la ODN Contiene puertos OLT, splitters, y fibras de planta externa

REGLETA

Circuitos de conexión que distribuyen el servicio a los clientes

SPLITTER: Dispositivos que dividen la señal óptica

e. CONECTORES: Dispositivo que permite unir la FO con otros elementos Diversos tipos: ST, SC, LC y FC

f. EMPALMES: Uniones entre los cables de Fusión ó térmico Adhesión (epóxido) Mecánico (Gel)

g. MANGAS: Cierres de empalmes Estructuras que protegen las conexiones y los dispositivos ópticos pasivos

h. ELEMENTOS DE LA RED:

Elementos Activos

OLT (Equipo Central Óptico) Transmisión y recepción de la señal.

Agrega tráfico de los usuarios

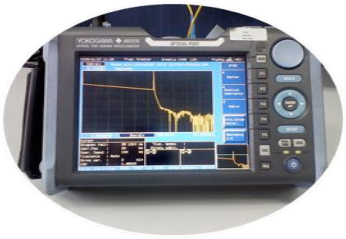
En ruta a la red de transporte

Interconecta con la red Metro.

MDU (Unidad para Viviendas Múltiples)

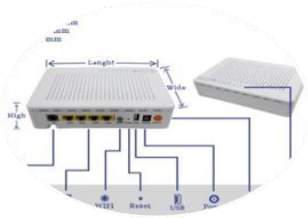
Unidad que usa los pares de cobre para servicio XDSL

Requieren energía eléctrica



ONU/ONT (Unidad de Red Óptica)

Dispositivo del usuario donde termina la Fibra óptica.



i. MODEM VDSL

Dispositivo que modula o demodula señales. Soporta velocidades entre 100/50 Mbps y 100/100 Mbps

j. OTDR (Reflectometría de Dominio de Tiempo Óptico)

Permite reducir los impactos x fallas en FO en sus tramos. Detecta variaciones en la Fibra Óptica

Herramientas para fibra óptica

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO VIII

SEGURIDAD DE LAS COMUNICACIONES Y CIBERDEFENSA

MARCO DOCTRINAL DE LA CIBERSEGURIDAD

1. Alcance y Definición

La Ciberseguridad es la extensión y aplicación de la doctrina de seguridad tradicional (que históricamente se enfocaba en lo físico y en la información en papel) a los sistemas de información, redes y datos digitales que sustentan las operaciones modernas. Su objetivo principal es asegurar la tríada CID (Confidencialidad, Integridad y Disponibilidad) de las comunicaciones y los datos en el ciberespacio.

a. Confidencialidad: Garantizar que la información solo sea accesible a aquellos autorizados a verla. Esto se logra mediante mecanismos como el cifrado y el control de acceso.

b. Integridad: Asegurar que los datos no han sido modificados, alterados o destruidos de forma no autorizada. Se verifica mediante el uso de hashes criptográficos y firmas digitales.

c. Disponibilidad: Garantizar que los sistemas y las redes de comunicaciones estén operativos y accesibles para los usuarios autorizados cuando se les necesite. Esto requiere resiliencia ante ataques de denegación de servicio (DoS/DDoS) y fallos del sistema.

2. El Ciberespacio como Dominio de Guerra

El Ciberespacio ha sido formalmente reconocido como el quinto dominio operacional, sumándose al terrestre, marítimo, aéreo y espacial. Es un campo de batalla único porque es artificial, global e instantáneo.

a. Objetivo de la Guerra Cibernética: El objetivo principal en este dominio es degradar, interrumpir o explotar las redes de Mando y Control (C2) del adversario. Al atacar las comunicaciones, se busca paralizar la toma de decisiones, la coordinación de fuerzas y la logística.

b. Rol de los Operadores de Comunicaciones: Los Operadores de Comunicaciones son la primera línea de defensa en el ciberespacio. Su entrenamiento, vigilancia constante y cumplimiento estricto de los protocolos de seguridad son críticos para mantener la integridad de la red de C2 y repeler incursiones en tiempo real. Un fallo en este nivel puede tener consecuencias tácticas y estratégicas inmediatas.

3. Los Tres Pilares de la Seguridad de Comunicaciones (COMSEC)

La seguridad integral de las comunicaciones (COMSEC) es un concepto holístico que requiere la convergencia y ejecución simultánea de tres áreas fundamentales para proteger las redes críticas:

Pilar de COMSEC	Descripción Detallada	Impacto y Ejemplos
Seguridad Física	Implica la protección del hardware, el cableado y la infraestructura	La falta de seguridad física puede anular cualquier medida digital. Ejemplos: El uso de jaulas Faraday o recintos con control de acceso, la vigilancia de centros de datos, la seguridad perimetral para evitar la

Pilar de COMSEC	Descripción Detallada	Impacto y Ejemplos
	contra el acceso, manipulación o daño físico no autorizado.	interrupción de la fibra óptica o la colocación de sellos anti-manipulación en el equipo sensible.
Seguridad Criptográfica	Se enfoca en la protección de la información en tránsito y en reposo mediante el uso de algoritmos matemáticos.	Es la base de la Confidencialidad e Integridad. Ejemplos: El cifrado de extremo a extremo de los mensajes (para asegurar la confidencialidad) y el uso de certificados digitales y algoritmos de hashing (para asegurar la autenticidad y la integridad).
Seguridad Informática (Ciberseguridad)	Se centra en la protección de la infraestructura lógica, software y sistemas operativos contra amenazas de origen digital.	Protege la disponibilidad y la operatividad de la red. Ejemplos: La implementación de firewalls, la gestión de parches de seguridad, la protección contra malware, y la detección de intrusiones a nivel de red y host.

4. SEGURIDAD INFORMÁTICA (CIBERDEFENSA) DE REDES

a. Principio de Mínimo Privilegio

El Principio de Mínimo Privilegio (PoLP) es una directriz fundamental de seguridad que establece que, a un usuario, sistema, o dispositivo (como un servidor o una aplicación) se le debe otorgar solo el nivel de acceso y los

permisos mínimos necesarios para cumplir su función específica y ninguna capacidad adicional.

1) Propósito: Limita el radio de explosión (blast radius). Si una cuenta de usuario es comprometida o si un malware infecta un sistema, el atacante solo puede acceder o dañar los recursos que estaban disponibles para ese nivel de privilegio, evitando la propagación lateral a sistemas críticos (C2). Un operador de radio, por ejemplo, solo necesita permisos para operar su terminal, no para modificar la configuración del servidor de e-mail central.

c. Segmentación y Arquitectura de Confianza Cero (Zero Trust)

Las redes de comunicaciones, especialmente las militares, deben dejar de lado la antigua filosofía del "castillo y foso" (donde todo es seguro una vez dentro del perímetro).

a. Segmentación de Red: La red debe dividirse en múltiples zonas o segmentos lógicos (VLANs), separando los sistemas de alta criticidad (C2), que manejan información sensible, de las redes administrativas o de invitados. Esto aísla los sistemas críticos. Un compromiso en la red de menor sensibilidad no afectará automáticamente a los sistemas de Mando.

b. Arquitectura de Confianza Cero (Zero Trust): Este modelo establece el principio: "Nunca confíes, siempre verifica." Niega el supuesto de que los usuarios o dispositivos dentro del perímetro de la red son inherentemente confiables.

c. Proceso: Toda solicitud de acceso, ya sea de una entidad interna o externa, debe ser verificada, autenticada y autorizada de forma rigurosa antes de concederse el acceso a un recurso específico, incluso si el usuario ya está conectado a la red.

La defensa de la red requiere una vigilancia activa y continua del tráfico.

a. Firewalls (Cortafuegos): Actúan como puntos de control de acceso en la red. Implementan políticas de filtrado (reglas de acceso) que dictan qué tráfico (puerto, protocolo, dirección IP) puede pasar entre redes o segmentos, bloqueando por defecto todo el tráfico no explícitamente permitido.

b. Sistemas de Detección/Prevención de Intrusiones (IDS/IPS):

1) IDS (Detección): Monitoriza el tráfico de red en busca de patrones de ataque conocidos (basados en firmas) o comportamientos anómalos (basados en heurística), generando una alerta al Operador de Comunicaciones.

2) IPS (Prevención): Realiza la misma detección que el IDS, pero también tiene la capacidad de tomar acciones automáticas para bloquear, descartar o restablecer la conexión maliciosa antes de que el ataque tenga éxito, actuando como una barrera de último recurso.

Gestión de la Configuración y Vulnerabilidades

La seguridad es un proceso continuo, no un estado final. El Oficial de Comunicaciones es responsable de garantizar que los sistemas mantengan una "postura de seguridad" constante.

a. Gestión de la Configuración: Asegurar que los sistemas operativos, los dispositivos de red y las aplicaciones críticas solo usen la configuración de seguridad aprobada (Baseline). Esto implica la desactivación de servicios innecesarios, la eliminación de cuentas por defecto y la implementación de políticas de contraseñas complejas.

b. Gestión de Vulnerabilidades: Un ciclo continuo para identificar y corregir fallas de seguridad:

1) Identificación (Escaneo): Uso de herramientas automatizadas para escanear la red, dispositivos y software en busca de vulnerabilidades conocidas (errores de código o configuración que pueden ser explotados por un atacante).

2) Mitigación (Patch Management): La aplicación inmediata y metódica de parches de seguridad y actualizaciones de software. Es crucial porque las vulnerabilidades conocidas son los vectores de ataque más comunes, y los atacantes suelen explotarlas poco después de que se publica el parche.

SEGURIDAD LÓGICA DE LAS TERMINALES (PUNTO FINAL)

Cifrado de Datos en Reposo

El cifrado no es solo para el tráfico de red, sino también para los datos cuando están almacenados (en reposo) en un dispositivo.

a. Mandato: Todos los datos sensibles, clasificados o críticos almacenados en discos duros, servidores, computadoras portátiles o terminales tácticas deben estar cifrados a nivel de disco completo (Full Disk Encryption - FDE).

b. Función de Seguridad: En el caso de pérdida, robo o captura del dispositivo por parte del adversario, el cifrado asegura que, sin la clave o contraseña correcta, la información permanece inaccesible, previniendo una brecha de Confidencialidad y mitigando el impacto de la pérdida física.

Control de Acceso y Autenticación Multifactor (MFA)

La seguridad en el punto de acceso requiere más de una simple contraseña.

a. Autenticación Multifactor (MFA): Requiere que el usuario proporcione múltiples "factores" de autenticación de diferentes categorías para obtener acceso a sistemas críticos:
    1. Algo que se sabe: Contraseña, PIN.
    2. Algo que se tiene: Tarjeta inteligente (CAC/PIV), token de seguridad, dispositivo móvil con clave de uso único (OTP).

3. (Opcional) Algo que se es: Datos biométricos (huella dactilar, escaneo de iris).

b. Requisito de Credenciales: La prohibición estricta de cuentas genéricas (p. ej., "Admin," "Operador") o compartidas es vital, ya que elimina la trazabilidad. Cada acción dentro del sistema debe estar ligada a una identidad única para garantizar la responsabilidad (accountability).

Control de Medios Extraíbles

Los medios extraíbles (USB, discos duros externos) representan un riesgo de seguridad significativo, actuando como vectores primarios de infección por malware (p. ej., Stuxnet utilizó este vector) o como vía para la exfiltración (robo) de datos sensibles.

a. Protocolo: Se establece una política de denegación por defecto. La conexión de cualquier medio extraíble a un sistema de comunicaciones o C2 está estrictamente prohibida a menos que se obtenga una autorización expresa del Oficial de Comunicaciones y se haya realizado una revisión de seguridad completa (p. ej., escaneo profundo de malware y verificación de archivos) antes de la conexión.

Ciberhigiene y Concienciación del Personal

El personal es considerado a menudo como el eslabón más débil de la cadena de seguridad, por lo que la formación constante en Ciberhigiene es esencial.

a. Detección de Ingeniería Social: Entrenamiento para reconocer y resistir técnicas de manipulación psicológica que buscan explotar el error humano.

1) Phishing: Intentos de obtener información confidencial (credenciales, datos) a través de correos electrónicos o mensajes fraudulentos que simulan ser entidades confiables.
2) Vishing: Phishing realizado a través de llamadas de voz (Voice Phishing).

b. Uso Seguro del Correo Electrónico: Instrucción en la verificación de la autenticidad del remitente y la inspección minuciosa de los encabezados del correo (dirección real) y los enlaces antes de abrirlos o hacer clic. Los adjuntos y enlaces de correos no verificados son un método principal para la entrega de ransomware y otro malware.

INTELIGENCIA ARTIFICIAL (IA) COMO HABILITADOR OPERACIONAL

Roles de la IA en el Ecosistema de Comunicaciones

La IA no solo mejora las comunicaciones, sino que es un multiplicador de fuerza (Force Multiplier) esencial para gestionar la complejidad y la velocidad del ciberespacio moderno, un ámbito que supera la capacidad de respuesta humana.

a. Optimización: La IA puede ajustar parámetros del sistema y del protocolo en tiempo real para mejorar el rendimiento de la red y el uso del ancho de banda.

b. Análisis Predictivo: Utiliza modelos de Machine Learning para prever fallos de hardware, congestión de la red o la trayectoria de un ataque cibernético.

c. Automatización de la Defensa: Permite que los sistemas tomen decisiones defensivas a velocidad de máquina, sin intervención humana, para bloquear amenazas instantáneas.

IA para la Gestión Dinámica del Espectro Electromagnético (EEM)

En un entorno operacional congestionado o sujeto a Guerra Electrónica (GE), la IA es crítica para garantizar la disponibilidad de las comunicaciones.

1. Asignación Automática: Los algoritmos de IA analizan las condiciones del espectro en tiempo real (interferencias, ruido, actividad enemiga) y pueden cambiar dinámicamente las frecuencias, los niveles de potencia o los protocolos de transmisión para evitar la interceptación o la interferencia activa (jamming) enemiga, manteniendo el enlace de comunicación.

2. Optimización de Enrutamiento: La IA evalúa la robustez, seguridad y latencia de múltiples vías de comunicación (radio, satélite, redes cableadas, etc.) y selecciona automáticamente la ruta más óptima y menos susceptible de ser interceptada o degradada en función de las condiciones operativas cambiantes.

IA en Ciberseguridad: Defensa Predictiva

La IA transforma la ciberdefensa de un modelo reactivo (responder al daño ya ocurrido) a uno predictivo (prevenir el ataque antes de que se complete).

a. Detección de Comportamiento (UEBA - User and Entity Behavior Analytics): La IA aprende y perfila los patrones normales de actividad (tráfico, acceso a archivos, comandos) para cada usuario y dispositivo. Una desviación sutil, como un acceso inusual a un servidor a las 3:00 AM o una transferencia de datos de gran volumen a una ubicación atípica, se marca como comportamiento anómalo y posible amenaza antes de que un ataque tradicional basado en firmas se formalice.

b. Fusión de Inteligencia: La IA combina y correlaciona datos de alerta de múltiples sensores (IDS/IPS, firewalls, honeypots, logs de EEM) para crear una imagen de alerta unificada. Esto proporciona al Mando una alerta temprana

consolidada y priorizada, acelerando la capacidad de respuesta táctica al pasar de manejar miles de alertas aisladas a una única "verdadera" amenaza.

RESPUESTA Y CONTINUIDAD OPERACIONAL CIBERNÉTICA

Plan de Respuesta a Incidentes Cibernéticos (PRIC)

El PRIC es un documento táctico esencial que detalla los pasos predefinidos y los roles de cada unidad para gestionar un incidente, asegurando una respuesta coherente, rápida y eficaz.

Contención: Es el paso más crítico inmediatamente después de la detección. Su objetivo es detener la propagación del ataque. Esto puede incluir el aislamiento del sistema afectado de la red, la desactivación de cuentas comprometidas o el bloqueo de direcciones IP maliciosas en el firewall.

Erradicación y Recuperación: Una vez contenido, el equipo elimina la causa raíz del incidente (p. ej., el malware o la vulnerabilidad explotada) y luego restaura los servicios y los sistemas a su estado operativo normal y seguro, idealmente utilizando imágenes y configuraciones limpias y probadas.

Coordinación: Asegurar que la información del incidente sea comunicada oportuna y con precisión a la cadena de mando, los equipos de ciberdefensa superior y las unidades afectadas, siguiendo el formato de reporte preestablecido.

Recuperación de Desastres y Respaldo de Información Crítica

La capacidad de continuidad operacional depende de la redundancia y de la gestión de backups.

a. Estrategia 3-2-1: Se debe implementar una estrategia de respaldo de información que incluya copias de datos, configuraciones y software operativo. La regla general es tener al menos tres copias de los datos, en dos tipos diferentes de medios de almacenamiento, con una copia almacenada fuera de sitio.

b. Almacenamiento Fuera de Línea (Off-line) y Fuera de Sitio (Off-site): El almacenamiento off-line (no conectado a la red, como cintas o discos externos físicamente desconectados) es vital para proteger contra el ransomware que puede cifrar o destruir los backups en línea. El almacenamiento off-site asegura la disponibilidad en caso de destrucción física del centro de comunicaciones.

Deberes del Operador ante la Sospecha de Intrusión

Las acciones inmediatas del Operador de Comunicaciones son cruciales para el éxito de la investigación forense posterior.

a. No apagar el equipo: Si se sospecha de compromiso, jamás se debe apagar o reiniciar el equipo a menos que se indique específicamente en el PRIC. Apagarlo resulta en la pérdida inmediata de la memoria volátil (RAM). Esta RAM contiene la evidencia forense vital del ataque: procesos en ejecución, conexiones de red activas, claves de cifrado y malware sin cifrar.

b. Aislar la conexión: La acción prioritaria es la contención. Se debe desconectar el equipo de la red de comunicaciones, ya sea retirando el cable de red (desconexión física) o deshabilitando la interfaz de red (desconexión lógica). Esto corta la comunicación entre el atacante y el malware, impidiendo la exfiltración de datos o la propagación.

c. Reportar inmediatamente: La urgencia del reporte debe ser prioritaria, detallando de forma precisa la anomalía (hora, sistema afectado, acción tomada) al Oficial de Comunicaciones y a la Unidad de Ciberdefensa, para iniciar el protocolo establecido en el PRIC.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO IX

COMUNICACIONES ALTERNATIVAS

1. GENERALIDADES

En el contexto militar, las Comunicaciones Alternativas se refieren a aquellos sistemas y medios que complementan o sustituyen a las comunicaciones principales (como las redes de radio y satélite cifradas de alta tecnología) para asegurar el flujo de información en el campo de batalla, especialmente cuando los sistemas primarios fallan o son interceptados/interferidos. Estas comunicaciones son cruciales para el Mando y Control en todos los niveles operativos.

2. TIPOS DE COMUNICACIONES MILITARES

Las comunicaciones militares abarcan una amplia gama, y las alternativas se encuentran a menudo en el nivel táctico (donde se desarrolla la acción directa).

a. Sistemas Principales (Convencionales):
   1) Radio Frecuencia (RF): Bandas HF, VHF y UHF (muchas con tecnología de radio definida por software - SDR).
   2) Comunicaciones por Satélite (SATCOM): Esenciales para enlaces de largo alcance y estratégicos.
   3) Redes Móviles Ad Hoc (MANETs): Redes descentralizadas y autoconfigurables que utilizan nodos (vehículos, soldados, drones).
   4) Telecomunicaciones Alámbricas: Cables de fibra óptica o alambres para enlaces de comando fijos o semi-permanentes.

b. Comunicaciones Alternativas o de Respaldo:
   1) Mensajería Física: El uso de mensajeros a pie, en vehículo o incluso con animales (históricamente, aunque menos común hoy) es la forma más básica de respaldo.

2) Medios Acústicos: Uso de códigos preestablecidos mediante silbatos, bocinas, campanas o incluso disparos controlados. Su alcance es limitado y se usa en fracciones pequeñas.
3) Medios Visuales:
   a) Señalización con Banderines (Semáforo): Un método antiguo, pero de respaldo.
   b) Gestos y Señales de Manos: Para comunicación silenciosa y de corta distancia entre unidades.
   c) Dispositivos de Señalización Visual: Como bengalas, pirotecnia, o luces codificadas (infrarrojas, etc.).
4) Sistemas de Campaña y Provisionales: Uso de líneas de teléfono de campaña (ej. el TA-43 que reemplazó al EE-8), o el tendido rápido de cables para comunicaciones telegráficas o telefónicas provisionales.
5) Radios de Alta Frecuencia (HF): Pueden servir como respaldo de largo alcance cuando el SATCOM no es viable, aunque su calidad y disponibilidad dependen de las condiciones atmosféricas.

3. IMPORTANCIA DE LAS COMUNICACIONES ALTERNATIVAS

La necesidad de sistemas alternativos radica en la resiliencia y seguridad:

a. Redundancia: Asegurar que la comunicación no se pierda si la red principal falla o es destruida.
b. Operaciones en Entornos Denegados: Cuando el enemigo emplea Guerra Electrónica (jamming o perturbación de frecuencia) que inhabilita los radios principales.
c. Sigilo/Silencio de radio: Para evitar la intercepción o localización del emisor, e recurre a comunicaciones no electrónicas o a protocolos estrictos de silencio de radio complementados con códigos de gestos.
d. Bajo Nivel Táctico: En el nivel de pelotón o escuadra, la comunicación puede ser puramente visual o acústica para mantener el sigilo.

SECCIÓN A

LAS COMUNICACIONES MILITARES ALTERNATIVAS

Las comunicaciones militares alternativas son sistemas de respaldo que permiten la transmisión de información a pesar de fallas o interferencias en los sistemas principales, utilizando tecnologías como radios tácticas con salto de frecuencia, satélites comerciales o de banda ancha, y redes de comunicaciones encriptadas. El objetivo es asegurar la resiliencia y continuidad de las comunicaciones en el campo de batalla para el mando y control.

1. TIPOS Y TECNOLOGÍAS
    a. Radios tácticas: Utilizan tecnologías como el espectro ensanchado y el salto de frecuencia para evitar interferencias y garantizar líneas de comunicación seguras. Las radios definidas por software (SDR) permiten ajustar frecuencias sobre la marcha para mayor adaptabilidad.

    b. Sistemas de satélites: Constelaciones de satélites comerciales o militares ofrecen cobertura global, alta velocidad y baja latencia, incluso en zonas remotas y disputadas. Su gran número proporciona redundancia, lo que asegura la comunicación continua incluso si algunos satélites fallan.

    c. Criptografía: Es el estudio y uso de métodos de codificación para asegurar que los mensajes solo puedan ser leídos por el destinatario previsto.

    d. Redes integradas: Se busca pasar de sistemas de comunicación aislados a un enfoque más interconectado, donde soldados, centros de mando y plataformas no tripuladas formen parte de una red cohesionada en tiempo real.

    e. Alfabeto militar o fonético: Se usa para deletrear letras y números por radio de manera clara, reduciendo malentendidos, especialmente en entornos ruidosos.

2. IMPORTANCIA

a. Continuidad: Las comunicaciones alternativas son cruciales para garantizar la continuidad de las operaciones militares.

b. Resiliencia: Proporcionan la capacidad de seguir operando incluso cuando los sistemas principales son vulnerables a ataques o fallas.

c. Flexibilidad: Permiten adaptar la comunicación a diferentes escenarios en el campo de batalla.

3. DESAFÍOS

a. Guerra electrónica: Las transmisiones de radio son vulnerables a la interceptación, monitoreo e interferencia.

b. Costos y despliegue: La adopción de nuevas tecnologías enfrenta desafíos en cuanto a costos y procesos de adquisición.

c. Integración: Es necesario integrar los nuevos sistemas con las redes militares existentes para lograr una comunicación más efectiva.

SECCIÓN B

¿QUÉ SON LAS COMUNICACIONES MILITARES ALTERNATIVAS (CMA)?

Las Comunicaciones Militares Alternativas son sistemas, métodos o procedimientos de comunicación que se emplean cuando las vías de comunicación principales (redes de radio e infraestructura de telecomunicaciones habituales) están comprometidas, inutilizables o no disponibles debido a condiciones de combate, fallas técnicas, daño físico, condiciones climáticas extremas o desastres. Las CMA buscan garantizar la continuidad operativa, la transmisión de información crítica y la coordinación entre unidades militares en escenarios donde la comunicación estándar no es fiable.

1. EN TÉRMINOS PRÁCTICOS, LAS CMA PUEDEN INCLUIR:
   a. Métodos de transmisión fuera de la banda normal, con tecnologías redundantes o improvisadas.
   b. Procedimientos de mando y control que dependen menos de la infraestructura de red.
   c. Soportes físicos o análogos (por ejemplo, mensajería terrestre o aérea) para mantener el flujo de información.

2. IMPORTANCIA DE LAS CMA
   a. Continuidad operativa: aseguran que las órdenes, el estado de situación y la inteligencia sigan disponibles durante fallos de red o ataques electrónicos.
   b. Resiliencia: aumentan la capacidad de respuesta ante ambos, interrupciones y degradación de la red.
   c. Redundancia estratégica: reducen la dependencia de un único medio de comunicación.
   d. Supervivencia en combate: permiten a las fuerzas mantenerse coordinadas en entornos de alta amenaza y destrucción de infraestructura.
   e. Seguridad y confidencialidad: algunas CMA pueden incluir métodos de bajo perfil o sigilosos que evitan la detección electrónica.

3. EJEMPLOS Y TIPOS DE CMA

Las CMA pueden clasificarse por distintos criterios: tecnología, medio de transmisión, y alcance. A continuación, se presentan ejemplos representativos:

   a. Por tecnología o medio de transmisión
      1) Mensajería física o manual: mensajeros, cabos de fibra improvisados, señales con luces (fónicas), banderas, señales ópticas y mensajería escrita.
   b. Referencias y contactos en tablero: tarjetas de información operativa, pizarras móviles, símbolos visuales.

c. Codificación y encriptación alternativa: sistemas de cifrado no convencionales o redundantes para evitar la intercepción.
d. Reducción de dependencia de radio: uso de líneas telefónicas terrestres, radio de corto alcance o equipos de baja probabilidad de detección.
e. Señalización visual y acústica: faroles, bengalas, silbatos, señales acústicas, semáforos temporales en el campo.
f. Mensajería aeronáutica y terrestres de corto alcance: aviones, helicópteros o vehículos para transportar órdenes y datos de forma directa.
g. Comunicaciones satelitales alternativas: uso de satélites no convencionales, frecuencias fuera de la banda normal, o servicios comerciales cuando estén disponibles y seguros.
h. Redes ad hoc y de campo: redes improvisadas entre unidades (mesh networks) es un sistema de Wi-Fi que utiliza múltiples nodos para crear una red única que cubre un área más amplia, en contraste con un único router tradicional. Los nodos trabajan juntos para transmitir la señal, lo que resulta en una cobertura más uniforme, velocidades más rápidas y una conexión más fiable en toda la casa. Las redes en malla permiten el "roaming" sin interrupciones entre nodos y tienen la capacidad de "auto-repararse" redirigiendo el tráfico si un nodo falla. con capacidades limitadas pero útiles en proximidad.

4. POR ALCANCE
   a. CMA de corto alcance: dentro de una unidad o entre escuadrones cercanos.
   b. CMA de alcance medio: entre brigadas o cuerpos cercanos.
   c. CMA de gran alcance: interunidades o entre teatros de operaciones, donde la comunicación suele ser más compleja y menos confiable.
5. POR CONTEXTO OPERACIONAL
   a. Operaciones bajo interrupción de energía o infraestructura: sistemas que funcionan sin electricidad estable o con fuentes alternativas.

b. Operaciones en entornos de alto riesgo de interceptación: métodos que minimizan la detección enemiga.

c. Desastres naturales o emergencias civiles: coordinación entre fuerzas militares y autoridades para gestión de crisis.

6. GLOSARIO DE TÉRMINOS CLAVE

a. CMA: Comunicaciones Militares Alternativas.

b. Mando y Control (M&C): proceso de dirección, toma de decisiones y ejecución de órdenes.

c. Red redundante: una red alternativa que entra en juego cuando la principal falla.

d. Cifrado/Encriptación: procesos para transformar información para que solo destinatarios autorizados puedan entenderla.

e. Mesh network (red en malla): red de dispositivos que se conectan entre sí de forma descentralizada para compartir información.

f. Interferencia electrónica: acciones que dificultan o bloquean las comunicaciones.

g. Resiliencia operativa: capacidad de mantener operaciones pese a adversidades.

h. Comunicaciones fuera de banda: canales que no forman parte de la red principal de comunicaciones.

i. Seguridad de la información: prácticas para proteger la confidencialidad, integridad y disponibilidad de la información.

7. FACTORES A CONSIDERAR AL DISEÑAR CMA

a. Disponibilidad y confiabilidad de medios alternativos: qué tan frecuentes y robustos son frente a fallos.

b. Tiempo de implementación: cuán rápido se pueden activar las CMA en una operación.

c. Capacidad de encriptación y seguridad: asegurar que la información siga siendo confidencial.

d. Entrenamiento y procedimientos: disponibilidad de tropas capacitadas y procedimientos claros para cambiar a CMA.

e. Compatibilidad operativa: coherencia entre CMA y el plan de Mando y Control.

f. Riesgos y limitaciones: posibles retrasos, malentendidos o pérdida de información con CMA.

g. Implementación y prácticas recomendadas

h. Plan de contingencia: incluir CMA como parte de los planes operativos y ejercicios de simulación.

i. Pruebas regulares: ejercicios de para verificar tiempos de activación y confiabilidad.

j. Procedimientos de seguridad: protocolos para el manejo seguro de métodos alternativos.

k. Capacitación continua: entrenamiento de personal en uso de CMA, incluyendo señalización, reconocimiento de códigos y protocolos de emergencia.

l. Documentación clara: manuales y tarjetas de referencia rápida para cada método CMA.

m. Coordinación interagencial: colaboración con otros cuerpos y agencias para asegurar interoperabilidad cuando se necesite.

8. DESAFÍOS Y LIMITACIONES

a. Capacidad limitada: CMA tiende a ofrecer menor ancho de banda y mayor latencia que las redes principales.

b. Riesgo de ambigüedad: malentendidos si no se estandarizan las señales y códigos.

c. Dependencia de entrenamiento: requieren práctica frecuente para eficacia real.

d. Propagación de errores: fallos en CMA pueden generar órdenes erróneas si no se verifica adecuadamente.

e. Interoperabilidad: diferencias entre fuerzas aliadas pueden dificultar la cooperación.

SECCIÓN C

ESTACIÓN DE RADIO COMUNITARIAS

GENERALIDADES

1. MARCO HISTÓRICO

Bisbal (1991) relata que en 1924 llega la radio a Venezuela, durante el mandato del general Juan Vicente Gómez. Ese mismo año, el Gobierno nacional otorgó la primera licencia para operar. Sin embargo, es en 1926 cuando el coronel Arturo Santana, junto con el coronel Roberto Scholtz y Alfredo Moller, crean la primera estación en el país, muy ligada al régimen imperante, que se llamó AYRE. En 1930, comienza a transmitirse programación regular a través de la estación 1-BC (Broadcasting Caracas), que representa el inicio de la radio comercial y privada en Venezuela.

En el período comprendido entre 1932 y 1936 se fundaron en el país las siguientes estaciones: Radiodifusora de Venezuela, Voz de Carabobo, Radiodifusora Maracaibo, Radio Libertador, La Voz del Táchira, Ecos del Zulia, Radio Valencia, Radio Valera, Ondas del Lago, Radio Popular, Radio Continente, Radio Coro, Radio Barquisimeto, Ecos del Orinoco, Radio Puerto Cabello, La Voz de la Fe, La Emisora Vargas y Radio Nacional, durante el gobierno del general Eleazar López Contreras, como servicio radiofónico oficial del Estado venezolano. A finales de la década de los cincuenta aparecen en el país los circuitos de radiodifusión.

El antiguo Ministerio de Transporte y Comunicaciones intentó democratizar el espectro de la banda FM. Sin embargo, en la práctica la democratización de los medios no se pudo ejecutar, porque los dueños de las estaciones AM tenían la

experiencia y los recursos económicos necesarios para la instalación de las nuevas estaciones FM.

Las concesiones FM se distribuyeron a grupos económicos de gran importancia en el país: el grupo Cisneros logró tramitar siete concesiones correspondientes a las emisoras Hot 94.1 (Rodolfo Rodríguez), 88.9 (Luis Chávez), 99.9 (Antonio Cerfati), 102.3 (Rosa Rodríguez y posteriormente Nelson Belfort), 96.3 (Mirla Castellanos) y 107.3 (Enrique Cuscó). El grupo Phelps sólo tuvo dos concesiones: la primera fue Caracas 92.9 (Peter Bottomey Armando Guía) y Ritmo 95.5 (Carlos Falkenhagen). De igual manera, el Grupo Capital gozaba de dos concesiones: la de Capital 104.5 (Radamés Lebrón y posteriormente Peter Taffin) y KYS 101.5 (Oswaldo Yépez). También se otorgó un permiso al Circuito Mundial. Sin embargo, también hubo concesiones que se otorgaron a particulares. Tal es el caso de Ávila 91.9, Suave 89.7, Imagen 88.1, Ambiente M. de Caracas 105.3, Radio Nacional (aún pertenece al Estado), Emisora Cultural de Caracas 97.7 y la radio de la Fundación Casa del Artista 96.3.

Las radios en Venezuela representan el primer medio de comunicación del país, por ser el de mayor inmediatez y democratización. La radio es un medio que agrupa a importantes tipos de audiencia, debido a que la segmentación del espectro ofrece programación para todos los gustos.

Las radios comunitarias, desde sus inicios en América Latina en la década de los setenta, han contribuido de manera directa en el ejercicio de la libertad de expresión de todos los miembros de las comunidades y de las organizaciones colectivas comprometidas con proyectos de interés social. Son medios que fueron concebidos como radios con fines políticos. Sin embargo, a mediados de los años ochenta, su misión original fue transformada y se convirtieron en radios abiertas a la participación popular, al servicio de las comunidades.

Datos oficiales de la Comisión Nacional de Telecomunicaciones (Conatel) confirman que en el país operan de forma legal 272 radios comunitarias, a pesar de las limitaciones que existen en el espectro radioeléctrico venezolano.

La mayoría de las radios comunitarias en Venezuela están ubicadas en zonas populares, lo que “permite la participación activa y autónoma de las personas residentes en la localidad, de representantes de movimientos sociales y de otras formas de organización colectiva en la programación, en los procesos de creación, en el planteamiento y en la gestión de la emisora. Por último, se basa en principios de la comunicación liberadora que tiene como norte la ampliación de la ciudadanía. Ella se inculca, perfecciona y recrea el conocimiento generado por la comunicación popular, comunitaria y alternativa en el contexto de los movimientos sociales en América Latina desde las últimas décadas del siglo XX”

Las radios comunitarias son productos de los procesos históricos en el mundo. La aparición de estos medios está asociada a los avances tecnológicos: el surgimiento de la tecnología FM, por ejemplo, abarató los costos para establecer una estación radial. Pero es preciso destacar que existen distintas visiones del significado del término “comunitario” en los medios de comunicación.

Las radios comunitarias causan un efecto en los sectores donde se ubican, a pesar de que en muchas de ellas la programación se basa mayoritariamente en música. Simplemente, se desarrolla dentro de la colectividad un sentido de orgullo y pertenencia hacia la radio. Ese sentido de pertenencia se alimenta a través de la difusión de anuncios y dedicatorios alusivos a la colectividad.

No obstante, uno de los principales peligros que corren los medios comunitarios es caer en la centralización de la programación por el mandato de la persona o fundación que dirige el medio. “La radio comunitaria no debe tener dueño, debe

pertenecer a la comunidad. En última instancia, la radio comunitaria típica es aquella que los vecinos reconocen como suya y por eso la protegen y participan en ella activamente" (Contratexto, 2006, p. 201).

Las comunitarias, no sólo en América Latina sino en el mundo, son vistas como instrumentos de desarrollo social, que reciben apoyo de los gobiernos, así como también de la Iglesia, Organizaciones no Gubernamentales e instituciones educativas.

El financiamiento de las radios comunitarias es uno de los puntos que ha generado mayor discusión dentro de la Comisión de Apoyo Técnico y Logístico de Conatel, por ser el despacho encargado del área de comunicaciones alternativas y comunitarias para radio y televisión en Venezuela.

El mantenimiento de las radios comunitarias es el principal reto que emprenden todas las fundaciones comunitarias luego de haber obtenido la licencia para operar en la frecuencia otorgada por el organismo regulador.

El financiamiento de estas radios es un tema que no sólo preocupa a quienes deben mantenerla sino también a los representantes de Conatel. El ingeniero Jackson Lobo, de la Comisión de Apoyo Técnico y Logístico de Medios Alternativos y Comunitarios, considera que debido al crecimiento acelerado que ha tenido este sector en los últimos cuatro años, ha sido imposible poder mantener un control adecuado sobre las 272 radios comunitarias que operan en el país, si se toma en cuenta que esta comisión está conformada por 17 personas para todo el territorio nacional.

2. CONCEPTOS BÁSICOS.

Una radio comunitaria es una estación de transmisión de radio que ha sido creada con intenciones de favorecer a una comunidad o núcleo poblacional y

cuyos intereses son el desarrollo de su comunidad. Dichas estaciones carecen de ánimo de lucro (lo que las diferencias de las radios piratas) aunque algunas se valen de patrocinios de pequeños comercios para su mantenimiento.

Varias estaciones de radio comunitarias, además de hacer transmisión radial vía antena, también lo hacen a través de Internet. Junto al resto de medios comunitarios forman parte del llamado tercer sector de la comunicación (siendo el primer sector los medios públicos, y el segundo los medios privados comerciales).

Comunidad: Conjunto de personas que residen o se encuentran domiciliadas en una localidad y que Conatel determina que se encuentran estrechamente vinculadas en razón de su problemática común y de sus características históricas, geográficas, culturales y tradicionales.

Esto quiere decir que para que un conjunto de personas sea considerado como una comunidad, por precepto de la normativa, Conatel debe someterla a una serie de variables para determinar su término de comunidad a posteriori.

Fundación comunitaria: Fundación de corte democrático, participativo y plural, constituida de conformidad con las previsiones establecidas en el Código Civil, cuyo objeto específico, exclusivo y excluyente consiste en asegurar la comunicación libre y plural de los miembros de una comunidad en una localidad

determinada, y que cumple con los requisitos exigidos por el reglamento para ostentar tal carácter.

Localidad: Zona de cobertura de un servicio de radiodifusión sonora comunitaria o televisión abierta comunitaria, de conformidad con la determinación que al efecto realice Conatel.

Período de transmisión: Tiempo de duración diaria de la programación emitida por la estación del servicio de radiodifusión sonora comunitaria o televisión abierta comunitaria.

Productor comunitario: Persona natural o jurídica que produce contenidos sonoros o audiovisuales, que ha sido formada y acreditada como productor comunitario por un operador de servicios de radiodifusión sonora comunitaria o televisión abierta comunitaria y que no está vinculada con ningún operador de radiodifusión sonora y televisión abierta.

Productor independiente: Persona natural o jurídica que produce contenidos sonoros o audiovisuales, que no ha sido acreditado como productor comunitario por un operador de servicios de radiodifusión sonora comunitaria o televisión abierta comunitaria y que no está vinculada con ningún operador de radiodifusión sonora y televisión abierta.

Producción comunitaria: Producción sonora o audiovisual elaborada por una fundación comunitaria o un productor comunitario, incluyendo su participación en todas las fases de elaboración, tales como la escritura, preproducción, producción y postproducción de la obra.

Operador comunitario: Fundación comunitaria habilitada para la prestación de los servicios de radiodifusión sonora comunitaria o televisión abierta comunitaria.

El artículo 5 contempla, por su parte, los requisitos que debe cumplir la fundación comunitaria para obtener una habilitación:

1. Capacidad e idoneidad legal del solicitante para la realización de la actividad.

2. Carácter de fundación comunitaria, en los términos establecidos en el Capítulo III del reglamento.

3. Carácter democrático, participativo y plural del proyecto.

4. Viabilidad económica del proyecto.

5. Disponibilidad del espectro radioeléctrico, en los términos del artículo 11 del reglamento.

7. Perfil social del proyecto.

8. Demás requisitos y condiciones previstas en la Ley Orgánica de Telecomunicaciones y sus reglamentos.

La zona de cobertura de los medios de comunicación comunitarios se limita al espacio geográfico de la localidad representada por la fundación comunitaria. El reglamento establece en el artículo 6 que Conatel “determinará las localidades en las cuales se prestarán los servicios”. Esos límites geográficos se representan por cada parroquia; es decir, cada una de estas circunscripciones debería tener un medio de comunicación comunitario.

3. CARACTERÍSTICAS.

a. La radio comunitaria defiende la democracia y respeta la pluralidad de opiniones.
b. Trabaja para solucionar los problemas sociales de las comunidades y desarrollar la educación, la ciencia, la cultura y el deporte.
c. Se ocupa de promover tanto los conocimientos como las actividades del colectivo.
d. Permite a los ciudadanos expresar sus ideas y promoverlas.
e. Sin fines de lucro: A diferencia de las radios comerciales, su objetivo principal no es generar ganancias, sino servir a la comunidad.
f. Gestión comunitaria: Su administración recae en los miembros de la comunidad, a menudo a través de consejos comunales.

g. Alcance local: Suelen transmitir en un área geográfica específica, respondiendo a las necesidades y particularidades de su entorno.
h. Enfoque participativo: Fomentan la participación ciudadana, permitiendo que la comunidad sea productora de contenidos y no solo receptora de información.
i. Función social y cultural: Sirven como espacio para la difusión de expresiones culturales locales, el debate de ideas, la educación y la defensa de derechos.
j. Representación de intereses: Actúan como mediadoras entre la comunidad y las instancias de poder, y visibilizan a sectores a menudo ignorados por los medios masivos.

SECCIÓN D

RADIOAFICIONADOS

GENERALIDADES

1. DEFINICIÓN

Los radioaficionados son aquellas personas naturales o jurídicas sin fines de lucro u organismos gubernamentales debidamente autorizados, cuya actividad tiene por objeto la instrucción individual, la intercomunicación y los estudios técnicos de la radiotecnia, técnica relativa a la telecomunicación por radio, así como a la construcción, manejo y reparación de aparatos emisores o receptores.

El Servicio de Radioaficionados es un servicio de radiocomunicación universal que tiene por objeto la instrucción individual, la intercomunicación y los estudios técnicos efectuados por personas debidamente habilitadas que se interesan en la radiotecnia con carácter exclusivamente personal y sin fines de lucro.

También se consideran dentro de este servicio, aquellas personas que utilizan estaciones espaciales situadas en satélites de la tierra para los mismos fines enunciados.

Los términos técnicos usados en este Reglamento tendrán el significado que se le atribuye en las reglas de la Unión Internacional de Telecomunicaciones (U.I.T.)

Los radioaficionados son personas autorizadas que se interesan en la radiotecnia para comunicarse, experimentar y realizar estudios técnicos sin fines de lucro. Se conectan con otros radioaficionados de todo el mundo a través de frecuencias de radio designadas y también ofrecen un servicio social valioso en situaciones de emergencia, ya que sus equipos están listos para operar cuando fallan otras telecomunicaciones. La actividad requiere una licencia para operar, la cual se obtiene tras demostrar conocimientos sobre la materia.

a. Actividades

   Instrucción e intercomunicación: Los radioaficionados realizan comunicaciones personales e interconectan con otros entusiastas alrededor del mundo.

b. Estudios técnicos y experimentación: Se interesan en la radiotecnia, lo que puede incluir la construcción y el diseño de equipos, y la experimentación con la transmisión de voz, datos e imágenes.
c. Servicios de emergencia: Juegan un papel crucial como sistema de comunicación de reserva durante desastres naturales u otras emergencias, cuando las redes convencionales fallan.
d. Radiogoniometría: Se trata de un deporte y una actividad de localización de transmisores ocultos utilizando receptores y mapas.

2. TIPOS DE PERMISOS

a. Se otorgará un (1) único permiso a cada radioaficionado, el cual habilita a su titular para poseer, instalar u operar equipos o Estaciones de Radioaficionados, en las bandas autorizadas según la categoría del permiso respectivo, el cual deberá ser presentado al serle requerido por las autoridades competentes. Los permisos otorgados a un Radioaficionado luego de haber cumplido con todos los requisitos establecidos en la Ley Orgánica de Telecomunicaciones, en el Reglamento de Radioaficionados y en el Instructivo para tal fin. Pueden ser clasificados en:

1) Radioaficionado Categoría “A”

Persona natural que haya aprobado el examen realizado por la Comisión Nacional de Telecomunicaciones, mediante el cual se verifica su idoneidad para realizar la actividad de Radioaficionado. El permiso tiene una vigencia no mayor a cinco (5) años.

2) Radioaficionado Categoría “B”

Radioaficionado u Organización de Radioaficionados que haya cumplido con los requisitos establecidos en la Ley Orgánica de Telecomunicaciones, este Reglamento y las demás normas aplicables. El permiso tiene una vigencia no mayor a cinco (5) años.

b. Todo permiso podrá ser revocado en cualquier momento mediante Resolución del Ministerio de Transporte y Comunicaciones debidamente motivada, de conformidad con lo establecido en la Ley que rige la materia y demás leyes aplicables.

3. ASPECTOS CLAVE

a. Autorización y licencia: Para operar, es necesario obtener una licencia de la autoridad reguladora correspondiente, que puede involucrar exámenes para demostrar los conocimientos técnicos.

b. Frecuencias asignadas: Operan en bandas de radiofrecuencia asignadas por organismos como la Unión Internacional de Telecomunicaciones (UIT) y las autoridades nacionales.
c. Organización: A menudo se asocian en clubes de radioaficionados, que son organizaciones no lucrativas que también ofrecen cursos de formación.
d. Alcance mundial: La comunidad de radioaficionados es global, con millones de operadores en casi todos los países del mundo.

4. DE LA OPERACIÓN DE LAS ESTACIONES DE RADIOAFICIONADOS

Las Estaciones de Radioaficionados solo serán operadas en el territorio de la República por personas debidamente habilitadas por el Conatel y en consecuencia, el titular de un permiso no debe permitir que persona alguna opere su estación sin el permiso correspondiente.

Las frecuencias atribuidas al Servicio de Radioaficionados podrán ser utilizadas en el territorio de la República, por todas aquellas personas debidamente habilitadas por el Conatel mediante el permiso de instalación y operación correspondiente, siempre que el mismo se encuentre vigente. Así mismo, las frecuencias deberán ser utilizadas de acuerdo con la categoría del permiso otorgado y acatando lo establecido en la Ley vigente sobre la materia. En tal sentido, no se asignarán frecuencias a su servicio para uso distinto del propio de la actividad, ni para uso exclusivo de particulares o instituciones de manera temporal ni permanente.

Todo operador deberá identificar sus transmisiones al iniciar y finalizar su comunicación y regularmente después de los primeros diez (10) minutos, por medio del distintivo de llamada asignado en su permiso vigente, haciendo uso del código fonético internacional o códigos aceptados internacionalmente.

Cuando un radioaficionado opere una estación habilitada a una organización, desde su sede y en nombre de esta, deberá identificarla por medio del distintivo de llamada asignada a ella, seguido de la frase, “operada por” y el distintivo de llamada señalado en su permiso vigente. En todo caso, solo podrá ser operadas bandas, modos y potencias autorizadas para la categoría del permiso que posee el operador. En caso de eventos especiales, solo se identificará el operador que haga uso de la estación, con distintivo de llamada.

Las comunicaciones entre Estaciones de Radioaficionados deben utilizarse utilizando un lenguaje claro y correcto, acatando las normas de cortesía y buenas costumbres.

Sé prohíbe la transmisión de anuncios publicitarios, mención o propagandas comerciales, religiosas o políticas, música, discursos o conferencias que no sean de carácter técnico, así como todas aquellas comunicaciones que de una u otra forma puedan atentar contra la seguridad del Estado, el orden político, la moral y las buenas costumbres.

Una vez habilitada y en operación, una estación repetidora o radioenlace solo podrá ser mudada, apagada o modificado su régimen de uso con autorización expresa del Ministerio de Transporte y Comunicaciones, o cuando las causas lo justifiquen, debiendo ser consignadas las pruebas correspondientes durante los diez días hábiles siguientes ante la Comisión Nacional de Telecomunicaciones (CONATEL)

El titular de un permiso se compromete a tomar las medidas necesarias para la operación de los equipos de que dispone sea tan pura y libre de emisiones no esenciales hasta donde lo permita la técnica, a fin de no interferir a otras estaciones o servicios por mal funcionamiento o inadecuada instalación de la misma.

Ninguna Estación de Radioaficionados podrá usarse enlazada ni servir de intermediaria o relevo de estaciones de otros servicios de telecomunicaciones, excepto en caso de emergencia nacional.

5. DE LOS DISTINTIVOS DE LLAMADA

Los distintivos de llamada asignados al Servicio de Radioaficionados estarán conformadas por dos (2) letras, o combinaciones de dígito y letra correspondiente a uno de los prefijos asignado a Venezuela por la Unión Internacional de Telecomunicaciones (U.I.T.), seguidas de un número del cero (0) al nueve (9) que designa el circuito radioeléctrico donde está ubicada la estación fija y de una (1), dos (2) o tres (3) letras denominadas sufijo.

Los prefijos serán designados de acuerdo a la categoría del permiso de instalación y operación de Estaciones de Radioaficionados que posea el solicitante. A tales efectos, se establece la siguiente clasificación: CATEGORIAS PREFIJOS “B” “A” Prefijos Especiales YV YY 4M o YW.

Los circuitos radioeléctricos estarán distribuidos de la siguiente manera:

cero	(0)	ISLA DE AVES
Uno	(1)	FALCÓN, TRUJILLO Y ZULIA
Dos	(2)	BARINAS, MÉRIDA Y TÁCHIRA
Tres	(3)	LARA, PORTUGUESA Y YARACUY
Cuatro	(4)	ARAGUA, CARABOBO Y COJEDES
Cinco	(5)	DISTRITO FEDERAL, GUÁRICO, MIRANDA Y DEPENDENCIAS FEDERALES (EXCEPTO ISLAS DE AVES)
Seis	(6)	ANZOÁTEGUI Y BOLÍVAR
Siete	(7)	NUEVA ESPARTA Y SUCRE

Ocho	(8)	MONAGAS Y DELTA AMACURO
Nueve	(9)	APURE Y AMAZONAS

Se otorgarán permisos para instalar y operar una Estación de Radioaficionados desde Isla de Aves a los venezolanos con permisos categoría “B” vigente o a las organizaciones debidamente registradas, de acuerdo con el procedimiento que a tal efecto se establezca en el Instructivo Técnico Administrativo, solo se podrá otorgar a extranjeros, cuando se cumplan con los siguientes requisitos:

a. Autorización por parte de las autoridades militares competentes.
b. Tener vigente el permiso de su país de origen, y de conformidad con los convenios.
c. Estar avalados por una expedición perteneciente a una organización venezolana.

6. DE LOS EVENTOS ESPECIALES

El Ministerio de Transporte y Comunicaciones podrá otorgar el permiso correspondiente para la realización de concursos, festivales o cualquier otro evento especial a efectuarse en cualesquiera de las bandas atribuidas al servicio de radioaficionados, el cual deberá ser solicitado dentro de un plazo no menor de quince (15) días hábiles antes de la fecha prevista para el evento, anexando los recaudos solicitados al efecto.

La organización autorizada para la realización de un evento deberá cumplir con lo estipulado en el permiso correspondiente.

Una ver otorgado el permiso para la realización de un evento, sus responsables deberán informar suficientemente a través de las frecuencias autorizadas para aquel, el motivo, bases, responsable y demás informaciones inherentes.

Al momento de iniciar el evento, la Estación responsable estará en la obligación de informar a los participantes las bases y condiciones del mismo, en la frecuencia autorizada en el permiso.

7. DE LAS INSPECCIONES

El Ministerio de Transporte y Comunicaciones podrá inspeccionar cualquier Estación de Radioaficionados con el objeto de comprobar que se cumplan las disposiciones que rigen la materia, El inspeccionado deberá presentar la documentación y prestar toda la colaboración al funcionario inspector, el cual deberá estar debidamente acreditado como tal por el Ministerio de Transporte y Comunicaciones.

Toda inspección requiere de la elaboración de un acta la cual contendrá la plena identificación de las partes intervinientes, lugar y fecha donde se realiza, propósito de la inspección y los datos e informaciones referente a la Estación de Radioaficionados inspeccionada. Una copia del acta será entregada al inspeccionado al momento de finalizar el acto.

Cuando la autoridad competente compruebe que un transmisor o Estación de Radioaficionados causa interferencia a otros servicios o estaciones de telecomunicaciones por causas imputables a la estación, podrá ordenar el cese de sus transmisiones, hasta el momento en que aquellas sean eliminadas, sin perjuicio de las demás sanciones de conformidad con la Ley de Telecomunicaciones.

8. DE LAS SANCIONES

Quienes para la obtención del permiso de instalación y operación de Estaciones de Radioaficionados, se hubieren valido de datos o documentos falsos, incurrirán en la pena máxima de revocación del mismo, sin perjuicio de las demás disposiciones penales vigentes, quienes infrinjan lo establecido en la

Ley de Telecomunicaciones, Acuerdos Internacionales suscritos por la República, este Reglamento o cualquier otra disposición que se dicte sobre la materia, será sancionado de acuerdo con lo establecido en la legislación vigente sobre telecomunicaciones.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO X

ASPECTOS FUNDAMENTALES DE OPERACIONES ELECTROMAGNÉTICAS

SECCIÓN A

1. Generalidades
    a. Concepto de Operaciones Electromagnéticas

    Las operaciones electromagnéticas militares son actividades destinadas a explotar, atacar, proteger y gestionar el espectro electromagnético para obtener una ventaja militar. Estas operaciones se conocen como guerra electrónica (EW) e incluyen acciones para interferir o interrumpir las comunicaciones, la navegación y los radares del adversario, a la vez que protegen las propias.

2. División para su Aplicación:
    a. Ataque electromagnético:

    Operaciones ofensivas diseñadas para interrumpir o neutralizar los sistemas electrónicos enemigos. Ejemplos incluyen la interferencia de señales, el uso de pulso electromagnético (EMP) para desactivar dispositivos electrónicos y el uso de ciberataques para atacar la red del adversario.

    a) Ejemplos de aplicaciones

    - Interferencia de señales:

    Bloquear o interferir con las comunicaciones por radio o los sistemas de navegación del enemigo.

    La interferencia de señales es cualquier perturbación no deseada que altera una señal útil, ya sea electrónica, electromagnética o de radiofrecuencia. Esto puede degradar la calidad de la transmisión, causar fallos o incluso impedir completamente la recepción, afectando a dispositivos como radios, televisores, teléfonos inalámbricos y sistemas de comunicación en general. Las interferencias pueden ser causadas por señales de

radiofrecuencia, problemas eléctricos o la superposición de ondas, como en el caso del Wi-Fi.

Tipos de interferencia

- Interferencia electromagnética (EMI): Afecta a sistemas de comunicación, especialmente cuando las señales se transmiten por cables.
- Interferencia de radiofrecuencia (RFI): Es un tipo común de interferencia que puede afectar la recepción de señales de radio, TV y Wi-Fi.
- Superposición de ondas: Ocurre cuando dos o más ondas se encuentran en el mismo medio. Esto puede ser constructivo (refuerza la señal, como en los auriculares con cancelación activa de ruido) o destructivo (cancela la señal).

Ejemplos de interferencia

- Televisión y radio: La recepción de canales puede verse interrumpida, con la aparición de "nieve" o puntos en la pantalla del televisor.
- Comunicaciones inalámbricas: En un entorno con muchos dispositivos conectados, la interferencia puede reducir la capacidad de la red y causar conexiones lentas o inestables.
- Telefonía inalámbrica: Las interferencias pueden causar ruidos o cortes en la línea.
- Entornos sensibles: En hospitales, aeropuertos o centrales eléctricas, incluso una mínima interferencia puede tener consecuencias graves debido a la sensibilidad de los equipos.

Soluciones

- Filtros: Se pueden utilizar filtros, como los filtros LTE, para bloquear la interferencia no deseada y permitir solo los canales correctos.
- Blindaje de cables: Los cables con un blindaje adecuado pueden proteger las señales de la interferencia electromagnética y de radiofrecuencia.
- Gestión de canales (Wi-Fi): Elegir canales de Wi-Fi menos congestionados puede ayudar a minimizar la interferencia entre redes.
- Contacto visual y gestos: En un entorno de aula, los profesores pueden usar "interferencia de señales" no verbales para corregir un comportamiento sin interrumpir la clase.

La interferencia es un problema que afecta a muchas áreas de la tecnología y la comunicación, y su control es esencial para garantizar un rendimiento óptimo y seguro de los sistemas.

- Supresión de defensas aéreas enemigas (SEAD):

  Deshabilitar los radares y las defensas aéreas enemigas para permitir que las aeronaves propias operen sin ser detectadas.

  La supresión de defensas aéreas enemigas (SEAD, por sus siglas en inglés) es una operación militar para neutralizar o destruir sistemas antiaéreos enemigos, como misiles superficie-aire (SAM) y artillería, con el fin de obtener la superioridad aérea. Esto se logra mediante ataques directos con misiles antirradiación, contramedidas electrónicas (EW) y otras tácticas para degradar las capacidades de detección y ataque del enemigo, especialmente en las primeras fases de un conflicto.

  <u>Objetivos de la operación</u>

  - Neutralizar y destruir misiles superficie-aire (SAM) y artillería antiaérea del enemigo.

- Abrir el espacio aéreo para permitir el paso seguro de aviones de ataque y bombardeo.
- Degradar las capacidades de comunicación y detección del enemigo

Tácticas y métodos

- Misiles antirradiación (ARM):

  Misiles como el AGM-88 HARM que se guían hacia la fuente de emisión de radar del sistema enemigo.
- Contramedidas electrónicas (EW):

  Uso de señuelos como el MALD-J, que imitan las señales de los aviones para desviar la atención de los sistemas de defensa.
- Ataques directos:

  Bombardeos y cañonazos dirigidos a las ubicaciones de los radares y lanzadores de misiles.
- Tácticas de ataque:

  Operaciones se centran en el inicio de los ataques y, cuando es posible, se realizan ataques a distancia para evitar el alcance de las defensas de corto alcance.

Origen y desarrollo

- Orígenes: El concepto de SEAD tiene sus raíces en la Segunda Guerra Mundial, con el uso de bombarderos especializados para encontrar y atacar radares enemigos.
- Guerra de Vietnam: La necesidad de estas operaciones se hizo más evidente con la introducción de los misiles superficie-aire soviéticos en Vietnam del Norte.
- Desarrollo moderno: La sofisticación de los sistemas antiaéreos actuales hace que la misión de SEAD sea una prioridad constante en la guerra moderna.

Ejemplos históricos

- Guerra del Yom Kippur (1973):

Se analizó la estrategia israelí para hacer frente a los sistemas de defensa aérea de Egipto y Siria, aunque con resultados mixtos.

- Invasión de Irak (2003):

Se llevaron a cabo ataques SEAD contra las defensas iraquíes, aunque las armas de corto alcance representaron un peligro hasta las etapas finales del conflicto.

- Guerra de navegación (NAVWAR):

Falsificar o interferir con las señales de navegación, como el GPS, para confundir a los sistemas del adversario.

La Guerra de los Navegadores, una competencia por el dominio del mercado de navegadores web (históricamente entre Netscape Navigator e Internet Explorer, y más tarde con otros navegadores como Firefox y Chrome), o la NAVWAR (Guerra de Navegación), que es un dominio de la guerra electrónica enfocado en el uso militar de sistemas de posicionamiento, navegación y cronometraje por satélite, como el GPS.

Guerra de los Navegadores (Tecnológica)

Una competencia entre diferentes programas (navegadores web) para dominar el mercado de acceso a internet.

- Primera guerra (años 90):

Se libró principalmente entre Netscape Navigator y Microsoft Internet Explorer.

- Cómo terminó:

Microsoft integró Internet Explorer en su sistema operativo Windows, lo que le dio una gran ventaja y finalmente llevó a la desaparición de Netscape.

- Segunda guerra (desde 2004):

Incluyó a navegadores como Internet Explorer, Firefox y Google Chrome.

NAVWAR (Guerra de Navegación - Militar)

Un campo de la guerra electrónica que se enfoca en la competencia por el control de las señales de los sistemas globales de navegación por satélite (GNSS) como el GPS.

- En qué consiste: Es la capacidad de un bando para explotar, engañar, interrumpir o proteger los sistemas de navegación de su adversario.
- Ejemplos de tácticas: Se pueden usar bloqueadores para interrumpir las señales o "spoofing" para crear ubicaciones falsas.
- Objetivo: Asegurar o negar la capacidad de navegación por satélite, que es vital para operaciones militares y civiles.

La Guerra de Navegación, o NAVWAR, representa un ámbito crítico dentro del amplio espectro de la Guerra Electrónica (EW), centrándose en la competencia por el dominio de las capacidades de posicionamiento, navegación y cronometraje (PNT), esenciales para las operaciones militares y civiles. Abarca una gama de medidas ofensivas y defensivas destinadas a explotar, engañar, interrumpir o proteger los sistemas de navegación por satélite, principalmente los Sistemas Globales de Navegación por Satélite (GNSS), que incluyen el GPS de Estados Unidos, el GLONASS de Rusia, el Galileo de Europa y el BeiDou de China. Estas constelaciones de satélites se utilizan para servicios comerciales y militares y proporcionan servicios de navegación a usuarios de todo el mundo.

La importancia estratégica del GNSS

El GNSS desempeña un papel fundamental en el mundo moderno, mucho más allá de sus aplicaciones militares. Es la base de infraestructuras críticas, desde las telecomunicaciones y las redes eléctricas hasta los sistemas bancarios. En el ámbito militar, el GNSS es la columna vertebral de las municiones guiadas de precisión, el seguimiento de tropas y activos en tiempo real, y las operaciones sincronizadas en los ámbitos aéreo, terrestre, marítimo, espacial y cibernético. Por lo tanto, la precisión y la fiabilidad de los datos PNT no son meros requisitos operativos, sino que están estrechamente ligadas a la seguridad nacional y la estabilidad global.

Vulnerabilidades y amenazas

A pesar de sus ventajas, la dependencia del GNSS presenta vulnerabilidades significativas. Las señales GNSS, al ser ondas de radio de baja potencia transmitidas desde miles de kilómetros de distancia en el espacio, son inherentemente susceptibles a interferencias intencionales o accidentales. NAVWAR explota estas vulnerabilidades mediante:

Interferencia: La transmisión deliberada de ruido de radiofrecuencia en las mismas frecuencias utilizadas por los receptores GNSS para ahogar las señales reales del satélite, volviéndolas inutilizables.

Suplantación de identidad: Más sofisticada que la interferencia, la suplantación de identidad implica la transmisión de señales GNSS falsas. Los receptores engañados por estas señales pueden generar posiciones y horas erróneas, lo que podría tener consecuencias desastrosas.

Ataques cibernéticos: Los ataques cibernéticos tienen como objetivo los enlaces de datos y los segmentos de control de la infraestructura GNSS y pueden alterar o interrumpir el flujo de información PNT precisa.

Contexto histórico

El concepto de NAVWAR no es nuevo, sino que ha evolucionado con la tecnología. Entre los primeros ejemplos se incluye el uso de inhibidores de señales durante la Segunda Guerra Mundial para interrumpir la radionavegación. La Guerra del Golfo de 1991 puso de relieve el valor estratégico del GPS, marcando el inicio de su uso militar generalizado y, en consecuencia, el advenimiento de las tácticas modernas de NAVWAR. Desde entonces, la carrera tecnológica se ha intensificado, con actores estatales y no estatales desarrollando medios cada vez más sofisticados para explotar las vulnerabilidades del GNSS.

El dilema del doble uso

Un aspecto singular de NAVWAR es su dilema de doble uso. Las mismas capacidades que posibilitan las operaciones militares podrían degradar las

operaciones de fuerzas amigas y dañar los sistemas civiles. El uso generalizado del GNSS en diversos sectores implica que las tecnologías NAVWAR tienen implicaciones mucho más allá del campo de batalla, afectando a todo, desde la aviación comercial hasta los servicios de emergencia. Esta interconexión exige un enfoque cauteloso en NAVWAR, equilibrando las capacidades ofensivas con los posibles riesgos para la infraestructura civil.

Conclusión

El futuro de NAVWAR es una compleja interacción de tecnología, estrategia y diplomacia. A medida que avanzamos hacia este futuro, la clave del éxito reside en la innovación, la colaboración y la búsqueda incesante de resiliencia. Al mantenernos a la vanguardia en la detección y mitigación de las amenazas de NAVWAR, podemos proteger los servicios PNT que sustentan nuestro estilo de vida moderno frente a los desafíos del futuro. El camino que nos espera es de constante vigilancia y adaptación mientras navegamos por el terreno en constante evolución de la guerra electrónica en la búsqueda de proteger y preservar las señales invisibles que nos guían a través del mundo.

a) Pulso electromagnético (EMP):

   Utilizar una ráfaga de energía para desactivar o destruir componentes electrónicos en un área determinada, como en un ataque de enjambre de drones.

   Un pulso electromagnético (EMP) es una ráfaga de energía electromagnética que puede dañar gravemente los equipos electrónicos y las redes eléctricas. Puede ser causado por eventos naturales, como tormentas solares, o por fuentes artificiales, como explosiones nucleares a gran altitud. La energía de un EMP puede transferirse a través de radiación, campos eléctricos o magnéticos, o por conducción eléctrica, y sus efectos dependen de la intensidad, el rango de frecuencias y la duración del pulso.

Causas del EMP

Explosiones nucleares:

Las explosiones nucleares, tanto en la superficie de la Tierra como a gran altitud, pueden generar potentes pulsos electromagnéticos.

Fenómenos solares:

Eventos solares extremos, como las erupciones solares, pueden causar fenómenos similares a un EMP que afectan a la Tierra.

Fuentes artificiales:

Se pueden crear pulsos electromagnéticos artificiales para aplicaciones específicas, aunque su uso puede ser complejo.

Efectos del EMP

Equipos electrónicos:

Un EMP puede dañar o destruir equipos electrónicos sensibles, como ordenadores, teléfonos y sistemas de control.

Redes eléctricas:

Puede interrumpir el suministro de energía eléctrica y dañar las líneas de alta tensión y los equipos de las centrales eléctricas.

Sistemas de comunicación:

Las comunicaciones, como las señales de radio y televisión, pueden verse afectadas por el EMP.

Amenaza física limitada:

Un EMP no representa una amenaza física directa para los seres humanos o la vida silvestre, ya que su principal efecto es sobre la electrónica.

Ejemplos históricos

Prueba nuclear de 1962: Una prueba nuclear a gran altitud causó que las luces del alumbrado público de Hawái se cortaran.

Una tormenta solar provocó un gran apagón en Quebec, Canadá.

Los pulsos electromagnéticos (PEM) son una preocupación creciente a nivel mundial. Los PEM, también conocidos como armas de energía directa, son utilizados por militares y fuerzas del orden de diversas maneras. Estas armas

PEM tienen la capacidad de impactar sistemas electrónicos de diversas maneras, desde interrumpir temporalmente las operaciones hasta destruirlos por completo.

A medida que más y más adversarios obtienen esta tecnología, la importancia de estar preparado aumenta exponencialmente.

¿Qué es un EMP?

Un pulso electromagnético (PEM) es una breve ráfaga de energía electromagnética que puede ser extremadamente dañina para los equipos electrónicos. La energía PEM puede transferirse en forma de radiación electromagnética, campo eléctrico, conducción eléctrica o campo magnético. Dado que los PEM tienen una corta duración, su impacto puede ocurrir en amplios rangos de frecuencias.

Los pulsos de un PEM se caracterizan por su tipo de energía, rango de frecuencias y forma de onda. El tipo de energía puede ser conducida, electromagnética o nuclear. Las características de la forma de onda incluyen la amplitud, la duración y la forma.

¿Cómo se producen los EMP?

Los PEM pueden producirse de forma natural y se producen a partir de equipos artificiales. Los PEM naturales incluyen rayos, descargas electrostáticas (ESD), tormentas geomagnéticas o eyecciones de masa coronal de origen solar. Los PEM artificiales incluyen sobretensiones en líneas eléctricas, pulsos generados por sistemas de ignición, pulsos electromagnéticos nucleares (NEMP) y pulsos electromagnéticos no nucleares (NNEMP). Los PEM militares pueden ser de origen nuclear o no nuclear.

¿Qué son los NEMP y los HEMP?

NEMP significa Pulso Electromagnético Nuclear. Un NEMP es un pulso rápido de radiación electromagnética resultante de una explosión nuclear que

causa sobretensiones dañinas de corriente y voltaje. La radiación emitida puede impactar el aire circundante ionizándolo. Esto crea un PEM secundario, ya que los átomos del aire pierden sus electrones y luego los recuperan.

Un pulso electromagnético de gran altitud (PEMA) produce rayos gamma que se convierten en PEM en la estratosfera media. Estos PEM impactan en una amplia zona dentro del campo de visión de la detonación. Al producirse en el aire más enrarecido de las altitudes más elevadas, el PEM es mucho más intenso.

¿Qué son las pruebas EMP, las pruebas NEMP y las pruebas HEMP?

Las pruebas de PEM pueden realizarse mediante simulación de pulso inducido o de pulso de amenaza. La simulación de pulso inducido se realiza con una pinza amperimétrica. El laboratorio de pruebas de PEM invertirá la pinza para inyectar una señal de onda sinusoidal amortiguada en un cable conectado al dispositivo bajo prueba. Este generador de onda sinusoidal amortiguada puede replicar las señales más comunes.

La simulación del pulso de amenaza se realiza mediante un generador de PEM. El tamaño del generador varía desde uno portátil hasta una gran instalación de pruebas al aire libre. El laboratorio de pruebas de PEM utiliza un pulso de bajo nivel para caracterizar la respuesta de la víctima antes de la inyección de la onda sinusoidal amortiguada. La prueba de PEM puede realizarse utilizando pulsos de alta energía para simular las condiciones reales de la amenaza.

b. Protección electromagnética:

Medidas para defender los propios sistemas contra ataques electrónicos enemigos. Esto incluye técnicas como la interferencia, la suplantación de identidad y la ciberseguridad, así como la contramedida electrónica para evitar la anulación de radares, sistemas de guía de armas y otros equipos.

Es el uso de contramedidas electrónicas (ECM) para defenderse de ataques enemigos y garantizar que los sistemas propios funcionen correctamente. Esto implica identificar y neutralizar, ignorar o evitar señales de interferencia enemigas, como el uso de bengalas contra misiles, técnicas de sigilo, cambio de frecuencias o señuelos de radiofrecuencia.

Cómo funciona:

- Identificación y análisis: Los sistemas de protección electrónica identifican las señales de interferencia o engaño del enemigo. Esto puede incluir el análisis de transmisiones de radar, radio o infrarrojas.
- Contramedidas activas y pasivas: Se utilizan tanto acciones activas como pasivas para contrarrestar las amenazas.
- Activas: Implican la emisión de señales propias para interferir, engañar o suplantar al enemigo.
- Pasivas: No requieren la emisión de energía. Un ejemplo son las bengalas que desvían misiles infrarrojos o el uso de materiales de baja observabilidad (sigilo).
- Adaptación a la amenaza: Los sistemas modernos son capaces de adaptarse a las señales enemigas. Pueden operar en diferentes frecuencias para evitar interferencias, o incluso usar las señales del enemigo como debilidad, como en el caso de misiles antirradiación que buscan la fuente de la señal del interferidor.

Ejemplos prácticos:

- Señuelos (Chaff/Flares): Se lanzan señuelos que imitan o desvían las señales de los misiles enemigos, haciéndolos menos efectivos.
- Técnicas de suplantación: Se emiten señales falsas para confundir a los sistemas de navegación del enemigo (por ejemplo, la suplantación de GPS), lo que reduce la precisión de sus proyectiles.
- Bloqueo: Se utilizan interferidores para saturar o bloquear las frecuencias de comunicación y navegación del enemigo.

Medidas de Seguridad:

Las medidas de seguridad persiguen dos objetivos, cuyo lapso debe buscarse aún en tiempo de paz.

- El objetivo técnico, tendiente a preservar la sorpresa técnica, y por ello es importante proteger rigurosamente los datos que pueden servir de información al respecto.
- El objetivo operacional, cuya consecución se extrema en tiempo de guerra o en crisis y que procura evitar que el enemigo pueda localizar, identificar y conocer el desplazamiento de las fuerzas propias; y de las tácticas y condiciones de empico de los medios. También se busca impedir al adversario la apropiación y descifrado de las informaciones transmitidas, y evitar que éste ponga en funcionamiento sus sistemas de armar guiadas a causa de las ondas emitidas por los equipos propios.

Las medidas de seguridad más comunes son las siguientes:

1) El silencio: Es la más general e importante, ya que confiere una seguridad absoluta, pero sus inconvenientes pueden en oportunidades ser desproporcionados, porque exige la privación de todo medio de transmisión. Es tarea del comando, asesorado por los especialistas, ponderar en cada situación táctica o estratégica las ventajas. Es a partir del tiempo de paz que el silencio se impone para dejar al adversario potencial en la ignorancia de las características técnicas e incluso la existencia de determinados equipos; la disciplina que esta medida impone sólo puede ser obtenida en el adiestramiento y hábito.
2) Utilización de antenas direccionales y limitación de potencia irradiada. Estas dos medidas son de eficacia menos segura, pero son menos limitativas que el silencio (radio silencio). Su efecto se consigue al limitar geográficamente la zona a partir de la cual se hace posible la intercepción por parte del enemigo.
3) Las emisiones breves: Es la medida menos constructiva en el aspecto operativo, pero la más vulnerable en el aspecto técnico; se busca con ella

dificultar la intercepción, la radiogoniometría, el análisis y la restitución de la información radiada.

4) El cifrado: Es la medida más eficaz para limitar los efectos de la intercepción. La importancia de su uso es vital, ante la imposibilidad de aplicar constantemente el silencio y en virtud de que otras medidas de seguridad no ofrecen una garantía absoluta, por tal motivo el cifrado se constituye una medida complementaria de seguridad.

Las Medidas de Defensa:

Las medidas de defensa tienen por objeto permitir el funcionamiento eficaz de los medios emisores de ondas, a pesar de las tentativas de perturbación o de engaño por parte del adversario.

Contra la perturbación existe una serie de medidas que a continuación se especifican:

1) Aumento de la potencia de los emisores propios.
2) Empleo de técnicas de modulación que anulen la perturbación.
3) Mejoramiento de la capacidad selectiva de los receptores.
4) Adiestramiento de los operadores.
5) Cambio de frecuencias.
6) Contra el engaño se actúa de forma que las señales del adversario sean rechazadas por los sistemas de recepción, para ello se emplea una única medida: La Autenticación, por medio de ella se comparan las características de la señal recibida, con las de la señal deseada; ésta comparación puede efectuarse electrónicamente o por los operadores, la eficacia de la autenticación depende en gran parte de la calidad de los equipos y de la disciplina del personal.

Apoyo electromagnético:

Actividades que apoyan las operaciones militares mediante la gestión del espectro electromagnético. Esto puede incluir la recopilación de inteligencia, la vigilancia, la coordinación de comunicaciones y la supresión de defensas aéreas enemigas (SEAD).

El apoyo electromagnético, se refiere a las Medidas de Apoyo Electrónico (ESM), que implican la detección, interceptación, localización y análisis de la energía electromagnética (EM) emitida por fuentes enemigas, como radares y sistemas de comunicación, para obtener información sobre la amenaza y el entorno táctico. Estas operaciones pasivas proporcionan conocimiento de la situación en tiempo real y son la base para el conocimiento de la situación, la detección de amenazas y la planificación de acciones futuras.

Funciones principales:

- Detección: Escuchar pasivamente el espectro electromagnético en busca de señales.
- Interceptación: Capturar las señales emitidas por el enemigo.
- Análisis: Identificar el tipo de señal para determinar su propósito (por ejemplo, un radar antiaéreo).
- Localización: Determinar el origen de la señal mediante técnicas como el ángulo de llegada.

Objetivos

- Obtener conocimiento de la situación: Proporcionar información crítica en tiempo real sobre la presencia y actividad del enemigo.
- Identificar amenazas: Determinar qué tipo de equipo o sistema enemigo está operando en el área.
- Planificar contramedidas: Recopilar datos que ayuden a planificar acciones de ataque electrónico (EA) o protección electrónica (EP).

Características clave

- Operación pasiva: Los sistemas ESM son pasivos, es decir, no emiten ninguna señal, lo que los hace indetectables para el enemigo.
- Amplio rango de frecuencia: Deben operar en un amplio espectro para detectar un abanico desconocido de amenazas.

- Alta sensibilidad: Deben ser capaces de detectar señales débiles que pueden ser enmascaradas por otras emisiones.
- Medición del ángulo de llegada: Fundamental para triangular y localizar la fuente de la señal.

En resumen, el apoyo electromagnético es una herramienta de inteligencia militar que permite "escuchar" al enemigo a través del espectro electromagnético, proporcionando información vital sin revelar la presencia del propio observador.

Técnicas para operar los sistemas de comunicaciones en un ambiente de operaciones electromagnéticas.

a. No utilizar los equipos de radio, mientras medios alternos, suficientes, rápidos y seguros estén disponibles (alambre, mensajero, medios visuales y acústicos).
b. Si los radios son utilizados, manténgalos en transmisión el tiempo mínimo indispensable.
c. Evitar la verbosidad por parte de los operadores durante el chequeo de los radios.
d. Evitar el envío de mensajes largos y no tácticos a través de redes de radio establecidas.
e. Acatar las disposiciones relativas a seguridad de las comunicaciones.
f. Entrenar a todo el personal en:
   1) Procedimiento radiotelefónico.
   2) Uso correcto de IOC/IPC.
   3) Uso apropiado de sistemas de autenticación.
   4) El propósito y función de todas las redes de radio.
   5) La composición completa de todas las redes de radio incluyendo estaciones, señales de llamadas y sufijos.
g. Uso de antenas direccionales.
h. Uso de potencia más baja requerida.

i. La selección del tipo de antena que reduzca la posibilidad de transmitir más allá del alcance deseado.
j. El uso de obstáculos naturales o fabricados para bloquear las transmisiones del enemigo.

El empleo de las técnicas antes mencionadas reducirá las capacidades del enemigo para:

a. Interceptar el tráfico de radio.
b. Descubrir información vital acerca de nuestro orden de batalla.
c. Determinar las frecuencias, señales de llamada y funciones de las redes.
d. Conocer las características de la voz de los operadores.
e. Identificar blancos potenciales para interferir.
f. Identificar una red de radio como blanco potencial para comunicaciones imitativas de recepción (CID).

La Protección electromagnética que el operador de radio pueda usar para contrarrestar los ataques electromagnéticos son:

a. Entrenar a todos los operadores para que reconozcan la diferencia entre la interferencia introducidas en las redes, por el enemigo y aquellas causadas por estaciones amigas, líneas de alto voltaje, condiciones atmosféricas y mal funcionamiento de los equipos.
b. Entrenar a los operadores en el reconocimiento de los tipos de interferencia más comunes usados por el enemigo.
c. Entrenar a los operadores en los procedimientos para reportar las interferencias del enemigo, en la forma correcta.
d. Continuar operando si es posible.
e. Uso de códigos de operación, códigos numéricos, y sistemas de autenticación.
f. No se dé por entendido, en comunicación clara, que ha detectado interferencias del enemigo.

g. No se dé por entendido que ha detectado comunicaciones imitativas de decepción.
h. Use medios alternos cuando sea posible.
i. Aumente la potencia cuando sea necesario.
j. Use un programa u horario aleatorio para las transmisiones.
k. Use antenas direccionales cuando sea posible.
l. Cambie las frecuencias.
m. Use antenas que le permitan maximizar la operación de las redes de radio.
n. Planifique con anticipación e informe muy bien al personal, con la finalidad de reducir la necesidad del uso de los radios.
o. Use técnicas de operación de radio que permitan o ayuden a recibir mensajes correctamente, ello incluye la disminución de la velocidad de transmisión, repetir palabras o deletrearlas.

El empleo de estas técnicas reducirá la capacidad del enemigo para:

a. Interrumpir las comunicaciones en los momentos críticos.
b. Interferir las comunicaciones para aislar el comando y control.
c. Usar comunicaciones imitativas de decepción para causar confusión e interrumpir el comando y control.

Nuevos campos de aplicación

Los nuevos campos de aplicación de la exploración radioelectrónica incluyen la guerra electrónica avanzada, como la supresión de drones y la protección contra interferencias; la minería moderna con la ayuda de Internet de las cosas (IoT) y análisis de datos de Inteligencia Artificial (IA) para optimizar la exploración y la exploración espacial, incluyendo la detección de asteroides.

Guerra electrónica y defensa

- Protección contra drones: Sistemas avanzados para detectar, inhibir y neutralizar drones en vuelo, cortando sus comunicaciones y señales de posicionamiento.
- Guerra electrónica de ataque: Uso de armas de energía dirigida y misiles antirradiación para detectar, atacar y suprimir las señales electrónicas del enemigo.
- Tecnologías de baja observabilidad: Aplicación de recubrimientos absorbentes de radar para reducir la firma de plataformas aéreas, navales o terrestres.
- Sistemas de advertencia: Desarrollo de sistemas de advertencia para detectar misiles y otras amenazas mediante sensores infrarrojos.

Exploración y minería

- Internet de las Cosas (IoT): Implementación de sensores y dispositivos conectados para monitorear y controlar equipos de forma remota, mejorando la eficiencia y seguridad en operaciones mineras.
- Inteligencia Artificial (IA) y análisis de datos: Uso de IA para interpretar datos geoespaciales y de perforación, optimizar la prospección y crear modelos digitales detallados del subsuelo.
- Cartografía digital: Sustitución de la cartografía tradicional por planos base digitales de alta calidad y mapeo con imágenes satelitales en tiempo real para una mayor precisión y seguridad.

Exploración espacial

Detección de cuerpos celestes: Uso de tecnología de exploración radioelectrónica para identificar y estudiar nuevos asteroides y otros objetos dentro del Sistema Solar.

Internet interplanetario: Desarrollo de redes de comunicación para la exploración espacial a larga distancia.

Investigación de exoplanetas: Aplicación de técnicas para buscar señales de radio que puedan indicar la presencia de vida en planetas fuera de nuestro sistema solar.

Dependencia del adversario

La dependencia del adversario en la exploración radioelectrónica, se refiere a la vulnerabilidad de las fuerzas militares que dependen de las señales y sistemas de radio para la exploración, navegación, comunicación y control. Esta dependencia crea oportunidades para que el adversario utilice la guerra electrónica para interferir, perturbar o incluso explotar estas señales. En resumen, se trata de una debilidad que se explota mediante guerra electrónica.

Dependencia del adversario en la exploración radioelectrónica

- Dependencia en la exploración y reconocimiento: Las fuerzas armadas que dependen de la exploración radioelectrónica (es decir, el uso de ondas de radio para recopilar información) pueden ser vulnerable a ser detectadas y rastreadas por el adversario.
- Vulnerabilidad a la interferencia: Si un adversario puede interferir con las señales de radio, puede bloquear las comunicaciones, interrumpir la navegación o incluso deshabilitar el control de sistemas críticos, como armas o drones.
- Vulnerabilidad a la explotación de las señales: El adversario puede explotar las señales radioelectrónicas para engañar a las fuerzas militares, por ejemplo, emitiendo señales falsas para desorientar a los pilotos o a los sistemas de navegación.
- Vulnerabilidad a la supresión: El adversario puede usar la guerra electrónica para suprimir las señales de radio de un adversario, lo que crea un entorno en el que el adversario no puede operar de manera efectiva.

Consecuencias

- Las fuerzas militares que dependen en gran medida de las señales de radio son vulnerables a ser interrumpidas por el adversario.
- La dependencia del adversario en la exploración radioelectrónica puede tener graves consecuencias para las operaciones militares.

- Las fuerzas militares que no pueden proteger sus señales de radio pueden ser vulnerables a ser atacadas o infiltradas.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO XI

VEHÍCULOS NO TRIPULADOS

(AÉREOS, TERRESTRES Y MARÍTIMOS)

SECCIÓN A

1. Generalidades.

Los antecedentes de los drones en otros países varían desde los primeros experimentos con globos no tripulados en la guerra austro-húngara del siglo XIX hasta los programas de desarrollo de drones militares y comerciales en países como el Reino Unido, Estados Unidos, Israel y China. La tecnología se desarrolló significativamente en Europa y Estados Unidos durante las guerras mundiales y la Guerra Fría, evolucionando a través de prototipos radiocontrolados y siendo impulsada posteriormente por los avances en electrónica, GPS y miniaturización, resultando en la creación de drones modernos para fines militares y, más recientemente, comerciales.

a. Desarrollo histórico y militar

1) Austria y Venecia (1849): Se considera el origen del concepto con el ataque austriaco sobre Venecia utilizando globos aerostáticos no tripulados cargados de explosivos.

2) Reino Unido (Primera Guerra Mundial): El Reino Unido construyó el Aerial Target en 1916, el primer avión no tripulado controlado por radio, que se usó en pruebas para convertirse en una bomba voladora.

3) Estados Unidos (Primera Guerra Mundial): Desarrollaron el Hewitt-Sperry Automatic Airplane y su mejora, el Kettering Bug, que fue probado como un ataque aéreo no tripulado, aunque no llegó a usarse en combate.

4) Estados Unidos (Segunda Guerra Mundial): La Naval Aircraft Factory construyó un dron de asalto con cámara de televisión que realizó ataques exitosos en 1942.

5) Alemania (Segunda Guerra Mundial): Se desarrolló el Fritz X, la primera arma guiada teledirigida utilizada en combate.

6) Guerra Fría: Se fabricaron drones como los Lightning Box en Estados Unidos, usados en Vietnam para misiones de reconocimiento y como armas.

7) Década de 1970 y 1980: Se consolidó la tecnología con modelos como el Aquila RPB Drone en Estados Unidos, y el Reino Unido lanzó el programa de la Marina Real con el de Havilland DH82B "Queen Bee".

b. Avances y comercialización

1) Década de 1990: Los avances en informática, miniaturización y GPS permitieron la creación de los drones modernos como el Predator, utilizado por primera vez en la Guerra del Golfo de 1991, y sentaron las bases para su uso por la policía.

2) Principios de 2000: Los drones de ataque estadounidenses se convirtieron en una herramienta clave en la lucha contra el terrorismo.

3) Años 2010:

1. Parrot (Francia): Lanzó el primer UAB (vehículo aéreo no tripulado) controlado por Wi-Fi y una aplicación móvil, a diferencia de los métodos anteriores de radiocontrol.

2. DJI (China): El modelo Phantom 4 integró IA y aprendizaje automático, permitiendo la evitación de obstáculos y el rastreo de personas sin GPS.

c. Actualidad:

1) Muchos países como Estados Unidos, Rusia, Israel, China e India, tienen programas activos de drones militares.

2) Países como Países Bajos han desplegado drones para operaciones de inteligencia de la OTAN.

3) Hay un creciente uso de drones comerciales para fotografía, filmación, entregas y otros fines personales y comerciales.

d. Otros países

1) Israel: Se ha destacado por su liderazgo en el desarrollo de drones, tanto militares como comerciales.

2) China: Ha desarrollado drones de combate y comerciales, con empresas como DJI que han liderado el mercado global de drones comerciales.

3) Rusia: Ha utilizado drones de manera extensa para misiones de reconocimiento en conflictos, como el que se ha reportado en Ucrania.

4) Unión Europea: Varios países han implementado programas de drones militares y comerciales. La Unión Europea también ha experimentado un aumento en la detección de drones en su espacio aéreo.

e. Terminología Universal

Los drones reciben varios nombres, principalmente según su clasificación o el tipo de tecnología que utilizan. Los términos más comunes son UAV (Vehículo Aéreo No Tripulado), UAS (Sistema Aéreo No Tripulado), RPA (Aeronave Pilotada Remotamente) y RPAS (Sistema de Aeronave Pilotada Remotamente), que se refieren tanto a la aeronave como a los sistemas que la controlan. También se les llama multirrotores o multicópteros según su configuración de rotores, como cuadricópteros, hexacópteros u octocópteros.

1) Términos por clasificación técnica y operativa

a) UAV (Unmanned Aerial Vehicle): Término técnico en inglés para Vehículo Aéreo No Tripulado.

b) UAS (Unmanned Aerial System): Se refiere a todo el sistema, incluyendo la aeronave, el control terrestre y las comunicaciones.

c) RPA (Remotely Piloted Aircraft): Se utiliza para destacar que la aeronave es controlada de forma remota por un piloto, lo que ayuda a disipar el miedo a la autonomía total.

d) RPAS (Remotely Piloted Aircraft System): Similar al UAS, pero enfatiza el sistema de control remoto. La Unión Europea utiliza este término para aeronaves de uso civil.

e) UCAV (Unmanned Combat Air Vehicle): Son conocidos como Drones de combate no tripulados.

f) UGV (Unmanned Ground Vehicle), es un vehículo que se desplaza por la superficie terrestre sin necesidad de un operador humano a bordo.

g) USV **(**Unmanned Surface Vehicle**):** son embarcaciones autónomas o controladas a distancia que operan sin tripulación a bordo.

h) UUV **(**Unmanned Underwater Vehicle)**:** on vehículos sumergibles que operan bajo el agua.

i) AUV (Autonomous Underwater Vehicle) para los submarinos autónomos.

2) Términos por diseño o configuración

1) Multirrotor / Multicóptero: Drones con múltiples rotores. Se les llama así por su configuración de rotores, como los cuadricópteros (4 rotores), hexacópteros (6 rotores) u octocópteros (8 rotores).

2) Ala rotatoria: Un término más amplio para los multirrotores, que son muy populares por su capacidad de vuelo estacionario y estabilidad.

3) FPV (First Person View): Drones equipados con cámaras y gafas especiales que ofrecen al piloto la sensación de estar dentro de la aeronave.

4) Drones de ataque unidireccional: Drones diseñados para un solo uso, donde la ojiva está integrada en el cuerpo y se destruye durante el ataque. También se les llama "drones suicidas".

2. Vehículo Aéreo no Tripulado (UAV)

Un vehículo aéreo no tripulado (UAV) es una aeronave que vuela sin piloto humano a bordo, pudiendo ser controlada de forma remota por un operador o volar de manera autónoma gracias a programas preestablecidos. Estos

vehículos pueden tener diversas formas y tamaños, y utilizan motores de explosión, eléctricos o de reacción, siendo utilizados tanto en aplicaciones militares como civiles.

a. Características principales

1) Control: Pueden ser controlados remotamente por un operador humano u operar de forma autónoma a través de un piloto automático, con distintos grados de autonomía.

2) Propulsión: Se impulsan mediante motores de explosión, eléctricos o de reacción. Los modelos civiles modernos a menudo utilizan baterías de litio, energía eléctrica o sistemas híbridos.

3) Diseño: Existen en una gran variedad de formas, tamaños y configuraciones, desde cuadricópteros hasta diseños de ala fija e híbridos de despegue y aterrizaje vertical (VTOL).

4) Componentes: Es parte de un sistema más amplio que incluye, un controlador terrestre y un sistema de comunicación.

b. Clasificación de vehículo aéreo no tripulado (UAV)

1) Clasificación por tipo de ala:

a) Ala fija: Estos equipos debido a su forma aerodinámica tienen la capacidad de aprovechar el viento lo cual les permite mantenerse en el aire de manera estable. En general puede decirse que su estética o diseño es muy parecido a los aviones de radiocontrol y son utilizados para realizar mapeos de superficies extensas. La característica que distingue a este tipo de equipos

es que no poseen hélices para realizar sus vuelos, éstos se mantienen en el aire gracias a sus propulsores, sin embargo, la principal desventaja es que son inestables en su vuelo cuando se encuentran maniobrando al tratar de evitar choques en zonas donde existan muchos obstáculos o bien en zonas boscosas.

b) Ala Rotatoria (multirrotor): Los equipos que pertenecen a esta división a su vez se clasifican de acuerdo con el número de alas o rotores con los que cuentan. Cuando se habla de la clasificación de acuerdo con el número de hélices o rotores que el UAV posee podemos encontrar:

1. Tricópteros: se componen por tres rotores verticales, es decir, tres hélices. Por lo general, tienen funciones muy simples, son relativamente fáciles de reparar, en la mayoría de los casos son económicos. Por su sencillez, suelen ser utilizados por aficionados, principiantes o bien por infantes a manera de juguete.

2. Cuadricópteros: Estas aeronaves son propulsadas por cuatro rotores o hélices. Gracias a ello, estos equipos tienen mayor potencia y estabilidad que los tricópteros y es por esa razón que se les pueden dar diferentes usos, un poco más profesionales para filmar o fotografiar. En general, tienen gran potencia de elevación, pueden permanecer estables y volar en cualquier dirección.

3. Hexacópteros: Como su nombre lo indica, estos equipos cuentan con seis rotores dispuestos de manera circular, por lo tanto, son muy estables y sus movimientos durante el vuelo son muy eficientes. La desventaja de estos drones es que son equipos costosos. Los rotores del hexacóptero son más grandes y complejos, lo que encarece su reparación en caso de que tengan algún daño.

4. Octacóptero: Este equipo tiene ocho rotores o hélices que funcionan al mismo tiempo, esto significa una mayor capacidad de vuelo con respecto a los equipos mencionados anteriormente. Debido a sus características, estos equipos tienen la capacidad de grabar videos o realizar tomas fotográficas con gran estabilidad y de gran calidad. Tiene la ventaja de llevar cargas útiles de gran peso, así como también el hecho de que, si llega a dañarse desde uno hasta cuatro de sus hélices, puede seguir volando con estabilidad. Estos vehículos aéreos no tripulados son muy rápidos y tienen la capacidad de volar bajo la lluvia y fuertes vientos gracias a sus ocho hélices.

2) Clasificación según su uso:

Los vehículos aéreos no tripulados pueden ser clasificados en dos categorías principales: civil y militar.

Los vehículos aéreos no tripulados civiles, son utilizados para una amplia variedad de tareas comerciales, científicas y recreativas, como la agricultura de precisión, la inspección de infraestructuras, la entrega de paquetes y el cine y la televisión.

Por otro lado, los vehículos aéreos no tripulados militares son diseñados específicamente para ser utilizados por las fuerzas armadas en una variedad de operaciones, desde la vigilancia hasta el combate. Aunque los drones militares y civiles tienen algunas similitudes en términos de diseño y tecnología, hay importantes diferencias en cuanto a su uso y especificaciones técnicas.

a) Vehículo aéreo no tripulado para uso civil

Dentro de la clasificación de estos equipos encontraremos desde aquellos que se consideran juguetes hasta los que se destinan a la investigación o bien a los que se les da un uso comercial en diferentes áreas.

Las áreas de aplicación pueden ser en ámbitos muy diversos. Uno de ellos es la fotogrametría en donde se realizan mapeos en zonas extensas o poder llegar a terrenos o espacios que son poco accesibles. Otro ámbito puede ser la realización de fotografía o videos tanto para cine como para televisión o bien para temas inmobiliarios, minería, cartografía, ingeniería, para agricultura, construcción, atención de emergencias y desastres, control de tráfico, topografía y mucho más. Esto es por mencionar algunos, sin embargo, en la actualidad el límite para el uso que se les puede dar a los drones es únicamente la imaginación.

En esta categoría podemos encontrar también los vehículos aéreos no tripulados muy básicos que funcionan perfecto para vuelos en interiores y que son de muy fácil manejo. Estos equipos tienen un precio muy accesible y pueden ser utilizados en algunos casos, por niños, supervisados por un adulto o bien pueden ser una muy buena opción para aquellas personas que se están iniciando en este mundo de los drones para tomar experiencia y poder pasar a utilizar drones un poco más avanzados y con características mucho más complejas.

b) Vehículo aéreo no tripulado para uso militar

La historia del uso de los vehículos aéreos no tripulados podríamos decir que se inicia en el ámbito militar y se remonta a la primera guerra mundial, aunque ya se tenían antecedentes de su utilización para ese momento. Son conocidos como Drones de combate no tripulados o bien los encontraremos como UCAV (por sus siglas en inglés: Unmanned Combat Air Vehicle).

Aun cuando estas aeronaves se utilizan para entrenamientos militares y combate, en cuestiones de orden militar también podemos observarlos realizando actividades de apoyo a la población, es decir, temas como abastecimiento de provisiones en lugares donde el acceso es difícil o bien para apoyar en la localización de personas después de alguna catástrofe o emergencia, entre otros.

3) Empleo de los Vehículo Aéreo no Tripulado (UAV)

1. Comunicaciones: El uso de Vehículos Aéreos no Tripulados en las comunicaciones militares ha revolucionado el campo de batalla. Han pasado de ser simples plataformas de vigilancia a convertirse en nodos de comunicación críticos y versátiles.

2. Un vehículo aéreo no tripulado puede actuar como una "torre de comunicaciones voladora" o un "satélite bajo demanda", solucionando uno de los problemas más antiguos y críticos en el combate: mantener un contacto fiable entre las unidades.

Los diferentes vehículos aéreos no tripulados se pueden utilizar como:

a) Relé de Comunicaciones (El Puente Aéreo)

Esta es la función más fundamental y común.

3. El Problema: El terreno (montañas, bosques densos, edificios en ciudades) bloquea las señales de radio, que necesitan línea de vista directa para funcionar correctamente. Una unidad en un valle o al otro lado de una colina puede quedar incomunicada.

4. La Solución: Se despliega un dron a una altitud media o alta. Este dron actúa como un repetidor. Recibe la señal de radio débil de una unidad terrestre y la retransmite con mayor potencia o desde una posición ventajosa a otra unidad o al centro de mando.

5. Beneficio: Extiende drásticamente el alcance de las radios de mano y de los vehículos, conectando fuerzas que de otro modo estarían aisladas y permitiendo la coordinación en terrenos complejos.

6. Torre de Comunicaciones Aérea (Creación de Redes Locales).

Más allá de solo repetir, los drones pueden llevar cargas específicas para crear redes de datos completas.

7. El Problema: En operaciones especiales o en el establecimiento de una base avanzada, no hay infraestructura de comunicaciones (internet, telefonía).

8. La Solución: Un vehículo aéreo no tripulado, especialmente uno de gran autonomía (HALE - Alta Altitud y Larga Resistencia), puede equiparse con una carga útil que funcione como una mini estación base de telefonía móvil (BTS) o un router Wi-Fi seguro.

9. Beneficio: Crea una "burbuja" de conectividad sobre un área específica. Las tropas pueden transmitir video de alta definición, datos de sensores, y realizar llamadas de voz seguras y encriptadas como si estuvieran en una oficina, incluso en medio de la nada.

b) Extensión de Enlace de Datos para Plataformas ISR

Las operaciones de Inteligencia, Vigilancia y Reconocimiento (ISR) dependen de la transmisión de video y datos en tiempo real.

El Problema: Un dron de vigilancia está operando muy lejos de su base, más allá del alcance directo de su enlace de datos. Perder el video en tiempo real es inaceptable.

La Solución: Se puede utilizar un segundo dron, cuya única misión es actuar como un retransmisor de enlace de datos. El dron de vigilancia transmite su video al dron de comunicaciones, y este lo reenvía a la estación de control en tierra

Beneficio: Permite que las fuerzas armadas mantengan la "conciencia situacional" sobre vastas distancias, manteniendo el flujo de información crítica sin interrupciones.

1. Operaciones Electromagnética

Los vehículos aéreos no tripulados (UAV) se utilizan en la guerra electrónica para interferir con las comunicaciones enemigas, realizar inteligencia, vigilancia y reconocimiento (ISR), y para desplegar contramedidas contra otros drones. Estos UAV pueden ser utilizados para:

a) Interferir señales: Bloquear frecuencias de radio para cortar las comunicaciones de otros UAV o interferir con sus señales de video para interrumpir el video en tiempo real. En un conflicto moderno contra un enemigo tecnológicamente avanzado, las comunicaciones son un objetivo principal. El enemigo puede estar interfiriendo (jamming) las frecuencias de radio o incluso atacando los satélites de comunicaciones. Las redes de drones ofrecen una alternativa resiliente, una Red Malla

(Mesh Network) haciendo que varios drones pueden volar en formación, creando una red donde cada dron se comunica con los demás. Si un dron es derribado o su señal es interferida, la red se reconfigura automáticamente y encuentra una nueva ruta para la información.

b) Suplantación de identidad (Spoofing): Manipular las señales GPS para desviar a los drones enemigos de su ruta o para guiarlos de regreso a su base.

c) Vigilancia y reconocimiento: Monitorear las comunicaciones y los sistemas electrónicos del enemigo para obtener inteligencia.

d) Ataques de precisión: Lanzar ataques dirigidos a objetivos específicos utilizando misiles guiados o bombas.

e) Contramedidas contra drones: Neutralizar amenazas de drones utilizando contramedidas electrónicas o incluso enjambres de drones autónomos.

Los UAVs modernos también se están volviendo cada vez más autónomos gracias a la inteligencia artificial, lo que les permite operar en enjambres y tomar decisiones en tiempo real.

10. Combate:

a) Ataque y ataque de precisión: Los UCAV están armados con misiles o bombas para atacar objetivos estratégicos, como se observa en la lucha contra grupos del crimen organizado. Pueden volar a muchos kilómetros de la línea del frente, esperando pasivamente en el espacio aéreo antes de localizar, identificar y atacar un objetivo. Tienen una capacidad única

para atacar un objetivo oculto a la vista o que solo aparece por un breve periodo.

b) Despliegue de enjambres de drones: Algunos modelos avanzados pueden desplegar otros drones más pequeños, incluidos drones kamikaze, para ataques coordinados.

11. Apoyo Logístico:

1) Logístico: También pueden cumplir funciones de logística, como el transporte de suministros a tropas en territorios hostiles.

2) Entrega de productos:

3) Última milla: Entrega directa al consumidor de paquetes ligeros, alimentos, medicamentos y otros productos, especialmente en áreas urbanas congestionadas o rurales remotas.

4) Suministros médicos: Transporte rápido y seguro de vacunas, sangre, medicamentos y desfibriladores en situaciones de emergencia o a zonas con infraestructura limitada.

5) Gestión de almacenes:

6) Inventario: Inspección y auditoría de existencias de forma rápida y sin contacto, usando cámaras y lectores de códigos de barras o RFID para verificar y localizar productos.

7) Monitoreo: Vigilancia de almacenes, muelles y patios para verificar la capacidad y localizar inventario de manera eficiente.

8) Monitoreo de infraestructuras:

9) Supervisión de la integridad de infraestructuras logísticas y de transporte para detectar posibles problemas.

10) Transporte de carga pesada (en desarrollo):

11) Cargas de hasta 200 kg: Algunos UAV están diseñados para transportar cargas más pesadas, como herramientas y depósitos, en entornos agrícolas o mineros.

12) Porta-drones: Vehículos más grandes con capacidad para transportar y lanzar múltiples drones más pequeños, como en aplicaciones militares para lanzar enjambres de drones.

3. Vehículo Terrestre no Tripulado (UGV)

Los vehículos no tripulados terrestres son robots equipados con sensores y sistemas de navegación que pueden operar de forma autónoma o remota, sin un conductor a bordo. Son útiles en tareas peligrosas, aburridas o imposibles para los humanos, como el desminado, la vigilancia, el transporte logístico en zonas de conflicto y la agricultura. Pueden ser teleoperados por un humano o tomar decisiones de manera autónoma basándose en sus sensores.

a. Características principales

1) Control remoto o autónomo: Pueden ser controlados directamente por un operador a distancia o funcionar de manera independiente a través de algoritmos programables.

2) Sensores avanzados: Incorporan tecnologías de posicionamiento, navegación y detección para percibir su entorno y ejecutar misiones de forma segura.

3) Diversidad de aplicaciones: Su uso abarca tanto el ámbito militar (reconocimiento, logística, apoyo de fuego) como el civil (agricultura, inspección de infraestructuras, seguridad).

4) Capacidad de operar en grupo: Pueden trabajar en conjunto, permitiendo a un solo operador supervisar múltiples unidades.

b. Aplicaciones

1) Militar: Realizan misiones de reconocimiento, vigilancia, transporte de suministros en zonas de combate y desactivación de explosivos (EOD).

2) Civil:

a) Agricultura: Análisis del suelo, control de plagas y cosecha.

b) Inspección: Revisión de puentes, túneles, presas y otras infraestructuras.

c) Seguridad: Patrullaje en áreas sensibles o peligrosas.

c. Ventajas

1) Ahorro de riesgo: Reducen el peligro para los operadores humanos en situaciones de riesgo.

2) Aumento de la productividad: Pueden operar de forma continua sin necesidad de descansos.

3) Capacidad de operación continua: Son ideales para tareas que requieren vigilancia constante o largas horas de trabajo.

d. Empleo de los Vehículo Terrestre no Tripulado (UGV)

1) Usos en comunicaciones militares

a) Vigilancia y reconocimiento: Pueden desplegarse en áreas peligrosas como zonas de combate, callejones estrechos o trincheras, recolectando inteligencia (videos, imágenes) y transmitiéndola a los centros de mando sin exponer personal humano.

b) Comunicaciones en zonas de difícil acceso: Sirven como "puntos de relevo" o nodos de comunicación para extender el alcance de las redes de comunicación o proporcionar conectividad en áreas donde la red principal no llega.

c) Navegación y posicionamiento: Equipados con sistemas de navegación inercial, pueden operar en entornos sin cobertura GPS (túneles, cañones urbanos, zonas boscosas), manteniendo la comunicación y la coordinación en todo momento.

d) Transporte seguro de información: Pueden ser utilizados para transportar dispositivos de almacenamiento de datos encriptados o para llevar equipos de comunicación de un punto a otro, asegurando la integridad de la información.

2) Características y ventajas

a) Autonomía y control remoto: Pueden operar de forma autónoma o ser controlados a distancia, ofreciendo flexibilidad en el campo de batalla.

b) Bajo riesgo para el personal: Su principal ventaja es que reducen el riesgo para los soldados al realizar misiones en entornos peligrosos.

c) Alta precisión: Son capaces de realizar tareas precisas como el reconocimiento o el transporte de material sensible con un alto grado de exactitud.

d) Resistencia: Están diseñados para soportar condiciones adversas, incluyendo golpes, vibraciones y temperaturas extremas.

4. Vehículo Marítimo no Tripulado

Los vehículos no tripulados marinos se dividen principalmente en dos categorías: los Vehículos de Superficie No Tripulados (USV), que operan en la superficie del agua, y los Vehículos Submarinos No Tripulados (UUV), que operan bajo el agua. Estos vehículos autónomos o controlados a distancia se utilizan en aplicaciones civiles y militares como vigilancia, reconocimiento, exploración, búsqueda y rescate, y guerra naval.

a. Vehículos de Superficie No Tripulados (USV)

1) Operan en la superficie del agua sin tripulación.

2) Se utilizan para vigilancia, reconocimiento e inteligencia (ISR).

3) Algunos están diseñados para llevar una carga explosiva

4) Pueden operar en solitario o ser lanzados desde buques nodriza.

b. Vehículos Submarinos No Tripulados (UUV)

1) Operan bajo el agua sin tripulación.

2) Son también conocidos como "drones submarinos".

3) Se utilizan para misiones de exploración, búsqueda de minas y otras tareas submarinas.

c. Aplicaciones y usos

1) Militar:

Vigilancia, reconocimiento, desminado inteligencia, guerra naval y operaciones de seguridad.

2) Civil:

Mapeo del fondo marino, investigación oceanográfica, búsqueda y rescate, y limpieza de desechos.

d. Empleo de los Vehículo Terrestre no Tripulado (VMNT)

1) Usos en comunicaciones militares

a) Redes móviles de comunicación: Pueden actuar como antenas de altura variable, creando redes de comunicación táctica y segura en áreas remotas o en medio de un combate.

b) Soporte en misiones complejas: Proporcionan una conexión continua para el control remoto de otras plataformas (aéreas o submarinas) y para la transmisión segura de datos sensibles.

c) Vigilancia y monitoreo: Su capacidad para operar durante largos periodos con sensores activos los convierte en herramientas ideales para la vigilancia marítima y fronteriza, recopilando datos de manera persistente. Pueden recopilar datos de inteligencia y vigilancia en tiempo real, transmitiendo imágenes y video a la base de operaciones.

2) Usos en otras Áreas

a) Guerra electrónica: Pueden realizar operaciones de guerra electrónica, interrumpiendo las comunicaciones o recopilando datos de inteligencia electrónica.

b) Gestión de misiones: Permiten integrar la información recopilada por los sensores a bordo con otros sistemas de combate, para gestionar misiones de forma más eficiente.

c) Operaciones nocturnas: Los sistemas de cámaras infrarrojas permiten operar de noche y en condiciones de baja visibilidad.

d) Sistemas de detección: Además de las cámaras, utilizan sonares para detectar objetos sumergidos y pueden comunicar la información a través de sus sistemas de comunicación.

3) Ventajas principales

a) Mejor comunicación: A diferencia de los vehículos submarinos, los vehículos de superficie no tripulados se benefician de la comunicación por radiofrecuencia, que es mucho más fácil y confiable en la superficie del agua.

b) Menor riesgo para el personal: Permiten realizar misiones en áreas peligrosas o de alto riesgo sin necesidad de poner en peligro a las tripulaciones humanas.

c) Operaciones extendidas en el tiempo: Pueden operar durante largos periodos (incluso meses) sin necesidad de reabastecimiento frecuente, gracias a soluciones de energía como células solares o energía de las olas.

d) Versatilidad y adaptabilidad: Pueden ser adaptados para múltiples roles, incluyendo vigilancia, reconocimiento, guerra electrónica, y como plataformas de comunicación elevadas.

e) Mayor capacidad de vigilancia: Pueden ser equipados con una variedad de sensores (cámaras, radar, sonares) y actuar como plataformas para extender la comunicación, proporcionando inteligencia en tiempo real sin interrupciones.

f) Reducción de la huella de personal: Requieren menos personal para su operación, lo que reduce los costos operativos y la logística asociada.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPÍTULO XII

EL SISTEMA DEFENSIVO TERRITORIAL

SECCIÓN A

1. GENERALIDADES

El Sistema Defensivo Territorial es un concepto estratégico y organizacional de la República Bolivariana de Venezuela, establecido en la Ley Orgánica de Seguridad de la Nación. Su propósito es garantizar la Defensa Integral de la Nación ante cualquier amenaza o agresión.

A. Concepto y Alcance

El Sistema Defensivo Territorial es el conjunto de medidas y actividades de carácter político, económico, militar, de seguridad, orden interior y defensa civil, organizadas desde tiempo de paz por el Estado y el pueblo. No es solo una estructura militar, sino un sistema cívico-militar que involucra a todos los órganos del Poder Público y a la ciudadanía.

B. Estructura de Mando y Control

El territorio nacional se organiza para la defensa mediante una estructura jerárquica de mando y control, liderada por el Comando Estratégico Operacional de la FANB (CEOFANB):

Regiones Estratégicas de Defensa Integral (REDI): Nivel estratégico de mando superior (Nacional/Regional).

Zonas Operativas de Defensa Integral (ZODI): Nivel intermedio de mando (Estadal/Zonal).

Áreas de Defensa Integral (ADI): Nivel táctico y local (Municipal/Subzonal), donde se concreta la participación popular.

C. Componentes Clave

El Sistema Defensivo Territorial se implementa a través de los Órganos de Dirección de la Defensa Integral (ODDI) en cada nivel territorial, los cuales coordinan todas las actividades necesarias, incluyendo la actividad esencial de Comunicaciones e Informática.

Terminología

Las Comunicaciones Militares son el eje nervioso que garantiza el correcto funcionamiento del Sistema Defensivo Territorial. Su misión principal es asegurar el Comando, Control y Comunicación de las operaciones cívico-militares.

1. El Trinomio Estratégico: C3 (Comando, Control y Comunicación)

Tiene como función permitir que el mando (Comando) reciba información para tomar decisiones (Control) y transmita las órdenes a las unidades de ejecución. Sin comunicaciones seguras y oportunas, el mando pierde su capacidad de dirección.

2. La Misión Fundamental

La misión de la actividad de Comunicaciones e Informática en el Sistema Defensivo Territorial es:

a. Garantizar el Enlace: Establecer y mantener redes de comunicación fiables entre el CEOFANB, las REDI, ZODI, ADI y las unidades de combate más bajas.
b. Asegurar la Redundancia y Resiliencia: Utilizar múltiples medios (radio, cable, satélite) y diversas bandas de frecuencia (HF, VHF, UHF) para que, si un sistema falla o es atacado, el flujo de órdenes y la información no se interrumpan.
c. Proveer Seguridad: Aplicar métodos de cifrado (codificación) y procedimientos estrictos para proteger la información sensible de la intercepción, localización (radiogoniometría) y el ciberataque enemigo.

3. El Rol del Oficial de Comunicaciones

El Oficial de Comunicaciones (u Oficial de C4I, que incluye Comando, Control, Comunicaciones e Informática) es el asesor del comandante en todos los asuntos de su área. Sus responsabilidades incluyen:

a. Planificación: Diseñar las redes de comunicaciones operativas y tácticas.
b. Operación: Poner en funcionamiento los equipos de radio, satélite y cable.
c. Seguridad: Implementar los procedimientos radiotelefónicos y de cifrado para evitar la fuga de información.
d. Mantenimiento: Asegurar el apresto operacional de todos los sistemas.

Es decir, las comunicaciones militares son un factor multiplicador de fuerza en el Sistema Defensivo Territorial; su buen funcionamiento permite una respuesta coordinada, oportuna y segura de todas las estructuras de defensa, desde el nivel estratégico hasta la Milicia en el área local.

4. Componentes del Sistema de Comunicaciones del Sistema Defensivo Territorial.

El sistema se puede dividir en tres grandes áreas interconectadas:

A) Comunicaciones Estratégicas y Operativas (El Esqueleto Institucional)

Este es el componente clásico militar, diseñado para el mando, control y coordinación de las Fuerzas Armada Nacional Bolivariana (FANB).

a. Redes de Radio Seguras: Sistemas de HF/VHF/UHF encriptados para comunicación táctica entre unidades terrestres, navales y aéreas.
b. Comunicaciones Satelitales: Teléfonos y terminales satelitales para garantizar el enlace en zonas remotas o cuando las infraestructuras terrestres fallan.
c. Fibra Óptica y Redes Privadas: El Estado ha invertido en su propia red de fibra óptica para conectar bases militares y centros de gobierno, buscando un canal seguro y de alta capacidad.
d. Sistemas de Ciberdefensa y Ciberataque: Unidades especializadas en proteger sus propias redes y, potencialmente, en neutralizar las redes enemigas.
e. Objetivo: Garantizar el Mando, Control y Comunicaciones (C3), permitiendo que el Alto Mando dirija las operaciones militares, comparta inteligencia en tiempo real y coordine la logística a nivel nacional.

5. Comunicaciones con la Población y Cuerpos de Reserva (El Tejido Social)

Este es el componente más distintivo del Sistema Defensivo Territorial, enfocado en la "Guerra de Todo el Pueblo". Utilizando diferentes medios:

a. Medios de Comunicación del Estado: Cadena nacional de radio y televisión (VTV, Radio Nacional, Venezolana de Televisión) para emitir directrices oficiales, alertas y discursos presidenciales.

b. Redes Sociales y Mensajería Instantánea: Uso intensivo de plataformas como Telegram, WeChat, Instagram, YouTube, TikTok son Canales oficiales del gobierno y de la FANB difunden información rápida, instrucciones de movilización y contra narrativas. Teniendo el Telegram especialmente la seguridad y capacidad para crear canales de difusión masiva.
c. Comunicación a Nivel Local: A través de los Jefes de Circuito Militar y los Consejos Federales de Gobierno, se busca establecer una red de comunicación que llegue directamente a las comunidades, organizaciones populares y la Milicia Nacional Bolivariana.
d. Objetivo: Movilización, adoctrinamiento y control social. Informar a la población sobre amenazas, organizar a la milicia y los cuerpos de reserva, coordinar la defensa de infraestructuras clave a nivel local (plantas de energía, puentes, etc.) y mantener la cohesión y la moral.

6. Guerra Psicológica y de la Información (El Frente Digital)

En el contexto moderno, el conflicto se libra tanto en el campo de batalla físico como en el espacio informativo.

a. Medios Públicos y Aliados: Uso de la televisión, radio y prensa nacional (como Correo del Orinoco), así como de medios internacionales aliados (como TeleSUR) para proyectar la narrativa oficial.
b. Operaciones en Redes Sociales: Creación y promoción de contenido que refuerza la soberanía nacional, desacredita a los adversarios (gobiernos extranjeros, oposición) y glorifica a la FANB. Esto incluye la activa participación de funcionarios y simpatizantes del gobierno.
c. Censura y Bloqueo: Capacidad para restringir el acceso a sitios web o plataformas digitales consideradas hostiles, y para limitar el acceso a internet en momentos de crisis (como se ha denunciado durante protestas).

d. Objetivo: Ganar la "batalla de las narrativas". Desmoralizar al enemigo, generar confusión, fortalecer la resistencia psicológica de la población y proyectar una imagen de fuerza y unidad, tanto hacia adentro como hacia afuera.

7. Desafíos y Vulnerabilidades del Sistema

A pesar del diseño integral, el sistema de comunicaciones del SDT enfrenta retos significativos:

a. Dependencia Tecnológica: La alta tecnología (satélites, componentes para redes encriptadas) a menudo proviene del extranjero (Rusia, China), lo que la hace vulnerable a sanciones o interrupciones en la cadena de suministro.
b. Fragilidad de la Infraestructura Crítica: La red eléctrica venezolana es extremadamente inestable. Los apagones masivos y frecuentes son la mayor amenaza para cualquier sistema de comunicaciones, dejando sin energía a repetidoras, centros de datos y estaciones de radio.
c. Brecha Digital y Cobertura: Aunque el uso de redes sociales es alto, existe una gran parte de la población en zonas rurales con acceso limitado o nulo a internet, lo que dificulta la comunicación capilar.
d. Credibilidad de la Fuente: La polarización política y la percepción de parcialidad de los medios estatales reducen su efectividad. Un segmento importante de la población no confía en la información oficial, lo que limita la capacidad de movilización unificada.
e. Seguridad Cibernética: A pesar de tener unidades de ciberdefensa, la infraestructura tecnológica del país es vulnerable a ataques preferidos por parte de actores estatales con mayores capacidades.

8. Ejemplos prácticos de su empleo

a. Ejercicios Militares "Escudo Bolivariano": Estos ejercicios anuales no solo prueban la capacidad de las tropas, sino que son un gran ensayo para todo el sistema de comunicaciones, desde el mando estratégico hasta la notificación a la población civil a través de cadenas nacionales y redes sociales.
b. Crisis Fronterizas: Durante el cierre de la frontera con Colombia en 2015 o la crisis diplomática de 2019, el sistema de comunicaciones fue clave para coordinar el despliegue militar, controlar la narrativa sobre la "amenaza" y justificar las acciones ante la población.
c. Intentonas de Golpe de Estado y Protestas: En eventos como el del 30 de abril de 2019, el control inmediato de las señales de radio y televisión y el uso masivo de las redes sociales por parte del gobierno fueron cruciales para desactivar la situación y presentar su versión de los hechos, evitando la propagación de información contraria.

En Venezuela, las comunicaciones en el Sistema Defensivo Territorial trascienden la función logística para convertirse en un arma estratégica y una herramienta de poder político. El modelo busca una simbiosis entre el mando militar y la participación civil, donde el flujo de información —tanto de arriba hacia abajo (directrices) como de abajo hacia arriba (reportes de situación)— es vital.

Sin embargo, su efectividad real está condicionada por su capacidad para superar sus propias vulnerabilidades, especialmente la precariedad de la infraestructura eléctrica y la desconfianza de una parte de la sociedad. El éxito o fracaso del Sistema Defensivo Territorial en una crisis hipotética no dependerá solo de las armas, sino de la resiliencia y el alcance de su sistema nervioso comunicacional.

La comunicación y la informática militar son elementos no negociables y estratégicos para la Fuerza Armada Nacional Bolivariana (FANB), especialmente en el marco del Plan Zamora 200 (enfocado en el orden interno y la disuasión de

amenazas a la seguridad nacional) y el Plan Independencia 200 (enfocado en la Defensa Integral y la resistencia popular frente a amenazas externas). Ambos planes, que promueven la unión cívico-militar-policial para la defensa territorial, dependen de la efectividad de estos sistemas para su éxito operativo y la preservación de la soberanía.

La función principal de las Comunicaciones es garantizar la relación de mando y la coordinación operacional en un entorno complejo y geográficamente disperso.

Tanto el Plan Zamora como el Plan Independencia se basan en el despliegue de la FANB y la Milicia Bolivariana en estructuras territoriales (REDI, ZODI, ADI). Las comunicaciones son el puente indispensable para que el Comando Estratégico Operacional (CEOFANB) pueda dirigir, planificar y controlar las operaciones en todos los niveles. Los sistemas informáticos son vitales para la recolección, procesamiento y difusión de inteligencia en tiempo real, esto permite a los cuerpos militares y de seguridad tomar decisiones rápidas y precisas ante amenazas, que van desde el crimen organizado transnacional hasta operaciones de desestabilización política.

Los planes exigen el movimiento de unidades y la activación de brigadas populares en áreas extensas, los sistemas de comunicaciones militares (radio, cable, satélite) deben ser móviles, robustos y resistentes a las interrupciones para asegurar la continuidad del servicio, la modernización de los Sistemas Transportables de Comunicaciones (como los que emplean frecuencias HF, VHF y TETRA) es un objetivo clave para mantener el apresto operacional y la capacidad de enlace en cualquier punto del territorio.

En escenarios de conmoción social o ataques a la infraestructura crítica los sistemas informáticos y de comunicaciones de la FANB son esenciales para proteger y gestionar el funcionamiento de los servicios públicos esenciales

(electricidad, agua, telecomunicaciones), impidiendo un colapso que provoque el caos.

En la dinámica de la Guerra Híbrida y la "Lucha No Armada", la seguridad de la información y la soberanía tecnológica adquieren una importancia crítica para la supervivencia del Estado-Nación.

La ciberguerra es vista como una amenaza latente que busca destruir o corromper la información y los sistemas de comando del enemigo, la Dirección de Tecnología e Información de las Comunicaciones del Ejercito Bolivariano se enfoca en establecer políticas de ciberdefensa para proteger los activos de información militar contra ataques internos y externos, garantizando la confidencialidad, integridad y disponibilidad de los datos.

En el marco del Plan Zamora, la seguridad informática es crucial para evitar la filtración de información sensible y contrarrestar las campañas de desinformación, engaño y manipulación de masas que se propagan a través de las redes sociales y otros medios electrónicos, buscando desmoralizar a la tropa y polarizar a la población, el desarrollo y la fabricación nacional de componentes, incluyendo sistemas de drones y equipos de comunicación militar, tienen como objetivo reducir la dependencia de proveedores extranjeros, lo cual es percibido como una vulnerabilidad en un conflicto.

El uso de métodos de cifrado y descifrado de mensajes (criptografía) en los equipos de radio es una práctica constante en el adiestramiento militar, indispensable para que las comunicaciones operacionales sean ininteligibles para cualquier adversario y se mantenga el secreto militar, fundamental para la sorpresa y el éxito táctico.

Los sistemas informáticos y de comunicaciones militares son más que herramientas; son el pilar habilitador de la doctrina de la Defensa Integral de la Nación y la ejecución de los planes Independencia y Zamora, su importancia radica en:

1. Garantizar la Cadena de Mando para un despliegue masivo y complejo.

2. Proteger el Estado de la ciberguerra y la guerra de la información.

3. Promover la Soberanía Tecnológica para mantener el apresto operacional ante cualquier contingencia externa.

También podemos hablar que, en el Plan Independencia, las Comunicaciones como Antídoto contra la Parálisis Estratégica que concibe con la estrategia nacional para enfrentar una agresión externa de alta intensidad y carácter híbrido, cuyo objetivo final es la "parálisis estratégica del país". Esta meta subraya la importancia absoluta de mantener operativos los sistemas de mando, control y las redes nacionales de información. La arquitectura de fases del plan revela una dependencia progresiva y crítica de las capacidades Comunicaciones y la Informática.

I. El Plan Zamora está dividido en diferentes fases:

1. Fase Plomo (Insurgencia/PCAE): Las acciones de exploración, neutralización y cerco dependen de un Sistema de Comando y Control ágil. La inteligencia de señales y las comunicaciones cifradas tácticas entre el Escalón Defensivo Territorial y el Escalón de Desgaste son vitales para identificar y aislar al enemigo en su fase inicial, impidiendo que consolide cabezas de playa informáticas o logísticas.

2. Fase Mercurio (Imposición de Pacificación): Al intentar impedir el acceso y persuadir, las operaciones de información se vuelven cruciales. La FANB requiere capacidades para emitir comunicados estratégicos, contrarrestar propaganda enemiga y mantener la moral de la población, utilizando todos los medios a su alcance, desde radiodifusoras estatales hasta redes sociales, protegidas por firewalls y sistemas anti-hackeo.
3. Fase Acero (Campaña Generalizada de Desgaste Sistemático): Esta es la fase más crítica para la infraestructura de Comunicaciones y la Informática. La mención explícita a la protección de infraestructura y su rehabilitación se traduce directamente en la ciberdefensa de los Sistemas que controlan la red eléctrica, el agua y el petróleo. Un ataque paralizante a estos sistemas lograría la parálisis estratégica que el plan busca evitar. La defensa anti-aérea, por su parte, depende de una red integrada de radares y sistemas de alerta temprana, cuyo corazón es un centro de computación de datos que procesa la información en tiempo real para dirigir las contramedidas. La incorporación del Escalón de Resistencia sugiere la preparación de redes de comunicaciones de respaldo y células de milicias con capacidad para operar en entornos de comunicaciones degradadas.
4. Fases Cobre y Bronce (Invasión Limitada y Aérea): El énfasis en el desgaste y la resistencia implica el uso de tácticas asimétricas. Aquí, las comunicaciones seguras y descentralizadas (como radios de largo alcance cifradas y enlaces satelitales tácticos) permiten a las unidades del Escalón de Resistencia operar de manera semiautónoma, hostigando al enemigo y reportando inteligencia, incluso si el comando central sufre interrupciones.
5. Fase Titanio (Guerra Popular Prolongada): Como fase final de contingencia, la Guerra Popular Prolongada depende de una arquitectura de comunicaciones resilientes y redundante. Se necesitarían redes clandestinas, protocolos de comunicación de baja probabilidad de interceptación (LPI/PI) y una logística de información que sobreviva a la ocupación o control enemigo de los nodos de comunicación principales. La informática se centraría en la preservación de

datos críticos y en sistemas de comunicación punto a punto extremadamente seguros.

La coherencia de la defensa, sustentada en el Escalón Defensivo Territorial a lo largo de todas las fases, solo es posible con un sistema de información unificado que permita visualizar el cuadro operacional completo, desde el nivel táctico local hasta el estratégico nacional.

II. El Plan Zamora: La Guerra Híbrida Interna y el Control del Espacio Informacional

El Plan Zamora representa la aplicación interna de la doctrina de defensa integral, concebido para restaurar el orden durante episodios de alteración del orden público en coordinación de la FANB, cuerpos de protección nacional y la Milicia Nacional en completa fusión. Su filosofía de derrotar a un "enemigo interno" mediante guerra asimétrica, híbrida y difusa coloca a las comunicaciones y la información en el centro de la contienda.

Análisis de las Amenazas y la Dimensión Ciber-Informática:

La lista de 20 amenazas que activan el Plan Zamora es un decálogo de vulnerabilidades nacionales, donde las Comunicaciones y la Informática tienen un rol protagónico:

La Amenaza a CANTV: La inclusión específica de "alteraciones en contra de los servicios básicos... CANTV" es la confirmación explícita de que la infraestructura de telecomunicaciones es un objetivo militar estratégico. Un ataque o sabotaje a CANTV no solo busca generar caos social, sino paralizar la capacidad de coordinación del Estado. Bajo el Plan Zamora, la protección de los centros de datos, las centrales telefónicas y las redes de fibra óptica de CANTV se convierte en una

misión prioritaria para la Guardia Nacional Bolivariana y otros componentes, requiriendo seguridad física y cibernética reforzada.

Guerra Económica y Control Logístico: Amenazas como la "parálisis del transporte", la "interrupción de la distribución de combustible" o el "acaparamiento" son, en esencia, problemas logísticos y de información. Contrarrestarlas exige sistemas informáticos de trazabilidad y control para monitorizar la cadena de suministro, redes de comunicación seguras para coordinar operativos de la GNB en puntos de distribución, y capacidades de ciber-inteligencia para identificar y desarticular redes de contrabando y especulación que se organizan, en parte, a través de medios digitales.

Coordinación Multi-Actor en Entornos Degradados: La filosofía del plan, que integra a la FANB con cuerpos de seguridad y la Milicia, presenta un desafío técnico enorme: lograr interoperabilidad entre sistemas disímiles. Mientras la FANB puede operar redes seguras cifradas, los grupos irregulares probablemente utilicen tecnologías comerciales (WhatsApp, radios comerciales). El plan debe prever protocolos de comunicación unificados, canales de emergencia y métodos para verificar la autenticidad de la información en un entorno de rumores y posible desinformación, que es característico de la guerra híbrida.

III. Síntesis Estratégica: El Rol Implícito y Decisivo de las Comunicaciones y la Informática en la Defensa Híbrida

La triangulación entre ambos planes revela un paradigma de defensa donde las Comunicaciones y la Informática son el elemento de cohesión. Aunque los documentos no listen hardware, la listica operacional demanda capacidades de Comunicaciones y la Informática avanzadas:

Resiliencia como Principio Central: Tanto la parálisis estratégica (Independencia) como la alteración de servicios básicos (Zamora) son dos caras de la misma moneda: la vulnerabilidad de la red nacional. La resiliencia tecnológica a través de redes independientes, energía de respaldo, centros de datos redundantes y protocolos de conmutación por error es el antídoto no declarado pero esencial.

La Columna Vertebral: La mención recurrente a "Escalones", "Control Operacional" y "Golpe y Maniobra" en el Plan Independencia, y la coordinación multi-agente en el Zamora, son inservibles sin un sistema de Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento integrado. Este sistema fusiona datos de radares, drones, informes de inteligencia humana y del Escalón Defensivo Territorial para crear una conciencia situacional única, permitiendo decisiones rápidas y precisas.

La Guerra Cognitiva e Informacional: Ambos planes reconocen un enemigo que opera en el espectro completo, incluido el cognitivo. La capacidad de proteger los propios medios de comunicación estatales de ciberataques, y al mismo tiempo, ejecutar operaciones de información y contra desinformación, es una capacidad implícita crítica para mantener la iniciativa narrativa y la cohesión social.

La comunicación militar son elementos no negociables y estratégicos para la Fuerza Armada Nacional Bolivariana (FANB), especialmente en el marco del Plan Zamora 200 (enfocado en el orden interno y la disuasión de amenazas a la seguridad nacional) y el Plan Independencia 200 (enfocado en la Defensa Integral y la resistencia popular frente a amenazas externas). Ambos planes que promueven la unión y coordinación rápida cívico-militar-policial, para la defensa territorial y lograr los objetivos fundamentales como lo son: la conducción operacional, la guerra de información/control del relato, y También dependen de la efectividad de estos sistemas para su éxito operativo y la preservación de la soberanía.

La Fuerza Armada Nacional Bolivariana, como cualquier fuerza armada moderna, depende de una estructura de comunicaciones Comando y Control (C2) y se integran en el concepto más amplio conocido como C4ISR (Comando, Control, Comunicaciones, Computadoras, Inteligencia, Vigilancia y Reconocimiento).

Los sistemas de comunicaciones de la Fuerza Armada Nacional Bolivariana son una mezcla de tecnología heredada, equipos de origen ruso, chino, irán. y algunos que se desarrollaron por las necesidades que se obtuvieron gracias a las sanciones internacionales que limitaron el acceso a tecnología occidental.

Estos sistemas de Radio Comunicaciones es el Pilar Fundamental en el Sistema Defensivo Territorial, ya que se convirtió en el medio más básico y extendido. Se dividen principalmente por bandas de frecuencia, cada una con un propósito táctico específico:

1. HF (Alta frecuencia - Onda Corta):

Comunicaciones de largo alcance (estratégicas y operativas), especialmente para unidades en áreas remotas como la selva amazónica o la frontera. No requiere línea de vista.

Características: Son vulnerables a la interferencia y al clima, pero fundamentales para la conexión entre grandes unidades y el alto mando. Suelen tener sistemas de cifrado de voz.

2. VHF/UHF (Muy alta Frecuencia):

Comunicaciones tácticas de corto y mediano alcance (línea de vista). Es el sistema principal para la infantería, unidades blindadas y aviación de bajo nivel.

Características: Ofrecen mayor calidad de voz y son más difíciles de interceptar que las HF. Los equipos modernos utilizan cifrado de salto de frecuencia para evitar la escucha e interferencia electrónica. Se utilizan radios portátiles, vehiculares y en centros de mando.

SECCIÓN B

COMUNICACIÓN POR SEÑALES VISUALES

1. INTRODUCCIÓN

En la doctrina militar bolivariana, nos adaptamos a las necesidades actuales de la Nación, en cuanto a la defensa integral, donde los escenarios de combate son cambiantes constantemente, nos enfrentamos a nuevos enemigos, y diversos escenarios. Durante las operaciones los comandantes deben mantener libertad de maniobra, mantener el ímpetu del ataque y evitar un combate extenso y costoso. Durante los combates, es muy importante lograr mantener las comunicaciones, utilizando cualquier medio disponible que sea necesario y que no nos delate frente al enemigo; mientras se logre mantener el contacto visual, se pasan señales a manera de difundir información y a veces son más fiables que las comunicaciones inalámbricas que nos pueden delatar, o que por el alto nivel de ruido en el combate, no se puedan escuchar las órdenes impartidas.

En este capítulo, se indican los aspectos fundamentales y básicos para que el personal profesional militar pueda, como comandante de pelotón, comandante de escuadra y jefe de equipo, incrementar el control sobre sus combatientes, emplear sus unidades subordinadas eficientemente y de igual forma proporcionar al personal subalterno, los conocimientos indispensables para desempeñarse eficientemente como parte de una unidad en combate, mejorando las técnicas para transmitir y recibir las órdenes. La intención es unificar los criterios de los combatientes de la

Fuerza Armada Nacional Bolivariana, especialmente, nuestras tropas terrestres sean a pie o en vehículos, y de esta manera, sin importar la unidad o región donde estén operando, mantener un criterio único y estandarizado al momento de utilizar las señales de brazos y manos.

La Fuerza Armada Nacional Bolivariana, en la actualidad está empleando en sus entrenamientos y maniobras el o de Resistencia Revolucionaria (MTRR), en el cual uno de los temas claves para todo comandante es mantener la comunicación con su personal, bajo las condiciones más adversas y de esta manera mantener el comando y control. En este caso sería; “Comandar con ayuda de gestos y señales de brazos de manos constituye un saber irremplazable que condiciona el completo dominio del acto elemental (comunicarse)”, lo cual resalta la importancia en el Sistema Defensivo Territorial, RESERVADO CEO – MC - RESERVADO establecer un lineamiento al momento de realizar operaciones militares y con este conocimiento mantener las comunicaciones.

2. JUSTIFICACIÓN

Cuando se esté en el fragor del combate, una de las principales adversidades va a ser el mantener el comando y control, debido a que las comunicaciones se pueden ver interrumpidas de muchas formas, por lo cual se plantean los siguientes escenarios:

a. Cuando fallen las comunicaciones inalámbricas.

b. Cuando el comandante tenga dificultad de comunicarse por los altos niveles de ruido en el campo de batalla.

c. Establecer comunicaciones en situaciones tácticas o situaciones de conducción, donde no es posible la comunicación verbal sin delatar su posición.

d. Las dificultades que el explorador u observador pueda tener al momento de transmitir información del enemigo a sus comandantes.

3. SEÑALES DE BRAZOS Y MANOS

Las señales que se muestran en esta propuesta son los medios comunes de transmitir mensajes visuales. Estas señales cuando las aplica el o la combatiente, le proporcionan un medio de comunicación que le permite un mayor control y coordinación entre él y otras personas o unidades. Ellas se deben dar correctamente y de una manera clara para que se puedan comprender. Se deben practicar hasta que su uso se convierta en costumbre.

Cuando uno o varios individuos de una unidad, han de ejecutar una acción o un movimiento, se debe dar una señal preliminar señalando hacia él o los individuos que ejecutarán el movimiento. A menos que se indique de otra manera, la persona que da la señal dará el frente a los individuos quienes van a recibir las instrucciones. Cuando se ha de ejecutar una acción o movimiento en conjunto, la señal de “ATENCIÓN” debe preceder a la señal de la acción o movimiento.

Es preferible una señal a una inacción; cuando se ha de utilizar una combinación de señales, deben darse en el orden en que se han de ejecutar. Por ejemplo, para dar la señal de reunirse en formación de columna de marcha, de primero la señal para reunirse y después la de columna de marcha. A continuación, serán mostradas ilustraciones que describen las señales de brazos y manos que son de uso más común, no obstante, a ello, estas señales no son exclusivas del jefe de escuadra o del comandante de pelotón, podrán establecerse señas particulares para diferentes actividades, estas señales que se indican se pueden repetir hasta que se confirmen o ejecuten.

a. Fundamentos para el empleo de las señales militares de brazos y manos Estas señales que se emplean deben tener tres premisas al momento de ser ejecutadas:

1) Mantener contacto visual: Es una manera efectiva de comunicarse cuando no se desea ser revelada nuestra posición o intenciones y a menudo es más confiable que el susurro de un micrófono de radio. Se debe tener un sistema estandarizado para el grupo o equipo. Cuando se esté en acción se debe mantener el contacto visual con los demás miembros del equipo cada quince segundo, por si alguno intenta indicar algo y el primero en visualizar la señal debe repetirla para asegurar que, si algún miembro del equipo aún no la ha visto, pueda recibir las órdenes.

2) Pasa las señales: Los miembros de los equipos de combate, deben acostumbrarse a pasar las señales, cuando un miembro del equipo utiliza una señal de brazos y manos, cada uno que la ve debe repetirla. Eso garantizará al comandante de equipo, comandante de escuadra o comandante de pelotón que la orden ha sido entendida, aumenta la posibilidad de comunicación a aquellos que se encuentren lejos en cualquier momento dado.

3) Todo el combatiente debe conocer las señales: Las señales de brazos y manos pueden utilizarse, así como están propuestas o modificarlas para un propósito concreto, pero en cualquier acción, se debe tener presente que cada uno del grupo la sepa y reconozca. Se recomienda al estar en marcha, mantener contacto visual con los otros miembros del equipo, para verificar que estén o no intentando pasar una información y repetir la información recibida, para comunicarse la a compañeros que no la hayan visto y para que el emisor sepa que la información ha sido recibida correctamente.

b. En el Sistema Defensivo Territorial se establece el Método Táctico de Resistencia Revolucionaria lo siguiente, en lo referente a las señales de brazos y manos: La comunicación por gestos debe cumplir con las siguientes condiciones:

1) Limitarse a los gestos reglamentarios conocidos por todos.

2) Efectuar gestos amplios y claramente separados de la silueta.

3) Efectuar los gestos con la mano “débil”, la mano “fuerte” debe estar con el armamento.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

CAPITULO XIII

CENTROS DE COMUNICACIONES

SECCIÓN A

1. GENERALIDADES DE LOS CENTROS DE COMUNICACIONES.
   a. Misión e importancia de las comunicaciones:

      La razón de ser de las comunicaciones militares y, por ende, del Centro General de Comunicaciones del Ejército Bolivariano radica en:

      1) Relación de Comando:

      Son esenciales para que el Ejército Bolivariano mantenga la relación de comando necesaria para el cumplimiento de las misiones, y permite las trasmisiones de ordenes e instrucciones del comandante y su estado mayor general.

      2) Administración y operación:

      Es la misión general del área de comunicaciones es administrar, planificar, operar, y mantener los sistemas de comunicaciones e informática del Ejército Bolivariano.

      3) Seguridad:

      Garantizan el comando y control, la confidencialidad, integridad y disponibilidad de los activos de información y comunicaciones protegiéndolo contra cualquier amenaza.

   b. Ubicación y rol del centro general de comunicaciones del Ejército Bolivariano (CGCEJB.)

      1) Está ubicada en la sede de la comandancia General del Ejército Bolivariano

      2) Cumple funciones como estación control de red, lo que implica supervisar directamente la capacidad de repuesta y preparación de todos los centros de comunicaciones del Ejército Bolivariano a nivel inferiores.

   c. Estructura y red de comunicaciones

a. El centro general de comunicaciones (CGCEJB), forma parte de la red más amplia de comunicaciones militares:

1) Dirección de Tecnología de la Información y la Comunicaciones, se encarga de controlar y evaluar las políticas tecnológicas y de Ciberseguridad.

2. PROPÓSITO DE LOS CENTROS DE COMUNICACIONES.

Establecer procedimientos para el uso de las instrucciones de Comunicaciones del Ejército Bolivariano, para regular la actividad operacional de los diferentes sistemas de comunicaciones disponibles (voz, data, video conferencia).

3. RESPONSABILIDADES DEL CENTROS DE COMUNICACIONES.

a. El Director de Tecnología de Información y las Comunicaciones a través del jefe del Centro General de Comunicación del Ejército Bolivariano, será responsable del cumplimiento de todas las normas e instrucciones establecidas en esta publicación. Así mismo deberá publicar las correcciones, alteraciones y cambios que hubiere lugar para mantener la actualización de las Instrucciones de las Comunicaciones.

b. Los Comandantes de Unidades Superiores, Tácticas, Fundamentales aisladas, Jefes de Centros de Tecnología de la Información y las Comunicaciones y los Jefes de los Centros de Adiestramiento de Combates del Ejército Bolivariano, Bases de Protección Fronterizas y Bases de Seguridad Territorial, serán responsables dentro de su jurisdicción por el cumplimiento de los procedimientos e instrucciones establecidas en esta publicación.

4. NORMAS GENERALES DE LOS CENTROS DE COMUNICACIONES.

a. Las Instrucciones Permanentes de Comunicaciones (IPC) están basadas en órdenes e instrucciones, que permiten el control y la coordinación de las comunicaciones que se emplean en las diferentes actividades operacionales y administrativas del Ejército Bolivariano, tanto en tiempo de paz, como de

excepción, constituye la guía necesaria para planificar las comunicaciones a fin de llevar a cabo el cumplimiento de la misión asignada.

b. Las normas prescritas constituyen órdenes del Comandante General del Ejército Bolivariano y como tal su incumplimiento podría acarrear sanciones disciplinarias acordes con la magnitud e importancia de la omisión, error o falta.
c. El uso indebido por parte de personal no autorizado, así como la pérdida total o parcial de este documento deberá ser participado inmediatamente a la Dirección de Tecnología de la Información y las Comunicaciones.
d. A cada una de las copias del documento se le asignará un número para facilitar su distribución y control.
e. En caso de integrarse cualquier elemento táctico, la Información que se requiera sobre facilidades de Comunicaciones será proporcionada por la DTIC. Para la realización de ejercicios y operaciones específicas o combinadas del ART-64 ley Constitucional de la FANB**,** donde se requiere el empleo de las comunicaciones con el CEOFANB, REDI, ZODI será empleado el INSCOFANB.

5. MARCO LEGAL:

a. Las principales leyes que establecen el marco de acción y las funciones de la FANB, en el área de comunicaciones son:

1) Constitución Nacional de la República Bolivariana de Venezuela
2) Ley Orgánica de la Fuerza Armada Nacional Bolivariana.
3) Del Código Orgánico de Justicia Militar; Título III de las Diversas Especies de Delitos.

4) Capítulo I de los Delitos Contra la Integridad, Independencia y Libertad de la Nación. Sección I de la Traición a la Patria. Artículo 464º Son Delitos de Traición a la Patria:

a. Formar parte de las fuerzas del enemigo.
b. Facilitar al enemigo exterior la entrada a la República o en cualquier forma el progreso de sus armas.

c. Practicar actos de hostilidad contra un país extranjero que expongan a Venezuela a peligro de guerra, ruptura de relaciones diplomáticas, represalias o retorsión.
d. Entrar en negociaciones con el enemigo para someter todo o parte del territorio de la República al dominio absoluto, mandato o protectorado extranjero.
e. Declararse en rebelión contra los Poderes Nacionales, si la República está empeñada en una guerra exterior.
f. Entregar indebidamente al enemigo las fuerzas o naves bajo su mando o, los lugares o elementos confiados a su custodia.
g. Fugarse en dirección al enemigo, estando en acción de guerra o dispuesto a entrar en ella.
h. Malversar caudales o efectos del Ejército en campaña, con daño de las operaciones de la guerra o perjuicio de las tropas.
i. Falsificar un documento referente al servicio militar o hacer, a sabiendas, uso de él cuando se emplee para causar perturbaciones o quebrantos en las operaciones de la guerra, u ocasione la entrega de una plaza o puesto militar.
j. Dar a sus superiores maliciosamente, noticias contrarias a lo que supiere acerca de las operaciones de la guerra.
k. Suministrar al enemigo memorias, datos o informes sobre la constitución, movilización, recursos, industrias de guerra fuerza o armamento de la Nación; revelar el plan de campaña o el secreto de alguna operación, expedición o negociación poner en su conocimiento el santo y seña o contraseña, órdenes y secretos militares, planos o descripciones de fortalezas, buques de guerra, arsenales, estaciones navales, plazas de guerra, canales, caminos, vías férreas, puertos, radas o aeropuertos, entregarles claves privadas para la situación y comunicación de las estaciones de iluminación, telegráficas, radiotelegráficas, telefónicas o radiotelefónicas y de otras instalaciones que deban mantenerse ocultas.
l. Arriar, mandar a arriar o forzar arriar la Bandera Nacional durante un combate con el fin de conseguir ventajas para el enemigo.

m. Impedir, con intención de favorecer al enemigo, que los buques o tropas nacionales reciban en tiempo de guerra los auxilios u órdenes que se les enviaren.
n. Impedir de cualquier modo el combate o el envío de auxilios para favorecer al enemigo.
o. Divulgar noticias que infundan pánico, desaliento o desorden en los buques o tropas, aun cuando sean verdaderas, siempre que se haya resuelto mantenerlas reservadas, o que tiendan a fomentar la dispersión de las tropas frente al enemigo, o ejecutar cualquier acto que pueda producir iguales consecuencias.
p. Mantener directa o indirectamente correspondencia con el enemigo sobre las operaciones de guerra de las Fuerzas Nacionales.
q. Poner en libertad a prisioneros de guerra con el fin de que vuelvan al ejército enemigo.
r. Servir de espía al enemigo u ocultar, hacer ocultar o poner a salvo a un espía o agente enemigo, si se conoce su condición.
s. Efectuar u ordenar reclutamiento dentro o fuera del territorio nacional, para engrosar las fuerzas del enemigo, seducir tropas de la Nación con el mismo fin o provocar la deserción de éstas.
t. Proporcionar al enemigo medios de hostilizar a la Nación o restar a ésta medios de defensa.
u. Servir de guía o piloto al enemigo para una operación militar o naval contra tropas o naves nacionales; o, siendo guía o piloto de éstas, desviarlas dolosamente del camino o rumbo que se proponían seguir.
v. Provocar la fuga o impedir la reacción en presencia del enemigo.
w. Tomar parte en maquinaciones para que un Jefe en operaciones de campañas, se rinda, capitule o se retire.
x. Inutilizar de propósito, en campaña o territorio declarado en estado de guerra, caminos, vías férreas, comunicaciones telegráficas o de otras clase y sus aparatos; causar averías de naves y demás elementos que estén al servicio de la Nación; destruir canales, puentes, obras de defensa, armas, municiones

o cualquiera otro material de guerra; o víveres para el abastecimiento de las fuerzas nacionales; interceptar convoyes o correspondencia; o de cualquier otro modo malicioso, poner entorpecimiento de las operaciones militares de las Fuerzas Armadas o facilitar las del enemigo.

y. Intentar por medios violentos cambiar la forma republicana de la Nación:
   1) Ponen en peligro la independencia de la Nación o la integridad de su territorio.
   2) Inducir o decidir a potencia extranjera a hacer la guerra contra la Nación, o atender en cualquier forma contra la soberanía nacional.
   3) Haber sido la causa de la derrota de las fuerzas nacionales.
   4) Impedir que una operación de guerra produzca las ventajas que debía producir.

   Del Código Orgánico de Justicia Militar; Título III de las Diversas Especies de Delitos. Capítulo I de los Delitos Contra la Integridad, Independencia y Libertad de la Nación. Sección II del Espionaje. Artículo 471º:

   Incurre en delito de espionaje toda persona que en cualquier sitio de la República o en alguna de la Embajadas, Legaciones, Consulados u otras oficinas venezolanas en el exterior, de cualquier manera, con el objeto de servir a un país extranjero con perjuicio para la República Bolivariana Venezuela.

6. EMPLEO DE LOS CENTROS DE COMUNICACIONES.
   a. Las instrucciones serán utilizadas por todas las Unidades del Ejército Bolivariano, empleándolas en ejercicios militares, situaciones de excepción, planes de campaña, y órdenes operacionales en existencia.
   b. La Dirección de Tecnología de la Información y las Comunicaciones, podrá dirigir mensajes de comprobación a los fines de verificar el conocimiento y correcto empleo de las (IPC) e (IOC), solicitando reportes diarios a las Unidades, así como realizar ejercicios planificados e imprevistos a fin de constatar la funcionalidad.

7. ALCANCE DE LOS CENTROS DE COMUNICACIONES.

a. El alcance ha sido desarrollado con el propósito de explicar la organización, procedimientos, normas y distribución de los Centros de Tecnología de la Información y las Comunicaciones del Ejército Bolivariano, tomando en cuenta el contenido del instructivo para la reorganización territorial de los Centros de comunicaciones de la Fuerza Armada Nacional Bolivariana (CEOFANB-DICOFANB-CC-01-14), según la organización del Componente Ejército, todos los Centros de Comunicaciones, (Centro Local de Tecnología de la Información y las Comunicaciones CLCTIC y Sub-Centro Local de Tecnología de la Información y las comunicaciones SCLCTIC), deberán mantener sus funciones como el organismo encargado del trámite y manejo de las comunicaciones dentro de la organización militar de comando, pero que se encuentra encuadrado en la organización operacional del sistema de comunicaciones de la FANB.

b. Las identificaciones de los Centros de Tecnología de Información y de las comunicaciones del Ejército Bolivariano serán las mismas estipuladas en el presente instructivo, con la salvedad que las que fueron escogidas por el CEOFANB, según el instructivo - CEOFANB DICOFANB-CC-01-14, mantendrán en forma operacional sus identificaciones, no dejando de cumplir las funciones según lo estipulado en el INSCOEJÉRCITO.

c. El Centro General de Tecnología de la Información y las Comunicaciones, prestara servicio al Comandante General y al Estado Mayor General del componente, así como darle facilidades al CEOFANB para su enlace con las Unidades o entidades, a través de los medios disponibles y los diferentes enlaces.

d. Organización**:** contiene una descripción detallada de los Centros de Tecnología de la Información y las Comunicaciones, delimitando su misión, funciones y organización.

1. CENTRO GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES:
   a. Misión:

      Procesar la transmisión, recepción, control y distribución de los mensajes oficiales u operaciones del Comando General del Ejército Bolivariano, con destino o provenientes de otras dependencias militares y civiles, mantener y operar los diferentes sistemas o medios disponibles con el propósito de permitir que el flujo de mensajes logre el cumplimiento de la misión asignada.

   b. Funciones:
      1) Procesar la correspondencia que origine el Comandante General del Ejército Bolivariano y su Estado Mayor General, así como otras dependencias orgánicas.
      2) Recepción y entrega de la correspondencia cuyo destino es el Comando General y el Estado Mayor o dependencias orgánicas.
      3) Supervisar que los operadores utilicen los medios adecuados para retrasmisión de mensajes originados del MPPD, CEOFANB, comando de componentes y dependencias militares de la FANB, así como las originadas desde las Unidades orgánicas del Ejército Bolivariano al Comando Superior.

   c. Organización:

      El Centro General de Tecnología de la Información y las Comunicaciones, está organizado por una jefatura, sección de medios, Centro de mensajes y la oficina de recepción, Información y entrega de documentos al público.

   d. Jefatura del Centro General de Tecnología de la Información y las Comunicaciones del Ejército Bolivariano:

      Es el responsable del funcionamiento del Centro General de Tecnología de la Información y las comunicaciones, manteniendo la disciplina, espíritu de cuerpo y moral del personal que labora en el centro.

e. Sección de Medios:

Es el responsable de operar, mantener la operatividad de los medios o factibilidades de comunicaciones instaladas. Tiene bajo su control los siguientes grupos de trabajo: la sección de medios alámbricos (Telefonía), sección de medios inalámbricos (Radios), Sistemas Informáticos y Criptografía.

f. Centro de Mensajes:

Es el responsable de procesar el tráfico de mensajes registrados por el Centro General de Comunicaciones del Ejército Bolivariano CGCEJB, llevando el control de la recepción, revisión, registro, transmisión, archivo y distribución.

g. Oficina de recepción, Información y entrega de documentos al público:

Es el responsable de recibir y distribuir, en forma permanente las correspondencias originadas o dirigidas al Comando General del Ejército Bolivariano y sus Unidades o dependencias orgánicas.

2. CENTRO LOCAL DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES:

a. Misión:

1) Transmitir, recibir y distribuir las correspondencias que se origine de y para las Unidades Orgánicas del Comando de la Unidad Superior, dependencias y Unidades del Ejército Bolivariano acantonadas en su jurisdicción.

2) Para los Centros locales que según el instructivo CEOFANB-DICOFANB-CC-01-14, cumplen la misión como ZODI o ADI, seguirán el cumplimiento del mencionado instructivo, pero el flujo de la correspondencia emanado de la Comandancia General del Ejército Bolivariano, debe cumplirse según lo estipulado por el INSCOEJÉRCITO.

b. Funciones:

1) Procesar la correspondencia de salida que se origine de y/o para todas las unidades orgánicas, dependencias o unidades militares del Comando de la Unidad Superior.
2) Recepción y entrega de todas correspondencias de entrada (radiogramas, oficios, etc.) en el menor tiempo posible.
3) La retransmisión de mensajes originados en un Sub-Centro Local con destino a Unidades orgánicas del comando de unidad superior, así como al Centro General de Comunicaciones del EJÉRCITO Bolivariano CGCEJB.

c. Organización:

1) Se mantiene el esquema del CGTIC.
2) Todos los Centros locales de Tecnología de Información y las Comunicaciones, estarán bajo el control administrativo y operativo de las unidades de tecnología y comunicaciones del Ejército Bolivariano.
3) En caso de ser ZODI o ADI, los CLTIC, deberán considerar el contenido del instructivo CEOFANB-DICOFANB-CC-01-14, para prestar el servicio en el momento que se requiera de acuerdo a su organización.

3. SUB-CENTRO LOCAL DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES:

a. Misión:

Transmitir, recibir y distribuir la correspondencia que se origine de y para las Unidades o dependencias acantonadas en el comando del fuerte o Bases de Protección Fronteriza y Base de Seguridad Territorial del Ejército Bolivariano.

b. Funciones:

1) Procesar la correspondencia de salida que se origine de y/o para las Unidades Tácticas y Fundamentales aisladas acantonadas en su área de responsabilidad.
2) Recepción y entrega de toda la correspondencia de entrada (radiograma, oficios, etc.) en el menor tiempo posible.

c. Organización:

1) Se mantiene el esquema del CGCEJB.
2) Todos los Sub-Centro Locales de Tecnología de la Información y las Comunicaciones estarán bajo el control administrativo y operativo de los comandantes de fuertes o del más antiguo de los comandantes de las Unidades Tácticas.
3) La existencia de dos (02) o más Unidades Tácticas o Fundamentales aisladas en una estructura o fuerte militar será obligatorio la creación de un SCLTIC.

8. PROCEDIMIENTOS DE LOS CENTROS DE COMUNICACIONES.

Contiene toda la Información relacionada con el manejo de la correspondencia de entrada y salida de los Centros de Tecnología de Información y las Comunicaciones.

1) Procedimiento para el manejo del mensaje de entrada:

a. El mensaje es recibido en la sección de medios por el operador de guardia, quien coloca el grupo fecha hora y los entrega al supervisor de guardia, después de haberlo asentado en la hoja de control del operador.
b. El supervisor de guardia verifica que el mensaje no tenga errores de recepción, lo asienta en la hoja de control y lo entrega al Centro de mensajes para asignarle el próximo número disponible en la hoja de control de entrada (formato CGE-CGTIC-05).
c. El anotador del Centro de mensaje completa la entrada del mensaje según requerimientos y selecciona el mensajero para llevar la comunicación a su destinatario.
d. Cuando el mensaje de entrada es clasificado. El supervisor de guardia verifica que el mensaje no tenga errores de recepción, lo registra en la hoja de control del supervisor y lo entrega en un sobre debidamente identificado al Centro de mensaje para asignarle el próximo número disponible en la hoja de control de entrada (formato CGE-CGTIC-05).
e. Se procede de la misma forma que el párrafo 3, añadiendo él envió de numero de control a criptografía, para su procesamiento y registro de archivos clasificados.

2. Procedimiento para el manejo del mensaje de salida:

a. El anotador de salida ejecuta las siguientes funciones:

1) Recibe la correspondencia (original y copia) del mensajero.

2) Revisa la legitimidad, su precedencia y la firma autorizada del oficial expedidor. Si la firma autorizada del oficial expedidor, si el mensaje no es legible o está incompleto, el anotador lo refiere al supervisor de guardia quien lo devuelve con la respectiva hoja de devolución.

3) Coloca el sello fechador sobre el original y copia del mensaje.

4) Asienta el mensaje en la hoja de control (formato CGE-CGTIC-05).

5) Con el mensaje ya procesado el supervisor selecciona el medio para su transmisión, lo registra en la hoja de control y lo entrega al operador para ejecutar su transmisión

3. Procedimiento para el manejo de la correspondencia en la oficina de recepción, Información y entrega de documentos al público:

a. El anotador recibe la correspondencia del Ejército Bolivariano de la dependencia emisora, verificando que tenga clara la dirección del destinatario, el número y sello de la dependencia (si la correspondencia presenta enmienda se devuelve con el sello del correo indicando la novedad).

b. Asigna el próximo número disponible en la hoja de control colocando el grupo fecha-hora y sello del correo a la correspondencia, enviándola a la sección de enrutamiento para su clasificación y ruta a seguir.

c. Con la correspondencia ya procesada en la sección de enrutamiento, el jefe de dicha sección selecciona la ruta para su distribución y entrega al destinatario.

9. NORMAS DE LOS CENTROS DE COMUNICACIONES.

Contiene las medidas a optimizar los diferentes registros que manejan los Centros de Tecnología de Información y las Comunicaciones, así como la especificación de cada uno de estos para asegurar que todos los integrantes actúen de acuerdo a la normativa vigente.

a. Consideraciones básicas de seguridad de comunicaciones:

Tomando en cuenta que, en la actualidad el uso de los diferentes medios de monitoreo o análisis del espectro electromagnético, los operadores deben cumplir con reglas básicas, las cuales deben ser cumplidas estrictamente, para evitar las perturbaciones o la radiolocalización de nuestras emisiones:

1) Deben ser normativa para transmitir algún mensaje clasificado, enviarlas cifradas y en modalidad seguro de los equipos utilizados para ellos (voz, data y video conferencia).
2) No se permitirá transmisión de mensajes cuando no hayan sido autorizados por el jefe del Centro o en su defecto por supervisor de guardia.
3) Antes de enviar cualquier mensaje por vía fonía, debe ser autenticado la base receptora.
4) Los mensajes enviados por vía Zimbra (data) deben ser confirmadas digitalmente por el sistema de mensajería y a su vez vía telefónica.
5) Para el momento de aplicar la modalidad de Centro Tácticos de Tecnología de Información y las Comunicaciones, se deben tomar las mismas consideraciones; pero, el tiempo de mantener un enlace no debe excederse de 5 minutos como norma para evitar su radiolocalización en caso de fonía.

A. Se deberán evitar las prácticas siguientes:

1. Empleo excesivo de potencia en la transmisión, no acorde con los requerimientos de enlace.
2. Empleo no autorizado del lenguaje claro de las frases de procedimientos radiotelefónico de las señales operativas aplicables.

B. Están prohibidas las prácticas siguientes:

1) Violación de radio-silencio.
2) Conversación entre operadores de asuntos no correspondientes a lo estipulado o no oficiales.
3) Lenguajes profanos, indecentes u obscenos.

C. Consideraciones básicas de seguridad física:

1) Evitar que personal ajenos o no autorizados, tengas acceso al material clasificado, por causas de descuido con este tipo de documentos, por lo que

se debe verificar siempre que este material sea dejado sobre los escritorios o tras-papelada, por lo que el jefe de Centro verificará al final de la jornada de trabajo la existencia de este material en esta condición.

2) No mostrar Información clasificada a ningún profesional en razón de su grado o posición y hacerlo solamente con las personas autorizadas que la requieran para su trabajo.

3) Establecer procedimientos de control a través de recibos, para la entrega y distribución del material procesados en el Centro.

4) El Centro de Comunicaciones no deberá permanecer sin custodia o bajo la responsabilidad de personas NO AUTORIZADAS.

5) En cuanto a las normas de Cripto-seguridad, el conocimiento o posesión del material clasificado deberá autorizarse solamente a aquellas personas cuyas funciones a si lo imponen.

D. Clasificación de seguridad:

1) Secreto:

Se asignará a la información es, documentos y materiales clasificados que requieran el más alto grado de protección y cuyo conocimiento y divulgación por parte de personas no autorizadas, puede causar graves daños a la nación de la República Bolivariana de Venezuela.

2) Confidencial:

Se asignará a la información es; documentos y materiales cuyo conocimiento y divulgación a personas no autorizadas pueden causar daños a los intereses Nacionales.

3) Reservado:

Se asignará a la información es, documentos y materiales que deben ser mantenidos fuera del alcance de personas no autorizadas.

E. Precedencia de los mensajes:

1) Urgente:

a. La correspondencia con esta precedencia tendrá prioridad de atención sobre todas las demás en el Centro de Tecnología de la Información y las comunicaciones.
b. Se asignará esta precedencia cuyo contenido sea de acción inmediata y que un retardo en su procedimiento pueda acarrear perturbaciones en la actividad administrativa y operacional.
c. Se incluye correspondencia cuyo contenido sea de índole operativa, como movimiento de Unidades, tropas y equipos.

2. Prioridad:

a. La correspondencia con esta precedencia será transmitida en forma prioritaria con relación a la ordinaria o de rutina.
b. Constituye la más alta precedencia que se le asigna a la correspondencia cuyo contenido o asunto sea de carácter administrativo.

3. Rutina:

a. La correspondencia con esta precedencia será transmitida en forma normal de acuerdo con el horario normal de labores del Centro de Tecnología de Información y las comunicaciones.
b. Se asignará esta precedencia a la correspondencia cuyo contenido o asunto, siendo de carácter administrativo, no tenga la suficiente importancia para justificar una precedencia más elevada.

F. Documentos relacionados con la administración del Centro de Tecnología de Información y las comunicaciones:

a. El Control de acceso al Centro de Tecnología de la Información y las comunicaciones (FORMATO CGE-CGTIC -01):

Este formato tiene la finalidad de controlar el acceso de personal al Centro de Tecnología de Información y las Comunicaciones, así mismo llevar la relación diaria de personal que ingresan al Centro, en la cual deberá plasmar su firma este formato también puede ser un libro foliado, llevando la misma forma.

1) Parte técnico Mensual (FORMATO CGE- CGTIC 02):

Este documento es una comunicación, en la cual los jefes de centros locales comunican mediante un mensaje de servicio al jefe de la Sección de Comunicaciones, las novedades de su dependencia y Sub-Centros, la Información comunicada se relaciona exclusivamente con el comportamiento de los equipos de los diferentes sistemas asignados.

2) Volumen de tráfico (FORMATO CGE- CGTIC 03):

Esta forma tiene como propósito informar el volumen de tráfico cursado mensualmente entre los Centros de Tecnología de la Información y las comunicaciones.

G. Registro de Correspondencia (FORMATO CGE- CGTIC-04):

Es un comprobante mediante el cual, los destinatarios de los mensajes constatan su recepción. Esta forma es preparada en el Centro de Mensaje y debe acompañar al mensaje en el momento de la entrega a su destinatario.

H. Control de Mensajes (FORMATO CGE- CGTIC 05):

Formulario preparado con la finalidad de asentar los mensajes y recibidos y transmitidos en los Centro de Tecnología de la Información y las Comunicaciones, constituye el registro principal relacionado con el control, de tráfico y establecimiento de responsabilidades (ver anexo 5)

I. Hoja de número del operador (FORMATO CGE- CGTIC -06):

Esta forma tiene como propósito asentarlos mensajes transmitidos y recibidos por los operadores; completando lo antes descrito en el punto 5, sirve como una constancia para el operador, de que el mensaje ha sido cursado o para aclarar cualquier acción e incidencia relacionada con el desempeño de sus funciones.

J. Hoja para devolución de mensajes (FORMATO CGE- CGTIC -07):

Esta forma es utilizada, a fin de dejar constancia de los mensajes devueltos por el Centro de Tecnología de Información y las Comunicaciones, debido a errores en su confección o ser firmados por personas no autorizadas como expedidores.

K. Control de llamadas radiotelefónicas (FORMATO CGE- CGTIC -08):

Mantiene un registro de los usuarios del sistema radiotelefónico y las ocurrencias relacionadas con el funcionamiento de la estación y

control de distribución (FORMATO CGE- CGTIC -09):

Normalmente se presentan en los Centros de Tecnología de Información y las Comunicaciones mensajes de tipo circular los cuales deben ser enviados a diversos destinatarios. Para el control apropiado de estas comunicaciones se ha ideado esta forma, la cual deberá ser anexada al mensaje original, en la misma deberán aparecer los organismos a los cuales se les va a enviar y en ella se anotará la fecha de transmisión y el nombre del Radio-Operador que recibió el mensaje.

L. Relación de Volumen de tráfico (FORMATO CGE- CGTIC -10):

Es un mensaje de servicio remitido al Centro de Tecnología de la Información y las Comunicaciones diariamente. Esta relación deberá coincidir con el Control de Mensajes, Hoja del Supervisor y Hoja del Operador del Centro.

M. Hoja de Control de Supervisor (FORMATO CGE- CGTIC -11):

Forma empleada para uso del supervisor de Guardia del Centro. Su propósito es relacionar las Comunicaciones recibidas y transmitidas a través del Centro durante el servicio las 24 horas.

11) Tareas de los Centros Generales de Comunicaciones (CGC).

a. El centro general de comunicaciones (CGC), es el centro de comunicaciones principal y se coordina con los demás centros de comunicaciones subordinadas. Sus tareas se pueden resumir en:

1) Mantener el enlace y la red de comunicación.

a) Trasmisión y recepción:

Es garantizar la transmisión, recepción, control y distribución de la correspondencia, reportes e instrucciones entre el comando general del Ejército y sus unidades subordinadas.

b) Integración:

Mantener el enlace con los centros de comunicaciones con los Grandes Comando y las Unidades Superiores del Ejército Bolivariano.

1) Soporte al Mando y Control:

Prever que los medios tecnológicos y humanos para que el comandante general del Ejército Bolivariano para que ejercer el comando efectivo, mediante él envió seguro y rápido de ordenes e instrucciones a las unidades subordinadas.

a) Flujo de información:

Facilitar el flujo de información obtenida del reconocimiento y de otras unidades en contacto con el enemigo hacia los puestos de comando.

b) Participar en la integración del sistema de comando, control, comunicaciones, inteligencia, contrainteligencia y vigilancia de la FANB.

“PÁGINA DEJADA EN BLANCO A EX PROFESO”

REFERENCIAS BIBLIOGRÁFICAS

- Constitución de la República Bolivariana de Venezuela, gaceta oficial N° 5.908, 2000.
- Ley Constitucional de la FANB, 2020.
- Manual de Comunicaciones MT-24-01, Ejército Bolivariano, 1993.
- Inscoejército, 2022.
- Reglamento sobre el servicio de los radioaficionados, 1993
- Apoyo electromagnético en guerra electrónica https://www.google.com/search?q=apoyo+electromagnetico+en+guerra+electronica&rlz=1C1MYPO_enVE1179VE1181&oq=apoyo+electromagnetico+en+guerra+electronica&gs_lcrp=EgZjaHJvbWUyCwgAEEUYChg5GKABMgkIARAhGAoYoAHSAQk5NTAwajBqMTWoAgiwAgHxBeFsE21LKLDx8QXhbBNtSyiw8Q&sourceid=chrome&ie=UTF-8&sxsrf=ANbL-n505I6R_idMsZhOGv7EVbSxamzocw:1768347986774&sec_act=sr
- Ataque Electrónico https://www.google.com/search?q=Ataque+Electr%C3%B3nico+%28EA+-+Electronic+Attack%29&rlz=1C1MYPO_enVE1179VE1181&oq=apoyo+electromagnetico+en+guerra+electronica&gs_lcrp=EgZjaHJvbWUyCwgAEEUYChg5GKABMgkIARAhGAoYoAHSAQk5NTAwajBqMTWoAgiwAgHxBeFsE21LKLDx8QXhbBNtSyiw8Q&sourceid=chrome&ie=UTF-8&sxsrf=ANbL-n505I6R_idMsZhOGv7EVbSxamzocw%3A1768347986774&sec_act=sr&mstk=AUtExfBd0ZMjeqUBDWx-3QNcWjSav4s2k6HYE-1qq8iluRo71NT9q6bY20CUSX4mNwATOnGNl6Ip338ufjI12kcvYm_vTDaVzLOjF_OodAOmqZobEAmd9mn4kEdeKdWTyKhTz3ypI5HvByPdmoWhKKu6SFiCYbTAhy_zj7JCuwWHVjifaQIwh1XbMS3Y-i7PKs5XkXakOZIgK3I8CYGUTbeIagwG3R-VSoWZYLnV7CQvVm0sxXIYAN1ytLJWerOoc5iIGpMU5GyZygv0WS139QBYGQwI&csui=3&ved=2ahUKEwiz0JbN2YmSAxXoRjABHdVjJXwQgK4QegQIAxAF
- Operaciones Electromagnéticas https://www.google.com/search?q=operaciones+electromagnetica&rlz=1C1MYPO_enVE1179VE1181&oq=operaciones+electromagnetica&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCggCEAAYgAQYogQyCggDEAAYgAQYogQyCggEEAAYgAQYogQyBwgFEAAY7wXSAQozNzc3Mmowajo1qAIIsAIB8QWwetI20dERzw&sourceid=chrome&ie=UTF-8

- Protección Electromagnética
https://www.google.com/search?q=Protecci%C3%B3n+electromagn%C3%A9tica%3A+&sca_esv=d9f24a9a5aa894d8&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifMcjgO7CMEdK8jgfyHIw0Thcl38uA%3A1761157590152&ei=1iH5aM2CCYKywt0PiOSbgAg&ved=0ahUKEwjNxbekt7iQAxUCmbAFHQjyBoAQ4dUDCBE&uact=5&oq=Protecci%C3%B3n+electromagn%C3%A9tica%3A+&gs_lp=Egxnd3Mtd2l6LXNlcnAiH1Byb3RlY2Npw7NuIGVsZWN0cm9tYWduw6l0aWNhOiAyBRAAGIAEMgYQABgWGB4yBhAAGBYYHjIGEAAYFhgeMgYQABgWGB4yBhAAGBYYHjIGEAAYFhgeMgYQABgWGB4yBhAAGBYYHjIGEAAYFhgeSPgQUABYAHAAeAGQAQCYAeAJoAHgCaoBAzctMbgBA8gBAPgBAvgBAZgCAaAC6QmYAwCSBwM3LTGgB6cHsgcDNy0xuAfpCcIHAzItMcgHBw&sclient=gws-wiz-serp

- Pulso electromagnético (EMP)
https://www.google.com/search?sca_esv=07cdbffa48f41bdb&rlz=1C1MYPO_enVE1179VE1181&cs=0&sxsrf=ANbL-n7OdY-MZZ2nHn7euw3Rd-OPG59D7A:1768348025476&q=Pulso+electromagn%C3%A9tico+(EMP)&sa=X&ved=2ahUKEwiW2teh7bWQAxUoRTABHU2aNigQxccNegQIKhAB&mstk=AUtExfDdrMbO9QEPcDUh-flr1VTB9Q4YWTmnOTiVwIiPqsayu387BYsY4IG2vKxOVnWNKiClRq_D99LbNVum-MiT8qReAZ8XBlJ-PQLN4E67is1u_F1HmgAOLjB1XoJt61hjhzux6rB_SQQfsyf_VfmVhoSkzeybVOE-3rja-SGLp1CGplGOwgku5OQfg0tjEDlNwHsNBBuHnEl036vc5jGkMm_tHgUNjVyDqC3jI6tbgzgXiE0_0RDOVKlfRa9evzcBkCAQJ2Po6hSzMyDC0p2BiJQK&csui=3&sec_act=sr

- Supresión de defensas aéreas enemigas
https://www.google.com/search?q=Supresi%C3%B3n+de+defensas+a%C3%A9reas+enemigas&sa=X&sca_esv=07cdbffa48f41bdb&rlz=1C1MYPO_enVE1179VE1181&cs=0&sxsrf=ANbL-n7LQcCncQobd4AlKrRLfUXYOC72bg%3A1768348037600&udm=50&fbs=ADc_l-bpk8W4E-qsVlOvbGJcDwpn60DczFdcvPnuv8WQohHLTbSVldBrj9mdwFjfwIgEUgSngOnSDVho99FxfCho2PSKWFrG-0tujUbE5EZVZqGupc2XtHwbeOHCQf4yNg3RGaUY4ruUpCA52nQoJOBN4IK6-l3FMtyrmUHGbrvtC3yN9qzdC5WdG_eXWQZmfwsUujGf48XCVDCdVvfbD_oiMDlbSLcCzw&aep=1&ntc=1&ved=2ahUKEwivg_vk2YmSAxV6mbAFHVV4IGwQ2J8OegQIDRAE&biw=1536&bih=730&dpr=1.25&aic=0&mstk=AUtExfDhNTAcF-Rge0xhMK5G-FuZZ-cAhLSLnr9DfSR-nGuDLXxfOyXa5_1Nb0quI3IkQpLEfSI8ZdDqHRPzCdmYUdpmJsVLBFbG8A7eRFsGSAG2CPnsyUXarCD8dObKgajiclAQgSQ3pn5ohW_FSm_n3d9R3f_zQ-BeZeU&csuir=1&mtid=gd1madyHCLKdwbkP-sKjwQE

- Antecedentes de vehículo no tripulados
  https://www.google.com/search?q=antecedentes+de+vehiculo+no+tripulados&sca_esv=d029728c4f6818f7&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifOI_jOt_1K5DS7ICrPEX2h4a6Mixg%3A1761267635572&ei=s8_6aKbXIoOLwbkPq-uxCQ&ved=0ahUKEwjm_Jae0buQAxWDRTABHat1LAEQ4dUDCBE&uact=5&oq=antecedentes+de+vehiculo+no+tripulados&gs_lp=Egxnd3Mtd2l6LXNlcnAiJmFudGVjZWRlbnRlcyBkZSB2ZWhpY3VsbyBubyB0cmlwdWxhZG9zMggQABiABBiiBDIFEAAY7wUyBRAAGO8FSKkPUNAHWNAHcAF4AZABAJgBvQGgAb0BqgEDMC4xuAEDyAEA-AEBmAICoALJAcICChAAGLADGNYEGEeYAwCIBgGQBgiSBwMxLjGgB5cEsgcDMC4xuAfCAcIHAzItMsgHCA&sclient=gws-wiz-serp

- Drones Marítimos Comunicaciones Militares
  https://www.google.com/search?q=drones+maritimos+comunicaciones+militares&sca_esv=d029728c4f6818f7&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifM2XgjR905V2W8NiHDyBidyaQ_8fg%3A1761265395960&ei=88b6aPCrOoaWwbkPy7z74AM&ved=0ahUKEwiw8Z_yyLuQAxUGSzABHUveHjwQ4dUDCBE&uact=5&oq=drones+maritimos+comunicaciones+militares&gs_lp=Egxnd3Mtd2l6LXNlcnAiKWRyb25lcyBtYXJpdGltb3MgY29tdW5pY2FjaW9uZXMgbWlsaXRhcmVzMgUQIRigATIFECEYnwVIkzJQqwVYiS1wAXgAkAEAmAH7AaABzBuqAQYwLjIzLjK4AQPIAQD4AQGYAhqgAvEcwgIIEAAYgAQYsAPCAgcQABiwAxgewgIIEAAYsAMY7wXCAgUQABiABMICBhAAGBYYHsICCBAAGIAEGKIEmAMAiAYBkAYFkgcGMS4yMi4zoAfWfLIHBjAuMjIuM7gH4BzCBwgwLjE2LjguMsgHXA&sclient=gws-wiz-serp

- Drones Marítimos uso Comunicaciones Militares
  https://www.google.com/search?q=drones+maritimos+uso+comunicaciones+militares&sca_esv=d029728c4f6818f7&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifNTvx1lKx6SAX_tTKNQMQOP9OCNoA%3A1761266449135&ei=Ecv6aMz7B_eIwbkP25qOoA8&ved=0ahUKEwiMyLjozLuQAxV3RDABHVuNA_QQ4dUDCBE&uact=5&oq=drones+maritimos+uso+comunicaciones+militares&gs_lp=Egxnd3Mtd2l6LXNlcnAiLWRyb25lcyBtYXJpdGltb3MgdXNvIGNvbXVuaWNhY2lvbmVzIG1pbGl0YXJlczIIEAAYgAQYogQyCBAAGIAEGKIEMggQABiABBiiBDIFEAAY7wVI7hBQ5wVY9Q1wAXgBkAEAmAGiAqABwQaqAQUwLjIuMrgBA8gBAPgBAZgCBaAC9gbCAgoQABiwAxjWBBhHwgIHECMYsAIYJ8ICBBAhGAqYAwCIBgGQBgiSBwUxLjIuMqAH0xKyBwUwLjIuMrgH3QbCBwcwLjEuMy4xyAcc&sclient=gws-wiz-serp

- Los Drones Marítimos.
  https://www.google.com/search?q=drones+maritimos&rlz=1C1MYPO_enVE1179VE1181&oq=drones+maritimos&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORiABDIHCAEQABiABDIICAIQABgWGB4yCAgDEAAYFhgeMggIBBAAGBYYHjIICAUQABgWGB4yBwgGEAAY7wUyCggHEAAYgAQYogQyCggIEAA

YgAQYogQyCggJEAAYgAQYogTSAQk2NDEyajBqMTWoAgywAgHxBXFlKhFQ3NO_&sourceid=chrome&ie=UTF-8

- Nombres que reciben los drones
https://www.google.com/search?q=nombres+que+reciben+los+drones+de+drones&sca_esv=d029728c4f6818f7&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifNN0VSMiiJSXg5vKt-gXNx6dcf3qA%3A1761268763829&ei=G9T6aL6wMuSNwbkPrtDECA&ved=0ahUKEwj-qZa41buQAxXkRjABHS4oEQEQ4dUDCBE&uact=5&oq=nombres+que+reciben+los+drones+de+drones&gs_lp=Egxnd3Mtd2l6LXNlcnAiKG5vbWJyZXMgcXVlIHJlY2liZW4gbG9zIGRyb25lcyBkZSBkcm9uZXMyCBAAGIAEGKIEMggQABiABBiiBDIIEAAYgAQYogQyBRAAGO8FMggQABiABBiiBEipQFCAFFjlPnAEeAGQAQCYAZEDoAHtJKoBCjAuMTYuNC4zLjG4AQPIAQD4AQGYAg2gAqkNwgIKEAAYsAMY1gQYR8ICBxAjGLACGCfCAgYQABgNGB7CAggQABgFGA0YHsICCBAhGKABGMMEwgIEECEYCpgDAIgGAZAGCJIHBzQuNi4yLjGgB4NnsgcHMC42LjIuMbgHjQ3CBwcwLjQuOC4xyAcx&sclient=gws-wiz-serp

- Vehículo Terrestre No Tripulado
https://www.google.com/search?q=VEHICULO+TERRESTRE+NO+TRIPULADO&sca_esv=d029728c4f6818f7&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifPkAk9Yt8bhUoZRWDJWv7La6Jp0IQ%3A1761268780789&ei=LNT6aIf3L42DwbkPl4ud2Aw&ved=0ahUKEwiHvaHA1buQAxWNQTABHZdFB8sQ4dUDCBE&uact=5&oq=VEHICULO+TERRESTRE+NO+TRIPULADO&gs_lp=Egxnd3Mtd2l6LXNlcnAiH1ZFSElDVUxPIFRFUlJFU1RSRSBOTyBUUklQVUxBRE9IpzhQAFi_NXABeAGQAQCYAb8BoAG3GaoBBTIwLjEyuAEDyAEA-AEBmAIVoAK3EagCFMICCxAuGIAEGLEDGIMBwgIIEAAYgAQYsQPCAgsQABiABBixAxiDAcICBRAuGIAEwgIFEAAYgATCAhEQLhiABBixAxjRAxiDARjHAcICGhAuGIAEGLEDGIMBGJcFGNwEGN4EGOAE2AEBwgINECMYgAQYJxiKBRjqAsICBxAjGCcY6gLCAhAQLhgDGLQCGOoCGI8B2AEBwgIQEAAYAxi0AhjqAhiPAdgBAcICBBAjGCfCAgoQIxiABBgnGIoFwgIIEC4YgAQYsQPCAgoQABiABBhDGIoFwgIOEC4YgAQYsQMY0QMYxwHCAg0QABiABBixAxhDGIoFwgIKEAAYgAQYFBiHAsICBhAAGBYYHsICCBAAGBYYChgemAMH8QVvzi7dBzMcCboGBggBEAEYFJIHBDcuMTSgB5C7AbIHBDYuMTS4B7ARwgcGMC4xNy40yAc-&sclient=gws-wiz-serp

- Vehículo de Submarino No Tripulado (USV): siglas en ingles
https://www.google.com/search?q=Veh%C3%ADculo+de+Submarino+No+Tripulado+%28USV%29%3A+siglas+en+ingles&sca_esv=f6d19e7077c59f8e&rlz=1C1MYPO_enVE1179VE1181&sxsrf=AE3TifPmuOydlBIKsYTtfR64gcZJhBCQpw%3A1761269838286&ei=Ttj6aN6gEc6XwbkPgaKEgAI&ved=0ahUKEwje_8G42buQAxXOSzABHQERASAQ4dUDCBE&uact=5&oq=Veh%C3%ADculo+de+Submarino+No+Tripulado+%28USV%29%3A+siglas+en+in

gles&gs_lp=Egxnd3Mtd2l6LXNlcnAiO1ZlaMOtY3VsbyBkZSBTdWJtYXJpbm8gTm8gVHJpcHVsYWRvIChVU1YpOiBzaWdsYXMgZW4gaW5nbGVzMggQABiABBiiBDIIEAAYgAQYogQyBRAAGO8FMggQABiABBiiBEidJVCtEljZInABeAGQAQCYAZ0BoAHGB6oBAzAuOLgBA8gBAPgBAZgCCKAC4gbCAgoQABiwAxjWBBhHmAMAiAYBkAYIkgcDMS43oAfvJrIHAzAuN7gH3QbCBwUwLjcuMcgHDw&sclient=gws-wiz-serp

- Vehículo de Superficie No Tripulado (USV): siglas en ingles https://www.google.com/search?q=Veh%C3%ADculo+de+Superficie+No+Tripulado+(USV)%3A+siglas+en+ingles&rlz=1C1MYPO_enVE1179VE1181&oq=Veh%C3%ADculo+de+Superficie+No+Tripulado+(USV)%3A+siglas+en+ingles&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCjExNDU0ajBqMTWoAgiwAgHxBaRaQwmVcvD2&sourceid=chrome&ie=UTF-8