MINISTERIO DE DEFENSA

COMUNICACIONES

SEGURIDAD DE COMUNICACIONES

LIMA – PERU

MINISTERIO DE DEFENSA

Lima, 24 de Julio del 1,998

COMUNICACIONES

SEGURIDAD DE COMUNICACIONES

		Párr	Pág
CAPITULO 1. GENERALIDADES			
Sección I.	**INTRODUCCION**		
	Finalidad.....	**01**	**07**
	Alcance.....	**02**	**07**
Sección II.	**SEGURIDAD DE LAS OPERACIONES (SEGOPE)**		
	Consideraciones Generales.....	**03**	**08**
	Concepto generales sobre Comando y Control (C^2).....	**04**	**09**
	Guerra de Comando y Control.....	**05**	**10**
	Tareas Críticas para los recursos de Guerra Electrónica.....	**06**	**11**
	Contra-medidas de Comando, Control y Comunicaciones.....	**07**	**13**
	Concepto de SEGOPE.....	**08**	**13**
	Categorías de las Medidas de SEGOPE.....	**09**	**13**
	Responsabilidades dentro del Proceso de SEGOPE.....	**10**	**15**
	Programa de SEGOPE.....	**11**	**18**
Sección III.	**PROCESO DE SEGURIDAD DE LAS OPERACIONES**		
	Concepto del Proceso de SEGOPE.....	**12**	**20**
	Paso 1: Identificar los Elementos de Búsqueda y Recolección enemiga.....	**13**	**21**
	Paso 2: Identificar los Perfiles de Nuestras Fuerzas y Recomendar Elementos esenciales de Información Amiga.....	**14**	**22**
	Paso 3: Identificar las vulnerabilidades de dades de nuestra fuerza.....	**15**	**28**
	Paso 4: Realizar análisis de riesgo		

y seleccionar EEIA..... 16 30
Paso 5: Recomendar medidas de SEGOPE (Contramedidas)..... 17 31
Paso 6: Seleccionar medidas de SEGOPE..... 18 33
Paso 7: Aplicar medidas de SEGOPE..... 19 34
Paso 8: Dirigir los esfuerzos para monitorear la efectividad de la aplicación de de medidas de SEGOPE..... 20 36
Paso 9: Monitorear la efectividad de las medidas de SEGOPE..... 21 36
Paso 10: Recomendar reajustes a las medidas de SEGOPE..... 22 37

Sección IV. CONTRAINTELIGENCIA

Conceptos Generales sobre Contra-inteligencia..... 23 38
Actividades de Contrainteligencia..... 24 38
Interfase de la Contrainteligencia con el Proceso SEGOPE..... 25 40
Base de datos de Contrainteligencia..... 26 43

CAPITULO 2. INTELIGENCIA Y CONTRAINTELIGENCIA DE TELEMÁTICA

Sección I. INTELIGENCIA DE TELEMÁTICA

Concepto de Inteligencia de Telemática..... 27 44
Clasificación de la INTETE..... 28 44
Proceso de INTETE..... 29 45

Sección II. CONTRAINTELIGENCIA DE TELEMÁTICA (C-INTETE)

Consideraciones Generales de C-INTETE..... 30 47
Proceso de C-INTETE..... 31 47
Base de Datos para el Proceso de C-INTETE..... 32 49
Evaluación de la Amenaza Electromagné-tica..... 33 55
Evaluación de nuestras vulnerabilidades Electromagnéticas..... 34 58
Desarrollo de las Opciones de Contramedida..... 35 62
Evaluación de la Aplicación de las

Contramedidas..... 36 64

CAPITULO 3. SEGURIDAD DE TELEMÁTICA

Sección I. GENERALIDADES

Concepto de Seguridad de Telemática..... 37 66
Necesidad de la SEGUTE..... 38 66
Relación de la SEGUTE con la C-INTETE 39 67
Funciones de Apoyo de la SEGUTE..... 40 67

Sección II. EVALUACION DE LAS VULNERABILIDADES DE SEGURIDAD DE TELEMÁTICA

Concepto de la Evaluación de las vulnera-bilidades de Seguridad de Telemática..... 41 70
Consideraciones generales sobre nuestras vulnerabilidades..... 42 70
Procedimiento que sigue la evaluación de las vulnerabilidades de SEGUTE..... 43 71
Determinación de rasgos, patrones y perfiles Electromagnéticos..... 44 71
Identificación de emisiones interrelacionadas (descriminadores)..... 45 74
Determinación de potenciales vulnerabilida-des..... 46 74
Graficación de las trayectorias de trasmi - sión e identificación de probables vulerabili-dades..... 47 74

Sección III. SUPERVISION DE SEGUTE

Propósito de la Supervisión de SEGUTE.... 48 76
Forma de conducir la supervisión de SEGUTE..... 49 76
Supervisión de la Evaluación de la amenaza electromagnética..... 50 77
Entrevistas y observaciones de SEGUTE..... 51 78
Informes de resultados de la supervisión de SEGUTE..... 52 78

CAPITULO 4. SEGURIDAD DE COMUNICACIONES

Sección I. CONCEPTO, CLASIFICACION Y RESPONSABILIDADES DE LAS SEGCOM

Concepto de SEGCOM.....	**53**	**80**
Clasificación de la SEGCOM.....	**54**	**80**
Responsabilidades de la SEGCOM.....	**55**	**81**

Sección II. SEGURIDAD FISICA DE COMUNICACIONES

Concepto de Seguridad Física de Comunicaciones.....	**56**	**84**
Consideracioes Generales sobre la Seguridad Física de Comunicaciones.....	**57**	**84**
Finalidad de la Seguridad Física de Comunicaciones.....	**58**	**85**
Medidas de Seguridad Física en los Centros de Comunicaciones permanentes.....	**59**	**85**
Medidas de Seguridad Física en los Centros de Comunicaciones de campaña.....	**60**	**88**
Seguridad Física del Material criptográfico.....	**61**	**91**

Sección III. SEGURIDAD CRIPTOGRAFICA

Concepto de Seguridad Criptográfica.....	**62**	**95**
Consideraciones Generales sobre Seguridad criptográfica.....	**63**	**95**
Finalidad de la Seguridad Criptográfica	**64**	**96**
Sistema Criptográfico.....	**65**	**96**
Técnicas para asegurar la Seguridad Criptográfica.....	**66**	**97**
Sistema de Código.....	**67**	**98**
Criptografiado de Mensajes.....	**68**	**99**
Reglas Fundamentales de Seguridad Criptográfica.....	**69**	**100**
Grado de Seguridad Criptográfica de un sistema.....	**70**	**104**
Factores Fundamentales en el establecimiento de un Sistema Criptográfico.....	**71**	**104**
Requisitos específicos que debe satisfacer un Sistema Criptográfico para uso militar en		

en general..... 72 105

Sección IV. SEGURIDAD DE TRASMISION

Concepto de Seguridad de Trasmisión..... 73 108
Medidas generales de SEGTRAS contra la interceptación..... 74 108
Medidas específicas de SEGTRAS contra la Interpretación..... 75 110
Codificación de voz (Seguridad Criptofónica)... 76 114
Seguridad de Trasmisión en el Sistema de Comunicaciones Permanente..... 77 115
Seguridad de Trasmisión en los sistemas de comunicaciones de Campaña..... 78 117
Medidas de SEGTRAS contra el engaño Electromagnético..... 79 120
Medidas de SEGTRAS contra la perturbación.... 80 139

Sección V. SEGURIDAD DE EMISION (TEMPEST)

Concepto de Seguridad de Emisión..... 81 141
Actividades o medidas de SEGEMI..... 82 141
Responsabilidades en la SEGEMI..... 83 142
Asistencia Técnica de TEMPEST..... 84 142
Inspecciones Técnicas de TEMPEST..... 85 142
Pruebas de Campo de TEMPEST..... 86 142
Pruebas y Análisis en ambientes controlados... 87 143
Certificación de Seguridad automática de Comunicaciones de Voz..... 88 143
Vigilancia de lugares TEMPEST..... 89 143

CAPITULO 5. SEGURIDAD ELECTRONICA

Sección I. GENERALIDADES

Inteligencia Electrónica del Adversario..... 90 144
Concepto de Seguridad Electrónica..... 91 144

Sección II. AREAS FUNCIONALES DE LA SEGELEC

Programa de SEGELEC.....	**92**	**145**
SEGELEC Inherente.....	**93**	**146**
SEGELEC Industrial.....	**94**	**146**
SEGELEC Operacional.....	**95**	**147**

CAPITULO 6. CENSURA DE COMUNICACIONES

Riesgo de Censura.....	**96**	**148**
Medidas de Control de Censura.....	**97**	**148**
Técnicas para asegurar la Censura.....	**98**	**148**
Prevención de los riesgos de Censura.....	**99**	**149**

ANEXO 1.	**INSTRUCCIONES PARA LLENAR EL FORMATO PARA LA CONFECCION DEL POV DE SEGURIDAD**	**150**
ANEXO 2.	**FORMATO DE DIRECTIVA CON NORMAS DE SEGURIDAD DE COMUNICACIONES**	**154**
ANEXO 3.	**FORMATO DE LA PIEZA IOCE**	**156**
ANEXO 4.	**DEFINICION DE TÉRMINOS**	**168**

CAPITULO 1

GENERALIDADES

SECCION I. INTRODUCCION

1. FINALIDAD

El presente manual tiene por finalidad uniformar normas y conceptos, incrementar los conocimientos y actualizar la doctrina básica sobre la seguridad de comunicaciones y sus repercusiones en el combate moderno.

2. ALCANCE

a. La presente publicación tiene por objeto ampliar y complementar los conocimientos sobre Seguridad Militar especificados en el ME 38-10 y Procedimientos de Contrainteligencia en el Ejército, particularmente de CI de Telemática electromagnéticas, prescribiendo las normas específicas relacionadas con la Seguridad de Comunicaciones.

b. Las normas y procedimientos que se prescriben en el presente manual están dirigidos al personal de Comunicaciones para su puesta en ejecución y a todos los oficiales para su Control y Supervisión.

SECCION II. SEGURIDAD DE LAS OPERACIONES (SEGOPE)

3. CONSIDERACIONES GENERALES

a. La doctrina actual de los Ejércitos acepta que el Comandante más hábil en "Visualizar el Campo de Batalla", obtendrá una ventaja táctica significativa; es decir, el Comandante que dispone de la mejor Inteligencia sobre el campo de batalla y la emplea eficazmente, logrará una marcada ventaja en el balance de la Potencia Combativa Relativa (PCR).

b. Para visualizar el campo de batalla, los esfuerzos de la Inteligencia tradicional se han concentrado sobre el enemigo inmediato a enfrentar. Sin embargo, la experiencia de los últimos conflictos, en donde la tecnología empleada por los Ejércitos, ha influido poderosamente en el equilibrio de las

fuerzas, al dar mayor énfasis al empleo de sistemas electrónicos y de comunicaciones; exige un análisis más profundo de otros factores que anteriormente no constituían una amenaza evidente a nuestras fuerzas, antes, durante y después del planeamiento de las operaciones.

c. Los factores o principios que hoy en día han cobrado auge y se han vuelto determinantes, aún sobre el factor numérico o principio de MASA, son los de: SEGURIDAD y SORPRESA. Lograr y conservar estos principios, exigen que nuestros Comandantes puedan impedir que el enemigo utilice su habilidad o capacidad de búsqueda de informaciones o al menos controlar su empleo. En esta sección trataremos sobre la SEGURIDAD.

d. **Conceptos Generales sobre la Seguridad**

(1) El concepto de seguridad es inmanente al hombre; la seguridad definida como el conjunto de medidas que cubren cualquier riesgo, genera un estado de confianza y tranquilidad a una persona o grupo, que proviene de la idea de que no hay peligro.

(2) La seguridad es un concepto permanente e integral, ya que es responsabilidad de todos y las medidas se conjugan en todo momento y cualquier descuido en alguna de sus partes puede poner en riesgo al conjunto.

(3) La seguridad descansa en:

(a) La información, que tenemos del enemigo y la que negamos al mismo.
(b) El dispositivo, que nos cubre del riesgo de acciones físicas del enemigo.

(c) Otros elementos, tales como el personal, el material, etc.

(4) La seguridad debe cubrir de todo riesgo a la información, material y al personal, lo que nos dará libertad de acción. Sin embargo se debe tener presente que ninguna medida de seguridad nos garantizará de manera absoluta, que el enemigo no podrá obtener información.

4. CONCEPTOS GENERALES SOBRE EL COMANDO Y CONTROL (C^2)

a. La habilidad táctica y un liderazgo efectivo, son los principales elementos de la potencia combativa sobre un moderno campo de batalla aeroterrestre. La tecnología actual ha integrado los factores de tiempo y espacio, que se requieren para unas operaciones de combate efectivas.

b. La alta movilidad de las fuerzas de combate aeroterrestres, así como la velocidad, alcance, precisión, exactitud y letalidad de los sistemas de armas, condicionan las rígidas demandas de los Comandantes y Oficiales del Estado Mayor. Por otro lado, los altamente sofisticados y multidisciplinarios Sistemas de Reconocimiento, Vigilancia y Adquisición de Blancos (S-RVAB), son todos predictivos; y sus computadores reaccionan más rápidas y precisas que el ser humano.

c. Las posibilidades mencionadas en el párrafo anterior cuando están integradas con los factores de tiempo y espacio, contribuyen a la victoria o a la derrota; colocando cada área del campo de batalla en virtualmente INSEGURA.

d. Las instalaciones y sistemas de C^2 son objetivos de Alta Prioridad (OAP) tanto para nuestras fuerzas como para el enemigo, ya que ambos emplearán un vasto "arreglo" de recursos y S-RVAB para identificar y localizar rápidamente estas instalaciones y sistemas, debido a que constituyen el punto neurálgico del proceso de toma de decisiones, al ubicarse en ellos los Puestos de Comando, lugares donde se planea, conduce y sostiene el combate, es decir, se comunica información de combate e inteligencia, se coordinan los apoyos y se proporciona la dirección / conducción de la fuerza como un todo.

e. Los Comandantes enemigos conducirán operaciones intensas de RVAB así como realizarán un planeamiento detallado antes de empezar una acción ofensiva. La priorización de sus objetivos estará orientado hacia el apoyo de los fuegos preparatorios de artillería y aviación, contra nuestras principales posiciones defensivas, reservas y Puestos de Comando. Una vez que las operaciones han comenzado, su esfuerzo se orientará a localizar y destruir las instalaciones y sistemas de C^2; intentando "quebrar" sistemáticamente, la habilidad de nuestros Comandantes tácticos para comandar y controlar sus tropas disponibles y sistemas de armas de apoyo. Su objetivo final será maximizar la degradación de nuestros sistemas de Comando, Control, Comunicaciones e Inteligencia (C^3 I).

f. Contra este accionar, nuestros Comandantes buscarán degradar o impedir que la habilidad de los Comandantes (Cmdtes) enemigos (enos) les permita conducir su acción o ataque tal como lo planearon, realizando a su vez un sistemático ataque sobre sus "nodos" y "enlaces de información" de sus sistemas de c^2, que apoyan su proceso de toma de decisiones.

g. La lucha por mantener la habilidad para comandar y controlar las fuerzas, al mismo tiempo que se intenta negarle esa misma habilidad al oponente, constituye una forma de "guerra de c^2".

5. GUERRA DE COMANDO Y CONTROL

a. La guerra de C^2 en las operaciones de combate aeroterrestre son complejas, cuando se ven como un cúmulo de Telemática electrónicas cruzando en todas direcciones el campo de batalla. Sin embargo esta forma de guerra C^2, puede reducirse a términos de referencia más simples y extendibles, cuando se le ve como acciones o actividades tangibles e intangibles.

b. Las actividades o acciones tangibles, son los "nodos" de Comando, Control y Comunicaciones (C^3), que presentan peculiaridades visuales a los Comandantes para verlos y dispararles. Las intangibles son los "Enlaces de Información" entre los nodos, que pueden interceptarse, identificarse y perturbarse.

c. Existirán también nodos que en si mismo, pueden interceptarse, identificarse y perturbarse. Dependiendo de la situación táctica y el efecto deseado de nuestras operaciones, pueden haber también nodos y enlaces que pueden verse y monitorearse, tanto para dispararles como para perturbarlos. Como una regla general, normalmente se perturbará y aniquilará a combatientes, sistemas y personal de apoyo, y órganos de búsqueda y reunión de información de los planificadores y coordinadores. Cuando el ataque a los planificadores y coordinadores no logra los efectos deseados, esta regla general obviamente será desechada.

d. Los recursos de guerra electrónica (GE) disponibles o recibidos en apoyo, para conducir operaciones de combate estrecho o cercano, aunque limitados; serán estrenados para lograr el éxito en las acciones intangibles de la guerra de C^2. Sin embargo las tareas críticas que estos recursos deban realizar para ganar esa guerra, comienza y termina con el Cmdte; por lo tanto sus necesidades operacionales de apoyo de GE serán tan importantes como aquellas necesidades de información que necesita la inteligencia.

6. TAREAS CRÍTICAS PARA LOS RECURSOS DE GE

a. La GE es un elemento esencial de la potencia combativa, ya que proporciona al Cmdte con medios pasivos y activos para proteger sus sistemas de C^3 al mismo tiempo que ataca los sistemas de C^3 del eno.

b. La protección de nuestro C^3, es la prioridad número uno para la GE de acuerdo al principio básico desarrollado en la estrategia de Contra Medidas

de Comando, Control y Comunicaciones (CMC^3). Se realiza a través de:

(1) Las Contra-contramedidas electrónicas (COCOME) o GE defensiva,

(a) Son responsabilidad de todos los soldados quienes usan o líderes quienes supervisan, el empleo de los equipos de comunicaciones-electrónicos (C-E).

(b) Las COCOME son en naturaleza pasivas y se emplean para proteger nuestros sistemas de C^3, contra las actividades de combate electrónico del enemigo.

(c) Las COCOME pasivas incluyen:

1. Procedimientos de anti-interceptación y radiolocalización. (Por ejemplo: Control de emisión, enmarcamiento y evasión).

2. Emisores con características antiperturbación (AJ: antijam) o de apagado automático.

3. Identificación de una amenaza electrónica contra nuestras instalaciones de C^3 y la remisión inmediata del Informe de Modificación, Intromisión, Perturbación e Interferencia de Telemática (MIPIS).

(2) Las Medidas de Apoyo de Guerra Electrónica (MAGE)

(a) Pueden proporcionar al Cmdte la posibilidad para interceptar, identificar y localizar los emisores enemigos. Representa una fuente de información que se necesita para perturbar, engañar, realizar COCOME, y otros empleos tácticos de las fuerzas de combate.

(b) Las MAGE apoyan a la destrucción y perturbación de los sistemas de C^3 enos, mediante la adquisición (detección) y reporte (Información de Combate) de datos sobre el objetivo.

(c) Las MAGE también apoyan a los esfuerzos del Cmdte para enfrentar la SEGOPE y el engaño de las fuerzas enemigas.

(3) Las Contramedidas Electrónicas (COME)

Proporciona al Cmdte dos posibilidades activas para proteger nuestros sistemas de C^3:

(a) Perturbación de pantalla, que consiste en la perturbación de los sistemas enemigos, de interceptación y radiolocalización de comunicaciones, para prevenir que éstos obtengan información o localicen nuestras comunicaciones de alto valor.

(b) Comunicaciones de alta potencia, que consiste en emplear a nuestros perturbadores como medios de comunicaciones para enlazarse entre ellos, en situaciones de combate críticas, en que la perturbación enemiga impide el comando y control de nuestras operaciones y no se cuenta en el instante con un medio alterno de enlace efectivo para trasmitir órdenes de ejecución inmediata; solicitar apoyo de fuego inmediato u otras situaciones similares.

c. Cada una de estas tareas derivadas de la Misión General de Guerra Electrónica e Inteligencia (OGEI: desarrollo de la situación, desarrollo del blanco, GE y Contrainteligencia), son esenciales para el éxito de la Seguridad de las operaciones planeadas y/o en curso.

d. Mayor información sobre el empleo de los recursos de GE, se pueden encontrar en los manuales y textos de GE.

7. CONTRA MEDIDAS DE COMANDO, CONTROL Y COMUNICACIONES (CMC^3)

a. Definición
Las CMC^3 están definidas como el conjunto de actividades militares que integran el empleo de la Seguridad de las Operaciones (SEGOPE), Engaño Militar, Perturbación electrónica y destrucción física, apoyado por la Inteligencia, para negar información; así como para influir, degradar o destruir el C^3 enemigo, al tiempo que protegemos nuestro C^3.

b. La estrategia de CMC^3 tendrá como primera prioridad proteger nuestro C^3. El apoyo de Inteligencia para la protección de nuestro C^3 se realizará a través del apoyo de Contrainteligencia a la SEGOPE y al engaño militar.

c. El blanco u objetivo de las CMC^3 será la estructura del C^3 enemigo, sin embargo el objetivo o meta final será la persona que toma decisiones, pues estas decisiones estarán influenciadas por lo que reciben a través de esa estructura, que está distribuida en los diferentes escalones de la cadena de comando.

d. Para que las CMC^3 sean efectivas, es necesario que las debilidades y

vulnerabilidades de los enlaces radiales y puestos de Comando enemigos, sean identificados, analizados y atacados; al mismo tiempo que protegemos nuestras vulnerabilidades.

e. El apoyo de Contrainteligencia a la SEGOPE, se orienta a contrarrestar o degradar los esfuerzos multidisciplinarios de la Inteligencia de imágenes y Contrainteligencia de Telemática (C-INTETE).

8. CONCEPTO DE SEGOPE

La SEGOPE consiste de un conjunto de acciones o medidas tomadas por un Cmdte para negar información al eno sobre sus posibilidades e intenciones, así como sobre sus planes, conducción de operaciones y actividades, mediante la identificación, control y protección de los indicadores que se asocien con la información a negar. Se ejecuta a través del Proceso de SEGOPE.

9. CATEGORÍAS DE LAS MEDIDAS DE SEGOPE

La SEGOPE incluye la aplicación coordinada de una variedad de medidas y procedimientos orientados a los requerimientos individuales para cada unidad, misión y situación. Esto requiere un esfuerzo totalmente integrado de acciones y medidas, agrupadas en tres grandes categorías: Medidas de Contravigilancia, Contramedidas y Engaño:

a. Medidas de Contrainteligencia.- Son aquellas técnicas de seguridad diseñadas y empleadas rutinariamente para prevenir o engañar a la Inteligencia enemiga, particularmente a su observación y explotación; sobre nuestras actividades y operaciones con la finalidad de proteger el verdadero status de éstas. Estas medidas estarán normalmente enumeradas o listadas en un POV de Unidad, e incluyen: camuflaje, humo, técnicas de seguridad de Telemática, puestos de observación, puesto de escucha, itinerario, frecuencias de patrullajes, cubiertas, procedimientos adecuadas de mantenimiento electrónico entre otras.

b. Contramedidas (CM)

(1) Son aquellas acciones que se toman para contrarrestar una actividad o un sistema específico de la inteligencia enemiga que no puede ser contrarrestado por más medidas de contravigilancia.

(2) Las contramedidas emplean artificios o técnicas con el objetivo de dañar, debilitar o degradar la efectividad operacional de la inteligencia enemiga.

(3) Las contramedidas pueden incluir medidas de protección y medidas ofensivas:

(a) Las medidas de protección incluyen aquellas acciones que se toman para protegernos contra la búsqueda de inteligencia enemiga, sin atacar directamente a sus sistemas de búsqueda.

(b) Las medidas ofensivas incluyen COME, apoyo de fuegos y maniobras directas contra los sistemas de búsqueda enemiga.

(4) Estas contramedidas pueden ser: destrucción del sistema de RVAB enemigo, Contrainteligencia humana, Contrainteligencia de imágenes y Contrainteligencia de Telemática.

c. **Engaño**.- Esta categoría está designada para inducir a error al enemigo mediante la manipulación, distorsión o falsificación de información; tratando que actúe de una manera que perjudique a sus intereses.

10. RESPONSABILIDADES DENTRO DEL PROCESO DE SEGOPE

a. El G-3 tiene la responsabilidad de EM para supervisar y coordinar todas las actividades de SEGOPE del Comando; para tal efecto deberá proporcionársele un elemento, a niveles GU y superiores, a fin de que sea éste quien realice las funciones de administrar y desarrollar las tareas y deberes específicas sobre SEGOPE.

b. El Elemento de SEGOPE que apoya al G-3, realice los deberes específicos siguientes:

(1) Asesorar al G-3 en el desarrollo de Elementos Esenciales de Información Amiga (EEIA)

(2) Preparar e implementar los planes y anexos de SEGOPE del Comando.

(3) Proporcionar datos para el desarrollo de los planes de engaño y revisarlos una vez terminados.

(4) Preparar y mantener actualizado los Procedimientos Operativos Vigentes (POV'S) de SEGOPE.

(5) Administrar el desarrollo, la conducción y supervisión de los programas de educación y entrenamiento de la SEGOPE.

c. El G-2 tiene la responsabilidad de EM en materias de inteligencia y contrainteligencia para apoyar a la SEGOPE. En el primer caso a través de la producción y difusión de la base de datos sobre la amenaza de los sistemas de búsqueda de información del enemigo; y en el segundo caso, determinando los riesgos que corren nuestras operaciones planeadas o en curso ante los sistemas de búsqueda enemiga. En este último caso, deberá contar con un negociado o Elemento de análisis de CI, que lo ayude en estas materias.

d. El elemento de Análisis de CI que apoya al G-2, realiza las funciones específicas siguientes:

(1) Mantener una base de datos sobre los sistemas de inteligencia eno.

(2) Analizar las posibilidades e intenciones de los órganos de búsqueda enemigas.

(3) Asesorar al G-3 en el desarrollo de "Perfiles" de nuestras fuerzas.

(4) Identificar nuestras vulnerabilidades.

(5) Apoyar al G-3 en el análisis de riesgos

(6) Asesorar en el desarrollo de EEIA.

(7) Recomendar medidas de SEGOPE

(8) Identificar oportunidades de engaño

(9) Asesorar en el planeamiento de engaño

(10) Asesorar en la preparación de planes y anexos de SEGOPE.

(11) Desarrollar necesidades de evaluación de SEGOPE.

e. El G-1, en lo que respecta al proceso de SEGOPE tiene la responsabilidad de:

(1) Identificar cualquier aspecto sensitivo de las operaciones de personal que podría explotar la inteligencia enemiga (desafección, corrupción, etc.).

(2) Desarrollar y mantener actualizado los Planes de Seguridad Física del PC y/o de los Cuarteles Generales, asegurándose que todas las previsiones en ellas contenidas sean incrementadas en períodos de tensión

(3) Revisar periódicamente los procedimientos de personal para asegurarse que estén acordes con las existentes necesidades de Seguridad de la Información.

f. El G-4, tiene la responsabilidad de asegurarse de que la administración de los abastecimientos y movimientos no comprometan las operaciones que se estén planeando o se estén conduciendo; a través de:

(1) La revisión de las órdenes y planes logísticos, para asegurar su concordancia con las políticas y procedimientos para SEGOPE.

(2) El desarrollo, coordinado con el G-3, del Plan logístico en apoyo a las medidas de SEGOPE.

g. El G-5, tiene la responsabilidad de incluir las medidas de SEGOPE en los planes de Operaciones de Asuntos civiles, y revisarlos periódicamente; para identificar indicadores sensibles a las operaciones.

h. El Cmdte de C-E, tiene un rol principal en las SEGOPE, desde que nuestras emisiones electromagnéticas son la fuente principal de información sobre nuestras fuerzas. Sus deberes específicos al respecto son:

(1) Desarrollar, en coordinación con el G-3, planes para implementar las COCOME.

(2) Evaluar el Anexo de C-E a la orden de Operaciones para detectar indicadores que puedan estar disponibles a la Inteligencia de Telemática (INTETE) enemiga.

(3) Asesora al G-3 en el desarrollo y conducción de un programa de entrenamiento en COCOME; y, en el empleo de las Instrucciones Operativas de Comunicaciones-Electrónicas (IOCE).

(4) Evaluar las probables consecuencias del combate electrónico enemigo dirigido contra nuestros sistemas de comunicaciones y su potencial impacto sobre la SEGOPE.

(5) Asesorar al Elemento de SEGOPE que apoya al G-3, sobre la selección y desarrollo de medidas de SEGOPE para C-E.

(6) Evaluar las probables consecuencias de nuestras operaciones de COME, sobre nuestras comunicaciones, para prevenir la interferencia

mutua

(7) Establecer los procedimientos y pedidos de información para los informes MIPIS.

(8) Establecer redes de comunicaciones seguras para satisfacer las necesidades de enlace.

(9) Asegurarse que todos los pedidos de equipamiento de seguridad de comunicaciones (hardware, software, apoyos según listas autorizadas de Stock: LAS, y listas de cargas prescritas: LCP) sean suministrados con oportunidad para que estén disponibles cuando sean necesitados.

(10) Asegurarse que el personal conozca las medidas de seguridad física del material de seguridad de Comunicaciones (cargador de claves, E-PROM, etc.).

(11) Asegurarse que el personal de comunicaciones conozca la operación del equipamiento de seguridad de comunicaciones.

(12) Asegurarse que el equipo de seguridad de comunicaciones sea empleado apropiadamente.

(13) Asesorar al Elemento de Análisis de contrainteligencia en el desarrollo de perfiles de nuestras comunicaciones.

i. El Cmdte de artillería, tiene la responsabilidad de asegurarse que todas las Unidades que empleen sistemas electrónicos (radares) para conducir sus operaciones de apoyo de fuegos terrestres y antiaéreo, no revelen peculiaridades electromagnéticas significativas que al combinarse con sus propias comunicaciones, proporcionen al enemigo una peculiaridad identificable.

11. PROGRAMA DE SEGOPE

a. El programa de SEGOPE es un proceso de naturaleza cíclica, que toma en consideración los cambios que se producen en la interrelación de nuestras vulnerabilidades con las posibilidades del enemigo.

b. Las posibilidades del enemigo se ven incrementadas cuando sus sistemas de inteligencia cuentan con apropiados y modernos recursos de búsqueda y obtención de información; por lo tanto los Cmdtes de nuestras fuerzas en todos los escalones deben tomar acciones especificas para minimizar la habilidad enemiga de emplear eficiente y eficazmente dichos recursos

contra nosotros. Estas acciones específicas están contenidas en el Programa de SEGOPE del Comando, que incluye la aplicación coordinada de una variedad de medidas y procedimientos que conforman necesidades únicas para cada Unidad, misión y situación, denominadas CATEGORÍAS (Tratadas en el párrafo 9).

c. El programa de SEGOPE se debe aplicar a todas las opns del Ejto, tales como: investigación y desarrollo de proyectos, ejercicios o maniobras tácticas, ejercicios de entrenamiento en tiempo de paz; y, actividades u opns militares en tiempo de guerra.

d. Los objetivos del programa de SEGOPE son: asegurar la seguridad del Comando y preservarlo del elemento sorpresa.

e. Para que el programa de SEGOPE sea efectivo se debe:
   (1) Establecer por el Comandante

   (2) Enfatizar en todos los niveles de comando

   (3) Diseñar para un propósito único: proveer seguridad al Comando.

   (4) Basar en las necesidades operacionales

   (5) Implantar agresivamente

   (6) Adaptar a los cambios de Situación

f. El programa de SEGOPE se desarrolla a través del Proceso de SEGOPE.

SECCION III. PROCESO DE SEGURIDAD DE LAS OPERACIONES

12. CONCEPTO DEL PROCESO DE SEGOPE (Ver figura 1)

El proceso de SEGOPE es una secuencia de pasos que busca organizar todas las acciones que envuelven al planeamiento continuo, reunión de información, análisis, informes, ejecución de órdenes e instrucciones; para dar al Comandante la seguridad necesaria y que éste no se vea sorprendido por el enemigo, los pasos que comprende este proceso son diez (10) y se explicarán a continuación.

13. PASO 1: IDENTIFICAR LOS ELEMENTOS DE BUSQUEDA Y RECOLECCIÓN ENEMIGA.

a. Este paso es una función de inteligencia realizada por el Elemento de Análisis de Contrainteligencia (EACI) para detectar, identificar y/o determinar elementos enos con posibilidades para hacer Inteligencia Humana, Inteligencia de Telemática e Inteligencia de Imágenes.

b. La base de datos para identificar estos elementos son básicamente la misma para cada categoría especifica de inteligencia (humana, de Telemática y de imágenes). Esta base de datos incluirá órganos y/o recursos de inteligencia enemiga orientados contra nuestras fuerzas, tales como:

(1) Unidades orgánicas (con posibilidades de reconocimiento e interceptores de radio y radar).

(2) Misiones (que tipo de información trasmiten, contra que unidad o emisor nuestro está orientado).

(3) Despliegue Táctico (a cuantos kilómetros desde nuestra línea de avanzada se encuentran o distancia desde otras unidades amigas o enemigas.

(4) Método de despliegue (infiltración, colocalizado con recursos COME)

(5) Posibilidades de sus recursos (radiolocalizar e interceptar con una precisión de un (01) grado en un rango de frecuencia de 20 a 80 Mhz por ejemplo).

(6) Como pasa su información (empleando radios HF por voz o por ráfagas de datos por ejemplo, o empleando redes de comunicaciones especiales).

(7) A quien pasa su información (PPCC, elementos aislados, etc)

(8) Tiempo de procesamiento de la información (o tiempo de reacción ante alguna contramedida que empleemos).

(9) Acciones que el Cmdte eno tomará basado en la información que dispone (ataca inmediatamente, asigna tarea a otro recurso para confirmar la información).

(10) Fortalezas y debilidades de los recursos.

c. Muchas veces al enemigo se le asignan posibilidades asombrosas y esto no siempre es verdad. Por ejemplo los recursos de INTETE y de MAGE no siempre pueden proporcionar información lo suficientemente precisa para que nos puedan atacar inmediatamente; consecuentemente, se deberán emplear otros recursos para confirmarles si alguna Unidad o emisor nuestro puede ser objetivo para su ataque.

d. Las fortalezas y debilidades de los recursos de inteligencia ena serán factores críticos en la conducción del análisis de riesgos (paso 4) y en la selección de contramedidas (paso 6).

e. El despliegue doctrinario de los recursos de inteligencia enemiga debe ser proyectado sobre un calco a escala. Conforme nuestra inteligencia confirma la posición actual de estos recursos, este calco será actualizado (este calco debe contener también las ubicaciones planeadas para nuestras fuerzas conforme al paso 2 y se emplearán en el paso 3 para determinar nuestras vulnerabilidades).

f. Además de los informes de recursos de búsqueda enemigos conocidos, el Elemento de Análisis de CI, debe recibir informes que contengan cualquier información de posibles ubicaciones de otros probables recursos de búsqueda. Por ejemplo si las tropas al contacto informan haber visto un camión con una antena especial ubicada en cierto punto entonces el analista examina su plantilla doctrinal (ver Empleo Táctico de GE: preparación de inteligencia del campo de batalla) para determinar que podría ser dicho camión.

g. La reducción de las posibilidades de los órganos de búsqueda enemigos, como resultado de las acciones de combate, son también ingresadas en la base de datos. Esto es importante ya que las medidas de SEGOPE (Contramedidas) no se aplican contra amenazas que no existen, por tanto conforme la cantidad de recursos de búsqueda enos y sus posibilidades aumentan o disminuyen, las CM necesitarán ser reevaluadas o reajustadas (Paso 10).

14. PASO 2: IDENTIFICAR LOS PERFILES DE NUESTRAS FUERZAS Y RECOMENDAR ELEMENTOS ESENCIALES DE INFORMACIÓN AMIGA (EEIA).

a. En este paso la base de datos nuestra es enriquecida a través del esfuerzo coordinado de los elementos de inteligencia y de operaciones. Este mejoramiento de la base de datos se realiza para emplearlos en la identificación de las partes componentes de los perfiles de nuestras fuerzas: rasgos, patrones e indicadores; que muestran como una unidad puede aparecer ante los "ojos del enemigo".

b. La base de datos de nuestras fuerzas es crucial para el planeamiento de las operaciones, debido a que ayudará en el desarrollo de los EEIA, las contramedidas, el valor de la precisión y la efectividad de los planes de engaño.

c. Perfiles de nuestras fuerzas

(1) Los perfiles son el resultado de las acciones, incluyendo el cronograma o sincronización de las mismas, llevadas a cabo por Unidades militares y por la tropa de manera individual.

(2) El análisis de los perfiles de una Unidad puede revelar rasgos y patrones sobre los procedimientos de esa Unidad, que con el tiempo puede emplearse para determinar nuestras intenciones.

(3) La integración de varios perfiles puede emplearse (por el eno) para ayudar a predecir o determinar probables formas de acción de nuestras fuerzas.

(4) El EACI desarrolla los perfiles para identificar todas las actividades en que las Unidades están empeñadas para: - determinar si éstas son debilidades que pueden ser fuentes de indicadores para el enemigo y - recomendar las respectivas correcciones a esas debilidades.

(5) Los Perfiles pueden desarrollarse para cada área o función de EM. (personal, inteligencia, logística, operaciones y comunicaciones) mediante la búsqueda y reunión de datos sobre nuestro equipamiento, actividades físicas y despliegues.

(6) A continuación se muestra una forma de desarrollar perfiles de nuestras fuerzas:

(a) Obtener del Plan de Operaciones de un escalón, las misiones asignadas a cada escalón subordinado inmediato y dividirlas en las cinco áreas o funciones de EM que conciernen a ellas

(Comando y comunicaciones, inteligencia, operación y maniobra y apoyo de personal y de logística).

(b) Determinar los rasgos físicos y electromagnético de cada uno de los escalones subordinados inmediatos en cada una de las cinco áreas tal como se muestra en la **figura 2**.

(7) Los perfiles para GU/Unidades individuales deberán ser desarrolladas por un Oficial de SEGOPE asignado a cada GU/Unidad. El oficial de SEGOPE del escalón superior compilará los perfiles individuales para desarrollar un perfil de ese escalón. Por ejemplo, el perfil de una GU puede incluir los perfiles de sus Unidades orgánicas dentro de la zona de operaciones de la GU, más los patrones que podrían ocurrir para apoyar la operación planeada. **(ver figura 3).**

(8) El perfil de la GU/Unidad de las figuras 2 y 3, nos muestra con cierta exactitud QUE ESTÁ HACIENDO LA UNIDAD, EL CUANDO Y EL DÓNDE LO ESTÁ HACIENDO.

FIGURA 2: PUESTO DE COMANDO DE UN BATALLON DE INFANTERÍA

FIGURA 3: PERFIL DE UNA DIVISION DE INFANTERIA

Comando y Control

PPCC/DIV (Desarrollado para el PCA/Div y PPCC de Batallones)

RASGOS FÍSICOS	**RASGOS ELECTROMAGNÉTICOS**
---	---
---	---
---	---

Acciones a tomar

- ¿Cuándo y cómo se moverán a la posición?
- ¿Quiénes ayudarán en la preparación de la posición?
- ¿Quiénes se colocarán cerca o con ellos?
- ¿Qué tan a menudo se redespliegarán?

Operaciones y Maniobra

RASGOS FÍSICOS	**RASGOS ELECTROMAGNÉTICOS**
---	---
---	---
---	---

Acciones a tomar

- ¿Cuándo y cómo se conducirán reconocimientos?
- ¿Cuándo y cómo se moverán a la posición?

- ¿Quienes prepararán su posición?

- ¿Cuándo las posiciones alternas serán reconocidas y preparadas?

- ¿Cómo serán suministrados los abastecimientos y por quién?

(9) Los perfiles deben ser un análisis profundo de 1os rasgos y patrones de una GU/unidad; y deben mostrar las interrelaciones de las Unidades de comando, de apoyo y de maniobra, ya que uno solo de ellos puede que no nos revele un EEIA. Sin embargo, los perfiles individuales pueden revelarnos como pueden ser apoyados por las unidades de Ingeniería, de Defensa Aérea, de Guerra Electrónica y de apoyo Logístico.

d. Los rasgos de nuestras fuerzas

(1) Son las características distintivas de una Unidad, como consecuencia de su presencia o actividad en el campo de batalla.

(2) Los rasgos se detectan porque varias unidades tienen diferente equipamiento, son de diferentes tamaños, emiten diferentes Telemática electromagnéticas, se despliegan diferente y tienen diferentes ruidos y olores asociados a ellas.

(3) La detección de rasgos individuales pueden ser agrupados por analistas enemigos para mostrarle instalaciones o unidades enteras, así como actividades claves, agrupaciones importantes de tropas, etc.

(4) Los rasgos pueden clasificarse en cuatro categorías:

(a) Imágenes (visuales, fotográficas, infrarrojos, laséricas, etc).

(b) Electromagnéticos (de comunicaciones y de no-comunicaciones).

(c) Acústicas (ruidos característicos de motores, etc).

(d) Olfatorias (gasolina, aceite, pólvora, comida, etc).

e. Los patrones de nuestras fuerzas

(1) Son la forma como una Unidad hace sus actividades. Son acciones estereotípicas que habitualmente ocurren en una serie de circunstancias dadas, las que a su vez estßn basadas en un POV,

concepto de la operación e instrucciones de coordinación (estos dos últimos obtenidos del Plan u Orden de Operaciones), mas la manera como esa Unidad tradicionalmente ha cumplido la misión y el modo como actualmente se ha planeado.

(2) Las unidades tienen POV'S para que ellos realicen virtualmente todo, por lo tanto los patrones se pueden predecir y desarrollar tanto por los Cmdtes como por los planificadores y ejecutores.

(3) Los tipos de patrones son tan numerosos como procedimientos en operaciones militares. Por ejemplo antes de cada operación ofensiva el volumen de las comunicaciones aumenta dramáticamente y luego igualmente cae dramáticamente justo antes del ataque. Un analista enemigo podría notar este patrón y ser capaz de predecir nuestras intenciones para futuras operaciones ofensivas.

(4) Otro ejemplo son los patrones de ubicaciones de los puestos de Comando, que pueden proporcionar al enemigo indicadores de las intenciones de nuestras fuerzas.

(5) Los patrones ocurren en casi todas las operaciones, ya que las unidades se basan en un POV para ayudarse en la conducción de una operación particular con un mínimo grado de dificultad (normalmente los POV'S consideran disposiciones para operaciones tales como el despliegue, movimiento hacia el contacto, entrada en línea, etc).

f. Tanto los rasgos como los patrones no son inherentemente malos, al menos que ellos revelen un EEIA o proporcionen al enemigo indicadores que puedan revelar un EEIA. De ser el caso esto último, los rasgos y patrones de esa Unidad deben examinarse.

g. <u>Indicadores de EEIA</u>

(1) Son actividades que pueden contribuir a la determinación de una de nuestras formas de acción.

(2) Durante la preparación de una operación táctica, resulta virtualmente imposible para nuestras fuerzas evitar o cubrir todos los indicadores. En muchos casos, estas actividades serán detectadas por el enemigo y empleadas para predecir nuestra probable forma de acción.

(3) Los indicadores que no se pueden eliminar o cubrir serán consideradas como la base para el desarrollo de un plan de engaño.

(4) La identificación e interpretación de indicadores específicos son tareas críticas para el analista; quien los buscará, analizará los hallados y hará apreciaciones de las posibilidades, vulnerabilidades e intenciones. Estos análisis orientan el pedido de información, el planeamiento y eventualmente preveen la base para las decisiones y órdenes.

h. Elementos Esenciales de Información Amiga (EEIA)

(1) Son preguntas claves sobre nuestras intenciones o posibilidades de nuestras fuerzas, que probablemente serán planteadas por quienes toman decisiones y/o planifican las operaciones enemigas, en circunstancias de tensión, conflicto o combate.

(2) La base de datos de nuestras fuerzas son actualizadas continuamente conforme existan cambios en las situaciones, operaciones, tácticas, equipamiento o personal; que pueda alterar cualquier rasgo, patrón o indicador que devele un EEIA.

(3) Una vez que los perfiles han sido determinados, éstos serán examinados tal como ellos se relacionen con la misión y el concepto de la operación, para determinar cual de ellos puede develar información crítica para el éxito de la operación.

(4) El G-2 y el G-3 desarrollan los EEIA'S basándose en el concepto de la operación, la orientación del Comandante, los informes después de la acción, evaluaciones de los otros miembros del EM, evaluación de las vulnerabilidades (Paso 3) y el análisis de riesgos (Paso 4). Aunque en este paso del proceso de SEGOPE, se recomiendan EEIA que han sido identificados, éstos serán limitados y priorizados hasta un cierto grado que permita mostrar perfiles específicos e indicadores que necesitan ser analizados en el paso 4.

(5) El punto clave a recordar acerca de las EEIA es que ellos priorizarán e identificarán los perfiles sobre los cuales el proceso de SEGOPE debería concentrarse.

15. PASO 3: IDENTIFICAR LAS VULNERABILIDADES DE NUESTRAS FUERZAS.

a. Concepto de nuestras vulnerabilidades

Nuestras vulnerabilidades son aquellos perfiles que revelan indicadores de los planes de una Unidad o procedimientos operacionales, que al menos que sean adecuadamente cubiertos con contramedidas, serán detectados por los recursos enemigos de búsqueda

y reunión de información; pudiendo comprometer los EEIA de una unidad, arriesgando así el éxito de un plan o de una operación.

b. Nuestras vulnerabilidades pueden incluir una pobre seguridad de las comunicaciones, pobre seguridad física y de la documentación, inadecuado empleo del camuflaje o cualquier otra actividad o patrón predecible que ofrezca indicadores de intenciones específicas.

c. Este paso es principalmente una función que debe realizar el EACI, apoyado según las necesidades por elemento de SEGOPE que apoya al G-3.

d. Nuestras vulnerabilidades son identificadas a través de la comparación de nuestros perfiles (o indicadores claves para la operación planeada) con las posibilidades de búsqueda y colección de la inteligencia enemiga. El tiempo, la fecha, la ubicación y el tipo de órgano de búsqueda son las primeras consideraciones importantes en este paso.

e. Una vulnerabilidad de nuestras fuerzas existirá, siempre y cuando el enemigo tenga la posibilidad de obtener información de nosotros (tiempo, fecha, ubicación y tipo de unidad o actividad) y procesarla a tiempo para reaccionar de tal manera que podría afectar el resultado de la operación. Este procesamiento y tiempo de reacción son las segundas consideraciones importantes durante este paso.

f. Se debe considerar también la posibilidad actual del colector enemigo (frecuencias, distancias, precisión, etc). Por ejemplo, el enemigo puede ser capaz de ubicar un PC con sus recursos MAGE o de INTETE, pero la precisión de esta ubicación no será suficiente para su destrucción inmediata (pero si para perturbar). Por eso, nuestras unidades pueden ser vulnerables a ser destruidas, sólo si el enemigo puede obtener ubicaciones precisas. Aquí es donde el procesamiento y el tiempo de reacción desempeña su rol; sin embargo aún si el enemigo obtiene información precisa, puede tomarle tres (03) horas el procesarla y nuestra unidad tendrá tiempo para moverse y no existirá vulnerabilidad.

g. Como una ayuda para la evaluación de las vulnerabilidades, las técnicas de preparación de inteligencia del campo de batalla (PIC), explicadas en el texto de Empleo Táctico de GE; pueden aplicarse para determinar nuestros rasgos y patrones, para que veamos nosotros mismos como nos verían los órganos y sistemas de búsqueda enemigos. Por ejemplo usando los calcos y plantillas de los pasos 1 y 2 del proceso de PIC, nos puede mostrar las ubicaciones de nuestras Unidades y las actividades, ubicaciones y posibilidades de los colectores enemigos; entonces cada perfil amigo puede compararse con la amenaza. Cuando se complete el proceso, tendremos una lista inicial de nuestras vulnerabilidades.

h. Obtenida la lista, el analista debe identificar dónde, cuándo y con qué el enemigo tiene la capacidad para obtener información sobre los indicadores identificados. Cada vulnerabilidad será enumerada con su amenaza (s) específica para ayudar al analista en su priorización para más tarde emplearla durante el análisis de riesgo (paso 4).

i. Esta lista de vulnerabilidades puede emplearse también como una forma de evaluar la credibilidad de la fuente de información (para el enemigo) y en la priorización de cada vulnerabilidad de acuerdo a su importancia para culminar con éxito la operación y para su suceptibilidad para la búsqueda.

16. PASO 4: REALIZAR ANALISIS DE RIESGOS Y SELECCIONAR EEIA

a. Concepto de Análisis de Riesgos

Es el proceso por medio del cual nuestra proyectadas vulnerabilidades son comparadas con las posibilidades enemigas para derrotar a nuestras fuerzas, determinándose los riesgos de nuestras operaciones cuando no se aplican contramedidas para proteger o controlar nuestras vulnerabilidades a ser detectados por los órganos de búsqueda enemigas; así como la comparación de los riesgos determinados, con el costo de implementar esas contramedidas (en términos de tiempo, equipamiento, recursos económicos-financieros y/o mano de obra) y su probable efectividad.

b. Este paso es principalmente una función de operaciones realizado por el elemento de SEGOPE que apoya al G-3 con el apoyo del EACI.

c. Cada priorizada vulnerabilidad de la lista del paso 3 será examinada para determinar el posible impacto del colector enemigo sobre el resultado de la operación. Deberá considerarse en este examen las potenciales pérdidas de tiempo, equipamiento y mano de obra.

d. Para determinar el factor de riesgo, se tendrán en cuenta las actividades actuales y pasadas de los órganos de busqueda enemigos. Los riesgos asociados con cada vulnerabilidad son agregados a la lista determinada en el paso 3.

e. Luego el costo de implementar varias medidas de SEGOPE (Contramedidas) son comparadas con los beneficios (en términos de reducción de riesgo) que pueden esperarse si son implemantadas. Este costo de implementar versus los beneficios; necesitan del esfuerzo coordinado de los elementos de Análisis de CI y de SEGOPE que apoya al G-3.

f. El resultado del análisis de riesgos incluyen la selección, por el G-3, de aquellos EEIA que son lo suficientemente críticos como para justificar la aplicación de contramedidas que los cubran del enemigo.

g. Una parte clave de este análisis es la identificación de EEIA críticos que no pueden ser protegidas o cubiertos razonablemente por las medidas de contravigilancia o las contramedidas. Estos EEIA se identifican para propósitos de recomendar actividades de engaño y se proveen al G-3 tan pronto como sea posible dentro de este paso.

h. En este paso también, se hacen esfuerzos para reducir la "Lista de lavandería" de las EEIA establecidas en el paso 2. Los EEIA deben limitarse a aquellos aspectos críticos de la operación que deben protegerse para el éxito de la misión (con contramedidas).

17. PASO 5: RECOMENDAR MEDIDAS DE SEGOPE (CONTRAMEDIDAS)

a. Las medidas de SEGOPE deben ser sistemáticamente desarrolladas para proteger los EEIA de la detección enemiga. Basado en el análisis de riesgos del paso 4, el EACI recomienda suficiente número de medidas de SEGOPE al G-3, para reducir, eliminar o tomar ventaja de las vulnerabilidades.

b. El número de medidas de SEGOPE que necesitan para proteger al EEIA dependerá de:

(1) La situación
(2) La importancia del EEIA para el éxito de la operación.
(3) La suceptibilidad del EEIA a la detección.
(4) La precisión o efectividad de las medidas en sí mismas.

c. Si sólo una medida de SEGOPE se necesita para reducir el riesgo a un nivel aceptable, entonces esa sola medida será empleada. Pero si se necesitan algunas medidas asociadas estrechamente, entonces se emplearán.

d. La decisión a tomar debe estar basada en la efectividad esperada de las medidas de SEGOPE que se están considerando. Será necesario considerar todas las fuentes y multidisciplinarios productores de inteligencia enemiga, cuando se identifican posibles medidas de SEGOPE. Si un aspecto de una identificada amenaza, tal como las MAGE, es obviada, la operación podría correr riesgo.

e. Cuando sea posible, el Comandante debe contar con algunas medidas o grupo de medidas por cada vulnerabilidad. A través de ello; sus opciones se

incrementan, agregando confianza a su proceso de toma de decisiones.

f. Las medidas de SEGOPE deben ser realísticas y viables o el comandante no debe aceptarlas. La imaginación y sentido común serán necesarios para cumplir este objetivo.

g. Las medidas de SEGOPE caen en tres categorías que fueron explicadas en el párrafo 9 de este capítulo y son: Contravigilancia, Contramedidas y Engaño. **(ver figura 4)**.

h. Para asesorar al G-3 y al comandante, el elemento de SEGOPE en coordinación con el Elemento de Análisis de CI provee Apreciaciones de SEGOPE, que incluirá toda la información contenida desde el paso 1 hasta el paso 4 de este proceso que pueda afectar a las operaciones en curso.

i. La apreciación de SEGOPE puede presentarse oralmente o de manera escrita. Cuando es escrita el formato a seguir contendrá los párrafos siguientes:

(1) Misión (nuestra)
(2) Zona de Operaciones (o área de influencia)
(3) Situación de Inteligencia y sabotaje enemigo.
(4) Posibilidades de Inteligencia y Sabotaje enemigo.
(5) Riesgos de SEGOPE y recomendaciones
(6) Conclusiones.

18. PASO 6: SELECCIONAR MEDIDAS DE SEGOPE

a. Una vez que la decisión se ha tomado para implantar medidas de SEGOPE, la selección estará basada en su efectividad para cubrir el EEIA de la

búsqueda enemiga.

b. Resolver el problema del recurso competente será una función del G-3, quien tendrá cinco (05) opciones para tomar o elegir:

(1) Aplicar una o más medidas de SEGOPE (particularmente contravigilancia o contramedidas).

(2) Aceptar el riesgo de detección (las medidas de SEGOPE no son necesarias).

(3) Emplear engaño

(4) Emplear cualquier combinación de las tres anteriores.

(5) Cancelar la misión (prohibir la actividad o cambiar la operación).

c. La no selección de medidas de SEGOPE deberá estar basado en una de las consideraciones siguientes:

(1) Si se detecta, la actividad debería estar apoyada con un plan de engaño.

(2) El Comandante está aceptando el riesgo asociado con la detección.

d. La selección de medidas de SEGOPE son difundidas y dispuestas en el Anexo de SEGOPE a la Orden de Operaciones, que en realidad constituye el Plan de SEGOPE. Este anexo consta de los siguientes párrafos:

(1) Situación

(2) Misión

(3) Ejecución (contramedidas)

(4) Administración

(5) Comando y C-E

e. Los EEIA (que deben estar mencionados en el párrafo 3 del anexo de SEGOPE) son colocados en orden de prioridad. Generalmente, estas prioridades coincidirán con las prioridades que asigna la doctrina enemiga para su reconocimiento y empleo de sus recursos de perturbación y de apoyo de fuegos.

19. PASO 7: APLICAR MEDIDAS DE SEGOPE

a. Una vez que las medidas de SEGOPE son implementadas por actividad, el G-3 determina que elemento de la organización deberá hacerlo. Esta decisión está basada en:

(1) El tipo de medida

(2) Los recursos disponibles

(3) La misión de cada elemento

b. La apropiada aplicación de las medidas de SEGOPE permite que actividades esenciales se lleven a cabo mientras se reduce la probabilidad que el enemigo pueda detectarlas o interpretar correctamente su significado.

c. El G-3 debe siempre considerar la destrucción de la capacidad de búsqueda de la inteligencia y la guerra electrónica enemiga, como una contramedida principal, por ejemplo, si se conoce que el enemigo emplea ampliamente el reconocimiento terrestre, el G-3 puede recomendar que patrullas de combate destruyan a esos elementos de reconocimiento. En otro caso, las unidades de GE enemigas con posiblidades de interceptar y radiolocalizar serán las mayores amenazas, entonces el G-3 puede priorizar el empleo de la artillería para destruirlas, o enviar una patrulla de combate con la misma misión.

d. Otra opción disponible al G-3 es recomendar la aplicación de una operación de engaño táctico que muestre al enemigo un cuadro falso. Esto requiere una coordinación estrecha, ya que este tipo de operación también debe estar apoyada por el escalón superior inmediato (en su esquema de maniobra)

e. En el diagrama de flujo de la figura 5, se muestra gráficamente el proceso de decisión para aplicar medidas de SEGOPE.

FIGURA 05: DIAGRAMA DE FLUJO

20. PASO 8: DIRIGIR LOS ESFUERZOS PARA MONITOREAR LA EFECTIVIDAD DE LA APLICACION DE MEDIDAS DE SEGOPE

a. Una vez implementadas, las medidas de SEGOPE deben evaluarse periódicamente. Esta efectividad se evalúa en términos de "QUE TAN BIEN" estas medidas cubren o protegen los EEIA. El EACI y el Elemento de SEGOPE planean y establecen juntos un programa para cumplir la misión.

b. El G-3 contribuye a la evaluación de esa efectividad a través de la identificación de áreas críticas de la operación que fueron y continúan siendo expuestas a altos niveles de riesgo.

c. El EACI contribuye con la identificación de áreas débiles basándose en archivos históricos y operaciones anteriores. Luego en base al conocimiento de los métodos y equipos de los órganos de búsqueda de la inteligencia enemiga, se identificarán áreas de particular atención (viéndolo desde el punto de vista del enemigo). Finalmente podrán recomendar los métodos que se emplearán durante el monitoreo de la efectividad de la aplicación de estas medidas de SEGOPE.

d. En la recomendación, el EACI determinará cuando se conducirá la evaluación, como se conducirá (alcance), que tipo de evaluación se conducirá (propósito) y quien la conducirá.

21. PASO 9: MONITOREAR LA EFECTIVIDAD DE LAS MEDIDAS DE SEGOPE

a. Este paso está estrechamente relacionado con el paso anterior, ya que aquí los Servicios apropiados de SEGOPE se completan y las medidas de SEGOPE son evaluadas por su efectividad.

b. Las evaluaciones de SEGOPE varían en alcance dependiendo de las necesidades de la Unidad. Ellas pueden variar desde evaluar una simple medida de SEGOPE implementada por un miembro de la organización (tal como un jefe de Patrulla, aplicando una lista de verificación de camuflaje o el Comandante de C-E reexaminando sus lóbulos posteriores o laterales de sus emisores multicanal), para establecer que equipo de SEGOPE experto en el área puede evaluar (Por ejemplo personal de GE y/o de INTETE para emisores multicanal).

c. Durante el desarrollo de los servicios de SEGOPE y de evaluaciones, los equipos asesoran al Cmdte y su EM sobre las prácticas de seguridad que pueden comprometer un EEIA o pueden proveer indicadores de cualquier operación planeada o en ejecución. Si cualquier acción indica posible compromiso de información esencial, la data es reportada al Elemento de

SEGOPE (G-3) o al EACI (G-2) para el análisis de la probable información develada y los riesgos a los cuales el Comando puede estar sometido. Ejemplos de reportes de data pueden ser:

(1) Sospechas de develación de EEIA designadas
(2) Serias violaciones de procedimientos de seguridad establecidos
(3) Bajas atribuibles a probables compromisos.
(4) Indicaciones que el enemigo ha priorizado el conocimiento de nuestra operación.

d. Los Servicios de SEGOPE, son organizaciones especializadas de Contrainteligencia y de Guerra Electrónica que apoyarán los procesos de evaluación y el desarrollo de los programas de SEGOPE. Algunos de ellos pueden ser:

(1) Vigilancia de seguridad de sistemas de procesamiento de datos.

(2) Análisis y monitoreo de Seguridad de Comunicaciones

(3) Inspecciones de criptofacilidades.

(4) Vigilancia de Contramedidas de carácter técnico.

22. PASO 10: RECOMENDAR REAJUSTES A LAS MEDIDAS DE SEGOPE

a. Este paso lo efectúan los elementos de SEGOPE y de Análisis de CI conjuntamente; para recomendar nuevos EEIA, cuando sea necesario, así como cambios en las medidas de SEGOPE que se recomendarán anteriormente. Este paso orienta los pasos del 1 al 4 ya que las posibilidades del enemigo y nuestras vulnerabilidades son dinámicas y no se pueden hacer reajustes posteriores a esos pasos.

b. Los "informes después de la acción" sobre las condiciones de SEGOPE y la efectividad de las medidas de SEGOPE previamente implementadas se presentan al Comandante y Oficiales de Operaciones. El detalle de los informes puede variar con la extensión de la operación, tamaño de la Unidad, tiempo disponible y la situación actual.

c. El propósito de los informes después de la acción es permitir a los analistas determinar los cambios necesarios que incremente la seguridad del comando.

SECCION IV. CONTRAINTELIGENCIA

23. CONCEPTOS GENERALES SOBRE CONTRAINTELIGENCIA

a. Contrainteligencia (CI).- Son aquellas operaciones de inteligencia conducidas para detectar (identificar la amenaza), evaluar (analizar la base de datos), contraactuar (recomendar contramedidas) o prevenir (neutralizar objetivos del enemigo) la búsqueda y/o sabotaje, el terrorismo o el asesinato; conducido por o en nombre de un país, una organización o una persona; operando en perjuicio o detrimento de nuestras fuerzas. La Contrainteligencia es una guerra, una diaria batalla conducida en una escala global.

b. Operaciones de Contrainteligencia (OCI).- Son aquellas que incluyen la identificación de la amenaza, determinación de nuestras vulnerabilidades a esa amenaza; y, la recomendación y evaluación de las medidas de seguridad.

c. Análisis de Contrainteligencia (ACI)

(1) Son un conjunto de actividades que incluyen el establecimiento y mantenimiento de una extensa base datos; tanto sobre las posibilidades de la inteligencia enemiga como sobre los indicadores, rasgos, patrones y perfiles de nuestras fuerzas. El resultado de este análisis será la evaluación de las vulnerablidades de nuestras fuerzas y la identificación de aquellas vulnerabilidades que deben ser cubiertas y/o protegidas en prioridad.

(2) La base de datos al incluir nuestros indicadores, rasgos, patrones y perfiles, mostrará como una Unidad podría aparecer ante los ojos del enemigo; y al relacionarla con las posibilidades del enemigo, será un factor clave en el planeamiento de las operaciones ya que ayudará en el desarrollo de EEIA, las contramedidas, apreciaciones precisas y un efectivo plan de engaño.

24. ACTIVIDADES DE CONTRAINTELIGENCIA

a. Todas las actividades de CI pueden agruparse en tres (03) grandes núcleos: Contrainteligencia de Telemática, Contrainteligencia humana y Contrainteligencia de imágenes.

b. **Contrainteligencia humana**, son un conjunto de acciones que buscan vencer los intentos enemigos de usar fuente humanas para buscar y recolectar información tratando de neutralizar sus esfuerzos de espionaje, sabotaje y subversión.

c. **Contrainteligencia de Imágenes**, son aquellas que se toman para determinar las capacidades y actividades de la inteligencia de imágenes enemigas. Estas acciones incluyen: vigilancia de los sistemas de radar, fotográficos, térmicos e infrarrojos; evaluación de nuestras operaciones para identificar patrones y peculiaridades de imágenes; identificar las vulnerabilidades de las mismas y desarrollar y recomendar las contramedidas.

d. **Contrainteligencia de Telemática**

(1) Son un conjunto de acciones que se toman para:

(a) Determinar las capacidades, posibilidades y actividades de la INTETE y GE enemigas.

(b) Apoyar nuestras operaciones mediante la identificación de patrones, perfiles y rasgos electromagnéticos.

(c) Desarrollar y recomendar contramedidas.

(d) Evaluar la efectividad de las contramedidas aplicadas.

(2) Las contramedidas recomendadas para hacer frente a la amenaza enemiga incluyen activas u ofensivas y pasivas o defensivas tales como: perturbación electrónica, engaño electrónico, control de emisión (CONEM), apropiados procedimientos operacionales de radio, apropiados procedimientos de instalación de emisores; etc.

(3) Las actividades de C-INTETE, a su vez se pueden agrupar en:

(a) Técnicas de SEGUTE, que comprende dos grandes áreas: Seguridad de Comunicaciones y Seguridad Electrónica (Ver capítulo 3)

(b) Asesoramiento y asistencia a las COCOME.

25. INTERFASE DE LA CONTRAINTELIGENCIA CON EL PROCESO SEGOPE

a. La Contrainteligencia apoya a cuatro áreas funcionales: SEGOPE, OPERACIONES EN LA ZONA DE RETAGUARDIA, ENGAÑO MILITAR Y CONTRACCION TERRORISTA. Sin embargo estas áreas realmente no

pueden estar separadas, las actividades de CI se superponen sobre ellas y se apoyarán mutuamente (ver figura 6). A pesar de ello se considera que el apoyo a la SEGOPE será predominante.

b. El apoyo de CI a la SEGOPE incluye:

(1) La identificación y análisis de las posibilidades del personal, de las actividades y de las Unidades con Sistemas de vigilancia, reconocimiento y adquisición de blancos del enemigo.

(2) La identificación y análisis de las Unidades de GE enemigas, sus ubicaciones y sus actividades.

(3) Asesoramiento en el desarrollo de nuestros perfiles.

(4) Determinación de nuestras vulnerabilidades a las actividades de los sistemas de GE y de RVAB enemigos.

(5) Recomendación y evaluación apropiada de medidas de SEGOPE y de engaño.

c. El apoyo de la CI a la SEGOPE es también un proceso, que se concentra en desbaratar o degradar los esfuerzos multidisciplinarios de la inteligencia enemiga. El personal de CI deberá trabajar coordinada y estrechamente con la sección operaciones del EM (G-3), ayudándolo a desarrollar "perfiles" de nuestras fuerzas para compararlos con las posibilidades de la inteligencia enemiga. La comparación resulta en la identificación de nuestras vulnerabilidades que deben protegerse. La protección se efectúa

desarrollándose CONTRAMEDIDAS que contrarresten los esfuerzos enemigos de su inteligencia humana, de imágenes y de Telemática, que amenacen a cada nivel o escalón.

d. La CI apoya a la SEGOPE, en todo el proceso descrito brevemente en los Sub-párrafos anteriores, para derrotar o degradar los esfuerzos de la Inteligencia enemiga.

e. Este apoyo se materializará mediante un proceso continuo que consta de cuatro pasos:

(1) Evaluación de la amenaza

(2) Evaluación de nuestras vulnerabilidades.

(3) Desarrollo de las opciones de contramedidas.

(4) Evaluación de la aplicación de contramedidas.

f. Este proceso de CI fluye dentro del cíclico proceso de la SEGOPE (Ver figura 7); sin embargo se presentarán dentro de él otros procesos cíclicos internos. Por ejemplo, verificaciones de la amenaza, cuando se están desarrollando las opciones de contramedidas, para asegurar que la contramedida propuesta tendrá el efecto deseado sobre nuestras opns. Otros procesos cíclicos internos se presentarán en el último paso "evaluación de la aplicación de contramedidas", que incluyen reverificaciones de:

(1) La amenaza, para ver que no se produjeron cambios.

(2) La implantación de contramedidas, para asegurar que las recomendaciones iniciales fueron válidas.

(3) Nuestras opns de Comunicaciones y Electrónica en curso, para asegurar que ellas se conducen como fueron planeadas.

g. La descripción y desarrollo de cada uno de los pasos de este proceso, se detallará en el capítulo siguiente; cuando se trate la contrainteligencia de Telemática; no obstante cabe mencionar que el proceso de CI enfatiza la necesidad de contar con una precisa aproximación analítica de las posibilidades enemigas para afectar nuestras opns. La clave es ser predictivo, basado en un profundo y cuidadoso conocimiento de las posibilidades y probables intenciones del enemigo, de nuestros planes y opns; y, de medidas de seguridad realísticas.

26. BASE DE DATOS DE CONTRAINTELIGENCIA

Para proporcionar asesoramiento oportuno al EM (respuesta) deberá existir de antemano una base de datos CI:

a. La base de datos CI, es una herramienta valiosa para los analistas de CI y se define como la reunión o recolección de información organizada para una rápida búsqueda, fácil acceso y recuperación, y referencia cruzada.

b. La base de datos es esencial en la producción de un efectivo análisis de la situación y desarrollo de opciones de contramedidas. El valor de la base de datos dependerá del volumen y precisión de la información que contiene.

c. La base de datos se desarrolla para áreas potencialmente clasificadas como de tensión u hostilidades, a través de la preparación de inteligencia del Campo de Batalla (PIC). Iniciadas las hostilidades la base de datos se mantiene y actualiza para reflejar toda la información en curso que podría afectar el análisis o el desarrollo de las opciones de contramedidas.

d. La base de datos debe ser organizada funcionalmente para que el proceso de CI sea exitoso. Esta base de datos debe proveer información concerniente tanto a las posibilidades de nuestras fuerzas como a las posibilidades de recolección enemiga.

e. Los elementos básicos de la base de datos incluye:

(a) Orden de Batalla (amigo y enemigo).
(b) Datos Técnicos (amigo y enemigo).
(c) Datos de las condiciones metereológicas y el clima.
(d) Datos del terreno.
(e) Gráficos, calcos e ilustraciones de la PIC.
(f) Resúmenes de Inteligencia.
(g) Carta y/o calco de situación.
(h) Diario de Sección de CI.

CAPITULO 2

INTELIGENCIA Y CONTRAINTELIGENCIA DE TELEMÁTICA

SECCIÓN I. INTELIGENCIA DE TELEMÁTICA

27. CONCEPTO DE INTELIGENCIA DE TELEMÁTICA (INTETE)

La INTETE es el producto resultante de la búsqueda, reunión, evaluación, análisis, integración e interceptación de la información proveniente de la interceptación electromagnética (E/MAG) de emisiones. Las emisiones E/MAG son campos de energía eléctrica y magnética que viajan a través del espacio, los cuales dependiendo de su frecuencia y rango de oscilación, serán conocidas por nombres tales como: ondas de radio, rayos gamma, rayos x, rayos ultravioleta, luz infrarroja y ondas de radar.

28. CLASIFICACIÓN DE LA INTETE

a. La INTETE se clasifica en:

(1) Inteligencia de Comunicaciones (INT/COM).

(2) Inteligencia Electrónica (INT/ELEC)

(3) Inteligencia Técnica (INT/TEC)

b. Inteligencia de Comunicaciones (INT/COM)

Comprende la interceptación y procesamiento de Telemática de comunicaciones extranjeras tales como voz, codigo Morse y radioteletipo; con la intención de obtener información para inteligencia sobre las intenciones, posibilidades, ubicaciones, tácticas y otros datos, del enemigo o de potenciales enemigos.

c. Inteligencia Electrónica (INTELEC)

Comprende la interceptación y procesamiento de Telemática de no-comunicaciones para determinar intenciones, posibilidades y ubicaciones; tanto de las características como de las funciones del equipamiento enemigo.

29. PROCESO DE INTETE

a. El proceso de INTETE comprende los pasos siguientes:

(1) Búsqueda
(2) Identificación
(3) Interceptación
(4) Radiolocalización
(5) Registro
(6) Análisis

(7) Difusión

b. Búsqueda

El proceso de INTETE comienza con la b·squeda. Los operadores de los interceptores reciben como tarea la búsqueda de Telemática de interés en una porción del espectro de frecuencias. Una vez que la señal es interceptada empieza la porción de inteligencia del proceso.

c. Identificación

Es el análisis del contenido de las comunicaciones o Telemática característicos del emisor, para identificar la señal y explotarla más adelante. El análisis puede ser tan simple como la identificación del lenguaje o "dejo"; o tan complicado como la determinación del código especial empleado por la Unidad enemiga.

d. Interceptación

Es el acto de escuchar, copiar o grabar emisiones por alguien diferente al grupo a que pertenece. Los objetivos de la interceptación son:

(1) Reunir emisiones para acumular información
(2) Determinar las ubicaciones y las características de los emisores.
(3) Determinar los parámetros, estructura y funciones de las emisores.
(4) Determinar los elementos organizacionales o individuales a que pertenecen los emisores de comunicaciones y no-comunicaciones.

e. Radiolocalización (RL)

Es la determinación de la ubicación de un emisor. La RL se emplea para determinar la dirección aproximada o "visada" de una antena trasmisora. Cuando la estación de RL obtiene una "línea de vista "(LVE)", proporciona una dirección aproximada al emisor, pero no la distancia, por lo que se necesitarán dos o tres LVE para proveer una ubicación más definitiva. Actualmente existen sistemas que con una sola visada puede determinar también la ubicación aproximada.

f. Registro

Es colocar todo el tráfico interceptado conjuntamente con otra data asociada, en archivos apropiados o registros de información; de tal manera que puedan fácilmente ser encontradas, retiradas, reunidas o relacionarlas entre sí. Esta información es empleada como una ayuda para el análisis.

g. Análisis

Es un examen sistemático de la data interceptada para identificar hechos significativos y derivar conclusiones. Toda la información sobre las Telemática interceptadas, incluyendo mensajes y tráfico de emisores de comunicaciones son entregados a un centro análisis. En este centro será combinada con información proveniente de otras numerosas fuentes, y

analizada para determinar las ubicaciones, posibilidades, actividades e intenciones enemigas.

h. Difusión
Consiste en difundir rápidamente la información y/o inteligencia útil para el proceso de toma de decisiones. Esta información y/o inteligencia puede emplearse para desarrollar planes o para una acción inmediata.

SECCIÓN II. CONTRAINTELIGENCIA DE TELEMÁTICA (C-INTETE)

30. CONSIDERACIONES GENERALES DE C-INTETE

a. La C-INTETE, como se mencionó en el párrafo 24, es una de las actividades de la CI, por lo tanto constituye también un proceso que enfatiza la necesidad de una fuerte aproximación analítica. La clave de ese proceso es ser "predictivo", basándose en el conocimiento del eno sobre sus posibilidades electromagnéticas y probables intenciones.

b. Conociendo las posibilidades e intenciones enemigas, entonces los planes y órdenes de nuestras fuerzas podrán adoptar medidas realísticas de seguridad.

c. La C-INTETE proporciona al Cmdte con el conocimiento de la evaluación de los riesgos electromagnéticos y probables éxitos de las alternativas antes que los planes puedan llevarse a cabo.

31. PROCESO DE C-INTETE (ver figura 8)

a. Al igual como se mencionó en el párrafo 25, la C-INTETE también apoya a la SEGOPE a través de un proceso que consta de los pasos siguientes:
   (1) Evaluación de la amenaza electromagnética
   (2) Evaluación de nuestras vulnerabilidades electromagnéticas.
   (3) Desarrollo de las opciones de contramedidas
   (4) Evaluación de la aplicación de las contramedidas.

FIGURA 8

b. Durante la aplicación de las posibilidades de C-INTETE, el EM del Comandante, debe ser capaz de misionar al EACI mediante la determinación de las implicaciones de seguridad de una forma de acción disponible y la recepción de una propuesta oportuna.

c. Un ejemplo de lo mencionado en el párrafo anterior puede ser:

   (1) Un analista de C-INTETE del EACI advierte de las implicancias del despliegue del Puesto de Comando (PC) de la GU bastante adelantado para un ataque.

   (2) La advertencia deriva del conocimiento que desde el punto de vista del enemigo, esta forma de ubicar el PC le proporcionarß indicadores sobre un patrón típico de nuestro ejército antes del ataque, así como una confirmación positiva de que ese ataque es inminente.

(3) Estos indicadores podrían causar que el enemigo intensifique sus actividades de búsqueda, empleando entre otros sus recursos de MAGE y de INTETE, para detectar cualquier rasgo electromagnético que devele la existencia del PC.

(4) Los rasgos electromagnéticos que develen el movimiento de un PC bien adelantado podrían hacer peligrar el éxito del ataque, al eliminarse el elemento de sorpresa.

d. Para proveer asesoramiento al EM del Comandante, el analista de C-INTETE, debe contar con una base de datos actualizada; particularmente que contenga plantillas doctrinales del enemigo (desarrolladas en el Proceso de PIC mencionado en el texto de Empleo Táctico de GE), rasgos, patrones y perfiles de nuestra fuerzas (desarrolladas durante el proceso de SEGOPE mencionando en este texto en el capítulo anterior) y cualquier otra información sobre contramedidas disponibles para su empleo inmediato.

e. Esta base de datos ayudará en el Proceso de C-INTETE, sin embargo se deberá tener acceso a informaciones provenientes del G-3 tales como:

(1) Ubicaciones propuestas por el Cmdte de C-E para los PPCC.

(2) Tiempo (fecha-hora) del movimiento de las PPCC.

(3) Enmascaramiento tentativo de los elementos

(4) Medios de comunicaciones y formas de emplearlos

f. Estas informaciones podrían también obtenerse de los POV 'S o haber sido determinadas a través de anteriores procesos de C-INTETE.

g. En los párrafos siguientes se tratarán con mayor detalle todos los pasos del proceso de C-INTETE y el desarrollo de la base de datos para C-INTETE.

32. BASE DE DATOS PARA EL PROCESO DE C-INTETE

a. Además de los conceptos mencionados en el párrafo 26, el desarrollo de la base de datos para C-INTETE contiene los elementos siguientes:

(1) Reunión o colección de información electromagnética

(2) Contenido de la base de datos

(3) Orden de batalla electrónico. (OBE)

(4) Plantillas del Proceso de PIC/PEC

(5) Empleo de la base de datos

b. Reunión o colección de información electromagnética

(1) Para que la base de datos sea una herramienta efectiva para el proceso de C-INTETE, se necesita contar con personal dedicado a tiempo completo para su desarrollo. Esto asegura que se familiaricen con nuestros sistemas de C-E y con los sistemas de MAGE y de INTETE enemigas, para que tengan la habilidad para compararlos y contrastarlos de manera oportuna.

(2) La reunión de información para la base de datos de C-INTETE se origina desde dos fuentes:

(a) La primera fuente es la que pertenece a los sistemas generales de C-E nuestros; y, de MAGE e INTETE enemigas. Esto significa obtener información técnica de los equipamientos.

(b) La segunda fuente se relaciona a la información sobre la Unidad/GU específica que será apoyada. Esto significa conocer como esa Unidad/GU emplea sus sistemas de C-E y cuantos de ellos estarán disponibles para la operación. Esta información puede obtenerse de:

1. Los COEq's
2. POV'S
3. Informes de situaciones de operatividad
4. Publicaciones doctrinarias.

(3) Primera Fuente

(a) Donde empezar y como continuar puede simplificarse si se establecen prioridades de b·squeda en una lista, basada en cómo el enemigo podría priorizar sus objetivos sobre nuestros sistemas e instalaciones de Comando, Control y Comunicaciones (C^3). La siguiente es una lista sugerida de como el enemigo podría orientar su esfuerzo de búsqueda y reunión de información:

1. Unidad/Sub-unidad de Comunicaciones
2. Puesto de Comando del 1er Escalón
3. Puesto de Comando Avanzado
4. Artillería de campaña

5. Aviación de Ejército
6. Artillería antiaérea
7. Unidades/Elementos de guerra electrónica
8. Unidades de Apoyo Logístico
9. Unidades/elementos de Caballería o reconocimiento
10. Elementos de maniobra

(b) La reunión de información sobre los sistemas generales de nuestras fuerzas, se basará en obtener archivos y registros de todos sus emisores de comunicaciones y no-comunicaciones, así como de sus sistemas de armas a los que se asocian. Esta información puede contener:

1. Radios de FM (voz), con y sin SEGCOM incorporados
2. Radios de BLU (voz), con y sin SEGCOM incorporados
3. Facsímiles
4. Multicanal
5. Antenas
6. Sistemas de retrasmisión
7. Comunicaciones satelitales
8. Enlaces de trasmisión de datos
9. Integración radio-alámbrica
10. Equipos de SEGCOM
11. Sistemas de fibra óptica
12. Sistemas telefónicos alámbricos
13. Radares de localización de objetivos en movimiento.
14. Radares de "traqueo o captura" de la artillería antiaérea.
15. Radares de adquisición de blancos
16. Sistemas de GPS'S
17. Radares de aproximación de la aviación
18. Sistemas de identificación amigo-enemigo (IFF)
19. Radares, radiosondas o balones de datos de clima.
20. Perturbadores de GE.
21. RL'S e interceptores de GE
22. Otros sistemas o emisores que empleen nuestras fuerzas

(c) La fuentes de información para la reunión de datos técnicos pueden ser:

1. Oficiales de Comunicaciones
2. Secciones III de los COEq's
3. Ordenes Administrativas/Logísticas
4. PECOSA'S

5. Manuales Técnicos
6. Operadores de los Sistemas/emisores
7. Personal de mantenimiento
8. Otros especialistas o conocedores de los equipos

(d) La reunión de información sobre los sistemas generales de MAGE e INTETE del enemigo, deberán originarse en los órganos de búsqueda de nuestra INTETE.

(4) Segunda Fuente

Las fuentes de información para conocer como una unidad emplea sus Sistemas (Como se despliega y opera) puede incluir:

(a) Cmdte de C-E/Oficial de Comunicaciones
(b) G-3 (Planes y Ordenes)
(c) Manuales y Textos
(d) POV'S
(e) Otras publicaciones doctrinarias

(5) Después de reunida la información sobre las dos fuentes, se deberá revisar los planes de operaciones de la Unidad, sus POV'S y sus Ordenes de Operaciones, que pueden revelar como serán empleados sus sistemas para una situación en particular. Adicionalmente, la configuración del despliegue de sus redes de comunicaciones pueden determinarse durante la revisión de los POVC'S, IOCE, IPCE y anexos/planes de comunicaciones.

(6) A continuación se presenta un ejemplo de la base de datos de un grupo de combate de Infantería: "un vehículo portatropa UR, un RT/VHF dos RT/FM a la mano, 12 fusiles, lanzagranadas y diversos equipos de camuflaje".

- Del inventario mostrado, se puede apreciar que cuenta con tres (03) radios de baja potencia que podrían producir rasgos electromagnéticos, sin embargo los RT a la mano sólo cuentan con dos frecuencias prefijadas que podrían crear un rasgo característico al grupo de combate; ya que el RT/VHF a la espalda aunque produzca emisiones sus rasgos pueden confundirse con los de una sección o compañía.
- Si para cada grupo de combate se hace el mismo análisis, hasta completar a una compañía e inclusive al propio batallón, la acumulación de rasgos totales electromagnéticos pueden mostrarnos la densidad de emisiones características de la Unidad, pues normalmente es conocido que los elementos

militares en todos los escalones se organizan bajo el concepto trial (a tres grupos, tres secciones, tres compañías, etc).

c. Contenido de la base de datos

(1) La base de datos debe estar organizada funcionalmente para que el proceso de C-INTETE tenga éxito. La forma como se organice debe permitir proveer información concerniente a las posibilidades electromagnéticas de nuestras fuerzas y a las posibilidades de MAGE y de INTETE del enemigo, Estos elementos básicos incluyen (ver figura 9):

(a) Orden de Batalla Electrónico (amigo y enemigo)
(b) Datos técnicos (amigo y enemigo)
(c) Datos del clima y condiciones metereológicas
(d) Datos del terreno
(e) Plantillas del proceso de PEC (preparación Electrónica del Campo de Batalla)
(f) Resúmenes de Inteligencia
(g) Cartas de Situación y Calcos
(h) Diarios de Sección/cuadernos de trabajo.

FIGURA 9: ELEMENTOS DE UNA BASE DE DATOS DE C-INTETE

(2) La organización de la información extractada de los elementos mencionados en el párrafo anterior será colocada en archivos apropiados de base de datos.

d. Orden de Batalla Electrónico (OBE)

(1) El OBE son calcos que se usan para describir gráficamete los emisores de comunicaciones y no-comunicaciones y sus asociadas Unidades, instalaciones y actividades, que han sido localizadas a través de MAGE y/o INTETE. El OBE se desarrollará tanto para nuestras fuerzas para fines de C-INTETE, como sobre las del enemigo para fines de INTETE y C-INTETE.

(2) Existirán muchos más emisores en una zona de operaciones que unidades; por lo tanto para obtener un calco de OBE expeditivo deberán emplearse cartas a escalas 1/50,000 y es recomendable construir calcos separados por cada elemento o dato de análisis. Estos elementos pueden incluir:

(a) Tipo de emisor
(b) Tipo de modulación
(c) Frecuencia radial de operación
(d) Identificación de la Unidad o nivel de comando
(e) Sistema de armas asociado
(f) Grupo fecha-hora de observación
(g) Número de identificación del mensaje anotado en el diario de sección de la Unidad que proporcionó la data.

(3) Los tipos de emisores y parámetros de la señal pueden asociarse con unidades en particular, que en algunos casos, ayudarán al analista a confirmar o negar la presencia de un tipo de unidad y/o actividad enemiga.

(4) No todos los elementos de análisis enumerados en "(2)" podrán conocerse o serán apropiados para un emisor en particular.

(5) Los datos obtenidos y analizados del OBE, formarán parte de la base de datos del orden de Batalla resultante de la integración de todas las fuentes de inteligencia para determinar:

(a) Dispositivo
(b) Composición
(c) Fuerza
(d) Nivel de entrenamiento
(e) Tácticas
(f) Logística
(g) Efectividad combativa
(h) Datos técnicos electrónicos (emisores de C-E por ejemplo)

(i) Otros datos según las necesidades.

e. Plantillas de preparación Electrónica del campo de batalla (PEC)

(1) Todo lo concerniente a la Preparación de Inteligencia del Campo de batalla (PIC) y preparación Electrónica del Campo de Batalla (PEC), es ampliamente discutido en el texto de Empleo Táctico de Guerra Electrónica, sin embargo a manera de ilustración en este párrafo se mencionarán sus aspectos más relevantes.

(2) La PIC es una sistemática aproximación al análisis del enemigo, del clima y CCMM, y al terreno en una área geográfica específica. La PEC relaciona este análisis con las emisiones electromágneticas.

(3) Una plantilla es una ilustración gráfica de la estructura, despliegue o posibilidad de una fuerza enemiga; normalmente dibujado a escala, que nos posibilitan:
(a) Visualizar las posibilidades enemigas
(b) Predecir la probable forma de acción (PFA) enemiga antes del combate
(c) Confirmar o negar esa PFA durante el combate
(d) Proporcionar un medio para una continua identificación de las vulnerabilidades y posibilidades de los recursos enemigos.

f. Empleo de la base de datos

(1) La base de datos provee la información básica que se necesita en el proceso de C-INTENSE, ya que nos permitirá identificar nuestras vulnerabilidades a través de la comparación de nuestros indicadores con las posibilidades de búsqueda electromagnética enemiga.

(2) Para emplear la base de datos se recurrirá a los Procesos de PIC, PEC y SEGOPE, que ayudarán al analista a determinar rasgos, patrones, indicadores y perfiles electromagnéticos.

33. EVALUACIÓN DE LA AMENAZA ELECTROMAGNÉTICA (Paso 1, del proceso C-INTENSE)

a. Objetivo de la evaluación
El objetivo de la evaluación de la amenaza electromagnética es determinar las posibilidades técnicas y operacionales de los recursos de MAGE y de INTETE enemigas, para detectar, explotar, dañar o destruir los Sistemas de Comunicaciones y electrónicos de nuestras fuerzas; a través de

informaciones que demuestren, presuman o provean evidencia del intento de conducir tales actividades.

b. Consideraciones generales

(1) La evaluación de la amenaza es una actividad continua y dinámica, que se lleva a cabo desde época de paz o períodos pre-operacionales hasta en períodos de combates.

(2) La evaluación es realizada por todos los escalones desde el nivel de batallón hasta los altos escalones presentes en una zona de acción o área de responsabilidad.

(3) La evaluación de la amenaza electromagnética continua aún sin existir específicas tareas o misiones para los recursos de C-INTETE.

(4) Esta evaluación también se realiza concurrentemente con los otros pasos del proceso de C-INTETE.

(5) La evaluación de la amenaza electromagnética generalmente determina.

(a) Posibilidades técnicas y operacionales de MAGE e INTETE ena
(b) Modos típicos de operación
(c) Despliegues y actividades actuales o recientes
(d) Prioridades de los recursos MAGE e INTETE enemigos conocidos.

c. Secuencia de evaluación de la amenaza electromagnética

(1) Los recursos MAGE y de INTETE enemigos conocidos son determinados de la base de datos. Cuando se recibe una tarea para apoyar una actividad u operación específica, la atención de la evaluación de la amenaza se centra en el refinamiento de la información genérica contenida en esa base de datos, para determinar de manera específica (a la máxima extensión) la amenaza electromagnética a esa actividad u operación.

(2) Identificación de los probables sistemas o unidades enemigas de búsqueda.

(a) El proceso empieza cuando un informe sobre los recursos de búsqueda electromagnética enemigos es recibido por el analista especialista del EACI.

(b) Estos informes podrían estar dando respuestas a todas o

algunas de las interrogantes siguientes:

1. Es el sistema/unidad de búsqueda electromagnética parte de un sistema/Escalón mayor?
2. ¿Cuáles son sus posibilidades?
3. ¿Lo está empleando de acuerdo a su doctrina?
4. ¿Cómo se ha obtenido la información?
5. ¿Cuántos sistemas iguales o similares fueron localizados?

(c) Basado en las respuestas a estas interrogantes el analista/especialista deberá identificar la Unidad de búsqueda electromagnética enemiga y determinar sus probables posibilidades y empleo doctrinario.

(3) Modificar los parßmetros de los recursos de búsqueda de acuerdo a la situación.

(a) El analista/especialista toma la información obtenida y la reajusta de acuerdo a la situación actual. Para esto, intrega la base de datos refinada, la información del clima y condiciones meteorológicas (CCMM) y la zona de operaciones (terreno), para considerar los elementos siguientes:

1. Efectos del terreno sobre los recursos de búsqueda electromagnética.

2. Efectos del clima y CCMM sobre los recursos de búsqueda electromagnética.

3. Efectos del terreno sobre los movimientos de los recursos de búsqueda electromagnética.

4. Efectos del clima y CCMM sobre los movimientos de los recursos de búsqueda electromagnética.

5. Ubicaciones anteriores de los recursos de búsqueda electromagnética.

6. Empleo previo que tuvieran estos recursos de búsqueda electromagnética.

(b) El resultado de la integración en los elementos considerados en el Sub párrafo anterior, deberán permitir al analista reajustar sus plantillas doctrinales a la situación actual.

(4) Predecir la amenaza enemiga para la búsqueda

(a) Empleando una carta topográfica (o satelital/ aerofotográfica), plantillas doctrinales y doctrina enemiga, el analista estará listo para predecir los lugares de posicionamiento de los recursos de búsqueda enemiga.

(b) Considerando el terreno, el clima/CCMM y los parámetros de los sistemas electromagnéticos, se desarrollarán calcos para diferentes alcances para cada sistema enemigo de búsqueda electromagnética.

(c) Estos calcos nos mostrarán el área de cobertura de los sistemas, y al colocarlos sobre las cartas topográficas, se podrán plotear las probables ubicaciones desde las cuales el enemigo podría conducir sus actividades de búsqueda.

(d) Basándose en como el enemigo conducía en el pasado estas actividades y el tiempo que le toma transferir información desde la ubicación del colector enemigo hasta su comandante; el analista hace una selección de la mejor probable ubicación de los colectores (individualmente).

(5) Confirmar la amenaza

(a) En este punto, el analista verifica los mensajes e informes para determinar si cualquier recurso de búsqueda/reunión ha sido visto o reportado. Si cualquier colector ha sido localizado, el analista realizará los ajustes necesarios.

(b) Pedidos específicos para una determinada confirmación puede realizarse al escalón superior u otro elemento que cuente con mayores y mejores sistemas de análisis, que le permitan al analista confirmar la amenaza.

34. EVALUACION DE NUESTRAS VULNERABILIDADES ELECTRO MAGNETICAS (Paso 2, del proceso de C-INTETE)

a. El éxito de este paso es altamente dependiente de la predicción de la amenaza.

b. La evaluación de nuestras vulnerabilidades electromagnéticas incluye:

(1) Examen de las características técnicas y operacionales de las comunicaciones y electrónica (C-E) del Comandante.
(2) Reunir y analizar los datos para identificar potenciales vulnerabilidades electromagnéticas.
(3) Evaluar las vulnerabilidades en el contexto de la evaluación de la amenaza.

c. En este paso el analista toma la predicción de la amenaza y la compara con el examen detallado de los rasgos de las C-E del comandante. Adicionalmente, esta evaluación es realizada para una área específica y para un período de tiempo determinado.

d. Secuencia de la evaluación de nuestras vulnerabilidades electromagnéticas (pasos)

(1) Conducir análisis de nuestros patrones electromagnéticos:

(a) Estudiando detalladamente las acciones electromagnéticas, estereotípicas que ocurren a menudo en circunstancias dadas.

(b) Los elementos de la base de datos que se empleen son aquellos que podrían dar al enemigo un indicio sobre el tipo de Unidad, su dispositivo, sus actividades o posibilidades de nuestras fuerzas.

(c) Empleando la orientación del Cmdte, el analista extrae los archivos pertinentes para determinar si se presentan nodos críticos electromagnéticos.

(2) Analizar rasgos electromagnéticos de nuestras fuerzas:

(a) Se realiza para determinar si algún equipo de C-E presenta características electromagnéticas distintivas al enemigo.

(b) En la base de datos se pueden encontrar características de los Equipos, así como en la sección III de los COEq's y otros documentos de situación de operatividad, que permitirán al analista identificar el equipamiento de la Unidad, equipos únicos o especiales a la Unidad y rasgos electromagnéticos de la actividad o de la unidad.

(3) Determinar perfiles electromagnéticos de nuestras fuerzas:

(a) El analista obtiene este resultado (determinación de perfiles) a través del análisis de patrones e identificación de rasgos, que al correlacionarlos con perfiles pasados producirá un perfil

de la Unidad actualizado.

(b) Los perfiles electromagnéticas de nuestras fuerzas se emplean para compilar una lista de Susceptibilidades que se convertirán posteriormente en Elementos Esenciales de Información Amiga (EEIA)

(4) Analizar nuestras formas de acción (F/A) y actividades de apoyo

(a) El analista "plotea" las ubicaciones actuales de nuestras unidades sobre una carta o mapa topográfico, que se obtienen de los mensajes de las propias unidades.

(b) Luego el analista "plotea" sobre la carta las ubicaciones planeadas y eventos de nuestras formas de acción. Si no se cuenta con información disponible, la extraerá de la base de datos y de los extractos de plantillas para formas de acción. Las plantillas son superpuestas sobre las direcciones de aproximación para determinar posiciones doctrinarias de nuestras fuerzas para las posiciones previstas en las formas de acción.

(c) Durante estos ploteos de posiciones, el analista debe ir modificando la aproximación doctrinaria de la F/A al terreno, a las CCMM y a los obstáculos.

(d) Al finalizar, el analista ubica los lugares donde pueden esperarse actividades significtivas; así como predice cuando estas podrían ocurrir. Con todo esto el analista estará en condiciones de priorizar los eventos de acuerdo a la importancia para la operación.

(5) Determinar indicadores de nuestras FF/A

(a) En este paso, el analista selecciona los indicadores, presentados en las ubicaciones planeadas de la F/A. Esta data podría haberse creado durante la determinación de los perfiles de nuestras unidades.

(b) Adicionalmente, el analista debe considerar las actividades del escalón inmediato superior y de elementos vecinos o adyacentes que podrían generar indicios al enemigo sobre nuestras formas de acción.

(c) El analista reúne toda la información sobre los indicadores y los modifica de acuerdo al terreno, las CCMM y la situación. Se deberá contar con los perfiles de las actuales y planeadas ubicaciones, con lo que se tendrá un cuadro completo para evaluar las vulnerabilidades.

(6) Determinar las prioridades de nuestras vulnerabilidades

(a) En este paso se estará listo para comparar nuestros perfiles contra las posibilidades enemigas de búsqueda y reunión de información electromagnética.

(b) Aquí se determina que indicadores son vulnerabilidades, para lo cual se tomará un indicador a la vez para analizarlo e identificar si el enemigo puede explotarlo, al mismo tiempo se anotará cuantos colectores pueden "ver" el indicador; luego se contrasta la amenaza con cada indicador, descartándose aquellos que no podrá ver al enemigo.

(c) Los indicadores que el enemigo puede detectar se convierten en vulnerabilidades, los que serán priorizadas de acuerdo a:

1. Su importancia.
2. Su exclusividad.
3. Susceptibilidad en nuestras formas de acción.

(d) La exclusividad de la vulnerabilidad, se identifica por cuantas veces ella podría aparecer dentro de nuestras formas de acción (la vulnerabilidad más común tendrá la menor prioridad).

(e) La importancia de la vulnerabilidad, esta dada por la que le asigna el analista luego de consultarla con el G-3.

(f) La susceptibilidad de nuestra F/A (a la búsqueda enemiga) está dada por el número y variedad de amenazas que tiene el indicador. Demasiadas de ellas reducirán la prioridad de la vulnerabilidad.

(g) Adicionalmente, el analista debe considerar proteger la vulnerabilidad. Si una vulnerabilidad es demasiado fácil o demasiado difícil de ser detectada por los órganos de búsqueda enemigos, entonces tendrá la más baja prioridad pare su protección.

(h) Las vulnerabilidades que no pueden ser protegidas serán tomadas en cuenta y la información que se obtenga de ellas serán puestas en conocimiento del Cmdte.

(i) Al finalizar todo este paso, el analista contará con una lista de indicadores que deberán ser considerados para convertirse en EEIA.

35. DESARROLLO DE LAS OPCIONES DE CONTRAMEDIDAS (Paso 3, del proceso de C-INTETE)

a. Este paso se realiza para que el analista de C-INTETE pueda alcanzar o cumplir su tarea, siempre y cuando sus recomendadas contramedidas:

(1) Sean realísticas.
(2) Puedan ser implantadas por el Comando.
(3) Apoyen al concepto de la Operación del Cmdte.

b. Lo que se busca en este paso es hacer una lista de opciones de contramedidas apropiadas que permitan identificar vulnerabilidades a proteger.

c. Las opciones de CM pueden variar debido a lo cumplicado de la amenaza, el tiempo y recursos disponibles al Cmdte.

d. Las opciones de CM deben ser priorizadas para que se puedan incluir en una Apreciación de su efectividad. El analista deberá seleccionar sólo una CM de todas las recomendadas.

e. Secuencia del desarrollo de las opciones de CM

(1) Determinar CM

(a) Cuando se determina una CM, se pueden tomar cualquiera de las tres opciones de CM siguientes:

1. El colector enemigo deberá ser considerado un objetivo a ser destruido o desorganizado.
2. La CM podría emplearse para reducir o eliminar la vulnerabilidad.
3. La vulnerabilidad podría emplearse como parte de una actividad de engaño.

(b) En el primer caso, el analista registra todos los posibles colectores para ser considerados como objetivos. Verifica el criterio que asumirá para que dichos objetivos puedan atacarse con COME, artillería u otro medio de destrucción y lo compara con los colectores. Si resulta que de esa comparación se pueden atacar, entonces se recomendará al G-3 que se les considere como objetivos.

(c) En el segundo caso, el analista emplea material de referencia (POV'S, P/O, O/O y archivos históricos) y registros de todos las posibles medidas de COCOME y SEGUTE (Seguridad de Telemática) para contrastarlas con las vulnerabilidades encontradas. El analista compara la posible CM contra cada vulnerabilidad para encontrar la CM que podría proteger más de un indicador al mismo tiempo.

(d) En el tercer caso, se registran todas las posibles actividades de engaño que se podrían emplear con la vulnerabilidad.

(e) Antes de recomendar la opción de CM, el analista selecciona la CM propuesta basado en:

1. Equipamiento disponible.
2. Posibilidad del Comando para ejecutar la CM
3. Habilidad del Cmdte para lograr esa posibilidad.
4. Tiempo requerido para realizar la CM.

(2) Analizar la apreciación de la efectividad

(a) Empleando el perfil de la Unidad y las posibilidades enas, el analista determina:
1. Probabilidad de que nuestras fuerzas puedan emplear con éxito la CM.
2. Probable efectividad de la CM ante el intento de degradarla por parte del enemigo.
3. Probabilidad de que el enemigo acepte o crea el engaño.

(b) Mientras se está realizando esta evaluación el analista debe asegurar que las opciones recomendadas no interfieran con las operaciones planeadas u operaciones de engaño que se están ejecutando.

(3) Realizar análisis de riesgo

a) El analista predice la reacción enemiga al EEIA y los efectos de esta reacción sobre nuestra F/A.
(b) Se debe comparar también los recursos y la efectividad de la CM, para determinar la mejor CM y cual EEIA no puede estar razonablemente protegido contra la búsqueda enemiga.

(4) Generar una lista de opciones de CM

(a) Compilar una lista de recomendaciones previamente evaluadas y agregar a ellas la apreciación de SEGOPE.

(b) Se debe tener también una lista de opciones de CM (con su análisis de riesgo) para el EACI.

36. EVALUACION DE LA APLICACION DE LAS CONTRAMEDIDAS (Paso 4, del proceso de C-INTETE)

a. En este paso se determina la efectividad de la CM que fuera adoptada por el Comandante. Esta evaluación permitirá descubrir:

(1) Que tan bien, la conducción de la operación concuerda con el concepto operacional planeado.
(2) Que tanto concuerda la amenaza confirmada, con la previamente evaluada en el paso 1.
(3) Si los rasgos, patrones y perfiles de Comunicaciones - electrónicas están conforme a aquellos esperados.
(4) En que grado la CM aplicada, influencia en el éxito de las operaciones.

b. Este paso proporciona al comandante el medio para determinar la efectividad de su esfuerzo de Seguridad de Telemática (SEGUTE) en la conducción total de las operaciones y contribuye significativamente a la base de datos del proceso de C-INTETE.

c. La evaluación de la aplicación (efectividad) de las CM se efectuará a través de:

(1) El monitoreo de la reacción enemiga a nuestras operaciones.
(2) La determinación si el enemigo ha prorizado el conocimiento de la operación o alguna debilidad específica de nuestras fuerzas.
(3) El monitoreo de nuestros sistemas de C-E.
(4) Pedidos de información.

d. Secuencia de la evaluación de contramedidas

(1) Confirmar la aplicación de la CM

El analista determina las más críticas CM'S que serán evaluadas y las monitorea para:

(a) Identificar los sistemas de búsqueda de nuestras fuerzas capaces de monitorear.
(b) Seleccionar los eventos que serán monitoreados
(c) Solicitar que se misionen a nuestros sistemas de búsqueda.

(2) Determinar indicadores para la amenaza

(a) Esto se puede hacer a través del monitoreo de los esfuerzos de búsqueda enemiga, ya que el analista deberá conocer si los sistemas de búsqueda del enemigo se están moviendo en la zona de operaciones por algunas otras razones que no sean las de maniobrar a nuestras fuerzas.
(b) Adicionalmente, este monitoreo de la situación enemiga puede ayudarnos a determinar, si éste esta pronosticando la acción de nuestras fuerzas empeñadas.

(3) Analizar la efectividad de la CM

(a) En esta parte el analista compara lo que se ha aprendido anteriormente, contra las actividades de nuestras fuerzas para identificar probables compromisos de información crítica.

(b) Buscando en los patrones enemigos de búsqueda sobre un período de tiempo y al compararlo con nuestras FF/A, el analista tratará de determinar si el enemigo ha priorizado el conocimiento de esas FF/A.

(c) Si se descubre que los esfuerzos de búsqueda del enemigo, llegan a conocer nuestras planeadas operaciones, esta información será trasladada inmediatamente al G-3 para su evaluación.

(4) Actualizar la base de datos

Toda la información obtenida debe estar en archivos apropiados y deberán actualizar la base de datos.

CAPITULO 3

SEGURIDAD DE TELEMÁTICA

SECCION I. GENERALIDADES

37. CONCEPTO DE SEGURIDAD DE TELEMÁTICA

a. Es un término genérico, que involucra una serie de medidas y/o actividades tanto de la Seguridad de las Operaciones (SEGOPE) como de la Contrainteligencia de Telemática (C-INTETE), destinadas a contrarrestar las actividades de Inteligencia de Telemática y de Guerra Electrónica del eno.

b. La SEGUTE busca la protección de la información operacional proveniente de nuestros emisores de comunicaciones y electrónicos, a través de la práctica de técnicas y tácticas de Seguridad de Comunicaciones (SEGCOM) y de Seguridad Electrónica (SEGELEC).

38. NECESIDAD DE LA SEGUTE

a. El éxito que normalmente obtiene la INTETE enemiga, se basa en tres aspectos importantes:

(1) Competencia técnica para realizar sus actividades y funciones.

(2) Recursos o equipamiento con que cuenta para conducir opns de inteligencia y de Guerra Electrónica.

(3) Oportunidades que se le presentan para explotar los emisores objetivos.

b. Los dos primeros aspectos son dependientes del eno, sin embargo el tercer aspecto depende de nuestras fuerzas, ya que podremos impedir los éxitos de la INTETE enemiga, negándole estas oportunidades.

c. Esta negación de oportunidades requerirá de un gran esfuerzo para desarrollar técnicas y programas efectivos de SEGUTE, que sólo se alcanzará si se tiene un profundo conocimiento del empleo de los Sistemas de Comunicaciones y Electrónica, así como del riesgo que representa su uso indiscriminado e inapropiado.

39. RELACION DE LA SEGUTE CON LA C-INTETE

a. La C-INTETE es una parte de la Contrainteligencia y apoya al proceso de toma de decisiones del Comandante. El esfuerzo de la C-INTETE está orientado al asesoramiento del Cmdte en el mantenimiento de la supervivencia de su fuerza, ayudándolo a preservar la seguridad y retener el elemento sorpresa. Este esfuerzo implica ser un miembro activo en el proceso de planeamiento.

b. Las técnicas de apoyo de la SEGUTE, previamente empleadas por la inteligencia, aún permanecen válidas; sin embargo el empleo de la información desarrollada ha cambiado radicalmente. Ahora las funciones de apoyo de SEGUTE apoyan al proceso de C-INTETE, el cual coloca a éstas, en perspectiva hacia el apoyo total proporcionado al Cmdte. Por ejemplo el monitoreo de SEGCOM (una técnica de apoyo de SEGUTE: colección de data "después del hecho") no será más un producto aislado; si se le emplea, deberá ser como parte de la evaluación de la aplicación de las contramedidas y para actualizar la base de datos de la C-INTETE.

40. FUNCIONES DE APOYO DE LA SEGUTE (Ver figura 10)

a. La SEGUTE se clasifica en una serie de funciones agrupados en dos áreas mayores denominados.

(1) Seguridad de Comunicaciones (SEGCOM)
(2) Seguridad Electrónica (SEGELEC)

b. La SEGCOM se subdivide a su vez en:

(1) Seguridad física.
(2) Seguridad Criptográfica.
(3) Seguridad de Trasmisión.
(4) Seguridad de Emisión.

c. La SEGUTE se subdivide a su vez en:

(1) Seguridad Inherente
(2) Seguridad Industrial
(3) Seguridad Operacional

Figura 10.- Funciones de Apoyo de la SEGUTE

d. Las funciones de apoyo de SEGUTE incluyen las actividades generales siguientes:

(1) Evaluación de las vulnerabilidades de SEGUTE (SEGCOM y SEGELEC).
(2) Monitoreo de SEGCOM.
(3) Análisis de criptoseguridad (cripto - acceso).
(4) Desarrollo de medidas de seguridad de trasmisión.
(5) Inspección de criptofacilidades (cripto - acceso).
(6) Asesoramiento a criptoredes.
(7) Asistencia y asesoramiento técnico de SEGELEC.
(8) Revisión de publicaciones de SEGUTE.
(9) Entrenamiento de SEGUTE.
(10) Asistencia y asesoramiento a las COCOME.

c. En la figura 11, se muestra como se agrupan las actividades generales de las funciones de apoyo de SEGUTE:

FIGURA 11

SECCION II. EVALUACION DE LAS VULNERABILIDADES DE SEGURIDAD DE TELEMÁTICA

41. CONCEPTO DE LA EVALUACION DE LAS VULNERABILIDADES DE SEGURIDAD DE TELEMÁTICA (SEGUTE)

a. Es una función de apoyo de la SEGUTE que se realiza para determinar hasta que punto los sistemas de emisores de comunicaciones y no-comunicaciones de nuestras fuerzas, así como sus radiaciones electromagnéticas, son susceptibles a ser explotados y/o desorganizados por el enemigo.

b. Durante la ejecución de esta función se compara las posibilidades INTETE del enemigo, con los perfiles electromagnéticos de nuestras fuerzas, identificando las vulnerabilidades a la amenaza de colección enemiga. Una vez identificadas nuestras vulnerabilidades se deberá proporcionar el consiguiente asesoramiento en el desarrollo e implantación de contramedidas.

42. CONSIDERACIONES GENERALES SOBRE NUESTRAS VULNERABILIDADES

a. Una vulnerabilidad es una debilidad que el enemigo puede explotar en detrimento de nuestras fuerzas. La identificación de potenciales vulnerabilidades es de significativa importancia para un Comandante antes y durante el combate; ya que cuando una debilidad se conoce, ella puede ser neutralizada con efectividad.

b. A pesar de lo expresado en el Sub-párrafo anterior, algunas circunstancias pueden influir contra la neutralización de algunas debilidades. Por ejemplo, un sistema o una actividad puede ser considerada crítica para el éxito de una misión, en tal caso el Comandante deberá evaluar el riesgo y determinar una forma de acción; pero esto sólo se podrá efectuar de manera eficaz si se conocen las vulnerabilidades, de lo contrario el balance o comparación entre las consideraciones de seguridad y los requerimientos operacionales será extremadamente difícil (más de lo que normalmente lo es).

c. Para seleccionar la mejor forma de acción, el Cmdte debe conocer no sólo los peligros, sino también la probabilidad de que ellos lleguen a ser desventajas u obstáculos para el éxito de la misión.

43. PROCEDIMIENTO QUE SIGUE LA EVALUACION DE LAS VULNERABILIDADES DE SEGUTE

El procedimiento para apreciar la vulnerabilidad electromagnética de una Unidad o actividad, se le conoce con el nombre de "evaluación de las vulnerabilidades electromagnéticas", la misma que comprende los pasos siguientes:

a. Determinar rasgos, patrones y perfiles electromagnéticos.
b. Identificar emisiones interrelacionados (discriminadores).
c. Determinar las potenciales vulnerabilidades.
d. Graficar trayectorias de trasmisión
e. Identificar probables vulnerabilidades.

44. DETERMINACION DE RASGOS, PATRONES Y PERFILES ELECTROMAGNETICOS (paso 1)

a. Además de lo señalado en los capítulos anteriores se debe tener en cuenta las consideraciones siguientes:

(1) **Los rasgos** comprenden o incluyen cuatro (04) categorías:

(a) Imágenes
(b) Electromagnéticos
(c) Acústicos
(d) Olfatorios

(2) Los rasgos electromagnéticos son el resultado de las radiaciones de emisores de comunicaciones y no-comunicaciones. En término más amplios, la detección de un rasgo electromagnético específico puede mostrar la presencia de una cierta actividad en un área. Tal detección podrían emplearlos otros sensores para limitar el área de búsqueda; y, por la agrupación de rasgos individuales un analista enemigo podría detectar instalaciones, unidades y actividades.

(3) **Los patrones electromagnéticos** comprende o incluyen nueve (09) categorías:

(a) Volumen de Tráfico.- La cantidad de trasmisiones cursadas entre estaciones en una red, fluctuará conforme la situación táctica cambia. Los patrones que se desarrollen pueden reflejar claramente varias fases de una operación de combate.

(b) Horarios regulares de operación.- Conociendo la probable

hora de una futura trasmisión, el enemigo sólo necesitará prender su interruptor en el horario establecido y continuar sus operaciones de interceptación. Los patrones desarrollados dirán al enemigo que es lo que estamos haciendo.

(c) **Duración de la operación del emisor.-** Esta categoría indicará a un analista enemigo, la relativa importancia de un emisor particular y la red en la cual opera. Cuando un emisor opera más tiempo que otro (p.e una ECR), provocará interés en el enemigo por saber que ocurre en las inmediaciones del terreno o área geográfica donde opera, a que Unidad está asociado o a que sistema de armas pertenece. Cuanto más tiempo trasmita un emisor, más probablemente el enemigo podrá ubicarlo, identificarlo y/o neutralizarlo por el fuego o por la perturbación.

(d) **Reconstrucción de redes.-** La identificación de una ECR y sus puestos o estaciones asociadas, permitirán determinar la estructura de la organización; y ayudarán al analista enemigo a reforzar sus conclusiones de inteligencia. El rango de frecuencias, las características de modulación, empleo de equipos de seguridad de voz y de terminología especializada, son las piezas del rompecabezas que el analista necesita para determinar el tipo de red y su relativo valor como blanco para la guerra electrónica y/o Inteligencia de Telemática.

(e) **Patrones de llamada.-** La IOCE e IPCE normalmente establecen instrucciones para llamadas y la secuencia de las mismas. Una ECR que viola o permite la violación de esta orden de llamada dando respuesta, puede establecer un patrón de llamada.

(f) **Distribución de Canales en los Sistemas multicanal.-** El uso específico de canales en una red multicanal para la trasmisión de tipos específicos de información pueden establecer patrones que pueden facilitar la identicación de Unidades, en los lugares donde se instalan los terminales. El empleo o no de canales basados en un fundamento continuo, puede también reflejar un patrón

(g) **Ubicación de los emisores.-** Los patrones también se pueden derivar de colocar los emisores en ciertas lugares, normalmente en los puntos más altos del terreno (especialmente en redes multicanal) o empleando terreno prominente en específicas direcciones de aproximación.

(h) Horario de Mantenimiento.- Cuando se debe establecer este horario no debe obedecer a reglas o procedimientos fijos, para evitar presentar patrones que puedan ser explotados por el enemigo.

(i) Patrones de reubicaciones de Sistemas de Comando y Control (c^2) .- Las Unidades que emplean una variedad de medios de comunicaciones, tendrán siempre instalaciones de C^2 y alternas (o de reserva). Durante los períodos de reubicación (o desplazamientos) es necesario mantener el c^3 así como continuar ejecutando misiones específicas; lo que se cumple utilizando una combinación de comunicaciones principales y alternas. Cuando el circuito alterno llega a activarse, tanto en el antiguo como en el nuevo lugar existirá una indicación de que algo está ocurriendo. Igualmente, cuando las comunicaciones se establezcan entre el antiguo y el nuevo lugar, o entre el nuevo lugar y las Unidades subordinadas del antiguo lugar, evidenciará un patrón de reubicación. La reducción de las capacidades de comunicaciones de una Unidad a un nivel específico, antes de un movimiento es también un patrón electromagnético susceptible de análisis.

b. Los equipos de comunicaciones y electrónicos, generalmente son de emisiones de línea recta; por lo que sus rasgos y patrones de radiación pueden detectarse con cierta facilidad; más aun si se conoce que los batallones y GGUUCC emplean equipos monocanales de voz y radioteletipos, así como el EO y escalones superiores emplean equipos multicanal con rasgos característicos. Los radares serán aún más fáciles de identificar.

c. La determinación de rasgos, patrones y perfiles electromagnéticos pueden permitir:

(1) Detectar otras trasmisiones en el área.

(2) Emplear radiogonometría para determinar ubicaciones.

(3) Categorizar las Telemática mediante el análisis de las mismas.

(4) Plotear los tipos de trasmisiones en una determinada área.

45. IDENTIFICACION DE EMISIONES INTERRELACIONADAS (DISCRIMINADORES) (paso 2)

a. Un analista de inteligencia o contrainteligencia de Telemática puede emplear la información obtenida en el paso anterior, para mostrar ubicaciones de PPCC, puntos de abastecimiento, principales armas de las Unidades, áreas de concentración y despliegues. Esta posibilidad se hará más factible si ciertos radios o radares son empleados exclusivamente asociados a Unidades específicas o sistemas de armas.

b. Cuanto más grande la Unidad, más grande y distintivo será su rasgo electromagnético, del que se podrá deducir: movimientos, información del orden de batalla, estructuras de sus redes de radio, despliegue táctico y en mayor o menor grado sus intenciones. TODO ESTO CON SOLO DETECTAR, IDENTIFICAR Y LOCALIZAR TRASMISORES SIN NECESIDAD DE LEER UN SOLO MENSAJE.

c. Adicionalmente al rasgo electromagnético, los patrones electromagnéticos pueden hacer que nuestros sistemas de comunicaciones y no-comunicaciones sean vulnerables a la explotación enemiga, al ser interrelacionados y/o discriminados, señalándonos perfiles que pueden convertirse en debilidades y fuentes de indicadores al enemigo.

46. DETERMINACION DE POTENCIALES VULNERABILIDADES (paso 3)

a. En este paso se comparan las posibilidades de interceptación del enemigo con nuestros perfiles electromagnéticos, posibilitándonos la determinación de que emisores o sistemas son potencialmente vulnerables a esa interceptación.

b. Este paso sigue la misma secuencia que el proceso de C-INTETE, que fue tratado en el capítulo anterior.

47. GRAFICACION DE LAS TRAYECTORIAS DE TRASMISION E IDENTIFICACION DE PROBABLES VULNERABILIDADES (paso 4 y 5)

a. Durante el cuarto paso se emplean diagramas o calcos para cada tipo de emisor y durante el quinto paso se comparan éstos con los diagramas o calcos de los posibles o probables colectores enemigos conocidos.

b. Durante estos pasos, las ubicaciones de los emisores amigos e interceptores enemigos son ploteados en ambos juegos de calcos o diagramas, superponiéndose. En los lugares donde se interceptan las trayectorias de trasmisión de un emisor amigo con un colector enemigo, el primero de ellos será considerado vulnerable.

c. Luego se analiza para determinar en que grado esta vulnerabilidad puede comprometer la actividad o misión de la Unidad a que pertenece el emisor. Teniendo esta información evaluativa, el Comandante decidirá si acepta el riesgo o desarrolla alguna contramedida para neutralizar esta vulnerabilidad.

SECCION III. SUPERVISION DE SEGUTE

48. PROPOSITO DE LA SUPERVISION DE SEGUTE

a. La supervisión de SEGUTE es el vehículo principal para realizar con éxito la evaluación de las vulnerabilidades de SEGUTE, cuyo propósito será

identificar areas para mejorar la efectividad operativa total de nuestras fuerzas, a través del incremento de las prácticas y procedimientos de SEGUTE.

b. Para alcanzar este propósito todos los sistemas de C-E asociados con una operación o función deberán examinarse, poniéndose particular atención sobre los medios de comunicaciones y la aplicación de los sistemas de no-comunicaciones.

c. Una supervisión de SEGUTE enfatiza técnicas tales como entrevistas al personal, observaciones "in situ", monitoreo y análisis de comunicaciones no-encriptadas, inspecciones de criptofacilidades, evaluaciones a las criptoredes e identificación de los perfiles electromagnéticos asociados con la operación o función.

49. FORMA DE CONDUCIR LA SUPERVISION DE SEGUTE

a. Para alcanzar el propósito de incrementar la efectividad de nuestras fuerzas, una supervisión de SEGUTE debe conducirse como una verificación de C-E y no como una investigación de violaciones de seguridad o de búsqueda de culpables para sancionarlos disciplinariamente.

b. El objeto de la supervisión de SEGUTE no es buscar culpables, sino conducir una examen paso a paso de todos los requerimientos de C-E para el planeamiento y ejecución de operaciones militares, ayudando de esta manera a los Comandantes en la eliminación de sus debilidades de SEGUTE que puedan ser fuentes de información para el enemigo.

c. La supervisión empieza con la etapa de planeamiento de una operación y continua a través de la ejecución y etapas post-evaluativas.

d. Lo fundamental de este concepto de supervisión, es reconocer el hecho de que el personal militar debe emplear sistemas de C-E para conducir sus operaciones. Por lo tanto existirán riesgos en su uso, que la supervisión buscará detectar, buscando de esta manera complementar a las operaciones que se conducen, para asegurar que los sistemas de C-E involucrados son empleados tan seguramente como sea posible.

e. La supervisión de SEGUTE se conduce para las practicas y procedimientos de comunicaciones y de no-comunicaciones y consta de los pasos siguientes:

(1) Reunir y documentarse de toda la data pertinente a la supervisión (particularmente sobre la amenaza electromagnética).

(2) Procesar y analizar la data reunida (para identificar las razones del interés de la INTETE enemigos).
(3) Desarrollar lo descubierto y extraer conclusiones (a través de entrevistas y observaciones).
(4) Desarrollar recomendaciones viables (basados en juicios realísticos de lo observado y escuchado).
(5) Preparar informes.

50. SUPERVISION DE LA EVALUACION DE LA AMENAZA ELECTROMAGNETICA

a. La necesidad para una supervisión de SEGUTE está directamente relacionada a la amenaza hostil. El impacto de una supervisión será mayor, si esa amenaza a los sistemas de C-E de un comando dado, puede definirse.

b. La definición de la amenaza también ayudará en la selección y priorización de materias para supervisar SEGUTE.

c. Se debe asegurar un conocimiento exacto de los éxitos de cualquier esfuerzo de INTETE enemiga, en todo caso se asumirá que cualquier enemigo puede desarrollar sus posibilidades para interceptar todos los tipos de trasmisiones de nuestros sistemas de C-E.

d. La identificación de la amenaza es una parte significativa de un completo análisis de nuestras vulnerabilidades. El interés de la INTETE enemiga en una operación o ejercicio de campaña de nuestras fuerzas deriva de muchas razones, entre las más importantes están el valor de la información proveniente de nuestras C-E y la vulnerabilidad de ellas, a la interceptación y explotación. Estas consideraciones se combinan para formar la base para las apreciaciones sobre el enemigo.

e. Siempre que sea posible, la información acerca de una amenaza específica sera puesta a consideración de una organización u operación que la solicita o emplea. Cuando falta una prueba positiva sobre el interés de la INTETE enemiga, se presumirá que ese interés será la base para conducir la supervisión.

51. ENTREVISTAS Y OBSERVACIONES DE SEGUTE

a. Una entrevista efectiva sera crucial para el éxito de la supervisión; por lo que se deberán entrevistar desde el Cmdte C-E, personal de SEGUTE, elementos seleccionados del G-3 y G-2 hasta cualquier Oficial, Técnico o Sub-oficial que origine, reciba o traslade información.

b. Estas entrevistas complementadas con las observaciones "in situ", proporcionan valorables criterios para ver y entender con claridad como la unidad actualmente trabaja (antes de saber de como debería trabajar).

c. El participar activamente en las operaciones que se están realizando en la unidad, es también una invalorable parte de la supervisión, pués permitirá al supervisor "ver y oir" lo que actualmente ocurre, antes que solo limitarse a obtener información a través de entrevistas y revisión de documentos.

d. Las Comunicaciones - Electrónicas serán observados como ocurren normalmente, para de esta manera formarse juicios realísticos y recomendar soluciones prácticas que permitan corregir una debilidad de SEGUTE.

52. INFORMES DE RESULTADOS DE LA SUPERVISION DE SEGUTE

a. Los especialistas de SEGUTE también proporcionan asistencia técnica en otras áreas de su competencia, entre ellas la SEGCOM.

b. La evaluación de inseguridades a la SEGCOM y los informes respectivos, estan relacionados con la reacción a los mismos y a una supervisión general de las acciones correctivas, que comprende:

- El monitoreo y revisión de todos estos informes de inseguridades de SEGCOM
- La determinación de si la información recibida es adecuada para la evaluación.

c. Resulta de particular importancia la revisión de incidentes para determinar si la influencia de la INTETE enemiga está presente. Esto requiere estrecha coordinación entre todos los elementos de apoyo de SEGOPE, para asegurarse que se dará asesoramiento preciso a la autoridad evaluadora.

d. Todas las organizaciones de CI, son responsables de proveer asesoramiento a los Comandantes, en la identificación de inseguridades así como en la preparación de los informes sobre el particular.

e. Las unidades de Comunicaciones y de GE deberán proporcionar expertos en la cobertura de la porción electromagnética y en el planeamiento del engaño; ya que serán ellos quienes tendrán información de "primera mano" sobre los rasgos y perfiles electromagnéticos de nuestras fuerzas y cuando/donde serán vulnerables. Sus informaciones constituirán elementos valiosos para la formulación de los planes de engaño y en el desarrollo de los argumentos.

CAPITULO 4

SEGURIDAD DE COMUNICACIONES

SECCION I. CONCEPTO, CLASIFICACION Y RESPONSABILIDADES DE LA SEGCOM

53. CONCEPTO DE SEGURIDAD DE COMUNICACIONES (SEGCOM)

a. La SEGCOM es un conjunto de medidas, acciones y/o actividades destinadas a proteger nuestras telecomunicaciones; fundamentalmente negando a personas no autorizadas, información procedente de las mismas y/o evitando la interferencia, interceptación o engaño a nuestras redes de comunicaciones.

b. La SEGCOM es la salvaguarda de nuestras telecomunicaciones de la explotación enemiga, que comprende un conjunto de técnicas que incluyen el uso de códigos y equipos de seguridad de voz, procedimientos de radio silencio, radiotelefónicos, etc.

54. CLASIFICACION DE LA SEGCOM (COMPONENTES ESENCIALES)

a. Las medidas, acciones y/o actividades de SEGCOM son los actos u operaciones de carácter pasivo y activo que se toman para obtener la condición de seguridad, eliminando todo riesgo que atente contra el material, el personal, los mensajes, la información y el funcionamiento de los medios y sistemas de telecomunicaciones.

b. La aplicación de las medidas de SEGCOM proporcionarán protección a través de los componentes esenciales sgtes:

(a) Seguridad física.
(b) Seguridad criptográfica.
(c) Seguridad de trasmisión.
(d) Seguridad de emisión (TEMPEST).

c. En la **figura 12**, se resumen los principales medidas dentro de cada componente esencial.

FIGURA 12

55. RESPONSABILIDADES DE LA SEGCOM

a. De la Dirección de Inteligencia del Ejército (DINTE)

(1) Revisar y actualizar periódicamente (Semestralmente), las normas y disposiciones sobre seguridad criptográfica.

(2) Estudiar y analizar los informes sobre infracciones a la seguridad de las comunicaciones, durante el funcionamiento de los medios y la seguridad criptográfica, a fin de determinar las causas y acciones correctivas que se requieran tomar para prevenir y evitar estas infracciones.

b. De la Jefatura de Comunicaciones del Ejército (JCOME)

(1) Revisar y actualizar periódicamente (Anualmente), las normas y disposiciones sobre seguridad de comunicaciones, durante el funcionamiento de los medios.

(2) Estudiar y analizar los informes sobre las infracciones de la seguridad de comunicaciones que reporte la DINTE, a fin de determinar las causas y recomendar las acciones correctivas .

(3) Estudiar y analizar los reportes técnicos sobre el grado de seguridad y confiabilidad de los equipos de seguridad criptográfica y codificadores de voz en uso en el Ejército, recomendando las acciones correctivas en caso de encontrar deficiencias técnicas que los haga vulnerables.

(4) Comprobar mediante inspecciones inopinadas, la seguridad de las comunicaciones durante el funcionamiento.

c. Del Ejército de Operaciones y/o Regiones Militares

(1) El C-2 del EO supervisa el cumplimiento de las normas y disposiciones sobre la seguridad criptográfica y la seguridad de las comunicaciones durante el funcionamiento de los medios.

(2) El departamento G-2 formulará el informe sobre las infracciones a la seguridad de las comunicaciones durante el funcionamiento de los medios y a la seguridad criptográfica, para lo cual dispone de los órganos correspondientes encargados de analizar nuestras comunicaciones con el fin de determinar su estado de seguridad en el área de responsabilidad del EO y/o RM.

d. De la Gran Unidad de Combate

(1) El G-2 de la GUC supervisa el cumplimiento de las normas y disposiciones sobre la seguridad criptográfica y la seguridad de las comunicaciones durante el funcionamiento de los medios.

(2) La sección G-2 formulará el informe sobre las infracciones de la seguridad de las comunicaciones durante el funcionamiento de los medios y a la seguridad criptográfica en el área de responsabilidad de la GUC.

e. Del Comandante de Comunicaciones (en todos los escalones)

(1) Coordinar con el C-2/G-2 sobre los aspectos siguientes:

(a) Apoyo de las actividades de inteligencia con medios de comunicaciones.

(b) Toma, reproducción y distribución de fotografías del terreno.

(c) Proporciona información técnica sobre posibilidades de comunicaciones y GE del enemigo.

(d) Recomendar los RPI (EEI) y RI (ONI) sobre comunicaciones, así como de GE del enemigo.

(e) Empleo de medidas de apoyo de guerra electrónica (MAGE) en apoyo a las actividades de inteligencia.

(f) Medidas de Seguridad de Comunicaciones.

(g) Ventajas y desventajas en el empleo de contramedidas de apoyo electrónico (COME) contra ciertos blancos.

(2) Realizar el planeamiento de seguridad de comunicaciones que incluye:

(a) Formulación del POV de seguridad de comunicaciones.

(b) Emisión de directivas que norman la seguridad de comunicaciones.

(c) Formulación de la IOCE e IPCE relacionadas con la seguridad de comunicaciones.

SECCION II. SEGURIDAD FISICA DE COMUNICACIONES

56. CONCEPTO DE SEGURIDAD FISICA DE COMUNICACIONES

a. Es el componente de la SEGCOM que resulta de la aplicación de medios físicos para resguardar y/o proteger al material y a la documentación de SEGCOM, contra el acceso u observación por personal no autorizado.

b. Estos medios físicos son controles que aseguran que el material y documentación de SEGCOM sean recibidos, empleados, archivados, transportados y destruidos de una manera segura.

57. CONSIDERACIONES GENERALES SOBRE LA SEGURIDAD FISICA DE COMUNICACIONES

a. La seguridad física está compuesta de un sistema integrado y mutuamente apoyado de controles y barreras; una variedad de artificios electromecánicos y electrónicos; y de procedimientos designados para resguardar al personal, documentos, información, material, equipo y facilidades, contra el espionaje, sabotaje, acceso no autorizado y otros actos criminales tales como robos y vandalismo.

b. La Policía Militar tiene la primera responsabilidad de EM por la seguridad física. Sin embargo, el personal de CI debe establecer un enlace estrecho y efectivo con el Oficial de la PM para: - evitar duplicar esfuerzos, - definir áreas de operación y - establecer adecuados controles.

c. La aprobación o autorización a las criptofacilidades (cripto - acceso) son solicitadas inicialmente por cada dependencia que manipula información y/o documentación de SEGCOM.

d. Las inspecciones de criptofacilidades sólo se orientarán a verificar los aspectos de la protección de material y documentación clasificada.

e. Se debe tener presente que existe un grado de interrelación entre la seguridad física y la seguridad de la información, la misma que varía de actividad a actividad. Por eso formular reglas o normas rígidas y rápidas, es muy difícil sino imposible; debiéndose evaluar constantemente durante las inspecciones esta interrelación y desarrollarse efectivos procedimientos para ambas áreas de interés.

f. La eficiencia de la seguridad física se basa en el principio de "defensa en profundidad", a través del desarrollo de un sistema de controles compuesto de una variedad de partes independientes pero integradas, trabajando juntos; buscando el efecto de detener, demorar o alertar sobre el acceso no autorizado o reaccionar inmediatamente al producirse éste.

g. Uno de los objetivos de aplicar este principio es la acumulación de tiempo de demora, de manera de incrementar el riesgo de detección a tal punto que ese riesgo supere los beneficios del intento de accesar.

h. **El elemento más crucial de cualquier sistema de seguridad física es el factor humano.**

58. FINALIDAD DE LA SEGURIDAD FISICA DE COMUNICACIONES

El conjunto de medidas de seguridad física están destinadas a:

a. Proteger el material y documentación de comunicaciones contra pérdidas, captura o destrucción por el enemigo.

b. Protección del material y documentación de comunicaciones, contra inspecciones no autorizadas que puedan proporcionar informaciones sobre las características de nuestros equipos y contenido de nuestros documentos.

c. El enemigo en su afán de impedir nuestras comunicaciones, considera a los equipos de telecomunicaciones como objetivos remunerativos para su destrucción; así mismo como los documentos de comunicaciones contienen información valiosa, tratará de obtenerlas o conocerlas para deducir inteligencia importante para sus operaciones. Las medidas de seguridad física, tratará de impedir estos riesgos.

d. Impedir el acceso a los equipos de comunicaciones, otorgándoles clasificación de seguridad, para negar al enemigo información sobre las características de éstas y reducir la eficiencia de su Guerra Electrónica.

59. MEDIDAS DE SEGURIDAD FISICA EN LOS CENTROS DE COMUNICACIONES PERMANENTES

a. MEDIDAS DE SEGURIDAD FISICA DEL MATERIAL

La seguridad física del material en los centros de comunicaciones se obtiene realizando las siguientes actividades:

(1) Evitar el acceso al personal no autorizado a los lugares donde se encuentran los medios de comunicaciones.

(2) Adoptar las medidas de seguridad contra incendios, empleando alarmas, extinguidores, letreros, afiches de seguridad, instrucción al personal, etc.

(3) Preveer y adoptar las medidas de seguridad contra ataques formulando el plan de defensa de la instalación.

(4) Preveer y adoptar las medidas de seguridad contra sabotaje y fenómenos naturales, formulando los planes correspondientes.

(5) Determinar zonas de exclusión y reservadas en la instalación.

(6) Proporcionar protección y control del material de comunicaciones en forma permanente, realizando inspecciones inopinadas.

(7) Preveer y adoptar las medidas de seguridad en las estaciones

repetidoras y terminales de la red troncal de microondas, en coordinación con la empresa operadora autorizada.

(8) Ocultando, tanto como sea posible, los trabajos de tendido de líneas que entran y/o salen de la central.

(9) Evitar la densidad de las líneas alámbricas en el empleo de la instalación de los teléfonos, teletipos, facsímil, etc, utilizando de ser posible ductos o canales adecuados.

(10) Evitar hacer comentarios sobre cambio y/o reparación de los equipos de comunicaciones.

(11) Mantener un archivo eficiente y adecuado de los diferentes documentos de los Centros de Comunicaciones.

b. MEDIDAS DE SEGURIDAD FISICA DE LOS DOCUMENTOS.

La seguridad física de los documentos en los centros de comunicaciones se obtiene aplicando las siguientes medidas:

(1) Todo documento oficial, con clasificación de seguridad en especial los códigos y sistemas criptográficos deben ser accesibles solo al personal autorizado.

(2) Todos los documentos clasificados deben guardarse en muebles seguros y en un local protegido contra el acceso de personal no autorizado.

(3) Garantizar la seguridad de la documentación durante su empleo, a fin de evitar su pérdida y/o divulgación.

(4) Los mensajes transmitidos por la sección operaciones, previo registro, serán devueltos a la sección criptográfica y administrativa según el caso, para su incineración correspondiente.

(5) Al caducar la vigencia de los documentos, serán incinerados y el acta correspondiente remitida a la autoridad responsable de su formulación y distribución.

(6) En caso de pérdida, comunicar al Elón Superior para el cambio inmediato de las piezas, códigos, claves, etc.

(7) Realizar el cambio de claves de caja de seguridad en forma periódica y/o cuando se crea necesario.

(8) La caja de seguridad y archivadores, deben tener las tarjetas de prioridades y los letreros de seguridad (interior y exterior).

(9) Incinerar diariamente las cintas perforadas, después de su explotación. (Mensajes por Teletipo).

(10) Devolver a la sección criptográfica, previo registro, la cinta correspondiente o la máquina criptográfica.

(11) Está terminantemente prohibido sacar duplicados y/o copias de los documentos clasificados, tales como códigos y sistemas criptográficos.

c. MEDIDAS DE SEGURIDAD FISICA DE LAS INSTALACIONES DE LOS CENTROS DE COMUNICACIONES

(1) Evitar el acceso a la instalación, al personal no autorizado, mediante el empleo de barreras, guardias y control de acceso.

(2) Determinar las zonas de exclusión y reservadas.

(3) Realizar el mantenimiento y conservación a la instalación.
(4) Realizar y/o actualizar el estudio de seguridad cuando sea necesario.

(5) A los centros de comunicaciones "NO INGRESARAN PERSONAS QUE NO TRABAJEN EN ELLAS " y cuando sea necesario ingresarán portando las tarjetas de visita a la altura del pecho izquierdo y con la autorización del jefe de la instalación.

(6) El personal que labora en los CC/CC usará permanentemente la tarjeta de seguridad correspondiente.

(7) Deberá emplearse vigilancia en forma permanente en los C/C para impedir el ingreso a quienes no tengan la autorización respectiva.

(8) El POV de seguridad debe contemplar las medidas de preservación contra incendios, sabotaje y manipuleo del material.

(9) En situaciones de emergencia el Escalón Superior puede designar personal de tropa para la vigilancia de estaciones de comunicaciones civiles o estatales necesarias para la defensa nacional.

(10) Cuando algún visitante porte maletín o paquete, se tendrá especial cuidado que el visitante no lo deje olvidado en la instalación.

60. MEDIDAS DE SEGURIDAD FISICA EN LOS CENTROS DE COMUNICACIONES DE CAMPAÑA

a. MEDIDAS DE SEGURIDAD FISICA DEL MATERIAL

La seguridad del material, se logra mediante la aplicación de los procedimientos de disimulación y protección.

(1) La disimulación se obtiene :

(a) Ocultando tanto como sea posible, los trabajos de tendido de línea, evitando alterar el aspecto del terreno.

(b) Evitando la densidad de las líneas alámbricas que se torna visible, generalmente a la entrada de las centrales de campaña.

(c) Reglamentando convenientemente la entrada, salida e itinerario de los mensajeros.

(d) Disimulando los emplazamientos de los puestos de radio, terminales y repetidoras del sistema multicanal de área.

(e) Enmascaramiento de los vehículos, campamentos y depósitos de material.

(2) La protección del material se obtiene :

(a) Vigilando, protegiendo y controlando los medios de comunicaciones en todo momento, incluyendo eventuales inventarios por muestreo.

(b) Ejecutando trabajos de fortificación contra la observación y ataques aéreos.

(c) Manteniendo planes de emergencia de destrucción cuando su captura por el enemigo sea inminente.

(d) Dando cuenta de toda violación o intento de violación de la seguridad del material (candados, chapas, sellos, etc).

(e) Ubicando a los centinelas en lugares que tengan protección de la observación y el fuego del enemigo.

b. MEDIDAS DE SEGURIDAD FISICA DE LOS DOCUMENTOS

Las medidas de seguridad que deben tomarse para proteger los archivos, códigos, mensajes y otros documentos de comunicación son:

(1) Todo documento oficial, con la clasificación de secreto, especialmente los códigos, sistemas criptográficos y mensajes deben ser accesibles sólo al personal autorizado, seleccionándolos por su conocimiento y lealtad.

(2) Limitar al mínimo el envío de documentos de carácter secreto a la zona de combate, a fin de evitar el peligro de ser capturados.

(3) Todo documento clasificado como secreto debe guardarse en muebles seguros y en un local protegido contra el acceso de personal no autorizado.

(4) Tener un plan detallado y simple para la destrucción de los documentos secretos, cuando su captura por el enemigo sea inminente.

(5) Informar inmediatamente toda violación a la seguridad de la documentación.

(6) El POV de seguridad debe contemplar las medidas de preservación contra incendios, sabotaje y manipulación de documentación.

c. MEDIDAS DE SEGURIDAD FISICA DEL LUGAR QUE OCUPE EL CENTRO DE COMUNICACIONES

(1) Teniendo en consideración que los centros de comunicaciones tienen una conformación diferente por la diversidad de equipos que en ellos se operan, se determinará la vigilancia adecuada mediante el estudio de seguridad en la zona, lugar y/o instalación que ocupa.

(2) Cuando el personal propio de los centros de comunicaciones no es suficiente para mantener la vigilancia diurna y nocturna, se solicitará al comando el personal necesario en refuerzo, debiendo en todo caso existir un oficial de la unidad que apoya.

(3) Cuando se viva situaciones que requiera vigilancia permanente de los centros de comunicaciones el Escalón Superior puede designar personal de tropa de acuerdo a las prioridades.

(4) El personal de Oficiales, Técnicos y Sub-Oficiales que trabajan en los diferentes sistemas, serán los únicos autorizados de ingresar y/o permanecer en el centro de comunicaciones.

(5) El personal militar que desea transmitir o enviar un mensaje lo hará mediante el empleo del C/M y/o sistema telefónico.

(6) Deberán emplearse centinelas permanentes de tal manera que impida el ingreso a quienes no trabajan en el C/C.

(7) Deberán emplearse mensajeros autorizados para hacer llegar los mensajes a los destinatarios.

(8) Tener un plan detallado y simple para la destrucción del centro de comunicaciones cuando su captura por el enemigo es inminente.

(9) En los centros de comunicaciones se debe evitar la calibración de los equipos a cada momento y con demasiada potencia y/o realizar conversaciones particulares sin autorización.

d. MEDIDAS DE SEGURIDAD EN EL CAMBIO DE UBICACION DE LOS CENTROS DE COMUNICACIONES

(1) Los cambios de ubicación de los centros de comunicaciones dentro de una zona militar, deben protegerse de la divulgación del hecho.

(2) El personal será alertado para que no divulgue información de movimiento.

(3) El personal de tropa no debe conocer el movimiento, sino en el momento de iniciarse los preparativos y en la medida que se requiere para el cumplimiento de la misión.

(4) Se suspenderá la salida del personal desde el momento en que se inicia la preparación material del movimiento.

(5) Debe en lo posible simularse un ejercicio conjunto con otra unidad que permita cubrir el desplazamiento.

(6) Salvo situaciones de emergencia se podrá emplear vehículos civiles con autorización del Escalón Superior correspondiente.

(7) El itinerario del recorrido no será puesto en conocimiento del personal de tropa.

(8) Con los EECC y el personal auxiliar se tomará las medidas mßs convenientes para que no divulguen el movimiento.

(9) La responsabilidad de hacer cumplir las disposiciones de seguridad durante la ejecución del cambio de estación es del jefe de la unidad que se desplaza, si es que el movimiento se realiza por tierra; de emplearse otros medios de transporte, la responsabilidad es del jefe del medio de transporte empleado, (aire y/o agua) reasumiéndola el jefe de la unidad cuando Úste es reconstituido a tierra en una nueva ubicación.

61. SEGURIDAD FISICA DEL MATERIAL CRIPTOGRAFICO

a. La seguridad física del material criptográfico son todas las medidas de seguridad que se adopten para evitar que el material y equipo criptográfico que se emplea en comunicaciones sea accesible a personal no autorizado.

b. Inspección de Facilidades (instalaciones) Criptográficas (Criptofacilidades)

(1) Es aquella que se realiza para determinar la condición general de seguridad física de la facilidad, verificando que una criptofacilidad satisfaga los criterios de seguridad física establecidos en los manuales y directivas de seguridad.

(2) Es un proceso de análisis y evaluación que incluye la identificación de discrepancias específicas, correcciones en el sitio donde sea posible, un análisis de las discrepancias en sus ambientes y sus relaciones entre sí. incluye también una evaluación del impacto de las discrepancias sobre la protección física del material de SEGCOM.

(3) La instalación física será la inicial orientación de la inspección, posteriormente se centrará en la protección física y procedimientos de control para el material de SEGCOM dentro de la organización inspeccionada.

(4) El procedimiento mencionado en el Subpárrafo anterior será extremadamente significativo en organizaciones tácticas, donde el material de SEGCOM, especialmente las criptoclaves que constantemente salen de sus instalaciones para ser empleadas en otros lugares.

c. Responsabilidad de protección

(1) La responsabilidad directa de proteger físicamente el material criptográfico y documentación criptografiada recae tanto en el comando como en las personas que están en posición física de ejercer el control directo de seguridad.

(2) Las inspecciones a las criptofacilidades deberán efectuarse por lo menos una vez al año, por personal especialista de C-INTETE; sin embargo en cada escalón deberá existir un responsable que permanentemente está verificando que se adopten las medidas de seguridad física que eviten que el material y equipo criptográfico empleado en comunicaciones sea accesible a personal no autorizado.

d. Prevención de los riesgos de Seguridad Física del Material Criptográfico

(1) Selección adecuada del personal que debe tener cripto acceso.

(2) Tomar medidas especiales de seguridad física para evitar que los elementos criptográficos sean substraídos o capturado.

(3) Nombrar el Oficial de Seguridad Criptográfica, responsable de la protección física de los elementos criptográficos.

e. Medidas de Seguridad Física del material criptográfico

(1) Respecto al Personal

En los lugares donde se trabaja con material y equipos criptográficos, los comandos nombrarán oficiales de armas a cuyo cargo estará la responsabilidad operativa y física. Las denominaciones de estos oficiales será:

(a) Oficiales de Seguridad Criptográfica.- Son los responsables directos de la Seguridad Criptográfica y de la protección física de los elementos criptografiados, quien (es) asesorarán al comando en todo lo relacionado a criptografía.

(b) Oficial Alterno de Seguridad Criptográfica.- Es el encargado de relevar al Oficial de Seguridad Criptográfica, que por motivos justificados debe ausentarse.

(c) Oficiales de Seguridad Física.- Son los responsables de la protección física de los elementos Criptografiados y de la protección de la información.

(d) Personal Auxiliar Criptográfico (AIC).- Es el personal encargado de:

1. Cifrar y Descifrar los mensajes con información

clasificada.

2. Emplear y/o utilizar los elementos criptográficos.
3. Mantener al día los registros y archivos relacionados con su trabajo.

(2) Respecto a los Locales

(a) El ambiente donde se realizan labores de criptografía debe estar protegida contra el acceso visual del material y de las operaciones que se ejecutan.

(b) La estructura del local debe ser de una consistencia tal que evite las penetraciones físicas mediante procedimientos de fuerza.

(3) Respecto al Almacenaje

El material y equipo criptográfico debe ser guardado o almacenado preferentemente en una caja fuerte con cerradura de combinación de tipo indicador de tres posiciones. Los artículos principales de criptografía no deben ser almacenadas conjuntamente con los artículos secundarios, accesorios o instrucciones de operación que se emplean en las actividades criptográficas.

f. Control de Material Criptográfico

El control del material criptográfico estará a cargo del Oficial de Seguridad Criptográfica y directamente del personal que lo tiene afectado a su cargo.

g. Acceso a las Secciones Criptográficas

El acceso a las secciones criptográficas será solamente para el personal que labore en dicha sección y en lo posible se debe restringir al máximo el acceso al personal no autorizado.

SECCION III . SEGURIDAD CRIPTOGRAFICA

62. CONCEPTO DE SEGURIDAD CRIPTOGRAFICA (Criptoseguridad)

a. Es el componente de la Seguridad de Comunicaciones (SEGCOM) que resulta de la aplicación de sistemas criptográficos, técnicamente sólidos seguros y confiables, así como que éstos sean apropiadamente empleados.

b. Se le conceptualiza también como el conjunto de medidas y procedimientos destinados a transformar el texto de un mensaje en claro en un texto ininteligible al monitoreo del eno.

63. CONSIDERACIONES GENERALES SOBRE SEGURIDAD CRIPTOGRAFICA

a. Ninguna medida de seguridad es absoluta, partiendo de ésta premisa debemos suponer que nuestras comunicaciones serán interceptadas tanto para hacer el análisis de tráfico como para conocer o interceptar nuestros mensajes.

b. El interés del enemigo por nuestras comunicaciones tienen su origen en el concepto básico de que el comando de la unidad implica la operatividad de los hombres o comandos subordinados, lo que obliga al enlace con ellos, y a través del cual pasan todas las decisiones o informaciones existiendo una permanente preocupación por conocer éstas.

c. El conjunto de medidas destinadas a hacer ininteligibles al texto de los mensajes se agrupan en lo que se llama seguridad criptográfica y se define como los procedimientos que transforma el texto claro de un mensaje en un texto enigmático, a fin de dar seguridad a las comunicaciones.

d. Todos los ejércitos, mantienen en sus sistemas de inteligencia un servicio de análisis de tráfico y criptoanálisis dedicados a la traducción de mensajes criptografiados que emplean diversos medios y elementos que se

complementan entre sí, constituyendo un poderoso órgano de obtención de informaciones.

e. Conociendo que la información que brinda el criptoanálisis de tráfico, es precisa segura y oportuna; obliga a que la actividad criptoanalítica sea continua, profunda y se intensifique cada vez más en su acción.

f. La historia ha demostrado que un Ejto que cuente con un organismo capaz de descriptografiar la correspondencia, es dueño de la situación; por ello corresponde negar toda información adoptando mayores seguridades, entablando una lucha constante entre los que envían los mensajes y quienes tratan de conocer el texto.

64. FINALIDAD DE LA SEGURIDAD CRIPTOGRAFICA

La Seguridad Criptográfica tiene por finalidad establecer las normas y procedimientos a fin de impedir y/o evitar que el enemigo o países interesados obtengan y/o neutralicen nuestras informaciones, interceptando nuestras comunicaciones mediante el uso de sistemas criptográficos.

65. SISTEMA CRIPTOGRAFICO

Es el conjunto de medios, técnica, procedimientos y medidas de control adaptados para proporcionar la seguridad criptográfica. Todo sistema criptográfico tiene riesgos que deben neutralizarse a fin de garantizar una adecuada Seguridad criptográfica:

a. Riesgos de la Seguridad Criptográfica

(1) **Cripto acceso**
El cripto acceso es el riesgo de la seguridad criptográfica que resulta del acceso que pudieran tener personal no autorizado a los elementos que constituyen el Sistema Criptográfico del Ejército.

(2) **Criptoanálisis**
Es el riesgo de la seguridad criptográfica mediante el cual, personal no autorizado realiza descriptados de los mensajes cifrados, obtenidos mediante la interpretación, sustracción o captura, reconstruyendo los procedimientos utilizados de un determinado sistema critográfico.

b. Medidas de Control de Seguridad Criptográfica

Son las medidas que se toman para neutralizar los riesgos que amenazan la seguridad criptográfica. Se clasifican en:

(1) Medidas de Control de Cripto Acceso
   (a) Adopción de procedimientos para otorgar la autorización de cripto acceso.
   (b) Control al personal con autorización de cripto acceso.

(2) Medidas de Negación al Cripto Análisis

   (a) Selección de Sistemas criptográficos ágiles y seguros

   (b) Adopción de procedimientos apropiados para la tramitación de mensajes criptográficos

   (c) Adopción de medidas de control físico

66. TECNICAS PARA ASEGURAR LA SEGURIDAD CRIPTOGRAFICA

a. Selección de Métodos de Criptografiado

(1) Transposición.- Consiste en la alteración del orden natural de los símbolos de un texto claro, mediante una "clave" o principio convencional, de cuyo empleo resulta un texto ilegible.

(2) Sustitución .- Consiste en reemplazar los símbolos del mensaje claro por otros preestablecidos, lo que da como resultado un texto ilegible.

(3) Equivalencia.- Consiste en el reemplazo de palabras o frases mediante códigos preestablecidos; el texto resultante es ilegible y breve.

(4) Automática.- Es el sistema mediante el cual el procedimiento de criptografiado se realiza utilizando equipos electrónicos especiales. El texto resultante queda agrupado e ilegible.

b. Combinación de los Métodos de Criptografiado

(1) Los Comandos disponen la selección del método apropiado de cifrado; puede emplearse una combinación de métodos para un doble cifrado de los mensajes proporcionándoles mayor margen de

seguridad, si bien significa mayor dificultad, proporcionan una mayor protección a las posibilidades de criptoanálisis.

(2) Es necesario elegir la mejor técnica; teniendo presente que no siempre la más difícil es la mejor. El procedimiento elegido debe ser sencillo, rápido, aunque difícil para el cripto-analista; y, desde luego aplicable a las comunicaciones alámbricas y radioeléctricas.

67. SISTEMA DE CODIGO

a. Concepto

(1) Un sistema de código es una forma de sustitución de más o menos alta especialización. El principio básico en que se apoyan los sistemas por sustitución es el reemplazo de las letras, cifras o símbolos.

(2) A veces se aplica el procedimiento de sustitución a grupo de letras y cuando se hace esto, los grupos son por lo común, de longitud determinada uniforme. En los sistemas que emplean cifras, las palabras a las cuales se aplica el tratamiento criptográfico, son las más pequeñas de las que se puede componer el texto claro.

(3) El principio básico en que se apoyan los sistemas de código es el reemplazo de palabras enteras, frases u oraciones completas que constituyen el texto claro del mensaje, con equivalentes escogidos arbitrariamente y que tienen poca o ninguna relación con los elementos que reemplazan. Estos equivalentes pueden ser otras palabras, grupos de letras, de cifras o combinaciones de éstas. Excepcionalmente se aplica el procedimiento de reemplazo o sustituciones a elementos más pequeños que palabras enteras, y cuando se hace esto, los elementos son letras aisladas, grupos de letras o símbolos.

(4) En los sistemas de código las palabras a las cuales se aplica el tratamiento criptográfico son conjuntos pequeños, tales como letras individuales combinadas en varios grupos de longitud irregular; es decir, palabras, frases u oraciones.

b. Interpretación del código

Esta expresión se aplica al criptografiado y descriptografiado de mensajes mediante un código. Para poner en claro un mensaje en código, el operador sustituye los equivalentes del código por las varias palabras, frases, oraciones y números del texto claro.

c. Estructura de un código

Los elementos de que se componen los grupos de código pueden ser de uno o más de los tipos siguientes:

(1) Palabras reales sacadas de uno o más idiomas.
(2) Palabras artificiales o grupo de letras que no tienen un significado verdadero y que se construyen más o menos sistemáticamente, colocando las vocales y las consonantes de tal modo que estas agrupaciones tengan apariencia y pronunciabilidad de palabras reales.

(3) Grupo de letras

(4) Grupo de números arábigos.

d. Código cifrado

Es aquel mensaje en código al cual se le aplica alguna técnica o método criptográfico. Es conveniente emplear este procedimiento cuando:

(1) El código básico se ha distribuido a un grupo muy numeroso de personas y hay riesgo de que el mensaje caiga en manos de personas no autorizadas.

(2) Hay que aumentar la seguridad de las comunicaciones estrictamente secretas.

68. CRIPTOGRAFIADO DE MENSAJES

a. Determinación de los mensajes que serán criptografiados

(1) Mensajes cifrados

(a) Los mensajes operacionales y administrativos clasificados ESTRICTAMENTE SECRETO Y SECRETO.

(b) Los mensajes CONFIDENCIALES que por su contenido merecen protección especial.

(2) Mensajes codificados

(a) Los mensajes operacionales y administrativos de acción

inmediata, en tiempo de guerra o ejercicios de guerra.

(b) Los mensajes operacionales y administrativos cuando los equipos de cifrado han quedado fuera de servicio.

b. Determinación de los mensajes que no serán criptografiados

(1) Los mensajes operacionales y administrativos Clasificados CONFIDENCIAL, RESERVADO, Y COMUN.

(2) Los mensajes operacionales ESTRICTAMENTE SECRETO y SECRETO, de extrema urgencia y que no haya tiempo para criptografiar, en guerra o ejercicios de guerra siempre que el mensaje sea de aplicación inmediata y no tenga repercusión para las operaciones.

(3) Estos mensajes, para ser transmitidos deben tener texto breve.

c. Trámite de Mensajes Clasificados en Texto claro

(1) Cada transmisión irá precedida de una autenticación de comunicaciones.

(2) Los mensajes transmitidos y recibidos llevarán un sello de "Transmisión en Texto Claro" y "Recibido en Texto Claro" respectivamente.

(3) La transmisión deberá efectuarse en el menor tiempo posible.

69. REGLAS FUNDAMENTALES DE SEGURIDAD CRIPTOGRAFICA

a. El incumplimiento de las reglas fundamentales de Seguridad Criptográfica facilita la labor de los analistas Criptográficos.

b. Las reglas que se mencionan son tanto para los expedidores de mensajes como para el personal criptográfico.

c. Dar instrucciones detalladas para los expedidores de mensajes, está fuera de alcance de este manual, sin embargo, es conveniente tener presente las siguientes recomendaciones:

(1) Se debe evitar las frases hechas especialmente al principio y al fin de un mensaje. La existencia de frases hechas, constituyen bases de muchos métodos empleados en el criptoanálisis. Realmente en

algunos casos el único método de solución posible es utilizar la existencia de frases hechas.

Toda clase de informes rutinarios se deben enviar por otros medios de comunicaciones que no sean susceptibles de interceptación.

(2) Se debe tener bastante cuidado en que los mensajes sean claros y concisos. Si un mensaje es ambiguo o incompleto, da por resultado una confusión innecesaria y pone en duda la exactitud de la operación criptográfica.

(3) Los mensajes se deben reducir mediante la supresión de palabras innecesarias. Se deben reducir al mínimo las conjunciones, preposiciones repetición de palabras y especialmente la puntuación. Cuando es necesaria la puntuación, esta se debe deletrear íntegramente o en forma abreviada.

Los números también se deben de deletrear. En los casos en que se tenga que usar letras del alfabeto como ocurren con ciertos símbolos que identifican cierto tipo de equipo, conviene representar estas letras mediante sus equivalencias fonéticas autorizadas.

(4) Siempre que sea factible, se deben usar las abreviaturas autorizadas.

(5) Se deben observar cuidadosamente las reglas (que rigen las clasificaciones) respecto a la manera de indicar las direcciones y formas .

(6) Se deben observar en todo momento, las reglas que rigen las clasificaciones de seguridad, a saber, SECRETO, CONFIDENCIAL, RESERVADO .

d. Gran parte del éxito que corona los esfuerzos de los analistas criptográficos se debe a la ignorancia o descuido de parte del personal criptográfico, rara vez los errores criptográficos graves son el resultado de infracciones voluntarias de las instrucciones, pero si el personal criptográfico se da cuenta de que el descuido y la ignorancia pone en peligro su propia vida y la de miles de compañeros de armas, prestará más atención a las reglas que se han establecido para servirles de guía. Las más importantes son:

(a) **Mensajes dudosos.-** No criptografiar nunca un mensaje que en opinión del criptografista, no está de acuerdo con lo convenido o con los reglamentos respecto a la redacción de mensajes hasta no haber consultado y obtenido la aprobación de alguien que tenga la autoridad para alterar el mensaje.

(b) **Mezcla de texto claro y texto criptografiado.-** No permitir nunca que el texto criptografiado aparezca en un criptograma junto con su

equivalencia en lenguaje claro o no mezclar texto criptografiado y claro excepto en los mensajes en que tales mezclas se permiten específicamente.
Esta mezcla incluye puntuación y abreviaturas de toda clase, semejantes mensajes proporcionan al enemigo indicios de gran valor; si un mensaje se ha de criptografiar parte de él, se debe criptografiar completamente.

(c) Texto de los mensajes.-

1. No repetir nunca en el texto claro el mismo texto de un mensaje que ya se haya enviado en forma criptografiada ni repetir en forma criptografiada el texto de un mensaje que haya sido enviado en forma clara .
Cualquier cosa que, a un enemigo alerta le permite comparar un trozo determinado de texto claro con un criptograma que se supone contiene este mismo texto claro, es sumamente peligroso para la seguridad del sistema criptográfico. En las situaciones en que se tenga que publicar información o en los casos en que muchas personas han intervenido en la transmisión de la información, la versión en texto claro se debe parafrasear muy cuidadosamente antes de la publicación, para reducir al mínimo los datos que un enemigo pudiera obtener de una comprobación exacta de texto criptografiado con el texto claro original equivalente.

2 Parafrasear un mensaje quiere decir, que este se vuelve a escribir de modo que se cambie lo más posible de la redacción original sin cambiar el sentido del mensaje. Esto se hace alterando la posición del sujeto, predicado y frases o cláusulas movidas en la oración y alterando lo más posible el lenguaje mediante el empleo de sinónimos o frases sinónimos. En esta operación se refiere la supresión a la ampliación del lenguaje del mensaje, porque si al parafrasear un mensaje ordinario este se extiende siguiendo el plan original un perito puede muy fácilmente reducir a sus expresiones más cortas el mensaje original. De ser posible, es muy importante eliminar las palabras repetidas y los nombres propios mediante el empleo de pronombres cuidadosamente escogidos; o utilizando las palabras "este", "aquel", "el mismo", "el antedicho" o "por los medios".
Después de parafrasearlo cuidadosamente, se puede transmitir el mensaje en otra clave o en otro código .

3. No envíe nunca el texto claro literal ni una versión parafraseada de un mensaje que se ha transmitido o se transmitirá en forma criptografiada.

4. No repetir nunca en diferente clave o sistema sin parafrasearlo, mensaje alguno criptografiado que se haya transmitido, a menos que lo autorice específicamente la autoridad corrrespondiente.

5. No transmitir nunca una clave de cifra nueva por medio de un mensaje criptografiado en una clave anticuada.

6. No poner nunca direcciones ni firmas criptografiadas al principio ni al fin de un texto criptografiado. Se debe esconderlas en el cuerpo del mensaje.

7. Incluir en la dirección de un mensaje criptografiado únicamente el mínimo de información necesaria para que el mensaje llegue al destinatario al cual va dirigido.

8. No contestar en lenguaje claro a ningún mensaje criptografiado.

9. No emplear nunca títulos abreviados como indicadores de mensajes criptografiados.

10. No emplear nunca letras de relleno a menos que se autorice específicamente su utilización.

11. No cifrar nunca ni poner en código ni disfrazar de ninguna manera el indicador de sistema a menos que esto se haya autorizado específicamente.

12. No poner nunca en la copia de un mensaje ninguna anotación respecto del sistema o acerca del asunto que trata el mensaje.

13. No archivar nunca mensajes criptografiados junto con sus equivalentes en texto claro, hay que destruir las hojas quemándolas.

14. Se debe comprobar, siempre que sea factible, la exactitud de los mensajes criptografiados antes de transmitirlos. Esta operación la debe efectuar un especialista que no sea el que criptografió inicialmente el mensaje.

70. GRADO DE SEGURIDAD CRIPTOGRAFICA DE UN SISTEMA

a. El grado de seguridad depende de lo cabal que sea el sistema en sí desde el punto de vista técnico. Esto a su vez determina la resistencia al análisis que ofrece el sistema.

b. El sistema criptográfico ideal para fines militares sería un sistema único e idóneo, para adaptarlo al empleo no sólo de los escalones mayores sino también a los elementos más pequeños presentes en la zona de combate, que además proporcionará un grado tan grande de seguridad criptográfica que por mucho tráfico disponible que hubiera y todos ellos en la misma clave, los criptogramas de este tráfico, resisten a la solución indefinidamente.

c. El mínimo grado que se puede ser, es que la seguridad criptográfica sea lo bastante alta para retardar su solución por el eno o por un tiempo suficiente para que cuando al fin se resuelva la información obtenida de esta manera haya perdido su valor inmediato táctico y mucho de su valor estratégico.

71. FACTORES FUNDAMENTALES EN EL ESTABLECIMIENTO DE UN SISTEMA CRIPTOGRAFICO

a. Los factores fundamentales en el orden de importancia relativa son:

(1) Confiabilidad
(2) Seguridad
(3) Rapidez
(4) Flexibilidad
(5) Economía

b. **La confiabilidad es de primera importancia.-** Confiabilidad, al aplicarse a un sistema o dispositivo criptográfico, quiere decir, que los criptogramas que producen la sección criptográfica de origen se pueden descriptografiar rápidamente, con exactitud y sin ambigüedad en la sección criptográfica receptora; que el sistema criptográfico, ya sea libro o máquina o dispositivo está a mano y en buenas condiciones de utilización para poder servirse de él en cualquier momento; y que al utilizarlo se pueda confiar en que sirve mientras se necesite. La confiabilidad implica sencillez; por lo general mientras más sencillo sea el sistema tanto más confiable es.

c. **Seguridad.-** es la protección que proporciona un sistema criptográfico cabal.

d. **La rapidez.-** es la celebridad con que se pueden criptografiar o descriptografiar los mensajes, generalmente se expresa en palabras o

grupos de cinco letras por minuto. Los requisitos expuestos de seguridad y rapidez varía según las circunstancias.
El personal de comunicaciones se debe regir por principios generales, subordinado a las condiciones del momento, más bien que por reglamento. La seguridad máxima en todo momento debe ser la meta, pero en mensajes que se envían entre sí las Comandancias Generales, se puede sacrificar un poco de rapidez para satisfacer mayores requisitos de seguridad, mientras que en un mensaje que se envían entre sí los Comandos Subordinados, la seguridad queda subordinada a los mayores requisitos de la rapidez. Por esta razón es preciso disponer de varios sistemas criptográficos para hacer frente a diversos tipos de situación.

e. **La flexibilidad.**- consiste en que un sistema criptográfico, puede ser reemplazado inmediatamente por otro sistema criptográfico.

f. **La Economía.-** Significa que mientras más sencillas sean las opns implicadas, más cortos serán los criptogramas producidos, menos el tiempo que se requiera para producir el material criptográfico a emplearse, así como la trasmisión de los mensajes, consiguiendo de esta manera economía en el trabajo criptográfico.

72. REQUISITOS ESPECIFICOS QUE DEBE SATISFACER UN SISTEMA CRIPTOGRAFICO PARA USO MILITAR EN GENERAL

a. Los criptogramas deben estar en forma apropiada para transmitirse mediante equipos y métodos telegráficos corrientes:

(1) Este requisito generalmente elimina todos los sistemas menos los que producen criptogramas hechos de caracteres que se trasmiten fácilmente mediante un sistema telegráfico que emplea el alfabeto Morse o el alfabeto del teletipo.

(2) Los sistemas criptográficos en que se usan guarismos no son tan convenientes como los que emplean letras porque las Telemática de los números arábigos en el sistema morse, son mas largos y para el Operador corriente, ya sea telegrafía o radiotelegrafía, son más difíciles de trasmitir que recibir.

(3) Los sistemas que producen criptogramas hechos de mezclas de letras y guarismos o letras, guarismos y signos de puntuación y que debe trasmitirse mediante el código morse no son a propósito para uso práctico. Sin embargo se permite emplearlo en los casos en que estas combinaciones se producen automáticamente mediante el mecanismo criptográfico y se trasmiten, reciben y descifran como se

hace en ciertos sistemas de cifrado por teletipo.

(4) Por ser apropiado para comunicación económica por Código Morse el texto criptografiado debe ser idóneo para poder arreglarlos en grupos uniformes de caracteres por las razones siguientes:

(a) En primer lugar, contribuye a la exactitud de la trasmisión telegráfica, pues el operador sabe que puede recibir un número determinado de caracteres en cada grupo, ni uno más ni uno menos.

(b) En segundo lugar generalmente dificulta aún más el criptoanálisis cuando no es extensa la longitud de las palabras, frases y oraciones del texto claro. Por lo general los grupos se componen de cinco caracteres, aunque de vez en cuando, en circunstancias especiales se pueden emplear otras agrupaciones. En los sistemas de cifrado por teletipo no hay que agrupar los caracteres de este modo.

b. Los canales ordinarios de comunicaciones sólo pueden atender un volumen de trafico limitado:

(1) Para su funcionamiento más eficiente es indispensable que se trasmitan el mínimo de caracteres verdaderamente necesarios para comunicar un mensaje determinado. Por consiguiente, el texto criptográfico no debe ser más largo que su texto equivalente.

(2) En un caso excepcional, el texto criptográfico puede ser más largo que el texto claro equivalente, pero un sistema en que el texto criptográfico, sea dos veces más largo que el texto equivalente es útil únicamente si tiene mérito sobresaliente; esto es, apropiado para cierto uso restringido o especial.

(3) Ningún sistema en que la longitud del texto criptográfico sea más largo del doble de la del texto claro es práctico para uso militar. La mayor parte de los sistemas criptográficos de uso corriente producen criptogramas cuya longitud es proporcional a la del mensaje original en texto claro o un poco más corto.

c. Los requisitos generales de confiabilidad y rapidez consisten en que las operaciones de criptografiar sean relativamente sencillas y rápidas.

(1) Dichas opns se pueden efectuar en condiciones difíciles en campaña y no deben requerir que se recuerde y aplique una serie larga de pasos o reglas, de otro modo, no sirve para opns. en la zona de

combate.

(2) Deben ser tales que reduzcan a un mínimo el esfuerzo mental del Operador o Especialista. Aquellos procedimientos complejos que requieren varios pasos distintos no son apropiados para el uso en la zona de combate, pero de vez en cuando los sistemas que no requieren más de dos pasos pueden servir para fines militares si cada uno de dichos pasos es sencillo y rápido.

d. Los dispositivos o instrumentos de cifrar en campa±a deben ser de poco peso, de construcción resistente y de funcionamiento sencillo que no requiera más de un operador. Los requisitos que han de satisfacer las máquinas cifradoras de alta velocidad que se emplean en las Comandancias Superiores son muy complejas para describirlas en un documento como este.

e. El sistema debe ser tal que los Especialistas Criptográficos puedan corregir fácil y rápidamente errores, lo que ocurre constantemente en comunicaciones criptográficas. Un sistema es inútil, si hay que pedir con frecuencia que se repita la trasmisión entera.

f. Los actuales sistemas o máquinas criptográficas en uso en el Ejército están descritas en los manuales de operación y mantenimiento; así como las normas y procedimientos de empleo, en las directivas e instrucciones emanadas o emitidas por la DINTE.

SECCION IV. SEGURIDAD DE TRASMISION

73. CONCEPTO DE SEGURIDAD DE TRASMISION (SEGTRAS)

a. Es el componente de la SEGCOM, destinado a proteger la trasmisión

durante el funcionamiento de los medios de telecomunicaciones de la interceptación, análisis de tráfico y contramedidas electrónicas (perturbación y engaño imitativo particularmente) que el eno podría efectuar con medios que no sean de criptoanálisis.

b. De una manera general la SEGTRAS incluye:

(1) Empleo exclusivo de procedimientos de operación autorizados en las redes radiotelefónicas, en especial el cambio frecuente de indicativos, frecuencias y operadores.
(2) Mantenimiento de la disciplina de red en todo momento.
(3) El empleo de procedimientos de autenticación
(4) El empleo de codificadores de voz
(5) Encriptar toda información clasificada y/o sensible antes de trasmitirla.
(6) Empleo de radio y del teléfono únicamente para asuntos oficiales y el mantenimiento de todas las conversaciones (trasmisiones) tan breves como sea posible.
(7) Enmascaramiento del lugar de trasmisión
(8) Empleo de cargas de antena falsa cuando se prueba.
(9) Establecimiento de bajas potencias (control de potencia) y antenas direccionales.

74. MEDIDAS GENERALES DE SEGTRAS CONTRA LA INTERCEPTACION

a. Generalidades

(1) La interceptación enemiga, es la actividad que realiza con la finalidad de escuchar y/o grabar las comunicaciones que se efectúan en nuestras redes, con el propósito de obtener informaciones.

(2) Todo Comandante, Oficial de Comunicaciones, operadores y cualquiera que se valga de las Comunicaciones, para trasmitir ordenes, efectuar coordinaciones, proporcionar informaciones, etc: debe comprender claramente la susceptibilidad de éstas a la interceptación.

(3) La extrema vulnerabilidad de las comunicaciones por radio las hace el blanco primordial de la INTETE y GE enemiga (MAGE). Generalmente la distancia no será problema para el eno en la interceptación por radio; lo único que se requerirá será un local apropiado, un vehículo debidamente acondicionado para la recepción de las Telemática emanadas y suficiente personal entrenado para la interceptación, el análisis del tráfico y la compilación de la información

militar resultante.

(4) Las comunicaciones alámbricas no están libres de la interceptación, aunque será más difícil efectuarla. Sin embargo el diseñador de la red y el operador deben conocer, si el teléfono está conectado en algún punto a un circuito de radio (integración radioalámbrica: IRA); de ser así a dicho circuito se le debe tratar como una red radial en lo que se refiere a la SEG TRAS.

b. Análisis de tráfico

(1) El análisis de tráfico es la actividad que consiste en interceptar las comunicaciones, estudiar su naturaleza, destinatario, promotor y contenido del mensaje que se trasmite o recibe, a fin de obtener información militar sin necesidad de recurrir al criptoanálisis.

(2) En términos generales, el análisis del tráfico es la captación y estudio minucioso de las comunicaciones a fin de penetrar en el "enmascaramiento" superpuesto a las redes de comunicaciones, mediante el estudio de:

(a) Volumen, dirección y curso de los mensajes.
(b) Frecuencia y horario de trasmisión empleado entre y dentro de las redes.
(c) Direcciones de las emisiones mediante la radiogonometría (radiolocalización).
(d) Sistema de asignación y cambios de indicativos de llamada.
(e) Ubicación geográfica de los trasmisores por procedimientos técnicos.
(f) Detalles de conversaciones entre los operadores que utilizan los equipos.

c. Monitoreo de SEGCOM

(1) Es una función del apoyo de la Seguridad de Trasmisión; y se le define como la escucha, la reproducción o el grabado, por cualquier medio, del contenido de las telecomunicaciones amigas; para proporcionar material para el análisis que permita determinar el grado de seguridad que proveen esas comunicaciones, al análisis de tráfico enemigo u opns de INTETE enemigas.

(2) En el pasado se consideraba al Monitoreo de SEGCOM como una técnica de vigilancia, pero debido a que el número de redes de radio con canales de voz que se pueden establecer en una zona de opns es ahora muy grande; y, que normalmente la cantidad de equipos de

monitoreo de que podrían disponer las Unidades de Comunicaciones (o Sub-Unidades de GE) son limitados; este monitoreo sólo proporcionaría una muestra limitada de las comunicaciones, deviniendo por ende en una medida inefectiva; al menos que haya sido bien planeada para cumplir un propósito específico.

(3) La necesidad del Monitoreo de SEGCOM será mejor determinado, si ésta proviene de un preciso análisis o de evaluación de la amenaza. Sin embargo, el monitoreo tendrá aún un propósito válido, cuando sea el único método para obtener datos requeridos para el estudio del tráfico de Comunicaciones (Análisis de tráfico). Por ejemplo, puede ser el mejor método para verificar lo adecuado de un programa de entrenamiento de SEGUTE o para determinar la efectividad de las COCOME.

(4) El monitoreo de SEGCOM juega un rol importante en el desarrollo de la base de datos necesario para planear y ejecutar exitosamente una protección electromagnética y/o una operación de engaño electrónico.

75. MEDIDAS ESPECIFICAS DE SEGTRAS CONTRA LA INTERPRETACION

a. Para adoptar las medidas específicas contra la interceptación, adecuadas a nuestra disponibilidad de personal y material, es necesario primero evaluar la situación en función de los siguientes factores: Posibilidades del enemigo y vulnerabilidad de nuestro sistema de comunicaciones.

b. <u>Posibilidades del enemigo</u>

(1) Para conocer las posibilidades que el enemigo tiene para interceptar nuestras trasmisiones se requiere disponer de una amplia información técnica, precisa y detallada sobre sus sistemas interceptores.

(2) Esta información fruto del análisis del material capturado, de los reconocimientos a sus emplazamientos y de las infiltraciones a sus instalaciones; deben referirse fundamentalmente a los siguientes aspectos:

(a) Unidades de interceptación con que cuenta.
(b) Dispositivos de las Unidades de interceptación.
(c) Organización de cada una de ellas.
(d) Características técnicas de sus equipos.
(e) Características de sus operaciones.
(f) Elementos de comunicaciones que constituyen sus

operaciones especiales.

c. <u>Vulnerabilidad de nuestro Sistema de Comunicaciones</u>

(1) La Vulnerabilidad de nuestro sistema puede deberse a:

- Los equipos de comunicaciones.
- El personal que lo opera
- La situación táctica.

(2) <u>Equipo de Comunicaciones</u>

(a) Los medios alámbricos pueden ser interceptados en toda su estructura por personal infiltrado o especialista, si la información es llevada por pulsos o por ondas portadoras.

(b) Los equipos radioeléctricos son extremadamente vulnerables a la interceptación, por la cual la seguridad de trasmisión será una consideración constante cuando se esta empleando el sistema radioeléctrico. El enemigo obtiene información militar, por medio del análisis del tráfico.

(c) Los mensajeros pueden ser interceptados por infiltrados o por ingreso equivocado a posiciones enemigas.

(3) <u>Personal Operador</u>

El personal operador facilita la actividad de interceptación del enemigo cuando no está capacitado para explotar las posibilidades del equipo a su cargo, o no mantiene la disciplina de operación y tráfico de comunicaciones.

(4) <u>Situación Táctica</u>

(a) En los establecimientos la situación de escasa visibilidad facilita la acción de los infiltrados sobre nuestros medios alámbricos o mensajeros, en este último caso, más aún si se extravían.

(b) El ataque es la fase de las operaciones en que las comunicaciones son más susceptibles a la interceptación; la velocidad de las operaciones pueden permitir que la seguridad contra la interceptación sea un factor secundario.

(c) Control de las Comunicaciones

1. Esta actividad debe ser permanente e integral cualquiera que sea la situación en que se encuentra, preferentemente durante y después de fases críticas o prolongadas de combate en las que puedan quedar afectadas la moral del personal.

2. Teniendo en cuenta la amplitud de los sistemas de comunicaciones de las grandes unidades será necesario organizar elementos con responsabilidad exclusiva del control de las comunicaciones dotándolos de personal y equipos para controlar cualquier medio y en cualquier parte de la zona de operaciones.

d. Seguridad contra la interceptación de los medios radioeléctricos

(1) Los medios radioeléctricos son extremadamente vulnerables a la interceptación; por consiguiente, deben recibir especial énfasis todos los planes y adiestramientos de seguridad de Comunicaciones orientados a los usuarios y operadores de los equipos de radio.

(2) Esta vulnerabilidad de los medios radioeléctricos los convierte en objetivo principal de los órganos de búsqueda electrónica del enemigo, los mismos que obtienen información militar por medio de análisis de tráfico de comunicaciones.

(3) Para lograr una mayor sorpresa táctica mediante la negación de la información militar de tráfico de comunicaciones, se puede ordenar el radio-silencio o el empleo restringido.

(a) En el radio-silencio todas las emisiones están prohibidas, pero los puestos deben estar en escucha y listos para funcionar; debe indicarse, tanto las redes que deben mantenerse en radio-silencio, como la hora de término.

(b) En el empleo restringido, están autorizados solamente las emisiones para el control de funcionamiento de los puestos y asimismo, se puede realizar trasmisiones de mensajes sólo cuando no existe otro medio.

(4) Otras medidas a adoptarse para dar seguridad a las comunicaciones radioeléctricas son:

(a) Empleo de radio telegrafía en lugar de radio telefonía cuando ambas pueden usarse indistintamente.

(b) Mantener la disciplina de tráfico, que puede comprender el respecto de todas las preescripciones existentes en la lOCE, Ordenes de Operaciones y otros documentos especialmente en los siguientes aspectos:

(a) Horario de tráfico.
(b) Frecuencias e indicativos.
(c) Autenticación de puestos y mensaje.
(d) Procedimientos criptográficos
(e) Radio silencio y empleo restringido.
(f) Procedimientos de explotación.
(g) Procedimiento de integración radioeléctrica, radio relevo y control remoto.

(c) No se debe violar el radio silencio ordenado.

(d) Evitar las particularidades personales de los mensajes.

(e) Restringir toda trasmisión al mínimo.

(f) Evitar trasmisiones innecesarias y pruebas excesivas.

(g) Operar con el mínimo de potencia radiada, que satisfaga la comunicación (Control de Potencia).

e. Seguridad contra la Interceptación de los Medios Alámbricos

(1) Las comunicaciones alámbricas son consideradas como más seguras que las comunicaciones por radio; pero esto es debido a que la interceptación de las comunicaciones radioeléctricas es mucho más fácil, no porque las líneas o circuitos alámbricos están libres de interceptación.

(2) Para la seguridad de su empleo deben adoptarse las medidas de seguridad establecidas en el párrafo "78.b".

f. Seguridad Contra la Interceptación de los Medios Opticos

La seguridad se obtiene mediante una buena ubicación de los medios ópticos que impida al enemigo percibir nuestras Telemática y que nos

permita a la vez comunicaciones rápidas y seguras por medio del empleo de banderines y semáforos. Algunas medidas son:

(1) Utilizar solamente las Telemática autorizadas.

(2) Hacer el despliegue de los paineles sólo cuando se tenga seguridad de la autenticidad de las aeronaves.

76. CODIFICACION DE VOZ (SEGURIDAD CRIPTOFONICA)

a. Antecedentes

(1) En el pasado, la manera de hacer ininteligible la voz trasmitida por líneas físicas o redes radioeléctrica, era empleando dispositivos electrónicos denominados INVERSORES DE VOZ. Estos dispositivos sin embargo no brindaban el grado de seguridad requerido, debido a que lo ·nico que hacÝan era variar el orden regular de las frecuencias de las sílabas que conforman una palabra o invertían las frecuencias simples o scrambers de código rotatorio.

(2) En la actualidad existe el cifrado de voz de alta seguridad en conversaciones trasmitidas a lo largo de canales ordinarios de voz, superando largamente la naturaleza del sistema de codificación de voz brindado por los scrambers, empleando mejores técnicas que mezclan frecuencia y tiempo. Tanto la introducción y generación de la clave, como el proceso de cifrado de la información hablada, están totalmente digitalizadas y solamente a la salida, la señal codificada/cifrada de voz queda reconvertida en una señal analógica adecuada para su trasmisión a lo largo de cualquier tipo de medio. El algoritmo de codificación o repetición de señal codificada es muy alto para que un equipo interceptor pueda descifrarlo en tiempo real o su descodificación demorará tanto, que hará inútil la información obtenida.

b. Finalidad

La seguridad criptofónica tiene por finalidad establecer las normas y procedimientos que impidan y/o eviten que potenciales enemigos obtengan y/o neutralicen nuestras informaciones, interceptando nuestros enlaces o introduciéndose a las redes con engaño electrónico. Esto se realiza mediante el empleo de sistemas criptofónicos apropiados.

c. Equipos de Criptofonía

Existen una variedad de equipos de criptofonía denominados CODIFICADORES DE VOZ, la inmensa mayoría son digitalizadas. La selección del más adecuado dependerá de las disponibilidades económicas, grado de seguridad requerido y situación táctica.

77. SEGURIDAD DE TRASMISION EN EL SISTEMA DE COMUNICACIONES PERMANENTE

a. Red Telefónica de larga distancia (Teléfono Rojo)

(1) El Teléfono Rojo debe ser atendido personalmente por la autoridad a quien se ha dotado de este medio o su representante autorizado.

(2) El teléfono Rojo instalado en las Oficinas de los Oficiales de Seguridad y/o permanencia, debe ser atendido personalmente por los Oficiales de Servicio, quienes deben de llevar un registro de llamadas. En caso de emergencia debidamente justificados, podrán ser atendidos por quién lo represente temporalmente.

(3) Está terminantemente prohibido emplear este medio para tratar asuntos clasificados como SECRETO O ESTRICTAMENTE SECRETO, si no se dispone del correspondiente sistema de Seguridad Criptofónico.

(4) Se prohibe el empleo de este medio por personas no autorizadas.

(5) Está prohibido realizar cualquier tipo de derivaciones de los abonados de esta red, así como integración a las redes de telefonía civil, telefonía automática local y las de integración radio telefónica (PHONE PATCH).

(6) Los usuarios del Teléfono Rojo, deben identificarse mutuamente antes de intercambiar informaciones.

b. Red de Telefonía Automática Local

(1) El empleo de este medio, debe circunscribirse solo a los asuntos del servicio que no sean de carácter clasificado.

(2) La recepción del Facsigrama clasificado debe realizarla el destinatario o representante autorizado.

c. Facsímil

(a) Para la trasmisión de documentos clasificados, el promotor o su

representante autorizado, se apersonará al C/C de la Unidad respectiva para la trasmisión del documento.

(b) La recepción del Facsigrama de las RRMM y GGUU debe realizarla un elemento de inteligencia, cuando estos son cursados por la DINTE o el SIE.

d. <u>Red Telegráfica</u>

(1) Todos los elementos de clasificación SECRETO o ESTRICTAMENTE SECRETO, deben de transmitirse en clave.

(2) La autorización para tramitar un mensaje en claro o en clave, debe darla el promotor de mensaje.

e. <u>Red de Comunicaciones Estratégica (Alterna)</u>

(1) Durante el funcionamiento de esta red deben emplearse los Cuadros de Indicativos, Frecuencias, Códigos y Sistemas de Autenticación, que contiene las Instrucciones Operativas de Comunicaciones y Electrónicas y las Instrucciones Permanentes de Comunicaciones y Electrónicas (IOCE e IPCE).

(2) Deben emplearse los procedimientos de explotación en el MACOFA.
(3) Está terminantemente prohibido establecer conversaciones particulares, entre operadores y tomar contacto con estaciones que no PERTENECEN a la red.

(4) Toda comunicación debe ser transmitida con autorización del Comando respectivo, y siguiendo los procedimientos establecidos para su trasmisión.

(5) Debe extremarse las medidas de autocontrol durante la explotación de este medio a fin de evitar la infidencia e indiscresiones tales como no emplear los autenticadores, trasmisión de grados, nombre, iniciales de dependencias o cargos, lugares geográficos, indisciplinas en el tráfico etc.

(6) Está terminantemente prohibido el establecimiento de PHONE PATCH para comunicaciones particulares, salvo casos debidamente autorizados y justificados por la autoridad competente.

(7) Cuando se establezca el PHONE PATCH para comunicaciones oficiales entre autoridades, deberá emplearse el correspondiente sistema de seguridad criptofónica en las estaciones correspondiente

que hacen la comunicación.

(8) Todo mensaje que contenga información clasificada necesariamente deberá ser cifrado o codificado antes de ser transmitido.

78. SEGURIDAD DE TRASMISION EN LOS SISTEMAS DE COMUNICACIONES DE CAMPAÑA

a. **Sistemas de Radio**

(1) Durante el funcionamiento de las redes de radio, deben emplearse obligatoriamente los cuadros de indicativos y de frecuencias, códigos y sistemas de autenticación que contienen las IOCE e IPCE.

(2) El empleo de este medio debe hacerse solamente cuando no exista la posibilidad de utilizar otro medio.

(3) La selección del medio de comunicaciones debe considerar su grado de seguridad relativa, debiendo establecerse el siguiente orden de preferencia: enlaces mediante líneas físicas, UHF, VHF y en alta frecuencia (HF) como medio alterno solo en caso de no contar con enlaces alámbricos, UHF o VHF.

(4) Deben extremarse las medidas de autocontrol durante la explotación de este medio, a fin de evitar las infidencias e indiscreciones tales, como no emplear los autenticadores de trasmisión de grados, lugares geográficos, indisciplinas en el tráfico, etc.

(5) Toda trasmisión debe hacerse con autorización del comando respectivo y empleando los procedimientos operativos vigentes (POV).

(6) No se deben mezclar textos enclavados o codificados con textos en claros.

(7) Se deben evitar las trasmisiones innecesarias, así como las pruebas excesivas y las conversaciones particulares entre operadores.

(8) Adecuarse a la velocidad de transmisión del operador más lento de la red.

(9) Está terminantemente prohibido el establecimiento del PHONE PATCH para comunicaciones particulares.

(10) Unicamente podrá establecerse el PHONE PATCH para comunicaciones oficiales, cuando las estaciones corresponsales

dispongan del equipo de codificación de voz.

(11) Todo mensaje que contiene información clasificada, necesariamente deberá ser enclavado o codificado antes de ser transmitido.

(l2) Debe hacerse máximo empleo de la radiotelegrafía en lugar de la radiotelefonía, cuando ambos pueden usarse indistintamente.

(13) Las comunicaciones en HF y VHF, en lo posible deben integrarse al sistema multicanal de área.

b. <u>Sistemas Alámbricos</u>

(1) No emplear los circuitos de retorno por tierra, sino en la zona de retaguardia.

(2) Está terminantemente prohibido emplear este medio para tratar asuntos clasificados.

(3) Cortar todos los circuitos que van hacia la zona no ocupada por tropas enemigas, salvo que el comando decida emplearlas exclusivamente con fines de contrainteligencia.

(4) Para la trasmisión de mensajes por circuitos telefónicos se seguirá el siguiente procedimiento.

(a) Cada mensaje o contacto de este tipo, deberá estar precedido por la palabra CONVENIO TELEFÓNICO, el mismo que será identificado por ambos interlocutores.

(b) El convenio telefónico, será diferente para cada mensaje y variará en la misma forma que los autenticadores transmitidos por radio.

(5) Deben emplearse los procedimientos de explotación establecidos en el MACOFA.

(6) Los usuarios de estos sistemas deben estimar las medidas de autocontrol durante su empleo, a fin de evitar las infidencias e indiscreciones.

(7) Debe ponerse especial énfasis en la instrucción de seguridad para los telefonistas teniendo presente que las interconexiones que establecen, únicamente interesan a los intercomunicados, estando prohibido que el telefonista escuche las conversaciones telefónicas.

(8) Toda información que adquiera el telefonista durante la operación del

tablero a su cargo, a excepción de lo relativo a las condiciones de la línea y el tráfico, deberá considerarse confidencial.

(9) Debe asegurarse una adecuada vigilancia y patrullaje a los circuitos alámbricos instalados.

c. Sistema Multicanal de Area (Radio Relevo)

(1) La medida de seguridad de comunicaciones dispuesta para el sistema de comunicaciones permanentemente del Ejército, también se aplicará durante el funcionamiento de los medios del sistema multicanal de área (Radio Relevo).

(2) Durante el despliegue e instalación del SMA deben emplearse preferentemente enlaces en VHF, con reveladores en casos necesarios. Solamente cuando no sea posible su empleo deberá utilizarse enlaces HF en períodos muy breves y haciendo uso de mensajes preestablecidos.

(3) Durante el planeamiento de las operaciones debe considerarse la protección física de las repetidoras y patrullajes entre estas.

(4) Deben extremarse las medidas de seguridad de comunicaciones en las repetidoras y canales asignadas para la integración de las estaciones de radio en HF o VHF, dándose estricto cumplimiento a las disposiciones de seguridad para los Sistemas de Radio y Sistemas Alámbricos.

79. MEDIDAS DE SEGTRAS CONTRA EL ENGAÑO ELECTRONICO

a. Las medidas de protección contra la intromisión de mensajes falsos se denomina AUTENTICACION cuyo objeto fundamental es verificar si las órdenes y los mensajes recibidos provienen realmente de los corresponsales de quienes se espera información o respuesta de algún mensaje, siendo la finalidad descubrir la verdadera identidad del corresponsal o puesto de radio con el que se está en enlace .

b. **Sistemas de autenticación**

(1) Concepto

Es un conjunto de letras y números acondicionados en forma aleatoria, de acuerdo a convenios previos entre los interesados. Utilizándolos según un procedimiento preestablecido, puede servir

para descubrir mensajes, puestos o redes falsas. Los sistemas de autenticación en actual uso están fundamentados, ya sea en listas preestablecidas o en métodos de adición.

(a) **Listas Preestablecidas.-** Son un conjunto de palabras, letras o números acondicionados, preparados y repartidos a los corresponsales con anterioridad; solamente se entrega a los corresponsales con quienes se va a trabajar, para que sean utilizados en la autenticación de mensajes. La forma de usarlas es trabajando los autenticadores para cada llamada de red o comunicación entre dos corresponsales, cuando el número de corresponsales aumenta, el procedimiento se dificulta.

(b) **Método de Adición.-** Este es más flexible que el anterior y consiste en asumir valores numéricos a todas las letras del alfabeto; por el procedimiento de adición se determina el autenticador. A continuación se muestra un ejemplo:

1. Ejemplo: Utilizando las listas de valor numérico que aparecen en el cuadro 1, el que transmite solicita una respuesta a dos o tres letras dadas. Por ejemplo para KHP el autenticador será la suma de (0+3+8)=11 (once), cantidad que el corresponsal deberá contestar.

CUADRO 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	8	5	6	2	0	1	3	7	9	0	5	2	4	4	3	8	1	0	7	2	5	3	9	4	9	2

2. El que recibe puede solicitar también la autenticación de quien transmitió. Los sistemas de autenticación de emergencia utilizan el método de la adición .

(2) Definiciones

(a) Elemento de Prueba

Es una letra o dígito utilizado como pregunta para la determinación de la autenticidad de un puesto, persona, orden o mensaje. El elemento de prueba se usará de acuerdo al sistema de autenticación empleado; por ejemplo "MB, K3" o "54", pueden ser elementos de prueba .

(b) Elementos de Tiempo

Es la hora que se utiliza como parte de la pregunta, acompañando a los elementos de prueba, para aumentar la seguridad. Por ejemplo el "TY" es el elemento de prueba y "14.35" es el elemento de tiempo complementario.

(c) Autenticador

Es una letra o dígito obtenido por un procedimiento preestablecido de antemano y que repetido se da en respuesta para confirmar la autenticidad de puesto, orden o mensaje. En casos especiales como en el método de adición el autenticador es un valor numérico.

(3) Sistema de Autenticación Nº 1 (Figura Nº 13)

(a) Descripción

La tabla consiste en :

1. Una columna de designaciones, que se encuentra colocada en el lado izquierdo, en ella aparece descrito el alfabeto normal, de arriba hacia abajo (de la A a la Z excepto las letras "ch", "ll" y Ñ). Las diez (10) primeras letras de la columna designación, proporcionan la tabla de sustitución para los dígitos del 1 al 0, los que se encuentran colocados correlativamente al costado izquierdo de las letras comprendidas entre la A y la J inclusive.

2. La columna de letras claves, se encuentra a la derecha de la tabla alfabética, está formada a su vez por dos columnas; la de la izquierda corresponde a un alfabeto en orden normal y la que está a la derecha contiene los equivalentes en clave.

3. Grupos de letras, que se encuentran en el centro de las dos columnas, en donde se colocan horizontalmente y de manera desordenada o aleatoria veintiseis (26) letras del alfabeto, agrupadas de a cinco letras cada grupo (excepto el último grupo que tendrá seis letras).

(b) Empleo de Sistema

1. Este estudio se hará tomando como ejemplo de elemento de prueba a las letras "ZS".

2. El autenticador se descubre en la forma siguiente :

   a. Ubique la "Z" en la columna de las designaciones, avance hacia la derecha sobre esa fila y observe que la letra "B" está inmediatamente a la derecha de la "S" ("B" es la letra clave).

   b. Localice "B" en la tabla alfabética de la derecha, se encontrará que "U" es el equivalente, por lo tanto "UU" será el autenticador.

   c. Si la segunda letra del elemento de prueba se ubica al final de una fila, la letra clave será la primera letra de dicha fila .

   d. El sistema de autenticación Nº 1 (Figura 13), se complementa con una tabla de sustitución, cuyo empleo se limita a las ocasiones en que los elementos de prueba sean numéricos .

FIGURA 13.

TABLA DEL SISTEMA DE AUTENTICACION

(4) Sistema de autenticación No. 2 (Figura No. 14)

(a) Descripción

Este sistema consiste en una tabla alfabética o tablero completo, una línea de designaciones; otra de sustitución, una columna de tiempo y otra de letras claves.

1. La tabla alfabética es un cuadro o tablero completo, de 26 x 26 letras que contiene en cada fila vertical un alfabeto completo en forma incoherente.

2. La línea de designaciones se encuentra en la parte superior de la tabla alfabética, consiste en un alfabeto completo ordenado en forma normal de la A a la Z (excepto las letras "ch", "ll" y ñ). Las diez primeras letras de la línea de designaciones proporcionan letras para la línea de sustitución de los dígitos del uno al cero, que se encuentran colocados correlativamente encima de la letra "A" a la "J".

3. La columna de tiempo está colocada al lado izquierdo de la tabla alfabética y en ella figuran las 24 horas del día numeradas desde 00 a 23. Cada una de las 24 filas horizontales corresponden a un designador de tiempo.

4. La columna de letras claves aparece a la derecha de la tabla alfabética y está formada por un alfabeto completo en forma incoherente. Para cada fila de las letras de la tabla alfabética corresponde una letra clave.

(b) Empleo del Sistema

Este estudio se llevará a cabo tomando como ejemplo de elemento de prueba "XG22.OO". El autenticador se descubre en la siguiente forma:

1. Ubique "X" en la línea de designaciones; baje por esta columna hasta encontrar la segunda letra del elemento de prueba "G", recorra sobre esta última línea horizontal hasta la letra clave que corresponde (en nuestro caso es "J").

FIGURA Nro 14
TABLA DEL SISTEMA DE AUTENTICACION
Nro 02

2. Localice la letra clave en la línea de designaciones; baje verticalmente hasta la intersección con la horizontal determinada por el elemento de tiempo; se encontrará que "I" es la letra que corresponde y en consecuencia "II" será el autenticador.
3. Si en el elemento de tiempo hubiera minutos, ellos no se tomarán en cuenta. Si los elementos de prueba, aparte del tiempo, son numerables se utilizará la línea de sustitución.

(5) Sistemas de Autenticación de Emergencia (FIG 15)

(a) Descripción del Sistema

Como se puede apreciar en la Fig Nº 15 hay un cuadro de 5x5 casilleros conteniendo cada uno de ellos una letra, así como un valor numérico. Para que las 26 letras del alfabeto hispano estén correspondidas en el cuadro en el primer casillero de la parte superior izquierda se colocan dos letras con su valor numérico .

(b) Construcción del Sistema

Para facilitar el aprendizaje de la construcción de este sistema, se desarrollará un ejemplo aplicativo:

1. Seleccionar una frase u oración clave:
   ESCUELA DE COMUNICACIONES DEL EJÉRCITO.
2. Suprimir de esa frase las letras repetidas, comenzando de izquierda a derecha (también se suprimen las letras ch, ll, ñ aunque no se repitan) y volver a escribir la frase sin las letra que se repitan:

   ESCULA DOMNI JRT.

3. Ordenar las letras que quedan en orden alfabético y colocar debajo de ellas un número correlativo, comenzando del 1:

A	C	D	E	I	J	L	M	N	O	R	S	T	U
1	2	3	4	5	6	7	8	9	10	11	12	13	14

4. Volver a escribir la frase clave, pero sin las letras suprimidas y colocar encima de ellas el n·mero que le correspondió según el paso anterior:

4	12	2	14	7	1	3	10	8	9	5	6	11	13
E	S	C	U	L	A	D	O	M	N	I	J	R	T

5. Colocar debajo de los números y de la frase clave, determinado en el paso anterior, las letras que falten, en orden alfabético:

4	12	2	14	7	1	3	10	8	9	5	6	11	13
E	S	C	U	L	A	D	O	M	N	I	J	R	T
B	F	G	H	K	P	Q	V	W	X	Y	Z		

6. Colocar los números en orden correlativo y debajo de cada uno de ellos las letras que le correspondieron según el paso anterior:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	C	D	E	I	J	L	M	N	O	R	S	T	U
P	G	Q	B	Y	Z	R	W	X	V		F		H

7. Colocar en una misma línea, las letras no suprimidas de la frase clave y a continuación las letras que faltan del alfabeto normal:

E S C U L A D O M N I J R T B F G H K P Q V W X Y Z

8. Colocar debajo de la línea de letras, determinada en el proceso anterior, números correlativos del 1 al 9, comenzando de izquierda a derecha. Repetir la serie hasta que todas las letras del alfabeto tengan asignado un valor numérico:

E	S	C	U	L	A	D	O	M	N	I	J	R	T	B	F	G	H	K	P	Q	V	W	Y	Z	
1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4	6	7	8	

9. Construir un cuadro con veinticinco casilleros interiores iguales. En seguida, tomar las dos letras, determinadas en el paso "6". Que se encuentran debajo del número 1 y colocarlas en el primer casillero interior ubicado en la parte superior izquierda. A continuación, asignar como valor numérico a estas dos letras el que corresponde, según el paso "8.", a la primera letra y colocar dicho valor en la parte inferior izquierda del primer casillero:

AP **6**				

10. Colocar en los casilleros siguientes, de izquierda a derecha y fila por fila, las letras de arriba hacia abajo del orden numérico consecutivo del paso "6."; colocando en el mismo casillero el valor numérico que

le corresponde a cada letra según el paso "8." El sistema resultante al final de todos estos pasos será la tabla de autenticación de la **figura 15**.

(c) Empleo del sistema

Los elementos de prueba se determinan conforme a lo prescrito en la IOCE. Cuando no haya prescripciones al respecto, quien solicita la autenticación, lo elegirá al azar. A continuación se discuten los diferentes casos que se presentan al emplear este sistema:

1. **Primer Caso**.- Cuando las letras del elemento de prueba están en diferente fila y diferente columna, se tomará como autenticador la suma de los números de la diagonal opuesta del rectángulo que forman. Ejm: sea "c" y "v" los elementos de prueba. Estas dos letras determinan un rectángulo imaginario del cual forman una diagonal. El autenticador será la suma de los valores numéricos de las letras "D" (7), "x" (6), que conforman la diagonal opuesta. El autenticador será entonces 7 + 6 = 13.

2. **Segundo Caso**.- Cuando las letras del elemento de prueba están en la misma fila horizontal, el autenticador es la suma de los valores numéricos correspondientes a las letras inmediatamente a la derecha de dichos

elementos. Ejemplo:
Elemento de prueba : "CD"
Autenticador : "11" (8+3)
Si uno de los elementos de prueba corresponde al extremo de una fila, se tomará el valor numérico de la primera letra de dicha fila. Ejemplo:
Elemento de prueba : "MW"
Autenticador : "13" (5+8)

3. **Tercer caso**.- Cuando la letra del elemento de prueba está en la misma columna (vertical). El autenticador es la suma de los valores situados inmediatamente debajo de los dichos elementos. Ejemplo:
Elemento de prueba : "YV"
Autenticador : "13" (9+4)

Si uno de los elementos de prueba corresponde al extremo inferior de una columna se tomará el valor numérico de la primera letra de dicha colmumna. Ejemplo:

Elemento de prueba : "KS"
Autenticador : 7 (1+6)

4. **Cuarto Caso**.- Si los elementos de prueba son las dos letras que han sido combinadas en la casilla superior izquierda, el autenticador será el doble del valor numérico asignado a este casillero.

Elemento de Prueba : "AP"
Autenticador : 12 (6+6)

(6) Sistema de Autenticación por el Método de Adición

(Figura Nº 16)

(a) Partes que comprende:

(1) Línea de designaciones.

(2) Tabla Numérica

(3) Línea Numérica Complementaria

(4) Línea de Valores

(b) Descripción del Sistema

1. Línea de Designaciones
Consta de una serie de 27 letras ordenadas en orden alfabético, ubicado en la parte superior.

2. Tabla Numérica
Es un conjunto de números de 1 al 60 colocados en orden correlativo, inmediatamente debajo de la línea de designaciones y tiene por objeto proporcionar el valor numérico a los minutos del elemento de tiempo.

3. Línea Numérica Complementaria
Empieza con 00, siguiendo en orden correlativo hasta 23, proporciona un medio de hallar el valor numérico de la hora incluida en los elementos de prueba.

4. Línea de Valores
Está constituida por números del 1 al 27 colocados en forma desordenada y ubicada en la parte inferior de la tabla. Asigna un valor a cada letra de la línea de designaciones, al número de la tabla numérica y a la hora de la línea numérica complementaria.

(c) Empleo del Sistema

1. Sea la estación AN 4, que transmite a la estación PVR un mensaje que fue firmado a las 09:57 y envía KS, como elemento de prueba. El autenticador se encontrará precedido en la forma que se indica a continuación:

A 7
N 22
4 17
p 17
V 23
R

.....
.....15
09 3
57 5
k
.....
.....14
S 1

Figura 16. Tabla del sistema de autenticación por el método de adición

2. El AUTENTICADOR será la suma de todos los valores hallados, en el caso del ejemplo 124.

3. Cuando no envían la "hora" en la comunicación, el valor numérico correspondiente, se halla en la línea de valores considerando la hora del momento en que recibe (sin minutos)

c. Autenticación de Estaciones o puestos radiales

(1) Para la autenticación de un puesto de radio, el que hace la llamada solicita la autenticación; escoge los elementos de prueba al azar que son tomados por el operador del puesto llamado, como base para encontrar el autenticador utilizando el sistema en vigencia.

(2) Cuando uno de los elementos de prueba sea un dígito, se deberá convertir a letras utilizando la tabla de sustitución que debe aparecer en todos los sistemas de autenticación .

(3) Procedimiento para las Estaciones que no entran a tiempo en la red.

Cuando un puesto no ha respondido en su turno, para entrar en la red, se autenticará por si mismo utilizando un elemento de prueba y enviará a la estación de control de Red los elementos necesarios; el puesto retrasado, puede considerarse dentro de la red.

(4) Procedimientos para las Estaciones que han respondido en forma incorrecta:

(a) Si alguna estación al entrar en la red responde incorrectamente el elemento de prueba de la estación anterior, la ECR espera hasta que todas las Estaciones hayan entrado en la red y entonces envía un elemento de prueba directamente a la Estación que respondió erróneamente; si la respuesta es correcta la red quedará abierta.

(b) Si la respuesta es incorrecta, la ECR transmite "Corrija la

Autenticación" enviando un nuevo elemento de prueba. Si este segundo elemento de prueba es respondido incorrectamente la ECR llama a la red y transmite; autenticar todas las "Trasmisiones".

(c) En caso de que una Estación no se autentique, no se le enviará tráfico a menos que los mensajes recibidos de ella están correctamente autenticados.

(d) Los pedidos de cambio y regulación de frecuencias provenientes de dicha estación no se tendrán en cuenta porque puede ser una estación enemiga que trata de regular su frecuencia con el objeto de realizar interferencia en la red.

d. Autenticación de Ordenes a la Red por la Estación de Control de la Red.

(1) En la sección Códigos y Claves de la IOCE pieza "sistema de Autenticación" se determina los grupos para la prueba de la red (Ver Figura No.17)

(2) La IOCE señala diariamente las dos letras que se deben tomar como elemento de prueba (Figura 19). La ECR se autentica transmitiendo un grupo de prueba en cada contacto, seguido del autenticador, obtenido del sistema en vigencia. Envía a su vez dos elementos de prueba escogidos al azar, con los que se autentican las estaciones subordinadas en orden alfabético. Estos proceden de igual manera hasta que hayan intervenido todas las estaciones de la red.

FIGURA Nº 17. GRUPOS PARA LA PRUEBA DE REDES DE RADIO

DIA	"A"	"B"	"C"	"D"	"E"
1	AVR	AJC	AOM	AXP	AWX
2	BTG	HVM	BWG	BQM	BDQ
3	CLG	CRE	DJB	CRE	DFI
4	TRE	FGE	HSJ	TRE	RYU

5	**KSU**	**ETY**	**ELO**	**AKD**	**QLP**
6	**LAU**	**RQU**	**FEX**	**ANE**	**AKL**

(3) Para la explotación damos el siguiente ejemplo:

(a) Datos

1. Red de Radio (Figura No.18)

2. Grupos para la prueba de las Redes de Radio (Figura No.17).

3. Elementos de prueba para la Prueba de las Redes de Radio (Figura No.19)

4. Sistema de Autenticación Nº 1 (Figura Nº 13)

5. Sistema de Autenticación Nº 2 (Figura Nº 14)

FIGURA Nº 18. RED DE RADIO

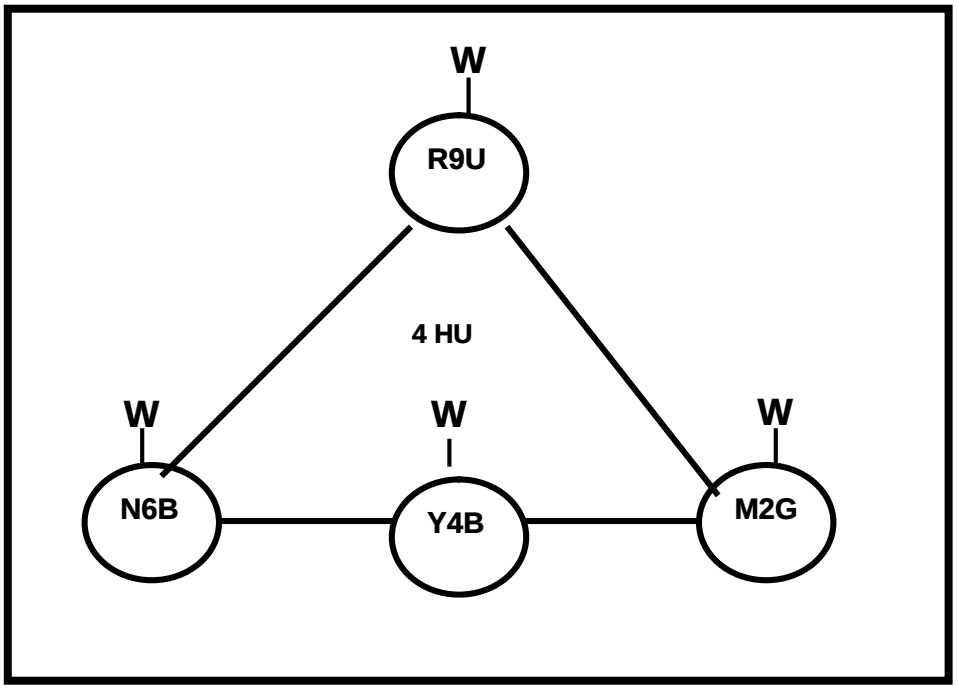


FIGURA Nº 19. ELEMENTOS DE PRUEBA DE LAS REDES DE RADIO

DIA	PRIMER CARÁCTER	SEGUNDO CARACTER
"A"	Primera Letra del Grupo para la Prueba de las Redes de Radio	Tercera Letra del Grupo para la Prueba de las Redes de Radio
"B"	Tercera Letra del Grupo para la Prueba de las Redes de Radio	Segunda Letra del Grupo para la Prueba de las Redes de Radio
"C"	Segunda Letra del Grupo para la Prueba de las Redes de Radio	Tercera Letra del Grupo para la Prueba de las Redes de Radio
"D"	Primera Letra del Grupo para la Prueba de las Redes de Radio	Segunda Letra del Grupo para la Prueba de las Redes de Radio
"E"	Tercera Letra del Grupo para la Prueba de las Redes de Radio	Primera Letra del Grupo para la Prueba de las Redes de Radio
"F"	Segunda Letra del Grupo para la Prueba de las Redes de Radio	Primera Letra del Grupo para la Prueba de las Redes de Radio

(b) Procedimientos y explicación

1. El día "A" la estación de control de red (ECR) apertura la red (empleando indicativo de red), con una prueba de red; para lo cual empleará la tabla de la figura 17 para seleccionar grupos de letras para esa prueba. Luego empleando la tabla de la figura 19 selecciona el elemento de prueba para el sistema de autenticación de la figura 13:
"4HU 4HU DE R9U R9U AVR MM AUTENTICACION RT 12.58 CAMBIO".

2. El grupo **"AVR"** es el primero del día **"A"** de la tabla de la figura 17, que al relacionarlo con la tabla de la figura 19, tenemos que para el día "A" se debe escoger la primera y tercera letra del grupo como elemento de prueba, es decir **"AR"**. Con este elemento se trabaja con el Sistema de autenticación de la figura 13 y se obtiene **"MM"** como su autenticador propio.

3. La ECR también pide que se autentiquen las estaciones subordinadas y ha enviado **"RT 12.58"**, que

constituye el elemento de prueba para emplear el sistema de autenticación de la figura 14.

4. Las estaciones empezarán a autenticarse en el orden establecido en la IOCE, que para el caso del ejemplo se ha considerado en orden alfabético:
"R9U DE M2G CC AUTENTICACION BN 13.01 CAMBIO".

5. **"CC"** constituye el autenticador de **"RT 1258"** en el Sistema de autenticación Nº 2 (Figura 14), con lo cual queda identificada ante la red. **"BN 13.01"**, es el elemento de prueba para la siguiente estación en orden alfabético, la que llamará a la ECR:
"R9U DE N6B XX AUTENTICACION QE 13.04 CAMBIO".

6. **"XX"** es el autenticador de **"BN 1301"**, con lo cual la estación queda identificada ante la red. **"QE 13.04"** es el elemento de prueba para la tercera y última estación de radio, que se identifican ante la red empleado el Sistema de autentificación Nº 02:
"R9U DE Y4B AA CAMBIO".

7. **"AA"** es el autenticador de **"QE 1304"**, con lo cual queda identificada ante la red, no trasmitiendo otro elemento de prueba por no existir mas estaciones en el ejemplo. Entonces la ECR da por terminada la autenticación de órdenes a la red, al haber sido identificadas todas las estaciones:
"4HU DE R9U TERMINADO"

e. Autenticación de Mensajes

Elementos de prueba para la autenticación de Mensajes

(1) La IOCE establece el convenio la forma como debe escogerse el elemento de prueba (Figura 20).

(2) Para la explotación damos el siguiente ejemplo:

(a) Datos

1. Red de Radio (Figura Nº 18)
2. Se vive el día "A" (Figura Nº 19)

3. Sistema de autenticación en vigencia Nº 1 (Figura Nº 13).
4. N6B ESTACION DE RADIO QUE TRANSMITE EL MENSAJE
5. Y4B ESTACION DE RADIO QUE RECIBE EL MENSAJE
6. Texto del mensaje : INFANTERIA ENEMIGA OCUPA CERRO MARTE.

(b) Procedimiento

1. "Y4B DE N6B INFANTER=A ENEMIGA OCUPA CERRO MARTE AUTENTICADOR SS CAMBIO".
2. "N6B DE Y4B COMPRENDIDO TERMINADO"
3. Como el autenticador SS recibido por la estación Y4B es correcto, luego el mensaje será verdadero.

FIGURA 20. ELEMENTOS PARA LA AUTENTICACION DE MENSAJES

DIA	PRIMER CARÁCTER	SEGUNDO CARACTER
"A"	Segunda Letra o Dígito del Indicativo de la Estación	Tercera Letra o Dígito del Texto del mensaje
"B"	Primera Letra o Dígito del Indicativo de la Estación	Quinta Letra o Dígito del Texto del mensaje
"C"	Tercera Letra o Dígito del Indicativo de la Estación	Segunda Letra o Dígito del Texto del mensaje

80. MEDIDAS DE SEGTRAS CONTRA LA PERTURBACION

a. Casi todos los Ejércitos del Mundo han incrementado su Tecnología con el fin de facilitar las comunicaciones, Comando y Control de sus Fuerzas con el mínimo de tiempo. Normalmente como todo proceso y/o adelanto, genera ciertas vulnerabilidades que debemos tener en cuenta, ya que el enemigo o los países interesados tratarán por todos los medios de crear o impedir que dichas Telemática electromagnéticas lleguen con claridad a las Estaciones o Puestos de Radio Receptoras, produciendo perturbaciones.

b. Las medidas de Seguridad de Trasmisión constituyen las actividades que hay que desplegar para liberarnos de las contra medidas pasivas y activas que tome el enemigo con respecto a nuestros equipos de comunicaciones, lo que constituyen las Contra-Contra Medidas (COCOME).

c. **Medidas Para Reducir los Efectos de la Perturbación**

(1) Reducción de los efectos de la perturbación

Una medida normal, es preveer la Interferencia, anticiparse a ella. Entre las medidas que pueden reducir los efectos de interferencias, tenemos:

(a) RADSIL
(b) Entrenamiento del Operador
(c) Asignación de Frecuencias Alternas a las UU.
(d) Vías Alternativas de Comunicaciones
(e) Operaciones de Ajustes y Calibración de Equipos.
(f) Instalación y Orientación de las Antenas
(g) Medidas de Seguridad de Comunicaciones

(2) Medidas que deben adoptarse

A fin de eliminar la identidad, así como determinar y disminuir las posibilidades de interferencia, se debe tener presente lo sgte:

(a) Mantener el equipo en óptimas condiciones de Operación.
(b) Reducir la transmisión al mínimo indispensable.
(c) Reducir la velocidad de Transmisión.
(d) Uso apropiado de los controles de recepción.
(e) Informe de Interferencia.
(f) Cumplir las Prescripciones de la IOCE y POVC.

(3) Necesidad de determinar el tipo de perturbación

Los operadores deben estar entrenados e identificar si las interferencias son o no intencionales y si son causadas por fuente externa o mal funcionamiento del receptor.
Entre las interferencias que se pueden presentar están las siguientes:

(a) Perturbaciones de Operaciones.
(b) Onda Continua.
(c) Interferencia de Equipo en mal Funcionamiento.
(d) Barrido Completo de Espectro.
(e) Emisión de sonido de tono bajo.
(f) Ruidos.

SECCION V. SEGURIDAD DE EMISION (TEMPEST)

81. CONCEPTO DE SEGURIDAD DE EMISION (SEGEMI)

a. Es el cuarto componente de la SEGCOM, que resulta de tomar una serie de medidas para negar a personas no autorizadas, información de valor la cual podría ser obtenida de la interceptación y del análisis de emanaciones comprometedoras.

b. El término en que los últimos años se viene asociando a tales esfuerzos es "TEMPEST" y/o control de emanaciones comprometedoras, ya que se refieren a la investigación y estudio de ellas. Normalmente, TEMPEST está orientado más a facilidades fijas y equipo electrónico que procesa información de alta clasificación.

82. ACTIVIDADES O MEDIDAS DE SEGEMI (TEMPEST)

a. Actividades que proporcionan apoyo técnico en la selección de TEMPEST Aprobada o equipos de deformación eléctrica para el procesamiento de información clasificada.

b. Pruebas instrumentales de facilidades operativas, que se conducen para determinar si las emanaciones comprometedoras son detectables más allá del espacio de control establecido.

c. Todas las actividades TEMPEST están destinadas a asesorar al Comandante en la evaluación de las vulnerabilidades de sus facilidades y para desarrollar planes que incrementen la Seguridad de emisión.

d. Las actividades de TEMPEST se desarrollan mediante tareas, ejecutadas por personal especialista de Contrainteligencia de Telemática y consiste básicamente en los siguiente:

(1) Asistencia Técnica.
(2) Inspecciones Técnicas.
(3) Pruebas de Campo.
(4) Pruebas y Análisis en ambientes controlados.
(5) Certificación de "Seguridad automática de Comunicaciones de voz".
(6) Revisión de planes de instalación de Ingeniería.
(7) Vigilancia de lugares TEMPEST.

83. RESPONSABILIDADES EN LA SEGEMI (TEMPEST)

a. El esfuerzo de la SEGEMI es predominantemente una responsabilidad del Organo de Inteligencia del más alto escalón en estrecha coordinación con el

Organo de Comunicaciones, Electrónica e Informática.

b. Esta responsabilidad se materializa a través de programas especiales de entrenamiento, orientado a contar con personal altamente calificado para apoyar operaciones TEMPEST en todos los escalones del Ejército.

c. El programa debe dar como resultado contar con personal capaz de efectuar reconocimientos iniciales de lugares, así como de inspecciones o verificaciones de los planes de instalación de Ingeniería, antes de que algún acceso seguro se construya. Después de la instalación, el personal entrenado debe poder ejecutar inspecciones periódicas para determinar la conformidad del acceso con el criterio preestablecido.

84. ASISTENCIA TECNICA DE TEMPEST

Incluye:

a. Asistencia a los Comandantes en todos los escalones, en la interpretación de políticas y criterios de TEMPEST.
b. Asistencia en la selección de TEMPEST-Aprobada o equipos de deformación eléctrica.
c. Asistencia en el planeamiento de la instalación de equipos de acuerdo al criterio TEMPEST.
d. Evaluación de la sensibilidad y vulnerabilidad de las facilidades para explotación TEMPEST y recomendaciones para incrementar la seguridad.

85. INSPECCIONES TECNICAS DE TEMPEST

Son exámenes visuales de una instalación, para determinar si el equipo electrónico empleado para procesar información clasificada, está instalado de acuerdo con los estándares preestablecidos, que minimizan problemas de emanaciones comprometedoras.

86. PRUEBAS DE CAMPO DE TEMPEST

a. Son exámenes detallados de equipos electrónicos o de un sistema electrónico completo, que procesan información clasificada. Las pruebas están más orientadas a instalaciones y actividades permanentes o fijas, que procesan información.

b. Las pruebas identificarán las características del sistema de procesamiento; es por eso que es impracticable su aplicación a un sistema electrónico

táctico o de campaña, donde las situaciones están cambiando constantemente.

c. Sin embargo en situaciones especiales, se podrán aplicar de manera selectiva, sólo con la finalidad de aumentar las pruebas del sistema táctico durante la fase de investigación y desarrollo (I & D) o cuando la prueba de I & D no se ha efectuado o se efectuó superficialmente.

d. Las pruebas de campo son llevadas a cabo por personal especialista "en el sitio", empleando equipamiento de detección y análisis de Telemática.

87. PRUEBAS Y ANALISIS EN AMBIENTES CONTROLADOS

a. Son exámenes instrumentales de sistemas o equipamientos electrónico que son o pueden ser empleados para procesar información clasificada.
b. Estas pruebas son efectuadas en laboratorios especialmente diseñados para determinar si el equipamiento bajo prueba exhibe emanaciones comprometedoras, y para determinar medidas que las minimicen o eliminen antes que dicho equipamiento sea empleado en campaña.

88. CERTIFICACION DE SEGURIDAD AUTOMATICA DE COMUNICACION DE VOZ

Es un examen visual de una facilidad que cumple función de terminal de un sistema de comunicaciones de voz seguro (con seguridad criptofónica). Este examen es efectuado una sola vez durante la inspección por personal especialista, quien verificará el cumplimiento de los requerimientos exigidos por el más alto escalón de Inteligencia, Comunicaciones, Electrónica e Informática.

89. VIGILANCIA DE LUGARES TEMPEST

a. Son exámenes visuales realizados por personal especialista, de un lugar o facilidad antes de alterar, construir o instalar equipamiento electrónico destinado al procesamiento de información clasificada.
b. Esta vigilancia es conducida para comprobar si las previsiones para la instalación del equipamiento electrónico, se están cumpliendo de acuerdo al criterio establecido para controlar las emanaciones comprometedoras; y, para advertir o alertar al Comandante sobre las necesarias correcciones o cambios.

CAPITULO 5

SEGURIDAD ELECTRONICA

SECCION I. GENERALIDADES

90. INTELIGENCIA ELECTRONICA DEL ADVERSARIO

a. Nuestros potenciales adversarios tienen las mismas posibilidades de obtener inteligencia electrónica de nuestros sistemas de armas, ya que en la práctica la doctrina de empleo de su inteligencia de Telemática es la misma; consecuentemente en este párrafo se hará una breve descripción de lo que es la Inteligencia Electrónica (INTEL)

b. Como se mencionó en el Capítulo 2, la INTEL es parte de la INTETE que consiste en el análisis de emisiones electromagnéticas que se obtienen por la interceptación y estudio de las Telemática de no-comunicaciones enemigas, tales como radares de los sistemas de vigilancia, de adquisición de blancos y de guiado de cohetes, así como de los provenientes de los sistemas de navegación.

c. La información que la INTEL enemiga podría obtener, le servirán posteriormente para completar y/o confirmar una base de datos o información útil sobre los probables objetivos, a los que podrá inmediata o posteriormente atacar con apoyo de fuego, apoyo aéreo ofensivo y/o con perturbación.

91. CONCEPTO DE SEGURIDAD ELECTRONICA (SEGELEC)

a. Es la parte de la SEGUTE, que contiene un conjunto de medidas y/o actividades, destinadas a proteger o negar información electrónicamente generada, que sea de valor a personas no autorizadas. También se puede conceptualizar como la salvaguarda de las emisiones que no son de comunicaciones (no-comunicaciones: radares, ayudas para la navegación, etc) de la explotación enemiga.

b. La SEGELEC, hasta hace algunos años ha sido menos visible que la SEGCOM, a pesar que siempre ha sido evidente y esencial asegurar que el vasto universo de emisores de no-comunicaciones, sea protegido de la explotación por personas no autorizadas.

SECCION II. AREAS FUNCIONALES DE LA SEGELEC

92. PROGRAMA DE SEGELEC

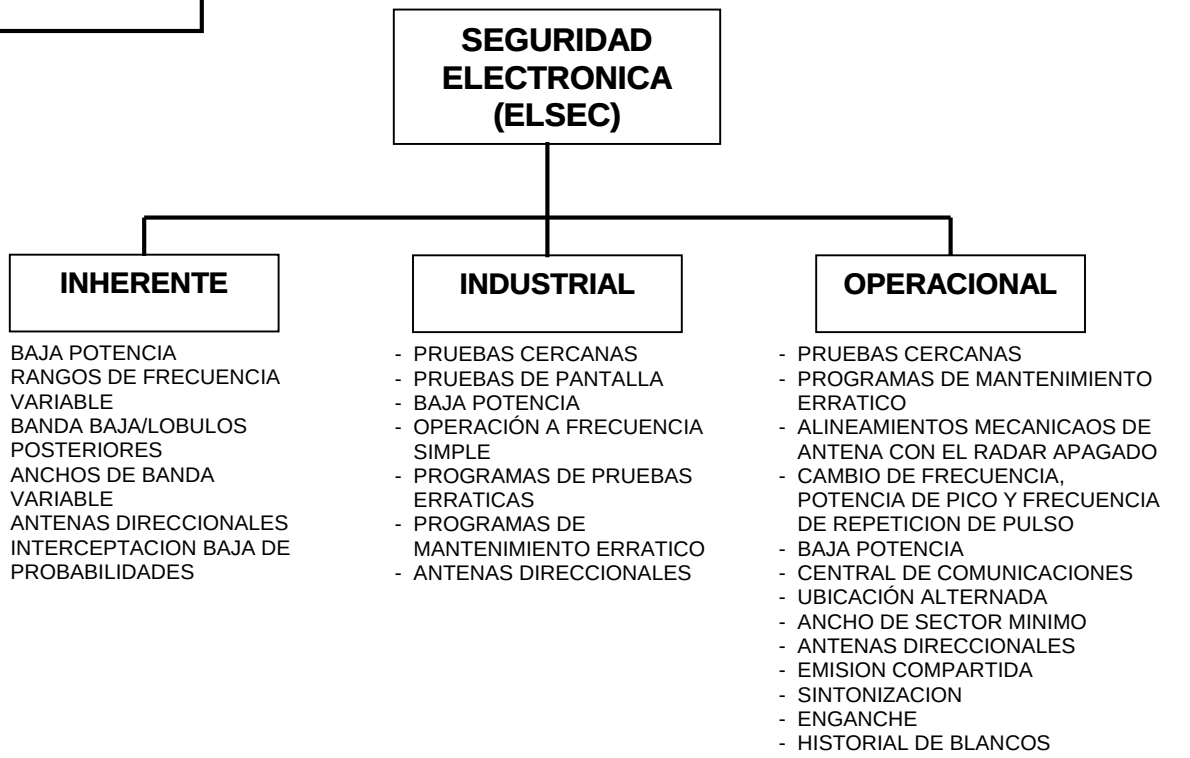
a. La SEGELEC se aplica durante las fases de la administración del ciclo de vida de un sistema electrónico, el mismo que se desarrolla normalmente a través de un programa.

b. De acuerdo a lo establecido en el párrafo anterior, un programa de SEGELEC, contendrá tres áreas funcionales que corresponderán a las tres fases del ciclos de vida:

(1) SEGELEC INHERENTE
(2) SEGELEC INDUSTRIAL
(3) SEGELEC OPERACIONAL

c. En la figura Nº 20 se resumen las tres áreas funcionales o cielos de vida del sistema.

FIGURA Nº 21



9.3 SEGELEC INHERENTE

a. Es la fase inicial que incluye las características de seguridad incorporadas interiormente en los componentes del equipo para reducir su susceptibilidad.

b. Actualmente, esta fase es el corazón del programa ya que la efectividad de

la SEGELEC en el combate dependerá directamente de las capacidades del equipo.

c. Algunos ejemplos del diseño de éstas técnicas, que normalmente se incluyen como especificaciones mínimas de seguridad son:

(1) Disponibilidad de montajes de baja potencia.
(2) Banda baja y lóbulos traseros para antenas.
(3) Rangos de frecuencia variable

d. Estas técnicas de diseño son también empleadas como características de las COCOME.

e. Los órganos del más alto escalón de comunicaciones, electrónica e informática, tienen la responsabilidad de velar porque las imágenes y técnicas que desarrollen un nuevo sistema, cumplan con la SEGELEC inherente; o que estas técnicas de diseño sean exigibles en los procesos de adquisición.

94. SEGELEC INDUSTRIAL

a. Es la segunda fase del programa dedicada a proteger las características y posibilidades de un nuevo sistema, durante su desarrollo y producción.

b. El espionaje industrial es la mayor amenaza hoy en día, por lo que esta fase será de responsabilidad de los órganos de más alto escalón de inteligencia en coordinación con los órganos de comunicaciones, electrónica e informática.

c. Algunas técnicas aplicables a esta fase son:
- Pruebas cercanas
- Pruebas de pantalla
- Operación de frecuencia simple
- Programas de pruebas erráticas
- Programas de mantenimiento errático
- Antenas direccionales

95. SEGELEC OPERACIONAL

a. Es la última fase del programa y se pone a prueba cuando el emisor es ubicado en el campo de batalla, o empleado en combate o entrenamiento a doble acción por el operador.

b. Durante esta fase, la amenaza de la Inteligencia Electrónica enemiga es enfrentada, y permitirá confirmar si son eficaces y efectivas la aplicación de

todos los tipos de técnicas y procedimientos de SEGELEC de las fases anteriores, asegurando una exitosa operación durante el combate.

c. Esta área funcional o fase final es de responsabilidad de los operadores y de sus Comandantes. La preparación de boletines técnicos y su distribución adecuada y oportuna, será de gran ayuda para la SEGELEC operacional.

CAPÍTULO 6

CENSURA DE COMUNICACIONES

96. RIESGOS DE LA CENSURA

Los riesgos de la Censura de Comunicaciones son los siguientes:

a. Acceso no Autorizado

Es el riesgo de la seguridad física que resulta del ingreso de personas no autorizadas a las instalaciones de comunicaciones y tomar conocimiento deliberada o casualmente, del contenido de los mensajes .

b. Infidencia de las Comunicaciones

Es el que resulta de facilitar al personal no autorizado, deliberadamente, por negligencia o descuido el contenido de los mensajes.

97. MEDIDAS DE CONTROL DE CENSURA

Son medidas que se toman para neutralizar los riesgos que amenazan la censura de comunicaciones.

a. Medidas para reducir el acceso no autorizado (detalladas en Capítulo 4: Sección II Seguridad Física de Comunicaciones).

b. Medidas para reducir la Infidencia
Adoctrinamiento del personal encargado de manejar los mensajes.

98. TECNICAS PARA ASEGURAR LA CENSURA

a. Clasificación de Seguridad

(1) Los mensajes se clasifican según la importancia de la información que contiene en:
(a) Estrictamente Secreto (ES)
(b) Secreto (S)
(c) Confidencial (C)
(d) Reservado (R)
(e) Común (Co)

(2) Los mensajes clasificados deben ser de conocimiento del Comandante, del Oficial de Seguridad Criptográfica y del personal de comunicaciones estrictamente relacionado con el asunto.

b. Tipos de censura

Existen 02 tipos de censura:

(1) Censura de rutina
(a) Mensaje reservado

(b) Mensaje común

(2) Censura especial
(a) Mensaje estrictamente secreto
(b) Mensaje secreto
(c) Mensaje confidencial

c. <u>Archivamiento Adecuado</u>

Mantener archivos separados de acuerdo a su clasificación de seguridad :

(1) Archivo de mensajes no clasificado

(2) Archivo de mensajes clasificados

d. <u>Incineración</u>

Incineración de los mensajes al vencimiento de su vigencia.

99. PREVENCION DE LOS RIESGOS DE CENSURA

a. Aplicación del Plan de Seguridad Física de Comunicaciones.

b. Conferencias periódicas sobre infidencias, así como colocar en lugares visibles de las instalaciones de comunicaciones, oficinas, etc, letreros advirtiendo del delito de Infidencia.

ANEXO 1. INSTRUCCIONES PARA LLENAR EL FORMATO PARA LA CONFECCION DEL POV DE SEGURIDAD

1. ENCABEZAMIENTO

Contiene el n·mero de la copia asignada al POV; Cuartel General, Unidad o Servicio que lo expide, el lugar de expedición y el Grupo Fecha/Hora.

2. CUERPO

a. Párrafo 1: En vigencia

(1) Fecha que entra en vigencia

(2) Unidades Subordinadas o reparticiones que regirán por el POV

b. Párrafo 2 : Organización

(1) **Elementos de Comando y Control.-** Se aumentará a los elementos que participan en la Dirección y Control de seguridad Militar.

(a) G-2 o S-2

(b) Otros elementos

(2) **Elementos de ejecución.-** Se enumeran a todos aquellos que participan en la ejecución de las Medidas de Seguridad Militar :

(a) Servicio de Guardia
(b) Servicio de Día
(c) Policía Militar
(d) Rondas
(e) Permanencias
(f) Servicio de Seguridad
(g) Servicio contra incendios
(h) Vigilantes
(i) Oficiales de "ESTRICTAMENTE SECRETO"
(j) OI
(k) AI
(l) Otros elementos

c. Párrafo 3 : Personal

(1) Disciplina Ley y Orden. Se indicarán :

(a) Servicio de Guardia : Efectivos, distribución y consigna relacionadas con la Seguridad Militar
(b) Servicio de Día
(c) Servicio de PM

(d) Otros Servicios

(2) Personal Civil : Se indicarán :

(a) Clasificación del Personal Civil de acuerdo con el grado de acceso a la documentación, material o equipo clasificado.

(b) Forma como se controlará al personal civil al ingresar a la instalación durante su permanencia y a la salida.

(3) Diversos : Se indicarán los archivos y registros que se llevarán por ejemplo :

(a) Registro de clasificación del personal
(b) Registros de los hijos de extranjeros y de los casados con extranjeros .
(c) Relaciones domiciliarias
(d) Personal sospechoso
(e) Archivo de investigaciones realizadas
(f) Archivos de Datos Biográficos
(g) Otros archivos y registros

d. Párrafo 4 : Contrainteligencia

(1) Seguridad de la información

(a) Medidas pasivas: Se indicarán:

1. Locales donde se guardará la documentación Clasificada y el archivo.
2. Mobiliario para guardar documentación
3. Afiches alusivos a la Seguridad que se utilizarán.
4. Otras medidas.

(b) Medidas Activas: Se indicarán:

1. Procedimientos a utilizar para la confección, reproducción, manejo, cuidado, distribución y recojo de la documentación clasificada.
2. Procedimientos de incineración y eliminación de copias, calcos, borradores y otros materiales empleados en la información clasificada.
3. Medidas para tomar en caso de extravío o pérdida de documentación clasificada.
4. Instrucciones para el empleo de las máquinas de cifrar y códigos.
5. Medidas de Seguridad de las Comunicaciones.
6. Medidas de Censura.
7. Medidas para destrucción de la documentación en caso

de emergencia.

8. Medidas de control de mesas de parte y Centro de Mensajes.
9. Otras medidas.

(2) Seguridad del Personal. Se indicarán:

(a) Relación del personal militar y civil con el grado de clasificación de seguridad que le corresponde: Furrieles, correspondencias empleados.

(b) Medidas por tomar en caso de ejecución de delitos contra el orden constitucional y la Seguridad del Ejército. Hacer mención a los planes para casos de alteración del orden público, planes de defensa de la instalación y planes contra actos subversivos, sedición, motín.

(c) Medidas de Seguridad relacionadas con el personal extraño que ingresa a la instalación visitantes, vendedores, etc

(3) Seguridad de las Instalaciones. Se indicará:

(a) Formas como se realiza el control de los accesos, hacer mención a la guardia.

(b) Forma como se realiza la custodia de locales, almacenes donde se guarda o almacena información, material y equipo clasificado.

(c) Forma como se realizará el control de vehículos que ingresan a la instalación.

(d) Medidas para asegurar el alumbrado de la instalación.- Responsabilidades.

(e) Sistema que se utiliza para combatir los incendios como debe funcionar.- Responsabilidades

(f) Medidas a tomar en caso de ataque desde el exterior a la instalación. Motines y sabotajes. Hacer mención a los planes de defensa de la instalación contra motines y contra sabotajes.

(g) Otras medidas.

e. Párrafo 5. Operaciones e Instalación

(1) Seguridad del Movimiento. Indicar las medidas que debe tomarse para dar seguridad a la Información en el caso de movimientos de tropa, transportes y embarques del material clasificado, maniobras u operaciones militares.

(2) Instrucción. Indicar la forma como se llevará a cabo la instrucción del personal en lo que se refiere a la seguridad militar, igualmente enumera las charlas o conferencias para Oficiales que se dictarán con referencia a la ejecución de delitos de traición a la patria, contra el orden constitucional y contra la seguridad de las Fuerzas Armadas.

f. Párrafo 6. Logística

Hacer mención a los encargados del mantenimiento del sistema de alumbrado, sistema contra incendios, vallas cercos, mobiliario y locales donde se guarda o almacena material, equipo o información clasificada.

g. Párrafo 7. Comando y Comunicaciones

(1) Oficina de control: Del Escalón Superior y de la Instalación.

(2) Sistema de Comunicaciones para la Seguridad: Describirlos e indicar su funcionamiento.

(3) Sistema de alarma: Describirlos e indicar su funcionamiento.

(4) Informes sobre Seguridad Militar.

(5) Término: Contiene: Firma, Anexos, la Distribución y la Autenticación

ANEXO 2. FORMATO DE DIRECTIVA CON NORMAS DE SEGURIDAD DE COMUNICACIONES

(MEMBRETE)

DIRECTIVA No. _____

Para la confección de Directivas con Normas de Seguridad de Comunicaciones.

1. Objeto

Dictar las disposiciones necesarias para la confección de las Directivas con Normas de Seguridad de Comunicaciones .

2. Finalidad

Capacitar al Oficial de Comunicaciones en la formulación de Directivas con Normas de Seguridad de Comunicaciones.

3. Alcance

a. Que los Oficiales de Comunicaciones tomen conocimiento de las disposiciones de detalle.

b. Coordinar las actividades necesarias para la confección de las Directivas con Normas de Seguridad de Comunicaciones, se realicen de acuerdo a las prescripciones reglamentarias.

4. Prescripciones Generales

a. Generalidades

Los problemas de Comunicaciones no tienen una solución tipo, pero cualquiera que sea el caso, la solución debe tener presente las Normas de Comunicaciones.

b. Normas de Comunicaciones

(1) La Unidad Superior es la responsable de instalar, operar y mantener el Sistema de Comunicaciones de las Unidades Subordinadas.

(2) La Unidad que apoya con sus fuegos, lleva sus medios de Comunicaciones a la Unidad apoyada, en caso de que el apoyo fuera diferente al del fuego, el problema se soluciona mediante coordinación.

(3) Las Comunicaciones Laterales se establecen según órdenes del Escalón Superior a Falta de instrucción, de izquierda a derecha.

(4) La repartición de los medios no es homogénea para cada operación, sino adaptada a la situación.

(5) Las necesidades de enlace se deberán satisfacer simultáneamente por varios medios de transmisiones constituyendo un sistema integrado.

(6) El Sistema de Comunicaciones, servirá de base para el sistema que debe apoyar la operación futura.
Sin embargo, debe tenerse presente que la misión de la GU, debe cumplirse y que todos y cada uno de los componentes deben sentirse responsables de ello. En la época actual que ha impreso a la guerra rapidez y dispersión de medios, la misión de la GU sólo se cumplirá si se dispone de un eficiente sistema de comunicaciones; sólo mediante el esfuerzo simultáneo de todos y cada uno se conseguirá establecer el Sistema de Comunicaciones necesario.

5. Prescripciones Particulares

En éste párrafo se indicarán aquellos aspectos de detalle que refiriéndose a normas de comunicaciones, solamente correspondan a determinadas Unidades, escalones o elementos en forma específica, sin ser general a todos.

6. Diversos

En éste párrafo se indicarán disposiciones que por su importancia no merecen ser consideradas en los párrafos anteriores.

ANEXO 3
FORMATOS DE PIEZAS DE IOT RELATIVAS A SEGURIDAD DE TRASMISIONES

SECRETO

COPIA Nº .... de Copias
IOCE.....
IIDE
LIMA
NOV 98
XY-5

PIEZA 5-3

En vigencia Día "D"

SISTEMA DE AUTENTICACION

1. SISTEMA DE AUTENTICACIÓN Nº 1

		RESPUESTA
A B C D E	F S G Y H Z A E X R M O B N W C R D G V P Y T J U L F S G Y H Z A E X R M O B N W C R D G V P Y T J U T A N F M V E L D K P A W Y O G S H X M Z O Q G T I V	A – O B – C C – N D – B E – X
F G H I J	M I C D S Z J K C Q U R A F B N F V F H X L T W G O Z I R P W N I D O K M V H G X S B U F L O A Y T V E F E Z D M X G T K S I A R I U P I C E Q V Y N O H	F – A G – M H – L I – V J – W
K L M N O	F X T O J I S N W E Y V D R M L Q H B C P Z G U K A U F A P X B Q I V G H C W R M N X I D S Y J O W Z T M C A Z B N S L D O R L T P Y K Q G H U X F V I W	K – D L – J M – Y N – P O – U
P Q R S T	B Q X A W Y P K C Z V G N L O S F E J M U H R I T O H U Y M X I I F V E L C J A W R B X G Z P N D Q K O P T A O S F Q E Z G C R B U J N L W D Y H M V X I	P – F Q – G R – E S – Q T – Z
U V W X Y Z	W V M Y E X D F C N L U H Z S Y A O J Q G T K B P R Z D P C O W F Y L V G A O B K M X H T I U E R N J S C B I A N O S E X J D K P F Y T L G U Q Z V H M R W	U – T V – H W – R X – I Y – K Z – S

Acuse Recibo

(Fdo) V.BLANCO C.
Gral Cmdte Gral

DISTRIBUCION:

Es copia
A. Contreras C.

SECRETO
1-1

COPIA Nº..... de .... Copias

IOCE
34-DI
LIMA
NOV 98
XY – 5

P I E Z A 5 - 1

En vigencia : Día “D”

SISTEMA DE AUTENTICACION DE EMERGENCIA

2. Sistema de Autenticación de Emergencia

N-F **5**	**R** **9**	**J** **2**	**Z** **5**	**U** **3**
E **9**	**G** **7**	**Y** **4**	**P** **2**	**B** **1**
A **4**	**C** **6**	**Q** **5**	**O** **3**	**I** **9**
W **1**	**K** **4**	**M** **8**	**S** **6**	**D** **3**
L **8**	**H** **1**	**T** **9**	**V** **5**	**X** **4**

Acuse recibo
DISTRIBUCION

(Fdo) V Blanco C
Gral Cmdte Gral

Es Copia
A. Contreras C.
G-3

SECRETO
1-1

COPIA Nº
IOCE
.....

LIMA
NOV 98
XY – 5

P I E Z A 6 – 1

En vigencia: Día “D”

CODIGO PARA MENSAJES

CLARO	CODIGO
Amancaes Hda	Gobardina
.....	Flores
Buena vista	Chocolate
.....	Alfalfa
Boca del Río	Mayo
.....	Señora
Cerro Alegre	Amor
.....	Celia
Cerro Las Lomas	Filo
Cerro Alturas Verdes	Antonio
Cerro Punta	Carlos
Cerro Punta Grande	Pomo
Cerro Negro	López
Cerro Huacho	Calco
.....	Borrador
Cerro Cucaracha	Junio
.....	Hilario
Cerro Ventana	Abril
.....	Negativo
El Arenal	Turco
.....	Tinta
Hornos	Auto
.....	Mano
Juncal	Lente
.....	Cura
La Pampa	Galón
.....	Cardenal
Las Huacas	Canguro
.....	
Ladera	
.....	
Oquendo Hda	
.....	

Puente El Soldado
.....
Puente Piedra
.....
Playa Oquendo
.....
Pan de Azúcar
.....
Quebrada Los Perros
.....
Romeral
.....
Río Rimac
.....
Río Chillón
.....
Santa Eulalia
.....

CLARO	**CODIGO**
San Nicolás	Carnicero
	Luna
Salitral	Sal
	Neptuno
Totoral Hda	Hoja
	Cajas
Ventanillas	Dama
	Zapato
Zapallal	Búfalo
	Egipto
Números	Tacna
	Uranio
O	Sodio
	Nitrato
1	Octubre
	Derecho
2	
3	
4	
5	

6
.....
7
.....
8
.....
9
.....

Acuse recibo
DISTRIBUCION

(Fdo) V BLANCO C
Gral Cmdte Gral

Es copia
_____

A. Contreras C.
G-3

SECRETO
1 – 1

COPIA Nº .... de ..... Copias
IOCE
.....
LIMA
NOV 98
XY – 5

P I E Z A 7 – 1

En vigencia: Día “D”

CODIGO DE UNIDADES

1. Trasmisión en Alfabeto Internacional Morse

UNIDAD	D	D+1	D+2	D+3
XX DE	DGW	ZBC	KTP	ALM
34 D MOTZ	JAV	HHD	FMH	NNO
CG	KUB	LGE	ISJ	RON
B – 80	DFM	HFD	JUY	VMP
B – 81	ETW	XIE	KGH	HLA
B – 82	AEY	FEC	CGH	LPL
BIB – 312	MBX	BJF	SRG	KTM
BTq 312	XIS	HDB	TCL	SOJ
GAC – 34	CPA	QJK	HRD	IDR
RCB – 34	JHK	IIM	RAB	TUV
Cía At – 34	OPJ	JAN	SLO	MCI
Cía Trasm 34	COC	LEN	TIN	JOR
B. Serv 34	MEN	PAU	UAT	HHO
B. Ing 34	XAB	ING	TOZ	COH

2. Trasmisión por Otros Medios

UNIDAD	D	D+1	D+2	D+3
XX DE	RUDY	ANTON	SAMUEL	JOSE
34 D MOTZ	JORGE	DARIO	TITO	CARLOS
CG	VICTOR	ELMER	TOMAS	JUAN
B – 80	ALEX	GASTON	ULISES	PERCY
B – 81	JAVIER	HECTOR	ALEJO	ABEL
B – 82	GERMAN	KIKO	RAUL	TEDY
BIB – 312	MIGUEL	LEO	CIRO	JAIME
BTq 312	TULIO	MIRO	JULIO	LUIS
GAC – 34	ERASMO	OSCAR	PEDRO	JULIO
RCB – 34	WALTER	PEPE	PIO	SIXTO
UNIDAD	**D**	**D+1**	**D+2**	**D+3**
Cía At – 34	MOISES	TELMO	FAVIO	GABRIEL

Cía Trasm 34	ADRIAN	LINO	MARIO	PABLO
B. Serv 34	POLO	LUCIO	HUGO	MANUEL
B. Ing 34	NICO	SIMON	JAIME	LINO

Acuse recibo
DISTRIBUCION

(Fdo) V BLANCO C
Gral Cmdte Gral

Es copia

_____
A. Contreras C.

SECRETO
1 – 1

SECRETO

COPIA Nº .... de ..... Copias
IOCE
II DE
LIMA
NOV 98
XY – 5

P I E Z A 8 – 1

En vigencia: Día "D"

CODIGO CRIPTOGRAFICO

TABLA PARA CIFRAR

FECHAS		A B C D E	F G H I J	K L M N O P	Q R S T	U V X Y Z
D HORA:0700	1	H E I F J	C Z Y V X	R K P U S N	T A Q O	M B L C D
	2	Y X U Z S	V T O H K	C D L G E Q	M P R N	A I F J B
	3	V Y X U Z	B S I E T	H J P R G L	A M O K	C D F Q N
	4	L A H O R	N T B C J	Q Z D Y J V	P S G U	M X F C K
	5	K O F Y R	U A M G D	T P L S X J	H C Q N	J B Z V E
D +1 HORA:0700	1	B Q R I U	J C Y S G	O K A F N Z	H D V M	X L W P T
	2	F D S L O	W X N A R	J Z C M I Q	Y B P T	V H K G U
	3	C E P N T	D Z M Q F	R B U J Y K	O G I V	H S X A L
	4	F Y G K D	O T E M U	N P B L X H	Q Z A R	V J I C S
	5	I E A Z J	G P C K X	H T D O N U	Y M V F	S L B R O
D +2 HORA:0700	1	C T U A S	O S J D P	H I N E X M	V D R K	Q F Y G L
	2	J B P T I	M A K R G	Y C X H F L	Y D Z O	Q U S E N
	3	P N Z M X	V G O K T	L E Q Y F C	J R A S	I D H B U
	4	M A Q R G	P B V H Z	F K I X N C	Y O E T	D S U L J
	5	G Q Z H X	C P V E Y	I N A O F E	B L J U	M T S K D
D +3 HORA:0700	1	G A H Z C	S I J B Q	K X D V O F	Y T L M	U R N E P
	2	S T F X I	Q C G H B	O A Z N R V	Y M P U	D K E J L
	3	H G I J X	A Q K N V	D C R L P M	X U B O	S F T E Y
	4	F O D K N	E Z J U G	M V B P I S	Q Z R A	T L Y H C
	5	K S B F L	T M Y G U	X N C O H Z	D J V P	I R E A Q
		A B C D E	**F G H I J**	**K L M N O P**	**Q R S T**	**U V X Y Z**

SECRETO
1 – 2

SECRETO

COPIA Nº .... de ..... Copias
IOCE
II DE
LIMA
NOV 98
XY – S

P I E Z A 8 – 1
(Continuación)

En vigencia: Día "D"

FECHAS		A B C D E	F G H I J K	L M N O P	Q R S T	U V X Y Z
D HORA:0700	1	S V Y Z B	D F A C E L	X U P T M	R K G Q	N I J H G
	2	U Z K L O	X N I V Y J	M Q T H E	P S E G	C F B A D
	3	Q F B X I	Y O K H L T	P R U S M	Z N G J	D A C B E
	4	B H I M I	X S C O J Z	A U F D Q	K E R G	P V N L T
	5	G V R J Z	C I Q P U A	M H T B L	S E N K	F Y O D X
D +1 HORA:0700	1	M A G R X	N J Q S F L	V T O K Y	B C I Z	E S U H P
	2	I R M B F	A Y V O K X	D N H E S	P J C T	Z U G Q L
	3	Y L A F B	J R U S N P	Z K D Q C	I K V B	M T X O G
	4	S M U E H	Q C P V X D	N I J F L	A T Z G	K U O B R
	5	C X H M B	T F K A E I	V R O N G	Z U Y L	P S J Q D
D +2 HORA:0700	1	D I A R N	V Y K L H P	Z P M F J	U S E B	C Q O X G
	2	G B L R Y	O J N E A H	P F Z T C	U I X B	V Q M K S
	3	S Y P B L	O G C U Q I	K D B M A	H T J Z	F E M R X
	4	B G P U S	K E I M Z L	Y A O R F	C D V T	X H N Q J
	5	M Q F Z I	O Q D K S Y	R U L N G	B P X V	T H E J C
D +3 HORA:0700	1	B I E M Y	P A C G H K	S T X O Z	J V F R	U N L Q D
	2	L P G U X	C H I E Y V	Z R N K S	F O A B	T J D Q M
	3	G T M L Z	X B A D E I	O Q J U P	H N V Y	S K R C F
	4	T M Z C F	A J U H O D	V K E B N	Q S P Y	I L R X G
	5	Y C M O X	D I Q U R A	E G L N T	Z V B F	J S K H P
		A B C D E	**F G H I J K**	**L M N O P**	**Q R S T**	**U V X Y Z**

Acuse Recibo (Fdo) V BLANCO C

DISTRIBUCION

Es copia
A. Contreras C.

G-2

SECRETO
2 – 2

COPIA Nº .... de ..... Copias
IOCE

II DE
LIMA
NOV 98
XY – 5

P I E Z A 9 - 3

En vigencia: Día “D”

CUADRO PARA EL ARMADO DE CRIPTOGRAFOS

PASADORES POR HUNDIRSE						POSICION DE LOS MONTADORES	
37	41	29	47	43	31	1--3	17--4
						2--1	18--3
01	02	01	03	02	04	3--6	19--4
02	04	03	05	04	06	4--3	20--2
05	07	04	06	08	08	5--2	21--3
06	09	05	08	12	10	6--4	22--5
09	11	08	10	14	11	7--3	23--4
11	14	11	14	16	12	8--5	24--5
15	18	15	17	17	14	9--1	25--4
17	20	17	20	19	18	10--4	26--5
19	24	19	22	21	20	11--3	27--2
20	25	21	24	23	21	12--2	28--6
21	27	25	26	26	23	13--4	29--3
25	29	28	30	28	26	14--3	30--2
28	33	--	32	31	29	15--5	31--1
33	36	--	34	33	31	16--1	32--2
37	37	--	36	34	--		
--	38	--	38	38	--		
--	40	--	39	41	--		
--	41	--	40	43	--		
--	--	--	42	--	--		
--	--	--	44	--	--		
--	--	--	47	--	--		

V E R I F I C A C I O N

EBNFA	SICBS	GSLKU	VCGUV	MOPOB	ASPYR	GKITM	HMOHW
KEUWT	ZFXXQ	HOGBO	YURDT	TKWNH	ECBLH	MEFUS	LDYJF
CVZGE	YNAVK	WMGG	WRAW				

Acuse Recibo

(Fdo) V BLANCO C
Gral Cmdte Gral

DISTRIBUCION

Es copia
A. Contreras C.
G-3
SECRETO
1 – 1
SECRETO

COPIA Nº
IOCE
II DE

LIMA
NOV 98
XY – 5

P I E Z A 10 - 3

En vigencia: Día "D"

LISTA DE LLAVES

CLAVE		DISCOS CLAVE	CLAVE		DISCOS CLAVE	CLAVE		DISCOS CLAVE	CLAVE		DISCOS CLAVE
ZAQ	:	PQOEIT	AZQ	:	QRWEUT	QAZ	:	WTRJOY	ZQA	:	IQWERU
AQZ	:	QUWTRO	QZA	:	TQREW	XSW	:	OIYURE	WSX	:	EPQOY
WXS	:	YQEOT	SXW	:	O	SWX	:	QUIOWR	XWS	:	YOUIPR
CDE	:	QTREWU	EDC	:	RPOIUW	ECD	:	TIOPYU	DEC	:	IOTYEW
CED	:	TQWOR	DEC	:	YPOIIEQ	RFV	:	EQRWIT	VER	:	QIUOWR
FRV	:	ALKSHJ	VRF	:	OPUITY	FRV	:	KLHJFG	RVF	:	GFDSAL
TGB	:	JHGFAS	GBT	:	SAFDGH	BTG	:	LAKSJD	TBG	:	GJHKLD
BGT	:	AFGDJK	GTB	:	JLGHSD	YHN	:	HJKLSD	HYN	:	HDSAKJ
NHY	:	KHGFDL	HNY	:	DJKLGH	YNH	:	AFGHKS	NYH	:	DHFKLA
UJN	:	GJDFLK	JUM	:	AFJHGS	MJU	:	DSQLHK	UMJ	:	HKJGFD
KLI	:	ZXCVBN	MUJ	:	LHJADF	IKL	:	VBCZXM	LKI	:	XCZNBV
OPI	:	ZMXNVC	ILK	:	BMNVCX	LIK	:	VNCMXZ	KIL	:	CVBXNM
POL	:	CVNBMX	PLO	:	ECBVMN	LPO	:	CZXRTY	OLP	:	HGFBVU
FGE	:	PKMJIN	JOP	:	QEWADS	QWA	:	POKMID	ASZ	:	BJFHTO
PNE	:	LIKHYR	GQW	:	JKTBVC	GCW	:	OILUJM	TVD	:	HTBGVF
JED	:	BGERDV	LKJ	:	C	LGW	:	OYKDHA	MIN	:	UBTCRZ
PEO	:	BDMHLI	AGC	:	YEHDNC	ILU	:	MQKLDY	YVF	:	GARCEX
HJR	:	QLMHBD	TYB	:	NWKOPS	NEF	:	UHIDRC	IRV	:	RAEWCX
OUK	:	LXODLR	RBZ	:	ZSXAEU	BCU	:	QECXTH	LUN	:	ZRGFTW
HNK	:	WXSUBI	KUV	:	IOKLHJ	MJE	:	TGBCJE	OLY	:	VQTMIL
UJC	:	PTISVE	MKE	:	LFINKC	UND	:	OPUIKG	UAN	:	ZIOCUY
AOF	:	RAWSDK	CXR	:	OTUBHD	COR	:	UHZUCL	JKR	:	XUBMVO
LFK	:	PNKMVB	CKJ	:	PEFGYV	INB	:	LXBVCW	SAK	:	XUJKNB
MQW	:	CPIOKD	QCR	:	WYCVOP	IGE	:	LKMVGA	IKB	:	ITUYNH
JDS	:	ZJAHFL	OMY	:	BMKYSP NEBAZO KIROQH	LAI	:	UVREQI	BEG	:	WFCIOX

Acuse Recibo

(Fdo) V BLANCO C
Gral Cmdte Gral

DISTRIBUCION

Es copia
A. Contreras C.
G-3
SECRETO
1 – 1

COPIA Nº .... de ..... Copias
IOCE
II DE .....
LIMA
NOV 98
XY – 5

P I E Z A 11 - 1

En vigencia: Día “D”

CODIGO DE PAINELES

1. Reconocimiento de Unidades

UNIDAD	D	D+1	D+3	D+2
Elón Superior	055	041	018	020
ADE	051	043	031	022
CG II DE	004	045	033	024
32 DM ge	014	047	035	026
34 Dmotz	053	049	037	028
Cía Cmdo 112	008	042	039	021
Cía Trasm 112	055	044	032	023
Btn PM 112	007	046	034	025
RCB 112	057	048	036	027
Bing 112	059	050	038	029
B Serv 112	052	002	040	030

2. Mensajes en Clave

SIGNIFICADO	CODIFICADO
LIMITE ZONA ROJAS	70
CONTINUAMOS AVANCE	71
AVIACION AZUL ACTIVA	72
REQUIERESE ARTILLERIA ALARGUE FUEGOS	73
OBJETIVOS BATIDOS	74
REPITA SU MENSAJE	75
HAY PERSONAL POR EVACUAR	76
ZONA ATERRIZAJE AVIONES	77
ZONA ATERRIZAJE HELICOPTEROS	78
URGENTE ENVIAR EQUIPO RADIO	79
DISPARE TRAZADORAS ZONA ENEMIGA	80
SOLICITO REPETIR MISION MISMOS OBJETIVOS	81
LIMITE ZONA DE DESEMBARQUE	82

SECRETO

1 – 2

SECRETO

COPIA Nº .... de ..... Copias
IOCE
II DE .....
LIMA
NOV 98
XY – 5

P I E Z A 11 - 1

En vigencia: Día “D”

CODIGO DE PAINELES

3. Código de Colores

a. IDENTIFICACION DE LA COLUMNA DE VEHICULOS

Vehículos	**D**	**D+1**	**D+2**	**D+3**
1º y último C/M Vehículos	ROJO NARANJA	VERDE NARANJA	NARANJA NARANJA	AZUL NARANJA
Peruanos	BLANCO	BLANCO	ROJO	ROJO

Acuse Recibo

(Fdo) V BLANCO C
Gral Cmdte Gral

DISTRIBUCION:

Es copia
A. Contreras C.
G-3

SECRETO
2 - 2

ANEXO 4. DEFINICION DE TERMINOS

1. ANALISIS DE TRAFICO

Es la técnica que permite obtener información sobre el enemigo mediante el estudio y evaluación de los procedimientos de explotación de radiotelefonía y radiotelegrafía.

2. CONTRAINTELIGENCIA

Es la actividad destinada a contrarrestar la inteligencia enemiga, engañar, prevenir adecuada y oportunamente para impedir se obtengan informaciones sobre nuestra situación, permitiendo al Comando a Actuar por sorpresa y prevenir contra el sabotaje y subversión; las actividades que comprende son:

(1) Seguridad Militar.
(2) Seguridad Civil.
(3) Seguridad de Puentes.
(4) Censura.
(5) Actividades especiales.

3. CONCEPTO DE SEGURIDAD

Estado de confianza y tranquilidad de una persona o grupo humano basado en el convencimiento que no hay ningún peligro y riesgo de temer, después de haber adoptado una serie de medidas o normas que eliminan todos los riesgos que se presenten.

4. ESCUCHA

Es la actividad de recepción que se realiza para obtener la información que contiene los mensajes cursados por el enemigo.

5. FUENTE DE INFORMACIONES

Es el personal, documento, actividad, local y objeto de la cual se obtiene informaciones.

6. GUERRA ELECTRONICA

La guerra electrónica es un proceso que consiste en acciones electromagnéticas activas y pasivas destinadas a conocer, inicialmente, como actúa el adversario en el espectro electromagnético. Sobre la base anterior definir las acciones y medios

necesarios con la finalidad de negar al enemigo, el uso libre y efectivo del espectro electromagnético, dificultando o anulando sus comunicaciones y el control de sus armas, y al mismo tiempo mediante acciones activas y usos de equipos electromagnéticos facilitarnos el empleo del espectro electromagnético, reduciendo o previniendo las acciones del enemigo.

7. INFORMACION Y SEGURIDAD

La seguridad descansa en la INFORMACION (que tenemos del enemigo y en la información que de nosotros negamos al mismo), en el dispositivo (que nos cubre del riesgo de acciones físicas del enemigo) y en otros elementos.

La seguridad al cubrirnos de todo riesgo, nos da libertad de acción.

Las comunicaciones constituyen una fuente de informaciones por ello el enemigo trata de interceptar nuestras comunicaciones para obtener informaciones y a su vez intenta penetrar en nuestra red para enviar mensajes falsos, así mismo intentarían destruir nuestros equipos o interferirlos.

8. INFORMACION MILITAR

Todo documento, hecho, acto, material diverso, fotografía diagrama, cartas, que sirva para conocer al enemigo al terreno y a las condiciones meteorológicas de la zona de operaciones.

9. INTELIGENCIA

Es la información procesada mediante el registro, la evaluación y la interpretación de la información disponible.

10. INTELIGENCIA DE COMUNICACIONES

Es el resultado del procesamiento de la información obtenida de las comunicaciones del enemigo, en base a la Información Técnica (frecuencias, tipo de señal, horario) que proporciona los elementos de Comunicaciones a los elementos de inteligencia de una fuerza.

11. INTELIGENCIA MILITAR

La Inteligencia Militar es el conocimiento de las posibilidades, vulnerabilidades y probables formas de acción de los enemigos externos e internos, actuales o probables, así como de la zona de operaciones, obtenida mediante la búsqueda y procesamiento de las informaciones disponibles, y que es utilizado para el planeamiento, preparación y conducción de las operaciones militares.

12. INTERCEPTACION

Es la actividad que consiste en una constante vigilancia del espectro electromagnético, para determinar la existencia y características radioeléctricas y físicas de las emisiones electromagnéticas que está produciendo el enemigo.

13. INTERFERENCIA DE COMUNICACIONES

Es cualquier energía no deseable que tienda a impedir o dificultar nuestras comunicaciones, y que puedan provenir del enemigo o de nuestros propios fuegos.

14. MATERIAL CLASIFICADO

Documento, material o equipo, cuyo conocimiento, utilización y/o empleo, sólo es permitido al personal debidamente autorizado.

15. MEDIDAS DE APOYO DE GUERRA ELECTRONICA

Es aquella parte de la Guerra Electrónica que comprende las acciones destinadas a buscar, interceptar, localizar e identificar energía electromagnética radiada con el fin de reconocer de inmediato la amenaza. Las medidas de apoyo electrónico constituye una fuente de información para realizar acciones de contramedidas electrónicas, así como el empleo táctico de fuerzas y recursos.

16. ORDEN DE BATALLA

Este término se aplica a un DOCUMENTO ESPECIAL DE SEGURIDAD, que contiene información sobre nuestras propias fuerzas, aliadas, o del enemigo y que comprende:

(1) Identificación de unidades.
(2) Dispositivo.
(3) Fuerza.
(4) Organización.
(5) Doctrina y Procedimientos Tácticos.
(6) Personalidades militares.
(7) Eficiencia combativa.
(8) Historial de las unidades.

17. RADIOLOCALIZACION

Es la actividad que permite determinar la ubicación geográfica desde donde se originan las emisiones electromagnéticas del enemigo.

18. RADIOVIGILANCIA

Búsqueda y detección de emisiones enemigas, procedentes de equipos de comunicaciones enemigos o amigos.

19. SEGURIDAD DE COMUNICACIONES

La Seguridad de Comunicaciones consiste en todas aquellas acciones destinadas a proteger a nuestras comunicaciones, fundamentalmente negando información de valor a toda persona no autorizada, de manera que no pueda derivar informaciones para el estudio de nuestras telecomunicaciones, o en el peor de los casos se confunda con la interpretación de tales informaciones.

20. SEGURIDAD MILITAR

Estado de confianza y tranquilidad del jefe y demás integrantes de una unidad, instalación o dependencia militar y del área de su responsabilidad, que se hace en el convencimiento de que no hay ningún peligro de temer, al haberse adoptado las medidas necesarias para evitar todo riesgo en el personal, la información, las instalaciones, el material y el equipo.

21. TEXTO CIFRADO

Se llama texto cifrado criptografiado a una serie de signos o grupo de signos, la mayor parte de las veces letras o cifras de apariencia inteligibles que presentan un carácter secreto.

22. TEXTO CLARO

Se llama texto en claro, a un texto escrito en idioma corriente Español o Extranjero.