REPUBLICA DEL ECUADOR

SECRETARIA GENERAL DEL CONSEJO DE SEGURIDAD NACIONAL

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

TRABAJO DE INVESTIGACION INDIVIDUAL
MAESTRIA EN SEGURIDAD Y DESARROLLO CON MENCION EN GESTION PUBLICA Y GERENCIA EMPRESARIAL

LA EVOLUCION CIENTIFICA Y TECNOLOGICA DE LA FUERZA TERRESTRE Y SU INFLUENCIA EN LA SEGURIDAD NACIONAL.

CRNL. EMC. CARLOS PROCEL S.

XXVIII CURSO

2000-2001

REPUBLICA DEL ECUADOR

SECRETARIA DEL CONSEJO DE SEGURIDAD NACIONAL

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

TRABAJO DE INVESTIGACION INDIVIDUAL

MAESTRIA EN SEGURIDAD Y DESARROLLO CON MENCION EN GESTION PUBLICA Y GERENCIA EMPRESARIAL

LA EVOLUCION CIENTIFICA Y TECNOLOGICA DE LA FUERZA TERRESTRE Y SU INFLUENCIA EN LA SEGURIDAD DEL ESTADO ECUATORIANO.

CRNL. EMC. ING. CARLOS PROCEL S.

XXVIII CURSO

2000-2001

DEDICATORIA

A mi esposa e hijos, por su comprensión y apoyo a este proceso de capacitación profesional.

Al Instituto de Altos Estudios Nacionales (IAEN) que con su Programa de Maestría en Seguridad y Desarrollo, nos ha permitido redefinir nuestro rol en la sociedad, pasando a ser profesionales críticos, capaces de plantear soluciones viables y oportunas a los problemas de seguridad y desarrollo que tiene nuestro país.

AGRADECIMIENTO

Al Sr. Economista Vicente Aguilera, Director de Tesis, por el invalorable esfuerzo desplegado en la asesoría del presente trabajo.

A los Sres. Directivos y Asesores de la Institución, que con sacrificio y esmero dedican todo su tiempo a la capacitación y preparación de quienes creemos en nuestro país.

INDICE GENERAL

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO I

INTRODUCCION

1. LEYES Y REGLAMENTOS

1.1. Constitución Política de la República del Ecuador

La República del Ecuador, fiel a sus orígenes históricos y decidida a progresar en la realización de su destino, en nombre de su pueblo, invoca la protección de Dios y se organiza fundamentalmente por medio de esta Constitución política.

Todas las instituciones públicas, se han creado y organizado bajo las disposiciones de la Constitución Política del Estado, y en la parte relacionada a la Fuerza Pública establece:

Art. 183.- La Fuerza Pública estará constituida por las Fuerzas Armadas y la Policía Nacional. Su misión, organización, preparación, empleo y control serán regulados por la ley.

Las Fuerzas Armadas tendrán como misión fundamental la conservación de la soberanía nacional, la defensa de la integridad e independencia del Estado y la garantía de su ordenamiento jurídico. Además de las Fuerzas Armadas permanentes, se organizarán fuerzas de reserva, según las necesidades de la seguridad nacional.

La Policía Nacional tendrá como misión fundamental garantizar la seguridad y el orden públicos. Constituirá fuerza auxiliar de las Fuerzas bajo la supervisión, evaluación y control del Consejo Nacional de Policía, cuya organización y funciones se regularán en la ley.

Art. 184.- La fuerza pública se debe la Estado. El Presidente de la República será su máxima autoridad y podrá delegarla en caso de

emergencia nacional, de acuerdo con la ley.

El mando Militar y Policial se ejercerán de acuerdo con la ley.

Art. 189.- El Consejo de Seguridad Nacional, cuya organización y funciones se regularán en la ley, será el organismo superior responsable de la defensa nacional, con la cual, los ecuatorianos y los residentes extranjeros estarán obligados a cooperar.

1.2. Ley de Seguridad Nacional

Art. 1.- La Seguridad Nacional del Ecuador, es responsabilidad del Estado.

Art. 2.- El Estado garantiza la supervivencia de la colectividad, la defensa del patrimonio nacional y la consecución y mantenimiento de los objetivos nacionales y, tiene la función primordial de fortalecer la unidad nacional, asegurar la vigencia de los derechos fundamentales del hombre y promover el progreso económico, social y cultural de sus habitantes, contrarrestando los factores adversos internos y externos por medio de las previsiones y acciones políticas, económicas, sociales y militares.

Art. 3.- Los ecuatorianos y los extranjeros en el territorio nacional, sean personas naturales o jurídicas son responsables y están obligados a cooperar por la seguridad nacional en la defensa de la soberanía e integridad territorial, con el Consejo de Seguridad Nacional y el Comando Conjunto de las Fuerzas Armadas, en la forma y condiciones determinadas en ésta y demás leyes.

1.3. Ley Orgánica de las Fuerzas Armadas

Art. 1.- La presente ley determina la misión y organización de las Fuerzas Armadas, así como las atribuciones principales de los organismos que las constituyen, al mismo tiempo que establece la relación de mando y

subordinación entre sus componentes.

Art. 2.- Las Fuerzas Armadas nacionales constituyen el principal instrumento de acción del Frente Militar.

Tiene como misión:

a. Mantener la soberanía nacional y garantizar la seguridad interna y externa del Estado,

b. Respetar y hacer respetar las leyes de la República,

c. Participar en el fortalecimiento del poder Nacional, para la consecución y mantenimiento de los Objetivos Nacionales Permanentes; y,

d. Participar en el desarrollo socio económico del país.

Art. 3. Las Fuerzas Armadas están constituidas por:

Fuerza Terrestre,

a. Fuerza Naval, y,

b. Fuerza Aérea.

Los efectivos de las Fuerzas Armadas estarán comprendidos por:

a. Fuerzas Permanentes, y,

b. Reservas.

Art. 4.- Los Organismos Superiores de las Fuerzas Armadas son:

a. Presidencia de la República: Comandante en Jefe de las Fuerzas Armadas,

b. Ministerio de Defensa Nacional,

c. Comando Conjunto de las Fuerzas Armadas,

d. Comando General de la Fuerza Terrestre,

e. Comando General de la Fuerza Naval,

f. Comando General de la Fuerza Aérea.

Art. 5.- Las Fuerzas Armadas Permanentes estarán constituidas por:

a. Oficiales, Aspirantes a Oficiales, Voluntarios, Aspirantes a Voluntarios y Conscriptos, inclusive las siete últimas levas licenciadas, Empleados Civiles y Especialistas Contratados.

Art. 6.- Para cumplir con la misión de las Fuerzas Armadas, la Fuerza Terrestre tiene como tareas: organizar, preparar y desarrollar el Poder Militar de acuerdo con la planificación prevista para tiempo de paz y de conflicto.

2. ORGANISMOS DE LA FUERZA TERRESTRE:

a. Operativos,

b. Administrativos, de Apoyo y de Desarrollo,

c. De Asesoramiento,

d. De Formación, Investigación y Perfeccionamiento.

Los organismos operativos son:

- ✓ Comando General de la Fuerza Terrestre,
- ✓ Unidades operativas mayores,
- ✓ Unidades operativas menores,

- ✓ Unidades tácticas especiales.

3. MISIÓN DE LA FUERZA TERRESTRE

La Fuerza Terrestre como parte de las Fuerzas Armadas participa de las siguientes misiones: conservar la Soberanía Nacional; defender la Integridad e Independencia del Estado ecuatoriano; garantizar el Ordenamiento Jurídico del Estado; colaborar en el Desarrollo Social y Económico del país, empleando sus recursos humanos y materiales, particularmente en actividades y áreas de carácter estratégico; y, colaborar e intervenir en los demás aspectos concernientes a la Seguridad Nacional, de acuerdo con la ley.

Además es responsable de: organizar, entrenar, equipar y mantener el Poder Militar Terrestre, así como participar en los procesos que garanticen la seguridad de la Nación y propender a su desarrollo con la finalidad de contribuir a la consecución y mantenimiento de los Objetivos Nacionales Permanentes, contemplados en la Constitución Política de la República, de acuerdo a la planificación prevista para tiempos de paz, de conflicto y de guerra.

4. ORGANIZACIÓN DE LA FUERZA TERRESTRE

La Estructura Organizacional de la Fuerza Terrestre, permite alcanzar los objetivos propuestos por el mando y el cumplimiento de las misiones de Seguridad y Desarrollo a ella encomendadas; para el efecto se han determinado políticas y normas que regulan su organización, con la finalidad de delimitar la línea de mando, autoridad, responsabilidad y subordinación de la dependencia orgánica. Esto facilita las coordinaciones horizontales y verticales para un mejor cumplimiento de las tareas prescritas y deducidas

en todos los campos.

En función de los preceptos establecidos en la Misión para la Fuerza Terrestre se ha establecido su Organización Estructural como se muestra en la Ilustración No 1.1.

En esta Organización se tienen diferentes Organos, siendo uno de ellos el Organo de Formación, Investigación y Perfeccionamiento, cuya misión es ñsatisfacer las necesidades de reclutamiento, capacitación, perfeccionamiento e investigación de la Fuerza Terrestreò

Otro de los órganos importantes es el de carácter Operativo, cuya misión es, permitir desde tiempo de paz, la preparación y el empleo, para cumplir con la Planificación Militar en la neutralización de los conflictos y la ejecución de la Guerra.

5. OBJETIVOS DE LA FUERZA TERRESTRE.

5.1. De Seguridad Externa:

- ✓ Desarrollar el Poder Militar,
- ✓ Planificar y ejecutar la Defensa Terrestre, en el marco de conducción del COMACO, en coordinación con las otras Fuerzas, Fuerzas Paramilitares y Defensa Civil,
- ✓ Emplear el Poder Militar Terrestre y mantener el esfuerzo de guerra.

5.2. De Seguridad Interna:

- ✓ Adecuar el Poder Militar a las necesidades de la Defensa Interna,
- ✓ Emplear el Poder Militar Terrestre como medio de solución de conflictos internos,

- ✓ Planificar y ejecutar la Defensa Interna en el marco de la conducción del COMACO en forma integrada con las Fuerza Paramilitares y Defensa Civil.

5.3. De Desarrollo:

- ✓ Desarrollar la Industria Militar,
- ✓ Contribuir al desarrollo de áreas estratégicas,
- ✓ Colaborar con el desarrollo industrial del país en áreas de interés, Estratégico-Militar, y,
- ✓ Desarrollar la Investigación Científica y Tecnológica en áreas del interés militar, que contribuyan además con el desarrollo del país.

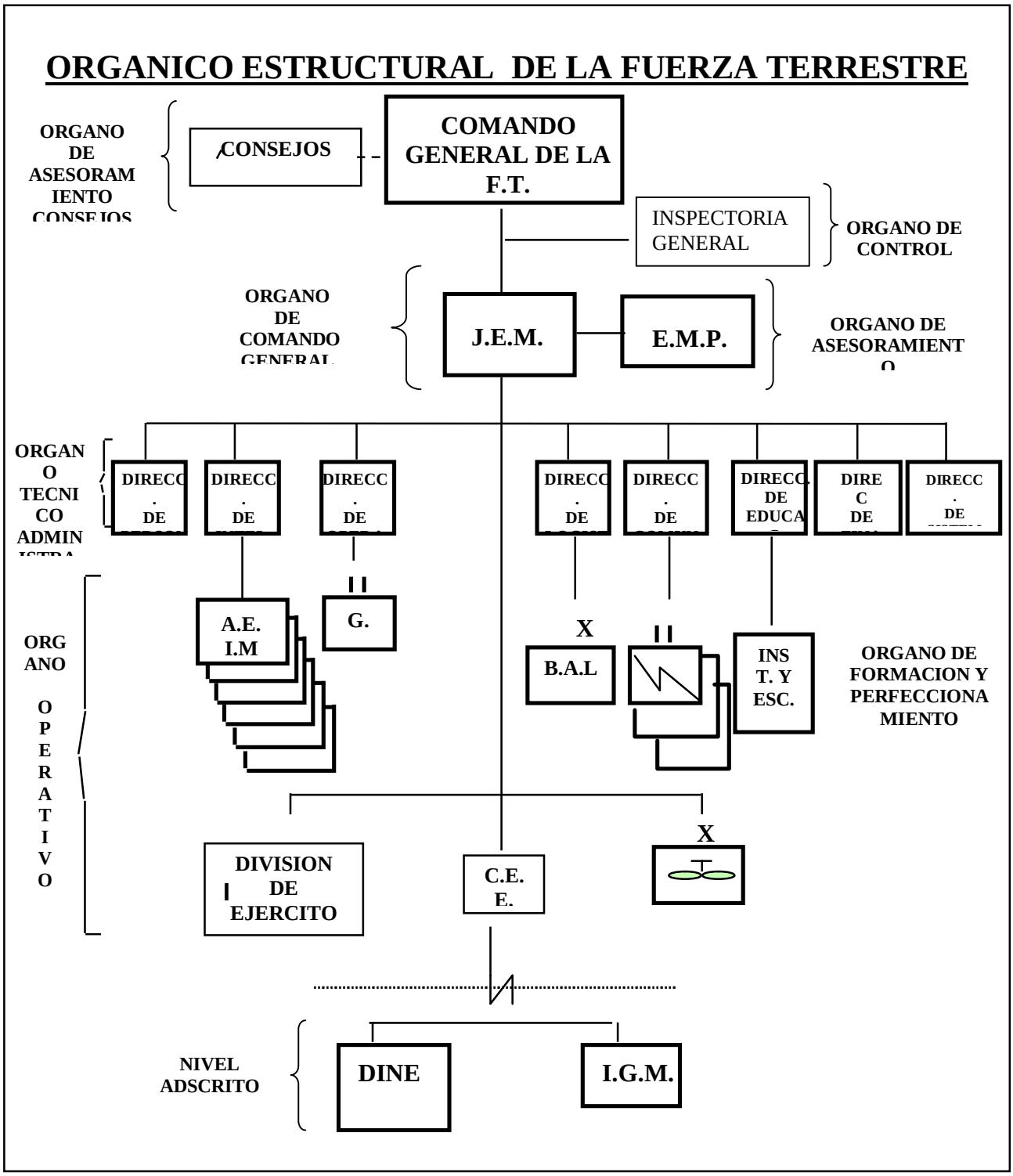


Ilustración No 1.1. Orgánico Estructural de la Fuerza Terrestre

CAPITULO II

EVOLUCION CIENTÍFICA Y TECNOLOGICA DE LA FUERZA TERRESTRE

1. ANTECEDENTES

El vertiginoso avance de la Ciencia y la Tecnología y su impacto en todos los ámbitos de la vida moderna, especialmente en lo relacionado a la industria militar, ha exigido a las FFAA ecuatorianas y en particular a la Fuerza Terrestre que se organice y se desarrolle para sustentar y estar acorde con dichos avances, con la finalidad de cumplir a cabalidad su misión fundamental de Seguridad y Desarrollo del Estado ecuatoriano.

En este contexto, la Fuerza Terrestre en cumplimiento de su misión, no podía abstraerse de estar involucrada en este incesante avance del mundo contemporáneo. Es así como durante su larga y fructífera trayectoria ha sido en muchos casos la pionera en el desarrollo científico e implementación tecnológica en nuestro país, iniciándose prácticamente en los albores de la década de los años cuarenta, adquiriendo mayor relevancia en la década de los años setenta, época en la que esta gloriosa institución de las FFAA alcanza un apoyo importantísimo para modernizar su equipo y armamento en campos específicos de acuerdo a las necesidades y amenazas internas y externas.

2. DESARROLLO TECNOLOGICO DE LAS UNIDADES Y ORGANISMOS DE LA F.T.

2.2. Caballería Blindada

El arma de Caballería Blindada, como se la conoce hoy en día, ha tenido una serie de etapas de desarrollo como especialidad misma y, dentro de esta, es importante resaltar el desarrollo tecnológico alcanzado dentro de sus filas por los técnicos que han

apoyado permanentemente la operación de la maquinaria militar en dotación de las Fuerzas Blindadas desde su origen como tales hasta la actualidad.

Haciendo un poco de historia, cabe trasladarse a los inicios de esta Arma de la Fuerza Terrestre en nuestro país, los que prácticamente se remontan al año de 1942, cuando al país llegan los tanques Marmon Harrington que fueron comprados a los EE.UU., iniciándose desde ese tiempo el trabajo de los mecánicos que se requerían para mantener el material. Las Fuerzas Blindadas se siguen desarrollando como Arma, conformando las diferentes Unidades y ocupando diferentes guarniciones en varias provincias del País. Posteriormente, por los años de 1960, es cuando arriban los tanques americanos M3A1 en una cantidad pequeña de 20 unidades, además de una serie de vehículos semioruga y otros con protección de blindaje exterior. Esto motiva a que se conformen mayores y mejor entrenados equipos de mantenimiento en las Fuerzas Blindadas, ubicadas en Playas y Quito.

En los años de 1969, luego de transcurrida casi una década, se adquieren los vehículos blindados M113 APC de fabricación americana que también en una cantidad de veinte, pasan a reforzar la capacidad de las Fuerzas Blindadas de aquel entonces. Con las experiencias de mantenimiento obtenidas, se consolidan equipos que son enviados a un curso de entrenamiento en operación y mantenimiento de estos últimos vehículos a la Escuela de las Américas en Panamá.

A partir de esta experiencia, van tomando mayor relevancia los trabajos de mantenimiento blindado, y el personal progresivamente se va especializando a través de la transferencia de tecnología que se consigue por los diferentes cursos y posteriormente con la llegada de nuevo material Francés que inicia su arribo con los vehículos AML-60, equipados con un

mortero de 60 mm. y AML-90 equipados con un cañón de 90 mm., los que llegan al país a partir del año de 1971.

El arribo del material Francés, comienza a marcar un nuevo hito en el desarrollo tecnológico de las Fuerzas Blindadas, pues, con él, llegan una cantidad importante de técnicos franceses, los mismos que conforman un grupo de asistencia técnica de entrenamiento en la operación, uso del material y su mantenimiento en los diferentes escalones. Con la adquisición del material blindado AMX-13 que se inicia a partir de 1972 hasta 1977, se consolida esta asistencia que por el lapso de cuatro años (hasta 1974), capacita al personal de conductores, artilleros, personal de comunicaciones, tripulaciones y personal de mantenimiento de las diferentes especialidades.

En estos cuatro años, nuestro personal viaja a realizar cursos de capacitación en Francia y posteriormente, a través de variados cursos y la asistencia francesa en el Ecuador, se multiplican aquellos en la Brigada Blindada No.1 ñGalápagosò, que luego, a partir de Febrero de 1974, pasa a constituirse en la Brigada Blindada No.11 ñGalápagosò en la Ciudad de Riobamba.

Se comienzan a distinguir y se crean los conceptos de los niveles de mantenimiento blindado, habiéndose realizado hasta ese entonces, únicamente el mantenimiento preventivo de I y II escalón, es decir el mantenimiento orgánico de las Unidades en los talleres creados en cada una de ellas.

A partir del año 1978, se conforma una llamada ñMisión Francesaò, la que con seis técnicos, y durante tres años, dictan sus cursos de mantenimiento de III y IV escalón a nuestro personal de mecánicos dando lugar a la creación del Taller de Mantenimiento de III y IV escalón blindado bajo el control del CAL-11 de la Brigada.

A partir de este año, con la permanencia de dos técnicos franceses

supervisores de los trabajos, los mismos que actuaban como enlace con los fabricantes, nuestro personal sigue multiplicando los cursos dictados de mantenimiento y va progresivamente adquiriendo mayores experiencias en la reparación de los equipos de dotación en la Brigada Blindada; siguiendo, por supuesto todas las indicaciones establecidas en los manuales de operación y mantenimiento entregados por los fabricantes para el efecto. Conforme pasan los años, se hace notorio el deterioro que va sufriendo el material, especialmente en su sistema motriz, conformado básicamente por un motor a gasolina marca "SOFAM", lo que incrementa la necesidad de mantenimiento correctivo y los daños comienzan a ser cada vez mas frecuentes, significando mayores egresos de recursos económicos y la consiguiente inhabilitación de los vehículos blindados.

Insertando la historia en esta investigación, es importante resaltar que a partir del 29 de Agosto de 1985, el Comando General del Ejército, dispone la fusión de las dos armas de Caballería y de Fuerzas Blindadas, pasando a conformar desde ese momento, la Caballería Blindada.

En los años siguientes y dadas las situaciones de tensión que se vivían con el vecino país del Sur, se resuelve dar paso a una modernización del material blindado, para recuperar sus capacidades e incrementar su efectividad. Para el efecto, se decide iniciar con la modernización del sistema de tiro, el que llega a ejecutarse en el año de 1990. Esta modernización consistía en incorporar a la torre de los vehículos blindados AMX-13 con cañón de 105 mm., un sistema de telemetría lasérico, adicionando un computador de tiro que se encarga de realizar los cálculos y corrección del tiro, optimizando la efectividad de los disparos sobre el objetivo a un 97%.

Estos trabajos, permiten que el personal especializado de torre, alcance un mayor nivel de capacitación; muy a pesar, de que en este módulo no se transfiere adecuadamente toda la tecnología referida a la electrónica

de los equipos nuevos instalados.

Casi paralelamente con la ejecución de este trabajo en la Brigada Blindada, se inicia un trabajo de investigación por parte de la Facultad de Ingeniería Mecánica de la ESPE. El objetivo de este: buscar una alternativa de solución a los problemas que aquejaban a los tanques en su sistema motriz y que obligaban a una actividad muy grande en los trabajos de IV escalón de mantenimiento, debido al requerimiento continuo de reemplazo de los motores y otros sistemas a fin de mantener operable el parque blindado.

Algunos países, entre ellos Francia, a través de varias firmas, presentaron opciones de repotenciación para los vehículos blindados, una de ellas probada sobre rutas ecuatorianas (la opción Francesa) y que no presentó resultados positivos.

Los trabajos de desarrollo de la unidad prototipo por parte de la ESPE, se concluyen en el año de 1990.

Este trabajo se apoyó en la colaboración de los talleres del Cuerpo de Ingenieros del Ejército y se ejecutó con auspicio económico de la Empresa Privada, en base a convenios de inversión de riesgo.

A partir de esta fecha, se vuelve a marcar otro hito en el desarrollo tecnológico de las Fuerzas Blindadas, en razón de que el mando militar decide aprobar la ejecución en serie de la remotorización de los vehículos blindados, trabajo que sería ejecutado por técnicos ecuatorianos de la Brigada Blindada, aprovechando sus instalaciones a las que se realizaron ciertos cambios, implementando además, la maquinaria y herramientas necesarias para el efecto.

A finales de 1991, se inicia con la selección del personal de voluntarios que laborarían en el taller de mantenimiento de IV escalón del CAL-11. La

base de la selección, se fundamentaba en la experiencia que disponía el personal de las diferentes Unidades como mecánicos de vehículos blindados.

Seguidamente, y en base a los requerimientos del trabajo que se ejecutaría, se capacita al personal seleccionado, utilizando la unidad prototipo como patrón de enseñanza del proceso. Se desarrollan los planos de fabricación y los diagramas de montaje, así como los diagramas de proceso, para que los trabajos tengan la secuencia y continuidad que permitan ejecutar un proceso de fabricación y montaje en serie, con equipos móviles de trabajo y puestos fijos de producción en razón de que el proceso tuvo que adaptarse a la infraestructura física existente.

La experiencia que progresivamente ha alcanzado el personal de mantenimiento, con la ejecución de los diferentes trabajos que involucró el proceso de la remotorización, ha permitido que se adquiera mayor destreza y habilidad en la realización de nuevos desarrollos de los prototipos que se requirieron para ejecutar los trabajos de repotenciación en los diferentes tipos de vehículos que conforman la familia AMX-13 de dotación en la 11-BCB ñGalápagosò

Luego de que este desarrollo fuera sometido a la aprobación del Mando, se dispone la ejecución del proyecto de remotorización de todos los vehículos blindados AMX-13 que dispone la Fuerza Terrestre, entre los que se encuentran:

- ✓ AMX-13 105 (cañón de 105 mm.),
- ✓ AMX-13 155 (Artillería autopropulsada de 155 mm.),
- ✓ AMX-13 RATAC (Radar Táctico),
- ✓ AMX-13 PC (Puesto de mando),

- ✓ AMX-13 PM (Porta-morteros),
- ✓ AMX-13 VCI (Transporte de tropas),
- ✓ AMX-13 M-55 (Vehículo Recuperador)

Los objetivos trazados para la ejecución de este proyecto, fueron entre otros:

- ✓ Prolongar sustancialmente la vida útil del material blindado,
- ✓ Obtener gran confiabilidad de funcionamiento bajo condiciones climáticas y de operación extremas, cumpliendo con normas militares internacionales,
- ✓ Montaje de un nuevo sistema motriz a diesel de última generación y de uso comercial, a fin de facilitar la provisión de repuestos en el mercado local,
- ✓ Mejorar la performance de los vehículos blindados, asegurando mayor capacidad de sobrepasamiento de obstáculos, incremento de velocidad y mayor autonomía.

Estos objetivos se alcanzaron con la incorporación de un sistema motriz de fabricación alemana marca DEUTZ, el mismo que dota al vehículo blindado de las siguientes características:

CUADRO COMPARATIVO DE CARACTERÍSTICAS OPERACIONALES DEL VEHÍCULO BLINDADO AMX-13 LUEGO DE LA REPOTENCIACIÓN.

CARACTERÍSTICAS	MOTOR A GASOLINA	MOTOR DIESEL
MARCA	SOFAM	DUTZ

POTENCIA EFECTIVA	193 HP a 3200 rpm	258 HP a 3200 rpm
TORQUE DEL MOTOR AL EJE	63 Kgm. a 2000 rpm	68 Kgm a 1700 rpm.
VELOCIDAD MAXIMA DEL VEHICULO	23 Km/h a 60 Km/h	30 Km/h a 73 Km/h
SUPERACION DE PENDIENTES		
Tanque cañón de 105 mm. (15 Ton.)	60%	80%
Obús autopropulsado 155 mm. (18 Ton.)	44%	60%
Transporte de Tropas (13 Ton.)	62%	85%
Obstáculo vertical	0.65	0.85 m.
RELACIÓN PESO/POTENCIA	13 HP / TON	17.2 HP / TON.
AUTONOMIA:		
Campo Traviesa	200 Km.	500 Km.
En carretera	350 Km.	650 Km.
Horas de operación contínua todo terreno	9 horas	21 horas

Velocidad de crucero	35 Km / h.	50 Km / h.

Las ventajas obtenidas a través de la ejecución de este proyecto, no han sido únicamente técnicas, al haber conseguido la recuperación de un material que por sus condiciones se encontraba en un período de obsolescencia, sino también económicas al permitir ahorrar ingentes recursos; pues, los costos finales del proyecto representaron un tercio de los ofertados por otras firmas extranjeras.

A estos resultados, debemos agregar, la oportunidad de que a través de este proyecto, se ha creado el Centro de Mantenimiento Blindado ñCEMABò, que permitirá a futuro garantizar la conservación de todo el material blindado de la Fuerza Terrestre; habiéndose conformando con un grupo de técnicos militares altamente capacitados para la ejecución de trabajos de IV y V escalón con herramientas, equipamiento y maquinaria moderna; lo que en el futuro facilitará la generación de nuevos proyectos de interés institucional, permitiendo consecuentemente el ahorro de ingentes recursos al país.

El proyecto en mención, se encuentra actualmente ejecutado en un 90 % y hasta mediados del año 2001, se habrá logrado concluir el 100 % de las unidades repotenciadas, devolviendo a la Brigada de Caballería Blindada No. 11 ñGalápagosò la completa operabilidad y capacidad para el cumplimiento de su misión en salvaguarda de la Soberanía Nacional.

Es importante destacar, los beneficios obtenidos con la ejecución de este tipo de proyectos, en los que aparte de ahorrar los recursos económicos que en tiempo de crisis son tan escasos y restringidos, crean alternativas de producción, pues, con la experiencia obtenida a través de estos proyectos y la capacitación lograda por nuestro personal, será posible incursionar en

otras instituciones de nuestro país para ofrecer soluciones a múltiples necesidades relacionadas con nuestro trabajo; presentar alternativas más económicas de solución y coadyuvar a una interrelación y colaboración más estrechas que beneficiarán a todas las partes en conjunto. En la actualidad, se ha iniciado en la investigación para solucionar los problemas que tienen los vehículos de la Artillería que transportan la munición de la Artillería para solucionar su problemática en poco corto plazo, de igual forma se han establecido contactos con las otras Fuerzas a fin de ofrecer nuestros servicios y

La capacidad tecnológica adquirida a través de la ejecución de estos proyectos, ha permitido mejorar las posibilidades de que nuestro personal técnico aporte en mayor grado al desarrollo y tecnificación de Fuerzas Armadas; concluyendo por consecuencia, la necesidad de que los miembros de la Institución, procuren permanentemente orientar su capacitación hacia un mayor profesionalismo y especialización dentro de todos los campos de las Armas, Servicios y Especialidades militares, lo que contribuirá con el engrandecimiento de la Institución y del País.

La confianza y solvencia alcanzadas por el personal de especialistas en material blindado, que conforman actualmente el CEMAB, ha permitido que en la actualidad no solamente se realicen trabajos de mantenimiento blindado, sino que se incursione en otros campos del accionar de la ingeniería mecánica, tales como: repotenciación de camiones tácticos de las Fuerzas Terrestre y Aérea, construcción de equipos y máquinas para las industrias del sector florícola, repotenciaciones vehiculares de la flota de Empresas Municipales (v.g. Proyecto con EMASEO) y otro amplio espectro de trabajos y proyectos especiales de carácter militar y civil.

Esto permitirá que en el futuro la prestación de servicios de nuestros Centros de Mantenimiento amplíe aún mas la participación activa de la Fuerza Terrestre en el convivir nacional con el desarrollo tecnológico

institucional, sin descuidar su misión básica de seguridad del Estado ecuatoriano.

2.2. Comunicaciones.

Una organización, cualquiera sea ésta, no puede desarrollar sus actividades en forma eficiente sin que exista una comunicación adecuada, lo que entendió muy bien el mando de la Fuerza Terrestre, por lo que en la década de los años setenta se inicia el proceso de conformación de una organización que pueda asumir las funciones de planificación y ejecución del proceso de comunicación entre las diferentes unidades que conforman la Fuerza Terrestre, para lo cual se inicia el equipamiento de Comunicaciones, dotándole a dicha organización del medio alámbrico para el cumplimiento de su misión, medio éste que había sido utilizado por todos los Ejércitos de los países desarrollados y que poco a poco se fue haciendo común en los países en desarrollo y por supuesto en el nuestro. Es así como la Fuerza Terrestre se constituye en la pionera en el uso de este medio de comunicación, que sin embargo de ser confiable, no podía enlazar regiones muy distantes y estaba expuesto a que se produzcan fallas por averías físicas en las líneas o a la interceptación por parte del enemigo, lo que exigía un sistema de encriptación de mensajes muy riguroso y una constante vigilancia de la red para disminuir la posibilidad de que se fugue información. Posteriormente y ante el avance tecnológico, la Fuerza Terrestre, se preocupa por la modernización de su sistema de comunicaciones para esa época, insertándose en la transmisión de voz vía radio, utilizando equipos de tecnología analógica que operaban en la banda de HF y VHF, dándole mayor importancia a la primera, logrando establecer la comunicación de voz a las regiones más apartadas de nuestra geografía ecuatoriana, con mejor calidad y confiabilidad respecto al medio alámbrico, dando así la institución armada un paso importante en este campo, constituyéndose en una de las pioneras en el empleo de esta nueva invención tecnológica en el país. Sin embargo, toda nueva invención en el campo de las comunicaciones trae

consigo nuevas formas de poder accesar a la información, utilizando medios no idóneos ya que este medio es susceptible a interceptación, lo que exige sistemas de encriptación más sofisticados y un cuidado extremo, condiciones que se logran gracias al alto grado de capacitación del personal de técnicos y operadores del sistema, quienes paralelamente a la implementación de este, se capacitaron en el país y en el exterior.

Frente a la necesidad de mantenerse actualizados tecnológicamente en lo que a comunicaciones respecta y, con el afán de brindar un servicio de comunicaciones de mejor calidad y más confiable que cubra todo el territorio ecuatoriano, se desarrolla e implementa a finales de los años setenta el sistema de comunicaciones vía microonda (MODE) de tecnología analógica, con terminales a las Unidades tipo Batallón inicialmente y posteriormente a nivel Compañía, para transmisión de voz y datos con medidas de Seguridad Militar (DATOTEK), este último en forma limitada debido a la tecnología con que fue implementada. Esto permitió a las FFAA dar un salto vertiginoso en el uso de la frecuencia que se encuentra en el orden de los GHz. Con la implementación de esta red de carácter administrativa y estratégica se logró contribuir notablemente al mantenimiento de la seguridad de nuestro país, siendo de gran importancia en el conflicto de 1982, ya que permitió a los mandos enviar y obtener información más confiable y de primera mano de cualquier reparto militar.

En el año de 1983, la Fuerza Terrestre, debido a los altos costos que representaban los equipos de comunicaciones con características militares, decide adquirir equipos de radio similares a los anteriores pero con características comerciales, para uso local en las diferentes Unidades Militares, obteniéndose resultados positivos y lográndose solventar la falta de equipo con características militares.

En el año de 1995 y ante la inminencia del conflicto armado con el Perú, se decide implementar un sistema de comunicaciones satelital, que

permitió mantener enlazados a los mandos con las Unidades Operativas, a través de voz y correo electrónico que se comienza a utilizar en la Fuerza Terrestre, en cualquier condición y distancia

Cabe destacar, que a pesar del mantenimiento y el cuidado prestado por los técnicos de las FFAA., la red MODE comenzó a deteriorarse y a presentar fallas continuas debido a la obsolecencia del material y a la falta de repuestos para su reparación, por lo que los mandos conscientes de la necesidad de tener un sistema de comunicaciones seguro y confiable, deciden en el año 1997 se inicie la planificación, el estudio, desarrollo e implementación de un nuevo sistema de comunicaciones que utilizara tecnología de punta, completamente digitalizado y que sirviera para transmisión de voz, datos y video a una velocidad de 128 Kb/s; proyecto este que en pocos meses estará implementado y en explotación. Esto permitirá adentrarnos en el fascinante mundo de las comunicaciones, sin restricciones en el aspecto técnico, con una amplia cobertura en todo el país, lo que permitirá mantener comunicadas a todas las unidades de la Fuerza Terrestre y, garantizar de esta manera el cumplimiento de la misión.

En forma paralela a la implementación de los sistemas de comunicaciones, el mando tomó el cuidado de capacitar al personal encargado de la operación y mantenimiento de los mismos, tanto en el país como en el exterior, teniendo actualmente la Fuerza Terrestre personal altamente capacitado para estos propósitos. De la misma forma se creó el Centro de Apoyo Logístico Electrónico (CALE), organismo encargado de la planificación logística y mantenimiento de las Comunicaciones, lo que ha permitido a la Fuerza cumplir con la misión de seguridad.

2.3. Artillería.

Esta arma de Apoyo a las unidades de la Fuerza Terrestre, ha experimentado un desarrollo tecnológico importante a partir de los años

sesenta, en que fueron adquiridos los primeros cañones de mediano alcance (OBUS de 105 mm), que permitieron proporcionar apoyo efectivo de fuego a las Unidades de Infantería de la Fuerza. Este avance de carácter tecnológico en esta clase de armamento, supuso tener más presencia de carácter disuasivo frente a una amenaza externa, ya que con su poder destructivo podía batir blancos de dimensiones considerables y a una distancia de 12 Km.; esto lógicamente permitía al mando de la Fuerza, tener la convicción de cumplir la misión de Seguridad a ella encomendada.

Con el transcurrir de los años, el desarrollo tecnológico alcanzado por la aviación enemiga, hace que esta se presente como una amenaza constante y peligrosa para nuestro país, puesto que la adquisición de modernas aeronaves con gran poder de destrucción y una considerable autonomía de vuelo, le permitía a esta rama de las FFAA. enemigas, alcanzar objetivos estratégicos en nuestro territorio y destruirlos con relativa facilidad. Ante esta posibilidad cierta, el mando de la Fuerza Terrestre, preocupado por esta amenaza, decide en el año 1977, la adquisición de un Sistema de Defensa Antiaéreo conocido como ñSISTEMA OERLIKONò, el mismo que sería utilizado en la protección antiaérea de las Unidades de Apoyo, Puestos de Mando y Areas Estratégicas de vital importancia para nuestro país..

El sistema en mención está compuesto por un Radar y un subsistema de armas. En lo relacionado al primer componente, este cuenta con tecnología electrónica de punta totalmente digitalizada, que utiliza el principio ñDOPLERò para el Barrido y Detección y para el Seguimiento a través de las antenas de Exploración y Seguimiento respectivamente. Con la capacidad que tiene este subsistema Radar, se puede detectar una aeronave a partir de los 17 Kms. de distancia y mediante el control por medio de una minicomputadora incorporada, se puede establecer automáticamente, en todo instante y bajo cualquier condición meteorológica, datos y parámetros importantes, como distancia, altitud y velocidad de la aeronave que

representa un peligro para nuestras fuerzas de tierra.

En lo relacionado al subsistema de armas, este está compuesto por tubos cañón de 35 mm., de tecnología actualizada, con capacidad de disparo efectivo a una distancia máxima de 4 Km., con una cadencia de tiro de 40 a 60 cartuchos por minuto. Estas armas están controladas totalmente mediante el subsistema Radar, el que mediante los datos obtenidos por la computadora referente a la aeronave enemiga, ordena el inicio de la cadena de fuego. En forma paralela, la Fuerza se preocupó por capacitar al personal de técnicos y operadores encargados del mantenimiento y operación del sistema respectivamente.

En lo que respecta al mantenimiento, el personal de Oficiales y Voluntarios encargados de esta actividad, fueron capacitados tanto en el exterior como en nuestro país, en las áreas de Electrónica y Mecánica, situación esta que permitió realizar la transferencia de tecnología entre los técnicos de la casa fabricante y los de la Fuerza Terrestre, al punto que hoy en día, el 90% del mantenimiento lo realizan los técnicos ecuatorianos, en los talleres del Centro de Mantenimiento de Armas ubicado en la Brigada Logística, permitiéndose con esto un ahorro considerable de recursos para nuestro país.

Posteriormente, debido a la necesidad imperiosa de contar con un material de tiro parabólico de gran alcance, y mayor poder de destrucción, la Fuerza Terrestre adquiere el sistema BM-21 de fabricación Rusa, el mismo que si bien no es de tecnología de punta, fue de gran importancia y utilidad en el conflicto del CENEPA en el año 1995, lográndose con este material la sorpresa frente al enemigo.

Igualmente y con la finalidad de modernizar el material de Artillería, se adquiere el sistema ñLanza Misiles TATRAò, con lo que permitió aumentar el poder de fuego, en apoyo a las Unidades de maniobra.

2.4. Guerra Electrónica

Guerra Electrónica es el conjunto de acciones que, utilizando la energía electromagnética, pretende asegurar la superioridad sobre el enemigo en el empleo del espectro electromagnético.

Se hace uso de este recurso natural limitado, cuya utilización en infinidad de aplicaciones lo hace más codiciado. Es necesario para nuestra Fuerza Terrestre disponer de medios que le han permitido el uso eficaz del espectro electromagnético, en las telecomunicaciones y a la vez que le permitan explorar las del enemigo, con fines de información e interrumpirlos para debilitar su maniobra.

Así, la Unidad de la Fuerza Terrestre, encargada de realizar la actividad de Guerra Electrónica, puede realizar o aplicar las siguientes medidas, en función de la tecnología disponible en apoyo a las operaciones:

- ✓ Medidas de Guerra Electrónica,
- ✓ Medidas de Apoyo Electrónico,
- ✓ Contra Medidas Electrónicas,
- ✓ Contra Contra Medidas Electrónicas.

2.4.1. Medidas de la Guerra Electrónica.

En el ambiente de la Guerra Electrónica es común hablar de las Contramedidas Electrónicas, sin referirse o sin tener conciencia de cuales son las medidas en contra de las cuales se deben aplicar las Contramedidas. Existe por lo tanto una relación íntima entre las medidas, como por ejemplo, sistemas de armas del enemigo, radares, proyectiles guiados, armas de artillería, redes de radio comunicaciones, comunicaciones vía satélite, etc. y las Contramedidas de la Guerra Electrónica, ya que a los

cambios y evolución de las medidas, se aplican nuevas Contramedidas que limitan o neutralizan estos cambios, lo que da como resultado una continua expansión de la Guerra Electrónica. ñLos sistemas de Guerra Electrónica incluyen todas las formas de energía electromagnética como son la radio, el radar, los rayos infrarrojos, los sistemas ópticos, los rayos láser, entre otros. Exceptuando la radiación producida por las armas nucleares, que entra en la categoría de guerra nuclearò

2.4.2.Medidas de Apoyo Electrónico.

Constituyen las acciones para buscar, interceptar, localizar, escuchar y analizar, registrar y evaluar la energía electromagnética radiada con la finalidad de explotar tales radiaciones en apoyo a las operaciones militares.

Las Medidas de Apoyo proporcionan la información necesaria para conducir cada fase de la Guerra Electrónica, facilitando la neutralización o eliminación de la amenaza enemiga, así como la detección de blancos redituables a nuestros sistemas de armas.

Se ha señalado con razón que todo dispositivo que utilice el espectro electromagnético puede ser interceptado o interferido, cuando se conocen por ejemplo sus frecuencias de operación y demás características explotables, a fin de atacarlo en la forma más conveniente y así neutralizar o limitar su efectividad.

El punto de partida de la Guerra Electrónica esta constituido por la información y el reconocimiento electrónico, funciones básicas de la Medidas de Apoyo y que son esencialmente actividades de producción de información destinadas principalmente a los que se aplican las Contramedidas Electrónicas y las Contra Contramedidas.

ñEl actual campo de batalla con sus amenazas abiertas y/o encubiertas, su sofisticado sistema de armas y la multiplicidad de fases especializadas,

representa un incremento en los problemas de mando y control de un Comandante para la utilización eficiente de los medios humanos y materiales puestos a su disposición en el cumplimiento de sus misiones de seguridadò

Para resolver este problema es conveniente adoptar un sistema integrado de mando y control. Tal sistema debe estar asociado con un sistema de comunicaciones e informática de diseño apropiado, y como resultado de esta asociación se tiene un nuevo sistema que recibe el nombre de ñ SISTEMA C3I2ò (COMANDO-CONTROL-COMUNICACIONES-INTELIGENCIA E INFORMATICA).

La Fuerza Terrestre depende por lo tanto y en alto grado de dispositivos electrónicos para la adquisición y difusión de información de valor militar y para el mando y control de las fuerzas y sistemas de armas de apoyo.

2.4.3.Contramedidas de Guerra Electrónica.

Son las de Guerra Electrónica destinadas a limitar o impedir el uso efectivo del espectro electromagnético por parte del enemigo. Comprenden:

- ✓ Perturbación. Es la deliberada radiación, re-radiación, reflexión o absorción de la energía electromagnética para impedir el empleo de los sistemas electromagnético del enemigo,

- ✓ Decepción. Es la deliberada radiación, re- radiación, reflexión o absorción de la energía electromagnética para engañar al enemigo en la interpretación o empleo de la información adquirida o transmitida por medios electrónicos. Esta puede ser Imitativa o Manipulativa.

2.4.4.Contra Contra medidas de Guerra Electrónica.

Comprende todas aquellas tácticas, técnicas y empleo de dispositivos

para asegurar el empleo efectivo del espectro por nuestras tropas, a pesar de las contramedidas que el enemigo emplee en contra de nuestras operaciones militares.

Cabe destacar que la Guerra Electrónica está basada en la radiación de energía electromagnética y no solamente en radiaciones ñElectrónicasò

El personal que lleva a cabo la Guerra Electrónica en apoyo a las Unidades de la Fuerza Terrestre deben aplicar las Contra Contramedidas con el objeto de hacer que el costo de la aplicación de las Contramedidas por parte del enemigo sea tan elevado que le resulte prohibitiva la aplicación de tales contramedidas. Esto implica disponer de los dispositivos adecuados como por ejemplo radares y el entrenamiento y la capacitación de los operadores para que puedan conocer las diferentes contramedidas que utilice el enemigo y seleccionar de inmediato las combinaciones apropiadas en contra de ellas.

La Guerra Electrónica, como una rama especializada, tiene características que le hacen diferente y única en el complejo campo de la tecnología, constituyéndose en un elemento vital en apoyo al combate, así una Unidad de Guerra Electrónica de la Fuerza, puede proporcionar información principalmente relacionada con:

- ✓ Contenido de mensajes,
- ✓ Actividad electromagnética adversaria,
- ✓ Despliegue de las unidades (incluidos los sistemas de armas),
- ✓ Localización de las fuerzas de tarea y los Puestos de Mando,
- ✓ Movimiento de los diferentes órganos de maniobra,
- ✓ En el aspecto técnico puede proporcionar información sobre:

- Características técnicas de la emisión.
- Tipos de equipos empleados.
- Procedimiento de empleo de los medios.

En función de la tecnología que dispone la Fuerza Terrestre, se pueden llevar a cabo acciones de Guerra Electrónica como: Inteligencia de Comunicaciones (COMINT) e Inteligencia Electrónica (ELINT); limitándose a escucha, localización, perturbación y decepción.

Inteligencia de Comunicaciones.

ñEscuchaò es la acción de observar una radiación electromagnética para intentar descubrir la información que transporta la señal, a efecto de obtener inteligencia. Y por supuesto, esta observación lleva consigo el hecho de la grabación o registro de la emisión para su análisis posterior, traducción o descriptación.

En principio toda emisión de radio puede ser escuchada por cualquiera que disponga del equipo apropiado y con sensibilidad suficiente para captarla. Con un RTF normal podemos escuchar las emisiones enemigas próximas. Pero en G.E, para aumentar el rendimiento de estas acciones, es preciso contar con receptores más complicados (automáticos, de mayor sensibilidad y que sean capaces de recibir señales de características diferentes).

Fundamentalmente se utilizan dos tipos de receptores: de exploración (o búsqueda) y de escucha, ambos automáticos y manuales.

Los primeros ñbuscanò señales en forma automática mediante un barrido del espectro, o de la banda del espectro asignado. Si una señal es interceptada y si el operador la estima interesante, la transfiere a uno de los

receptores de escucha para su observación y grabación, y el continúa su exploración en busca de nuevas señales.

La escucha en VHF es relativamente fácil ya que en esta banda, normalmente, la señal está modulada en frecuencia prácticamente sin ruidos, y hay una menor densidad de señales.

En la banda de HF el problema se complica enormemente, por el nivel de ruido que suele acompañar a la señal y por el gran número de señales en la misma frecuencia, con distinto nivel de entrada, procedentes de emisiones múltiples recibidas por onda directa y reflejada.

La localización de emisiones electromagnética se basa en lo que conocemos por ñradiogonometríaò, que consiste en determinar a través de una señal electromagnética recibida, su dirección de llegada. Un radiogoniómetro pues, en esencia, consta de un receptor; de un bien orientado sistema de antenas y de un discriminador de dirección.

Para onda directa, es necesario disponer como mínimo de dos radiogoniómetros para obtener localizaciones, ya que la intersección de las dos direcciones nos dará la situación probable del emisor.

Cabe destacar que cuanto mayor sea el número de goniómetros que usemos para la localización de una misma señal, mayor será la precisión que obtengamos en la localización.

Otra de las acciones de Guerra Electrónica es la ñPerturbaciónò que consiste en la utilización de un transmisor con características análogas al transmisor que deseamos perturbar, sea porque la señal llega al receptor víctima con un nivel adecuado.

En lo que se refiere a la acción de ñDecepciónò, esta puede ser Imitativa y Manipulativa, según pretendamos imitar las emisiones del

enemigo, o crear falsas redes propias.

2.5. Informática

El proceso de automatización de la Fuerza Terrestre se inicia en la década de los años 60, siendo esta la pionera en lo que a procesamiento automático de datos se refiere, a nivel nacional, contando para la época, automatizados los procesos de Personal y Sueldos que se realizaban en la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas utilizando equipos de Tabulación.

De acuerdo a la tecnología disponible, se desarrollaron básicamente dos archivos:

- ✓ El Escalafón General,
- ✓ El Escalafón por Unidades.

Para fines de los años sesenta hasta el año 1972 se realizan los procesos en la Dirección de .Movilización. de las FF.AA. en un equipo IBM 360/20, procesándose igualmente la nómina de PERSONAL y lo relacionado a SUELDOS.

Para este equipo los archivos son idénticos al anterior, los mismos que son grabados en cintas magnéticas. Para la explotación de estos datos era necesaria la realización de algoritmos y sentencias de programación en el lenguaje de programación llamado RPG, lográndose con esta nueva tecnología mayor rapidez y confiabilidad en el proceso de la información lo que a su vez permitía asesorar al Mando de la Fuerza Terrestre en la toma de decisiones.

En este proceso de avance tecnológico, y con el ánimo de estar acorde al mismo, el Departamento de Procesamiento de Datos de la Fuerza

Terrestre adquiere el equipo IBM 370/145 y Base de Datos Jerárquica con lenguaje de programación de tercera generación, COBOL y DL/1.

En 1985 la Fuerza Terrestre adquiere un equipo WANG 100 que luego se actualiza por un modelo Wang 8420 en 1990.

En el equipo WANG se desarrolla e implementa el Sistema Automatizado de Manejo de Personal SAMPE, el mismo que está constituído por archivos convencionales para ser procesados en lenguaje COBOL.

El Sistema Automatizado de manejo de Personal, tiene los siguientes módulos:

- ✓ Actualización,
- ✓ Datos de filiación,
- ✓ Pases,
- ✓ Ascensos,
- ✓ Condecoraciones,
- ✓ Faltas y castigos,
- ✓ Subjudice,
- ✓ Calificación anual,
- ✓ Cursos,
- ✓ Salidas al exterior,
- ✓ Suspensión de funciones,

- ✓ Profesorado,
- ✓ Cargos de importancia,
- ✓ Distinciones recibidas,
- ✓ Numero de cédula,
- ✓ Apellidos y nombres,
- ✓ Consultas de:
  - Datos de filiación
  - Datos militares actuales.
  - Familiares.
  - Guarniciones

A partir de los años noventa, la Fuerza Terrestre se empeñó en modernizar su sistema de información, iniciando con el análisis y diseño de los sistemas de Personal, Inteligencia, Logística entre los más importantes, los mismos que son detallados en el Capítulo III de la presente Tesis. Esto le ha permitido al mando tener información actualizada y confiable, de acuerdo a los adelantos tecnológicos de la era moderna, con equipos renovados y software desarrollado e implementado con la última tecnología.

3. CENTRO DE INVESTIGACIÓN CIENTIFICA Y TECNOLOGICA DE LA FUERZA TERRESTRE.

La Fuerza Terrestre, frente a las necesidades de actualizar su material bélico, se preocupó por crear el Centro de Investigación Científica y Tecnológica (CICTE), en donde se puede desarrollar la investigación que

permita actualizar la tecnología del equipo y material bélico disponible o crear nueva tecnología, aplicando el conocimiento humano en la búsqueda de nuevas alternativas para la solución de un determinado problema; esto por supuesto constituye un gran sacrificio económico para la Fuerza, que sin embargo a la postre ahorrará ingentes recursos a la misma y permitirá que seamos menos dependientes de los países industrializados.

Dentro de las Fuerzas Armadas de nuestro país, la Fuerza Terrestre crea el Centro de Investigaciones Científicas y Tecnológicas del Ejército (CICTE), el 28 de diciembre de 1988, cuya Misión es la de centralizar y coordinar las actividades de Investigación Científica y Tecnológica que requiere la Fuerza Terrestre, para facilitar la ejecución de proyectos de investigación. Además proporcionará asesoramiento técnico a fin de contribuir en el mejor cumplimiento de las misiones de las Unidades Operativas.

En cumplimiento de la misión, el (CICTE) ha realizado una serie de trabajos de investigación, orientados a solucionar problemas de orden técnico-operacional, lo que ha permitido disminuir la dependencia tecnológica y abaratar los costos de mantenimiento, reparación y modernización del material que dispone la Fuerza, en virtud que un alto porcentaje de nuestro material y equipo es de fabricación extranjera.

En lo que respecta al área de la electrónica aplicada se desarrolló en el año de 1997 un sistema de guerra electrónica en el campo de la interceptación de comunicaciones, cuyo diseño e implementación se lo realizo completamente en el CICTE, con técnicos especializados de la ESPE y de la Fuerza Terrestre. (ilustración No 2.1).

Actualmente se dispone de un modelo modernizado, consiguiendo desarrollar un sistema altamente confiable que permite realizar la detección automática de la presencia de señales electromagneticas, alta probabilidad

de detección (95%) de señales de corta duración, grabación digital de audio, generación automática de base de datos de señales detectadas e integración con DF (Radilocalización), vía LAN (redes de área local) o RS-232 (puerto serial) mediante el Software desarrollado en su totalidad en las Instituciones antes mencionadas.

Ilustración No 2.1. Sistema de Guerra Electrónica

En el área de Investigación Científica básica se han desarrollado nuevos métodos para el diseño de sistemas lasércicos de baja potencia, lo que permitirá a la Fuerza Terrestre tener el instrumento necesario para determinar distancias a un blanco determinado con gran precisión.

En el campo de la aeronavegación, se ha desarrollado un instrumento de Radio Ayuda de alta tecnología, para orientar naves aéreas en operaciones militares, en aeropuertos estratégicos, durante días y noches con perturbaciones climatológicas, cuyos resultados cumplieron con todas las exigencias requeridas por la aeronavegación. (ilustración No 2.2).

Para las Unidades de Infantería, se desarrolla el CONTROL

DIRECTOR DE TIRO PARA MORTEROS, cuya función es permitir el cálculo de la corrección de tiro de morteros con ayuda de una mini estación meteorológica, a través de un Centro Director de Tiro (CDT).

Esto permitirá disponer de un equipo electrónico portátil, que eficientemente permita calcular la corrección de tiro de morteros con ayuda de una mini estación meteorológica, por un CDT; esta innovación le proporcionará al combatiente facilidad para la operación eficiente del mortero. (Ilustración No 2.3)

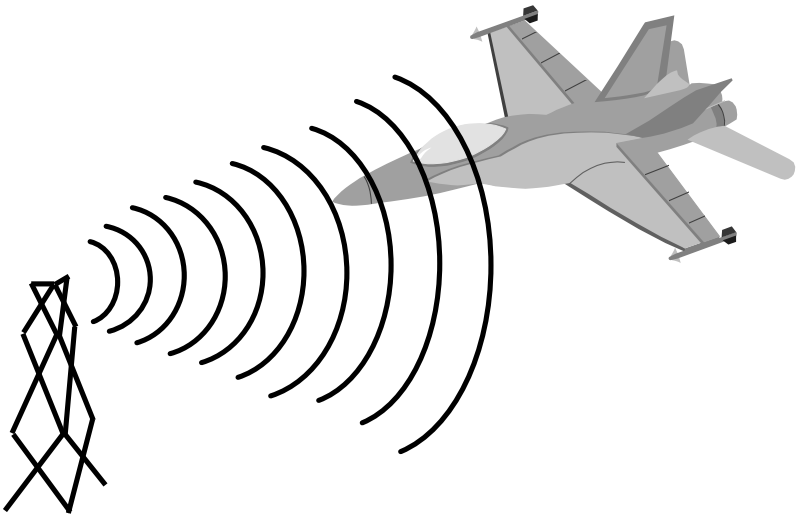


Ilustración No 2.2. Ayuda de Aeronavegación

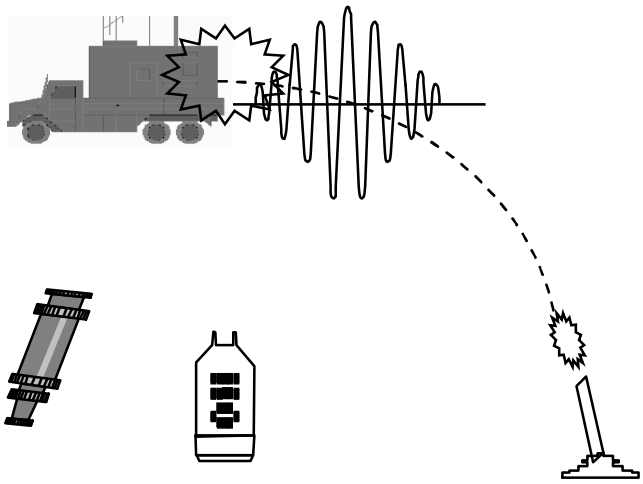


Ilustración No 2.3. Sistema de Control de Tiro

En el área de Comunicaciones se desarrolló un sistema que permita dar seguridad a las comunicaciones, de forma que el combatiente disponga de un medio seguro y confiable de comunicación, protegida e invulnerable ante la antagónica interceptación por parte del enemigo que facilita la tecnología moderna.

Para la Brigada Blindada, se ejecutó el proyecto de Repotenciación y Modernización de los Radares de Dirección de Tiro (RATAC), dotándoles de dispositivos y elementos electrónicos modernos, así como también de software con tecnología de punta. (Ilustración No 2.4)

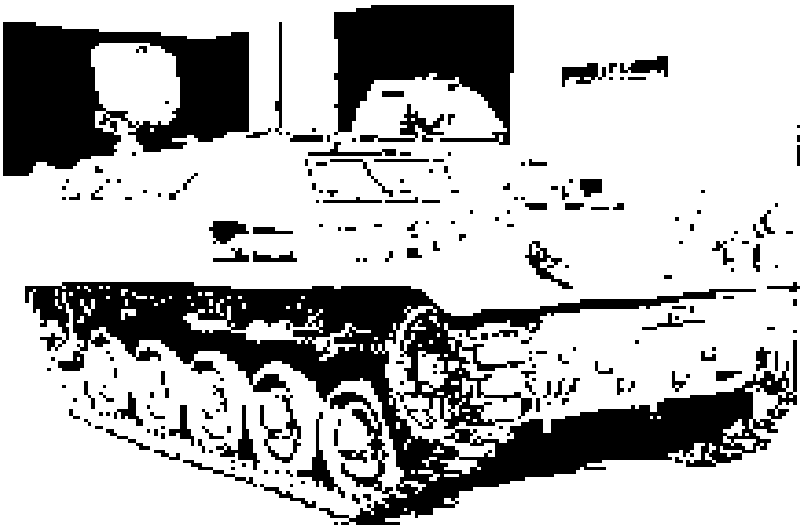


Ilustración No 2.4. Radar Director de Tiro de Artillería

Otro de los proyectos ejecutados con tecnología propia es el de construcción de un sistema de JAMMING PARA RADARES, que permita realizar interferencia a los radares enemigos con un dispositivo portátil, compacto , eficiente y de fácil manejo. (Ilustración No 2.5)

Para la Artillería, se llevó a cabo la repotenciación y modernización de la ametralladora múltiple, lo que permitió recuperar este material que prácticamente estaba en la obsolecencia, logrando con esto tener un referente tecnológico para futuros procesos de este género, cumpliendo además con dos objetivos: aporte al enriquecimiento de la tecnología nacional y ahorro de divisas para el país. (Ilustración No 2.6)

El CICTE, además de los proyectos enunciados, ha desarrollado otros de mucha utilidad para las Unidades Militares de la Fuerza Terrestre y otros organismos de las FFAA ecuatorianas y de carácter civil.

Como se puede abstraer el CICTE ha incursionado satisfactoriamente en los campos de la investigación científica y de la innovación tecnológica en apoyo a las Unidades de la Fuerza Terrestre, ya que desde su creación se han desarrollado más de cuarenta proyectos, que han permitido mejorar y mod erza.

CAPITULO III

SISTEMAS INFORMÁTICOS DISPONIBLES EN LA FUERZA TERRESTRE.

1 LA ERA DE LA INFORMACION[1]

La creatividad y el ingenio del hombre permitieron el desarrollo de las civilizaciones, mejorando el nivel de vida y simultáneamente desarrollando la defensa común. Pero las distintas sociedades y culturas evolucionaron a ritmos diferentes, aún hasta nuestros días. Durante mucho tiempo, las transformaciones sustanciales fueron lentas y casi imperceptibles pero, en los últimos decenios, esos cambios evidenciaron una progresiva aceleración. En particular los recientes avances en el campo de la información han dado inicio a una nueva era de constantes progresos que modificará la vida en todas sus facetas y que, inexorablemente prevalecerá sobre la era anterior.

Aquel grupo de naciones que "domine la información" obtendrá ventajas en todos los ámbitos, incluido el Militar que resultarán inalcanzables para sus competidores,. Es así que las Fuerzas Armadas de muchos países desarrollados, iniciaron las investigaciones y sus posibles efectos sobre la guerra y han desarrollado medios en la actualidad que pocos años atrás hubieran sido considerados sólo de ficción. En este contexto, la era de la información ha podido introducir conceptos nuevos que permitirán a las Fuerzas oponentes diferenciarse de sus similares de la era industrial, pues serán capaces de efectuar operaciones simultáneas y conocerán al instante la situación tanto propia como del enemigo. Serán más letales, más veloces en la toma de decisiones y más precisas en la ejecución. Sin embargo la interoperabilidad en las coaliciones será un serio problema a resolver.

De la misma forma que la era industrial cambió las Fuerzas Militares,

[1] Gordon R. Sullivan. Military Review

de igual forma lo hizo la era de la información. Las naciones industrializadas entregaron a sus fuerzas militares ñherramientasò muy diferentes a las que ofrecían las naciones agrarias. Las naciones basadas en información equiparán y organizarán a sus ejércitos de una manera diferente a como lo hicieron sus homólogos industrializados. La importancia no estriba en si los cambios tecnológicos son los responsables de los cambios organizacionales o conceptuales, o viceversa. El verdadero problema es el siguiente: el surgimiento de la era de la información cambiará fundamentalmente la conducción de la guerra, de la misma forma que lo hizo la era industrial un siglo y medio atrás. Todo eso está ocurriendo hoy, en circunstancias en que los objetivos militares requeridos para garantizar la victoria, durante la era industrial aumentaron. Recordemos que estos no incluían solamente a las fuerzas enemigas, sino también la capacidad y recursos bélicos del mismo: su infraestructura, sus industrias y materia prima, etc., por lo que obviamente una fuerza armada no podía alcanzar estos objetivos en una batalla decisiva.

La era de la información tal como lo hizo la era industrial antes, afectará las estructuras sociales, políticas y corporativas, al igual que la mayoría de las instituciones y organizaciones públicas y por supuesto las Fuerzas Militares[2].

A medida que avanza la era de la información, las fuerzas militares, no gastarán dinero en una nueva tecnología para emplearla con métodos anticuados como tampoco preguntarán cómo podrán hacer las cosas mejor y más rápidamente. Estas interrogantes ya se han solucionado en las primeras etapas de la era de la información." Por el contrario estas se preguntarán: "¿Por qué hacemos algunas cosas?"

Las fuerzas militares, tendrán éxito cuando puedan explotar todo el potencial de la tecnología computarizada, dentro de nuevas concepciones y

[2] Alvin Tofller "The Corporate Identy Crisis"

cuando desarrollen nuevos métodos de administración de los recursos y mejoramiento de los procesos en la toma de decisiones. Es decir, tendrán éxitos aquellos que con mayor rapidez puedan "olvidar" las reglas de la era industrial y adopten las nuevas prácticas de la era de la información.

Otros aspectos que también están sufriendo cambios son los conceptos sobre la soberanía nacional, el orden internacional, amenazas a la seguridad de nuestra nación, la naturaleza de la competencia económica y otros. Vivimos una época de transición entre la era industrial y la de la información. Son tiempos confusos, llenos de incertidumbres y cambios, y hasta a veces de caos. Las organizaciones que logren éxito serán aquéllas que conduzcan a sus sectores a través de estas condiciones casi caóticas[3].

Finalmente, la era de la información triunfará, sin embargo, aun quedarán vestigios de la era industrial y la agraria. Mientras algunos ejércitos dependerán de la informática, otros permanecerán en los tiempos industriales o agrarios, y otros permanecerán entre los dos.

Ante el dilema de que el concepto de "guerra" se está expandiendo en varias direcciones (al menos dos) en los actuales momentos, las Fuerzas Armadas de nuestro país, ya no pueden ver la guerra simplemente como los ejércitos de una nación-estado combatiendo entre sí. Estas naciones-estado no cuentan con un monopolio al momento de ir a la guerra; hoy en día, una variedad de entidades pueden librar la guerra, entre las cuales tenemos principalmente las organizaciones terroristas, carteles de narcotráfico, pandillas y otros carteles del crimen.

Por supuesto, que no puede dejar de manifestarse que se está ampliando el concepto de guerra, relacionado con el combate convencional. La era de la información cambiará el enfoque de la guerra en comparación con la era industrial, tal como la industrial lo hizo con la agraria. Los estados agrarios no pueden regenerar su capacidad bélica, por lo que una fuerza

armada solamente tiene que derrotar a un ejército de un estado agrario a fin de alcanzar la victoria. Dicha victoria, sin embargo, requiere una fuerza armada con la preparación necesaria no sólo para destruir porciones suficientes de las fuerzas armadas enemigas, sino también su infraestructura, recursos e industrias; es decir, la destrucción de su capacidad para librar una guerra. En el caso de un estado basado en la informática la cuestión va un paso más allá. No solamente implicará la destrucción suficiente de las fuerzas armadas y de la capacidad física de realizar la guerra, sino también el dominio de su sistema de información.

Es así como la variedad y la ambigüedad son características de la era de la información; variedad y ambigüedad en la clase de enemigo que enfrentaremos, de guerra que libraremos, los requisitos para la victoria y las condiciones bajo las cuales nuestra Fuerza Terrestre emplee sus medios, Las operaciones entre agencias; las reglas precisas de combate, ejecutadas con alto grado de profesionalismo; tal vez las percepciones erróneas respecto a las bajas; la reducción de tiempo entre la "crisis" observada y el desplazamiento de las tropas y el cumplimiento de la misión, todo lo que contribuye a que el uso de la fuerza militar sea único. Al campo de batalla ya han llegado las ventajas de la era de la información: velocidad, adaptabilidad y precisión. Solamente los soldados, líderes y organizaciones altamente capacitados, los cuales pueden usar estos tres factores en beneficio propio, serán los que saldrán victoriosos en este ambiente. En el Ejército de hoy existen requisitos militares de la era de la información.

El tipo de ejército que puede usar las ventajas que ofrece la era de la información y triunfar bajo estas condiciones difiere del ejército de producción en masa de la era industrial. Las exitosas empresas y corporaciones de la era de la información han tenido que olvidarse de las prácticas industriales y aplicar nuevos principios y conceptos en sus organizaciones, procesos y operaciones. De la misma forma, las

[3] The New York Times

organizaciones militares deben llegar a la misma conclusión.

Naturalmente, la aplicación en el ámbito militar no será justamente igual que en el mundo de las empresas, ya que existe una diferencia fundamental entre ambas culturas; resulta muy importante reconocer esta diferencia. No obstante, debemos reconocer que los conceptos rectores de la era de la información transformarán las organizaciones, procedimientos y operaciones del Ejército, al igual que la conducción de la guerra.

Las campañas sucesivas que se desarrollaron durante la era industrial desaparecerán. En su lugar, surgirán las operaciones simultáneas, lo que producirá la parálisis casi instantánea y la destrucción de las fuerzas enemigas, sus capacidades bélicas y su red de información a través de todo el teatro de operaciones.

Los ejércitos de la era de la información compartirán una concientización sobre la situación, la cual se basará en información amiga y enemiga actualizada y casi completa, y que será distribuida entre todos los elementos de una Unidad militar. En esta situación, las fuerzas operacionales y tácticas serán las primeras en conocer la ubicación del enemigo, sean éstos enemigos "agrarios", "industriales" o enemigos que se encuentren en proceso de formar parte de la era de la información. Obviamente, este "conocimiento" nunca será absoluto y sería un error asumir que podría alcanzar un grado de "perfección"; sin embargo, será mucho mejor que el alcanzado en épocas anteriores. En este sentido, los ejércitos de la era de la información conocerán la ubicación de sus propias fuerzas con mayor precisión que antes, a la vez que podrán impedir que el enemigo tenga acceso a esta información. Por último, esta información amiga y enemiga se distribuirá entre todas las fuerzas, con el fin de crear una percepción común del campo de batalla entre los comandantes y estados mayores de los ejércitos de la era de la información. Este conocimiento compartido de la situación, complementado con la agilidad

para conducir operaciones continuas diurnas y nocturnas, es lo que les permitirá a los ejércitos de la era de la información observar, decidir, y actuar con mayor rapidez, más precisión y mayor decisión que sus enemigos. La velocidad y la precisión se están tornando en los requisitos predominantes en el campo de batalla.

La velocidad y la precisión resultan de las unidades de maniobra, sistemas de apoyo de fuego y de sostenimiento y de las plataformas de mando y control enlazadas digitalmente. En los ejércitos de la era de la información, las mismas serán organizadas como parte de una red conjunta que incluya las plataformas y los sistemas de las fuerzas terrestres, marítimas y aéreas. La guerra futura por lo tanto será una guerra conjunta; el todo de una fuerza es mayor que la suma de sus partes.

El concepto de fuego directo, en la era de la información se redefinirá, en dicha era los ejércitos podrán disparar o moverse en contra de sus enemigos y blancos aún cuando éstos se encuentren a muchos kilómetros de distancia.

Los ejércitos de la era de la información diferirán de los de la era industrial. En primer lugar, serán más flexibles y versátiles. A su vez serán más reducidos, aunque con mayor capacidad, pero solamente si se les equipan con tecnología moderna, son bien adiestrados y dirigidos, si emplean una doctrina actualizada y si su organización se "ajusta" a su tecnología y doctrina.[4]

No obstante, la historia sugiere que ningún ejército de tiempo de paz ha logrado perfeccionar todos estos aspectos. Según señala Michael Howard, en tiempos de paz todos los ejércitos estarán erróneos; los ejércitos victoriosos serán aquellos que no estén tan errados. Y en tiempo de guerra, los ejércitos victoriosos serán aquéllos que logren adaptarse rápidamente." Por lo tanto, el sentido común estratégico señala que la

optimización de una fuerza en tiempo de paz implica un alto riesgo, por lo que debe retener cierta "abundancia" y "medidas de seguridad".

En segundo lugar, los ejércitos de la era de la información diferirán de los de la era industrial en el proceso que emplearán para crear y sostener las capacidades de la era de la información. Por ejemplo, las estructuras de la fuerza que pueden explotar y maximizar la velocidad y precisión reemplazarán los diseños de la fuerza de la era industrial. Las fuerzas de la era de la información no se basarán en su desgaste; las reglas de asignación de fuerza, al igual que los factores de reemplazo o pérdida de personal y equipo cambiarán. Además, un proceso de adquisición capaz de mantenerse a la par con el ritmo de innovación y producción tecnológica reemplazará el proceso actual de la era industrial, como también cambiarán los procedimientos para la toma de decisiones.

Cabe destacar que existen cuatro tipos de información que servirán como núcleo para la construcción de los procesos y organizaciones dentro de una fuerza armada en la era de la información, a saber:

- ✓ Información sobre contenido - información simple tipo inventario sobre la cantidad, ubicación y clase de artículos,
- ✓ Información sobre forma - descripciones sobre la forma y composición de los objetos,
- ✓ Información sobre conducta-simulación tridimensional que pronosticará la conducta de objetos físicos, logrando así entablar "juegos de guerra" respecto a los cursos de acción disponibles,
- ✓ Información sobre acción - información que instantáneamente pasa a convertirse en acción."

En esta era de la información, poco a poco se podrá reemplazar los

[4] Michael Howard "Military Science in an Age of Peace"

ejercicios de tiro y de campaña por una variedad de simulaciones y otros tipos de programas computarizados.

La era de la información les dará a los Comandantes un conjunto de opciones más resistente y sofisticado: operaciones reales y simulaciones construidas, al igual que ejercicios simulados interactivos y de realidad virtual. Este tipo de simulaciones no reemplazarán las operaciones reales, sino que por el contrario, nos permitirán realizar más de las mismas.

El equipo de las primeras etapas de la era de la información puede ser muy similar al que tenemos ahora. Sin embargo, los tanques, los vehículos de combate de Infantería, las piezas de Artillería, los lanzacohetes, los helicópteros, los vehículos de apoyo de mando y control, de ingenieros y de logística, y los camiones serán más "inteligentes". Esto ocurrirá debido a las computadoras, otras tecnologías más avanzadas y a la red de información. Aún más, todos estos equipos estarán conectados a otros sistemas similares de otros servicios. La resultante fuerza conjunta, digital e integrada, necesitará sistemas de abastecimiento, de mantenimiento y de servicio diferentes a las que han apoyado al ejército de masa de la era industrial. Por lo tanto, tenemos que alterar la regla empleada para determinar cuál combate, apoyo de combate y apoyo de servicio de combate está "asociado" con nuestros actuales modelos. Asimismo, se deben cambiar los factores de planificación de apoyo incluidos en los manuales logísticos y juegos de guerra. De otra forma se crearía una brecha entre el potencial operacional y la capacidad de sostenimiento.

Por último, la capacitación del liderazgo cambiará con el fin de acomodar las nuevas destrezas conceptuales, técnicas y organizacionales requeridas por los miembros de la institución armada en la era de la información.

En este contexto, el mando de la Fuerza Terrestre, consciente de la importancia del proceso de la información, como una herramienta

fundamental para la toma de decisiones, inicia la automatización de varios de sus procesos en el año 1960, teniendo como organismo encargado de la parte informática al Departamento de Informática del Ejército ñDINFEò, y se inicia con el procesamiento de datos de Personal y Sueldos, utilizando el lenguaje ñCobolò en un computador central ñVS 800ò de IBM y los equipos WANG, plataforma que se utilizó por varios años con mucho éxito, siendo los miembros de la Fuerza Terrestre los encargados del desarrollo, implementación y mantenimiento de este sistema, situación que mejoró y agilitó los procesos que se llevan a cabo en esas dependencias, permitiéndole a la Fuerza, cumplir con mayor eficiencia la misión asignada por el Estado ecuatoriano.

El avance tecnológico de la informática en la última década ha hecho que la Fuerza Terrestre sienta la necesidad de actualizarse en este campo, pues los sistemas disponibles comenzaban a entrar en la obsolecencia y por lo tanto su misión específica de seguridad no se podía cumplir a cabalidad, porque el Mando no disponía de información con la rapidez y confianza adecuados para la época. Es en estas circunstancias que se decide iniciar el proceso de modernización de los sistemas informáticos de la Fuerza Terrestre, teniendo entre los principales:

2. SISTEMA DE INFORMACION DE PERSONAL DE LA FUERZA TERRESTRE (SIPER)

La Fuerza Terrestre, como se manifestó anteriormente, cuenta con sistemas desarrollados en COBOL para administrar la nómina del Personal Militar (Oficiales y Voluntarios), Personal de Empleados Civiles, Conscriptos y pago de Remuneraciones.

Estos sistemas que se implementaron en la década de los años setenta, han cumplido su ciclo de vida, no tienen integración entre sí, y existe redundancia de datos por lo que se reemplaza con un nuevo sistema denominado SIPER, en el que se incluye la Racionalización de Procesos

así como la integración con el resto de sistemas del SIFTE (Sistema de Información de la Fuerza Terrestre).

Con este sistema desarrollado por elementos de la Fuerza Terrestre, se busca alcanzar que el manejo de personal sea llevado a cabo de una manera técnica, con una verdadera racionalización del recurso humano que labora en las diferentes dependencias y unidades de la Fuerza Terrestre, y que permita el correcto asesoramiento de personal al Comandante de la Fuerza para la toma de decisiones en lo que a este recurso se refiere, apoyados en la herramienta informática.

2.1. Módulos

El sistema de Personal para el correcto desempeño, ha sido desarrollado en diferentes módulos de acuerdo a las necesidades de la Dirección de Personal y de la Fuerza Terrestre.

- ✓ Planificación .- Analiza el personal que la Fuerza Terrestre necesita para cumplir con su objetivo, la evaluación del desempeño y el control del personal que debe realizarse, en lo relacionado a:
  - Previsión de Recursos Humanos,
  - Evaluación de Desempeño, y,
  - Control de Personal
- ✓ Ingreso .- Contempla la selección y reclutamiento del personal que formará parte de la Fuerza Terrestre, tanto para Oficiales como para Voluntarios:
  - Reclutamiento,
  - Selección, y,

- Insubsistencias y Reincorporaciones

✓ Capacitación .- Se encarga de la capacitación que debe tener el personal perteneciente a la Fuerza Terrestre para que cumpla funciones orgánicas de acuerdo a los requisitos que pide el puesto y al plan de carrera.

- Entrenamiento,
- Ambiente Laboral, y,
- Plan de Carrera

✓ Estímulos.- Estímulo que el personal tiene en la carrera dentro de la Institución.

- Ascensos,
- Reubicaciones,
- Permisos,
- Licencias,
- Condecoraciones, y,
- Méritos y Deméritos

✓ Remuneraciones.- Se encarga de las remuneraciones salariales del personal de la Fuerza Terrestre

- Estudio Salarial
- Cálculo Rol de Pagos
- Cálculo de Pago a Unidades

- Asignación Económica Exterior
- Liquidación del Rol

✓ Asignaciones.- Se encarga de la selección del personal que deben cumplir funciones especiales, comisión de servicios, pases

- Funciones Especiales
- Pases
- Traslados
- Fijaciones
- Pases de Guerra
- Comisión de Servicios

✓ Rectificaciones.- Rectificacionies de datos de identificación y proceso de los canjes de despachos y especialidades

- Datos de identificación
- Canjes de Despachos y Especialidades

✓ Situación de Personal.- Mantiene un control de la situación del personal de acuerdo a la Ley de Personal de las Fuerzas Armadas

- A Disposición
- Disponibilidad
- Cancelación y Destitución

✓ Reservas.- Manejo del personal de reservistas asignados a la Fuerza Terrestre para el completamiento del Orgánico

- Actualización de Reservas

- Completamiento Orgánico

Existen procesos que son centralizados y se ejecutan en la Dirección de Personal como el caso de pases, ascensos, condecoraciones; otros procesos son descentralizados que pueden ejecutarse en las Unidades como los permisos y control de asistencia.

En las Unidades se requiere tener una red LAN, cuyo servidor contendrá el modelo de la Base de Datos de Personal y los datos a manejarse será únicamente del personal que pertenezca a esa Unidad, es decir, se implementarán base de datos distribuidas en las Unidades.

2.2. Tecnología utilizada

- ✓ La plataforma considerada es Cliente ï Servidor:
- ✓ Sistema Operativo SOLARIS
- ✓ Base de Datos ORACLE
- ✓ Front End POWER BUILDER

En la Dirección de Personal las PCs están conectadas como estaciones de trabajo al Servidor Sun Enterprices 450

- ✓ Red LAN con NT en las Unidades
- ✓ Red WAN de la Fuerza Terrestre a través de la Red MODE

Este sistema contempla los procesos que se realicen en todos los niveles de la Fuerza Terrestre permitiendo que la información se actualice desde cualquier punto ya sea en línea o a través de medios magnéticos y consolidar hacia los niveles superiores de mando y viceversa.

En la actualidad se está utilizando la red LAN en la Comandancia General de la Fuerza Terrestre, para la transmisión de datos entre los diversos Departamentos de la Dirección de Personal.

La posterior implementación en las Unidades dependerá de la infraestructura que cada una tenga para realizar la instalación del sistema automatizado SIPER y la conexión en línea entre las Unidades depende del proyecto Red de Datos de la Fuerza Terrestre estimándose que en el año 2005 estén todas las unidades conectadas en la red WAN.

3. SISTEMA DE INTELIGENCIA:

El Comando de la Fuerza Terrestre, consideró que uno de los aspectos más importantes para tener éxito en el desarrollo de un conflicto es, el conocimiento de las fuerzas enemigas. Por este motivo, se decide iniciar el desarrollo e implementación del Sistema de la Dirección de Inteligencia, el mismo que permite tener información referente a los siguientes aspectos:

- ✓ Para Defensa Externa; el ñOrden de Batallaò esta información le permite al mando de la Fuerza Terrestre tener un conocimiento completo y oportuno del enemigo referente a:
  - Organización,
  - Misión,
  - Dispositivo,
  - Armamento en dotación,
  - Equipo en dotación,
- ✓ Para Defensa Interna, permite tener información sobre:

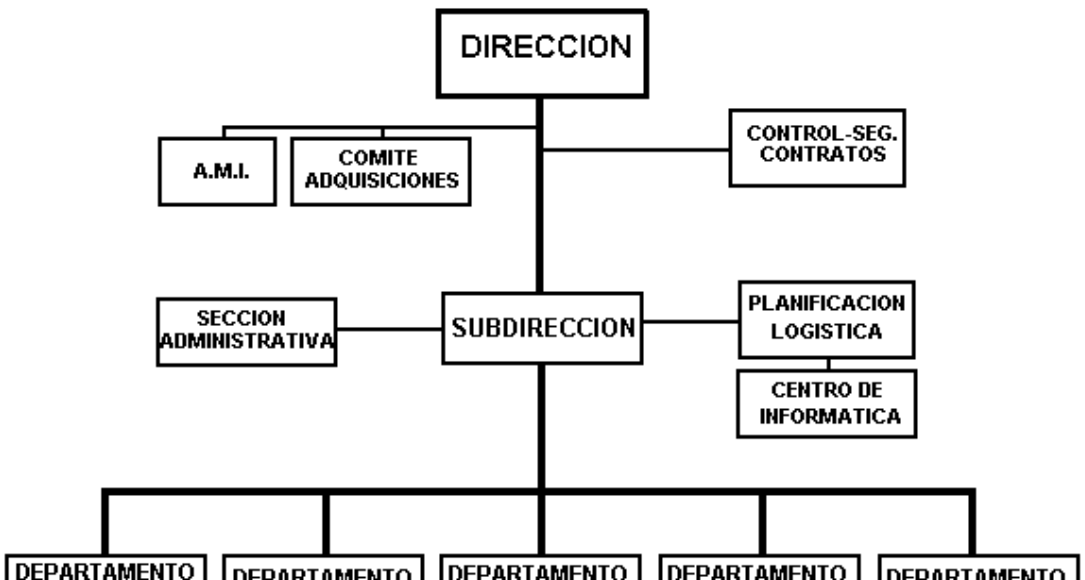
- Autoridades importantes,
- Grupos insurgentes,
- Partidos Políticos,
- Personalidades importantes e influyentes del país.

4. SISTEMA DE LOGISTICA (SILOG)

Vista la necesidad del mando de tener información actualizada y confiable en el campo de Logística, que le permita tomar decisiones acertadas, se inicia el análisis y desarrollo del Sistema de Logística en el año 1994 con los Subsistemas de Abastecimiento, Mantenimiento, Transportes y Sanidad, dependientes de la Dirección de Logística; cuya Misión es: ñAsesorar al Comandante General de la Fuerza Terrestre, en el conocimiento, estudio y proposición de los aspectos relativos a la planificación, organización, control, ejecución y evaluación del sistema logístico, a fin de mantener en óptimas condiciones la capacidad logística de la Fuerza, tanto en tiempo de paz como de guerra capaz de permitirle el cumplimiento de la misiónò

4.1. Organización de la Dirección de Logística

Para el cumplimiento de la Misión la Dirección de Logística tiene la siguiente organización:



4.1.1. Tareas fundamentales:

- ✓ Establecer y mantener actualizada la doctrina logística institucional, supervisando su cumplimento.

- ✓ Elaborar y tener actualizada la planificación y políticas logísticas de la Fuerza Terrestre y supervisar su cumplimiento.

- ✓ Dirigir y controlar la planificación logística de las unidades operativas de la Fuerza, con el fin de mantenerla actualizada y asegurar su empleo oportuno de los servicios logísticos en el cumplimiento de sus misiones específicas.

- ✓ Estudiar el progreso y evaluación de los procedimientos de apoyo logístico, con el fin de proponer las modificaciones y renovación de las mismas.

- ✓ Ejecutar los planes de adquisiciones y dirigir a través de la Brigada de Apoyo Logístico, la distribución de acuerdo a las prioridades de planificación.

- ✓ Proponer medidas tendientes a optimizar la administración logística de la Fuerza, que considere el mantenimiento, recuperación y

reemplazo del material.

Para el apoyo a la Fuerza Terrestre el Sistema Logístico tiene la siguiente organización:

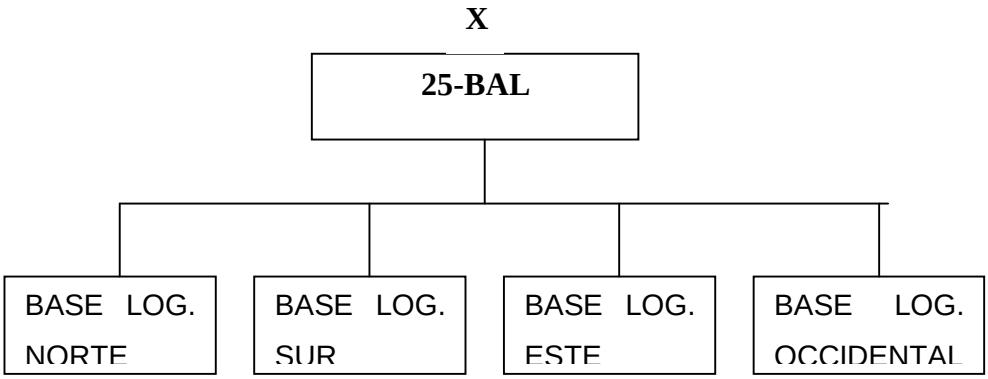
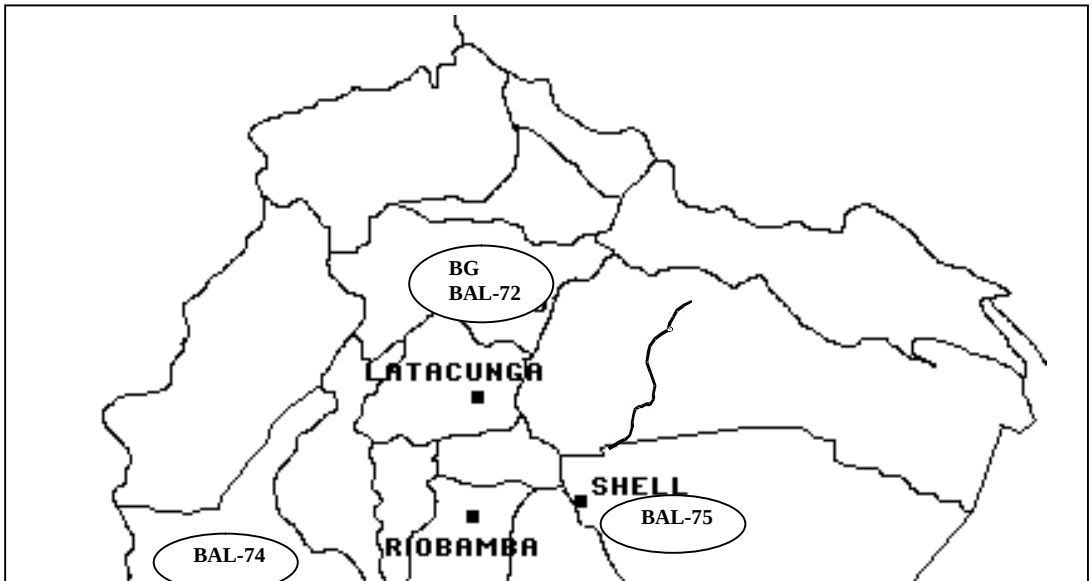


Ilustración No.3.2 Organización del SILOG.

4.1.2. Distribución de la Base General y Bases Logísticas en el Territorio Nacional.

Para apoyar las operaciones de las Unidades de la Fuerza, la Base General y las Bases Logísticas se han dislocado en el territorio nacional, de forma tal que sea más ágil y oportuno el proceso logístico.



4.1.3. Base General de la Fuerza Terrestre

MISION.

Ejecutar el apoyo logístico y administrativo en tiempo de paz y de guerra, hacia las unidades y dependencias de la Fuerza Terrestre, mediante un procedimiento normal descentralizado, desde sus instalaciones ubicadas en Quito, a fin de alcanzar y mantener un alto grado de operatividad y apoyar eficazmente a la Fuerza y a sus operaciones militares en el cumplimiento de su misión.

TAREAS FUNDAMENTALES:

- ✓ Recibir, almacenar, distribuir y evacuar los abastecimientos, adquiridos por la Dirección de Logística de la Fuerza Terrestre, a través de sus instalaciones logísticas ubicadas en territorio nacional.

- ✓ Planificar, organizar e implementar la infraestructura logística en cada

una de sus instalaciones, a fin de facilitar la recepción, almacenamiento, mantenimiento y distribución de los abastecimientos necesarios para la operación y funcionamiento de las unidades de la Fuerza Terrestre.

- ✓ Con sus instalaciones especializadas, constituirse en el V Escalón de mantenimiento de material de Guerra, Transportes y Abastecimientos especiales de Intendencia y responsabilizarse por su ejecución.

- ✓ Organizar las unidades logísticas que materialicen las instalaciones y ejecuten las misiones de abastecer, atender y evacuar los requerimientos realizados por las unidades y dependencias de la Fuerza.

- ✓ Coordinar con las Jefaturas de los Servicios Logísticos el desarrollo, empleo, capacitación y organización de los mismos en beneficio de las operaciones de apoyo de servicio de combate a las unidades y dependencias de la Fuerza Terrestre.

- ✓ Desarrollar y actualizar periódicamente la Apreciación Logística de la Base General, a fin de generar los planes logísticos en cada una de las Bases, incluidos en ellos, el Plan de Explotación de Recursos Nacionales y el Plan de Organización y Funcionamiento de las Bases.

EMPLEO:

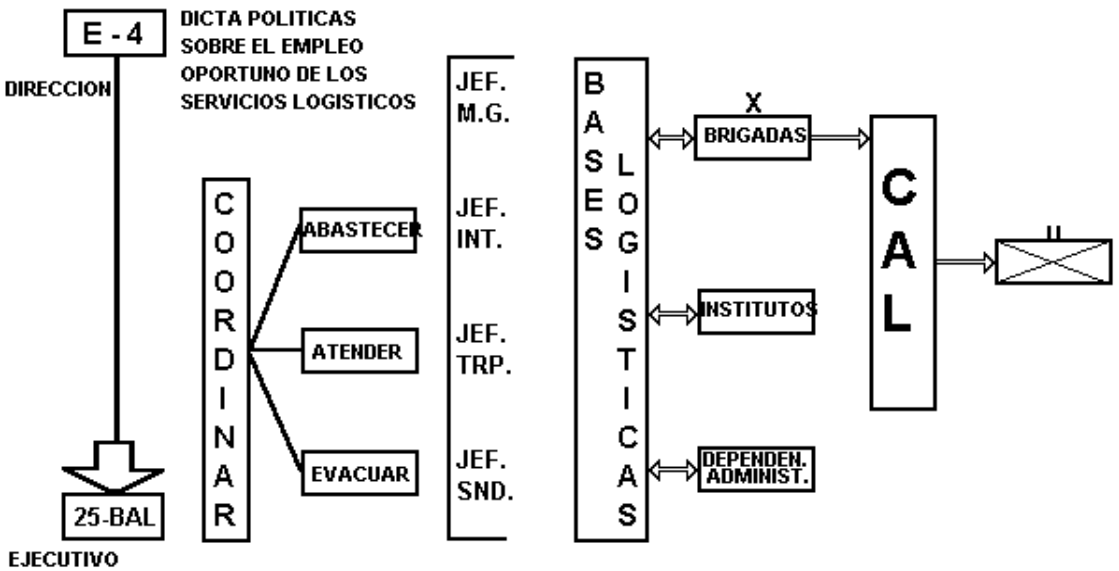


Ilustración No.3.4 Materialización del Apoyo Logístico de la Base General

3.3.5. Base Logística

4.1.4. Base Logística

MISION:

Ejecutar el apoyo logístico y administrativo en tiempo de paz y de guerra, hacia las unidades de su jurisdicción, mediante un procedimiento normal descentralizado, desde sus instalaciones, a fin de alcanzar y mantener un alto grado de operatividad y apoyar eficazmente a las unidades militares en el cumplimiento de su misión.

TAREAS FUNDAMENTALES:

- ✓ Recibir, almacenar, distribuir y evacuar los abastecimientos de todo tipo, dispuestos por el Comando de la Base General, hasta y desde las unidades de su jurisdicción.

- ✓ Desarrollar la infraestructura logística de sus instalaciones basándose en la planificación y organización remitida por el Comando de la Base General.

- ✓ Desarrollar y mantener actualizada la Apreciación Logística de su jurisdicción al igual que el Plan de Explotación de Recursos de la Zona y el Plan de Organización y Funcionamiento de la Base.

- ✓ Constituirse en el IV Escalón de Mantenimiento de Material de Guerra, Transportes y abastecimientos especiales y responsabilizarse de su ejecución.

- ✓ Proveer servidumbre logística a las unidades que de acuerdo al Plan de Campaña de la Fuerza tengan que emplearse en su jurisdicción, para lo cual planificará y mantendrá actualizado el Plan de Funcionamiento y Organización de la Base para tiempo de guerra.

EMPLEO:

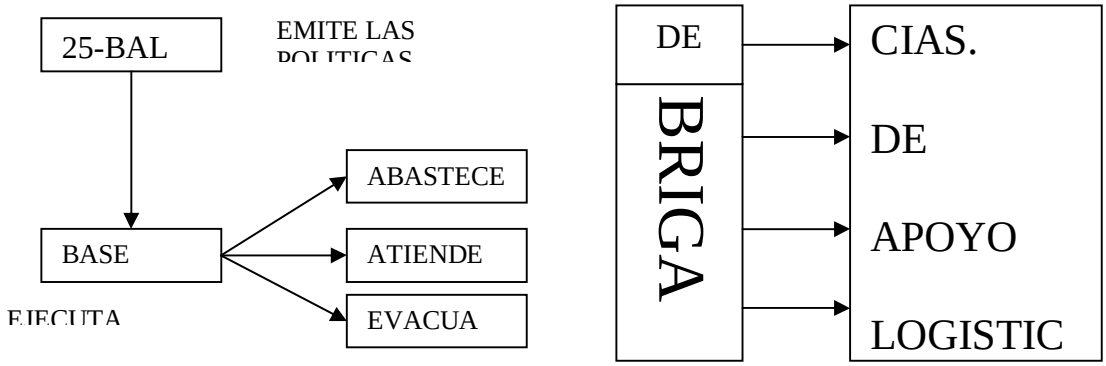


Ilustración No.3.5 Materialización del Apoyo Logístico de una Base Logística

4.2 Estructura del ñSILOGò

Para el cumplimiento de la misión el SILOG presenta la siguiente estructura que ha sido desarrollado en base a las apreciaciones y misiones encomendadas por el Mando de la Fuerza.

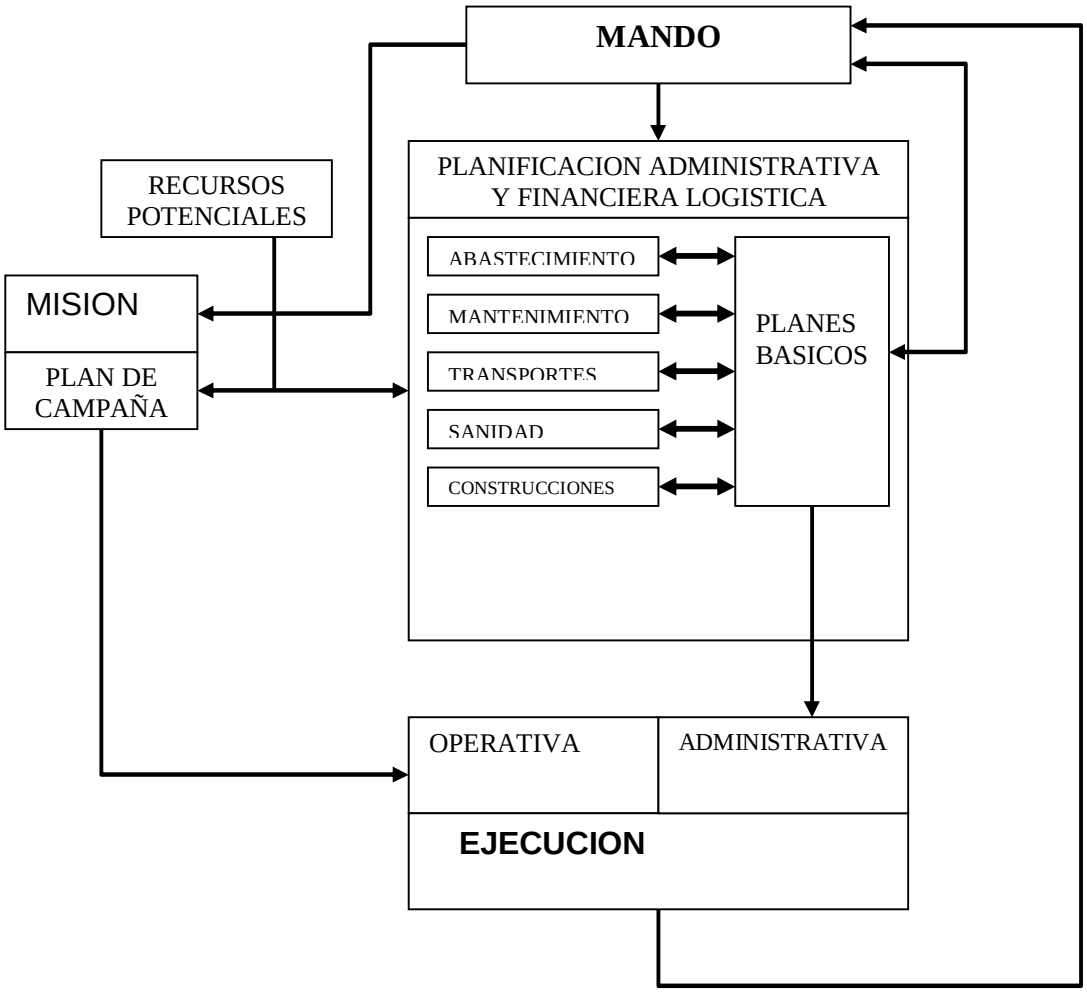


Ilustración N 3.6 Estructura Sistémica del ñSILOGò

4.3. Funciones implementadas en el "SILOG"

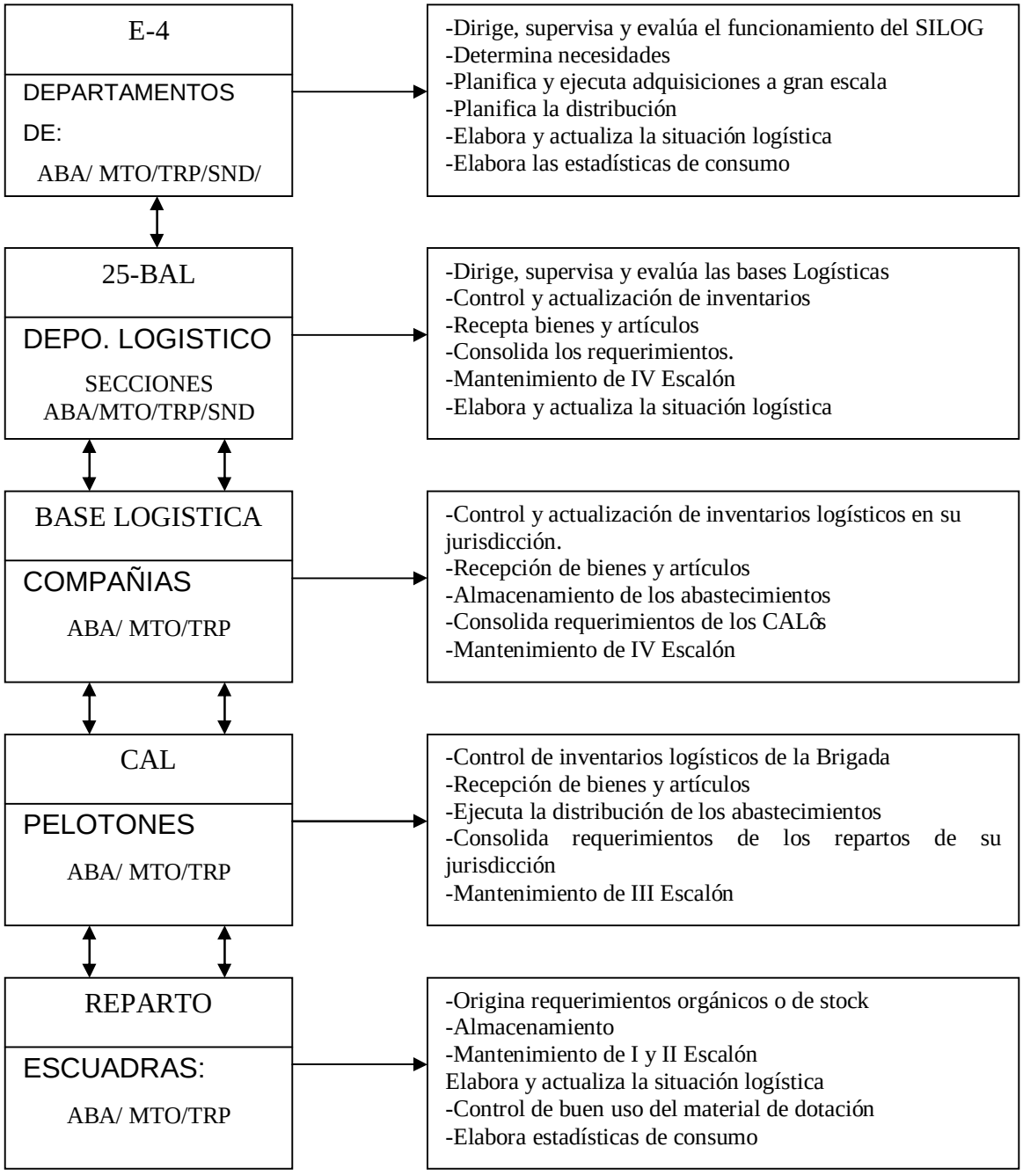


Ilustración No. 3.7 Funciones desarrolladas en el Canal Logístico

4.4. Automatización del "SILOG"

El siguiente gráfico presenta el esquema del SILOG, para trabajar en forma automatizada.

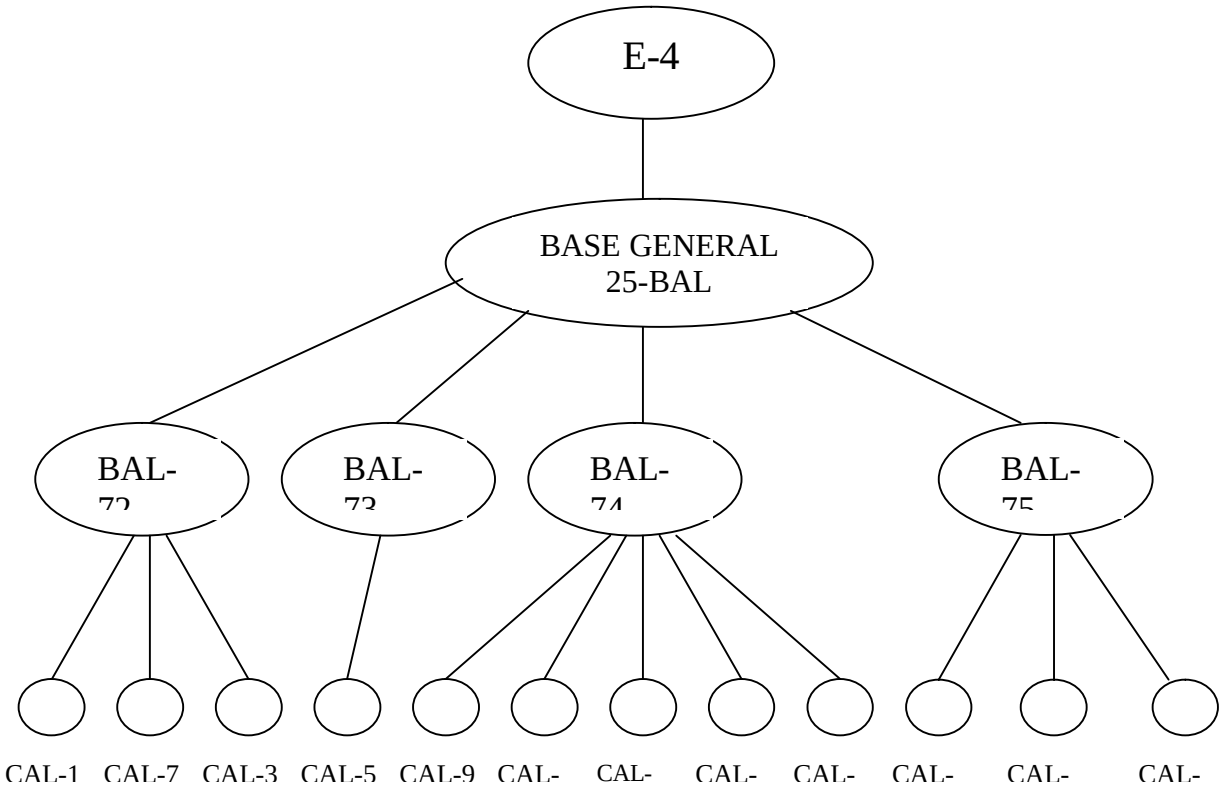


Ilustración No.3.8 Esquema del ñSILOGò

Este esquema que se halla implementado, permite básicamente el control de inventarios, en tiempo real, lo que le da al Mando de la Fuerza Terrestre el conocimiento suficiente del estado en que se encuentra la logística en cualquier reparto de la misma, en apoyo a las operaciones, teniendo así, la capacidad para tomar decisiones en el menor tiempo posible y sin poner en riesgo los abastecimientos necesarios para la difícil empresa de la seguridad del Estado ecuatoriano.

En la siguiente ilustración, se presenta un modelo de Red Logística

implementada para apoyar a las Unidades de la 13-BI.

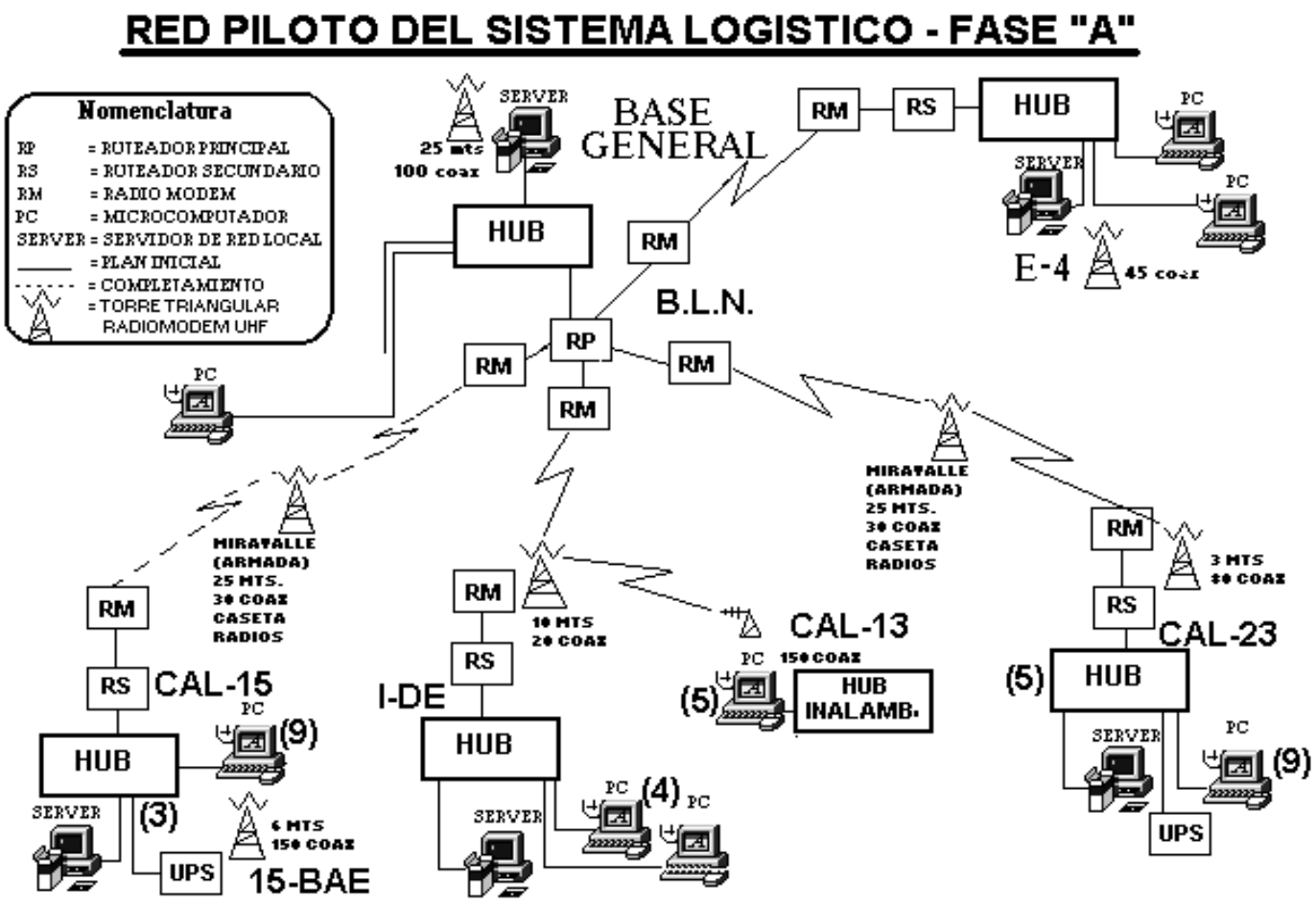


Ilustración No 3.9 Red del Sistema Logístico, implementada en apoyo a la I-DE

El modelo presentado en el gráfico anterior, es el que permite mantener la información entre las siguientes unidades conectadas en red:

- ✓ Dirección de Logística,
- ✓ Brigada de Apoyo Logístico No 25,
- ✓ Batallón de Apoyo Logístico No 72,

- ✓ CAL-13,
- ✓ CAL-15,
- ✓ CAL-23,
- ✓ I-DE

La red diseñada en la que se sustenta el SILOG, tiene un Servidor Central en cada una de las Bases Logísticas, las que se comunican con las Compañías de Apoyo Logístico (CALs), como su Escalón Inferior, en donde se genera la información y a su vez también se comunican con la Base General como Escalón Superior para enviar a aquella, la misma que consolida en el Servidor de esta unidad para ser presentada al Director de Logística en el Comando General de la Fuerza Terrestre. La comunicación se realiza utilizando un sistema mixto de comunicaciones compuesto por el medio alámbrico en el interior de las unidades y el medio radio para la comunicación entre los escalones logísticos y en algunos casos se utiliza el medio de comunicación satelital que dispone la Fuerza Terrestre. Posteriormente se utilizará como medio principal de comunicación de datos, la red de comunicación de datos del Sistema de Comunicaciones MODE, cuya modernización se halla en proceso, lo que permitirá integrar de manera eficiente las Bases Logísticas ubicadas en Quito, Durán, Cuenca y La Shell.

Aspectos Tecnológicos

Las características tecnológicas de la red son:

- ✓ Redes de arquitectura Cliente Servidor,
- ✓ Interface Gráfica de Usuario,
- ✓ Base de Datos Relacional,Herramientas CASE,

- ✓ Front-End para desarrollo,
- ✓ Red de datos digital (WAN) con una velocidad de 64 Kbps utilizando radiomodems.

Para controlar las existencias de: Material de Guerra, Intendencia, Transporte, Sanidad; control del movimiento de Materiales (ingresos, egresos); apoyo a los procesos de planificación y compra de materiales; permite realizar el seguimiento a la distribución de abastecimientos; realizar consultas a diferentes niveles de consolidación; obtener cuadros y gráficos estadísticos de los movimientos; y, permitir a cada escalón del Canal Logístico para que pueda accesar a la información que requiera.

En este sistema la Fuerza Terrestre incorpora tecnología informática y de comunicación de datos de punta, transformando la anticuada modalidad de procesamiento de datos de la Institución.

Sistema Operativo

El Sistema Operativo utilizado por el servidor es el SOLARIS, que es un SO UNIX con características propias del fabricante

Base de Datos.

El motor de la base de datos para el servidor Central es el INFORMIX, el mismo que presenta una buena performance y confiabilidad. La arquitectura es paralela Cliente/Servidor.

En particular la Fuerza Terrestre está trabajando con el motor de la base de datos Informix DSA (Arquitectura Dinámica Escalable), que provee soporte para sistemas SMP (múltiples procesadores simétricos instalados sobre un mismo computador). Adicionalmente la arquitectura soporta sistemas multiprocesadores y sistemas de máquinas de paralelismo masivo.

Su arquitectura consiste de múltiples procesadores virtuales, cada uno de los cuales corre múltiples threads en un contexto de switches.

Cabe indicar que la arquitectura DSA, es una arquitectura de última generación en base de datos diseñada para obtener el máximo provecho del poder de procesamiento de los sistemas paralelos.

Productos INFORMIX de la Fuerza Terrestre.

Los productos Informix que se hallan instalados en el Sistema Logístico son los siguientes:

- ✓ ONLINE Run Time- Licencia 32 usuarios para E-4, CAL-13, CAL-15,
- ✓ STAR Run Time- Licencia 32 usuarios para E-4, CAL-13, CAL-15,
- ✓ ONLINE Run Time- Licencia 64 usuarios para 25-BAL,
- ✓ STAR Run Time- Licencia 64 usuarios para 25-BAL,
- ✓ ESTÁNDAR ENGINE Run Time- Licencia 8 usuarios para CAL-13,
- ✓ INET para los usuarios con Power Builder, para permitir el procesamiento cliente-servidor.

4.5. Sistema de Inventarios

Características:

- ✓ Basado en un modelo conceptual y sobre objetivos institucionales,
- ✓ Desarrollado e implementado integramente por personal de la Fuerza Terrestre,

- ✓ Incluye amplios recursos de información para el usuario (reportes, gráficos, consultas, etc), lo que le permite al mando gerenciar la información de la manera más sencilla y confiable en la toma de decisiones,

- ✓ Permite el control de las existencias y de los movimientos de los materiales de las bodegas,

- ✓ Se realiza el control de los requerimientos de las unidades,Se emplea como apoyo a los procesos de planificación y compra de materiales,

- ✓ Cada escalón del Canal Logístico puede accesar a la información que requiera,

- ✓ Permite el seguimiento de la distribución de los materiales,

- ✓ Presenta facilidades para el análisis del movimiento de inventarios

CAPITULO IV

PROPUESTA DE SEGURIDAD INFORMATICA PARA LOS SISTEMAS DE LA FUERZA TERRESTRE.

1. TEORIA DE SEGURIDAD INFORMATICA

En nuestros días es prácticamente imposible manejar la actividad de procesamiento de datos sin el concurso de la tecnología de seguridad informática; por cuanto existen especialistas (***hackers)*** persistentes, que se empeñan en desentrañar los sistemas computacionales y averiguar como funcionan. Estas personas dedicadas a la violación de seguridades informáticas, que se les conoce como ***vándalos,*** quieren tener acceso a los sistemas por cualesquiera de las siguientes razones:

- ✓ Sólo por diversión,
- ✓ Para explorar los sistemas informáticos y datos,
- ✓ Para obtener información sobre el sistema informático y datos,
- ✓ Para ñrobarò recursos del sistema,
- ✓ Como tiempo de CPU

Por lo antes indicado; toda la información procesada a través de un computador, es susceptible de ser interceptada o accesada, con fines de copiado, adulteración o borrado, violentando las normas de manejo de información; siendo necesario tomar todas las medidas precautelatorias a fin de reforzar la privacidad e integridad de la información.

En este contexto, entonces, a menos que los datos que se traten de proteger se encuentren en una computadora dentro de una habitación en la que se controle el acceso y no existan conexiones con el exterior, esos

datos estarán siempre en peligro y expuestos a que sean obtenidos por personas ajenas a la institución.

Se conoce que en todo el mundo, todos los días se producen entradas no autorizadas y violaciones de seguridad de los sistemas informáticos. Estos violadores no son solo vándalos de Internet, sino también personas que trabajan en el centro de datos o gente que tiene alguna relación con la institución de interés; estos pueden robar tiempo de computadora y servicios para su uso personal o fines ajenos a aquella. Frente a estos problemas se ha desarrollado toda una tecnología en seguridad informática, la cual se expone a continuación.

1.1. Seguridad de datos, Integridad y Confidencialidad de la información

Se entiende claramente, que en un computador lo que se desea proteger es que nadie borre los archivos; que personal no autorizado entre en los mismos para obtener datos de interés, que no se cambie la configuración de cualquiera de los periféricos o produzca algún desarreglo en el computador, que nadie que no este autorizado tenga acceso a información privada o confidencial (datos delicados ocultos o secretos).

Estos tópicos se conocen como: Integridad[5] y Confidencialidad de Datos[6].

Formalmente, existen tres tipos de acceso a la información:

- ✓ Permiso de lectura,
- ✓ Permiso de escritura,
- ✓ Permiso de ejecución

Hay que destacar que las políticas de acceso son elaboradas en

[5] Integridad: es la forma como se deben proteger los datos

función de los recursos y no de los usuarios

Ejemplo: Los documentos de una unidad, son de interés para el Comandante y para la secretaria, por lo tanto, los dos tienen permiso de acceso sea para lectura o escritura.

En cambio, un documento que sea de carácter personal para el Comandante puede ser de acceso tanto para lectura como escritura únicamente para este.

1.2. Virus Computacionales.

Un virus computacional, es aquel que ñinfectaò archivos computacionales (sea de datos o programas), alterando la estructura e información contenida en estos, con los efectos colaterales siguientes:

- ✓ Borra el disco duro en alguna fecha particular (ejemplo el virus ñChile mierdaò, producto chileno de exportación que borra el disco duro del computador infectado el día nacional de Chile, esto es el 18 de septiembre),
- ✓ Aumenta el tamaño de los archivos y así, se necesita por lo tanto mayor espacio en el disco,
- ✓ Mueve los archivos de ubicación,
- ✓ Altera las partes sensibles de otros archivos o les borra,
- ✓ Despliega mensajes o reinicializa el sistema,
- ✓ Encipta el disco duro (casos en que un virus encripta el contenido del disco duro atacado, comenzando por los archivos más antiguos),

Un virus puede venir en cualquier programa, independientemente de

---

[6] Confidencialidad: proceso de mantener la información secreta

la fuente. Cuando se ejecuta aquel, muchas personas confían en que el mismo no contenga virus.

Afortunadamente, en forma paralela se han desarrollado programas conocidos como ñantivirusò, los mismos que permiten verificar la existencia de virus en un archivo de datos o programas y lo realiza ejecutando verificaciones sobre los archivos, buscando ñhuellasò usuales. El problema actual es que hay una cantidad muy grande de virus de diferentes tipos que van apareciendo día a día, lo que hace muy difícil mantener una estadística completa de todas las variedades, a más de que estos se disfrazan y son ñmetamorfos[7]ò.

1.3. Autenticación y autorización de acceso.

El trabajo colaborativo actual, que se desarrolla en cualquier oficina o departamento, necesita de una red de datos local (interna dentro de ellos, LAN) y un sistema operativo asociado multiusuario[8] o cliente servidor[9].

La primera preocupación es la seguridad que la red debe tener para mantener los principios de confidencialidad, protección e inviolabilidad de los datos contenidos en el sistema o que se transfieren por la red, entonces se deben analizar las diferentes posibilidades de violación de la seguridad que se presentan, así tenemos:

- ✓ Un usuario tratando de accesar a la red, mediante un password. A esta área de seguridad se la conoce como ñautentificaciónò y corresponde a la pregunta que se hace el computador. ¿Como saber que es realmente el usuario autorizado y no otro?.

La respuesta usual es : **a través de una clave de acceso.**

---

[7] Término utilizado para denotar que un virus computacional es cambiante.
[8] Característica del Sistema Operativo para correr en varias plataformas.
[9] Red conformada por un servidor central y varias computadoras, clientes.

Se considera que actualmente un 99% de los sistemas de autentificación son basados en claves de acceso para permitir el ingreso de cualquier persona, entonces en este esquema se debe analizar ¿qué riesgos potenciales de violentar la seguridad existen?, consiguiendo las siguientes posibilidades:

- ✓ Un usuario puede ñprestaròla clave de acceso a otra persona, violentando así los principios de seguridad que deben observar todos los miembros de una institución en cuanto a gerenciamiento de datos, poniendo en grave riesgo la integridad y confiabilidad de los mismos, con el riesgo de que estas claves de acceso se propaguen y terminen al final siendo públicas.

  El correctivo que se debe tomar , es simplemente una política adecuada y una administración que logre concientizar a la gente, de los riesgos de ñprestaròla clave de acceso a otros usuarios que no pertenezcan al grupo de trabajo o al departamento. Se puede presentar también el caso en que un usuario pertenezca a varios grupos de usuarios a la vez.

- ✓ Alguna persona puede ñadivinaròla clave de acceso de otra persona. El mecanismo de password en algunos sistemas adolece de muchas fallas. Es fácil escribir un programa que haga una revisión automática de passwords, intentando por ejemplo:

  - Clave de acceso igual al nombre del usuario o derivadas de él. Eje. ñJuan", ñMaríaò, etc.,

  - Claves típicas como ñalfaò, ñbetaò, ñgrupoò, etc.,

  - Claves derivadas de algún dato del usuario: número de teléfono, número de domicilio, nombre de la calle donde vive, etc.,

  - Claves derivadas del trabajo que realiza: nombre de alguno de los

recursos, nombre de alguno de los archivos etc.,

Como se puede anotar, la posibilidad de encontrar un password adivinable es considerablemente alta. Se debe por lo tanto educar a los usuarios acerca de elegir su password de manera inteligente. A manera de ejemplo, se ha demostrado que al menos un 1% de los passwords de la gente de habla hispana corresponde a un nombre femenino de los veinte más comunes seguido de un dígito. Esto significa que si se prueba estos veinte passwords con doscientas veintinueve personas, se tiene un 90% de probabilidad de acertar al menos en uno. Un ataque probando clave tras clave de manera automatizada en algunos sistemas puede generar unos diez mil intentos diferentes por minuto, o sea que al cabo de cinco minutos se puede tener un 90% de probabilidad de acertar un password.

Ante estas posibilidades. ¿Existen soluciones?. La verdad es que hay al menos tres:

- Mantener un registro de los intentos fallidos de acceso.,
- Producir un retardo de varios segundos cuando se produce un intento fallido de acceso.,
- Desconectar el computador después de unos pocos intentos fallidos de acceso (tres o cuatro como máximo).

1.4. Seguridad de Red

En este punto se examinan con detalle la seguridad de red. Se pretende explicar que es la seguridad, como puede protegerse y de que medios se dispone para ayudarse en estas tareas, así presentamos los niveles de seguridad:

- ✓ **Niveles de seguridad**

De acuerdo a las normas de seguridad establecidas por el Departamento de la Defensa de los EEUU, los criterios estándar de evaluación de computadoras confiables, conocidos como Libro Naranja, usan varios niveles de seguridad para proteger de ataques al Hardware, Software y la información almacenada. Estos niveles se refieren a diferentes tipos de seguridad física, autentificación de usuario, confiabilidad del software de sistema operativo y aplicaciones de usuario. Estos estándares también imponen límites a los sistemas que pueden conectarse al suyo.

El Libro Naranja ha permanecido sin cambios desde que se adoptó como estándar del Departamento de la Defensa en 1985. Durante muchos años, se ha constituído en el método básico para evaluar la seguridad de sistemas operativos multiusuario en mainframes y minicomputadores. Otros subsistemas, como las bases de datos y redes, han sido evaluados mediante las interpretaciones del Libro Naranja, como la interpretación de bases de datos confiables y la interpretación de redes confiables.

- **Nivel D1**

Este nivel es la forma más baja de seguridad. Esta forma establece que el sistema entero no es confiable. No se dispone de protección para el Hardware; el sistema operativo se compromete fácilmente y no existe autentificación respecto de los usuarios y los derechos a tener acceso a la información almacenada en la computadora. Este nivel de seguridad por lo general se refiere a los sistema operativos como MS-DOS, MS-WINDOWS y el Sistema 7.x de Apple Macintosh.

Estos sistemas operativos no distinguen entre los usuarios y no tienen definido ningún método para determinar quien está en el teclado. Así mismo, no tiene ningún control con respecto a la información a la que se puede tener acceso en las unidades de disco duro de la computadora.

- **Nivel C**

Este Nivel tiene dos Subniveles de seguridad: el C1 y el C2.

Subnivel C1

Este nivel, ñsistema de protección de seguridad discrecionalò, se refiere a la seguridad disponible en un sistema con cierto nivel de protección para el hardware, ya que este no puede comprometerse fácilmente, aunque es posible. Los usuarios deben identificarse ante el sistema mediante su ñLoginò y su contraseña. Se emplea esta combinación para determinar los derechos de acceso a programas e información que tiene cada usuario.

Subnivel C2

Este subnivel está diseñado para ayudar a resolver los problemas

anteriores.

Además de las funciones del C1, este nivel cuenta con características adicionales que crean un ambiente de acceso controlado. Este tiene la capacidad de restringir aun más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, con base no solo en los permisos, sino tambien en los niveles de autorización. Además, este nivel de seguridad requiere que se audite el sistema, lo cual implica registrar una auditoría por cada acción que ocurra en el sistema.

- **Nivel B**

Este nivel consta de dos Subniveles:

Subnivel B1.

Este nivel también llamado ñProtección de seguridad etiquetadaò, es el primer nivel con soporte para seguridad multinivel, como el secreto y el ultrasecreto. En este subnivel se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

Subnivel B2.

Este Subnivel conocido como ñProtección Estructuradaò, requiere que todos los objetos estén etiquetados. Los dispositivos como discos, cintas y terminales pueden tener asignado uno o varios niveles de seguridad. Este es el primer nivel en el que se aborda el problema de la comunicación de un objeto con otro que se encuentra en un nivel de seguridad inferior.

Nivel A

Conocido como de ñdiseño Verificadoò, constituye actualmente el

nivel de seguridad más alto en todo el Libro Naranja. Cuenta con un proceso escrito de diseño, control y verificación. Para alcanzar este nivel de seguridad, deben incluirse todos los componentes de los niveles inferiores; el diseño debe verificarse matemáticamente, y debe realizarse un análisis de los canales cubiertos y de distribución confiable.

2. CONSIDERACIONES EN MATERIA DE SEGURIDAD PARA LOS SISTEMAS DE LA FUERZA TERRESTRE.

2.1. Política de Seguridad

Al desarrollar e implementar las políticas que reflejan la seguridad en una red determinada, pueden adoptarse dos formatos principales:

Lo que no-se permite expresamente esta prohibido.- Es el primer enfoque de seguridad. Esto significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida. Por ejemplo, si se decide permitir transferencias de FTP (FILE TRANSFERENCE PROTOCOL) anónimo con una máquina en particular, pero negar los servicios telnet, entonces la documentación de FTP y no de telnet ilustra este enfoque.

Lo que no-se prohibe expresamente esta permitido. Esto significa que, a menos que se indique expresamente que cierto servicio no está disponible, todo lo demás sí lo estará. Por ejemplo si no se dice que están prohibidas las sesiones de telnet con un host determinado, entonces sí están permitidas (Sin embargo, se puede impedir este servicio, no permitiendo la conexión con el puerto TCP/IP.)

Al margen de la línea de pensamiento que se siga, las razones detrás de definir una política de seguridad, es determinar que acciones deben tomarse en caso de que se comprometa la seguridad de una organización. La política también debe dirigirse a describir que acciones se toleran y cuáles

no.

2.2. Seguridad de Redes.

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la organización. Vale la pena implementar una política de seguridad, si los recursos y la información que la organización tiene en las redes merecen protegerse. La mayoría de las organizaciones tienen en las redes información delicada y secretos importantes; esto debe protegerse del vandalismo del mismo modo que se protegen otros bienes.

La mayoría de los diseñadores de redes, por lo general empiezan a implementar soluciones de firewall (pared de fuego), antes de que se haya identificado un problema particular de seguridad de red. Quizá, una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de inter-redes y recursos cuyo acceso se permitirá a los usuarios, y cuáles tendrán que restringirse debido a los riesgos de seguridad.

Si actualmente los usuarios tienen acceso irrestricto a la red, se torna difícil aplicar una política que limite ese acceso. También se debe tomar en cuenta, que la política de seguridad que debe usar es tal, que no disminuirá la capacidad de su organización. Una política de red que impide que los usuarios cumplan efectivamente con las tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo que la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

2.3. Política de seguridad del Sitio

Una organización puede tener muchos sitios, y cada uno contar con las propias redes. En organizaciones grandes, como es el caso de la Fuerza Terrestre, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes. Si esos sitios no están conectados a través de una red interna, cada uno de ellos puede tener las propias políticas de seguridad de red. Sin embargo, si los sitios están conectados mediante una red interna, la política de red debe abarcar todos los objetivos de los sitios interconectados.

En general, un sitio es cualquier parte de la organización que posee computadoras y recursos relacionados con redes. Algunos, no todos de esos recursos son los siguientes:

- ✓ Estaciones de trabajo,
- ✓ Computadoras hosts y servidores,
- ✓ Dispositivos de interconexión: gateways, routers, bridges, repetidores,
- ✓ Servidores de terminal,
- ✓ Software para conexión de red y de aplicaciones,
- ✓ Cables de red,
- ✓ La información de archivos y bases de datos

La política de seguridad del sitio debe tomar en cuenta la protección de esos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar a necesidades y requerimientos de seguridad de todas las redes interconectadas.

2.4. Planteamiento de la Política de Seguridad

Definir una política de seguridad de red significa elaborar

procedimientos y planes que salvaguarden los recursos de la red contra pérdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ✓ ¿Qué recursos se está tratando de proteger?,
- ✓ ¿De quiénes necesita proteger los recursos?,
- ✓ ¿Qué tan posibles son las amenazas?,
- ✓ ¿Qué tan importante es el recurso?,
- ✓ ¿Qué medidas puede implementar para proteger los bienes de forma económica oportuna?,
- ✓ Examine periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

La hoja de trabajo que se presenta en la ilustración No 4.1, sirve para ayudar a canalizar las ideas conforme a estos lineamientos.

La columna ñNúmero de recursos de redò es un número de red de identificación interna de los recursos que van a ser protegidos (si se aplica).

La columna ñNombre del recurso de redòes la descripción en lenguaje común de los recursos.

La ñImportanciaòdel recurso puede estar en una escala numérica del 0 al 10, o en expresiones vagas de lenguaje natural como bajo, alto, media, muy alto, etcétera.

Recursos de la Red	**Tipo de usuario**	**Posibilidad**	**Medidas que se**

Ord.	Nombre	Importancia	del que se debe proteger los recursos	de amenaza	implementarán para proteger la Red

Ilustración No 4.1. Formato para planificar la Seguridad

La columna ñTipo de usuario del que hay que proteger al recursoò puede tener designaciones como interno, externo, invitado o nombres de grupos como usuarios de contabilidad, asistentes corporativos, etc.

La columna ñPosibilidad de una amenazaò puede estar en una escala numérica del 0 al 10, o en expresiones de lenguaje natural como baja, alta, media, muy alta, etcétera.

La columna ñMedidas que se implementarán para proteger la Redò puede tener valores tales como permisos de sistema operativo para archivos y directorios; ñpistas/alertas de auditoríaò para servicios de red; routers de selección y ñfirewallsò para hosts y dispositivos para conectividad de red; y cualquier otra descripción del tipo de control de seguridad.

En general, el costo de proteger la red de una amenaza debe ser menor que el de recuperación, en caso de que se viera afectado por una amenaza de seguridad. Si no se tiene el conocimiento suficiente de lo que está protegiendo y de las fuentes de la amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

Es importante, hacer que en el diseño de la política de seguridad

participe gente adecuada, por las características mismas de la Institución armada. Quizá ya tenga grupos de usuarios que podrían considerar que su especialidad es la implementación de la política de seguridad de red. Estos grupos podrían incluir a quienes están implicados en el control de auditoría, grupos de sistemas de información y organizaciones que manejan la seguridad física. Si se desea que la política de seguridad tenga apoyo, es importante hacer participar a estos grupos, de modo que se obtenga su cooperación y aceptación de la política de seguridad de red.

2.5. Responsabilidad en la Política de Seguridad

Un aspecto importante de la Política de Seguridad de red es, asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Es difícil que una política de seguridad se anticipe a todas las amenazas posibles. Sin embargo, las políticas sí pueden asegurar que para cada tipo de problema haya alguna persona que lo pueda manejar de manera responsable. Pueden haber muchos niveles de seguridad relacionados con la política de seguridad. Por ejemplo, cada usuario de la red debe ser responsable de cuidar su contraseña. El usuario que permite que su contraseña se vea comprometida incrementa la posibilidad de poner en riesgo otras cuentas y recursos. Por otra parte los administradores de la red y del sistema son responsables de administrar la seguridad general de la red.

2.6. Análisis de Riesgo

Cuando se establece una política de seguridad de red, es importante que se comprenda que la razón para crear esta es, en primer lugar, asegurar que los esfuerzos dedicados a la seguridad sean costeables. Esto significa que se debe conocer cuáles recursos vale la pena proteger y cuáles son más importantes que otros. También debe identificar la fuente de amenazas de la que está protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red,

muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas pérdidas causadas por los usuarios internos son mucho mayores, que aquellas causadas por usuarios externos.

El análisis de riesgo implica determinar lo siguiente.

- ✓ Qué se necesita proteger,
- ✓ De qué se necesita protegerlo,
- ✓ Cómo protegerlo.

Los riesgos deben clasificarse por el nivel de importancia y gravedad de la pérdida. No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor. En el análisis de riesgo hay que determinar los siguientes factores:

- ✓ Estimación del riesgo de perder el recurso (Ri),
- ✓ Estimación de la importancia del recurso (Wi).

Puede asignarse un valor numérico, para cuantificar el riesgo de perder un recurso. Por ejemplo, puede asignarse un valor de 0 a 10 al riesgo (Ri) de perder un recurso, en donde 0 representa que no hay riesgo y 10 representa el más alto riesgo. De igual modo, a la importancia de un recurso (Wi) se le puede asignar un valor del 0 a 1 en donde 0 representa que no tiene importancia y 1 representa la máxima importancia. El riesgo evaluado del recurso será el producto del valor del riesgo y de su importancia (también llamada peso). Esto puede escribirse como sigue:

WRi = Ri*Wi

WRi = Riesgo evaluado del recurso ñò

Ri = Riesgo del recurso ñò

Wi = Importancia (peso) del recurso ñò

En una red simplificada con un router, un servidor y un bridge; suponiendo que los administradores de la red y del sistema hayan encontrado las siguientes estimaciones del riesgo y de la importancia de los dispositivos de red.

Router:

R1 = 7

W1 = 0.4

Bridge:

R2 = 4

W2 = 0.5

Servidor:

R3 = 8

W3 = 0.7

El cálculo de los riesgos evaluados de estos dispositivos se muestra a continuación:

Router:

WR1 = R1 * W1 = 7 * 0.4 = 2.8

Bridge:

WR2 = R2 * W2 = 4*0.5 = 2

Servidor:

WR3 = R3 * W3 = 8 * 0.7 = 5.6

En la ilustración 4.2, se muestra una hoja de trabajo que se puede usar para registrar los cálculos anteriores.

La columna ñNúmero de recursos de redò es un número de red de identificación interna del recurso (si se aplica).

Recursos de la Red		**Riesgo de los recursos de la Red (Ri)**	**Importancia (peso)del recurso (Wi)**	**Riesgo evaluado. (Ri * Wi)**
N Ord	**Nombre**			

Ilustración 4.2, Formato para Análisis de Riesgo de Seguridad

La columna ñNombre del recurso de redò es una descripción en lenguaje común de los recursos.

La columna ñRiesgo de los recursos de red (Ri)" puede estar en una escala numérica del 0 al 10 en expresiones ñvagasò de lenguaje natural como: bajo, medio, alto, muy alto, etcétera.

De igual modo, la columna ñImportancia (peso) del recurso (Wi)" puede estar en una escala numérica del 0 al 1, o en expresiones ñvagasòde lenguaje natural como bajo, medio, alto, muy alto, etcétera.

Si se usa valores numéricos en las columnas de riesgo e importancia, puede calcular el valor de la columna ñRiesgo evaluado (Ri*Wi)ò, como el producto de los valores de riesgo y peso

El riesgo general de los recursos de la red se puede calcular mediante la siguiente fórmula:

WR = (R1*W1 + R2*W2 + ... + Rn*Wn)/(W1 + W2 + ... + Wn)

El riesgo general de la red del ejemplo sería como sigue:

WR = (R1*W1 + R2*W2 + R3*W3) /(W1 + W2 +W3)

= (2.8 + 2 + 5.6) / (0.4 + 0.5 + 0.7)

= 10.4/1.6

= 6.5

La evaluación de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se defina en la política de seguridad del sitio.

Otros factores que hay que considerar al estimar el riesgo de un recurso de red son su disponibilidad, integridad y confidencialidad.

La ***disponibilidad*** de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo.

La ***integridad*** de un recurso es la medida de qué tan importante es que éste o los datos del mismo sean consistentes. Esto es de particular importancia para los recursos de bases de datos.

La ***confidencialidad*** se aplica a recursos, tales como archivos de datos, a los cuales se desee restringir el acceso.

2.7. Recursos de Red que requieren protección

Los recursos de red que se debe considerar al calcular las amenazas a la seguridad general, son:

- ✓ **Hardware**: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers,
- ✓ **Software**: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones,
- ✓ **Datos**: durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos, en tránsitos a través de medios de comunicación,
- ✓ **Documentación:** sobre programas, hardware, sistemas, procedimientos administrativos locales,
- ✓ **Suministros**: papel, formularios, cintas, medios magnéticos.

2.8. Identificación de las Amenazas

Una vez que se han identificado los recursos que requieren protección, se debe identificar las amenazas a las que están expuestos. Pueden examinarse las amenazas para determinar qué posibilidad de pérdida existe. También se debe identificar de qué amenazas se está tratando de proteger a los recursos.

- ✓ **Definición del acceso no Autorizado**

El acceso a los recursos de la red debe estar permitido sólo a los usuarios autorizados. Esto se llama acceso autorizado. Una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de cómputo. Este acceso puede tornar muchas formas, como

el uso de la cuenta de otro usuario para tener acceso a la red y los recursos. En general, se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado.

La gravedad del acceso no autorizado depende del sitio y de la naturaleza de la pérdida potencial. En algunos sitios, el solo hecho de conceder acceso a un usuario no autorizado puede causar daños irreparables por la cobertura negativa de los medios.

Algunos sitios, debido a su tamaño y visibilidad, pueden ser objetivos más frecuentes que otros, como el caso específico de centros de cómputo y redes de organismos y unidades militares.

- ✓ **Riesgos de revelación de Información**

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Se debe determinar el valor y delicadeza de la información guardada en las computadoras. En el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información específica de un producto representan una ventaja competitiva. Las bodegas de las unidades militares, los departamentos de Personal, Inteligencia, Operaciones, Financieros etc., mantienen información confidencial, cuyos sistemas pueden ser objeto de espionaje por parte del personal enemigo que directa o indirectamente puedan tener acceso a la misma y cuya revelación puede ser perjudicial para la seguridad de la Institución militar.

A nivel del sistema, la revelación de un archivo de contraseñas puede volverlo vulnerable a accesos no autorizados en el futuro. Para muchas organizaciones, un vistazo a una propuesta o un proyecto de investigación que represente muchos años de trabajo puede darle a su competidor una ventaja injusta.

✓ **Negación del Servicio**

Las redes vinculan recursos valiosos, como computadoras y bases de datos, y proporcionan servicios de los cuales depende una organización militar. La mayoría de los usuarios depende de estos servicios para realizar su trabajo con eficacia. Sí no están disponibles estos servicios, se corre el grave peligro de no tener los datos necesarios para la toma de decisiones oportunas.

Es difícil predecir la forma en que se produzca la negación del servicio. Los siguientes son algunos ejemplos de cómo la negación de servicios puede afectar una red.

- La red puede volverse inservible por un paquete extraviado,
- La red puede volverse inservible por inundación de tráfico,
- La red puede ser fraccionada al desactivar un componente importante, como el router que enlaza los segmentos de la red,
- Un virus puede alentar o invalidar un sistema de cómputo al consumir los recursos del sistema,
- Los dispositivos reales que protegen a la red podrían subvertirse,
- Se debe determinar qué servicios son absolutamente esenciales y, para cada uno de ellos, determinar el efecto de su pérdida. También debe contar con políticas de contingencia para recuperarse de tales pérdidas.

2.9. Uso y responsabilidad de la Red

Existen numerosas cuestiones que deben abordarse al elaborar una

política de seguridad:

- ✓ ¿Quién está autorizado para usar los recursos?,
- ✓ ¿Cuál es el uso adecuado de los recursos?,
- ✓ ¿Quién está autorizado para conceder acceso y aprobar el uso,
- ✓ ¿Quién puede tener privilegios de administración del sistema?,
- ✓ ¿Cuáles son los derechos y las responsabilidades del usuario?,
- ✓ ¿Cuáles son los derechos y las responsabilidades del administrador del sistema, en comparación con los de los usuarios?,
- ✓ ¿Qué se hace con la información delicada?

2.10. Identificación de quién está autorizado para usar los recursos de la Red

Debe hacerse una lista de los usuarios que necesitan tener acceso a los recursos de la red. No es necesario enlistar a cada usuario. La mayoría de estos pueden dividirse en grupos como usuarios de Inteligencia, Personal, Operaciones, Logística, etc. También se debe tomar en cuenta una clase llamada usuarios externos. Esta se compone de los usuarios que tengan acceso a una red desde otras partes, como estaciones de trabajo autónomas y otras redes, pueden o no ser parte de la institución, o bien, pueden ser empleados que tengan acceso a la red desde los hogares o durante un viaje.

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, se establecen los lineamientos del uso aceptable de dichos recursos. Aquellos dependerán de la clase de usuarios, como desarrolladores de software, operadores, usuarios externos, etc. Se debe tener lineamientos separados para cada clase. La política debe establecer

que tipo de uso aceptable y cual es inaceptable, así como que tipo de uso está restringido. La responsabilidad de cada usuario existe al margen de los mecanismos de seguridad implantados. No tiene caso construir costosos mecanismos con altos grados de seguridad si un usuario puede revelar la información copiando archivos en disco o cinta y poner los datos a disposición de usuarios no autorizados.

2.11. Determinación de responsabilidades del Usuario

Es muy importante que la política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red. La siguiente es una lista de los aspectos que se puede abordar respecto de las responsabilidades de los usuarios:

- ✓ Lineamientos acerca del uso de los recursos de red, tales como, qué usuarios están restringidos y cuáles son las restricciones,
- ✓ Qué constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red,
- ✓ ¿Está permitido que los usuarios compartan cuentas o permitan a otros usar la suya?,
- ✓ ¿Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a las cuentas?,
- ✓ Política de contraseña de usuario: ¿con qué frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hay al respecto?,
- ✓ ¿Los usuarios son responsables de hacer respaldos de los datos o es esto responsabilidad del administrador del sistema?,

- ✓ Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

  En este aspecto, la Asociación de Correo Electrónico (EMA, Electronic Mail Association) recomienda que todo sitio debe tener una política acerca de la protección de la privacidad de los usuarios. Las organizaciones deben establecer políticas que no se limiten al correo electrónico, sino que también abarque otros medios, como discos, cintas y documentos impresos.

2.12. Determinación de Responsabilidades de los Administradores de Sistemas

Muchas veces, el administrador del sistema necesita recabar información del directorio privado de un usuario para diagnosticar problemas del sistema. Los usuarios por otra parte tienen el derecho de conservar su privacidad. Existe, por lo tanto una contradicción entre el derecho del usuario a la privacidad y las necesidades del administrador del sistema. Cuando se presentan amenazas a la seguridad de la red, el administrador del sistema tendrá mayor necesidad de recabar información de los archivos, incluidos los del directorio base de los usuarios.

La política de seguridad de la red debe especificar el grado al que el administrador del sistema pueda examinar los directorios y archivos privados de los usuarios para justificar problemas del sistema e investigar violaciones de la seguridad. Si la seguridad de la red está en riesgo, la política debe permitir mayor flexibilidad para que el administrador solucione los problemas de seguridad. Otros aspectos relacionados que se debe abordar son los siguientes:

- ✓ ¿Puede el administrador revisar o leer los archivos de un usuario por alguna razón?,

- ✓ ¿Los administradores de la red tienen el derecho de examinar el trafico de la red o del host?,

- ✓ ¿Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización, por tener acceso no autorizado a los datos privados de otras personas?

2.13. Que hacer con la Información Delicada

Debido a que los datos contenidos en los sistemas de la Fuerza Terrestre, son de carácter altamente confidencial, se debe determinar qué tipo de datos delicados pueden almacenarse en un sistema específico. Desde el punto de vista de la seguridad, la información en extremo delicada, como nóminas y planes, organización, información de inteligencia, etc., debe estar restringida a unos cuantos hosts y administradores de sistemas. Para concederle a un usuario acceso a un servicio de un host, se debe considerar qué otros servicios e información se proporcionan y a los cuales el usuario podría tener acceso. Si el usuario no tiene necesidad de manejar información delicada, no debe tener una cuenta en un sistema que contenga dicho material.

También debe considerar si existe una seguridad adecuada en el sistema para proteger la información delicada. Por otra parte, asegurar un sistema puede implicar hardware, software y costos adicionales de administración, por lo cual puede no ser rentable asegurar datos en un host que no sea muy importante para la organización o los usuarios.

La política también debe tomar en cuenta el hecho de que se necesita decirle a los usuarios que pueden guardar información delicada, que servicios son apropiados para el almacenamiento de dichos datos.

2.14. Plan de Acción cuando se viole la Política de Seguridad

Cada vez que se viola la Política de Seguridad, el sistema está sujeto

a amenazas. Si no se producen cambios en la seguridad de la red cuando ésta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posible. Si la política de seguridad es demasiado restrictiva, o está explicada inadecuadamente, es muy probable que sea violada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que se establezcan deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando se detecte una violación a la política de seguridad, debe determinar si ésta ocurrió debido a la negligencia de un usuario, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. En este último caso, la violación quizá haya sido efectuada no sólo por una persona, sino por un grupo que a sabiendas realizó un acto en violación directa de la política de seguridad. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas que se deben tomar.

Debe llevarse a cabo una investigación para determinar las circunstancias en torno a la violación de seguridad, y cómo y por qué ocurrió. La política de seguridad debe contener lineamientos acerca de las acciones correctivas para las fallas de seguridad. Es razonable esperar que el tipo y severidad de la acción dependerán de la gravedad de la violación.

2.15. Respuestas a las Violaciones de la Política de Seguridad

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable del acto. Las violaciones a la política pueden ser

cometidas por una gran variedad de usuarios; algunos pueden ser locales y otros externos. Los usuarios locales son llamados usuarios internos y los externos, usuarios foráneos. Por lo general, la distinción entre ambos tipos esta basada en los ***límites*** de red***, administrativos, legales o políticos***.

El tipo de ***límite*** determina cuál debe ser la respuesta a la violación de la seguridad.

La organización debe definir la acción según el tipo de violación. Estas acciones requieren ser definidas con claridad, con base en el tipo de usuario que haya violado la política de seguridad de cómputo. Los usuarios internos y externos de la red deben estar conscientes de la política de seguridad. Si hay usuarios externos que utilicen legalmente la red, es responsabilidad de la organización verificar que esas personas conozcan las políticas que se han establecido. Esto es de particular importancia si se tiene que emprender acciones legales en contra de los transgresores. Si se ha producido una pérdida significativa, quizá se tendrá que tomar acciones más drásticas.

El documento de la política de seguridad también debe contener procedimientos para manejar cada tipo de incidente de violación. Debe llevarse un registro apropiado de tales violaciones, el cual ha de revisarse periódicamente para observar tendencias y tal vez ajustar la política de seguridad para que dicha política tome en cuenta cualquier nuevo tipo de amenaza.

2.16. Respuestas a las violaciones de la Política de Seguridad por usuarios locales

Esto podría ocurrir en las siguientes situaciones:

- ✓ Un usuario local viola la política de seguridad de un sitio local,
- ✓ Debido a que se viola la política de seguridad interna, se tendrá más

control sobre el tipo de respuesta ante esta violación de seguridad,

- ✓ Un usuario local viola la política de seguridad de un sitio remoto,
- ✓ Esto podría ocurrir a través de una conexión como Internet. Esta situación se complica por el hecho de que está implicada otra organización, y cualquier respuesta que se tome tendrá que discutirse con la organización cuya política de seguridad fue violada por un usuario local nuestro.

2.17. Estrategias de respuesta ante Incidentes de Seguridad

Existen dos tipos de estrategias de respuesta ante incidentes de seguridad:

Proteja y continúe

Si los administradores de la política de seguridad sienten que la organización es bastante vulnerable, quizá sea una buena estrategia, proteger y continuar. El objetivo de esta política es proteger de inmediato a la red y restablecerla a su situación normal, para que los usuarios puedan seguir usándola. Para hacer esto, se tendrá que interferir activamente con las acciones de intruso y evitar mayor acceso. A esto debe seguir el análisis del daño causado.

En ocasiones no es posible restablecer la red de inmediato a su funcionamiento normal; quizá tenga que aislar los segmentos y apagar sistemas, con el objeto de evitar más accesos no autorizados en el sistema. La desventaja de este procedimiento es que los intrusos saben que ya fueron detectados y tomarán medidas para evitar que sean rastreados. Asimismo, el intruso puede reaccionar a su estrategia de protección atacando el sitio con otro método; por lo menos, es probable que el intruso

continúe su vandalismo en otro sitio.

La estrategia de proteger y continuar puede usarse en las siguientes circunstancias:

- ✓ Si los recursos de la red no están bien protegidos de los intrusos,
- ✓ Si la continua actividad del intruso pudiera resultar en daños y riesgos financieros considerables,
- ✓ Si existen considerables riesgos para los usuarios actuales de la red,
- ✓ Si en el momento del ataque no se conocen los tipos de usuario de una gran red interna.

Persiga y demande

Esta estrategia adopta el principio de que el objetivo principal es permitir que los intrusos continúen las actividades mientras se los vigila. Esto debe hacerse en forma lo más discreta posible, de modo que los intrusos no se den cuenta de que se los está vigilando. Deben registrarse las actividades de los intrusos, para que haya pruebas disponibles en la fase de demanda de esta estrategia. La desventaja es que el intruso seguirá robando información o haciendo otros daños, y de todos modos se estará sujeto a demandas legales derivadas del daño al sistema y la pérdida de información.

En las siguientes circunstancias se puede seguir la estrategia de ***perseguir y demandar***:

- ✓ Si los recursos del sistema están bien protegidos,
- ✓ Si se trata de un ataque concentrado y ya ha ocurrido antes,
- ✓ Si el sitio es muy notorio y ha sido víctima de ataques,

- ✓ Si el sitio está dispuesto a arriesgar los recursos de la red permitiendo que continúe la intromisión,

- ✓ Si puede controlarse el acceso del intruso,

- ✓ Si las herramientas de vigilancia están bien desarrolladas para crear registros adecuados y recabar evidencias para la demanda,

- ✓ Si cuenta con personal capacitado interno para construir rápidamente herramientas especializadas.

2.18. Interpretación y Publicación de la Política de Seguridad

Es importante identificar a las personas que interpretarán la política. Generalmente no es aconsejable que sea una sola persona, ya que podría no estar disponible el momento de la crisis. Se puede designar a un Comité, pero también se recomienda que no esté constituido por muchos miembros. De vez en cuando, se convocará al comité de política de seguridad para interpretar, repasar y revisar el documento.

Una vez que se haya redactado la política de seguridad y se haya alcanzado el consenso en sus puntos, el sitio debe asegurarse de que la declaración de política se divulgue y discuta ampliamente. Podrán utilizarse listas de correo. Puede reforzarse la nueva política mediante educación interna, como seminarios de capacitación, sesiones informativas, talleres, reuniones personales con el administrador.

En ocasiones, los nuevos programas son recibidos con entusiasmo al principio, cuando todos están conscientes de la política. Con el tiempo, empero, existe la tendencia a olvidar el contenido. Los usuarios necesitan recordatorios periódicos. Asimismo, cuando llegan usuarios nuevos a la red, éstos necesitan conocer la política de seguridad.

Los recordatorios periódicos (debidamente programados) y la

capacitación contínua acerca de la política, incrementarán las posibilidades de que los usuarios sigan dicha política de seguridad. Debe incluirse la política de seguridad en el paquete de información de los usuarios nuevos. Algunas organizaciones requieren que cada usuario de la red firme una declaración en la que se especifique que han leído y comprendido la política.

2.19. Identificación y Prevención de problemas de Seguridad

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente cómo deberán protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deberán implementarse para evitar problemas de seguridad. La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad.

Antes de establecer los procedimientos de seguridad se debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo. Pueden usarse las secciones anteriores, ñPlanteamiento de la política de seguridadò y "Análisis de riesgo", así como los formatos indicados en las ilustraciones 4.1 y 4.2, como guía para centrar la atención en los recursos más importantes de la red.

Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas tengan más protección de la que necesitan, y que otras áreas más importantes no tengan suficiente protección.

Establecer una política de seguridad eficaz, requiere considerable esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario para que los usuarios

de la red la entiendan adecuadamente.

Además de realizar el análisis de riesgo de los recursos de la red, se deben identificar otros puntos vulnerables. La siguiente lista: puntos de acceso, sistemas configurados inadecuadamente, problemas de software, amenazas internas y seguridad física; intentan describir algunas de las áreas más problemáticas. Esta lista lo puede orientar en la dirección correcta, pero de ningún modo está completa, ya que es probable que un sitio tenga algunos puntos vulnerables particulares.

- ✓ **Puntos de Acceso**

Los puntos de acceso son los puntos de entrada (también llamados de ingreso), para los usuarios no autorizados. El tener muchos puntos de acceso incrementan los riesgos de seguridad de la red.

Por lo tanto; puede evitarse las posibilidades de acceso, si la política de seguridad de la red le informa al usuario que están prohibidas las conexiones privadas a través de las estaciones de trabajo individuales. Esta situación también subraya la importancia de tener una política de seguridad en la que se define con claridad la política de uso aceptable para la red.

Si se quiere conectar a Internet, se debe tener por lo mínimo un vínculo con redes fuera de la organización. El vínculo de red hace disponibles numerosos servicios de red, tanto dentro como fuera de esta, y cada servicio es susceptible de ser comprometido.

Los servidores terminales pueden representar un riesgo si no están protegidos adecuadamente. Muchos de los servidores terminales que hay en el mercado no requieren ningún tipo de su autentificación. Se debe consultar al distribuidor acerca de la capacidad de autentificación del servidor terminal. Los intrusos pueden utilizar a dichos servidores para disfrazar sus acciones, marcando al servidor terminal y teniendo acceso a la

red interna.

- ✓ **Sistemas mal configurados**

Cuando los intrusos penetran en la red, por lo general tratan de subvertir los hosts del sistema. Los blancos preferidos son los hosts que actúan como servidores. Si el host está mal configurado, el sistema puede ser subvertido con facilidad, los sistemas mal configurados son responsables de numerosos problemas de seguridad de red.

Los modernos sistemas operativos y su software correspondiente se han vuelto tan complicados, que entender cómo funciona el sistema no sólo es un trabajo de tiempo completo, sino que requiere conocimientos especializados. Los distribuidores también pueden ser responsables de la mala configuración de los sistemas. Muchos envían los sistemas con la seguridad totalmente abierta. Las contraseñas de cuentas importantes pueden no estar establecidas, o usar combinaciones de contraseñas y logins fácilmente descifrables.

- ✓ **Problemas de Software**

Al aumentar la complejidad del software, también aumenta el número y la complejidad de los problemas de un sistema determinado. A menos que se encuentren formas revolucionarias de crear software, éste nunca estará por completo libre de errores. Las fallas de seguridad conocidas públicamente se vuelven métodos comunes de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida, el intruso puede usar los puntos débiles del código de software que se ejecuta en modo privilegiado para tener acceso privilegiado al sistema.

Los administradores de sistemas deben estar conscientes de los puntos débiles de sus sistemas operativos y tienen la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se

descubran estos problemas.

- ✓ **Amenazas Internas**

Por lo general, los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario interno decide subvertir la red, puede representar una considerable amenaza a la seguridad de la red. Si se tiene acceso físico a los componentes de un sistema, éste es fácil de subvertir. Por ejemplo, pueden manipularse fácilmente las estaciones de trabajo para que otorguen acceso privilegiado.

- ✓ **Seguridad Física**

Si la computadora misma no está físicamente segura, pueden ignorarse fácilmente los mecanismos de seguridad del software. En el caso de las estaciones de trabajo DOS/Windows, ni siquiera existe un nivel de contraseña de protección. Si se deja desatendida una estación de trabajo, sus discos pueden ser cambiados o si se deja en modo privilegiado, la estación estará completamente abierta. Asimismo, el intruso puede parar la máquina y regresarla a modo privilegiado, o tomar cualquier medida para dejar al sistema abierto para ataques futuros.

Todos los recursos importantes de la red, como las backbones, los vínculos de comunicación, los hosts, los servidores importantes y los mecanismos clave deben estar ubicados en una área físicamente segura. Por ejemplo, el mecanismo de autentificación requiere que el servidor esté físicamente seguro. **Físicamente seguro,** significa que la máquina esté guardada en una habitación o colocada de tal modo que se restrinja el acceso físico a ella.

En ocasiones no es fácil asegurar físicamente las máquinas. En esos casos, se debe tener cuidado para no confiar demasiado en esas máquinas. Se debe limitar el acceso desde máquinas no seguras hacia las más

seguras.

- ✓ **Vulnerabilidad de la Confidencialidad**

Las siguientes son algunas de las situaciones en las que la información delicada es vulnerable de ser divulgada.

- Cuando la información está almacenada en un sistema de cómputo,
- Cuando la información está en tránsito hacia otro sistema en la red,
- Cuando la información está almacenada en cintas de respaldo.

El acceso a la información que está almacenada en una computadora, está controlado mediante los permisos de archivo (lectura, escritura, ejecución), las listas de control de acceso (ACL) y otros mecanismos similares. La información en tránsito puede protegerse mediante la encriptación o firewalls. La encriptación puede usarse para proteger la información en las tres situaciones. El acceso a la información almacenada en cintas puede controlarse mediante la seguridad física, como puede ser, guardar las cintas en una caja de seguridad o en un área inaccesible.

2.20. Detección y vigilancia de actividades no autorizadas.

Si ocurre una intrusión o un intento de intrusión, debe detectarse tan pronto como sea posible. Se puede implantar varios procedimientos sencillos para detectar el uso no autorizado de un sistema de cómputo. Algunos procedimientos se basan en herramientas proporcionadas con el sistema operativo por el proveedor.

- ✓ **Inspección del uso del Sistema**

El administrador del sistema puede realizar periódicamente la inspección. Si no, puede usarse software elaborado con este fin. La inspección de un sistema implica revisar varias de sus partes y buscar cualquier cosa que sea inusual.

La inspección debe hacerse con regularidad. No es suficiente hacerla cada mes o cada semana, ya que esto provocaría una brecha de seguridad que no sería detectada en mucho tiempo. Algunas violaciones de seguridad pueden detectarse unas cuantas horas después de haberse cometido, en cuyo caso no tiene sentido la inspección semanal o mensual. El objetivo de la inspección es detectar la brecha de seguridad en forma oportuna, de modo que se pueda reaccionar adecuadamente a ella.

Si se utiliza herramientas de inspección, debe examinar periódicamente la información de éstas.

- ✓ **Mecanismos de Inspección**

Muchos sistemas operativos almacenan la información de conexiones en archivos de registro especiales. El administrador del sistema debe examinar regularmente estos archivos de registro para detectar el uso no autorizado del sistema. Se puede utilizar el siguiente método para dicho

control.

Puede comparar las listas de los usuarios que estén conectados en ese momento con los registros de las conexiones anteriores. La mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días. Una cuenta que muestre actividad fuera del horario ñormalò del usuario debe inspeccionarse de cerca. Quizá un intruso esté usando esa cuenta. También puede alertarse a los usuarios para que observen el último mensaje de conexión que aparece al momento de hacer su primera conexión. Si notan algún horario inusual deben avisarle al administrador del sistema.

- ✓ **Horario de Inspección**

Los administradores del sistema deben inspeccionar con frecuencia y regularidad a lo largo de todo el día. Puede resultar muy fastidioso inspeccionar por horarios fijos, pero pueden ejecutarse comandos de inspección a cualquier hora, en los momentos desocupados.

Si se ejecutan los comandos de inspección con frecuencia, se familiarizará rápidamente con la información normal de estas herramientas de inspección. Esto le ayudará a detectar la información inusual. Es posible intentar automatizar este proceso ejecutando herramientas de búsqueda sobre la información, y se pueden buscar ciertos patrones fijos, pero generalmente es difícil detectar toda la información inusual causada por la intrusión en el sistema. El cerebro humano sigue siendo mejor que la mayoría de los programas para detectar sutiles diferencias en los registros de inspección.

Si se ejecuta diversos comandos de inspección a diferentes horas del día, será difícil que un intruso prediga sus acciones. El intruso no puede saber cuándo el administrador correrá el comando de inspección para desplegar a los usuarios conectados, por lo que corre mayor riesgo de ser

detectado. Por otra parte, si el intruso sabe que todos los días, a las seis de la tarde, el sistema se revisa para ver que todos se hayan desconectado, esperará a que concluya esta revisión antes de conectarse.

La inspección es útil, pero también puede ser subvertida. Algunos intrusos pueden darse cuenta de los mecanismos estándar de registro de conexiones que se usen en el sistema y pueden tratar de desactivarlos. La inspección periódica puede detectar a los intrusos, pero no ofrece ninguna garantía de que el sistema esté a salvo. No es un método infalible para detectar a los intrusos.

- ✓ **Procedimientos de Reporte**

En caso de que se detecte algún acceso no autorizado, debe haber procedimientos para reportar este acceso y a quién será informado. Además, su política de seguridad debe cubrir los siguientes aspectos:

- Procedimientos de administración de cuentas,
- Procedimientos de administración de configuración,
- Procedimientos de recuperación,
- Procedimiento de reporte de problemas para los administradores del sistema.

- ✓ **Uso de la Encriptación para Proteger la Red**

Puede usarse la encriptación para proteger los datos en tránsito, así como los almacenados. Algunos proveedores ofrecen dispositivos de encriptación de hardware que pueden usarse para encriptar y desencriptar datos en conexiones de punto a punto.

La **Encriptación** puede definirse como el proceso de tomar información que se encuentra en cualquier forma legible y convertirla a una forma que no pueda ser entendida por otros.

Si el receptor de los datos encriptados desea leerlos, debe convertirlos a su forma original en un proceso llamado **Desencriptación**, el cual es el inverso del proceso de encriptación. Para llevar a cabo la desencriptación, el receptor debe contar con un dato especial llamado clave. La clave debe guardarse y distribuirse con extremo cuidado.

La ventaja de usar encriptación es que, aun si el intruso logra vencer otros métodos de protección de datos (listas de control de acceso, permisos de archivo, contraseñas, etcétera), los datos no tendrán significado para él.

Existen muchos tipos de paquetes de encriptación, tanto en hardware como en software. Los paquetes de software de encriptación están disponibles en forma comercial o gratuita. El hardware de encriptación por lo general se construye en torno a procesadores dedicados y es mucho más rápido que su equivalente en software. Por otra parte, si el intruso tiene acceso al hardware, puede elaborar esquemas de desencriptación basados en el mismo hardware que utilizará para un ataque intenso contra la información encriptada.

Los datos que están en tránsito en una red son vulnerables a la interceptación. En algunos sitios se prefiere encriptar todo el archivo, como paso adicional antes de enviarlo. Esto en ocasiones se llama **encriptación de extremo a extremo**. En otros sitios se prefiere encriptar los datos en forma dinámica conforme llegan a la red, mediante hardware de encriptación que crea un **vinculo seguro**.

- ✓ **Estándar de Encriptación de Datos (DES)**

El DES es un mecanismo de encriptación de datos muy utilizado y del

cual existen varias implementaciones tanto en software como en hardware. El DES transforma información de texto llano en datos encriptados, llamado texto cifrado mediante un algoritmo especial y un valor semilla llamado clave. Si el receptor conoce la clave, puede usarla para convertir el texto cifrado en los datos originales.

Un punto débil potencial de todos los sistemas de encriptación es la necesidad de recordar la clave mediante la cual fueron encriptados los datos. En este sentido es similar al problema de recordar la contraseña. Si la clave está por escrito y una persona no autorizada la llega a conocer, los datos originales podrán ser leídos. Si se olvida la clave, entonces no se podrán recuperar los datos originales.

2.21. Encriptación de Datos

Los avances tecnológicos en la actualidad han permitido que usuarios (hackers) u organizaciones interesadas en obtener nuestra información, puedan interferir inclusive en sofisticados sistemas computacionales y de comunicación de datos. En respuesta a este problema se ha desarrollado toda una tecnología en seguridad para transmisión de datos denominada **encriptamiento.**

Los equipos que permiten realizar encriptamiento, se los denomina **encriptores.** Estos equipos permiten conservar la seguridad, reduciendo la vulnerabilidad en un enlace de datos (analógico o digital) principalmente de:

- ✓ Interceptación,
- ✓ Interferencia,
- ✓ Modificación, o
- ✓ Destrucción de los datos,

sean estos accidental o con intencionalidad previa. El fundamento de funcionamiento se basa en la utilización de un algoritmo denominado DES (Data Encryption Standard) el mismo que modifica la posición de los bits dentro de la trama del paquete de datos y de un sistema de administración de claves (Keys) que son variables electrónicas que ingresan como parámetros del DES y lo activan. La finalidad de este algoritmo es proteger los enlaces:

- ✓ Punto a punto,
- ✓ Multipunto,
- ✓ Dial-up,
- ✓ Dedicados

Los tipos de enlaces que pueden manejar son sincrónicos y/o asincrónicos.

2.22. Administración de Claves

Como se indicó anteriormente, las claves permiten ñalimentarò a los algoritmos DES utilizados para encriptar los datos en el transmisor y decriptar los mismos en el receptor. Para disponer de redes totalmente seguras es indispensable contar con el control de las claves. Por tanto es necesario poder realizar las siguientes actividades en total seguridad:

- ✓ Generar,
- ✓ Almacenar,
- ✓ Distribuir,

- ✓ Destruir

Las claves son generalmente de 2 tipos:

- ✓ Claves de encriptamiento de datos (KD),
- ✓ Claves de encriptamiento de claves (KK)

El margen de seguridad esta definido por la *longitud de la clave,* la que generalmente es de 64 o 128 bits. Mientras mayor sea el tamaño de la clave, es mayor la seguridad.

2.23. Generación de claves y Almacenamiento

Los encriptores de datos, generalmente disponen de memoria no-volatil en donde se generan y almacenan automáticamente las claves, cuyos modos de más comunes son:

- ✓ Seguro,
- ✓ Standby,
- ✓ Bypass

2.24. Memoria de Backup

El encriptador de datos debe disponer de una batería de larga duración que sirva de backup cuando se corte la energía eléctrica que alimenta el equipo, y que permita a la memoria principal conservar las claves, los parámetros del sistema, y el reloj.

2.25. Firewall

El Firewall es una **pared de fuego** que da seguridad a la red interna, pudiendo tener intercambio de información limitado con los usuarios externos en el Internet. Es muy selectivo en el control de acceso. Aísla la

red interna de otras redes en la Internet y provee aplicaciones típicas de TCP/IP que accesan máquinas fuera de la red segura. El firewall actúa como barrera entre la red interna y el resto de la Internet. Generalmente utiliza software desarrollado por la Universidad de California, Berkeley y sus proveedores.

Existen muchas maneras por la cual el firewall protege la red. El firewall provee servicios que prohibe o permite el acceso basado en nombre de usuario, nombre host, y protocolo TCP/IP. Un firewall puede proveer además una variedad de servicios permitiendo a usuarios autorizados pasar y mantener fuera a los no autorizados. Toda comunicación entre la red segura e Internet tiene que pasar por el firewall. El mundo exterior no puede ver la estructura de la red y esto mantiene seguro a los datos corporativos.

- ✓ **Servicios y Barreras**

Generalmente un firewall dispone de servicios y barreras para permitir el acceso a usuarios de redes Intranet a servicios Internet. Existe en redes TCP/IP host dedicados, el cual contiene varias tarjetas de interfaz de red, mediante las cuales se permite el acceso a cualquiera de los segmentos de redes LAN. El término gateway es usado para describir la función de enrutamiento desarrollada por los hosts de base múltiple. Actualmente, el ruteo se refiere a enrutar el tráfico entre distintos segmentos de red, mientras que el término gateway se refiere a las funciones de las capas superiores del modelo OSI.

- ✓ **Routers de Selección**

Muchos routers proporcionan la capacidad de seleccionar paquetes con base en criterios como tipo de protocolo, los campos de dirección de origen y dirección de destino para un tipo particular de protocolo y los campos de control que son parte del protocolo.

Estos reuters proporcionan un mecanismo poderoso para controlar el tipo de tráfico de red que puede existir en cualquier segmento de una red. Al controlar este tipo de tráfico, los routers de selección pueden controlar el tipo de servicios que puede existir en un segmento de red. Por lo tanto, pueden restringirse servicios que pueden poner en peligro la seguridad de la red.

- ✓ **Filtración de paquetes**

Por lo general, un filtro de paquetes (router de selección) se coloca entre uno o más segmentos de red. Estos segmentos de red están clasificados como segmentos de red externos (Internet) o internos (red A, red B, etc.). Los segmentos de red externos conectan la red con redes externas como Internet. Los segmentos de red internos se utilizan para conectar los hosts de la institución y otros recursos de la red.

- ✓ **Configuración tipo de Firewall**

En general, una firewall se coloca entre la red interna confiable y la red externa no confiable. La firewall actúa como un punto de cierre que monitorea y rechaza el tráfico de la red al nivel de aplicación. Las firewalls también pueden operar en las capas de red y transporte, en cuyo caso examinan los encabezados IP y de TCP de paquetes entrantes y salientes, y rechazan o pasan paquetes con base en las reglas de filtración de paquetes programadas.

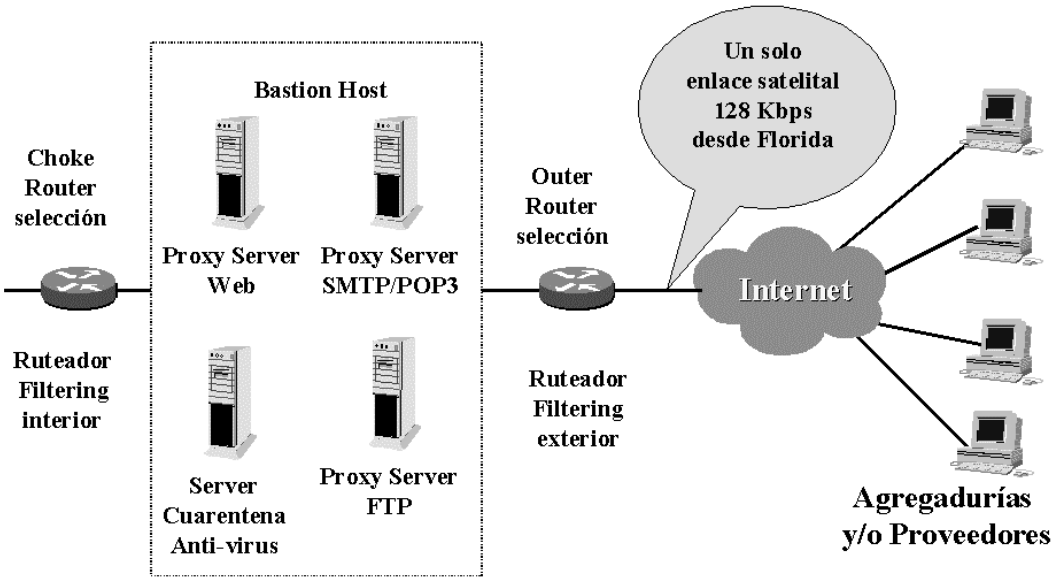


Ilustración 4.1 Configuración tipo de Firewall

La firewall es el principal instrumento utilizado para la implementación de una política de seguridad de la red de una organización. En muchos casos se necesitan técnicas de mejoramiento de la autentificación, la seguridad y la privacía para aumentar la seguridad de la red o implementar otros aspectos de la **política de seguridad.**

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES:

- ✓ La Fuerza Terrestre, como institución que forma parte de las Fuerzas Armadas, tiene como misión fundamental establecida en la Constitución del Estado ecuatoriano, la preservación de la Soberanía y el apoyo al Desarrollo.

- ✓ Para dar cumplimiento a su misión de Seguridad, la Fuerza Terrestre se ha modernizado, en el aspecto técnico y científico, adquiriendo material bélico y logístico adecuado para los momentos en que fue requerida su presencia.

- ✓ De la misma forma, se ha preocupado por la capacitación adecuada del personal de Oficiales, Voluntarios y Empleados Civiles, que se han constituido en los elementos fundamentales para alcanzar los objetivos propuestos por la Institución Armada.

- ✓ Los avances más importantes en el campo de desarrollo tecnológico, han alcanzado las Armas de Caballería Blindada, Artillería, Comunicaciones, sin embargo, la crisis económica por la que atraviesa nuestro país, ha limitado el fortalecimiento de la Fuerza en los campos científico y tecnológico en los últimos años.

- ✓ La Fuerza Terrestre, a partir de la década de los años setenta, ha sido una de las instituciones pioneras en el país, en el desarrollo de Sistemas Informáticos.

- ✓ Debido al creciente desarrollo tecnológico del procesamiento de la información, la Fuerza Terrestre, consciente de la importancia del manejo del mismo, ha desarrollado Sistemas de Información con tecnología de

punta, lo que le ha permitido al Mando tomar decisiones adecuadas y oportunas en el cumplimiento de la misión; así tenemos los Sistemas de Logística, Personal, Inteligencia, que luego conformarán el Sistema Integrado de Información de la Fuerza Terrestre.

- ✓ La implementación de un Sistema de Comunicaciones con tecnología de punta, permitirá a las Unidades de la Fuerza Terrestre una comunicación confiable y segura.

- ✓ Sin embargo, en los actuales momentos, los sistemas disponibles en la Fuerza Terrestre, no disponen de seguridad informática, siendo fácilmente susceptibles a interceptación y violación de la confidencialidad de la información que ellos manejan, por lo que atenta a los intereses de la Institución y viola la reglamentación de seguridad que debe existir..

- ✓ La tecnología de hardware y software de computación cambia dinámicamente; por ende, la tecnología de seguridad informática. Este dinamismo hace que aparezcan cada día nuevos elementos para seguridad, lo que hace que el tratamiento de este tema sea especializado, por su amplitud, selección compleja y en muchos casos de un alto costo de implementación; haciéndose necesaria la presencia de técnicos con conocimientos sólidos en esta nueva especialización y en función del cumplimiento de la Misión de la Fuerza Terrestre y por ende de las FFAA.

- ✓ Se requiere implementar la política de seguridad informática en los diferentes Sistemas de la Fuerza Terrestre.

2. RECOMENDACIONES

- ✓ La Fuerza Terrestre, para estar acorde tecnológicamente a los momentos actuales, debe implementar una política de modernización de su equipo y material bélico, de acuerdo a las posibilidades y disponibilidades

económicas del país; así como la capacitación permanente del personal de Oficiales, Voluntarios y Empleados Civiles.

- ✓ Fortalecer los Institutos de Educación y de Investigación Científica y Tecnológica de la Fuerza Terrestre.

- ✓ Actualizar los Sistemas de Información de la Fuerza Terrestre y desarrollar los que sean necesarios, para mantener intactas las posibilidades de utilizar en óptimas condiciones la información que le permita al Mando la toma de las decisiones oportunas y adecuadas.

- ✓ Implementar en los Sistemas de la Fuerza, las políticas de Seguridad que se han analizado en la presente tesis.

- ✓ A través de los Centros de Investigación y Mantenimiento que disponen las Unidades e Instituciones de la Fuerza Terrestre, proporcionar servicios especializados en las mencionadas áreas, a las instituciones y organismos de las FFAA, así como también a las instituciones públicas y privadas que lo requieran, a fin de colaborar con el desarrollo del país y realizar actividades de autogestión.

REFERENCIAS BIBLIOGRAFICAS

- BRUCE C, Carlos: SISTEMAS DE COMUNICACIÓN; Mc. Graw Hill 1980.
- SHANMUGAN S. K: SISTEMAS DE COMUNICACIÓN ANALOGICA Y DIGITAL; John Wiley & Sons, 1979.
- MOHAMED Z. : ADMINISTRACION DE CALIDAD TOTAL; Panorama, 1996.
- DEL POZO D., Hernán: LA EDUCACION COMO PILAR FUNDAMENTAL DEL DESARROLLO Y SEGURIDAD; Tesis de Grado, IAEN, 2000.
- PRESSMAN R. S: INGENIERIA DE SOFTWARE; Mc. Graw Hill, 1992.

LEYES Y REGLAMENTOS

- CONSTITUCION POLITICA DEL ESTADO ECUATORIANO, RO. No 1.11 de agosto de 1998, Quito.
- LEY DE SEGURIDAD NACIONAL Y SU REGLAMENTO GENERAL.
- RAGLAMENTO DE FUNCIONAMIENTO DEL SILOG.

REVISTAS

- PC WORLD: DE VIAJE POR EL INTERNET; 2000.
- PC WORLD: CONECCIONES EN RED.
- MILITARY REVIEW: LA DOCTRINA MILITAR; junio 1998.
- MILITARY REVIEW: TECNOLOGIA DEL EJERCITO DESPUES DEL PROXIMO; octubre 1998.
- MILITARY REVIEW: LA ERA DE LA INFORMACION; enero 2000.