CAPITULO I

SITUACION INFORMATICA ACTUAL

1.1 INFORMACIÓN DE LA FUERZA TERRESTRE

1.1.1 Historia

La Historia del Ecuador guarda en sus páginas la estirpe de sus guerreros aborígenes, en una época en la que la sangre y la bravura andina alimentaron las raíces de lo que hoy reconocemos como nuestra identidad militar ecuatoriana, la misma que se ha fortalecido con las milicias coloniales, las gestas libertarias y las fuerzas militares de la República.

Todo este legado de valor, virtud, lealtad y estirpe guerrera, ha sido plasmada por nuestros grandes historiadores y escritores, en sus letras que contemplan la grandeza de una institución en cuyo regazo se funden los ideales de servicio, de unión, y vocación por la defensa de nuestro territorio.

Gratos recuerdos iluminan la historia militar ecuatoriana; especialmente cuando se habla de los hechos gloriosos en Pichincha, Tarqui, Paquisha, y en el Alto Cenepa.
Este es el Ejército Ecuatoriano: una entidad perpetua y comprometida con su patria, presente a través de estas letras como un testimonio del verdadero significado que

guarda el corazón y la conciencia de todos y cada uno de sus soldados en el fiel cumplimiento de su misión [1].

1.1.2 Misión de la Fuerza Terrestre

La Fuerza Terrestre como uno de los órganos del Comando Conjunto de las Fuerzas Armadas participa en la conservación de la Soberanía Nacional, la defensa de la integridad e independencia del Estado, garantiza su ordenamiento jurídico, contribuye al desarrollo social y económico del país, así como, coopera o interviene, según el caso, en el mantenimiento del orden público, con la finalidad de coadyuvar a la consecución de los objetivos nacionales [2].

1.1.3 Estructura Funcional de la Comandancia General de la Fuerza Terrestre.

Comandancia General de la Fuerza Terrestre

Estado Mayor Planificador.

Jefatura de Comunicación Social.

Inspectoría General del Ejército.

Dirección de Personal.

Dirección de Inteligencia.

Dirección de Operaciones.

Dirección de Logística.

[1] Fuente: http:// www.ejercito.mil.ec
[2] Fuente: http:// www.ejercito.mil.ec

Dirección de Bienestar de Personal.

Dirección de Educación de la Fuerza Terrestre.

Dirección de Comunicaciones y Sistemas DICOMSI.

Dirección de Sanidad.

Dirección de Institutos.

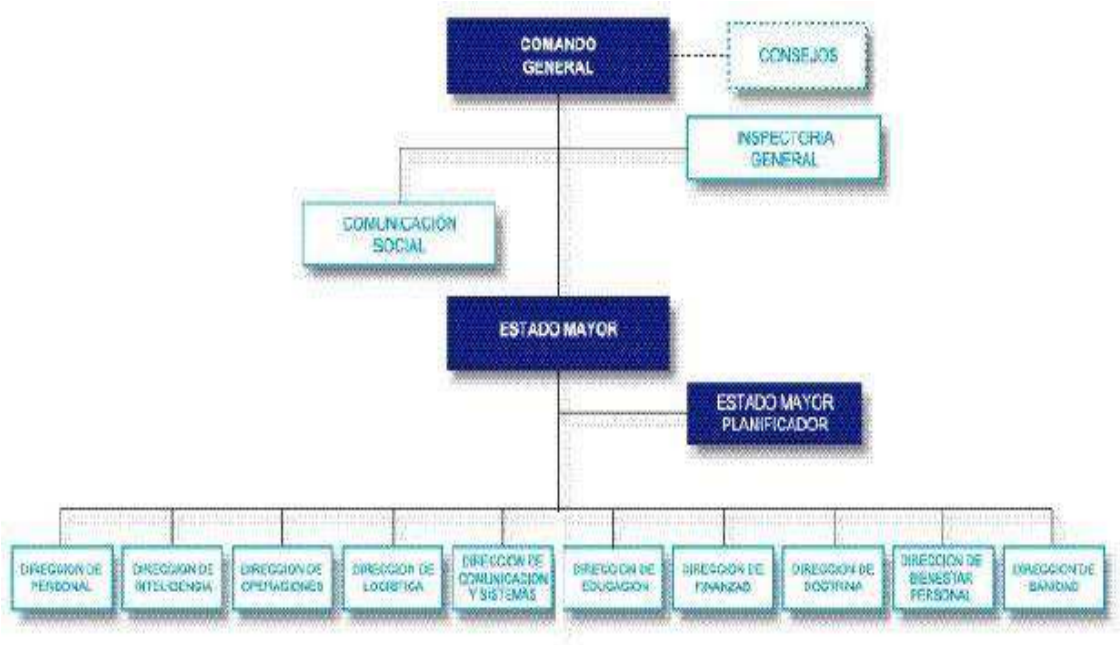

GRAFICO # 1. ORGANIGRAMA DE LA COMANDANCIA GENERAL DE LA FUERZA TERRESTRE

1.1.3.1 Estructura funcional de la Dirección de Comunicaciones y Sistemas DICOMSI

La Dirección de Comunicaciones y Sistemas en su estructura funcional administrativa está determinada de la siguiente manera:

Director.

Dirigir, coordinar y supervisar el desarrollo de todos y cada uno de los proyectos informáticos y de comunicaciones; con la finalidad de proporcionar el enlace entre los diferentes escalones de mando, a fin de permitir el desarrollo y conducción de las operaciones.

Subdirector.

Coordinar el desarrollo de los proyectos destinados a esta dirección; manteniendo el Orden Jerárquico y cumpliendo a cabalidad con los objetivos para los que se crearon el departamento.

Jefe del Centro de Control.

Ejecutar y desarrollar los proyectos planteados por el mando militar, manteniendo un Orden Jerárquico en coordinación con el personal militar encargado para la ejecución de los mismos.

1.2 SITUACION ACTUAL DE LOS SERVIDORES

1.2.1 Detalle de los equipos existentes en el Centro de Control y el cuarto de equipos.

En la actualidad la DICOMSI con la finalidad de proporcionar los servicios informáticos y satisfacer las necesidades de los usuarios de los mismos cuenta con un Centro de Control en el cual se encuentran ubicados los diferentes servidores para sus respectivas funciones; estos se detallan a continuación .

Servidores que se encuentran en funcionamiento en el cuarto de equipos.

CANTIDAD	NUMERACION	DESCRIPCIÓN
1	1	Servidor DNS Primario
1	2	Servidor DNS Secundario
1	3	Servidor WEB-MAIL

Tabla # 1. SERVIDORES DEL CUARTO DE EQUIPOS DEL CENTRO DE CONTROL.

Servidor DNS Primario.

SUN ULTRA 5

564 BITS

128 MHZ RAM

1 DISCO DURO DE 8 GB

PROCESADOR ULTRA SPARK C3 360 MHZ

Servidor DNS Secundario

DELL 2500 CC

768 MHZ RAM

3 DISCOS DUROS DE 36 GB

256 MHZ CACHE

PROCESADOR PENTIUM III 933 MHZ

SERVIDOR WEB - MAIL

DELL 2500 CC

1.2 GB RAM

3 DISCOS DUROS DE 18 GB

256 MHZ CACHE

2 PROCESADORES PENTIUM III 933 MHZ – 133 MHZ

Es importante mencionar que el personal que tiene acceso al Centro de Control contará con varios equipos para su utilización, con la finalidad de poder prestar el contingente de trabajo requerido para sus funciones.

CANTIDAD	NUMERACION	DESCRIPCIÓN
1	1	PC Portátil Varios
1	2	PC para administración
1	3	PC para administración
1	4	PC para Soporte Us. Remotos
1	5	PC para administración
1	6	PC para la guardia
1	7	PC para el Jefe Ctro. Ctrl.

TABLA # 2. CUADRO DE EQUIPOS DEL CENTRO DE CONTROL

1.2.2 Detalle de los sistemas operativos y paquetes que se encuentran instalados en los servidores en la actualidad

Con la finalidad de poder realizar un análisis de la situación actual de los servidores que serán objeto de nuestro estudio, es necesario conocer exactamente el tipo de sistema operativo y los paquetes instalados en los servidores web y de correo electrónico así como las versiones y actualizaciones de los mismos.

1.2.2.1 Servidor web

En la actualidad se encuentra implantado un servidor web con los siguientes paquetes y sistema operativo instalado:

Red Hat Linux 7.2
Apache_1.3.20-16.i386
Apache-conf-0.8.1-1.noarch
Apache-devel-1.3.20-16
Apache-manual-1.3.20-16

Teniendo como resultado un servidor web inseguro, ya que la tendencia actual es tener un servidor Web-SSL que garantice el transporte de datos en la Internet.

1.2.2.2 Servidor de correo electrónico

En la actualidad se encuentra implantado un servidor de correo electrónico con los siguientes paquetes y sistema operativo instalado:

Red Hat Linux 7.2

Sendmail-8.11.6.3

Sendmail-cf-8.11.6.3

Sendmail-devel-8.11.6.3

Sendmail-doc-8.11.6.3

Xinet-2.3.3-1

Imap-2000c-15

Imap-devel-2000c-15

Php-imap-4.0.6-7

Fetchmail-5.9.0-1

WEB-MAIL

Squirrelmail-1.0.2.7-4.noarch

Mysql-3.23.41-1

Php-mysql-4.0.6-7

Php-4.0.6-7

Teniendo en la actualidad un servidor de correo electrónico con fallas de seguridad, ya que es necesario actualizar el sistema operativo y por ende los paquetes necesarios para la instalación de los respectivo servicios que prestará el servidor.

Además no se cuenta con un sistema de firma digital que garantice la autenticidad, integridad y el no repudio de los correos electrónicos. Siendo esta una de las necesidades más imperiosas en la configuración del servidor para un mejor servicio a los usuarios del mismo.

1.3 FUNCIONALIDAD Y FALLAS DE SEGURIDAD DEL SOFTWARE DE LOS SERVIDORES DE CORREO ELECTRÓNICO, SERVIDOR WEB , WEB – MAIL.

1.3.1 Sistema Operativo Red Hat Linux 7.2

1.3.1.1 Concepto

Linux es un sistema operativo gratuito de 32 ó 64 bits parar redes, similar a UNIX, con código abierto, optimizado para Internet (utilizado por los piratas

con mucha frecuencia) que pueden funcionar en distintos tipos de hardware, incluyendo los procesadores Intel (X86) o RISC [3].

Linux se basó sobre UNIX, con una gran característica: este sistema operativo sería Software Libre. Esto significa que una vez que el usuario compra un cd o bien lo descarga gratuitamente desde Internet, es libre de redistribuirlo y modificarlo a su antojo, siempre que, como lo indica la Licencia Pública General GNU, del modo que ha dispuesto la Free Software Fundation, se incluya el código fuente. Esto también incluye el derecho a poder instalar Linux en cualquier número de ordenadores o equipos de cómputo que el usuario desee.

1.3.1.2 Características

- Sistema operativo multitarea y multiusuario.
- Multiprocesador en esta versión del núcleo soporta múltiples procesadores.
- Creado para numerosas plataformas: Intel, Macintosh, Alpha, SPARC.
- Orientado para trabajo de redes con aplicaciones nativas que son portadas para soportar comunicación tanto como cliente y servidor

[3] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

como: FTP, http, TCP/IP, PPP, UUCP, SMTP, SNMP, gopher, wais, news, web, acceso remoto, compartir recursos mediante la red etc.

- Posee un file sistema de archivos propio denominado ext2.

1.3.1.3 Problemas de seguridad

Entre los principales problemas de seguridad no se puede considerar al sistema operativo en si; ya que las fallas de seguridad se dan en las versiones de los paquetes utilizados por el sistema operativo para la versión que se está estudiando es decir Red Hat Linux 7.2. Sin embargo es importante mencionar los problemas que conllevan mantener un sistema de archivos ext2, que se utiliza normalmente con Red Hat Linux 7.2 y que se solucionan al utilizar Red Hat Linux 9.0 con un sistema de archivos ext3.

Sistema de archivos ext2.

- Disponibilidad; tras un corte eléctrico o una caída inesperada del sistema, denominado también cierre no limpio del mismo, se debe

comprobar con el programa fsck cada sistema de archivo ext2 montado en la máquina para ver si es consistente [4]

El proceso de comprobación lleva mucho tiempo y puede prolongar el tiempo de arranque del sistema de una manera significativa, especialmente si existe una gran cantidad de volúmenes que contienen un elevado número de archivos.

Esto conlleva que durante este proceso no se pueda acceder a los datos de los volúmenes.

Con la característica journaling, del sistema de archivos ext3 que se implementa en Red Hat Linux 9.0 ya no es necesario realizar este tipo de comprobación en el sistema de archivos después de un cierre no limpio del sistema. Con el sistema de archivos ext3, únicamente se realiza una comprobación de consistencia en los casos puntuales en los que se produce determinados errores de hardware, como , por ejemplo fallos en el disco duro [5].

[4] Fuente: http://www.europe.redhat.com/documentation/
[5] Fuente: http://www.europe.redhat.com/documentation/

El tiempo empleado para recuperar un sistema de archivos ext3 tras un cierre no limpio del sistema no depende del tamaño del sistema de archivos ni del número de los mismos, sino del tamaño del journal, utilizado para mantener la consistencia en el sistema [6].

Por defecto la recuperación del tamaño del journal tarda alrededor de un segundo, según la velocidad del hardware.

- Integridad de datos; el sistema de archivos ext2 proporciona una integridad de datos considerada como de nivel aceptable. Mientras que el sistema de archivos ext3 que utiliza Red Hat Linux 9.0 proporciona una integridad de datos superior cuando se produce un cierre no limpio del sistema [7].

El sistema de archivos ext3 permite seleccionar el tipo y el nivel de protección de los datos. Por defecto, Red Hat Linux 9.0 configura los volúmenes ext3 para que el nivel de consistencia sea elevado en relación con el estado del sistema de archivos.

[6] Fuente. http://www.europe.redhat.com/documentation/
[7] Fuente: http://www.europe.redhat.com/documentation/

- Velocidad; el sistema de archivos ext3, a parte de permitir escribir datos de una vez, en la mayoría de los casos tiene un rendimiento superior al que proporciona ext2, porque los journlas de ext3 optimizan el movimiento de los cabezales de los discos duros [8].

  Se pueden seleccionar tres modos de journaling para optimizar la velocidad, sin ver comprometida la integridad de los datos.

Soporte de controladores.

Una de los principales problemas en la actualidad para mantener un sistema operativo como Red Hat linux 7.2, es su poco soporte de controladores para hardware. Pero esto ya no es un problema al utilizar Red Hat Linux 9.0, se puede configurar cualquier hardware para su utilización en los servidores; esto se ha conseguido gracias al aporte de la comunidad Linux en el desarrollo de controladores. Es importante mencionar que la mayoría de los controladores ya vienen predispuestos en la compilación del sistema operativo, por lo que será necesario configurar únicamente en casos excepcionales un controlador adicional. En la actualidad casi en su totalidad los fabricantes de hardware proporcionan los controladores necesarios para Linux.

[8] Fuente: http://www.europe.redhat.com/documentation

1.3.2 Servidor de páginas Web (Apache).

1.3.2.1 Concepto.

Sin lugar a duda el servidor web número uno es Apache. Se diseño originalmente para trabajar en maquinas Unix y sus múltiples variantes; sin embargo, hoy en día está disponible para su utilización práctica en la totalidad de sistemas operativos.

El servidor web Apache es uno de los mayores triunfos del software libre.

1.3.2.2 Características.

El servidor web utilizado en la actualidad por el servidor de páginas Web, es Apache-1.3.20 el mismo presenta las siguientes características.

- Multiplataforma.
- Servidor web conforme al protocolo http/1.1

- Modular; puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona, y con al API de programación de módulos, para el desarrollo de módulos específicos.
- Se desarrolla de forma abierta.
- Extensible; gracias a ser modular se han desarrollado diversas extensiones entre las que destacan PHP.

Problemas de Seguridad

- Todas las versiones del servidor Web Apache 1.X se ven afectadas por una vulnerabilidad en las funciones encargadas de procesar las peticiones erróneas codificadas de forma troceada. Se trata de una vulnerabilidad explotable de forma remota. Cuando un atacante remoto envíe una serie de peticiones codificadas de una forma especial, la vulnerabilidad puede provocar la finalización del proceso hijo que está procesando la petición. Por tanto el atacante puede provocar una condición de denegación de servicio [9].

- Adicionalmente, en las versiones 1.x de Apache, se produce un desbordamiento de memoria intermedia. En las plataformas Linux de

[9] Fuente://bugs.apache.org/index

32- bit, este desbordamiento originará una violación de segmentación y el proceso finalizará [10].

- En las plataformas de 64-bit, este desbordamiento puede llegar a ser controlado por el atacante para forzar la ejecución de código [11].

Las versiones 2.x de Apache detectan de forma correcta la situación de error, por lo que no es posible que el atacante ejecute código en el servidor.

Protección de datos en transito.

Por defecto las comunicaciones basadas en la web tienen varias debilidades. Por lo que al mantener un servidor web únicamente con Apache sin ningún modulo de seguridad adicional, se mantendrán los consiguientes problemas en el transporte de los datos por la red.

- HTTP no ofrece mecanismo de encriptación, llevando a que terceras personas puedan husmear en el tráfico entre los usuarios finales y el servidor.

[10] Fuente://bugs.apache.org/index
[11] Fuente://bugs.apache.org/index

De este modo la sesión entre el usuario y el servidor tiene poca o ninguna privacidad [12].

- http es un protocolo sin estado; no almacena información sobre los usuarios[13].

- http no proporciona ningún medio de autentificar una sesión en curso. Por lo tanto no puede determinar si una tercera persona no fiable ha secuestrado la sesión actual [14] .

Se considera que al mantener los servidores sin los módulos de criptografía adecuadas para garantizar un transporte de datos seguro; será el principal problema de seguridad a solucionar. Y este problema solo se logrará solucionar al implementar un servidor HTTPS es decir se deberá incorporar al Apache los módulos de seguridad SSL.

[12] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[13] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[14] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

1.3.3 Servidor de correo electrónico.

1.3.3.1 Concepto

Sendmail (SMTP) , el protocolo de transporte de e-mail más utilizado es el protocolo de transferencia de correo (SMTP), a diario se lo utiliza para transmitir millones de mensajes de correo electrónico a todo el mundo [15].

Sendmail (SMTP)

- Acepta un mensaje entrante .
- Comprueba las direcciones del mensaje.
- Si son direcciones locales, almacena el mensaje para recuperarlo.
- Si son direcciones remotas envía el mensaje.

Se los puede considerar funcionalmente similares a los routers de paquetes, excepto en que se aplican exclusivamente al e-mail.

[15] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

1.3.3.2 Problemas de seguridad.

- Complejidad en la configuración en las versiones anteriores a la distribución 8.12, por lo que la principal falla de seguridad se origina en una configuración inadecuada de sendmail [16].

Es vulnerable a ataques de negación de servicios, se descubrieron fallas importantes de seguridad en versiones anteriores a sendmail-8.12 que causarían la negación de servicios, entre las más importantes se mencionarán las siguientes:

- Fallo de desbordamiento del buffer de MIME, recibir una cabecera errónea de mime esta causaría que se pueda ejecutar algún tipo de código oculto en el mensaje y pueda causar destrozos en el servidor [17].
- Desbordamiento del buffer HELO, el intruso puede disfrazar su origen pasando una cadena anormalmente grande junto con el comando HELO haciendo imposible detectar la IP de origen lo que causaría problemas

[16] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

[17] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

en el servidor causando problemas a los usuarios al tener negación de servicios [18].

1.3.4 Web-mail

1.3.4.1 Concepto

Squirrelmail es un interesante, extensible, funcional y robusto software para correo que permite acceder al usuario a su correo electrónico desde el navegador de su predilección.

1.3.4.2 Problemas de seguridad

Se podría considerar como la principal falla de seguridad en esta versión es la carencia de un software que me permita interactuar con gnupg, para poder proporcionar al usuario la posibilidad de acceder a los beneficios de la criptografía y la firma digital.

[18] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002