CAPITULO IV

PROPUESTA DE SEGURIDADES.

4.1. INSTALACION DE RED HAD LINUX 9.0

A continuación se explica cómo realizar una instalación personalizada de Red Hat Linux desde el CD-ROM, utilizando el programa de instalación gráfica.

Ver la explicación paso a paso de la instalación en el cd anexo2.

4.2. CONFIGURACION DEL SERVIDOR SEGURO APACHE

Al configurar un servidor de correo electrónico y web, y tener acceso al correo electrónico vía web-mail es necesario mantener un servidor web seguro es decir HTTPS que garantice la transmisión de los datos en la red.

Para nuestra propuesta de implantación es necesario acceder a un Certificado Digital de una Autoridad Certificadora , pero en el caso del Ecuador al no existir una empresa que

preste este tipo de servicios y al no contar con una Ley que garantice la Certificación Digital, y tomando en consideración que la Comandancia General de la Fuerza Terrestre es una institución en la que su organización puede comprobar fácilmente la identidad de los usuarios y los servidores, pues cuenta con una estructura jerárquica, administrativa y de dirección sólida; bastará con la utilización de un Certificado Digital Auto firmado que garantizará todas las necesidades de seguridad requeridas por la institución en mención.

Pero por la naturaleza del presente proyecto ponemos en consideración como propuesta inicial la utilización del mencionado Certificado Auto firmado, así como la utilización de un certificado de una empresa certificadora, para el caso Verising de los EE.UU, entendiéndose que se indicará desde como realizar la petición del certificado hasta la demostración con un demo proporcionado por dicha empresa certificadora.

Para poder instalar y configurar un servidor HTTPS adecuadamente es necesario considerar lo siguiente.

4.2.1. Paquetes necesarios para un servidor web seguro.

Los paquetes necesarios para instalar y configurar un servidor web seguro son:

httpd-2.0.40-21.i386

mod-ssl-2.0.20-21.i386

openssl-0.9.7a-2.i386

httpd-manual-2.0.40-21.i386

Es necesario recalcar que para una adecuada seguridad se instalen los paquetes con estas versiones, ya que en distribuciones anteriores podrían existir problemas de seguridad.

4.2.2. Instalación de paquetes.

rpm –q httpd-2.0.40-21.i386

rpm –q mod-ssl-2.0.20-21.i386

rpm –q openssl-0.9.7a-2.i386

rpm –q httpd-manual-2.0.40-21.i386

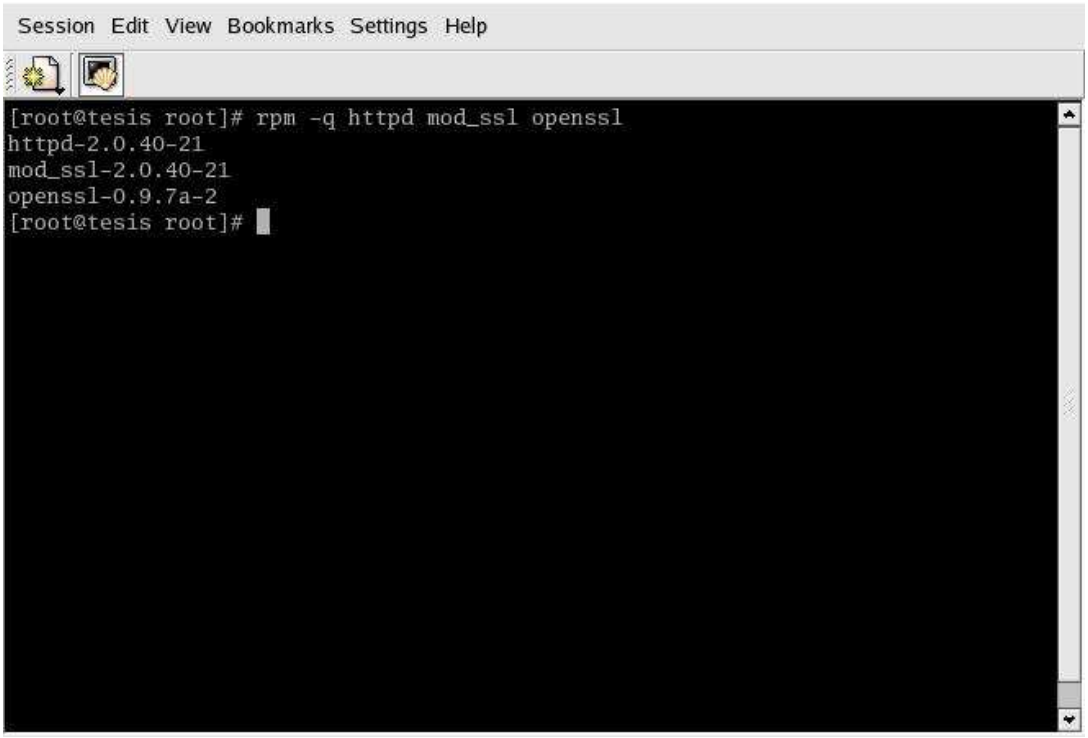

GRAFICO # 22. INSTALACIÓN DE LOS PAQUETE PARA LA CONFIGURACIÓN DEL SERVIDOR WEB

Como se puede ver en la salida de consola de Linux al verificar la existencia de los paquetes en el sistema; estos ya se encuentran instalados por lo que no será necesario realizar una nueva instalación de los paquetes mencionados. Es importante indicar que la instalación de estos paquetes se la realizó en la instalación del sistema operativo.

4.2.3. Configuración del servidor con un certificado auto firmado.

4.2.3.1.Generación de una clave.

Lo primero para generar un certificado auto firmado será generar una clave para lo cual deberemos abrir una consola de Linux como root.

Lo primero será ubicarnos en el directorio /etc/httpd/conf y eliminar los certificados simulados que por defecto se crean al momento de la instalación del sistema operativo.

```
# cd  /etc/httpd/conf
# rm ssl.key/server.key
# rm ssl.crt/server.crt
```

En la siguiente figura se podrá observar los certificados que fueron creados por el sistema y que deberán ser borrados.

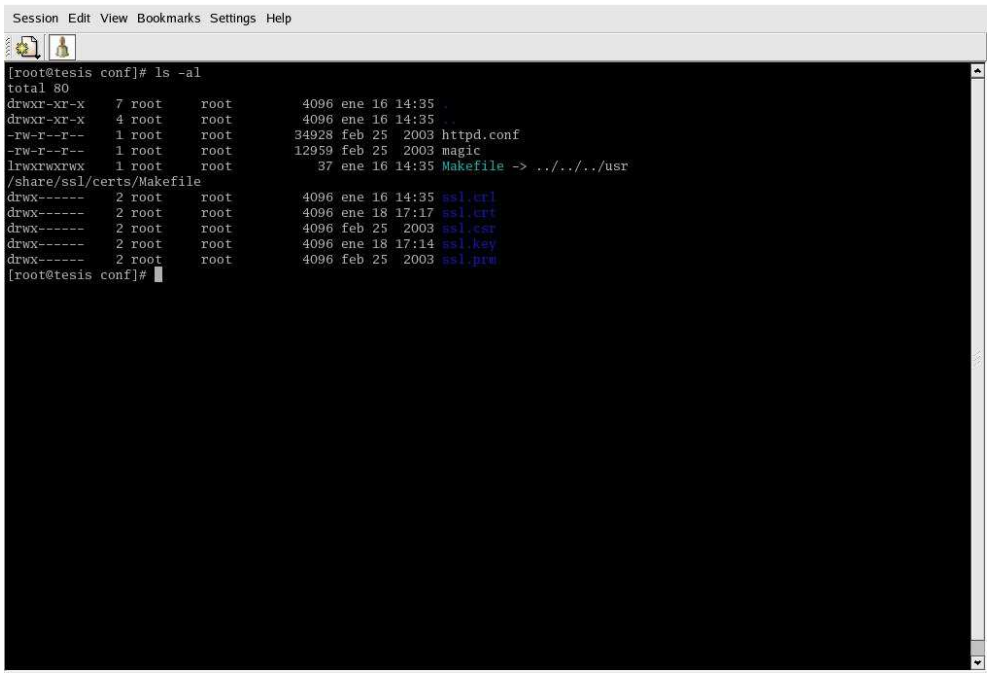

GRAFICO # 23 . CERTIFICADOS CREADOS POR EL SISTEMA

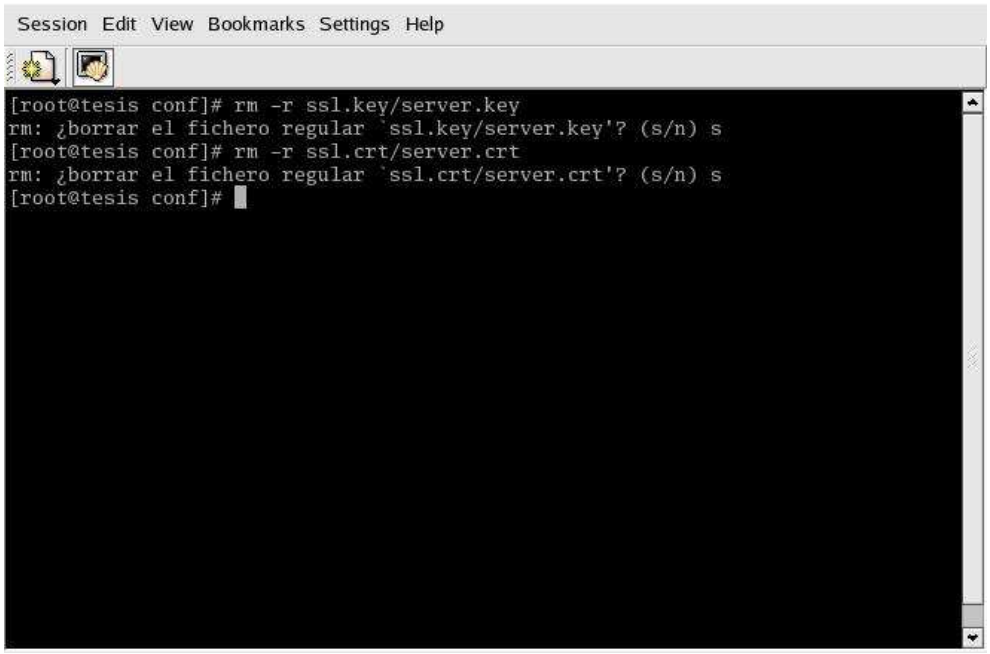

GRAFICO # 24. ELIMINACION DE LOS CERTIFICADOS PREEXISTENTES EN EL SISTEMA.

Una vez que se haya eliminado los certificados existentes por defecto en el sistema, se deberá generar la clave aleatoria con el comando genkey y dentro del directorio /usr/share/ssl/certs; es importante que se tome en consideración las normas indicadas para la creación de una contraseña que se mencionaron en el Capitulo II del presente documento, para la generación de esta contraseña.

cd /usr/share/ssl/certs

make genkey

Al realizar estas instrucciones en la consola de Linux el sistema le pedirá que introduzca su contraseña como se mostrará en la siguiente figura:

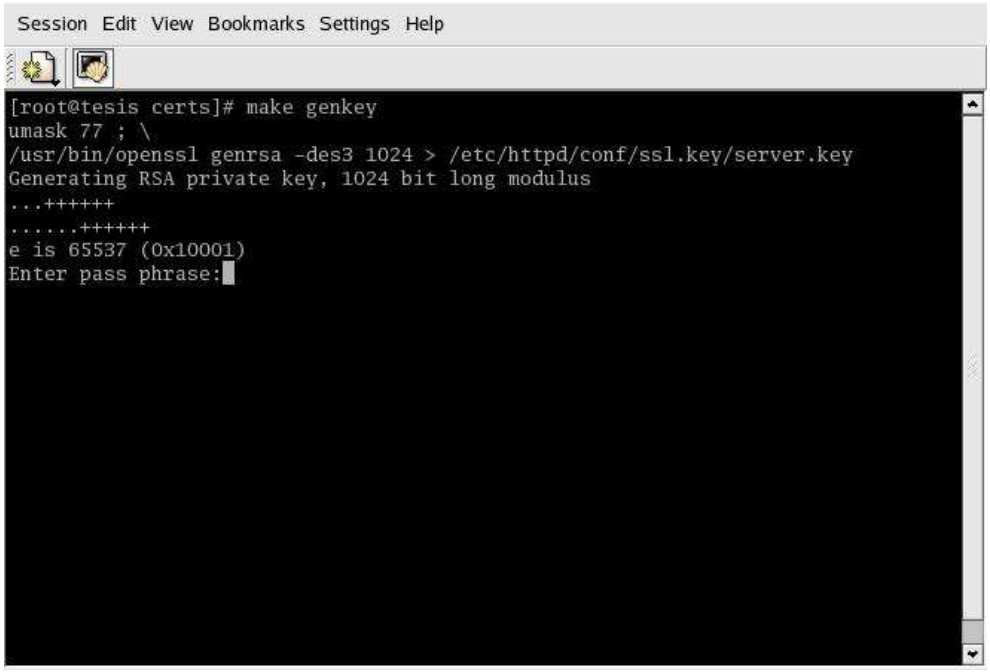

GRAFICO # 25. GENERACIÓN DEL ARCHIVO SERVER.KEY SALIDA INICIAL DEL SISTEMA.

Después de introducir la respectiva contraseña como lo requiere el sistema, el mismo generará la clave aleatoria y nos mostrará la siguiente salida.

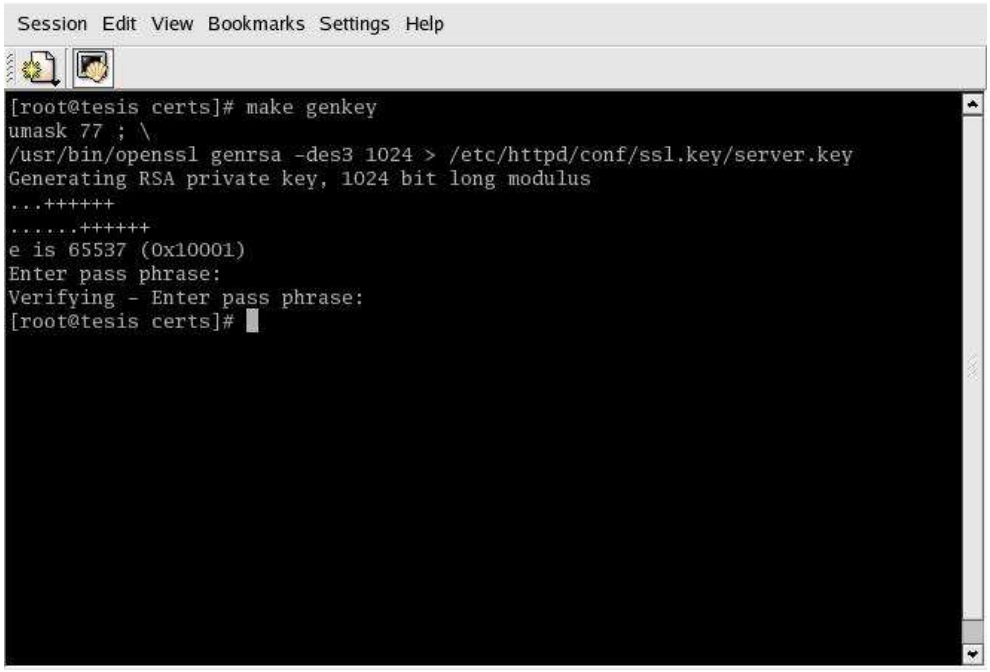

GRAFICO # 26. GENERACIÓN DEL ARCHIVO SERVER.KEY SALIDA FINAL DEL SISTEMA.

El sistema una vez terminado esta tarea ha construido un archivo llamado server.key, en el cual se encuentra almacenado la contraseña, este archivo se guardará en el directorio /etc/httpd/conf/ssl.key/

Es importante que se recuerde cual fue la contraseña introducida, pues esta será requerida por el sistema para reiniciar el servidor.

4.2.3.2. Creación del certificado auto firmado.

Una vez creado la clave aleatoria, se creará el mencionado certificado; para esto es necesario que nos ubiquemos dentro del directorio /usr/share/ssl/certs/ y se proceda a generar el certificado con la siguiente comando make testcert.

```
# cd  /usr/share/ssl/certs/
# make testcert
```

Y el sistema nos mostrará las siguientes salidas de pantalla que las debemos ir llenando de acuerdo a las exigencias del mismo.

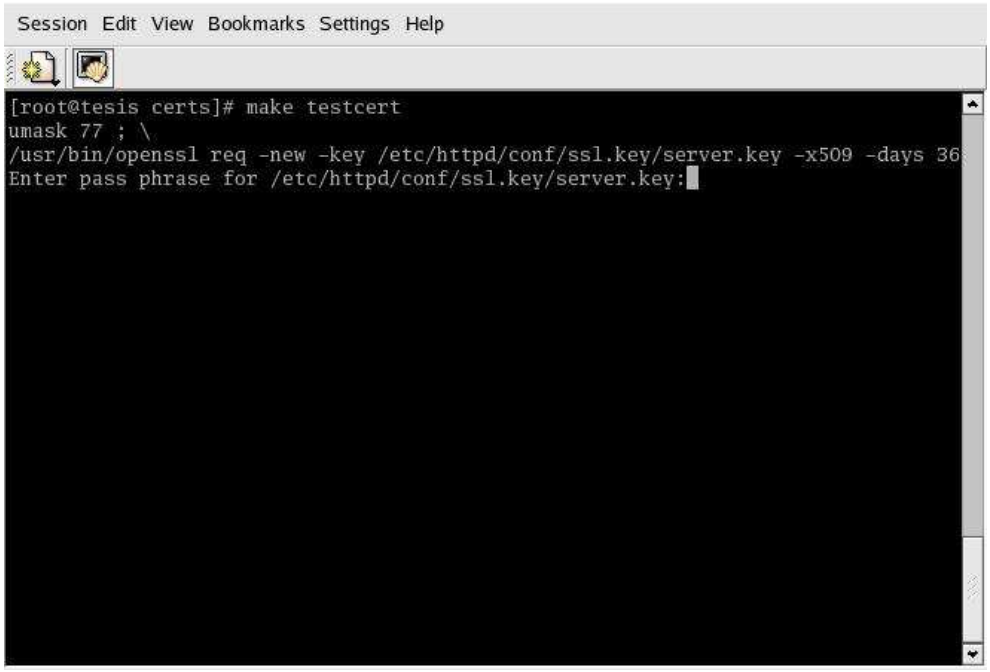

GRAFICO # 27. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 1.

En la anterior figura el sistema nos pide que ingresemos la contraseña que introducimos al momento de generar la clave aleatoria para poder continuar y generar el certificado.

Una vez introducida la contraseña requerida, se presentarán una serie de pantallas que las llenaremos con la información que el sistema lo requiera, teniendo en consideración la información de la institución para al cual se esta generando el certificado, en el caso la Comandancia General de la Fuerza Terrestre.

Otro punto a tomar en consideración es el nombre del servidor , el formato requerido es nombre_maquina.dominio, para nuestro caso tesis.ejercito.mil.ec.

Un punto adicional será la dirección de correo para emitir cualquier mensaje al administrador del sistema, es importante que sea la dirección que se utilizó para la creación de las zonas en la configuración del DNS (no imprescindible) o en su defecto sea la del administrador del servidor de correo electrónico, es decir del alias para root, en el caso de existir diferentes administradores. Bastará con leer la solicitud del sistema para llenar los campos restantes.

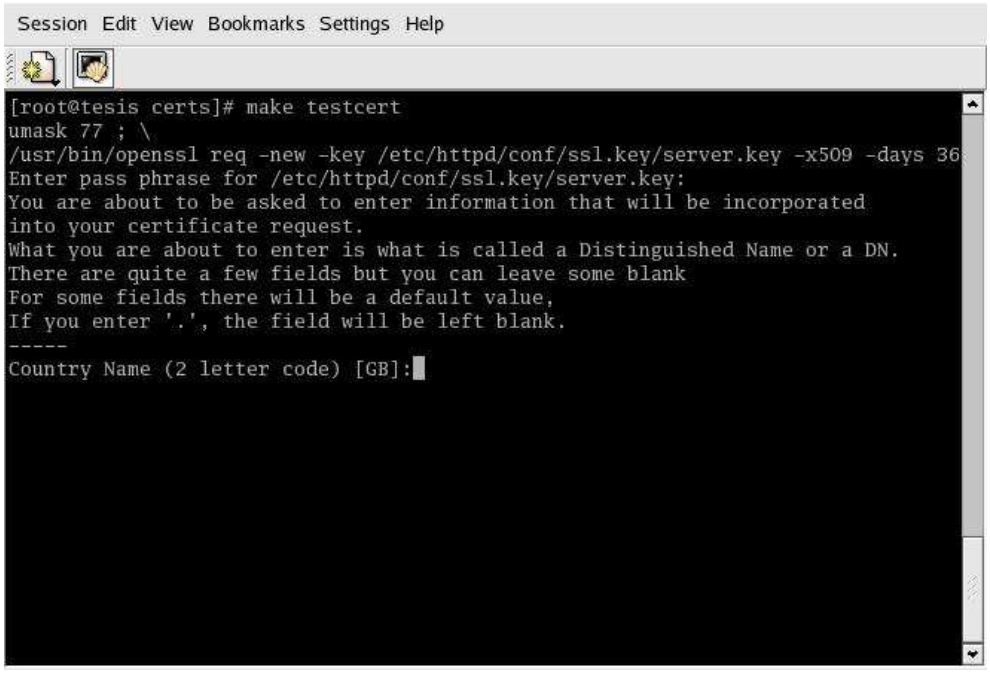

GRAFICO # 28. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 2.

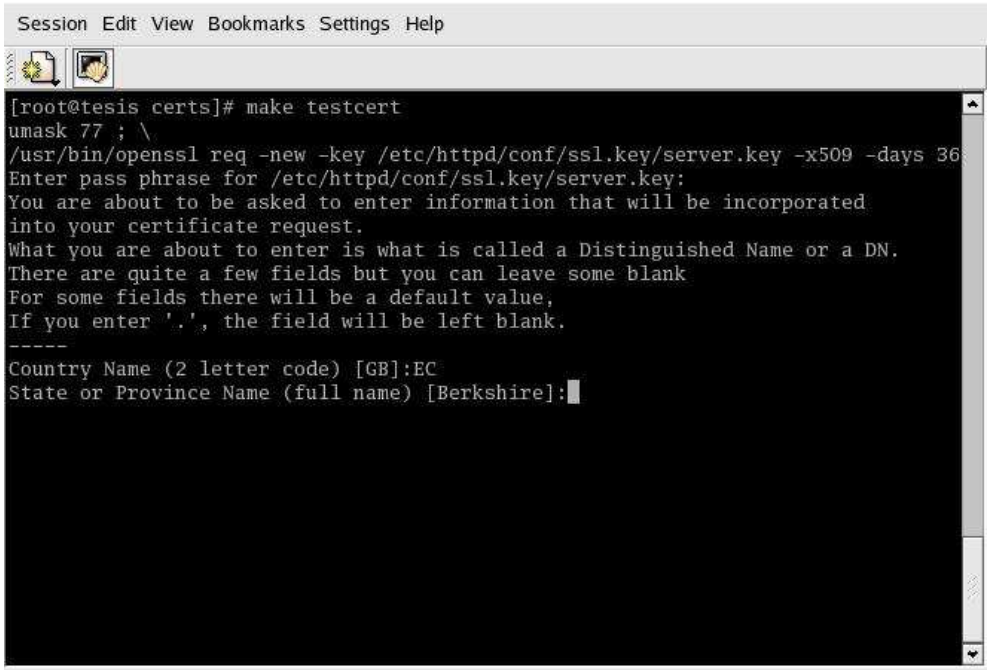

GRAFICO # 29. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 3.

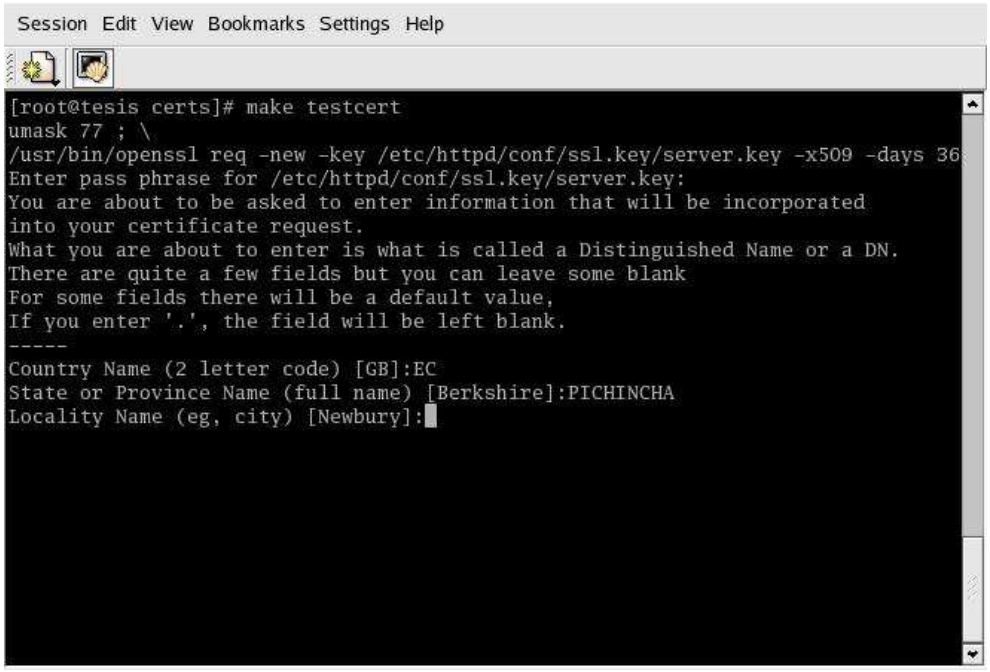

GRAFICO # 30. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 4.

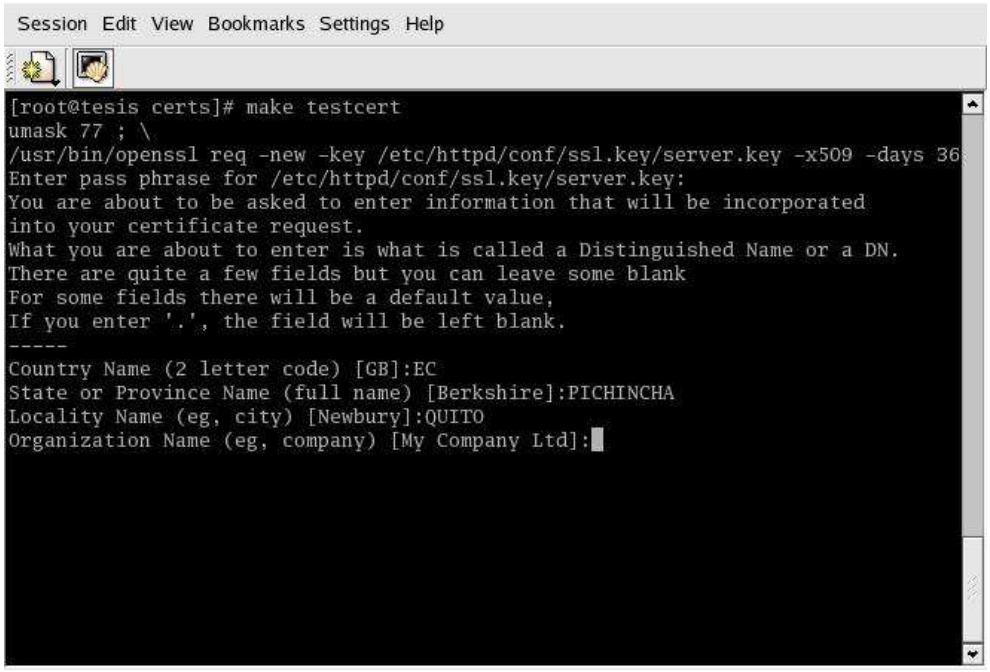

GRAFICO # 31. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 5.

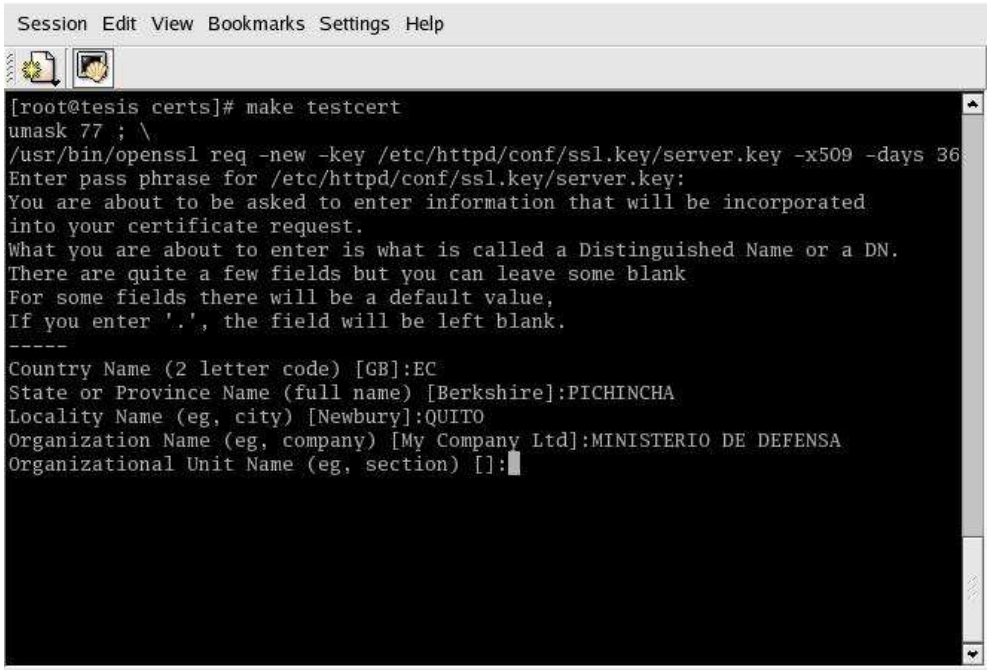

GRAFICO # 32. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 6.

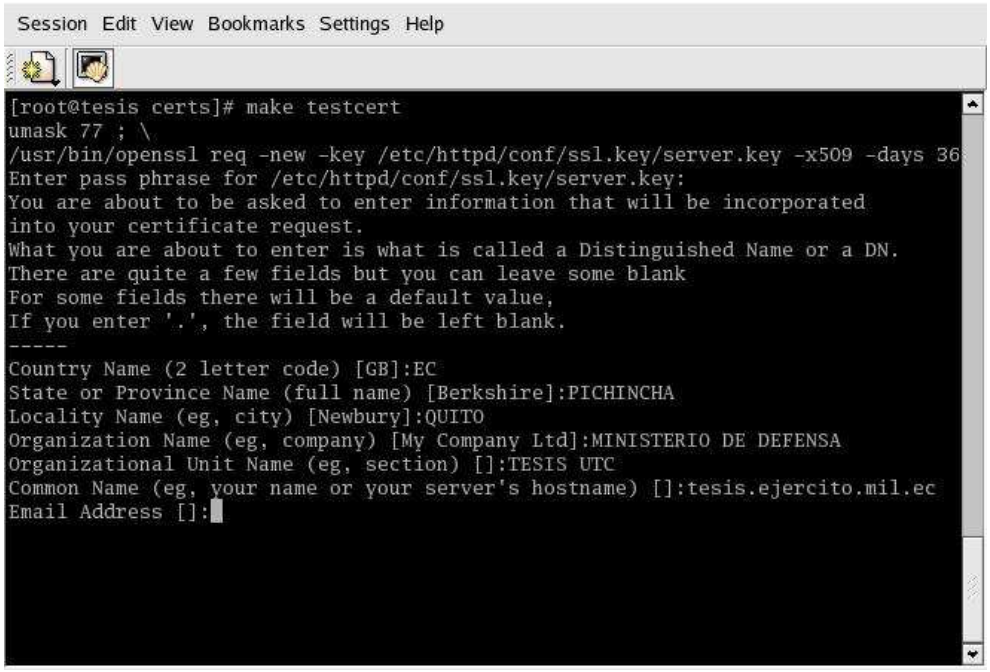

GRAFICO # 33. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 7.

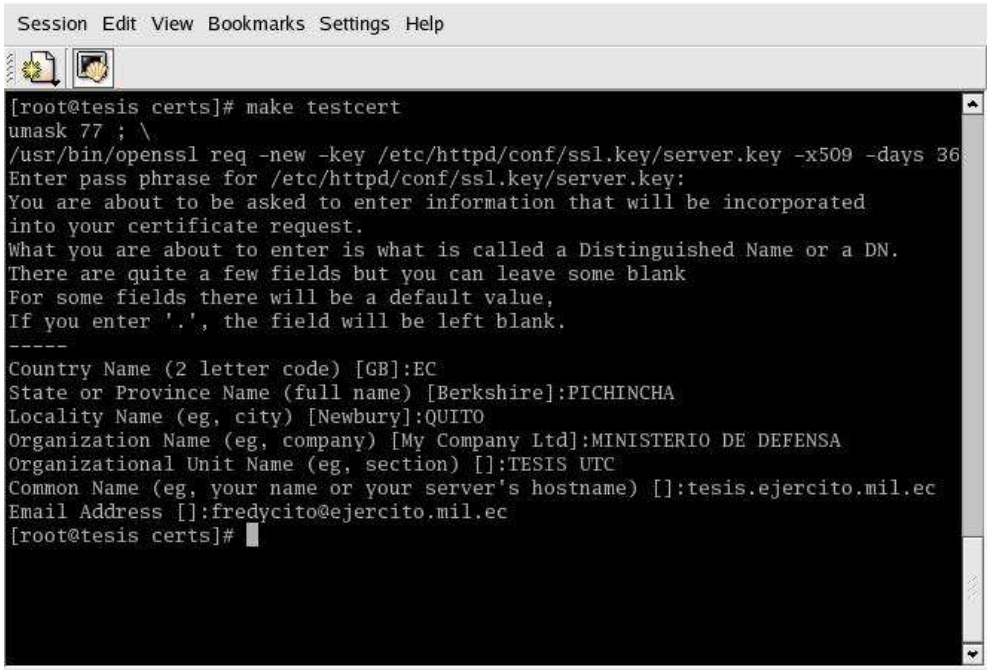

GRAFICO # 34. CREACIÓN DE UN CERTIFICADO AUTOFIRMADO. PASO 8.

Después de que se proporcionó la información correcta para la generación del certificado; este se ha generado y se ubicará en el directorio en el que fue creado es decir /usr/share/ssl/certs.

4.2.3.3. Comprobación del certificado auto firmado creado para la institución.

Una vez creado el certificado bastará con dirigir un navegador de Internet, indicando la dirección del servidor es decir ejercito.mil.ec.

Antes de realizar esta acción es importante reiniciar el servidor.

service httpd restart

Al reiniciar el servidor este pedirá que se introduzca la contraseña para verificar la autenticidad del administrador como medida de seguridad. La contraseña requerida es la que se creó en el momento de generar la clave aleatoria.

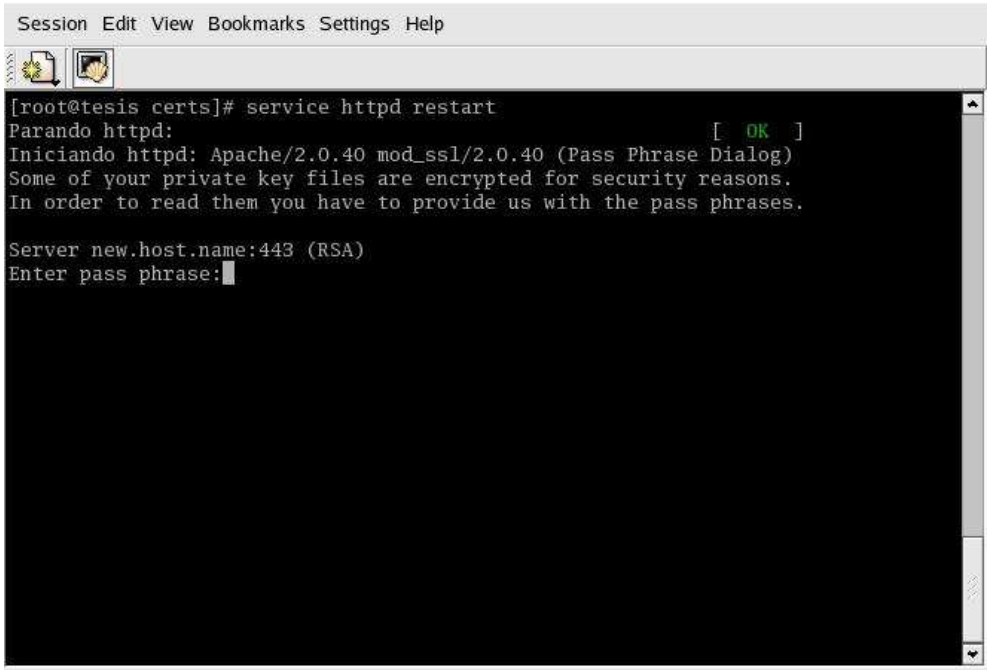

GRAFICO # 35. ARRANQUE DEL SERVIDOR SEGURO WEB SSL. INGRESO DE LA CLAVE PARA EL SERVER .KEY

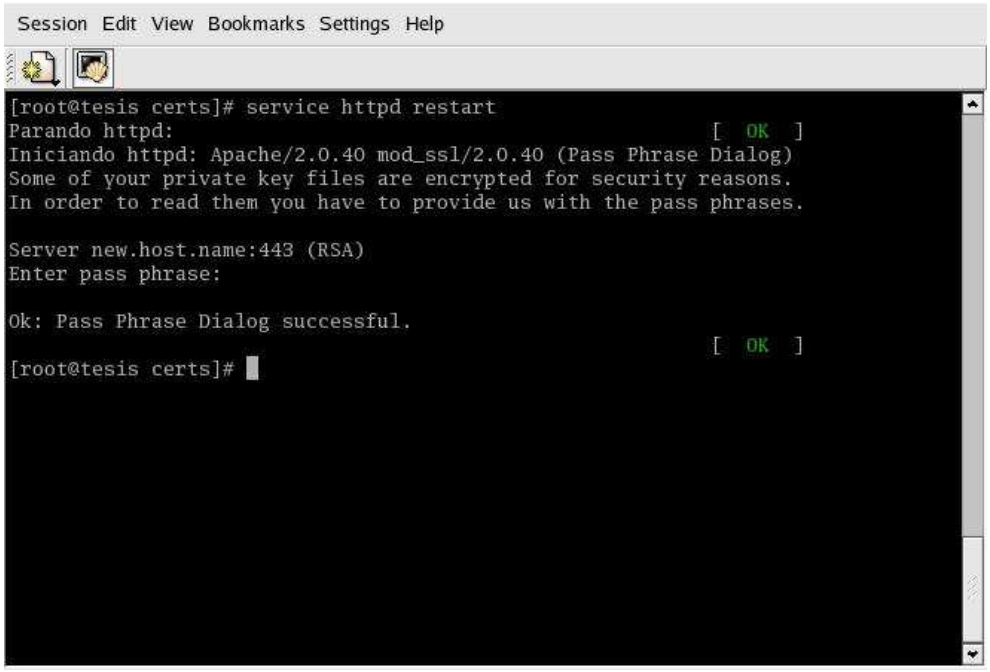

GRAFICO # 36. SALIDA DEL SISTEMA SEÑALANDO EL ESTADO DEL SERVIDOR WEB SSL

Verificada la autenticidad del administrador se procederá a levantar un navegador de Internet como se mencionó anteriormente y como lo muestran las siguientes figuras.

Al ser este un certificado auto firmado el navegador no aceptará el mismo automáticamente por los que bastará con seguir las peticiones que se muestren y se podrá acceder al sitio.

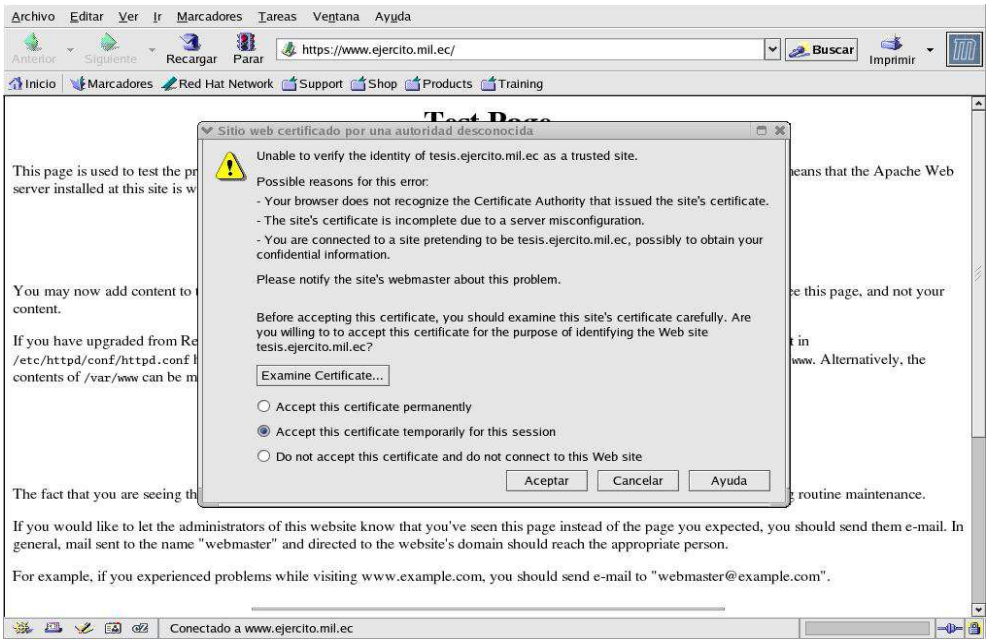

GRAFICO # 37. COMPROBACIÓN DEL CERTIFICADO Y EL SERVIDOR WEB SSL

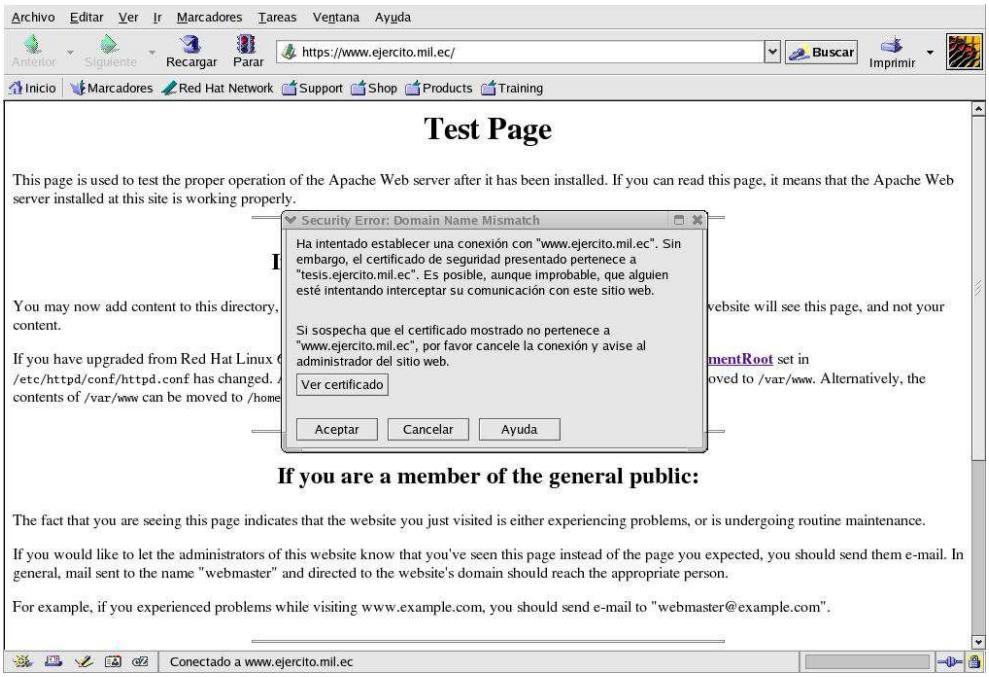

GRAFICO # 38. COMPROBACIÓN DEL CERTIFICADO. Y EL SERVIDOR WEB SSL

Como se puede ver en la barra de direcciones de la pantalla del navegador se tiene un sitio https://www.ejercito.mil.ec .

4.2.4. Configuración del servidor con un certificado de una Autoridad Certificadora (Verising)

Como se mencionó anteriormente, se pondrá a consideración la configuración con un certificado proporcionado por una Autoridad Certificadora . Para el caso se

utilizará un demo de Verising por ser reconocida como una entidad certificadora seria a nivel mundial, residente en los EE.UU.

Para realizar esta configuración se necesitan de igual manera que los paquetes de seguridad y para el servidor estén instalados así como se deberá borrar los certificados y claves existentes que fueron creados por defecto por el sistema en el momento de la instalación del mismo.

Además se deberá crear una clave aleatoria de la misma forma como se creo para la generación del certificado auto firmado. Todo esto bajo las mismas consideraciones que ya se realizaron anteriormente. Posterior a esto se procederá con los siguientes pasos.

4.2.4.1.Generar una petición de certificado para enviarla a la Autoridad Certificadora.

Para la utilización de un demo adecuado se debe generar una petición a la Autoridad Certificadora mencionada, pues esta deberá verificar la información para poder proporcionar el demo que utilizaremos para esta configuración.

El modelo de petición que se mostrará a continuación es el mismo que se utilizará para comprar el certificado a Verising, para la utilización definitiva del certificado.

Para generar el pedido debemos ubicarnos en el directorio /usr/share/ssl/certs y ejecutar el comando make certreq. Los comando deben ser ejecutados desde una consola de Linux y como root.

```
# cd  /usr/share/ssl/certs
# make certreq
```

El sistema generará una salida en la que se nos pedirá que ingresemos la clave aleatoria antes generada así:

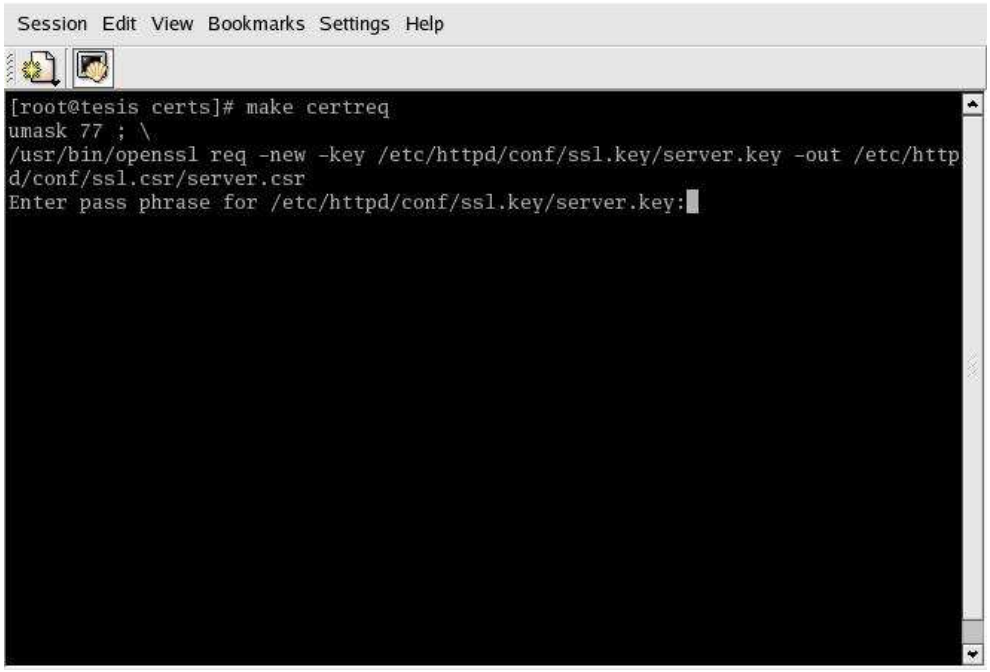

GRAFICO # 39. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. GENERACION SERVER.KEY

Una vez que el sistema compruebe la clave ingresada, generará una serie de pantallas en las que se nos pedirá que ingresemos los datos correspondientes a la institución para la cual es el certificado a otorgar.

Es importante mencionar que los datos deben ser ingresados con las consideraciones que se mencionaron al generar el certificado auto firmado.

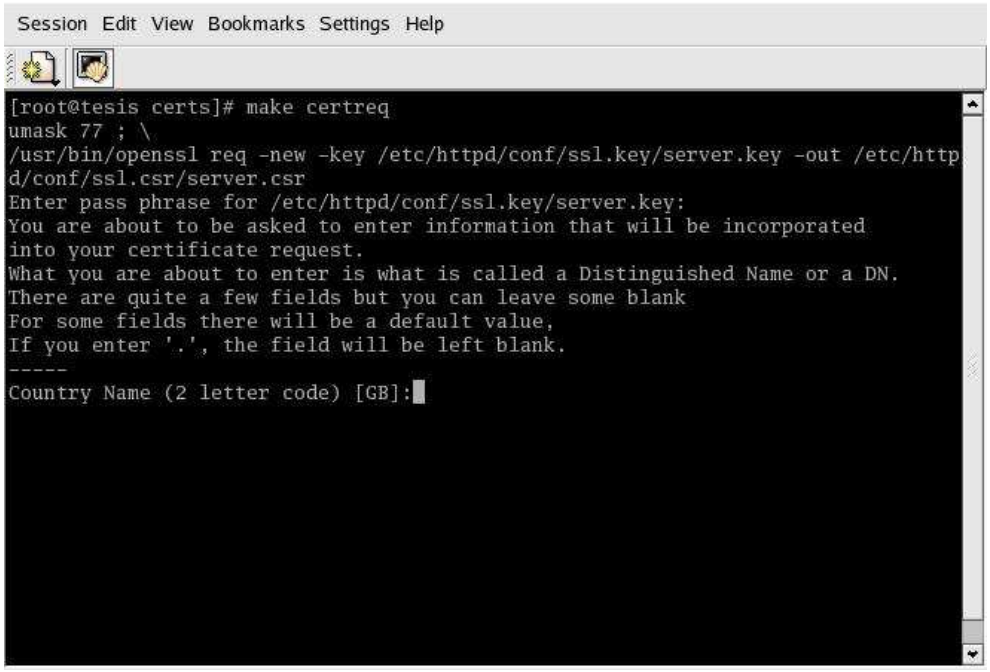

GRAFICO # 40. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 1.

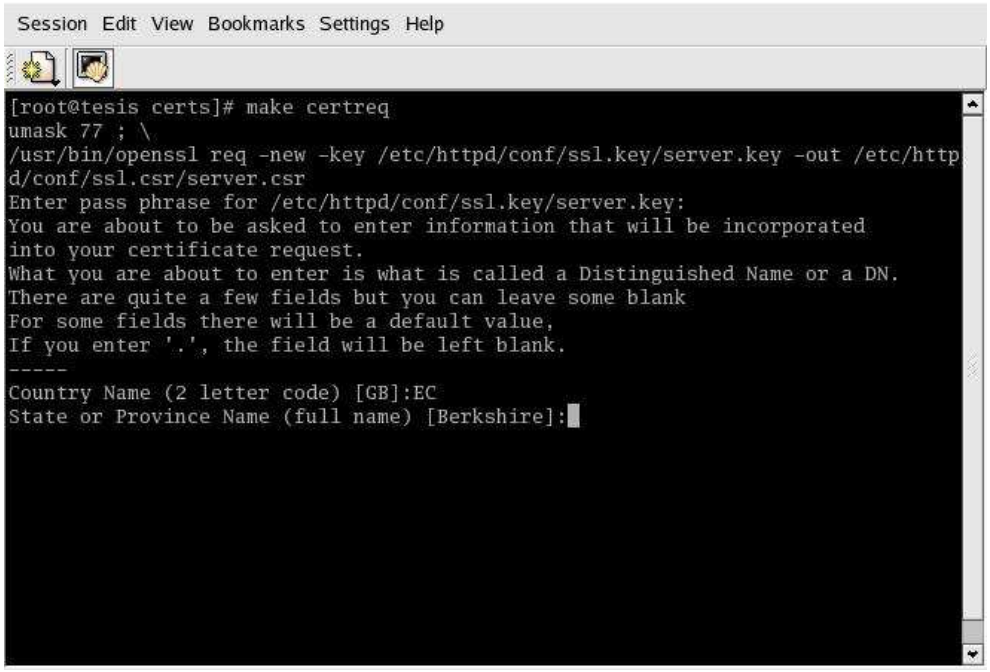

GRAFICO # 41. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 2.

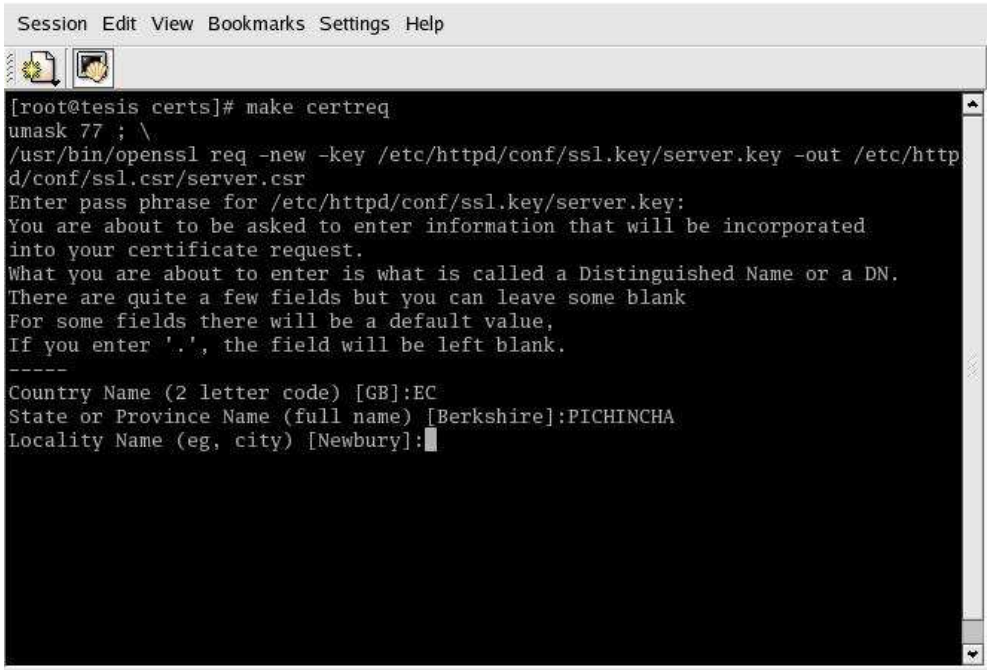

GRAFICO # 42. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 3.

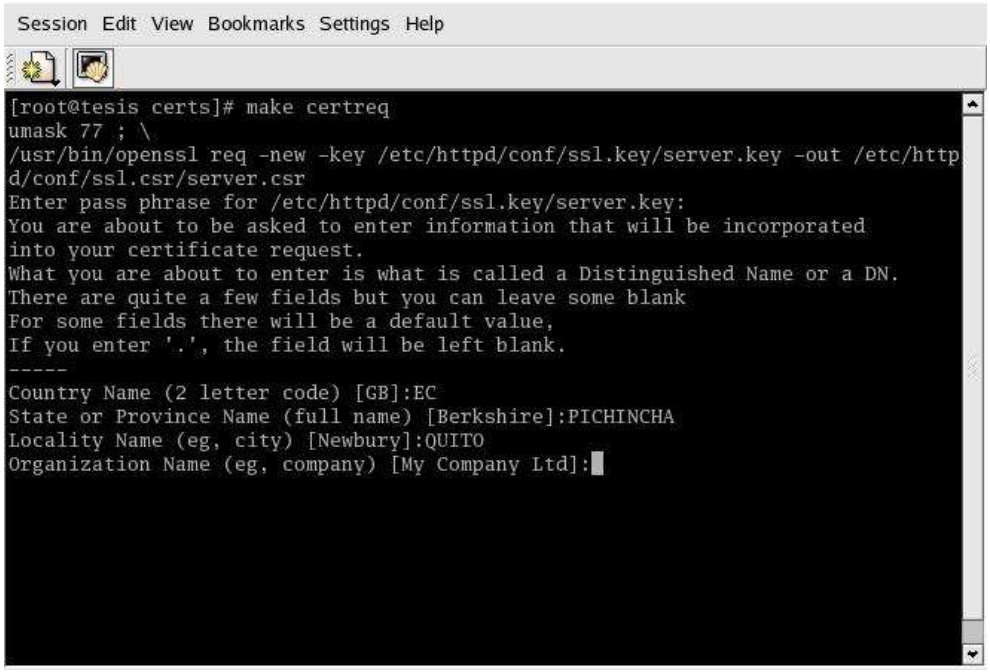

GRAFICO # 43. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 4.

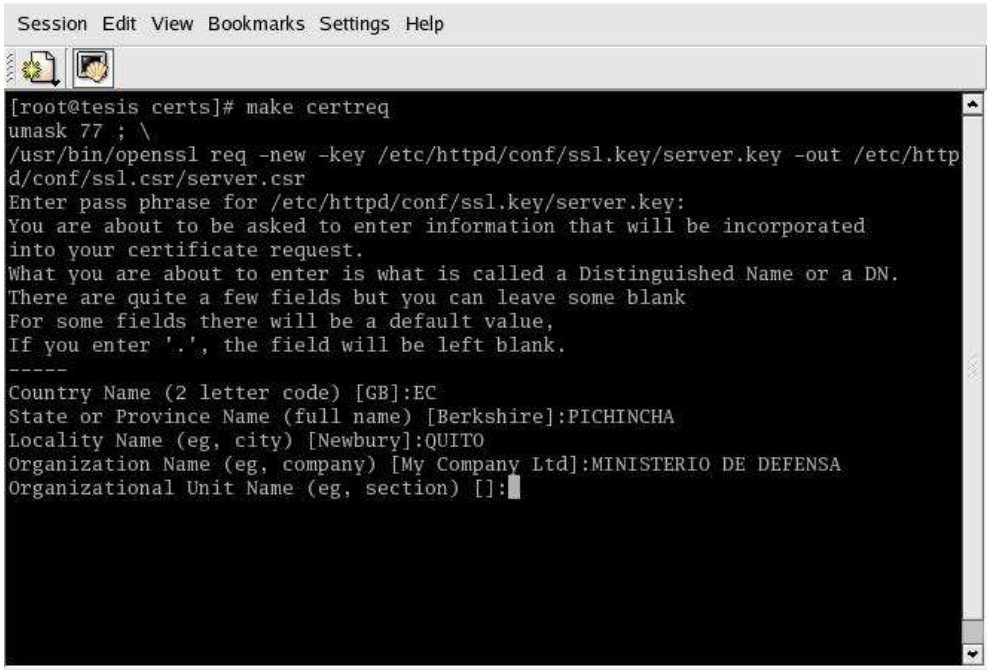

GRAFICO # 44. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 5.

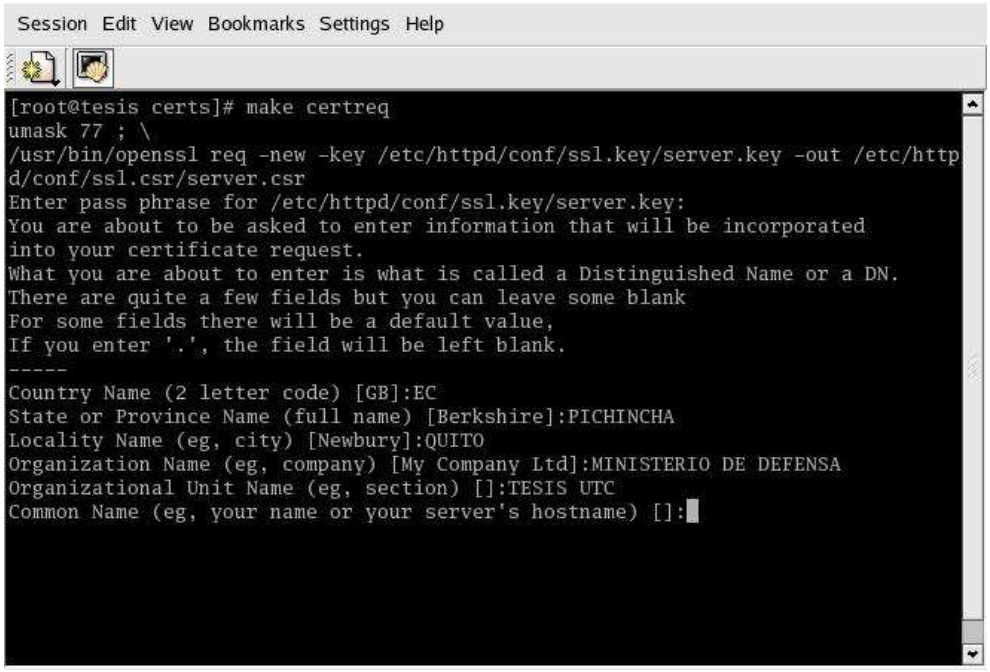

GRAFICO # 45. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 6.

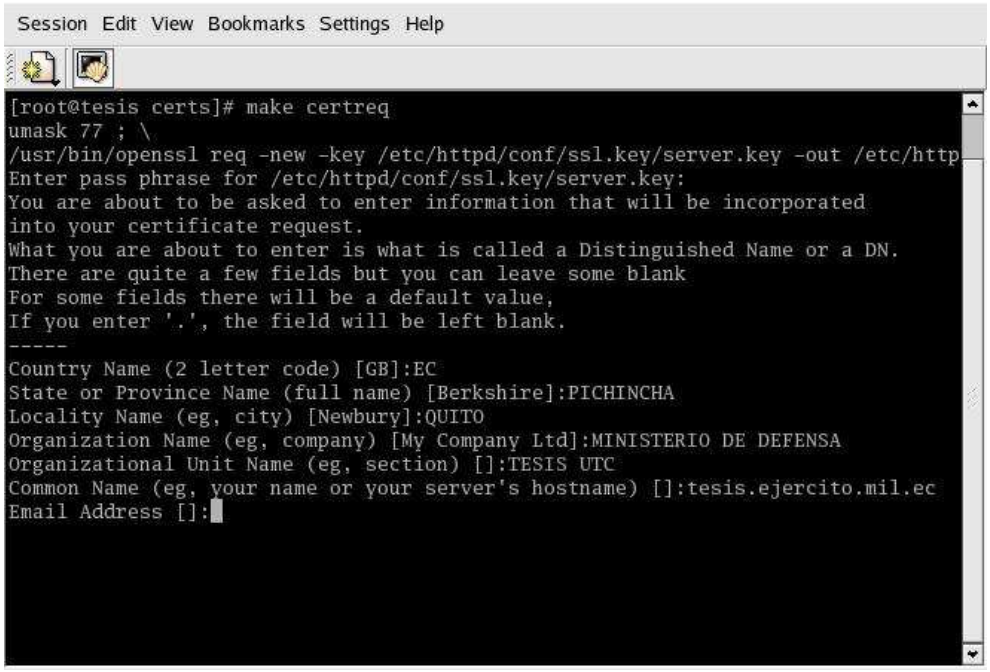

GRAFICO # 46. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 7.

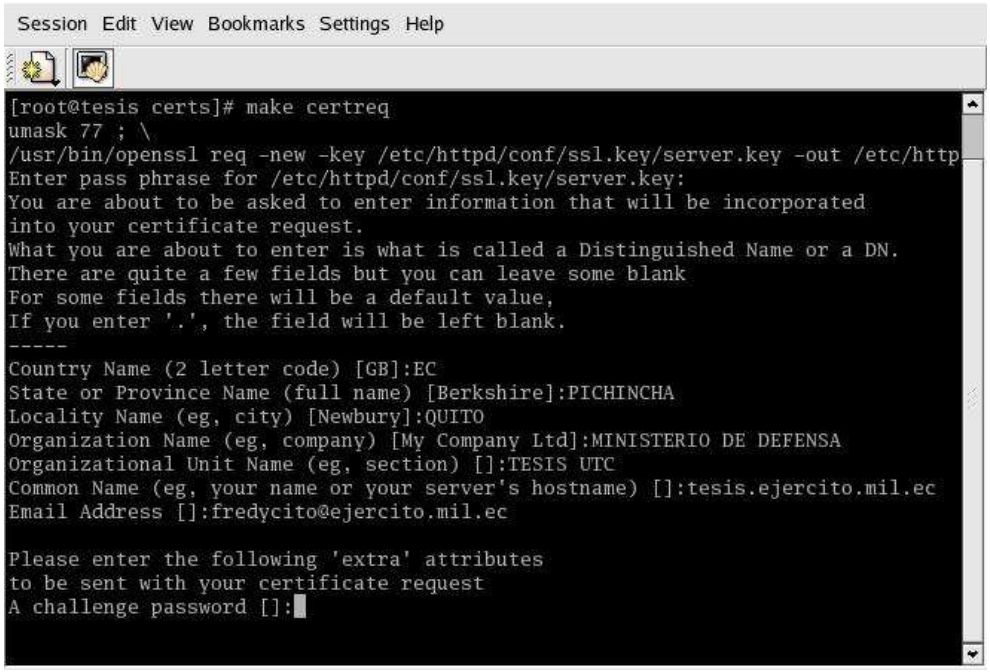

GRAFICO # 47. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 8.

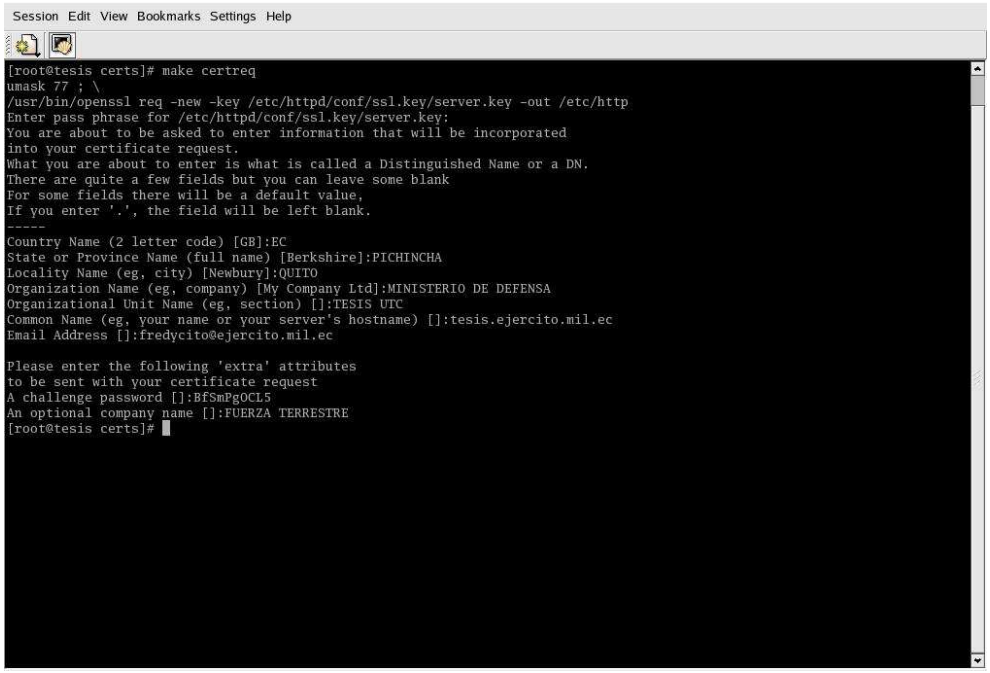

GRAFICO # 48. GENERACION DE LA PETICIÓN DE CERTIFICADO A LA EMPRESA CERTIFICADORA. PASO 9.

Una vez generado el archivo de petición se podrá descargar del sitio oficial de Verising, el demo requerido.

Para realizar la descarga la Autoridad Certificadora requerirá que se envíe esta petición , es decir el archivo que se creó al generar el pedido; este archivo se encuentra en el directorio /etc/httpd/conf/ssl.csr/ y se deberá enviar el archivo server.csr.

Cuando la Autoridad Certificadora compruebe la autenticidad de la petición enviará el demo por correo electrónico y se podrá continuar con la configuración

4.2.4.2.Configuración del demo y verificación del funcionamiento del servidor.

Al obtener el certificado bastará con pegar el mismo en el directorio /etc/httpd/conf/ssl.crt/ con el nombre server.cert y al momento de reiniciar el sistema este lo reconocerá por defecto. Y se podrá comprobar de la misma manera como se la realizó con el certificado auto firmado.

4.3. CONFIGURACION DEL SERVIDOR DE CORREO ELECTRONICO SENDMAIL

Para poder obtener un servidor de correo electrónico con un nivel de seguridad adecuado y que pueda brindar las características de acceso al mismo vía web-mail se recomienda la utilización de Sendmail como servidor de correo electrónico.

El mismo que al ser configurado con las consideraciones que se mencionan a continuación, cumplirá con los requisitos de funcionalidad, disponibilidad y seguridad propuestos por los autores de esta tesis, en consideración a los estándares de seguridad mencionados en el capitulo anterior del presente documento

4.3.1. Paquetes necesarios para un servidor de correo electrónico utilizando Sendmail.

sendmail-8.12.8-4.i386

sendmail-cf-8.12.8-4.i386

sendmail-devel-8.12.8-4.i386

sendmail-doc-8.12.8-4.i386

xinetd-2.3.10-6.i386

imap-2001a-18.i386

imap-devel-2001a-18-2001

php-imap-2001a-18-2001

fetchmail-6.2.0-3.i386

Es importante señalar que por razones de seguridad es necesario utilizar las versiones que se mencionan en este documento, pues versiones anteriores podrían tener problemas de seguridad.

4.3.2. Instalación de los paquetes necesarios para un servidor de correo electrónico con Sendmail

Como se ha mencionado anteriormente al realizar una instalación tipo servidor del sistema operativo Red Hat Linux , en la que se determinó que paquetes se debían instalar bastará con verificar que los paquetes mencionados se encuentren instalados; para lo cual desde una consola de Linux como root, ejecutar las respectivas instrucciones de verificación

```
# rpm –q  sendmail-8.12.8-4.i386
# rpm –q sendmail-cf-8.12.8-4.i386
# rpm –q sendmail-devel-8.12.8-4.i386
# rpm –q sendmail-doc-8.12.8-4.i386
# rpm –q xinetd-2.3.10-6.i386
# rpm –q imap-2001a-18.i386
# rpm –q imap-devel-2001a-18-2001
# rpm –q php-imap-2001a-18-2001
```

rpm –q fetchmail-6.2.0-3.i386

El sistema mostrará una salida indicando la existencia o no de la instalación de los paquetes en mención , en el caso de no constar alguno de ellos se deberá ejecutar la instrucción rpm –ivh y la dirección y nombre del paquete faltante.

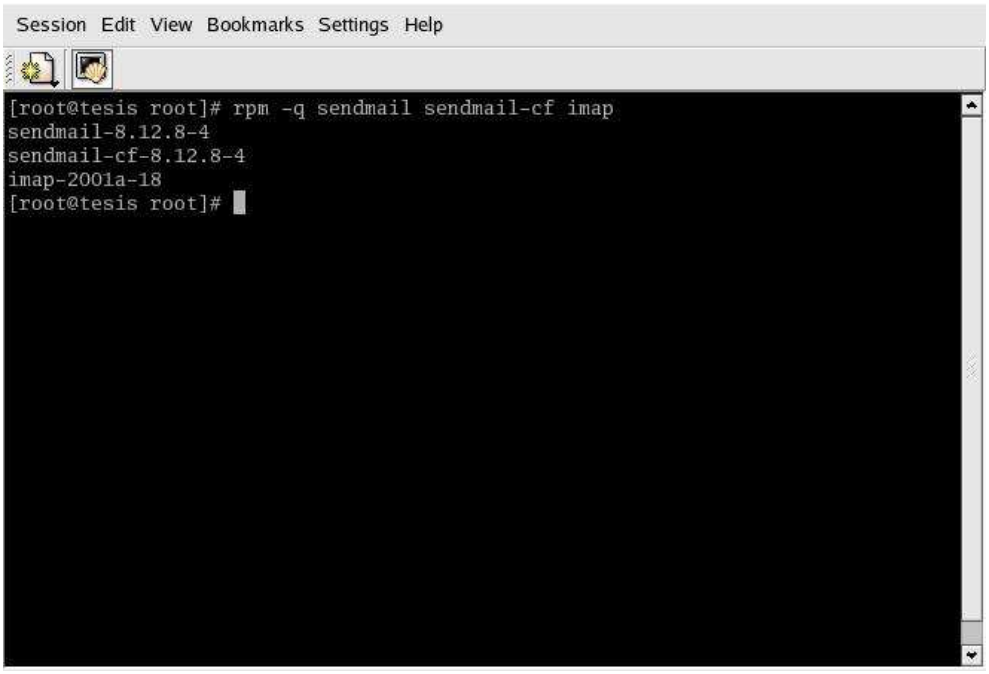

GRAFICO # 49. INSTALACIÓN DE LOS PAQUETES PARA LA CONFIGURACION DEL SERVIDOR DE CORREO ELCTRONICO

4.3.3. Verificación de requisitos previos a la instalación.

Para poder configurar adecuadamente todos los parámetros del servidor de correo electrónico con Sendmail, es necesario comprobar algunos parámetros en el servidor, con la finalidad de conocer varias especificaciones que se utilizarán en el proceso de la misma .

4.3.3.1. Determinar los parámetros de red.

Aunque parezca anecdótico, es necesario volver a comprobar los parámetros de red local, con la finalidad de poder determinar que maquinas o redes de nuestra intranet tendrán acceso al servidor y por ello estarán en la posibilidad de enviar o no correo electrónico.

Por motivos de seguridad al mantener un servidor de correo electrónico para la Fuerza Terrestre, el mismo que dará este servicio vía web-mail en la Internet e Intranet en la Comandancia General de la Fuerza Terrestre; por razones de orden jerárquico y política interna en la institución, solo se presta este servicio a determinadas personas y departamentos en la Comandancia General de la

Fuerza Terrestre, pues este solo está determinado para Directores, Subdirectores de departamentos y altos Jefes Militares .

Por lo que será necesario determinar las personas que tendrán una cuenta de correo electrónico y las maquinas en los departamentos que podrán o no enviar correo.

Para poder realizar esto se verificará el archivo /etc/sysconfig/network en el cual se verificarán el nombre de la maquina y domino que se utilizará como servidor; así como el gateway, los mismos que deberán corresponder a las configuraciones determinadas para este servidor.

vi /etc/sysconfig/network

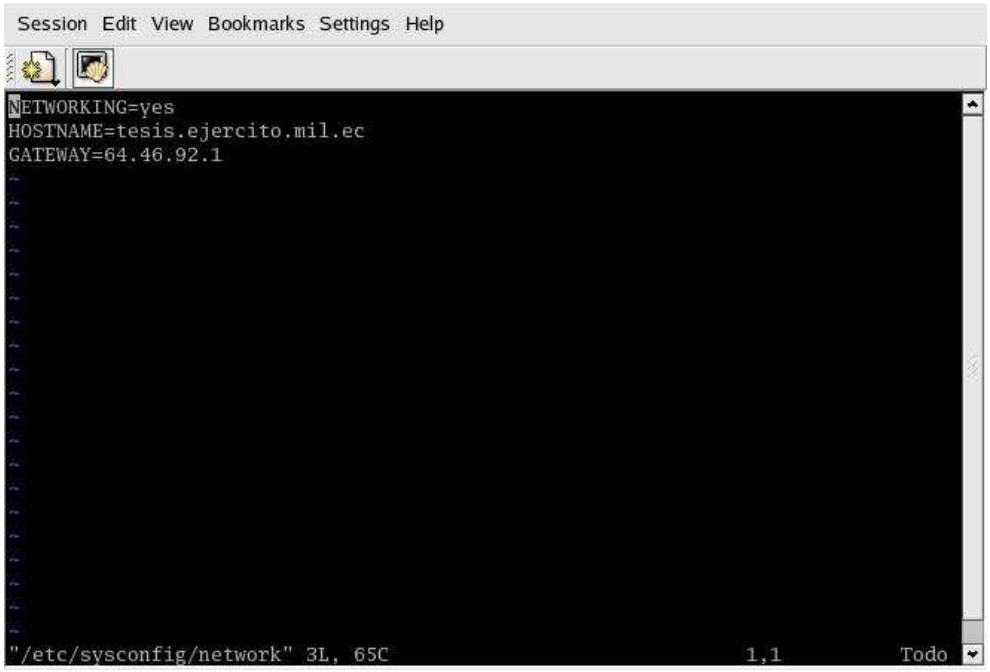

GRAFICO # 50. DETERMINACIÓN DE LOS PARÁMETROS DE RED.

Las direcciones de los hosts y las direcciones IP de la Intranet que podrán utilizar el servidor se determinarán en el archivo /etc/hosts

vi /etc/hosts

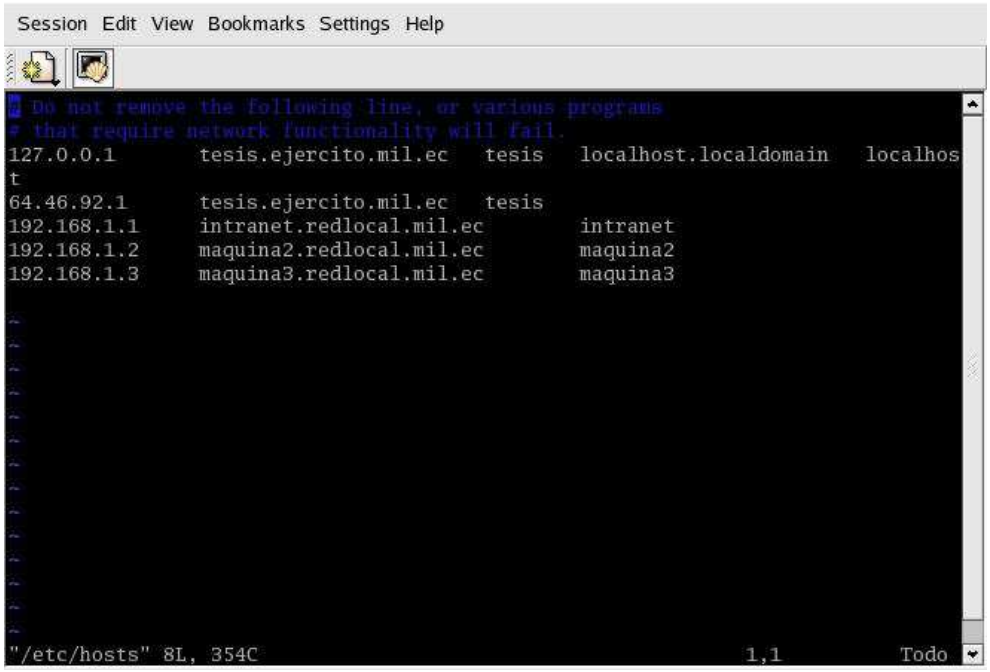

GRAFICO # 51. SELECCIÓN DE LOS USUARIOS DE LA INTRANET QUE PUEDEN UTILIZAR EL SERVIDOR DE CORREO ELECTRONICO

Verificación de los parámetros de DNS , en el cual se deberá configurar los parámetros para la intranet y la dirección real del servidor a la Internet.

vi /etc/resolv.conf

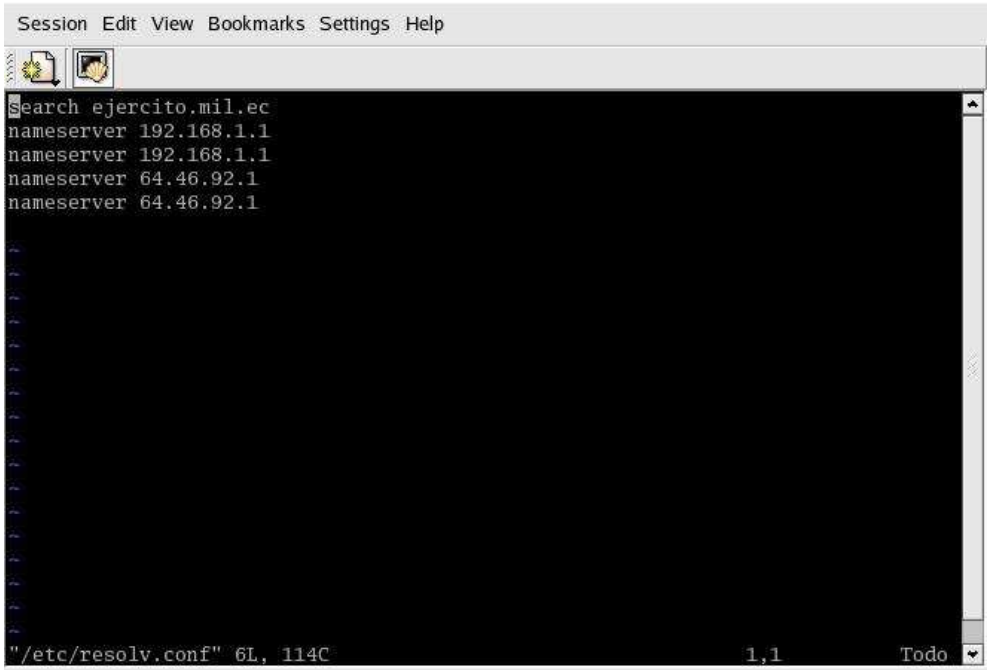

GRAFICO # 52. VERIFICACIÓN DE LOS PARÁMETROS DE DNS PARA LOS CUALES RESPONDERA EL SERVIDOR DE CORREO ELECTRONICO

4.3.4. Configurando sendmail.

Para poder establecer correctamente la configuración para este servidor se deberá determinar todos y cada uno de los posibles alias que tendrá el servidor a configurar, así como los posibles sub-dominios, es decir todos los posibles dominios para los cuales estaremos recibiendo correo en un momento dado.

Esta configuración se la realizará en el archivo local-host-names que se encuentra en el directorio /etc/mail/, para esta configuración se a determinado lo siguiente:

ejercito.mil.ec

tesis.ejercito.mil.ec

mail.ejercito.mil.ec

redlocal.ejercito.mil.ec

intranet.mil.ec

mail.redllocal.mil.ec

Estos parámetros se editarán en el archivo que se menciono utilizando el editor de texto vi desde una consola de linux como root.

vi /etc/mail/local-host-names

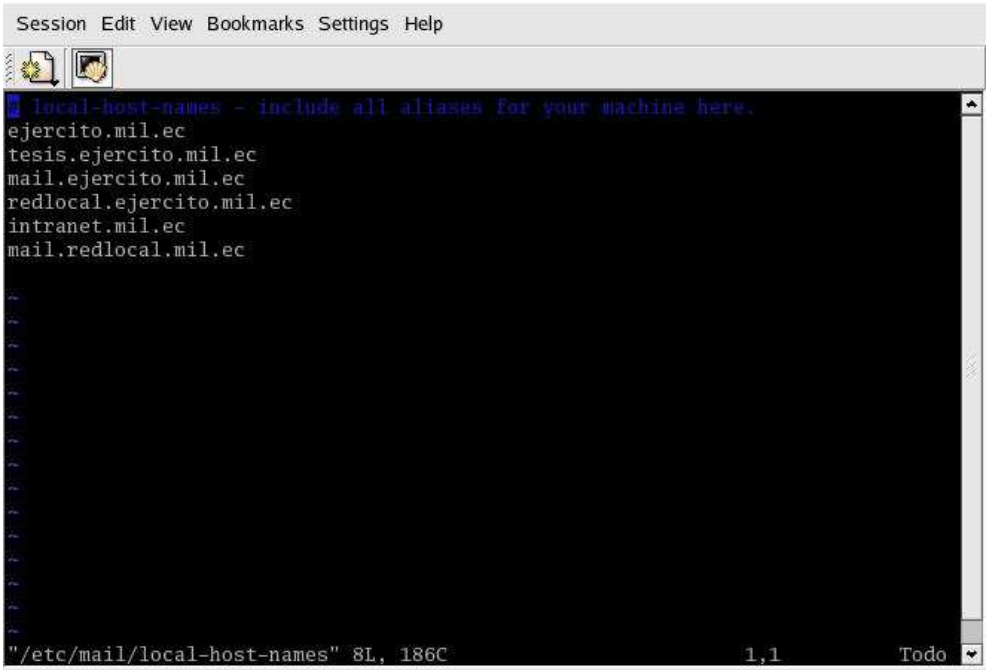

GRAFICO # 53. DETERMINACIÓN DE LOS DOMINIOS Y SUBDOMINIOS ASI COMO LOS ALIAS A LOS CUALES RESPONDERA EL SERVIDOR DE CORREO ELCTRONICO.

Una vez realizada esta tarea, se procederá a preparar el servidor de correo para su configuración para lo cual se recomienda respaldar el archivo sendmail.mc por razones de seguridad.

cp /etc/mail/sendmail.mc /etc/mail/etc/sendmail.mc.default

El siguiente paso será habilitar el servicio para la red local , es importante señalar que se habilitará para toda la red local por lo que es necesario establecer correctamente las restricciones de uso en la configuración de los hosts que se menciono anteriormente como medida de seguridad, no se deberá habilitar redes completas, únicamente se habilitarán maquinas reales con su dirección específica.

No se recomienda habilitar en este archivo peticiones de escucha para sendmail desde redes locales, se deberá hacerlo desde el archivo hosts como se indicó, pues esto podría causar que se habilite para maquinas que no deberían tener acceso al servidor.

El archivo se editará desde el editor vi de la consola de Linux como root. Para realizar la tarea mencionada se habilitará la intranet, deshabilitando la interfaz loopback comentando la respectiva línea en el archivo mencionado como se mostrará en la figura.

vi /etc/mail/sendmail.mc

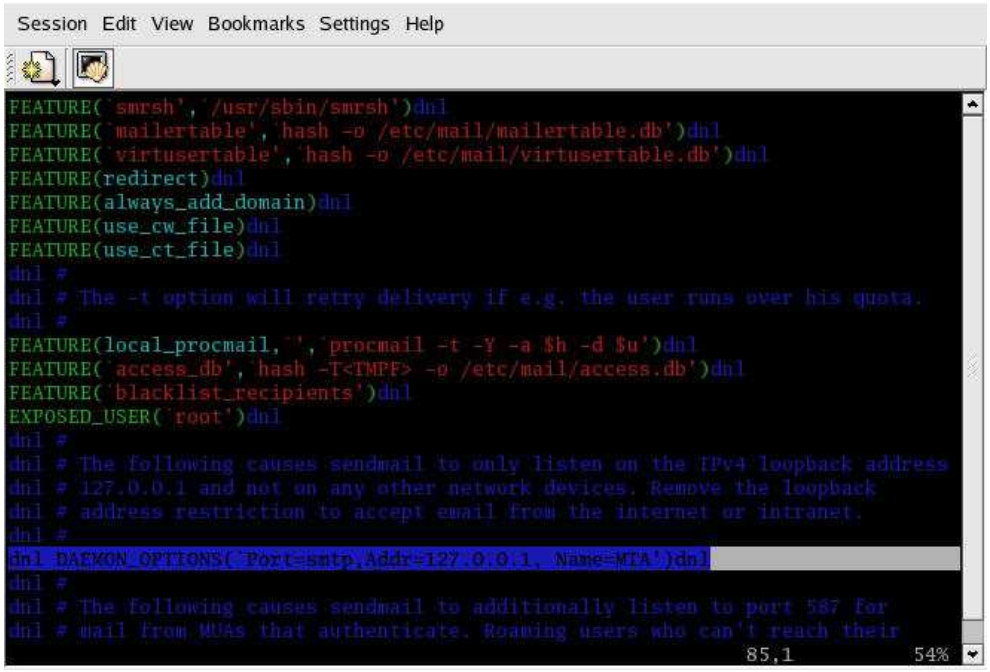

GRAFICO # 54. CONFIGURACIÓN DE EL ARCHIVO PRINCIPAL DE SENDMAIL

Como medida de seguridad será imprescindible filtrar todas las posibles direcciones así como dominios no resueltos que puedan tratar de dañar el servidor. Es importante conocer que el correo proveniente de dominios no resueltos, es decir que no están registrados en un DNS, se lo considerará como peligroso y deberá ser rechazado por el servidor.

Esta configuración se la conseguirá al configurar el archivo sendmail.mc, para repeler este tipo de correo, es decir solo aceptará correo establecido en la configuración del archivo local-host-names en el que se determino los posibles

dominios y sub-dominios que enviaran correo y para los mismos se recibirá correo y que ya se la realizó anteriormente. Además con esto se definirá una configuración perfecta para evitar el spam.

En el archivo sendmail.mc bastará con deshabilitar la opción ‘accept_unresolvable_domains’ de la misma manera como se hizo con el loopback

vi /etc/mail/sendmail.mc

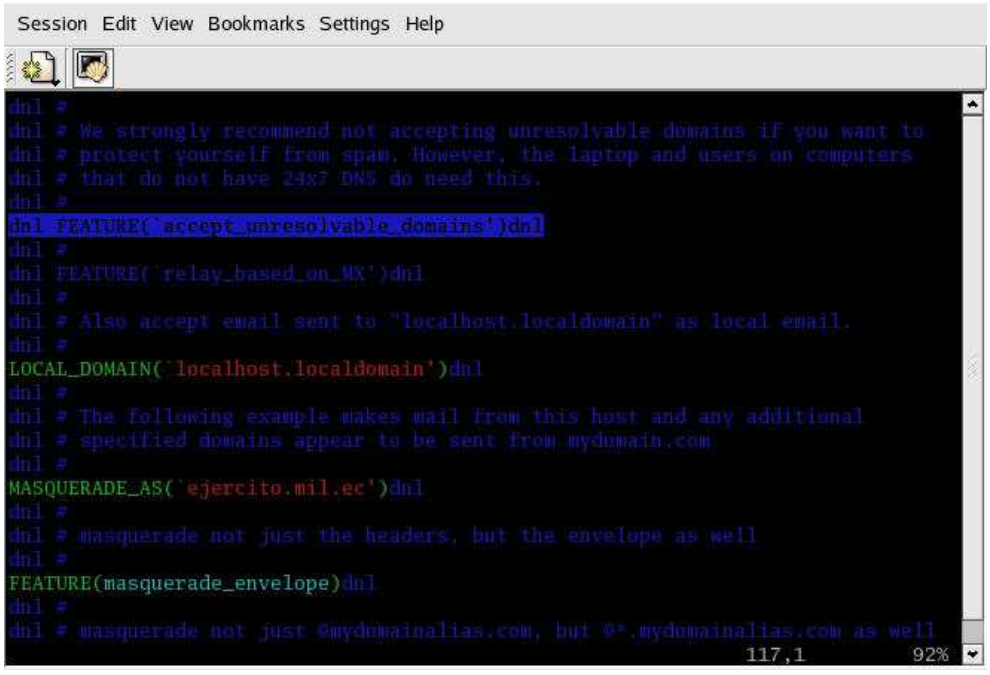

GRAFICO # 55. CONFIGURACIÓN DE EL ARCHIVO PRINCIPAL DE SENDMAIL

Ya realizadas las dos configuraciones anteriores, se procederá a establecer la máscara con la cual se enviará el correo electrónico y que será determinada para todos los usuarios de este servidor de correo electrónico.

La máscara que se definirá deberá corresponder al dominio con el cual fueron configurado los anteriores servidores es decir DNS y HTTPS pues todos estos trabajarán en conjunto para el funcionamiento adecuado de la propuesta al final. Deberá corresponder al dominio de la institución para la cual se configuró los servidores en este caso ejercito.mil.ec

Para realizar esto se añadirá al archivo sendmail.mc nuestra mascara para el correo; para lograr esto utilizaremos el editor de texto vi desde la consola de Linux para poder editar el archivo y realizar la configuración respectiva.

vi /etc/mail/sednmail.mc

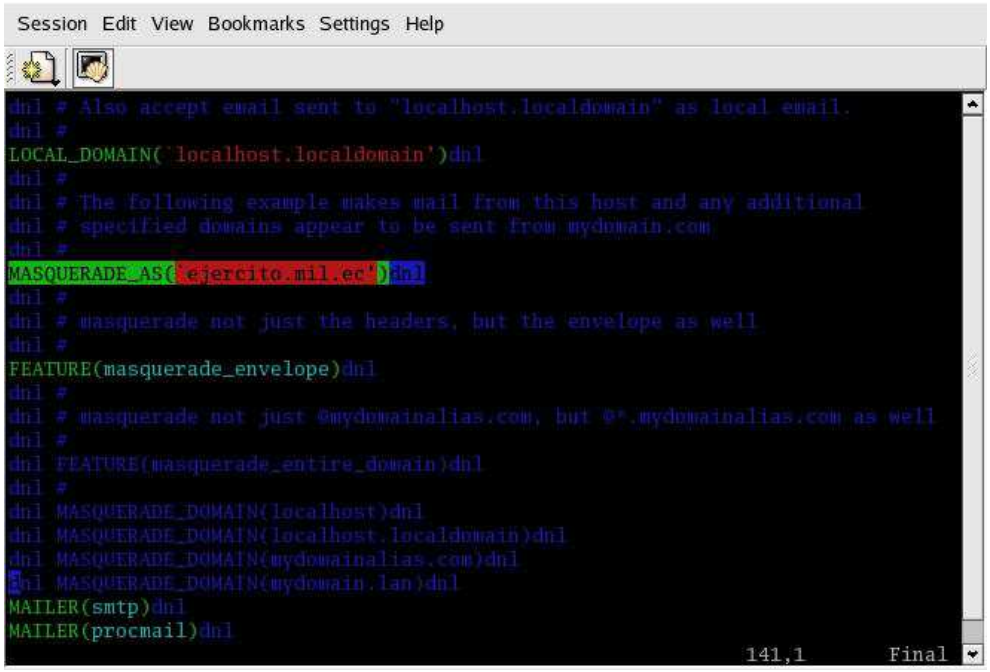

GRAFICO # 56. CONFIGURACIÓN DE EL ARCHIVO PRINCIPAL DE SENDMAIL

Al termino de la configuración del archivo sendmail.mc, es necesario generar el archivo sendmail.cf utilizando como base el archivo que acabamos de configurar; para esto utilizaremos el siguiente comando desde la consola de linux m4.

m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

Es importante mencionar que este archivo debe ser generado en el directorio /etc/mail/ de no hacerlo así el servidor no podría direccionar el archivo de configuración generado.

Al concluir con al configuración del archivo sednmail.mc continuaremos por definir los dominios a los cuales se podrá enviar correo electrónico. Por seguridad para este servidor se establecerá únicamente los dominios y sub-dominios que corresponden a la intranet y para el mismo servidor en la Internet.

Para esto se deberá generar el archivo relay-domains en el directorio /etc/mail se considerará explícitamente los siguientes parámetros:

ejercito.mil.ec

tesis.ejercito.mil.ec

intranet.redlocal.mil.ec

redlocal.mil.ec

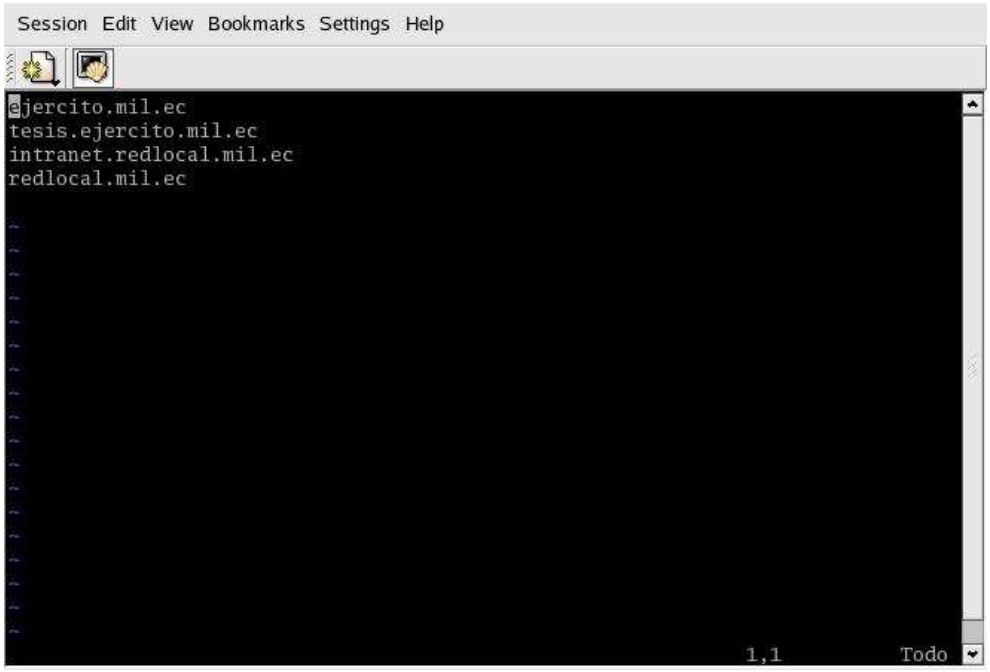

GRAFICO # 57. CONFIGURACIÓN DE LOS DOMINIOS DE SEGURIDAD A LOS Y DESDE LOS CUALES SE PODRA ENVIAR Y RECIBIR CORREO

Como se puede observar en la figura solo constan los parámetros mencionados, los mismos que fueron establecidos también en al configuración del DNS por razones de seguridad.

Adicionalmente como un filtro mas de uso y restricción del servidor se establecerán nuevamente las direcciones de las maquinas dentro de la intranet así como su salida a la Internet para uso de correo electrónico, pero de una manera mas explicita; consiguiendo un total control de las maquinas y usuarios que tendrán acceso al mismo. Esta configuración se la realizará en el archivo access

que se encuentra en el directorio /etc/mail; se utilizará la consola de Linux y el editor vi.

vi /etc/access

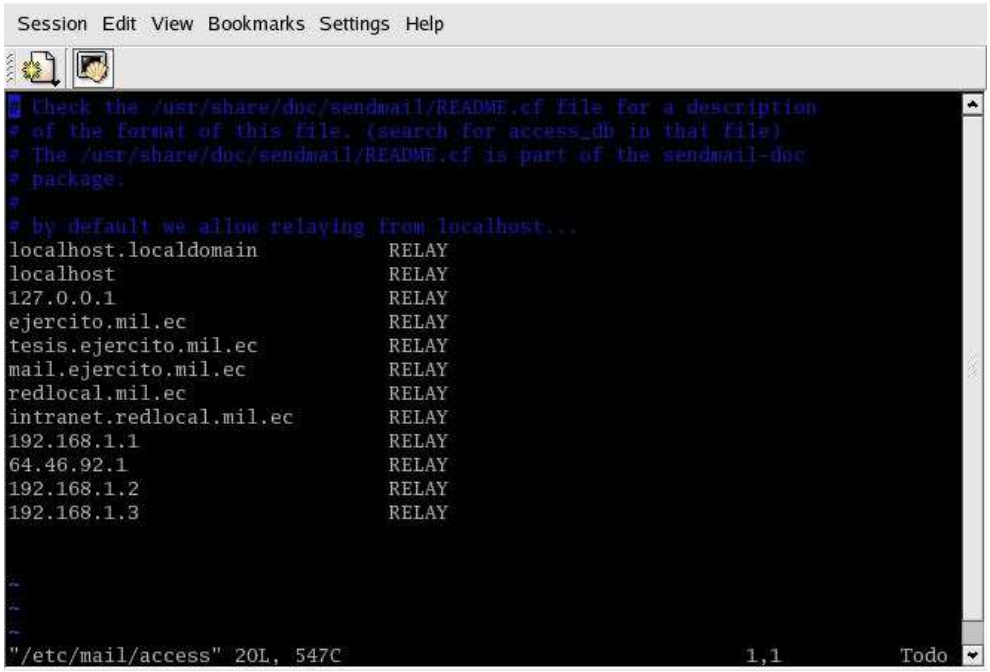

GRAFICO # 58. FILTRO ADICIONAL DE SEGURIDAD. ARCHIVO ACCESS

Como seguridad adicional se podrá configurar el spam bloqueando direcciones indeseables de correo electrónico en este archivo. Pero como ya se realizó esta configuración en el archivo sendmail.mc esto no será estrictamente necesario.

Al termino de esta configuración se deberá compilar este archivo con la finalidad de generar otro archivo en formato de base de datos a fin de ser utilizado por sendmail. Bastará con ejecutar el comando make desde el directorio /etc/mail desde una consola de Linux.

```
# cd /etc/mail

# make
```

Es importante generar un alias para la cuenta de root del servidor , este alias deberá corresponder a la dirección de correo electrónico del administrador al cual le llegarán cualquier informe de posibles errores o fallas en el sistema.

Para esto editaremos desde la consola de Linux el archivo alias que se encuentra en el directorio /etc y en este designaremos la cuenta de alias par root.

```
# cd /etc

# vi alias
```

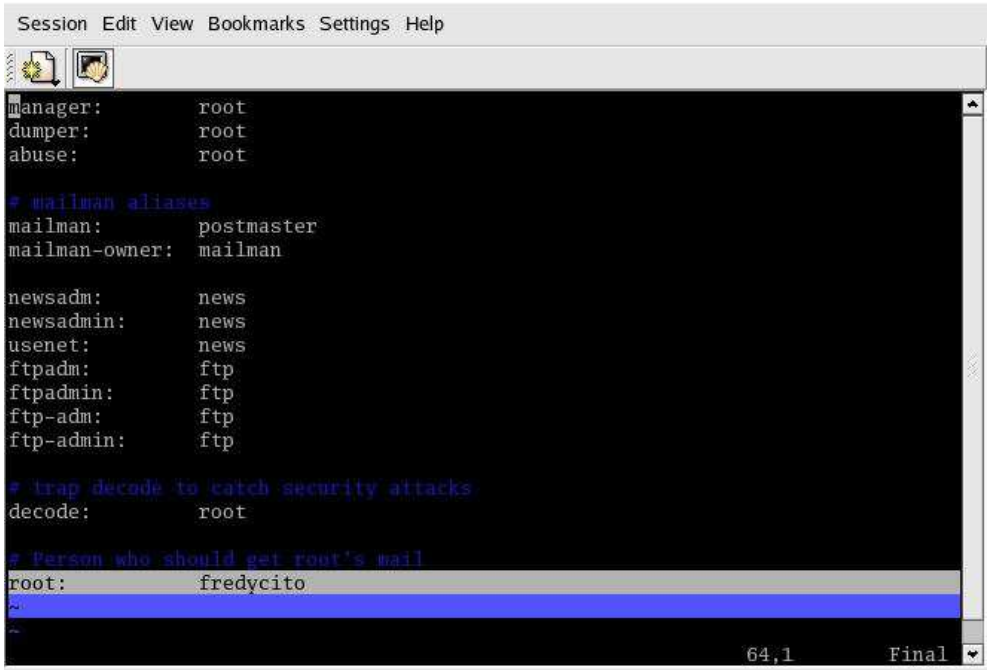

GRAFICO # 59. CONFIGURACIÓN DE LA CUENTA DE SEGURIDAD PARA ROOT, DESIGNACIÓN DE LA CUENTA DE ALIAS

Como se puede ver en la figura se designo el alias para root como fredycito pero para que este cambio surta efecto se deberá ejecutar el comando newaliases desde la consola de Linux

/sbin/newaliases

Al termino de las configuraciones estaremos listos para verificar y arrancar el servidor, bastará con reiniciar sendmail.

service sendmail restart

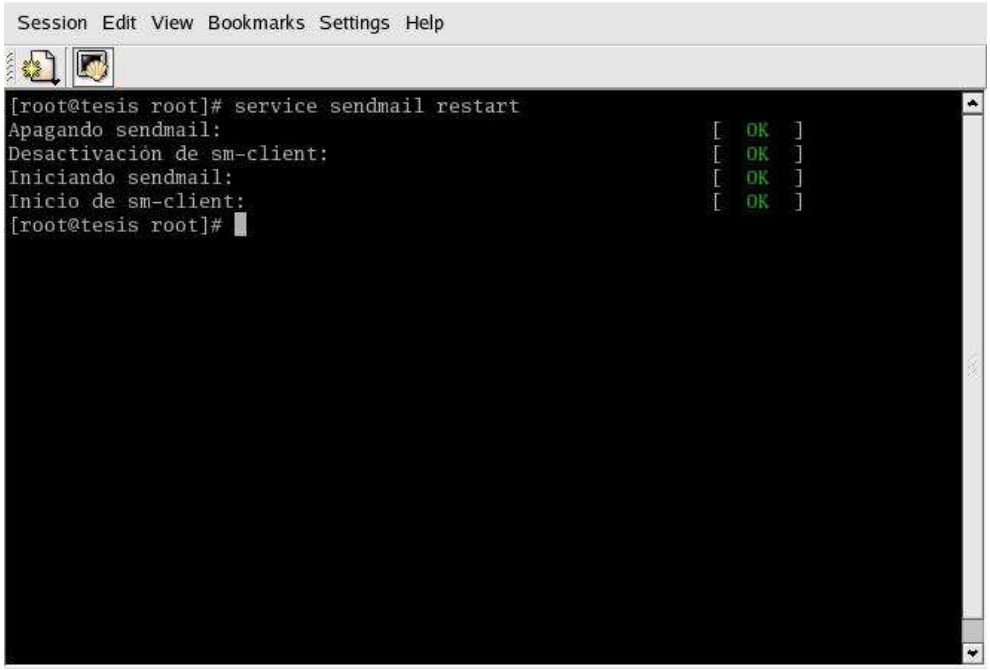

GRAFICO # 60. VERIFICACION Y ARRANQUE DEL SERVIDOR DE CORREO ELECTRONICO

Una vez que se a comprobado el arranque del servidor, configuraremos este servicio a fin de que se levante al iniciar el sistema, para lo cual ejecutaremos la siguiente instrucción .

chkconfig sendmail on

4.3.4.1.Consideraciones adicionales de seguridad para Sendmail

Por la naturaleza de la información en el correo electrónico para la Comandancia General del Ejercito, es necesario establecer un margen más elevado de seguridad que el que ya hemos establecido al configurar el servidor de correo electrónico.

Es importante evitar un posible ataque al servidor que no pueda controlar las configuraciones anteriores; se podría considerar una saturación del servidor por parte de algún usuario mal intencionado, desencadenando en una denegación de servicio.

Cada una de las configuraciones de seguridad que mencionaremos a continuación se establecerán en el archivo sendmail.mc para esto se deberá editar el mencionado archivo e insertar las respectivas líneas de instrucción de acuerdo sea el caso, debajo de la última línea que incluya define y arriba de la línea que incluya FEATURE.

Numero máximo de destinatarios. Es importante limitar el número máximo de destinatarios el sistema por defecto permitirá 256 destinatarios, por seguridad se

limitará a un máximo de 100 destinatarios, con al finalidad de controlar la sobresaturación del servidor.

define (′confMAX_RCPTS_PER_MESSAGE’, ‘20’)dnl

Tiempo de letargo. Es necesario establecer el tiempo de letargo para los usuarios que sobrepasen la configuración anterior, pues el sistema por defecto no establece un tiempo determinado par este tipo de situaciones en las que el usuario sobrepase el numero de destinatarios. El tiempo máximo que se establecerá es de 2 segundos.

define (′confBAD_RCPT_THROTTLE’, ‘2’)dnl

Deshabilitar nombres de usuarios a posibles espías. Es importante tratar de deshabilitar posibles puertas de acceso al sistema al directorio en el que encuentran almacenados los nombres de los usuarios del sistema. Eso se consigue deshabilitando varios comando SMTP como son EXPN y VRFY los cuales son utilizados por los spammers para acceder a los nombres de los usuarios; adicionalmente se deberá deshabilitar las notificaciones de entrega, ya que este constituye un mecanismo para verificar la existencia de una cuenta; con

esto se configurará el sistema para que obligatoriamente solicite HELO o EHLO antes de utilizar el comando MAIL. Pues muchos de los programas espía que viajan mediante correo electrónico ni siquiera se molestan en enviar el HELO o EHLO.

define (′confPRIVACY_FLACS' , 'goaway')dnl

Evitar desbordamiento de búfer en IMAP. Uno de los mas grandes problemas de los servidores de correo electrónico se presenta cuando alguien consigue que el sistema no registre las transacciones que se están realizando, con sus respectivas consecuencias. Esto lo consiguen cuando algún problema utilizado por piratas informáticos mediante el spam consiguen generar cabeceras de correo electrónico muy grandes por consecuencia los MTA no podrán registrar las transacciones.

La solución optima para evitar esto es limitar la cabecera de los correos; un correo electrónico ordinario por mas exagerado que este sea máximo tendrá una cabecear de 5kb a 6kb por lo que este será el parámetro para limitar el tamaño de la cabecera de los mensajes. Estos e consigue mediante la siguiente instrucción en la que se deberá establecer el tamaño en bytes. Lo recomendable es 16kb.

define (′confMAX_HEADERS_LENGTH’, ‘16384’)dnl

Garantizar el tráfico. Una de las maneras mas idóneas de garantizar el trafico de correo es limitando el tamaño del mismo en bytes para este. Las especificaciones de tamaño se especificarán de acuerdo al criterio del administrador del sistema; sin embargo se recomienda a un máximo de 3MB .

define (′confMAX_MESSAGE_SIZE’, ‘314728’)dnl

Optimizar el uso del servidor. Es importante optimizar el uso del servidor, limitando el numero de conexiones simultaneas al mismo. Sendmail por defecto no establece un limite para el numero de procesos hijos. Esto podría causar que el servidor se constituya en una espera interminable ya que tendría que atender todas las peticiones a la vez. Al limitar el numero de conexiones simultaneas se conseguirá que el servidor pueda atender de una manera optima a las primeras consiguiendo terminar y atender a las peticiones en espera.

Este parámetro deberá ser analizado por el administrador del sistema, en consideración al hardware existente para el servidor. Para el mismo parámetro

de seguridad se deberá considerar el número de conexiones por segundo ya que sendmail no establece parámetros para esto.

define (′confMAX_DAEMON_CHILDREN’, ‘5’)dnl

define (′confCONNECTION_RATE_THROTTLE’, ‘5’)dnl

Ocultar parámetros del software . Una consideración imprescindible de seguridad es ocultar el nombre y la versión del software que se está utilizando para el servidor de correo electrónico. Pues una de las primeras vulnerabilidades de los sistemas es conocer el nombre y la versión del software.

Al conocer estos dos parámetros cualquier delincuente informático podrá tratar de buscar las posibles fallas de seguridad con mayor facilidad y atacar el sistema, al ocultar estos dos parámetros será imposible que logre descubrir posibles vulnerabilidades en el sistema.

define (′confSMTP_LOGIN_MSG’, ‘$j ; $b’)dnl

4.3.5. Configuración de los servicios POP3 e IMAP

Se deberá habilitar los servicios pop3 e imap, pero por razones de seguridad se habilitará para SSL es decir pop3s e imaps es decir autentificación con criptografía .

Es importante señalar que no se dará servicio como tal a pop3 e imap, la razón es que al utilizar firma digital y al mantener un nivel de seguridad optimo; el servidor de correo electrónico no permitirá la descarga de claves o contraseñas para la utilización de firma digital fuera del servidor. Pero por la necesidad de estos protocolos para el funcionamiento del servidor de correo electrónico desde la aplicación de web-mail se los configurará y habilitará como necesidad de squirrelmail como servidor de web-mail únicamente.

Las opciones de POP3 seguro con criptografía e IMAP seguro con criptografía se configurarán desde la consola de Linux editando los respectivos archivos de configuración, en los cuales se habilitará el servicio que necesitamos para el funcionamiento de todo el sistema como tal.

```
# cd /etc/xinetd/

# vi pop3s

# vi imaps
```

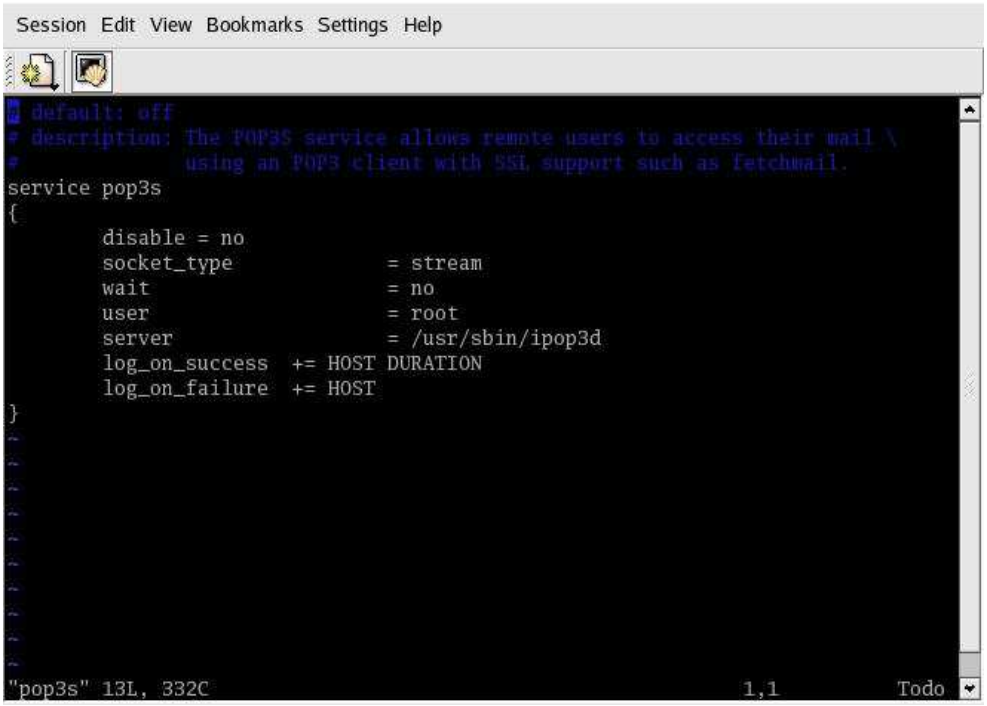

GRAFICO # 61 . CONFIGURACIÓN DE EL PROTOCOLO POP3 PARA SSL.

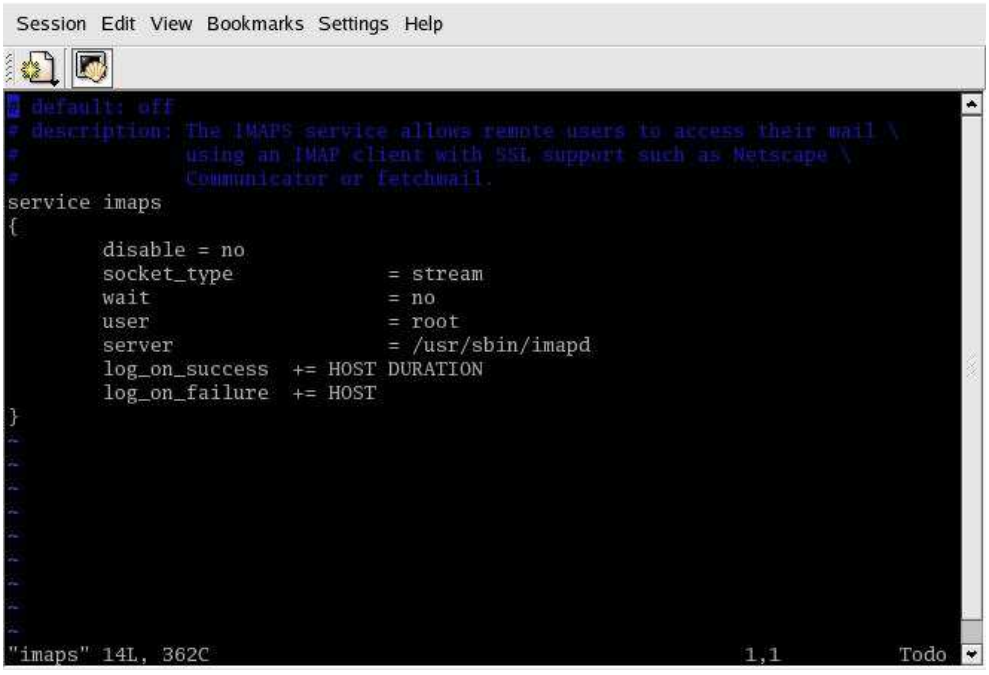

GRAFICO # 62. CONFIGURACION DE EL PROTOCOLO IMAP PARA SSL

Bastará simplemente con habilitar el servicio como se puede ver en las figuras anteriores.

Concluido con esto se realizará el arranque del servicio y la configuración del mismo para arrancar cuando se inicie el sistema únicamente.

service xinetd restart

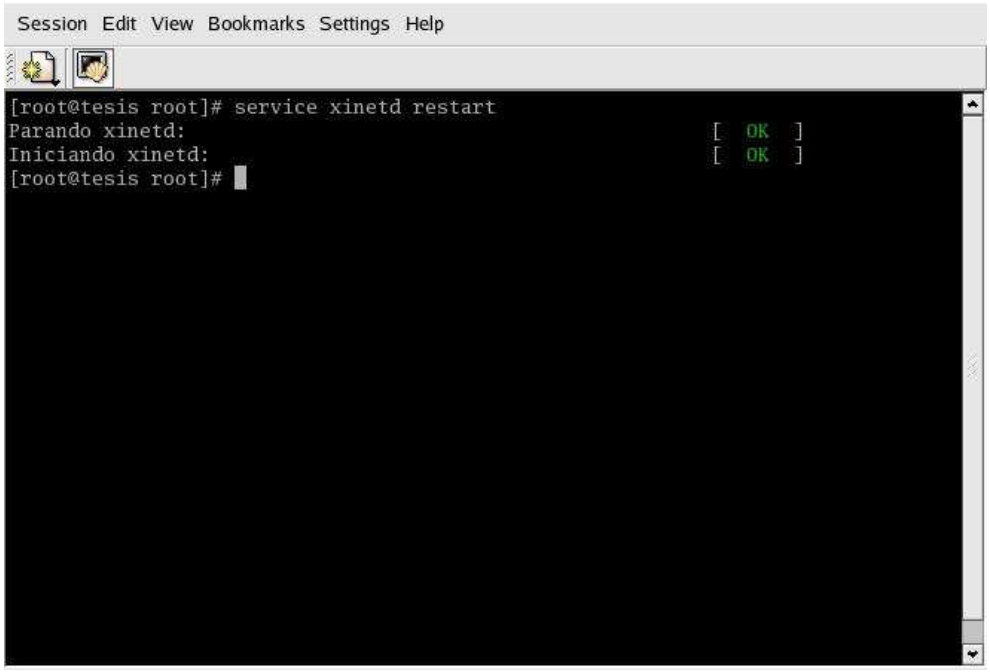

GRAFICO # 63. VERIFICACIÓN Y ARRANQUE DEL SERVICIO XINETD (POP3S e IMAPS)

```
# chkconfig xinetd on
```

Con esto se ha establecido la configuración para imap y pop3 para SSL

4.4. CONFIGURACION DE LA INTERFAZ WEB-MAIL

Una de los servicios importantes y en consideración a las necesidades de la institución para la cual se esta realizando esta propuesta, que debe brindar el servidor de correo electrónico es el acceso al mismo en la Internet con una interfaz fácil de usar y que cumpla con los requisitos de seguridad que se están mencionando y se pueda implementar la función de firma digital a través del mismo.

Por consiguiente se ha establecido como web-mail el uso de SQUIRRELMAIL por ser un software robusto y de fácil utilización por el usuario, además de ser parte de la comunidad Linux por lo que estará dentro de sus condiciones de uso y modificación.

Adicionalmente presta una gran flexibilidad para la incorporación de software adicional, lo que nos será de mucha utilidad para poder implementar un software para firma digital, que se lo explicará posteriormente.

4.4.1. Paquetes necesarios para la configuración de Web-Mail Squirrelmail.

Squirrelmail-1.4.2-3.noarch

Php-mysql-4.2.2-17.i386

Mysql-3.23.54.a-11.i386

Es importante mencionar que se utilicen estas versiones pues al utilizar versiones anteriores se podría tener fallas de seguridad.

La versión de squirrelmail que se esta señalando en este documento no consta en los cds de instalación de Red Hat 9.0 por lo que será necesario descargase de la Internet esta versión por considerarse la mas apropiada para la utilización de firma digital con gnupg.

Como requisitos previos a la configuración de squirrelmail se deberá cumplir con lo siguiente.

Servidor DNS perfectamente instalado y configurado.

Servidor HTTPS perfectamente instalado y configurado

Servidor de Correo Electrónico perfectamente Instalado y configurado

4.4.2. Instalación de los paquetes necesarios para la configuración de Squirrelmail

En la instalación del sistema operativo Red Hat Linux se realizo un instalación tipo servidor por lo que ya se encuentran instalados los paquetes concernientes a la base de datos así como sus dependencias de igual manera php sus dependencias y paquetes adicionales, necesarios para su funcionamiento. Sin embargo se realizará una confirmación de la instalación de los mismos como la hemos realizado en los casos anteriores al citar este punto.

```
# rpm –q httpd
# rpm –q mysql
# rpm –q php-mysql
# rpm –q php-imap
```

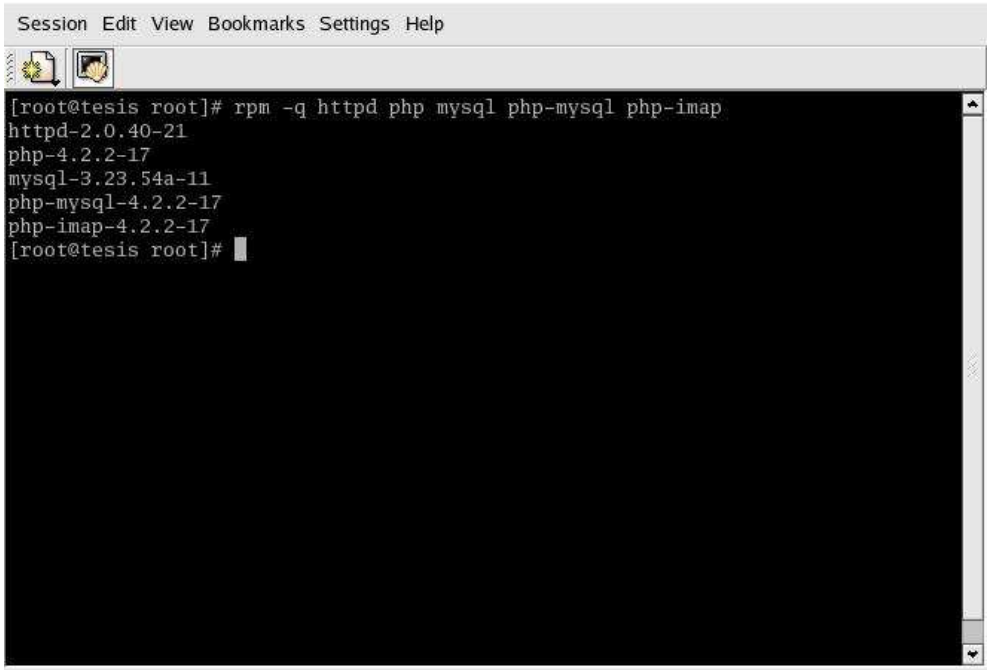

GRAFICO # 64. INSTALACION DE LOS PAQUETES NECESARIOS PARA LA CONFIGURACIÓN DE WEB-MAIL

Para la instalación de squirrelmail se recomiendo descargar el rpm de la dirección http://www.squirrelmail.org y proceder a la instalación desde la consola de Linux con el comando rpm

rpm –ivh squirrelmail-1.4.2-3.noarch.rpm

4.4.3. Configuración de Squirrelmail

Para realizar una correcta instalación con las adecuadas medidas de seguridad se deberá seguir los siguientes procedimientos.

4.4.3.1. Configuración de un alias como medida de seguridad.

Muchos autores recomiendan que no se cambie el nombre del directorio en el que se ubicará la interfaz de squirrelmail; sin embargo como medida de seguridad se recomienda hacerlo ya que esto no permitirá un fácil acceso al directorio de squirrelmail por parte de un delincuente informático; se considera por parte de los autores una importante medida de seguridad pues se puede constituir en una importante puerta de acceso para personas mal intencionadas que busquen hacer daño al sistema ya que dicho directorio para el alias se encuentra en los directorios públicos del servidor de páginas web.

Además permitirá una mejor administración así como una personalización más aceptable por parte del administrador del sistema.

Para realizar este proceso, desde una consola de Linux como root, mediante la utilización de un editor de texto, se procederá a editar el archivo squirrelmail.conf; este archivo de configuración se encuentra ubicado en el directorio /etc/httpd/conf.d/

cd /etc/httpd/conf.d/

#vi squirrelmail.conf

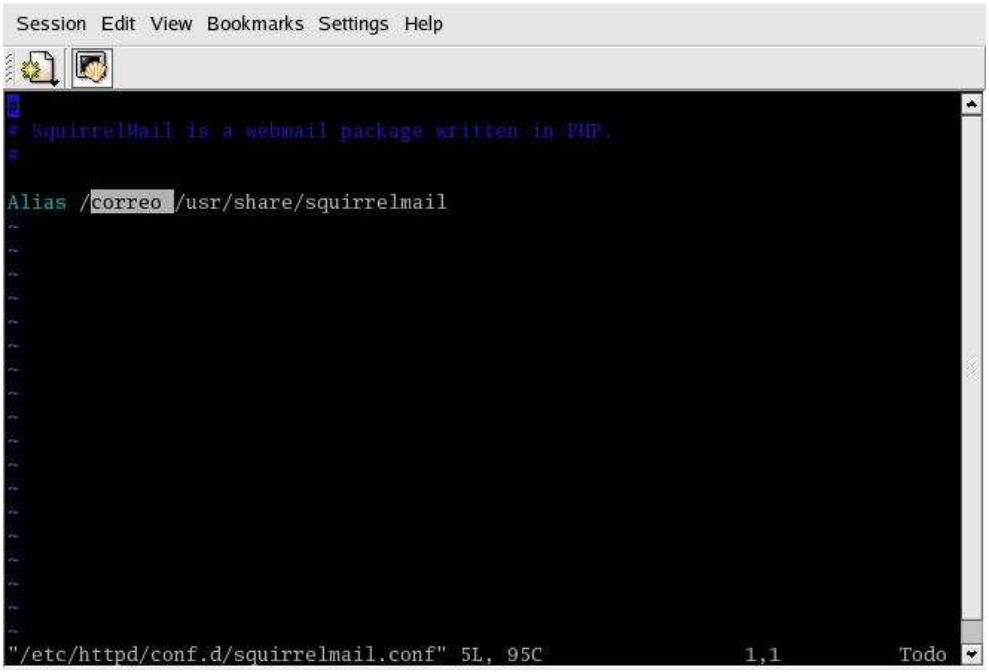

GRAFICO # 65. CONFIGURACIÓN DE EL ALIAS Y REDIRECCIONAMIENTO DE LA CARPETA PRINCIPLA DE WEB-MAIL

Para nuestro caso como se puede observar en la figura, se establece el alias para webmail como correo; es importante que este alias se mantenga en concordancia con la aplicación a la que hace referencia, para una mejor administración.

4.4.3.2.Configuración de las interfaces de acceso al correo electrónico.

Para realizar una configuración adecuada de las interfaz de acceso al correo electrónico de squirrelmail es necesario que el administrador del sistema tenga perfectamente definido varias necesidades del usuario; entre las más importantes podemos mencionar el idioma de la interfaz, la cantidad de herramientas que necesitará el usuario para la administración de su correo entre otras .

Desde una consola de Linux como root, ejecutaremos el guión de configuración ./conf.pl de squirrelamil; al ejecutar este guión de configuración permitirá una interfaz de fácil administración por parte de quien realice esta configuración.

El guión de configuración que se menciono anteriormente se encuentra en el directorio /usr/squirrelmail/config/ y se ejecutará de la siguiente manera.

cd /usr/squirrelmail/config/

./config.pl

Al ejecutar estos dos comandos se nos desplegará la siguiente pantalla.

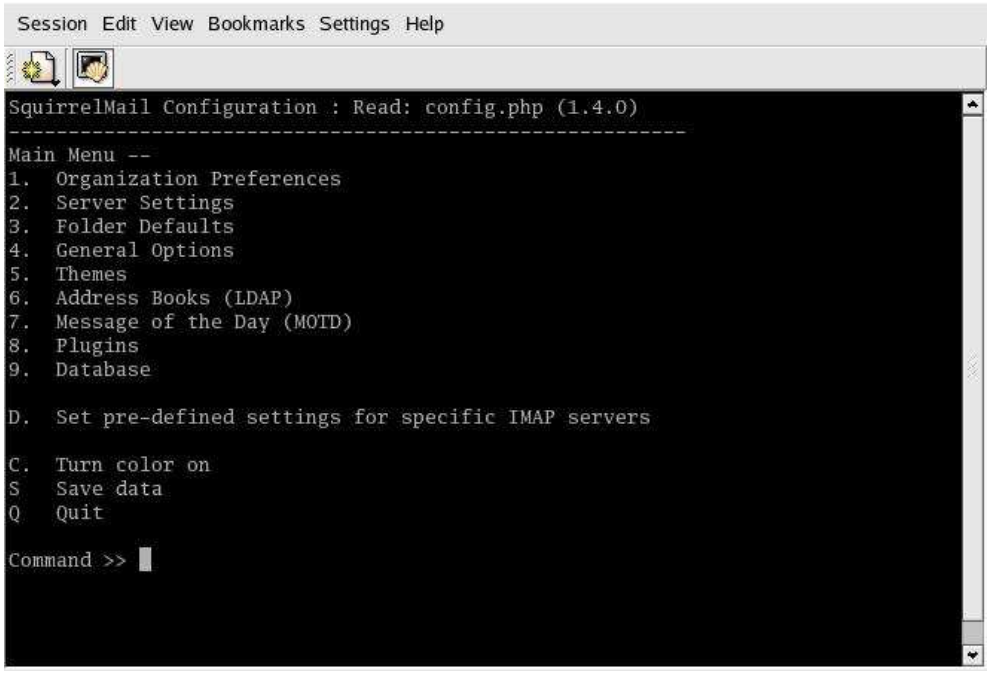

GRAFICO # 66. CONFIGURACIÓN DEL WEB-MAIL

En la figura anterior se puede observar la pantalla inicial de configuración; en esta encontraremos un menú de opciones que nos ayudarán a configurar los parámetros que necesitamos. Para acceder a cualquier opción del menú bastará con escribir el número que se encuentra a la izquierda junto al titulo del menú.

Organization preferentes . Preferencias de Configuración; se deberá definir los siguientes parámetros:

Nombre de la organización

Logotipo de la organización; dimensiones y directorio en el que se encuentra

Mensaje de la barra de título de la ventana del navegador.

El idioma que utilizará la interfaz del usuario

URL y el título de la página principal de acceso al sistema.

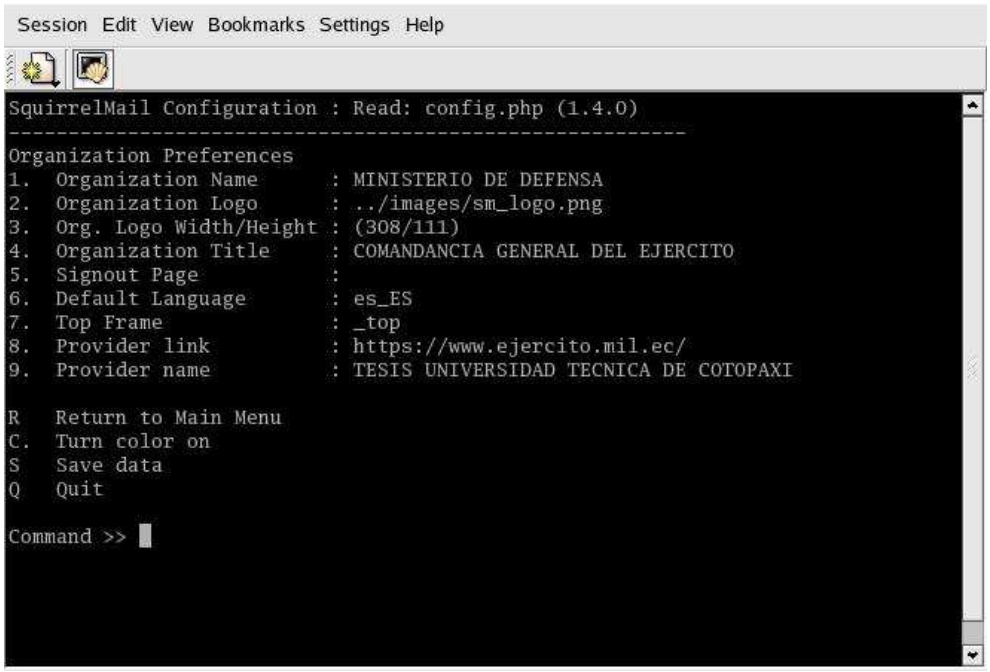

GRAFICO # 67. CONFIGURACIÓN DE EL WEB-MAIL. PASO 1

Como se puede observar en al figura se han establecidos los parámetros de la organización así como se ha establecido que el idioma para la interfaz del usuario sea el español.

Server Settings. Opciones para los servidores; esta pantalla me permitirá configurar las opciones de acceso hacia los otros servidores como el DNS y en especial al servidor Web.

En este caso por tratarse de una aplicación únicamente demostrativa en la que conviven en una misma máquina Servidor de Paginas Web , Servidor DNS y Servidor de Correo Electrónico bastará con establecer el dominio que se configuró en el Servidor DNS.

En el caso practico en el que la determinación de los servidores sea una máquina particular para cada uno se deberá establecer dichos servidores en esta sección de la configuración

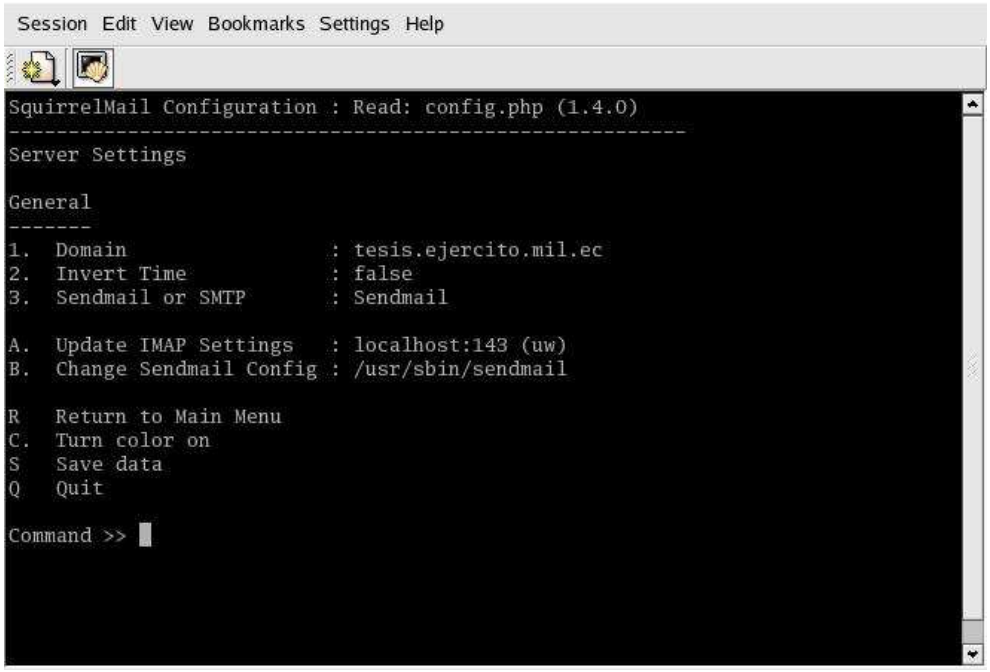

GRAFICO # 68. CONFIGURACIÓN DE EL WEB-MAIL. PASO 2

Adicionalmente se podrá modificar la opción de configuración hacia el servidor de correo electrónico, para nuestro caso al tener como servidor de correo electrónico a sendmail se deberá mantener el path hacia este servidor.

Fólder Defaults. Configuración de carpetas; en esta carpeta se deberá configurar las opciones de carpeta sus alias con las que se presentará en la interfaz de correo al usuario .

Por defecto todas estas carpetas tienen sus nombres y configuraciones en Ingles pese a cambiar el idioma a español estas mantendrán sus nombres iniciales que se muestran en la pantalla de configuración; no se puede determinar la utilidad de cambiar el idioma de las carpetas pero por ser el idioma más utilizado el español se recomienda cambiar sus nombres a éste idioma.

Sin embargo no se recomienda el cambio de directorio principal de las carpetas en donde se almacenará el correo; ya que al mantener la carpeta /mail por defecto se podrá realizar una mejor administración por parte del usuario del correo almacenado en el servidor.

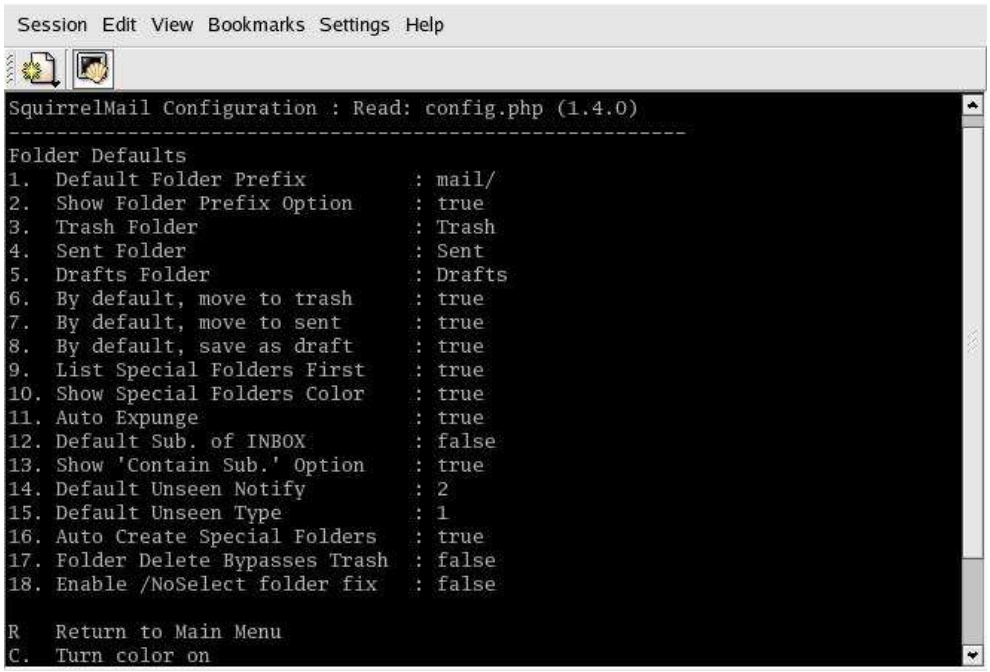

GRAFICO # 69. CONFIGURACIÓN DE EL WEB-MAIL. PASO 3

Como se puede observar en la anterior figura no se realizó cambios en los nombres de las carpetas pues para el usuario será por demás entendido la determinación de las carpetas aunque mantengan sus nombres en Ingles. La necesidad de cambio se puede considerar al gusto del administrador del sistema.

General Options. Opciones Generales; al llegar a esta parte de la configuración de squirrelmail, se podrá determinar varios aspectos del sistema.

La mayoría de estos aspectos son de carácter informativo como es el estándar ISO, los directorios de datos, directorio documentos adjuntos etc. Es recomendable no realizar ningún cambio en esta sección de squirrelmail, ya que se manejarán estos valores por defecto.

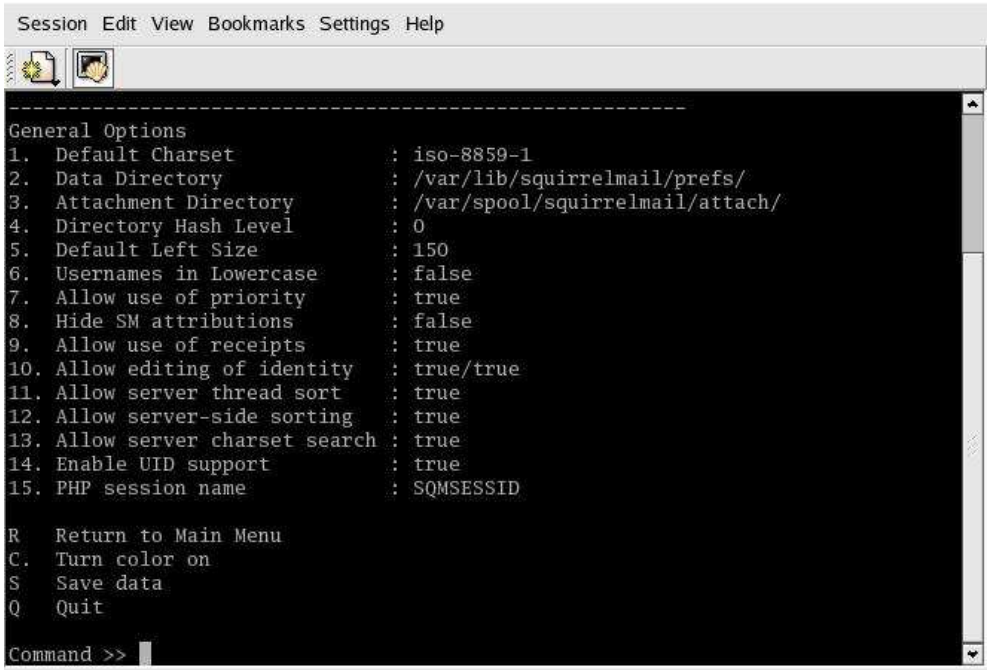

GRAFICO # 70. CONFIGRACIÓN DE EL WEB-MAIL. PASO 4

Themes. Temas; esta pantalla de configuración nos indicará cuales so los temas a los que el usuario tendrá acceso para la personalización de su correo, entre estas estarán : colores para las pantallas de su interfaz, marcado de correo entrante, saliente, leído etc.

No se recomienda realizar ningún cambio pues el usuario podrá tener la libertad de personalizar su interfaz de acceso de acuerdo a su gusto de personalización; por lo que logrará tener un máximo de aceptación por parte del mismo, al darle la posibilidad de personalizar su correo.

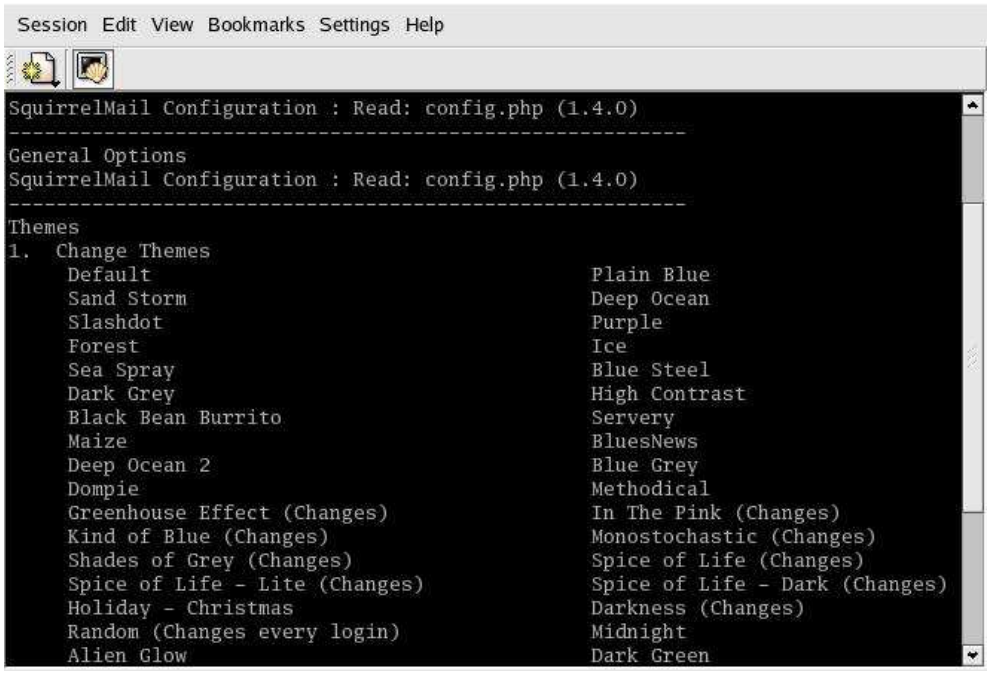

GRAFICO # 71. CONFIGURACIÓN DE EL WEB-MAIL. PASO 5

Pantallas Predeterminas par el uso de squirrelmail. En las siguientes pantallas no es aconsejable realizar ningún tipo de configuración pues todos los datos preexistentes por defecto serán utilizados por los binarios de squirrelmail para una mejor servicio del usuario.

Addres Books

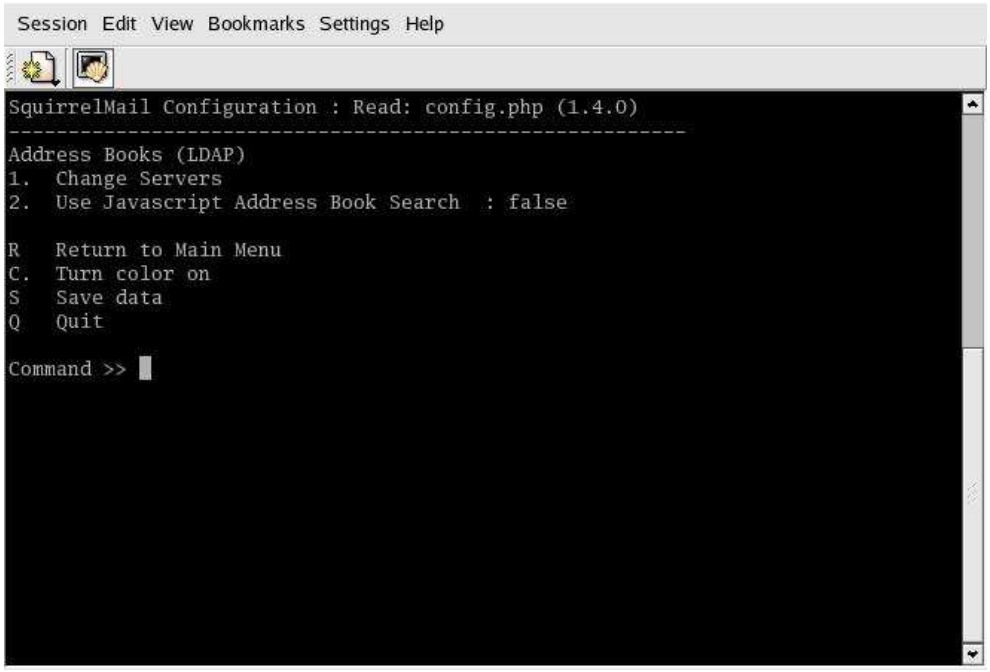

GRAFICO # 72. CONFIGURACIÓN DE EL WEB-MAIL. PASO 6

Message of the Day

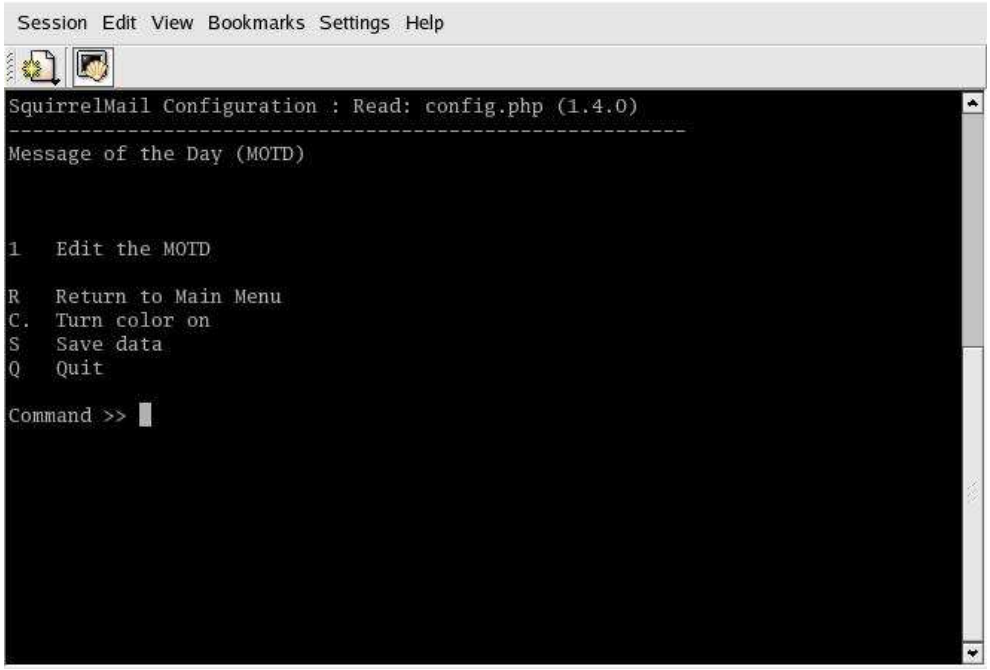

GRAFICO # 73. CONFIGURACIÓN DE EL WEB-MAIL. PASO 7

Plugins. Software adicional; squirrelmail posee una característica importante a nivel de web-mail; la particularidad de permitir la incorporación de software adicional para una mejor administración por parte del usuario al correo existente o simplemente para una mejor calidad de interfaz.

Para poder implementar un software de firma digital desde esta interfaz, haremos uso de esta particularidad. Esto nos permitirá ejecutar todas las tareas

de firma digital y disfrutar de su seguridad desde una interfaz gráfica y de fácil utilización por parte del usuario. Es importante considerar el uso de GNUGPG como software para la firma digital, así como del plugin respectivo para squirrelmail.

Para un funcionamiento adecuando, se deberá realizar las respectivas modificaciones en el software para este efecto. Todas las modificaciones se las realizará en función a las necesidades de la institución y bajo las normas de software libre. Por una necesidad adicional de seguridad para los servidores de correo electrónico de la Comandancia General del Ejercito se ha considerado toda esta planificación y desarrollo del software de firma digital para squirrelmail para satisfacer los requerimientos institucionales.

Para poder incluir el mencionado software, bastará con compilar el mismo en el directorio /usr/share/squirrelmail/config/plugins/ lo que permitirá que ya sea reconocido por el ./conf.pl de squirrelmail y nos permita su respectiva configuración simplemente con activarlo al escoger su opción de plugin que se presentará en al pantalla respectiva, como se mostrará en la figura.

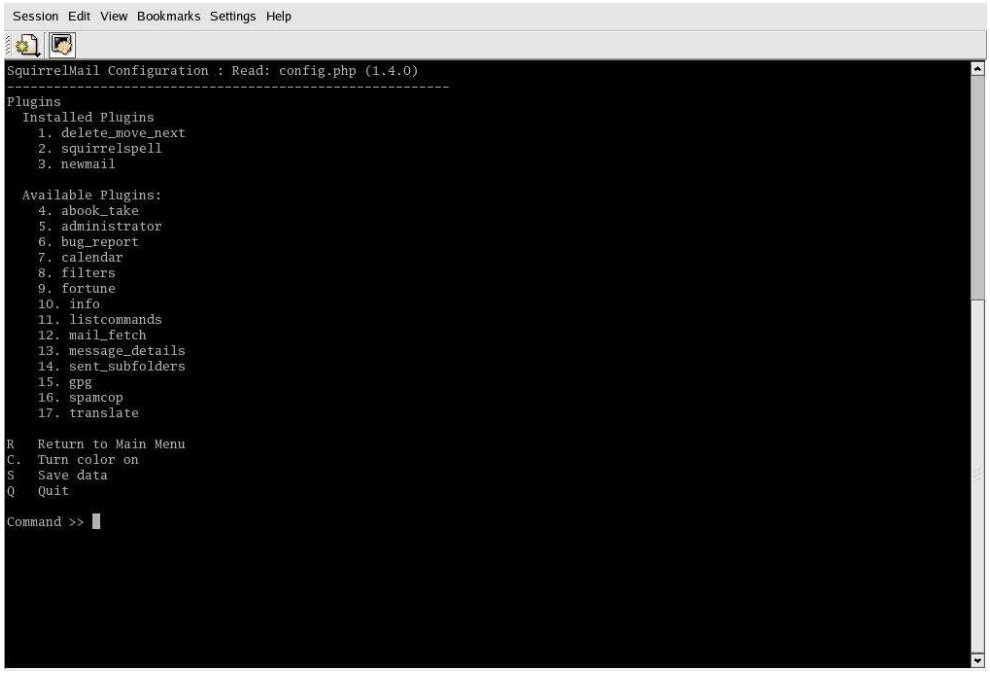

GRAFICO # 74. CONFIGURACIÓN DE EL WEB-MAIL. PASO 8

Al termino de todas estas configuraciones tendremos un servidor de correo electrónico con interfaz web-mail y con la funcionalidad de poder utilizar un software de firma digital para el mismo.

Para realizar su uso bastara con apuntar un browser de Internet a la dirección https://www.ejercito.mil.ec/correo o desde su respectivo enlace de al página principal que se realizo par el efecto.

Es necesario recalcar que se deberá reiniciar el servicio httpd como se mencionó en citados anteriores, para poder utilizar nuestro servidor de correo electrónico con todas las utilidades que se aplicó al mismo.

4.6. DESARROLLO DE LA APLICACIÓN PARA ENCRIPTACION Y FIRMA DIGITAL COMPATIBLE CON SQUIRRELMAIL.

4.6.1 Selección del método de desarrollo de software.

Antes de poder elegir un método de desarrollo de software, es necesario recopilar toda la información pertinente a las necesidades del usuario, las opciones administrativas del servidor en el cual estará corriendo la aplicación así como la compatibilidad con varios programas utilizados ya en la configuración del servidor de correo electrónico.

Uno de los puntos mas relevantes a considerarse antes de elegir el método de desarrollo de software será el conocer de la existencia de un plugin para encriptación y firma digital compatible con Squirrelmail.

Nuestra aplicación partirá de este plugin ya existente, el mismo que será adecuado en función a las necesidades de los usuarios de correo electrónico de la Fuerza Terrestre de la cual se recopilo la información inicial.

Squirrelmail proporciona el código fuente y los binarios del software para encriptación y firma digital con las características y necesidades de dependencias que son compatibles para la utilización en nuestra propuesta de seguridades que fueron mencionadas en el capitulo anterior.

A partir de lo mencionado se puede establecer, que el método más idóneo para nuestro desarrollo es, Creación de Prototipos de Software Mediante la Utilización de Componentes de Software Reutilizables

4.6.2 Creación de Prototipos de Software.

Un paradigma de construcción de prototipos, comienza con la recolección de requisitos. El desarrollador y el cliente encuentran y definen los objetivos globales para el software, identifican los requisitos conocidos y las áreas del esquema en donde es obligatoria mas definición [33].

Un enfoque para crear prototipos rápidos es ensamblar, mas que construir, el prototipo mediante la utilización de componentes de software existentes [34].

[33] Fuente: Ingeniería de Software un Enfoque Práctico, McGRAW-HILL, Interamericana de España 2001
[34] Fuente: Ingeniería de Software un Enfoque Práctico, McGRAW-HILL, Interamericana de España 2001

4.6.2.1 Definición de los objetivos globales del software.

Desarrollar un software, para incrementar la seguridad en el tráfico de mensajes en el sistema de correo electrónico y autentificar la firma digital.

4.6.2.2 Definición de los requisitos del software.

El software desarrollado deberá ser compatible con Squirrelmail 2.4 por su fiabilidad y alta seguridad en el manejo de correo electrónico desde una interfaz web.

Este software deberá trabajar con GNUPG o GPG para garantizar la encriptación y la firma digital, por considerarse este paquete el ideal para firma digital.

Deberá permitir al usuario manipular las respectivas contraseñas o claves mediante su interfaz de correo electrónico, permitiendo el acceso al servidor de claves, únicamente para la utilización de los servicios que preste el mismo, mas no para administración o manipulación deliberada del servidor de claves desde la Internet.

Su interfaz de acceso para el usuario deberá ser intuitiva de fácil uso y configuración de ser necesario.

Deberá mantener los estándares de Software Libre, ya que la presente propuesta está considerada con la utilización única y exclusivamente de software libre.

4.6.2.3 Selección de componentes.

Al establecer una línea de utilización de software libre, en todas y cada una de las configuraciones propuestas anteriormente; y al ser un factor importante el web-mail utilizado “Squirrelmail”. Se consideró que nuestra plataforma inicial será este web-mail, de allí se estableció la elección de todos los componentes que se utilizaron en esta etapa de la investigación y desarrollo.

Interfaz desde la cual se accederá al software de firma digital y al correo electrónico.

Squirrelmail 1.4.2-3..noarch

Software inicial de desarrollo de la aplicación.

gpg-2.0.1

Software para firma digital, encriptación.

gnupg.1.2.3

4.6.2.4 Análisis de los componentes.

GNUPG .1.2.3 software para firma digital y encriptación.

Gnupg es la herramienta para la comunicación segura y almacenamiento de los datos. Puede ser utilizada para la encriptación de datos para crear firmas digitales.

Gnupg utiliza algoritmos predefinidos DSA y El Gamal, pero también soporta los algoritmos RSA

El Gamal esta disponible para ser utilizado en firma digital; debido a su gran fiabilidad y tamaño; sin embargo se requerirá de un mayor capacidad de procesamiento para utilizar este algoritmo.

También presenta una utilidad con algoritmos simétricos como, AES, 3DES, Blowfish, CAST5 y Twofish. Además presenta a disposición otros como MD5, RIPEMD160 y SHA1; que serán de gran utilidad al momento de la utilización de GnuPG.

GPG-2.0.1 plugin para firma digital de squirrelmail.

La versión que se utilizará, a partir de la cual se procederá a construir otro prototipo es gpg-2.0.1, a la misma a la que se puede acceder desde la

pagina

http://www.squirrelmail.org/plugin_download.php?id=153&rev=988

desde la cual se pueden acceder a los binarios y las fuentes del mismo.

4.6.2.5 Adaptación de los componentes necesarios para la aplicación.

En esta parte del proceso de desarrollo de software, se procedió a adaptar el componente principal del prototipo de firma digital. Para poder realizar esta tarea es importante conocer el funcionamiento en conjunto de todos los componentes.

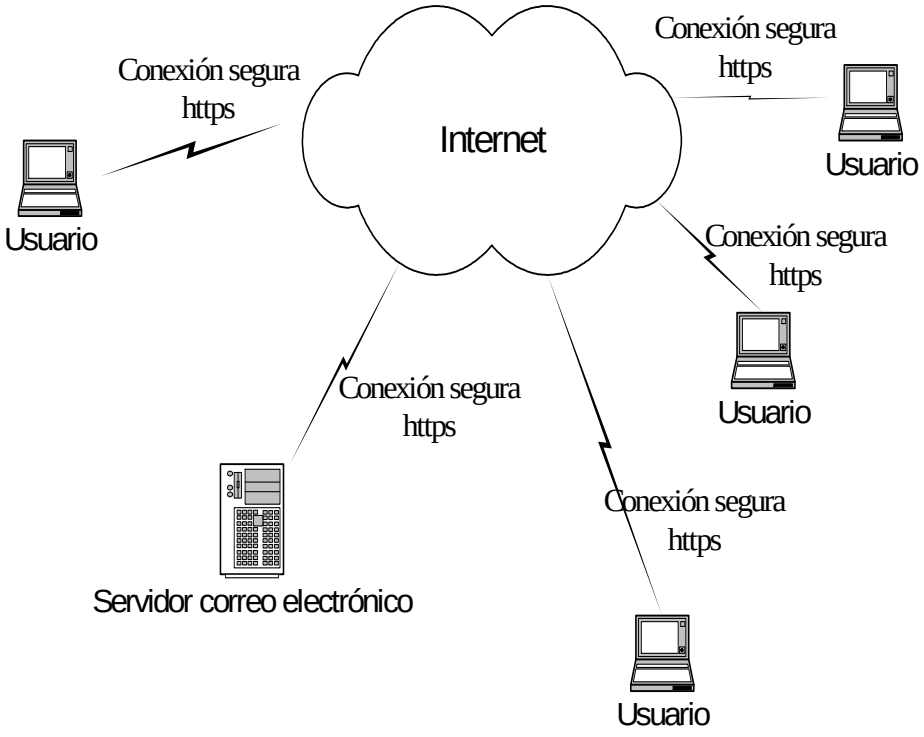

GRAFICO # 75. MODELO DE ACCESO AL SERVIDOR

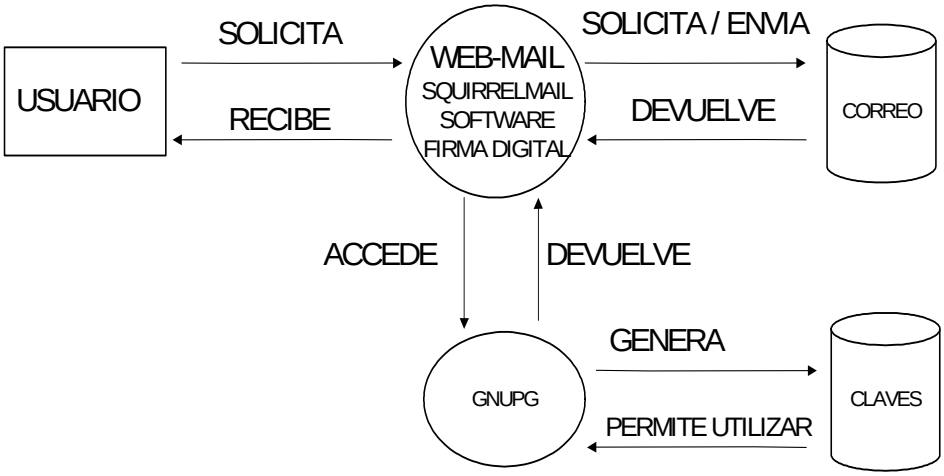

GRAFICO # 76. DIAGRAMA FLUJO DE DATOS

Como se pude observar en el anterior diagrama nuestra adaptación del componente, es enfocado directamente al software de acceso a GNUPG, que se encuentra funcionando desde el web-mail.

Al estudiar el funcionamiento del componente inicial, se concluyó que la principal falla de seguridad que presenta, el plugin para firma digital original; es la de presentar un acceso indiscriminado al servidor de claves, solicitando que este sea un servidor publico de los mencionados archivos, con los pertinentes peligros que se estudiaron anteriormente.

En la siguiente figura se puede observar la mencionada pantalla, la misma que fue eliminada para el funcionamiento adecuado de nuestro prototipo .

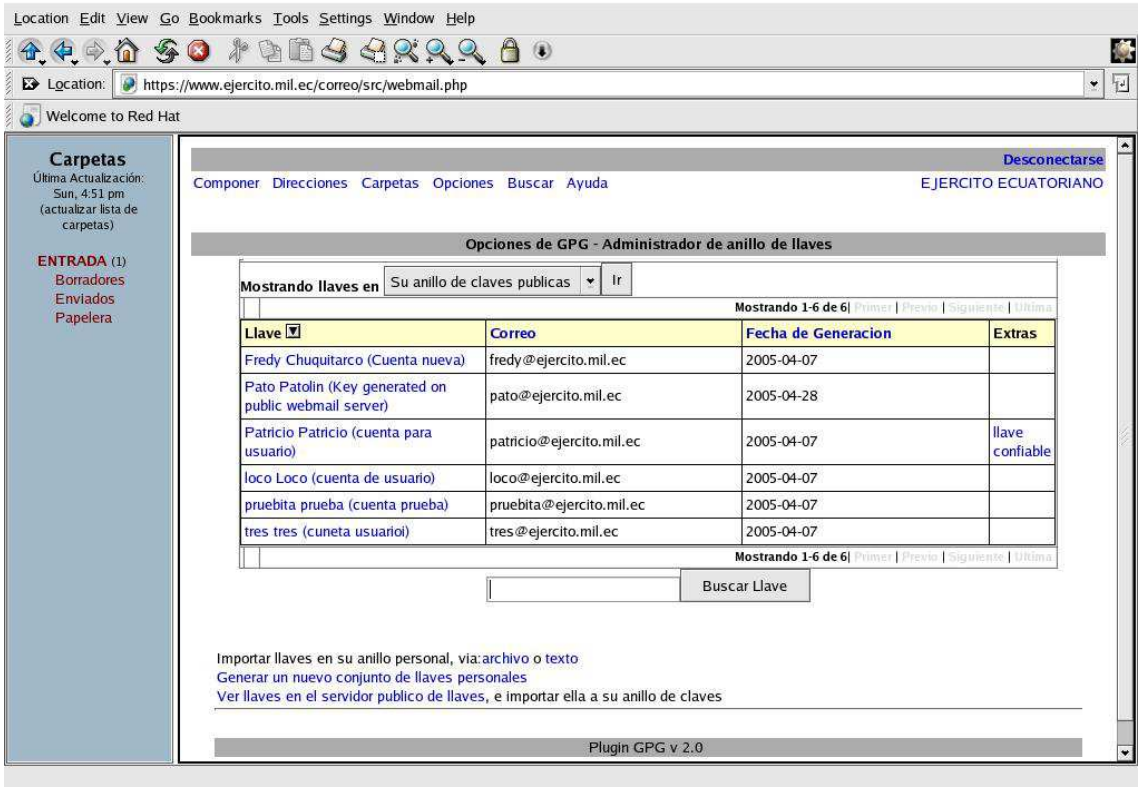

GRAFICO # 77. PANTALLA INCIAL DE ACCESO AL SERVIDOR DE CLAVES

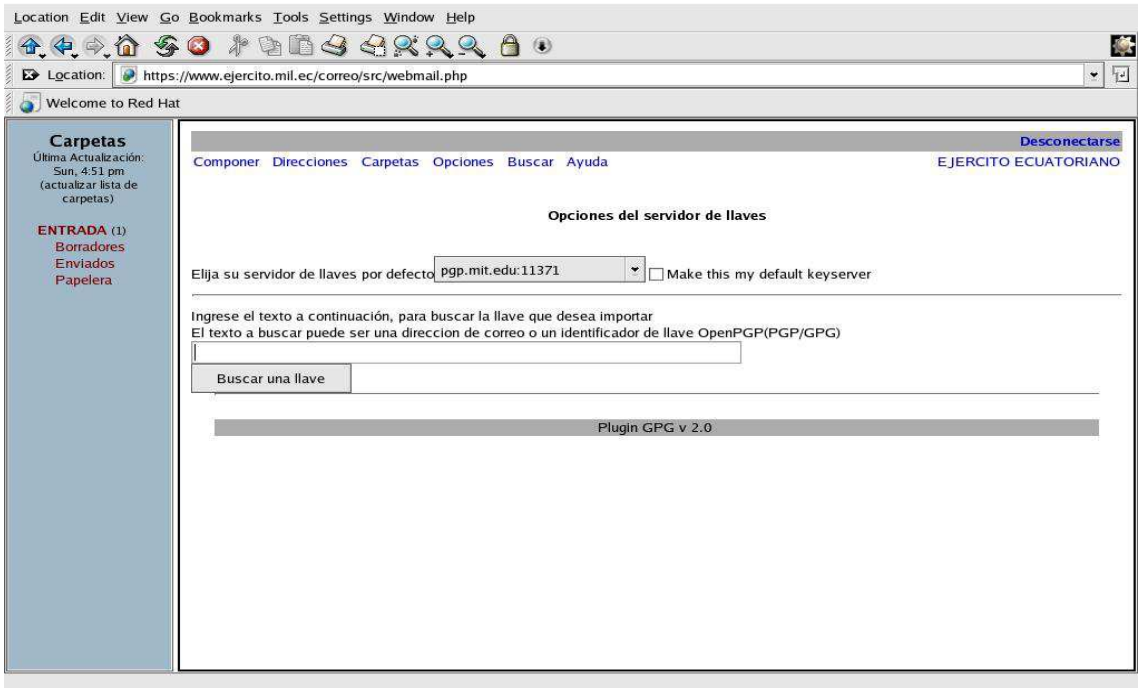

GRAFICO # 78. PANTALLA DE BUSQUEDA DE CLAVES EN EL SERVIDOR

Al mantener estas dos interfaces, muchos usuarios tendrían acceso a claves que no les corresponden, pues el servidor de claves se encontraría desprotegido.

Constituye esta variación al software inicial un aporte de seguridad por parte de los autores, en consideración a los requerimientos de la Comandancia General del Ejercito.

4.6.2.6 Integración de los componentes.

Una vez concluida la construcción de la aplicación se procederá a su integración. Para lo cual se deberá compilar los binarios en el directorio /usr/share/squirrelmail/plugins; con la finalidad que squirrelmail pueda reconocerlo como un plugin instalado y que permita al archivo de configuración de squirrelmail subir el plugin para su utilización

Al mantener en el directorio plugin de squirrelmail nuestra aplicación, el archivo de configuración conf.pl podrá instalarlo fácilmente, bastará con activar el servicio.

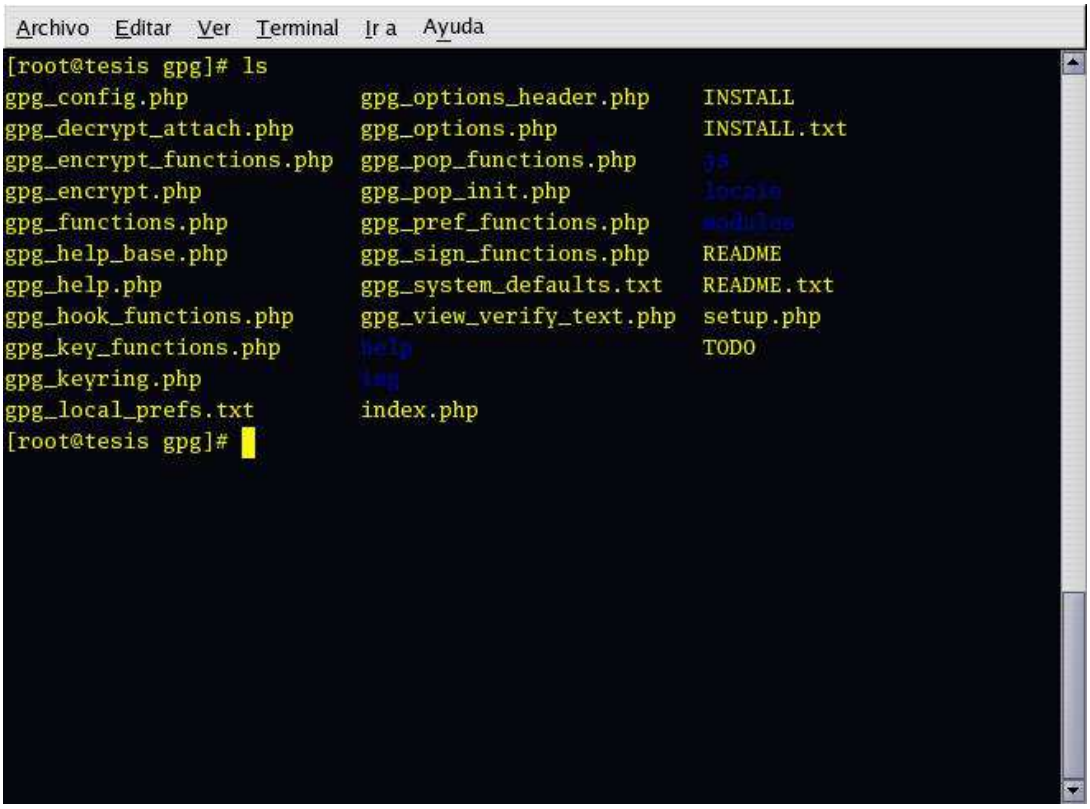

GRAFICO # 79. IINSTEGRACION DE LOS COMPONENTES

Para poder realizar esto, es necesario ejecutar la instrucción

/usr/share/squirrelmail/conf/conf.pl y se levantará la pantalla principal de configuración de squirrelmail, de la misma se escogerá la opción 8 y se instalará el plugin señalando el número por defecto.

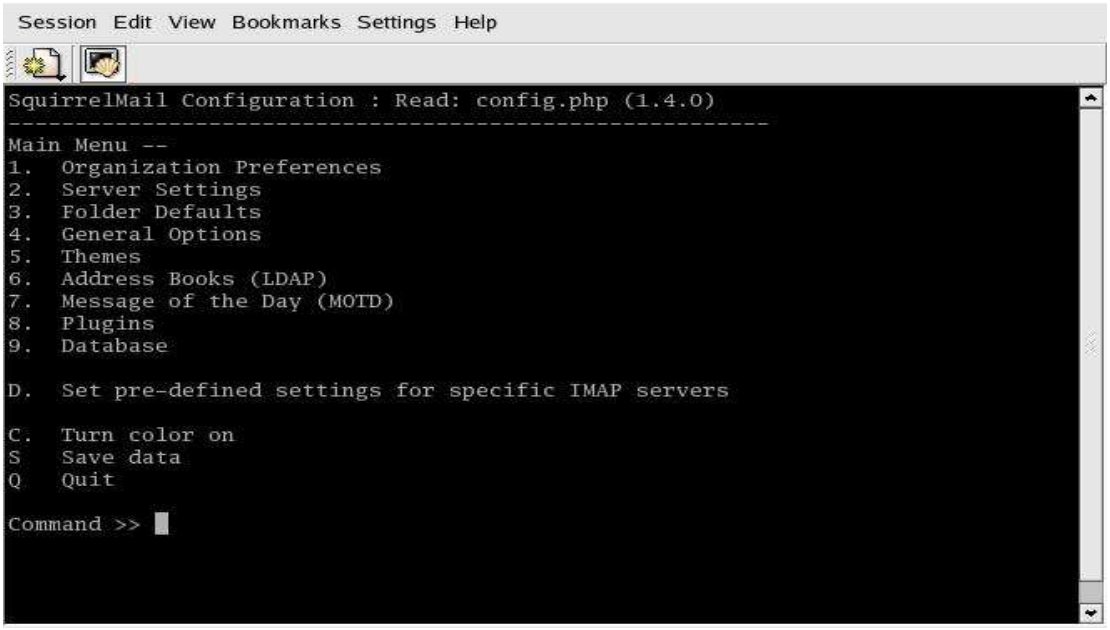

GRAFICO # 80. CONFIGURACIÓN DE EL SOFTWARE DE FIRMA DIGITAL EN ELWEB-MAIL

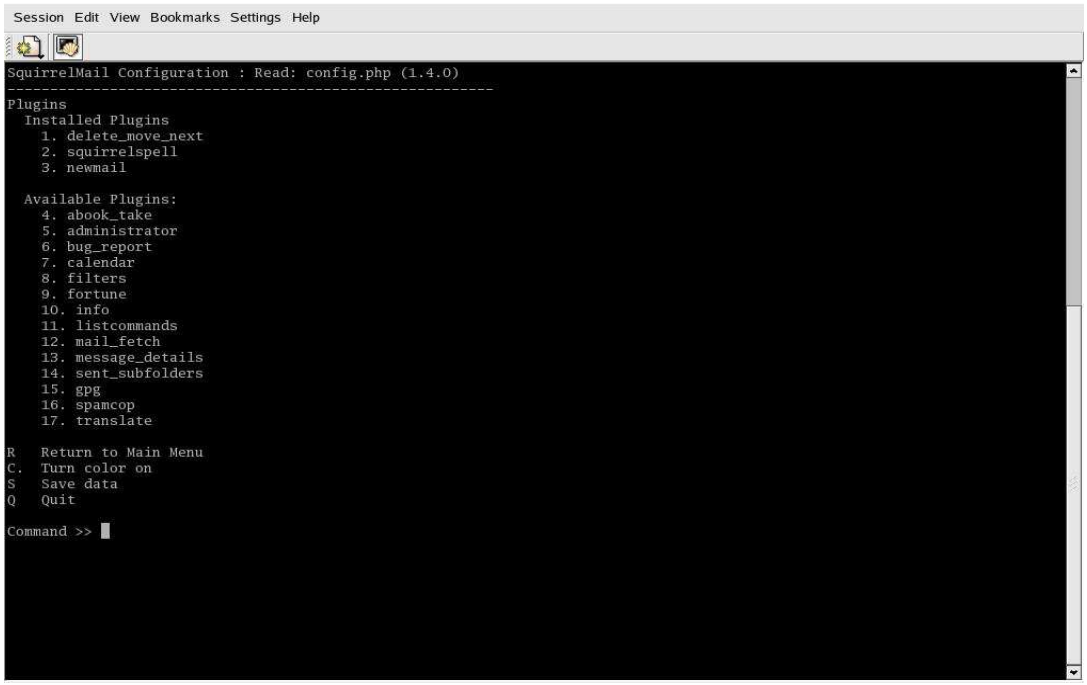

GRAFICO # 81. CONFIGURACIÓN DE EL SOFTWARE DE FIRMA DIGITAL EN ELWEB-MAIL

No será necesario ninguna configuración adicional en el plugin ya que este fue creado a partir de un modelo ya existente, con la finalidad de garantizar su funcionamiento con los nuevos requisitos, para los cuales fue creado.

Para poder utilizar nuestra aplicación es decir un servidor de correo electrónico con firma digital bastará con reiniciar los servicios como se menciono en el capitulo anterior y utilizar nuestro navegador predilecto apuntando a la dirección http://www.ejericito.mil.ec y luego al link https://www.ejercio.mil.ec/correo.

Todo el software compilado y los fuentes respectivos se encuentran en el cd anexo # 3.