CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 VERIFICACION DE OBJETIVOS

- Para poder desarrollar una propuesta confiable de seguridades, enmarcada en las necesidades de la Comandancia General del Ejército y en las tendencias actuales de seguridad; un punto importante para desarrollar nuestra investigación, fue el diagnostico inicial de la operatividad de los servidores tanto de correo electrónico como servidor web. Mediante este diagnostico se determinó que tipo de funciones y servicios presta cada uno de los servidores; así como, la plataforma en la que estos están configurados, y cada uno de los paquetes utilizados para la configuración de los mismos, su distribución y funcionamiento.

  Con este diagnostico inicial se pudo determinar, fallas de seguridad en la plataforma utilizada Red Hat Linux 7.2 y en los paquetes que se encuentran instalados; al precisar su distribución y su última actualización se puede conocer sus fallas de seguridad dadas en esas versiones de software.

- Partiendo de un análisis de operatividad de los servidores, y los requerimientos actuales de la Comandancia General del Ejercito; se consideró primordial la utilización de un protocolo de transporte de datos en la Internet que garantice integridad, confidencialidad y autenticidad en los datos siendo este uno de los principales

requerimientos de la institución, conjuntamente con la utilización de firma digital para el correo electrónico en la Comandancia General del ejercito.

Este requerimiento de seguridad se pudo cumplir al implementa el protocolo SSL para el transporte de datos en la red y la utilización de un software de firma digital en el correo electrónico, el mismo que se desarrollo en función de los requerimientos de la institución para la cual se desarrollo la propuesta. Con esto se cumplió con el objetivo principal de esta investigación, proporcionando un protocolo seguro de transporte de datos en la Internet, un software para firma digital y cada una de las consideraciones de seguridad que se las realizó para lograr concluir con satisfacción los objetivos propuestos.

5.2 CONCLUSIONES

- Una de las principales fallas de seguridad es la falta de actualización del software utilizado en los servidores, partiendo desde la versión del sistema operativo y cada uno de los paquetes que se utilizaron en la configuración de los mismos.

- La correcta elección del método de desarrollo de software, garantiza el desarrollo del mismo en todas sus etapas, en nuestro caso al utilizar el método de construcción de prototipos utilizando componentes de software reutilizables, permitió que la aplicación cumpla con los estándares de software libre así como también con las necesidades de la Comandancia General del Ejercito. Al iniciar el desarrollo del prototipo, tomando como componente inicial un software que fue creado por la comunidad de software

libre, el mismo que fue creado para garantizar la firma digital utilizando gnupg como recurso principal para encriptar y firmar el correo electrónico; garantiza el funcionamiento adecuado del prototipo en función de las necesidades de la institución en mención .

- Al implementar en el servidor el protocolo SSL, mediante la utilización de mod_ssl para apache se garantiza la transmisión de los datos en la red, todo esto pudo ser comprobado al visualizar el protocolo de transporte utilizado https mediante el puerto 443, así como al visualizar el correspondiente certificado digital que fue requerido para esta institución y proporcionado como demo por la empresa Verising; con el mismo que se realizó la configuración del servidor.

- Se comprobó la solidez de la encriptación, la generación y transmisión de claves y la fiabilidad de la utilización de la firma digital al utilizar Gnupg o GPG como base para la generación de claves, encriptación y firma digital; ya que el software de firma digital requiere de una conexión segura para realizar las tareas para las que fue creado, así la aplicación comprueba el funcionamiento del servidor web SSL y el servidor comprobará y garantizará la tareas del prototipo para firma digital y la generación de claves con gnupg.

- En la actualidad la creciente demanda de software libre en el Ecuador y en el mundo, han hecho que todos los paquetes utilizados para la configuración de los servidores que fueron objeto de nuestro estudio, día a día evolucionen, logrando de esta manera

mantener un software de calidad con distribuciones gratuitas, con toda la documentación necesaria para poder utilizarlos y en el caso de ser requerida los códigos fuentes para ser modificados en función de nuestra necesidad. Esto, conjuntamente con la posibilidad, que de existir alguna falla de seguridad en los paquetes, la comunidad de software libre en el mundo respaldará la solución del problema generado o descubierto, además de su comprobada robustez y seguridad ; hicieron que se utilice como plataforma y software para configuración de servidores software libre.

5.3 COMPROBACION DE LA HIPÓTESIS

Con la terminación de este proyecto, se pudo comprobar la hipótesis planteada al inicio de la investigación. Nuestra propuesta de seguridades cumple con todas y cada una de las necesidades de seguridad requeridas e investigadas para los servidores de paginas web y correo electrónico de la Comandancia General del Ejercito. Con la demostración del funcionamiento del software para firma digital, la implementación del protocolo seguro SSL con un certificado digital proporcionado por Verising y la configuración de muchos parámetros de seguridad para los servidores, en cada una de sus etapas de configuración e instalación, se pudo demostrar y comprobar la confidencialidad, integridad y disponibilidad de la información en un sistema seguro, al utilizar los parámetros y consideraciones que se proponen en este documento, mediante una demostración de todo esto en una aplicación y demostración práctica con todo lo mencionado.

5.4 RECOMENDACIONES

- Es importante recomendar, a las personas que utilicen esta investigación como base para poner en funcionamiento esta propuesta, que se realicen las configuraciones y comprobaciones de los servidores en función de los parámetros que se consideran en este documento; ya que las mismas fueron elaboradas, comprobadas y documentadas, a partir de un estudio y verificación de cada una de ellas.

- Se recomienda tomar en consideración, el estudio propuesto para seguridades no solo en la configuración de servidores, sino también el propuesto para la generación de claves, identificación y restricción de las personas que tendrán acceso al área en donde se encuentren ubicado los servidores.

- Cuando se inicie la configuración de los servidores, se recomienda realizarlas en el orden considerado en esta investigación, ya que de esta manera se podrá mantener una secuencia en función de necesidades de funcionamiento de una u otra aplicación.

- Se recomienda, antes de realizar la instalación del software de firma digital, comprobar el adecuado funcionamiento de todos los servidores; será imprescindible realizar pruebas iniciales de el web mail, con al finalidad de poder establecer un punto de comprobación del funcionamiento de los mismos, todo esto hará que se más fácil la instalación y verificación de la firma digital.

- Las personas encargadas de realizar las instalaciones y configuraciones de los servidores, deberán poseer conocimientos sólidos de Linux así como de el funcionamiento y protocolos de DNS, CORREO ELECTRÓNICO, SSL, FIRMA DIGITAL, HTTP, HTTPS, POP3, IMAP.

- Las personas que se encargarán de la administración de los servidores, deberán conocer el funcionamiento de los mismos así como también deberán poseer conocimientos sólidos en la administración de sistemas Linux.

- Se recomienda que antes de realizar la instalación de los paquetes, se revise la distribución de los mismos en sus respectivas paginas web con la finalidad de mantenerse al día con las actualizaciones, evitando de esta manera posibles fallas de seguridad que se hayan descubierto en versiones anteriores.