CAPITULO VII

7. CONCLUSIONES Y RECOMENDACIONES

7.1 VERIFICACION DE LA HIPOTESIS

Una vez terminada la investigación, se establece que la hipótesis planteada para el desarrollo de la Tesis "Metodología para el desarrollo de firewalls de software mediante Java. Aplicación: implementación de un prototipo para la UTN" se ha cumplido, ya que se ha logrado implementar un prototipo de firewall de software tipo Proxy GET HTTP, utilizando el lenguaje de programación Java.

Además se ha podido demostrar que la implementación de una Política de Seguridad Informática es el primer paso a realizarse antes de implementar cualquier tipo de seguridad en una red, ya que en esta se describen las posibles amenazas y soluciones a problemas de seguridad.

Se ha logrado dar acceso seguro a Internet a los usuarios de la red local, ya que se ha configurado un Servidor de Acceso a Internet con un sistema operativo estable como es Linux RedHat 7.1, el cual presenta opciones de seguridad para configurar los diferentes servicios que se brindan, convirtiéndose de esta forma en un complemento a la Política de Seguridad y al prototipo de firewall implementado.

Finalmente se puede decir que la seguridad de acceso a Internet de la Universidad Técnica del Norte se ha establecido de manera correcta, pero siempre deben haber actualizaciones para que la seguridad sea óptima y este acorde con los avances tecnológicos.

7.2 CONCLUSIONES

- La Universidad Técnica del Norte posee un servicio de Internet muy lento ya que posee un solo servidor el cual se satura con rapidez debido a que son muchas las máquinas que conforman de la red y la conexión es de 128 bps existiendo de esta manera horas pico en las cuales no se puede tener acceso a este servicio.

- La seguridad es un aspecto que nunca debe descuidarse dentro de la Universidad Técnica y al contrario siempre debe mejorarse para que la institución esté protegida de posibles daños que los usuarios externos pueden causarle porque pueden generar muchas pérdidas económicas ya sean hardware dañado, información importante pérdida, etc.

- Los servicios que se ofrecen a través de Internet traen muchos beneficios a los usuarios, pero estos debe ser configurados correctamente y con las medidas de seguridad apropiadas para que no se conviertan en agujeros de seguridad con lo cual la Universidad quedará indefensa ante posibles ataques de personas indebidas.

- La colaboración de los usuarios internos que pertenecen a la Universidad Técnica del Norte, es un apoyo fundamental para garantizar la seguridad de la red interna ya que si los usuarios no colaboran existirá un rechazo a la seguridad y por ende no funcionará generando gastos para la Universidad.

- El acceso físico a los recursos de red, debe limitarse únicamente al personal que necesita acceder a los mismos, limitándolos a utilizarlos únicamente en horas de trabajo y que cuenten con la vigilancia respectiva de la persona encargada

responsabilizando a cada usuario de la máquina de la Universidad que este a cargo.

- La Universidad Técnica del Norte deberá instalar un firewall ya que estos ayudan a una red a estar protegida, por lo tanto la universidad deben instalar componentes de este tipo, para así lograr la seguridad que sus facultades necesitan el momento que deciden conectarse a Internet teniendo de está manera una completa seguridad.

- Los firewalls de software y de hardware, tienen sus beneficios y limitaciones, por lo cual antes de instalar cualquier tipo de firewall, es necesario realizar un estudio previo para poder saber lo que realmente se necesita, para de esta manera poder realizar la mejor inversión evitando el desperdicio de tiempo, dinero , etc.; Lo cual genera pérdidas para la Universidad.

- Dentro de la Universidad se deberá mantener una actualización y mantenimiento del firewall de manera continuo, nunca se debe dejar pasar mucho tiempo antes de adquirir un nueva versión, pues siempre se encontrarán mejoras en los nuevos productos y por lo tanto mayores condiciones de seguridad para la red institucional.

- La Universidad Técnica del Norte no deberá escatimar recursos, cuando de seguridad se trata, ya que los problemas en los cuales puede verse involucrada son muy grandes cuando existe pérdida de información importante y confidencial que puede encontrarse en los equipos, con lo cual el gasto será mayor que el costo de instalar un firewall o configurar servicios de manera apropiada.

- Para elaborar una Política de Seguridad Informática se debe tener en cuenta lo siguiente:

- Que recursos se desea proteger
- De quienes se desea proteger
- Como se va ha proteger

Teniendo en cuenta que los recursos que se van ha proteger no sólo son los recursos de hardware o de software sino que también se debe tomar en cuenta todas las infraestructuras de la organización.

- La Política de Seguridad Informática es un documento que describe la seguridad de la organización, esta debe ser clara, concisa y directa indicando las posibles amenazas para tratar de proteger los recursos y de esta manera salvaguardar la inversión de la organización.

- No se puede pensar en implementar un firewall primero si no tenemos implementada una buena Política de Seguridad Informática ya que por más bueno que sea el firewall no podrá proteger de los problemas que puedan suceder fuera de la red, se debe tener en cuenta que los problemas no solo suceden dentro de la red sino que también pueden ser problemas dentro de la organización.

- Una buena Política de Seguridad Informática debe estar escrita en un lenguaje común fácil de entender, los términos deben ser lo más simples capaces de ayudar a entender la política, sin tecnicismos y términos legales que impidan su comprensión, siendo más fácil su implementación.

- La Política de Seguridad Informática no puede especificar con exactitud todo aquello que puede pasar dentro de la red organizacional ya que existen muchos problemas que pueden ir suscitándose en el desarrollo diario de la organización,

teniendo en cuenta que dichos problemas y por esto ser catalogada como inservible.

- Para que una Política de Seguridad Informática pueda ser implementada debe ser entendida por todos los usuarios, para que estos no tengan resistencia al cambio y se adapten a dichos cambios que se especifican dentro de la Política de Seguridad Informática, teniendo en cuenta que dicha política no obligará a los usuarios a realizar cosas que vayan en perjuicio del mismo.

- Toda Política de Seguridad Informática debe poseer un plan de acción a ser seguido en caso de ser violada, determinando porque se realizo dicha violación y tomando las respectivas acciones para que esto no vuelva a suceder, lo cual permitirá que la organización modifique la política y de esta manera se irá alimentándose de las experiencias que sucedan dentro de la red.

- Para elegir un firewall de hardware para la organización se debe tener en cuenta todos los factores que influyen en la toma de decisión ya sean :

    - Económicos
    - Limitaciones de hardware
    - Documentación e información del firewall

  Todos estos factores nos pueden ayudar de una manera efectiva a la hora de escoger un firewall para la organización tratando en lo más posible que se cumplan.

- Un firewall por más bueno que sea no sirve de nada si no hay una persona que sepa administrarlo y solucionar los problemas más básicos que puedan suscitarse ya que si el

firewall tiene problemas y no exista quien los soluciones se tendrá que suspenderlo momentáneamente y con esto la red quedará indefensa ante los posibles ataques de personas que no pertenezcan a la organización.

- Se debe tener en cuenta que un firewall de hardware no puede realizar todas las acciones de protección de la red, este sólo solucionará los problemas que puedan suscitarse dentro del flujo de datos de la red; hay que tener en cuenta que existen muchas amenazas que no están inmersas en la red y que pueden afectarla directamente ya sean como daños físicos, perdidas de hardware, etc.

- El lenguaje de programación Java es fácil de instalar, no necesita muchos requerimientos de hardware e incluye APIs y paquetes de clases que permite a los programadores desarrollar aplicaciones estables y de fácil administración, las mismas que pueden permanentemente ser mejoradas ya que el JDK está constantemente en desarrollo y cada versión incluye funcionalidades adicionales, con las cuales se logra la implementación de software adecuado.

- El desarrollo de programas de red en la Universidad es importante ya que se podrá mantener un control de la aplicación pudiendo mejorarla de acuerdo con las necesidad que se vayan sucitandose, lo cual permitirá con el tiempo generar aplicaciones de red buenas y fáciles de administrar, las cuales tendrán la ventaja de que no implican ningún costo y pueden irse actualizando de acuerdo a las necesidades reales de la institución .

- El prototipo de firewall de software UTN proxy al ejecutarse no consume muchos recursos de hardware ya que está desarrollado en un lenguaje de programación que al ser

compilado genera un código intermedio conocido como bytecode el mismo que optimiza el rendimiento de la aplicación y a la vez permite la ejecución de la misma en varias plataformas sin necesidad de realizar muchas modificaciones al código fuente.

- Una herramienta de seguridad, que controla el tráfico que fluye entre dos redes siempre debe generar archivos logs, los cuales guardarán información importante que puede ayudar a tomar decisiones sobre la seguridad de las redes implicadas y de esta manera se logrará un mayor control de la información y del uso que los usuarios dan a los recursos informáticos.

7.2 RECOMENDACIONES

- La Universidad Técnica del Norte debería realizar un estudio de los servicios brindados por diferentes ISP's, con la finalidad de poder escoger otras opciones y mejorar el servicio que se brinda a los usuarios. Lo más apropiado sería la adquisición de un enlace satelital, el mismo que sería más estable y a la vez permitiría mejorar el rendimiento de las conexiones de los usuarios de la red interna.

- En la Universidad Técnica del Norte se deben mejorar los controles de acceso físico a las áreas que contengan equipos activos importantes de la red de datos controlando que los usuarios que accedan sean los usuarios autentificados y con sus debidos permisos, estos controles se deberán aplicar también a los edificios ya sea con tarjetas de presentación para poder tener acceso a áreas que contengan recursos importantes.

- La Universidad debería invertir en la adquisición de nuevas tecnologías de comunicación en redes, para así mejorar los servicios que se brinda y de esta manera llegar a ser una institución educativa con un mejor nivel académico y un mejor reconocimiento a nivel local y nacional, lo cual permitirá que nuevos estudiantes se interesen en ingresar a formar parte de la universidad para poder concluir sus estudios superiores.

- En la Universidad Técnica del Norte debe existir una persona encargada de la Administración del Servidor de Acceso a Internet con lo cual se facilitará el servicio mejorándolo y resolviendo problemas que pudieran suscitarse con lo cual la universidad quedaría sin este servicio.
- Se debería estudiar la posibilidad de que la Universidad Técnica del Norte se convierta en un ISP para conexiones

empresariales, de tal manera que la institución pueda comprar anchos de banda para luego venderlos a organizaciones que necesiten acceso a Internet.

- Establecer un gran caché local, que permita mejorar la velocidad de acceso a páginas visitadas anteriormente, para lo cual podría adquirir un RAID 5 de discos SCSI, a fin de anexarlo a filesystem de Linux logrando de esta manera que la mayoría de accesos de los clientes de la red interna sean locales y no exista la necesidad de conectarse permanentemente a Internet.

- Con el fin de mejorar la seguridad en un futuro la Universidad debe estudiar la posibilidad de adquirir un firewall de hardware, el cual brindará mayor seguridad para la red de la institución, impidiendo de esta manera que la seguridad sea sobrepasada por usuarios restringidos.

- Los archivos de log del servidor deben revisarse diariamente, para poder determinar todo lo que está sucediendo dentro de la red de la universidad y de esta manera tomar las respectivas medidas para solucionar los problemas que pueden presentarse, este archivo log nos permitirá descubrir quienes desean ingresar de manera indebida a la red y realizar daños dentro de ella.

- Las contraseñas de administración de los servidores de las facultades, únicamente deben ser conocidas por los responsables de la administración de los mismos, teniendo cuidado de que dichas contraseñas no caigan en manos de personas inescrupulosas las cuales no dudarán en hacer daño, estas contraseñas deben ser cambiadas periódicamente, no deben involucrar fechas fáciles de ser descubiertas y deben ser guardadas en un lugar seguro, el archivo que contenga las

contraseñas deberá encontrarse encriptado para poder impedir que sea leído.

- Permanentemente deben investigarse los avances en cuanto a seguridad de redes, para de esta manera estar siempre protegidos de los nuevos peligros que constantemente aparecen en Internet, ya que sino se realizan los debidos estudios de los avances tecnológicos las seguridades de la red quedarán obsoletas en poco tiempo y por lo tanto será mucho más fácil violarla, produciendo daños en los equipos de la universidad.

- Deben adquirirse más servidores para ejecutar los servicios separadamente y así lograr un mejor rendimiento, ya que en la actualidad sólo se cuenta con un servidor el cual tiende a saturarse y no brindar los servicios de manera adecuada, si se dispone de más servidores se dará un mejor servicio con lo cual se mejora la rapidez de la red de la universidad.

- Implementar nuevos protocolos al firewall desarrollado, para de esta manera tener un mejor control de los servicios que se brinda a los clientes, teniendo en cuenta que de está manera el firewall desarrollado se irá haciendo más seguro con lo cual brindará un mejor servicio.

- Dar a conocer a los usuarios las restricciones que existen en cuanto a los accesos que ellos pueden tener cuando se conectan a Internet, ya que de ese modo se podrá mantener un control de los sitios visitados e impedir que varía información inservible se encuentre en los equipos de la red saturándolos y haciendo que el tráfico de está sea mas lento .

- Revisar periódicamente el software instalado en los computadores, para así evitar el uso inapropiado de los

equipos, no se debe permitir que se instale software que no este permitido ya que con esto se puede generar problemas ya sea durante la instalación de dicho software o después cuando las computadoras se saturan, esto puede causar daños en el hardware.

- En caso de detectarse problemas de seguridad, tomar decisiones oportunas, caso contrario las cosas pueden complicarse y la institución podría involucrarse en conflictos con otras organizaciones, es por eso que la Universidad Técnica del Norte debe contar con una buena política de Seguridad Informática con lo cual se obtendrá soluciones rápidas y oportunas.

- Adquirir cintas magnéticas para realizar los respaldos del servidor a través de la red y no localmente como se hace ahora, estos respaldos deben guardarse en lugares seguros que cuenten con las respectivas normas ya que no se podrá aventurar y perder la información de los backups, debe existir por lo menos dos copias de la información importante guardados en sitios diferentes.

- Se debe tener en cuenta que a la hora de generar una Política de Seguridad Informática se debe considerar todos los recursos que pueden ser afectados de manera directa e indirectamente para poder protegerlos, sin dejar ningún detalle por más pequeño que sea, ya sea que de esta manera se ahorrara muchas pérdidas a la organización.

- Toda organización debe poseer un buen inventario de todos los recursos ya que este permitirá saber con precisión que tipo de recursos existen y como los vamos a proteger con la Política de Seguridad Informática, de la misma manera como existe el inventario de recursos se deberá tener un control de todos los

usuarios autentificados para poder clasificarlos y de esta manera poder asignar los debidos permisos.

- Antes de empezar en una Seguridad para la red de la organización se debe elaborar primero una buena Política de Seguridad Informática ya que con ella la organización se evitará varios problemas que no se toman en cuenta al realizar una seguridad de manera breve y con esto generar varios gastos que conllevan la mala estructuración de dicha seguridad generando varias pérdidas para la organización.

- Cuando se desee realizar una Política de Seguridad Informática no se debe pasar por alto todas las posibles amenazas por más pequeñas que sea y por más difíciles que se piense que puedan suceder, no se puede dejar de lado ninguna de las cosas para poder decir que la Política de Seguridad Informática no tendrá fallas, pero siempre se debe tener en cuenta que existirá cosas que por más evidentes que sean se las pasará por alto.

- Para que no exista resistencia en la implementación de la Política de Seguridad Informática se debe tomar en cuenta a todos y cada uno de los usuarios de la organización ya sea realizando cuestionarios referentes a la protección de los recursos del área donde desempeñan sus funciones, encuestas, foros, etc. De esta manera los usuarios podrán exponer todas sus ideas y que sepan que esas ideas van ha ser puestas en práctica.

- Siempre debe existir un plan de acción a ser efectuado si la Política de Seguridad Informática llega a ser violada, este plan debe estar escrito en el mismo lenguaje que se utilizó para desarrollar la política, este plan de acción debe existir aunque se piense que no se lo va hacer utilizado y que no pase que en el momento que se lo necesite recién ponerse a realizarlo.

- Para poder decidir que firewall compramos debe existir un buen sustento de información, ayuda técnica en el momento indicado; ya que si no disponemos de las ayudas indicadas como podremos solucionar los problemas que puedan suceder con el firewall. La ayuda técnica desempeña un papel importante porque sin está el firewall puede quedar sin uso hasta que se pueda solucionar el problema que tenga.

- Se debe tener una persona encargada del normal funcionamiento del firewall, por lo tanto esta persona debe ser capacitada periódicamente con cursos de actualización, manejo del firewall para poder solucionar futuros problemas que puedan suscitarse, es recomendable que esta persona tenga por lo menos dos personas que sepan del manejo del firewall ya que alguna vez el encargado no estará dentro de la organización ya sea por capacitación, calamidades, etc.

- Se debe concretizar a todos los usuarios sobre el buen funcionamiento de la red y todos sus partes así como también de los edificios, suministros, etc.; ya que del desarrollo de la organización depende el desarrollo de sus usuarios, por eso es que se debe realizar campañas para fomentar la idea de preservar los recursos que posea la organización.

- El lenguaje de programación Java debe ser tomado como referencia para el desarrollo de aplicaciones ya que es muy eficiente debido a que incluye muchas herramientas que permiten realizar programas óptimos por lo cual hoy en día es usado para el desarrollo de varias aplicaciones, tales como los conocidos Applets de Java.

- Se debe realizar mayor énfasis en el desarrollo de aplicaciones de red para la Universidad, ya que de ese modo se podrá obtener muchas ganancias y reconocimiento para la

institución, estos programas deberán ser en su totalidad generados bajo la vigilancia de personal de la universidad desde el inicio hasta el funcionamiento de los mismos.