UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

"EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ."

Tesis Presentada previa a la obtención del Título de Ingeniero en Informática y Sistemas Computacionales.

Autores:

Avalos Mera Iveth Yesenia

Vizcaíno Bautista Marcelo Javier

Directora

Ing. Verónica Zapata Yánez

La Maná – Ecuador

Agosto 2015

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LA MANÁ – ECUADOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de Miembros del Tribunal de Grado aprueban el presente Informe técnico de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Unidad Académica de Ciencias de la Ingeniería y Aplicadas; por cuanto, los postulantes:

- Avalos Mera Iveth Yesenia
- Vizcaíno Bautista Marcelo Javier

Con el título de tesis: **"EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ."**

PERIODO 2015 han considerado las recomendaciones emitidas oportunamente y reúnen los méritos suficientes para ser sometidos al acto de Defensa de Tesis. Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

.....	**.....**
MSc. Edison Aimacaña	**MSc. Carlos Chavez**
PRESIDENTE	**MIEMBRO**
.....	**.....**
MSc. Julio Oña	**Ing. Verónica Zapata**
OPOSITOR	**DIRECTORA**

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LA MANÁ – ECUADOR

AVAL DE AUTORÍA

Los criterios emitidos en el presente trabajo de investigación: **"EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ."** son de exclusiva responsabilidad de los autores.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo de investigación a la Universidad Técnica de Cotopaxi, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

…….	…….
Avalos Mera Iveth Yesenia	Vizcaíno Bautista Marcelo Javier

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LA MANÁ – ECUADOR

AVAL DEL DIRECTOR DE TESIS

En calidad de Directo de Trabajo de Investigación sobre el tema:

"EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ." De los señores estudiantes; Srta. Avalos Mera Iveth Yesenia con C.I.: 0503366544 y el Sr. Vizcaíno Bautista Marcelo Javier con C.I.: 050262354-9 postulante de la Carrera de Ingeniería en Sistemas

CERTIFICO QUE:

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes científicos - técnicos necesarios para ser sometidos a la **Evaluación del Tribunal de Validación de Tesis** que el Honorable Consejo Académico de la Unidad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe para su correspondiente estudio y calificación.

La Maná, 16 Junio del 2015.

……..

Ing. Verónica Zapata Yánez

DIRECTORA DE TESIS

CERTIFICACIÓN

El suscrito, Lcdo. Ringo John López Bustamante Mg.Sc. Coordinador Académico y Administrativo de la Universidad Técnica de Cotopaxi, extensión la Maná, Certifico que las Sres. Avalos Mera Iveth Yesenia y Vizcaíno Bautista Marcelo Javier portadores de la cédula de ciudadanía N° 050336654-4 y 050262354-9 respectivamente egresados de la Carrera de Ingeniería en Informática y Sistemas Computacionales, desarrollaron su tesis titulada "EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ", la misma que fue ejecutada e implementada con satisfacción en el Laboratorio de Redes, ubicado en el primer piso alto del Bloque Académico "A" de la Extensión La Maná

Particular que comunico para fines pertinentes

ATENTAMENTE

"POR LA VINCULACIÓN DE LA UNIVERSIDAD CON EL PUEBLO"

La Maná, junio 24 del 2015

Lcdo.Mg.Sc.Ringo López Bustamante
COORDINADOR DE LA EXTENSIÓN
Universidad Técnica de Cotopaxi- La Maná

RLB/ea

AGRADECIMIENTO

Un agradecimiento muy especial a Dios quien me dio la vida y por llenarme de bendiciones en todo este tiempo, a él que con su infinito amor me ha dado la fuerzas para terminar mi carrera Universitaria.

A mis padres, por todo el esfuerzo que hicieron para darme una profesión y hacer de mí una persona de bien, gracias por los sacrificios y la paciencia que demostraron todos estos años; gracias a ustedes he llegado a donde estoy.

A mi esposa e hijo que han sido el pilar fundamental para poder alcanzar esta meta. Que sin duda alguna en el trayecto de mi vida me han demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

Agradezco también la confianza y el apoyo brindado por parte de mi madre, ya que sin dudarlo ha estado apoyándome en las buenas y en las malas. A mi padre, que con sus consejos me ha ayudado a afrontar los retos que se me han presentado a lo largo de mi vida. Y sé que están orgullosos de la persona en la cual me he convertido.

A mis hermanas y sobrinas, quienes han sido amigas fieles y sinceras, en las que he podido confiar y apoyarme para seguir adelante. Gracias a todas aquellas personas que de una u otra forma me ayudaron en especial a ti mi abuelita me ayudaste a crecer como persona y ahora como profesional. Agradezco también de manera especial a nuestra tutora de tesis quién con sus conocimientos y apoyo supo guiar el desarrollo de la presente tesis desde el inicio hasta su culminación.

“Ahora puedo decir que todo lo que soy es gracias a todos ustedes”

Marcelo Javier Vizcaíno Bautista

AGRADECIMIENTO

Siendo la gratitud una virtud del hombre que sabe valorar las acciones educativas, presento mis más efusivos AGRADECIMIENTOS;

Este proyecto es el resultado del esfuerzo conjunto de todos los que formamos el grupo de trabajo.

A mis padres quienes a lo largo de toda mi vida han apoyado y motivado mi formación académica, creyeron en mí en todo momento y no dudaron de mis habilidades.

A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza me dieron el mejor regalo que un hijo debe recibir el estudio, ya que gracias a ellos obtendré el título de la vida.

Y finalmente un eterno agradecimiento a esta prestigiosa Universidad la cual abre sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien de manera especial a mí tutora Ing. Verónica Zapata Yanes que revisó permanentemente mi trabajo.

Avalos Mera Iveth Yesenia

DEDICATORIA

Este trabajo investigativo se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas presentados, enseñándome afrontar y superar todas las adversidades, sin que nunca baje la cabeza y cuide mi dignidad, gracias por permitirme llegar hasta este momento tan importante de mi vida profesional.

A mi familia quienes por ellos soy lo que soy.

A mi hijo Nicolás, a ti te dedico mi trabajo de tesis, tú la bendición más grande que Dios pudo dar, tú el motor para sobre salir de todas las adversidades, eres y serás tú hijo mío la persona por la que yo me comprometa a crecer día a día como un profesional de excelencia.

Tú me darás las fuerzas necesaria para sobresalir de obstáculos, gracias a ti mejore mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para poder conseguir éste mi objetivo.

"**La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar**".

Thomas Chalmers.

Marcelo Javier Vizcaíno Bautista

DEDICATORIA

Este Proyecto está dedicado con mucho cariño y gratitud para quienes confiaron en mí; porque me han enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento, me han dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio dedico.

A Dios por ser mi mejor amigo, mi fortaleza, por darme todo lo que tengo y no dejarme caer nunca.

A mis padres Wilson y María, a mis Suegros y a mi Esposo por su comprensión y ayuda en los momentos buenos y malos.

Avalos Mera Iveth Yesenia

INDICE GENERAL

ÍNDICE

ÍNDICE GRÁFICOS

INDICE TABLAS

RESUMEN

El activo más importante de toda organización es la información, razón por la cual en la actualidad las empresas e instituciones invierten cuantiosas cantidades de dinero buscando precautelar la integridad de los datos aunque estas prácticas pueden volverse costoso.

La seguridad de la información no es solamente el establecer un firewall para proteger, o aplicar soluciones parches para corregir las vulnerabilidades en el software o contratar espacio en discos para cuidar de la información mediante backups, aunque todas estas son soluciones al momento, siempre es necesario proteger ya que con estas medidas se requiere la confidencialidad que es mantener la información de personas no autorizadas, la integridad de la información para evitar alteraciones y por supuesto la disponibilidad para asegurar el acceso de la información y los activos que se requieran.

Se realizó la implementación de mecanismos de seguridad estos ayudaran a contrarrestar todos los problemas de seguridad se los efectuó mediante la configuración de implementación de IpTables en el servidor de Linux Centos al igual que se efectuó la evaluación de los posibles ataques de negación de servicios a los que está expuesto el laboratorio de redes de la de la Universidad Técnica de Cotopaxi.

En base a lo expuesto la Universidad Técnica de Cotopaxi extensión de La Maná plantea un laboratorio de seguridades a todo nivel para garantizar la calidad de la educación, en base a principios, normas y estándares de seguridad de la información, desarrollando mecanismos y formas que permitan asegurar los principios básicos de seguridad de la información, ya que desde siempre existe el riesgo de sufrir alteraciones o perdidas de la misma, con la aparición de nuevas formas de hackeo y crackeo tanto interno como externamente de la red de datos.

ABSTRACT

The most important asset of any organization is information, which is why today enterprises and institutions invest substantial amounts of money seeking safeguard the integrity of the data even though these practices can become expensive.

The information security is not only to establish a firewall to protect or implement solutions patches to fix vulnerabilities in software or hire space on disks to take care of the information through backups, although all these solutions are momentary, it is always necessary to protect since with these measures is required the confidentiality of information by unauthorized persons, the integrity of the information to prevent disturbances and granted the availability to ensure access of information and the assets required.

Implementing security mechanisms such help counteract all security issues was held they were the made by configuring iptables in the Linux server Centos as well as the assessment of potential Denial of services performed at thewhich it is exposed laboratory networks of the Technical University of Cotopaxi.

Based on the foregoing, the Cotopaxi Technical University La Mana, proposes a securities laboratory at all levels to ensure the quality of education, based on principles, norms and standards for information security, developing mechanisms and forms to ensure the basic principles of information security, as there is always the risk of interruption or loss of the same, with the emergence of new forms of hacking and cracking both internally and externally of the data network.

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LA MANÁ – ECUADOR

AVAL DE LA TRADUCCIÓN AL IDIOMA INGLES

En calidad de Docente del Idioma Inglés del Centro Cultural de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal CERTIFICO que: La traducción del resumen de tesis al Idioma Inglés presentado por los señores Egresados de la Carrera de Ingeniería en Informática y Sistemas Computacionales: Srta. Avalos Mera Iveth Yesenia y el Sr. Vizcaíno Bautista Marcelo Javier, cuyo título versa : **"EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ."**
Lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimaren conveniente.

La Maná, 18 de mayo del 2015

Atentamente,

Lcdo. Sebastián Fernando Ramón Amores.
DOCENTE
C.C. 050301668-5

INTRODUCCION

En la Actualidad existen muchas formas, métodos y técnicas para realizar ataques a una red, muchas de ellas no solo buscan el objetivo de alterar la información. En cuestión de seguridad informática existe una permanente labor para enfrentar a los atacantes, existen profesionales encargados de proteger redes informáticas y los usuarios sin duda deben saber y conocer los diferentes riesgos a lo que están expuestos, el conocimiento de esto puede ayudarnos a protegernos mejor y mantener al margen de cualquier tipo de vulnerabilidad en el sistema informático.

En la actualidad la mayoría de ataques se vuelven cada vez más difíciles de detectar pero estos pasarían hacer los más comunes: monitoreo no autorizados en sistemas, ataque a contraseñas, denegación de servicios y suplantación de identidad.

Los objetivos más comunes de estos ataques es ingresar al sistema de la víctima, a través de la red, haciendo uso de una conexión remota, con credenciales (nombre de usuario y contraseña) falsas y una vez vulnerada podría esta información ser modificada sustituida o hurtada con fines maliciosos. Por lo cual nosotros hemos visto necesario evaluar el laboratorio de redes de comunicación de la Universidad Técnica de Cotopaxi Extensión La Maná las posibles vulnerabilidades que existen y a la vez proponer nuevas técnicas de protección

El proyecto de investigación tiene como fin realizar un análisis de seguridad de software para el laboratorio de redes y comunicación de la red Universidad Técnica de Cotopaxi Extensión La Maná, revisando el estado actual de la red, tomando en cuenta las vulnerabilidades de seguridad posteriormente se efectuara la instalación de herramientas informática que nos permita brindar seguridad a nuestra infraestructura.

Para lo que se ha subdivido este proyecto en tres Capítulos:

Capítulo I: Marco teórico y conceptual que respalda a la investigación con partes de datos bibliográficos para el análisis e implementación de herramientas que van acorde con el tema de investigación para beneficio de la red de datos de la institución

Capítulo II: Se encuentra el estudio y definición de los resultados derivados de las encuestas y su tabulación, para conocer los criterios dados por beneficiarios de nuestra investigación, y así conocer sus necesidades para plantear la factibilidad de la propuesta

Capitulo III: Una vez definidas las necesidades que tiene el laboratorio de redes de la Universidad Técnica de Cotopaxi Extensión La Maná en la red, se implementó varios mecanismos de seguridad en el laboratorio.

CAPÍTULO I

1. FUNDAMENTACIÓN TEÓRICA

1.1. Redes

Según, MATÍAS, Katz.2013.Redes y Seguridad.2013. Alfa omega. Pág. 2 El término "red" es usado desde hace muchos años para identificar a toda estructura que combine los métodos físicos y técnicos necesarios para interconectar equipos informáticos con el propósito de lograr un intercambio efectivo de información en un entorno específico, ya sea laboral, personal o global. Las redes son altamente efectivas para poder compartir todo tipo de información y recursos que estén disponibles en nuestras computadoras, proyectándonos de herramientas para centralizar y distribuir, según sea necesario las diferentes necesidades informáticas que podamos tener.

Según, JOSE, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.79. Una red de ordenadores consiste en una serie de hosts autónomos y dispositivos especiales módems, routers, pasarelas, multiplexores, etc.) Interconectados entre sí. Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de las mismas, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

Según los autores, Una red es un conjunto de computadoras enlazadas entre si y/o con otros equipos, para transmitir y recibir datos o información, La red de computadoras permite compartir recursos a distancia, aumenta la velocidad de la transmisión de datos (es más rápido acceder a un archivo por una red que a través de Internet. Donde cada uno de los integrantes comparte información, servicios y recursos con el otro.

1.1.2. Factores de una Red.

Según, MATÍAS, Katz.2013.Redes y Seguridad.2013. Alfaomega. Pág. 5 Los factores más importantes que debe cubrir una correcta administración de red son (en orden de prioridad) la funcionalidad, seguridad y rapidez (FSR).Una red debe ser funcional ósea que debe funcionar, sino no tiene razón de existir, por eso el enfoque principal dentro de la administración de una red debe ser justamente asegurarse y preservar que la red funcione.

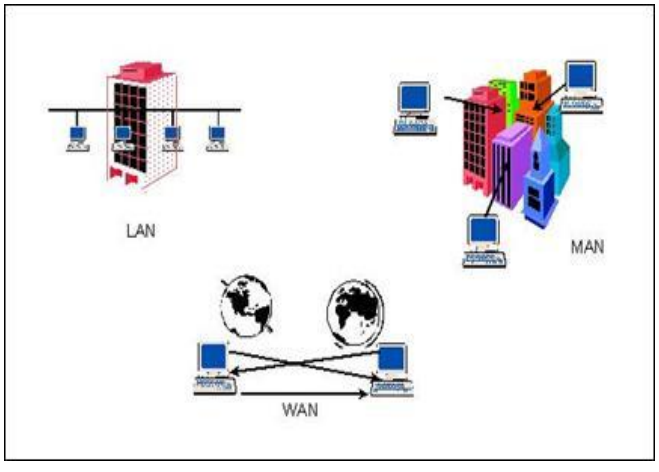
Consecuentemente, una red debe ser segura. Es decir, debe cumplir con las necesidades básicas de seguridad para el entorno y la información que maneja. Estos niveles de seguridad son relativos y variables, y deben ser medidos y administrados previamente. Es muy importante asegurarse que estos niveles de seguridad no interfieran con la estabilidad y funcionalidad de la red. Por último, una red funcional y segura debe trabajar de manera rápida. Esto significa que se deberán implementar las herramientas necesarias para que la información fluya lo más rápidamente posible, siempre y cuando esta rapidez no disminuya los niveles de seguridad y funcionalidad de la red, previamente establecidos.

Según los autores, una red debe cumplir con su funcionabilidad como son segura, rápida, confiable la misma que debe estar operativa siempre para poder cumplir así las necesidades para la cual fue implementada, tener en cuenta que está siempre debe tener una trasferencia de información rápida y segura pero tampoco descuidarse de todos sus niveles de seguridad niveles que deben ser administrados previamente de una forma relativa o variable.

1.2. Tipos de redes.

Existen diferentes tipos de redes. Según su amplitud de cobertura. Cada una posee diferentes características, y utiliza distintos componentes para su implementación

GRAFICO 1.1. Tipos de Red



Fuente: *http://joan004.tripod.com/compo.htm*

Realizado por: *Autores*

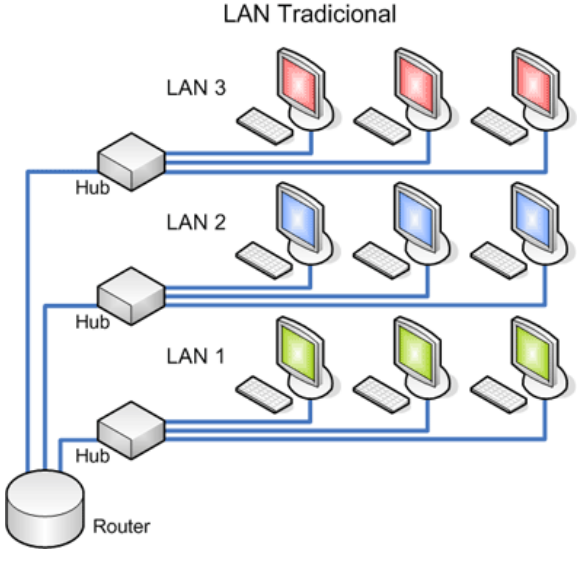
1.2.1 Redes LAN (Local Area Network)

Según, JOSE, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.79. Las redes de área local son redes de ordenadores cuya extensión es reducida, de menos de 1km. Son redes pequeñas habituales en oficinas y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que aun solo cable se conectan todas las maquinas. La velocidad de transmisión más típica es la de 100 Bit/s, aunque también están utilizándose 1 Gbit/s, y hasta 10 Gbit/s, en empresas grandes.

Según, Vieites Álvaro Gómez. Enciclopedia de la Seguridad Informática. 2011. Alfaomega. Pág. 62. Una red de área local es un sistema de comunicaciones constituido por un hardware y un software que se distribuyen por una extensión limitada en el que existen una serie de recursos compatibles, a lo que tienen acceso los usuarios para compartir la información de trabajo. También llamada Red de Área Local, este sistema de computadoras permite la comunicación entre computadoras, la característica principal de esta red es que la distancia es de 200m y 1km.

Una red LAN se limita a un área especial relativamente pequeña no muy extensa, tales como puede ser un hogar o una organización. Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas, ondas de radio, satélites, fibra óptica entre otras. Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos.

GRAFICO 1.2. Red LAN



Fuente: *http://www.anexom.es*

Realizado por: *Autores*

1.2.2. Redes MAN

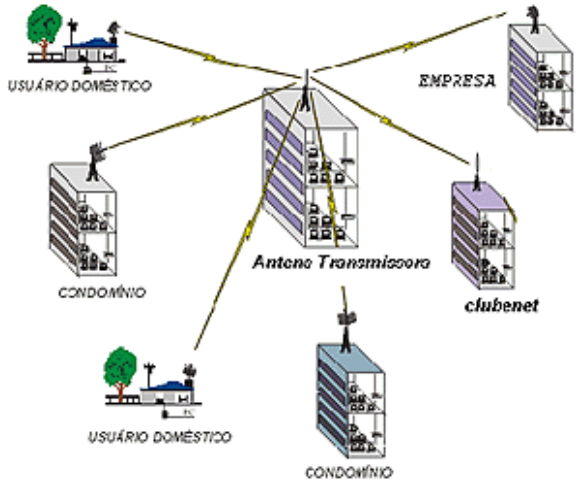
Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 39 Las redes MAN (MetropolitanArea Network, Red de área metropolitana). Están muy relacionadas con las redes LAN. De hecho, su mayor diferencia es únicamente es el hecho de poseer un área de cobertura geográfica significativamente mayor.

Estas redes pueden ser utilizadas para interconectar diferentes edificios o complejos que se encuentren físicamente cercanos. Se podría decir que una red MAN es un conjunto de redes LAN agrupadas e interconectadas.

Según, JOSÉ, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.79 Redes MAN (MetropolitanArea Network). Las redes de área metropolitana son redes de ordenadores de tamaño superior a la de una LAN, soliendo abarcar el tamaño de una ciudad, aproximadamente hasta unos 10 km. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en una misma área metropolitana, o de operadores que ofrecen sus servicios a otras empresas.

Una red MAN es cuya red superior a la LAN ya que esta abarca una extensión más amplia y se la utiliza para interconectar con diferentes edificios. Las redes MAN pueden ser públicas o privadas. Estas redes se desarrollan con dos buses unidireccionales, lo que quiere decir que cada uno actúa independientemente del otro respecto a la transferencia de datos. Cabe mencionar que ambas opciones son seguras dado que no permiten la lectura o la alteración de su señal sin que se interrumpa el enlace físicamente.

GRAFICO 1.3. Red MAN



Fuente: *http://isunicor.wikispaces.com*

Realizado por: *Autores*

1.2.3. Redes WAN

Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 40. Las redes WAN (Wide Área Network, Red de área amplia) son redes de gran amplitud, generalmente utilizadas para conectar sitios geográficos significativamente alejados, por ejemplo, continentes cruzando océanos.

Este tipo de red utilizado para interconectar a nuestro planeta por completo, permitiéndonos comunicarnos con nuestros pares a miles de Kilómetros de distancia en cuestión de segundos.

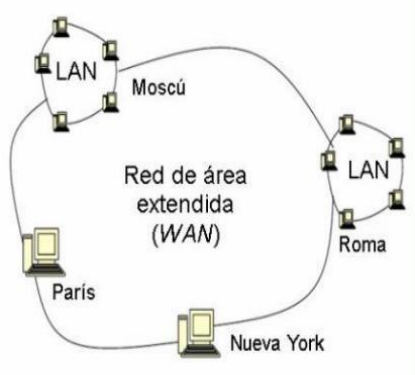
Las redes WAN están formadas por concentradores de red de gran tamaño y funcionamiento complejo, ubicados en lugares específicos y conectados a través de cables tendidos por tierra o por mar, y satélites gravitando en el espacio.

La red WAN más popular es internet, que nos permite acceder a contenido publicado en cualquier parte del mundo, instantáneamente.

Según, JOSE, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.79. Redes WAN (Wide Area Network) Son redes de área amplia tienen un tamaño superior a una MAN, y consisten en un conjunto de nodos o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de dispositivos tales como módems y routers. Su tamaño no tiene límite y puede llegar a cubrir todo el planeta.

Según los autores, Una red WAN es aquella que se caracteriza por ser una red muy extensa ya que abarca países, hasta un planeta también se pude decir que es el conjuntos de puerto, nodos de redes LAN. Una red MAN es cuya red superior a la LAN ya que esta abarca una extensión más amplia y se la utiliza para interconectar con diferentes edificios. Los ordenadores conectados a una red de área ancha normalmente están conectados a través de redes públicas, como la red de teléfono.

GRAFICO 1.4. Red WAN



Fuente: *http://cmapspublic.ihmc.us*

Realizado por: *Autores*

1.3. Topologías De Red

Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 45. Las diferentes topologías indican la forma en la que se interconectan los dispositivos de red. Generalmente, las topologías están formadas por diferentes armados de red respecto a los componentes de la capa1 (física), y ocasionalmente con los componentes de la capa 2 (enlace).

Cada topología cuenta con sus ventajas y desventajas, y debe ser cuidadosamente seleccionada a la hora de diseñar la red a implementar. Veamos las diferentes topologías existentes.

1.3.1. Topología Mesh (Malla)

La topología mesh (malla) refleja una implementación en la cual todos los equipos poseen conexiones directas hacia el resto. Cada uno de los equipos en la red posee un dispositivo de entrada/salida para cada conexión necesaria, y los enlaces entre equipos son “punto a punto”, es decir comienzan la conexión en un equipo y terminan en el otro.

Según, José Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.82.En una topología de malla, cada nodo se enlaza con otros nodos, al menos dos, y siempre hay la posibilidad de establecer rutas alternativas. Las ventajas son que, como cada nodo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de otros enlaces hasta llegar al destino. Además esta topología permite que la información circule por varias rutas a través de la red.

La Desventaja física principal es que solo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumada.

La topología en Malla es muy importante e interesante ya que si esta red llegara a desaparecer un nodo no afectaría en lo absoluto a los demás nodos y continuaría funcionando igualmente ya que se encuentran enlazadas entre sí, Contiene múltiples caminos para llegar al destino lo cual favorece, ya que si hay tráfico de información, se podrá tomar una ruta alterna para hacer llegar la información al destino.

1.3.2. Topología en Anillo

Según, JOSÉ, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.81. Una topología en anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.
Una topología en anillo doble consta de dos anillos concéntricos, donde cada nodo de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Esta topología incrementa la confiabilidad y flexibilidad de la red ya que al haber un segundo anillo redundante que conecta los mismos dispositivos, en caso de rotura de uno de ellos, el tráfico se mantiene por el otro.

Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 48. Una red ring es fácilmente implementarle, su mantenimiento es reducido. En caso de encontrarse problemas, simplemente se debe desconectar el equipo en falla y cerrar el anillo nuevamente; y en caso de querer ampliar la red, simplemente alcanza con abrir una de las conexiones y conectarlas al nuevo equipo.

Asimismo que las comunicaciones son simples entre dos equipos, el dato por trasladar presenta una baja complejidad en su diseño y estructura. Una desventaja principal radica en el tamaño de la red. Una red ring solo será eficiente cuando esté formada por una cantidad de equipos reducida. A medida que el anillo crece, los enlaces se degradan, las fallas aumentan y las transferencias se hacen significativamente lentas.

La topología en anillo es aquella que no abarca muchos equipos por lo que no es tan recomendable usarla mientras más equipos se utilicen menor será su eficiencia. Los componentes de la red se sitúan de forma circular, y al transmitir la información puede pasar por varios computadores antes de llegar a su destino, los equipos se comunican por turnos y se crea un bucle de equipos en el cual cada uno "tiene su turno para hablar" después del otro.

1.3.3. Topología en Bus

Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 49 Las redes bus se caracterizan por poseer un canal único de comunicación, con conexiones multipunto. Es decir, existe un único cable principal de comunicación al cual se conectan físicamente los equipos que deban pertenecer a la red: La red presenta un cable central de comunicación, denominado bus, al cual se conectan los dispositivos mediante un cable individual por equipo. En las finalizaciones del cable debe colocarse un terminador, que permita cerrar el bus mediante la emanación de ecos por cada señal que recibe. En caso de expandir la red, el terminador puede reemplazarse por un conector de puente conectado a otro bus, de manera simple.

Según, JOSE, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.82. la topología en bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada nodo está conectado a un cable común, por lo que se puede comunicar directamente, y la ruptura del cable hace que los nos queden desconectados. Es la topología más común en pequeñas LAN, con un hub o switch en uno de los extremos.

Esta topología es **s**imple y fácil de arreglar cuando se encuentra el problema ocasionado en la red, es más económica ya que requiere menos cableado que otras topologías. Además en esta red cuyos componentes de la red se sitúan linealmente a lo largo del cable o medio de transmisión en cual tiene en cada extremo un dispositivo llamado terminador que cierra el programa.

1.3.4. Topología en Árbol

Según JOSE, Manuel Huidobro y Ramón Jesús Millán Tejedor. 2009. Redes de Datos y Convergencia IP. 2009. Copiringht. Pág.82 La topología en árbol es similar es similar a la topología en estrella extendida, salvo en que no tiene un nodo centra. El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en un extremo del enlace troncal generalmente se encuentra un servidor (host).

Según el sitio web (http://www.ecured.cu/index.php/Red_en_%C3%A1rbol) La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

La Topología Árbol es aquella en la que la conexión se da de forma jerárquica, o en forma de árbol, como su nombre lo indica, ya que posee un nodo conectado a otros en forma ramificada. Cuando las redes son bastante grandes, se pueden tener pequeñas sub redes conectadas entre sí por un nodo central, en esta topología cuando recuerda una ramificación se denomina árbol.

1.3.5. Topología Estrella

En una red estrella típica, la señal pasa de la tarjeta de red (NIC) de la computadora que está enviando el mensaje al Hub y este se encarga de enviar el mensaje a todos los puertos. La topología estrella es similar a la Bus, todas las computadoras reciben el mensaje pero solo la computadora con la dirección, igual a la dirección del mensaje puede leerlo.

Según, MATÍAS, Katz.2013. Redes y Seguridad. 2013. Alfaomega. Pág. 49 La topología star (estrella) es la primera en presentar un dispositivo de conexión adicional para lograr la comunicación entre equipos: el concentrado.

En estas redes, los dispositivos no están conectados entre sí, sino que comparten el medio de comunicación al conectarse todos a un mismo componente que recibe, gestiona y reenvía los datos que los equipos se envíen entre ellos.

Según los autores, Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste, los componentes de esta red es la Tarjeta de interface, Cable de dos hilos sin blindaje y el Distribuidor Central (HUB), en ocasiones existe un nodo central encargado de gestionar y controlar la comunicación dentro de la red este es un caso típico de una topología en estrella.

1.4. Seguridad Informática

Según, ÁLVARO, Gómez Vieites.2013.Seguridad en Equipos Informáticos. 2013. Starbook. Pág. 16 Podemos definir a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Así mismo, es necesario considerar otros aspectos o cuestiones relacionados cuando se habla de seguridad informática.

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en acceso a los servicios ofrecidos y a la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter persona, etc.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático, etc.

Según, JULIO, Gómez López.2011.Administracion de Sistemas Operativos. 2011. Ra-Ma. Pág. 76 la Real Academia de la Lengua, seguridad es la cualidad de seguro, es decir, de estar libre y exento de todo daño, peligro o riesgo. En informática, como en tantas facetas de la vida, la seguridad entendida según la definición anterior es prácticamente imposible de conseguir, por lo que se ha relajado acercándose más al concepto de fiabilidad; se entiende un sistema seguro como aquel que se comporta como se espera de él.

De los sistemas informáticos, ya sean sistemas operativos, servicios o aplicaciones, se dice que son seguros si cumplen las siguientes características:

- **Confidencialidad.** Requiere que la información, sea accesible únicamente por las entidades autorizadas.
- **Integridad.** Requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y re actuación de los mensajes transmitidos.
- **No repudio.** Ofrece protección a un usuario frente a otro usuario que niegue posteriormente que se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitan la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, Las firmas digitales constituyen el mecanismo más empleado para este fin.
- **Disponibilidad.** Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

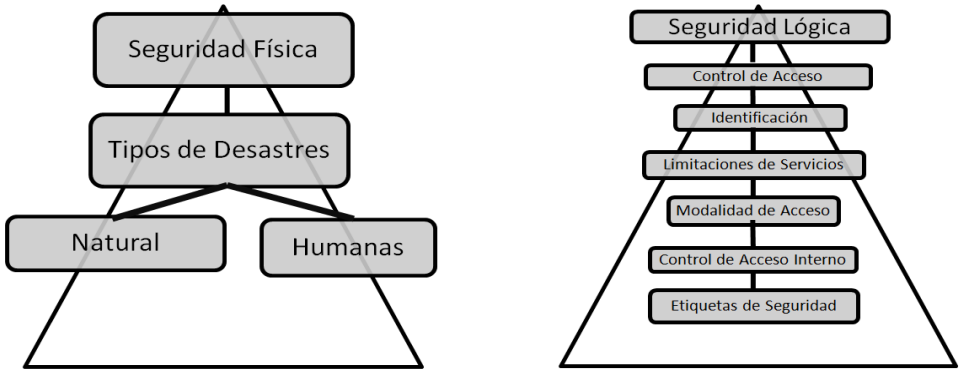
La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema, además es un estado de cualquier tipo de información informático o no que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

1.5. Tipos De Seguridad

La seguridad informática se dedica a la protección de sus sistemas, existen dos tipos Seguridad Física aplicada a sus equipos y a la infraestructura ya que es la parte fundamental de la información, Seguridad lógica es la que se define por salvaguardar la protección de los contenidos e información estos dos tipos tienen un solo fin mantener la integridad, confiabilidad autenticidad y disponibilidad de la información la cual es muy significativa para los usuarios

En función de lo expuestos podemos clasificar a la seguridad informática en dos fundamentales, ya que estos son muy importantes, en la actualidad se viene implementando con mayor frecuencia, y los cuales se subdividen en la siguiente tabla.

GRAFICO 1.5. Tipos de Seguridad



Fuente: *http://www.ecured.cu/index.php/Red_de_computadoras*

Realizado por: *Autores*

1.5.1. Seguridad Física

Según, JULIO, Gómez López.2011.Administracion de Sistemas Operativos. 2011. Ra-Ma. Pág. 95, El equipamiento hardware de un sistema informático es, probablemente, la parte más cara, aunque, por el contrario, la más fácil de reemplazar. Sin embargo, existen unas pautas generales, muchas de ellas dictadas por el sentido común, que pueden ayudar a prevenir problemas con el hardware del sistema y de la red de comunicaciones.

Desde el punto de vista de la prevención, es altamente recomendable aislar los elementos hardware en recintos cerrados y protegido su acceso mediante cualquier mecanismo. Dependiendo de la importancia de la organización y su sistema a proteger puede ir desde una puerta con llave hasta los más modernos controles de acceso mediante reconocimiento de huella dactilar u ocultar, que impida el acceso a personal no autorizado. En el caso de las instalaciones de redes de computadoras, el cableado debe distribuirse mediante elementos que impidan el acceso de cualquier usuario a ellos que, por la simple alteración del campo electromagnético del cable,

con la herramienta apropiada, puede detectarse la información que se transmite y afectar a la confidencialidad de las transmisiones.

La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial y a los controles y mecanismos de seguridad como puede ser dentro y alrededor de un Centro de Cómputo. El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización. Acceso físico, Desastres naturales y Alteraciones del entorno.

1.5.2. Seguridad Lógica

1.5.2.1. Modelo De Seguridad Aaa

Según, ÁLVARO, Gómez Vieites.2013.Seguridad en Equipos Informáticos. 2013. Starbook. Pág. 12, El modelo de seguridad AAA (Authentication, Autorization & Accounting). Que podríamos traducir por "Autenticación, Autorización y contabilidad (Registro y auditoria)" se utiliza para poder identificar a los usuarios y controlar su acceso a los distintos recursos de un sistema informático, registrando además como se utilizan dichos recursos.

Este modelo se basa por lo tanto, en tres elementos fundamentales:

- **Identificación y autenticación de los usuarios:** la identificación es el proceso por el que el usuario presenta una determinada identidad para acceder a un sistema mientras que la autenticación permite validar la identidad del usuario.

- **Control de acceso** a los recursos del sistema informático: equipos, aplicaciones, servicios y datos, en función de las políticas establecidas por la organización.
- **Registro del uso de los recursos** del sistema por parte de los usuarios y de las aplicaciones, utilizando para ello los logs (registros de actividad) del sistema.

Consiste en la aplicación de barreras y procedimientos que resguarden al acceso de los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo, así la seguridad lógica, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad, además consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."
Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

1.6. Seguridad en Redes

Según, SERPA PAZ, Guillermo Adan. Noviembre 17, 2014, p 2.En la actualidad estamos propensos ataques que ponen en vulnerable toda la información esto lleva a que esté en riesgo la integridad de dicha información. Los mismos riesgos que no solo provienen dentro de la institución, sino también desde el exterior, para trabajar de forma veremos la ayuda del Sistema de gestión de la seguridad de la información (SGSI) Sistema de gestión de la seguridad de la información (SGSI) este sistema nos ayuda a gestionar y minimizar las vulnerabilidades a las que están expuestas, ordena, analiza y controla amenazas que pueden terminar en riegos para nuestra información

Según, CHAVEZ FLORES, Alejandra T. Octubre 2009, Al abordar el tema de Seguridad de redes, se debe tener muy en claro que no existe una seguridad en términos absolutos. Sólo se pueden reducir las oportunidades de que un sistema sea comprometido o minimizar la duración y daños provocados a raíz de un ataque. Al tratar el asunto, se está considerando que se encuentran en riesgo tres elementos:

- Confidencialidad
- Integridad
- Disponibilidad

Seguridad en redes de datos no existe algo eficaz para proteger todo en absoluto solo minimizar las vulnerabilidades y posibles ataques, formar barreras de seguridad para que el ataque no sea destructivo y genere daños en la información. Se basa igual en muchos pasos que debemos llevar para manteneros al margen de los problemas que podamos estar expuestos.

Según, Álvaro Gómez Vieites. (2011). "Enciclopedia de la Seguridad Informática". México: Alfaomega.ISBN: 978-607-707-181-5Entre los principales objetivos de la Seguridad Informática se destacan los siguientes:

- Minimizar y gestionar los riesgos, detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para cumplir con estos objetivos una organización debe contemplar cuatro planes de actuación:

- **Técnico:** Tanto a nivel físico como a nivel lógico.
- **Legal:** Algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad, por ejemplo el sector de servicios financieros.
- **Humano:** Sensibilización, formación de empleados y directivos, definición de funciones y obligaciones del personal.
- **Organizativo:** Definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

En el mundo aparecen y existen nuevos e interesantes tipos de sucesos, aún se encuentran fallas y problemas con la seguridad son tan difíciles de generar técnicas de un adecuado uso, en muchos casos esto sucede cuando no hay el suficiente conocimiento sobre los eminentes riesgos que conllevan, y para esto se necesita formas y métodos seguros para concienciar las acciones, capacitando y llenando de mejores conocimientos y prácticas.

El mantener con seguridad a los sistemas de información es una disciplina que tiende a una continua evolución. La finalidad de seguridad es la de tolerar que una organización cumplan con sus objetivos, satisfagan sus necesidades para eso se debe tener un minucioso cuidado en dicha implementación

1.7. Servidor

Según DOUGLAS Comer, Redes Globales De Información Tcp/Ip, Segunda Edición, Prentice Hill, pág. 19, Es la máquina principal de la red. Se encarga de administrar los recursos de ésta y el flujo de la información. Algunos servidores son dedicados, es decir, realizan tareas específicas. Por ejemplo, un servidor de impresión está dedicado a imprimir; un servidor de comunicaciones controla el flujo de los datos, etc.

1.7.1. Tipos De Servidores

En la actualidad existen una variedad de servidores para múltiples aplicaciones, que son utilizadas por instituciones públicas y privadas en las cuales podemos citar los siguientes.

1.7.1.1. Servidor Web.-Básicamente un servidor Web es un computador preparado y acondicionado para estar permanentemente conectado a una red de alta velocidad. Esta red de alta velocidad forma parte de Internet, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML.

1.7.1.2. Servidores de Aplicaciones.- (Application Servers). Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan. "Los servidores de aplicación también brindan a los desarrolladores una Interfaz para Programación de Aplicaciones (API), de tal manera que no tengan que preocuparse por el sistema operativo

1.7.1.3. Servidores Proxy (Proxy Server).- Los servidores Proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones. Funcionamiento Un Proxy permite a otros equipos conectarse a una red de forma indirecta a través de él.

- Manejo de sus bases de datos ya sea desde el mismo servidor o desde sus aplicaciones remotas.
- Sincronización de sus bases de datos o la de sus clientes entre varios servidores.

Según, Windows Server Administration Fundamentals. Microsoft Official Academic Course. 111 River Street, Hoboken, NJ 07030: John Wiley & Sons. 2011. p. 21. ISBN 978-0-470-90182-3.Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor".

Según los autores, Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando.

Según lo expuesto por los autores. Es el centro donde se almacena toda la información de una red este se lo puede instalar en cualquier computador siempre y cuando cumpla con las características necesarias. Es el administrador de recursos para el tráfico de flujo ya que se lo programa para tares especificas existen varios tipos de servidores pero están citados 3 de los más importantes tales como los de Servidor Web, Aplicaciones, Proxy (Proxy Server), Es capaz de satisfacer necesidades dependiendo el cliente lo requiera ya que dicho trabajo lo hacen mediante cliente-servidor, este software se lo instala en computadores con el fin de brindar seguridad a toda la información ya que sirve para compartir información, recursos tanto de software o hardware, los servidores más comunes brindan servicios en una red donde esta entra en funcionamiento, con el contexto de redes en internet y protocolos (IP)

1.8. Firewalls

Según GABRIEL VERDEJO, Álvarez: Seguridad En Redes Ip: Ids 2011. Pag 72. Durante mucho tiempo el mecanismo de seguridad en redes más extendido ha sido únicamente el uso de un firewall. Este sistema nos permite de una manera simple y eficaz aplicar filtros tanto para el tráfico de entrada como para el de salida en nuestra red. Podemos diferenciar entre dos políticas básicas de configuración de firewalls:

1.8.1. Permisividad máxima (*alloweverything*) dónde el uso de filtros es mínimo o inexistente.

Esta política permite prácticamente la circulación de todo el tráfico y se utiliza principalmente en Intranets/LAN, campus universitarios y organizaciones dónde la libertad de uso de aplicaciones (o la gran cantidad de ellas) es necesaria para el funcionamiento ordinario del sistema. Es una política que dificulta enormemente el uso de otros sistemas y deja a la red muy vulnerable a prácticamente cualquier tipo de ataque interno o externo. En estos casos se recomienda segmentar la red en dominios y acotar cada uno de estos dominios, ya que raramente todos los ordenadores tienen que acceder a todos los recursos disponibles de la red.

1.8.2. Permisividad mínima (*denyeverything*) aplica la política contraria a la anterior.

En este caso se deniega acceso a todos los servicios de la red y se van permitiendo accesos a estos a medida que se necesiten. De esta forma es bastante improbable que recibamos un ataque a un servicio que desconocíamos que teníamos en la red. Por otro lado, el trabajo de otros sistemas se facilita enormemente ya que pueden configurarse para que detecten fácilmente cualquier comportamiento anómalo en la red (simplemente se debe monitorizar los accesos a los servicios y comprobar si esos accesos están permitido expresamente o no).

Cabe notar que este tipo de política requiere un gran esfuerzo ya que es poco flexible y en organizaciones con gran cantidad de usuarios con diferentes requerimientos puede llevar a tener que permitir tantos accesos cruzados que deje de ser práctico. Destacar que el simple uso de un firewall puede crear una falsa sensación de seguridad que de nada sirve si no son configurados y "mantenidos al día" (aplicación de los parches/patches del fabricante, supervisión y adaptación al tráfico de la red...). Muchas organizaciones con cientos de ordenadores y decenas de firewalls no disponen de una sola persona cualificada asignada exclusivamente a su mantenimiento.

Según, MOLL MONRREAL, Pedro. Seguridad Informática, 2014. Pag,18. Cortafuegos en ingles Firewall es una parte de un sistema o una red que está diseñada para controlar las comunicaciones del ordenador con el exterior siguiendo un conjunto de normas o reglas. Todos los mensajes que entren o salgan de la internet pasan atreves del cortafuegos que examina cada mensaje y bloque aquellos que no cumplen con los criterios de seguridad específicos. Los cortafuegos pueden ser implemento de hardware o software o una combinación de ambos

Existen dos políticas básicas en la configuración de cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política Restrictiva.-**Se deniega todo el tráfico excepto el que esta explícitamente permitido, esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales

- **Política Permisiva.-**Se permite el tráfico de todo menos de lo que esta explícitamente denegado. Esta aproximación la suelen utilizar Universidades, Centros de investigación y Servicios Públicos de acceso al internet.

Cuando se produce la comunicación entre dos ordenadores, esta se establece utilizando la dirección IP de ambos equipos.

Una vez establecida, cada aplicación o servicio envía sus paquetes (puerto de salida) o a la vez al (puerto de entrada) .la finalidad del firewall es la de permitir o denegar en tráfico de información por dicho puerto, examinando dichos paquetes que lo legan. Los puertos son abiertos según las aplicaciones o programas que van utilizarlos

Según lo expuesto por los autores. Es una combinación de componentes con el hardware y software, encargado de filtrar información la cual entra y sale de la red con su fin de bloquear en caso de ser necesario. Cortafuegos que sirve como un método de seguridad aplicando filtros de una manera simple y eficiente tener el control del tráfico de información de nuestra red la cual está basada en tipos tanto Máxima tiene el control del flujo sobre la red de una forma escaza o inexistente la cual hace que la información este vulnerable ante cualquier anomalía. Y Mínima es todo lo contrario aplica todas las políticas de seguridad faltantes en la anterior.

1.9. Sistemas Operativos

1.9.1. Windows Server 2012

Según, CHARTE OJEDA Francisco, Microsoft windows server 2012 Anaya Multimedia. Pag 448. ISBN 9788441533202 Este sistema ofrece grandes beneficios a proveedores de Hosting y a empresas para realizar sus tareas ya que permite el manejo de escalabilidad y dinamismo. Es un sistema operativo de servidor que permite al ordenador manejar funciones de red como servidor de impresión, controlador de dominio, servidor web y servidor de archivos. También es la plataforma para aplicaciones de servidor separado.

Características de Windows Server

Las principales características del sistema operativo Windows Server 2012 son las siguientes:

- Protección contra malware en la carga de controladores en memoria
- Nuevo proceso de reparación de sistemas
- Reduce tiempos de espera en los Terminal Services
- Administración de direcciones IP
- Soporta escenarios adicionales, incluyendo conexiones de modo de transporte de extremo a extremo de IPSec
- Proporciona interoperabilidad para Windows con otros sistemas operativos que utilizan seguridad de extremo a extremo
- No posee la edición Enterprise que estanque los trabajos.
- Cierre limpio de Servicios
- Inclusión de una consola mejorada con soporte GUI para administración
- Administración de energía
- Mejoras en el rendimiento de la virtualización
- Utiliza la interfaz de Windows PowerShell.
- Utiliza certificados para el mecanismo de autenticación

Analizado lo establecido, Windows Server 2012 es una de las últimas versiones lanzada por Microsoft, es un servidor que ofrece muchos beneficios a las instituciones y empresas con un manejo confiable y eficaz. Muestra características como de protección y administración.

1.9.2. Linux / GNU Software Libre

Según, Roca, M. "Empresa y Administración en España y Cataluña": (2007). España: UOC. Pag. 21, La noción del software libre inicia con Richard Stallman, y aunque en la actualidad se habla de software libre y de software gratuito no hay que confundir el concepto de libre con gratis. Un software libre debe entenderse como aquello en que el usuario tiene la libertad de acceder a su código, usarlo, copiarlo, estudiarlo, modificarlo, y redistribuirlo libremente.

Si el usuario ha modificado el código o ha creado alguna herramienta, este no puede negar tal código ya que al ser libre, otro usuario puede acceder a este, sin embargo la persona quien modificó el software puede optar por redistribuirlo sin costo alguno, o a su vez pedir dinero por su código.

Dentro del software libre existen ciertas libertades los mismos que se definen a continuación

Libertad 0: Permite que el software pueda ser usado para cualquier propósito.

Libertad 1: Puede ser estudiado y posteriormente modificado por un determinado usuario, adaptando tales modificaciones a sus necesidades, para ello esta libertad garantiza el acceso al código fuente.

Libertad 2: Permite que el software pueda ser distribuido libremente de la voluntad del autor. Es decir un usuario puede copiar, vender o prestar el software a las personas que este lo desee.

Libertad 3: Permite que un usuario pueda mejorar el software y hacerlo público, de modo que toda la comunidad se beneficie.

Analizamos y decimos que, el software libre como su nombre lo dice permanece en completa libertad de que los usuarios puedan trabajar ejecutar, estudiar, cambiar y mejorar la productividad del software de una forma libre sin recargos o algún costo, es una herramienta para desarrollar estudios a las personas, ya que se lo adquiere en el Internet sin ningún tipo de limitación, dejando de que nuevos productos se desarrollen sin la necesidad de que partan desde cero.

1.9.3. Kali Linux

Según, WILLIE Pritchett, Kali Linux Cookbook, año 2013 Pág. 52. Es la distribución Linux para auditorías de seguridad por excelencia, está basada en la popular distribución Debían, ahora los desarrolladores han lanzado la versión 1.1.0 estable. La principal característica de esta nueva versión es que incorpora un soporte hardware mucho mayor que las versiones anteriores, y además sus desarrolladores se han centrado en la estabilidad.

Esta nueva versión de Kali Linux ejecuta el kernel Linux 3.18, que es justamente el kernel recomendado para auditorías inalámbricas ya que mejora la compatibilidad con los diferentes controladores Wi-Fi, además se han actualizado todos sus drivers para proporcionar la máxima estabilidad y también el mejor rendimiento posible. Otra característica destacable es que soporta Nvidia Optimus, esta tecnología fue creada por Nvidia y permite a los ordenadores portátiles incorporar dos chips gráficos (uno de menor rendimiento y menor consumo, y otro de mayor rendimiento y mayor consumo) y cambiar entre ellos de forma transparente mediante software con la finalidad de ofrecer el mejor rendimiento en aplicaciones gráficas exigentes u otros usos como por ejemplo el cracking de contraseñas, y también un menor consumo de energía en caso de no usar aplicaciones exigentes. Asimismo esta nueva versión de Kali Linux ha actualizado las herramientas para VirtualBox, OpenVM.

Según, RODERICK Smith, LPIC-1: LINUX PROFESSIONAL INSTITUTE CERTIFICATION (3ª ED.) título. ANAYA MULTIMEDIA, 2013 año Pag 92. Es la nueva generación de la conocida distribución Linux BackTrack, la cual se utiliza para realizar Auditorías de Seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad y cubrir las huellas. Este documento proporciona una excelente guía práctica para utilizar las herramientas más populares incluidas en de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios Kali Linux, las cuales abarcan las bases de las Pruebas de Penetración. Así el tema, como para los novatos.

Características de Kali Linux

Kali Linux es una completa mismo este documento es una excelente fuente de conocimiento tanto para profesionales inmersos en reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el VCS.

• Más de 300 herramientas de Pruebas de Penetración

• Es Libre y siempre lo será

• Árbol Git Open Source

• Cumple con FHS (Filesystem Hierarchy Standart)

• Amplio soporte para dispositivos inalámbricos

• Parches al Kernel para inyección.

• Entorno de desarrollo seguro

• Paquetes y repositorios firmados con GPG

• Varios lenguajes

Según los autores, El Sistema Operativo Kali es la nueva generación de Linux fue desarrollado a partir de la distribución de BackTrack ya que se encuentra usada comúnmente para la seguridad que contiene una gran cantidad de herramientas para ayudar a identificar vulnerabilidades además, Kali intenta que los interesados comprendan la necesidad de crear aplicaciones seguras así como pueda servir de base para aquellos que deseen continuar en el mundo de la seguridad informática.

1.10. Protocolo IPV4

Según, Joel Barrios Dueñas, 2012. Introducción a IP versión 4. Pág. 18. IPv4 es la versión 4 del Protocolo de Internet (IP o Inernet Protocol) y constituye la primera versión de IP que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicial mente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force) en septiembre de 1981, documento que dejó obsoleto al RFC 760 de enero de 1980. IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet). Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de mejor esfuerzo).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de TCP o UDP.

El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

Según los autores Protocolo de internet que se mostró por primera vez como IP luego cambiando a Ipv4 siendo este el más utilizado en los últimos tiempos este protocolo cuenta con características no favorables ya que no proporciona garantías en el intercambio de datos, como en datagramas no fiables. IPv4 es un protocolo de Internet, el sistema de identificación que utiliza Internet para enviar información entre dispositivos.

1.11. Protocolo IPV6

Según, ARIGANELLO Ernesto, Redes Cisco. Guía de estudio para la Certificación Ccna Routing Y Switching, RA-MA, año 2014. Pág. 12. Debido al crecimiento del Internet y la sofisticación de los dispositivos electrónicos, las soluciones propuestas con el fin de escalar el espacio de direccionamiento de Internet IPv4, no serán suficientes para cubrir la necesidad de las mismas en los próximos años. Como consecuencia de este escenario, el Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) elaboró una serie de especificaciones para definir un protocolo IP de Siguiente Generación (IP Next Generation, IPng) que actualmente se conoce como Protocolo de Internet versión 6.

Espacio mayor de direccionamiento

El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionables. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas.

Según, PHILIPPE Freddi. Windows Server 2008: Los Servicios De Red Tcp/Ip Año2010 Pág. 42. IPv6 empieza a ganar terreno en el mercado del gobierno federal de los E.E.U.U. y los portadores asiáticos de comunicaciones. El gobierno federal piensa incluir soporte IPv6 para sus redes antes del 2008.

El nuevo portal go6 incluye información más comprensiva sobre IPv6 en la web. Fue creado por Hexago, un vendedor canadiense de IPv6. Cuenta con experiencia en la implementación y aplicación de IPv6. Nos proveen acceso a las últimas herramientas e informaciones sobre la nueva versión del Protocolo de Internet.

A pesar de que IPv6 fue diseñado para ofrecer una seguridad mejor que Ipv4, la seguridad sigue siendo una edición en nuevas instalaciones debido a la escasez de las herramientas de seguridad para estos protocolos. Para ello podemos hacer uso de los cortafuegos (firewall) actuales.

Características de la IPv6

Quizás las principales características de la IPv6 se síntetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatiblidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma.
- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.

Ipv6 hoy en día, ha generado una buena expectativa, esta nueva versión del Protocolo de Internet está destinada a sustituir al estándar IPv4, la misma que cuenta con un límite de direcciones de red, lo cual impide el crecimiento de la red, por lo que la IPv6 aparece con el gran objetivo de complementar, y a la larga reemplazar, el protocolo IPv4 que usan la mayoría de servicios de internet para operar hoy en día en la red. La preparación para IPv6 tiene carácter urgente ya que se alcanzó el límite de las direcciones IPv4 disponibles por la Autoridad de números asignados para internet.

1.12. Lynis

Según, PÉREZ Ignacio, Aprende a Auditar La Seguridad, Año 2014. Pág. 7. Es una herramienta de seguridad diseñada para sistemas tipo Unix (Linux, FreeBSD, OpenBSD, PcBSD, Mac OS X, Solaris), que permite examinar su configuración, en la busqueda de posibles vulnerabilidades, convirtiéndose además en un interesante complemento a los módulos de seguridad que proveen AppArmor o SELinux, así como aplicaciones específicas del estilo de Rkunter o Chkrootkit.

Lynis no sólo nos muestra los defectos de seguridad que podemos tener en nuestro equipo, sino que también nos informa de la configuración general del sistema, los paquetes instalados y posibles errores de configuración, abarcando un gran cantidad de datos: boot loaders, networking, virtualización, criptografía, memoria y procesos, configuración de impresoras, firewalls (iptables, pf), kernel, usuarios/grupos, bases de datos.

Según, MARTÍNEZ Lorenzo , Herramienta De Auditoría Para Hardening *NIX Año 2010 Pág. 5. Lynis es una herramienta de seguridad que ha sido diseñada para auditar sistemas operativos basados en UNIX. Examina la configuración del sistema y busca vulnerabilidades que puedan ocasionarnos problemas. Es importante destacar que Lynis no arregla los fallos que pueda encontrar, ya que eso es trabajo del administrador del sistema.

Si existe una herramienta capaz de buscar vulnerabilidades automáticamente, que nos puede ayudar bastante al momento en que estemos verificando nuestro sistema en busca de fallas de seguridad, esta herramienta se llama Lynis.

Según lo expuesto por los autores Lynis es una herramienta de sistema y auditoría de seguridad para sistemas basados en Linux, Mac OS y Unix que proporciona información detallada en lo bien que un sistema está y lo que puede hacer para mejorar sus defensas. El software es de código abierto y de uso gratuito, se actualiza de forma regular, para mantenerse al día con las nuevas tecnologías y mejorar las existentes, Con Lynis en su núcleo, tiene la seguridad de software actualizado estable y regular.

1.13. Normas Iso

Según, INTERNATIONAL ORGANIZATION OF ESTANDARDIZATION). ISO/IEC 27001:2005. http://www.iso.org/iso/catalogue_detail?csnumber=42103, Citado el 24 de 20ISO / IEC 27002: cubre todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). ISO / IEC 27001: 2005 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información documentado en el contexto de los riesgos globales de negocio de la organización.

- Usar dentro de las organizaciones para formular requisitos y objetivos de seguridad.
- Utilizar dentro de una organización, como marco para el proceso de implementación y gestión de controles para asegurar que se cumplan los objetivos específicos de seguridad de una organización.
- Identificación y clarificación de los procesos de gestión de seguridad de la información existentes.

Según lo expuesto reúne todos los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) Su origen en la norma BS 7799- 2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

1.14. IpTables

Según, PERPIÑAN Antonio, En Seguridad de Sistemas GNU/Linux, Año 2011, Pág. 23. **Iptables** es el nombre de la herramienta de espacio de usuario (**User Space**, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de **NAT**. **Iptables** es la herramienta estándar de todas las distribuciones modernas de GNU/Linux

Según, MONROY Fernando, Corre Linux Corre, Año 2013, Pág. 28. IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables está integrado con el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Según los autores, Iptables es una herramienta de firewall bajo la plataforma de Linux, básicamente es un conjunto de reglas que nosotros podemos aplicarlas dentro de un servidor siendo este un script el cual según vaya ejecutando correctamente su eficiencia mejorara para el funcionamiento del firewall.

CAPITULO II

2. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

INVESTIGACIÓN RELACIONADA CON LA INVESTIGACIÓN DE CAMPO

2.1. Caracterización De La Institución

La Universidad Técnica de Cotopaxi es una institución de educación superior pública, autónoma, laica y gratuita, somos una institución alternativa con visión de futuro de alcance nacional y regional sin fines de lucro que orienta su trabajo hacia los sectores populares de campo y la ciudad. Nos esforzamos para alcanzar cada día metas superiores, planteándonos como retos, la formación de profesionales integrales en los ámbitos de pre y posgrado, el desarrollo paulatino de la investigación científica y la vinculación con la sociedad a partir de proyectos generales y específicos, con la participación plena de todos sus elementos.

La institución toma actualmente profesionales al servicio del pueblo, realizando esfuerzos para alcanza cada día metas superiores y más competitivas, contribuyendo con una acción transformadora en la lucha de alcanzar una sociedad más justa equitativa y solidaria. Es por ello que la Universidad Técnica de Cotopaxi asume su identidad con gran responsabilidad: "Por la vinculación de la universidad con el pueblo".

2.1.1. Reseña Histórica

La Universidad Técnica de Cotopaxi Extensión La Maná es el resultado de un proceso de organización y lucha. La idea de gestionar la presencia de esta Institución, surgió en el año de 1998. En 1999, siendo rector de la Universidad Técnica de

Cotopaxi, el Lcdo. Rómulo Álvarez, se inician los primeros contactos con este centro de educación superior para ver la posibilidad de abrir una extensión en La Maná.

El 16 de mayo de 1999, con la presencia del Rector de la Universidad y varios representantes de las instituciones locales, se constituye el primer Comité, dirigido por el Lcdo. Miguel Acurio, como presidente y el Ing. Enrique Chicaiza, vicepresidente. La tarea inicial fue investigar los requisitos técnicos y legales para que este objetivo del pueblo Lamanense se haga realidad. A inicios de 2000, las principales autoridades universitarias acogen con beneplácito la iniciativa planteada y acuerdan poner en funcionamiento un paralelo de Ingeniería Agronómica en La Maná, considerando que las características naturales de este cantón son eminentemente agropecuarias.

El 3 de Febrero de 2001 e constituye un nuevo Comité de Pro Universidad a fin de ampliar esta aspiración hacia las fuerzas vivas e instituciones cantonales.

El 2 de mayo de 2001, el Comité, ansioso de ver plasmados sus ideales, se traslada a Latacunga con el objeto de expresar el reconocimiento y gratitud a las autoridades universitarias para la decisión de contribuir al desarrollo intelectual y cultural de nuestro cantón a través del funcionamiento de un paralelo de la UTC, a la vez, reforzar y reiterar los anhelos de cientos de jóvenes que se hallan impedidos de acceder a una institución superior.

El 8 de mayo del 2001, el Comité pidió al Ing. Rodrigo Armas. Alcalde de La Maná se le reciba en comisión ante el Consejo Cantonal para solicitar la donación de uno de los varios espacios que la Ilustre Municipalidad contaba en el sector urbano. La situación fue favorable para la UTC con un área de terreno ubicado en el sector de la Playita. El Consejo acepto la propuesta y resolvió conceder en comodato estos terrenos, lo cual se constituyó en otra victoria para el objetivo final. También se firmó un convenio de prestación mutua con el Colegio Rafael Vásconez Gómez por un lapso de cinco años. El 9 de marzo de 2002. Se inauguró la Oficina Universitaria por parte del Arq. Francisco Ulloa, en un local arrendado.

De igual manera se gestiona ante el Padre Carlos Jiménez (Curia), la donación de un solar que el poseía en la ciudadela los Almendros, lugar donde se construyó el moderno edificio universitario, el mismo que fue inaugurado el 7 de octubre del 2006, con presencia de autoridades locales, provinciales, medios de comunicación, estudiantes, docentes y comunidad en general.

La Universidad Técnica de Cotopaxi Sede La Maná cuenta con su edificio principal en el Cantón del mismo nombre en la Parroquia El Triunfo. Barrio Los Almendros: entre la Avenida Los Almendros y la Calle Pujilí.

2.1.2. Misión

La Universidad "Técnica de Cotopaxi", es pionera en desarrollar una educación para la emancipación; forma profesionales humanísticas y de calidad con elevado nivel académico científico y tecnológico; sobre la base de principios de solidaridad, justicia, equidad y libertad, genera y difunde el conocimiento, la ciencia, el arte y la cultura a través de la investigación científica: y se vincula con la sociedad para contribuir a la transformación social económica del país.

2.1.3. Visión

En el año 2015 seremos una universidad acreditada y líder a nivel nacional en la formación integral de profesionales críticos, solidarios y comprometidos en el cambio social: en la ejecución de proyectos de investigación que aporten a la solución de los problemas de la región y del país, en un marco de alianzas estratégicas nacionales e internacionales dotada de infraestructura física y tecnológica moderna, de una planta docente y administrativa de excelencia; que mediante un sistema integral de gestión le permite garantizar la calidad de sus proyectos y alcanzar reconocimiento social.

2.2. Diseño Metodológico

2.2.1. Métodos De Investigación

Método analítico

Es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos.

El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías. Este método es aquel que, una vez analizado las razones de investigación se puede encontrar respuestas al objeto de estudio, y así dar a conocer el comportamiento de un hecho o fenómeno

RAMON, Ruiz. Historia y evolución del pensamiento científico Sinaloa México 2006 P.182 ISBN-13: 978-84-690-6369-9

Método Inductivo Deductivo

Método de indiferencia basado en la lógica y relacionado con el estudio de hechos particulares, aunque es deductivo en un sentido inductivo en sentido contrario. Deductivo constituye una característica del proceso de enfoque cuantitativo. Inductivo pilar sobre el que se apoya el enfoque cuantitativo.

Método Hipotético Deductivo

Consiste en un procedimiento que parte de unas aseveraciones en calidad de hipótesis y Busca refutar y falsear tales hipótesis, deduciendo de ellas conclusiones que deben confrontarse con hechos. Es la afirmación del problema, las cual busca desmentir tales hipótesis confrontando la realidad

AROSEMENA, Rafaella. Metodología de la Investigación. (Material Gráfico Proyectable). Ecuador: Guayaquil, (2009). 83 Diapositivas.

2.2.2. Tipos De Investigación

Investigación bibliográfica

La Investigación Bibliográfica es aquella que depende exclusivamente de fuentes de datos secundarios, o sea, aquella información que existe en documentos y material de índole permanente y a la que se puede acudir como fuente de referencia

Información tomas de partes de textos, documentos y elementos de investigación que sirven como fuente de investigación.

Investigación de campo

La investigación de campo es aquella en la que el mismo objeto de estudio sirve como fuente de información para el investigador, el cual recoge directamente los datos de las conductas observadas

Datos tomados desde la fuente de investigación las cuales va dirigida al objeto de estudiado.

EYSSAUTIER DE LA MORA, Maurice. Metodología de la investigación: desarrollo de la inteligencia. Thomson: 2006. 319 p. ISBN: 9706863842, 9789706863843.

2.2.3. Técnicas De Investigación

Encuesta

Según Arias (2006) manifiesta que "la encuesta consiste en obtener información acerca de un grupo de individuos. Constituye un test escrito que el investigador formula a un grupo de personas" (p. 43).

Instrumentos

Hemos visto necesarios utilizar instrumentos que ayuden a la recolección y recopilación de la información, y que la misma facilite el manejo de dicha información para la elaboración de nuestro proyecto de investigativo, el instrumento a aplicarse es el siguiente:

Formulario de Encuesta

Es un instrumento muy eficaz de investigación social, mediante la consulta a un determinado grupo de personas elegidas mediante una fórmula estadística, realizada con ayuda de un cuestionario que contiene preguntas cerradas, que sirve para la obtención de información.

2.3. Población

La presente investigación la hemos desarrollado tomando en cuenta una muestra de la totalidad del personal docente, alumnos de la carrera de Ingeniería en Sistemas de la Universidad Técnica de Cotopaxi.

TABLA 2.1. POBLACIÓN

INVOLUCRADOS	CANTIDAD
Profesores	5
Estudiantes	104
Total	109

Fuente: *Coordinación de Carrera*

Realizado por*: Autores*

2.4. Muestreo

La aplicación de encuestas a los estudiantes se ha realizado a través de la aplicación de la técnica del muestreo en base a la siguiente fórmula

$$n = \frac{N * O^2 * Z^2}{(N-1) * E^2 + O^2 * Z^2}$$

n= ?

N= Número de población

O= 0.5 varianza

Z= 1.96 nivel de confianza

E= 0.06 error máximo admisible

$$n = \frac{109 * 0.5^2 * 1.96^2}{(109-1) * 0.06^2 + 0.5^2 * 1.96^2}$$

$$n = \frac{109 * 0.25 * 3.84}{109 * 0.0036 + 0.25 * 3.84}$$

$$n = \frac{104.6}{1.4}$$

$$n = 74.7$$

TABLA 2.2. MUESTRA

INVOLUCRADOS	CANTIDAD
Profesores	5
Estudiantes	104
Total	109
Muestra	75

2.5. Análisis E Interpretación De Los Resultados

Para tener una visión mucho más clara sobre la investigación planteada, se vio en la necesidad de aplicar como método investigativo la encuesta, la misma que va dirigida, a personas beneficiarias del proyecto investigativo en la Universidad Técnica de Cotopaxi Extensión La Maná.

TABLA 2.3. OPERALIZACION DE LAS VARIABLES

HIPOTESIS	VARIABLE	INDICADOORES
La implementación de mecanismos de seguridad permitirá un eficaz y buen control de seguridad en el intercambio de información por parte de los estudiantes como docentes de la Universidad Técnica de Cotopaxi. Extensión La Maná	**Variable Dependiente** La implementación de los mecanismos de seguridad en el laboratorio de redes.	Confiabilidad Accesibilidad Autenticidad Flexibilidad Integridad
	Variable Independiente Un adecuado control de la seguridad en el intercambio de información por parte de las personas que usaran el laboratorio de redes de la Universidad Técnica de Cotopaxi. Extensión La Maná	Accesibilidad Autenticidad Flexibilidad

2.6. Análisis e interpretación de resultados de las encuestas dirigidas a los estudiantes de la carrera de Ingeniería en Informática y Sistemas

1.- ¿Conoce usted sobre Seguridad en Redes de comunicaciones?

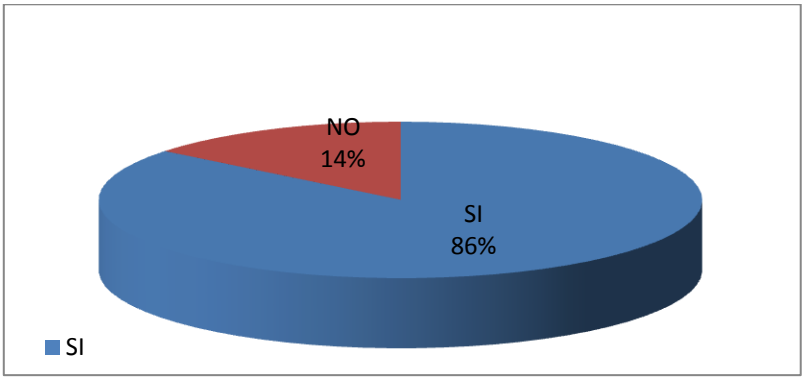
Tabla 2.4. Resultado de la pregunta N° 1

Respuesta	Frecuencia	Porcentaje
SI	**64**	**86 %**
NO	**11**	**14 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.1. Seguridad en redes



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

La mayoría de encuestados tiene conocimientos de la seguridad en redes de comunicaciones, las seguridad en una red es de mucha importancia para proteger los datos que dentro de una institución se puede generar.

2.- ¿Considera importante la implementación de mecanismos de seguridad en el laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná?

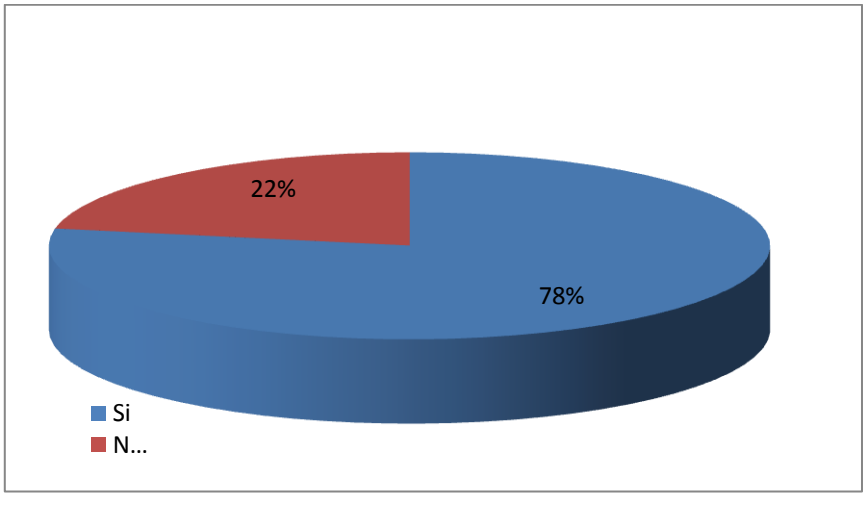
Tabla 2.5. Resultado de la pregunta N° 2

Respuesta	Frecuencia	Porcentaje
SI	**72**	**78 %**
NO	**3**	**22 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.2. Conoce los beneficios de implementación de seguridad en el laboratorio



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

La respuesta en su mayoría fue acogida por un si ya que es muy relevante el contar con los diferentes beneficios de seguridad, la misma que será empleada mediante mecanismos eficientes y eficaces en cuanto a seguridad.

3.- ¿Cree que el laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná debe tener un control permanente de seguridad?

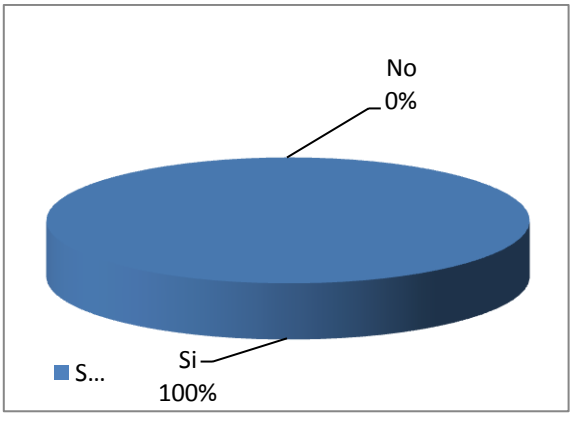
Tabla 2.6. Resultado de la pregunta N° 3

Respuesta	Frecuencia	Porcentaje
SI	**75**	**100 %**
NO	**0**	**0 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.3. El Laboratorio debe tener un control Permanente de Seguridad



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

Los encuestados están de acuerdo que exista un control permanente de seguridad laboratorio de redes ya que es la base fundamental parta el correcto funcionamiento del mismo, por lo que el 100% dijeron que si ya que en informática la seguridad es muy importante para la confiabilidad del uso de información.

4.- ¿Considera que el laboratorio de redes de comunicaciones debe contar con métodos de seguridad que beneficie la protección de la información?

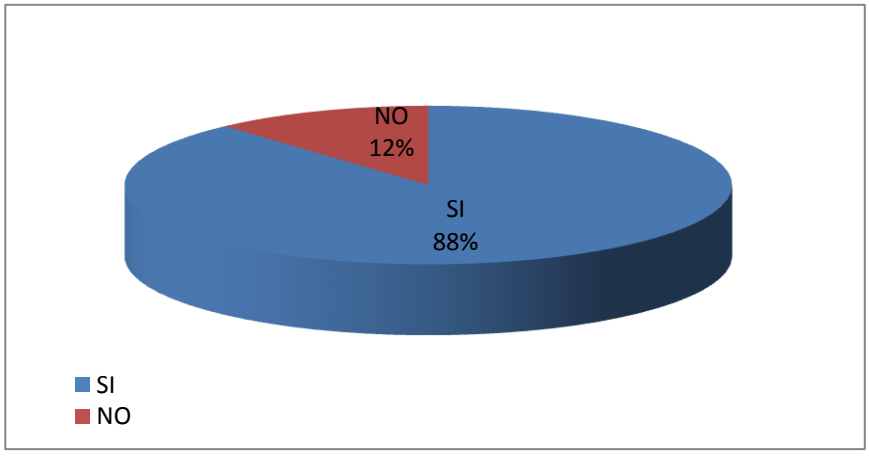
Tabla 2.7. Resultado de la pregunta N° 4

Respuesta	Frecuencia	Porcentaje
SI	**66**	**12%**
NO	**9**	**88 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.4. El laboratorio de redes debe contar con métodos de seguridad



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

El laboratorio de redes de comunicación debe tener un adecuado y exigente mecanismo de seguridad para poder salvaguardar toda la información que contenga, por lo que la mayoría de población encuestada vio como necesario el de mantener métodos correctos de seguridad para así la información esté exenta de algún peligro

5.- ¿Piensa usted que se debe salvaguardar la integridad de la información almacenada dentro del laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná?

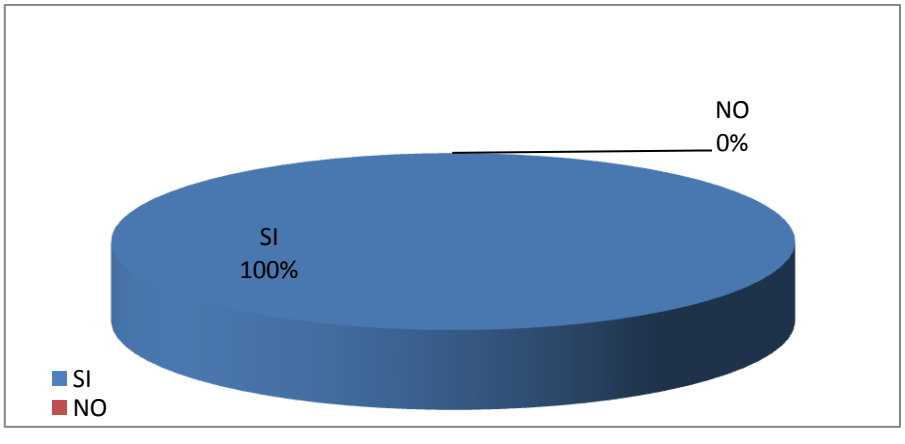
Tabla 2.8. Resultado de la pregunta N° 5

Respuesta	Frecuencia	Porcentaje
SI	**75**	**100 %**
NO	**0**	**0 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.5. Se debe salvaguardar la integridad de la información almacenada dentro Del laboratorio



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

Toda la información que contenga el laboratorio debe ser almacenada de una forma segura ya que en la actualidad se corre muchos riesgo como robo, distorsión y sabotaje, se busca implementar seguridad que proteja la integridad de la información para que sea confiable el uso de la información por parte de cualquier usuario teniendo como un rotundo 100% dicha pregunta

6.- ¿Piensa que el laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná debería tener un sistema de control para detectar y prevenir el ingreso de personas no autorizadas?

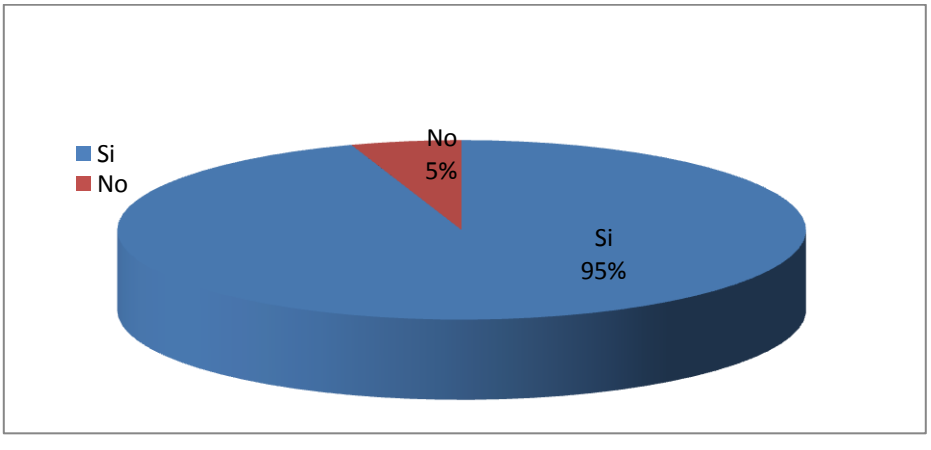
Tabla 2.9. Resultado de la pregunta N° 6

Respuesta	Frecuencia	Porcentaje
SI	**71**	**95 %**
NO	**4**	**5%**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.6. El laboratorio de redes debería tener un sistema de control para personas no autorizadas?



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

Todo laboratorio o centro de cómputo debe contar con un minucioso sistema de control para el ingreso de personas no autorizadas por lo que se tiene previsto llevar un exhaustivo control de seguridad para así salvaguardar la información y los diferentes componentes informáticos que reposa dentro del laboratorio.

7.- ¿Considera que el aprendizaje mejorara con la implementación del laboratorio de redes de comunicaciones en la Universidad Técnica de Cotopaxi Extensión La Maná?

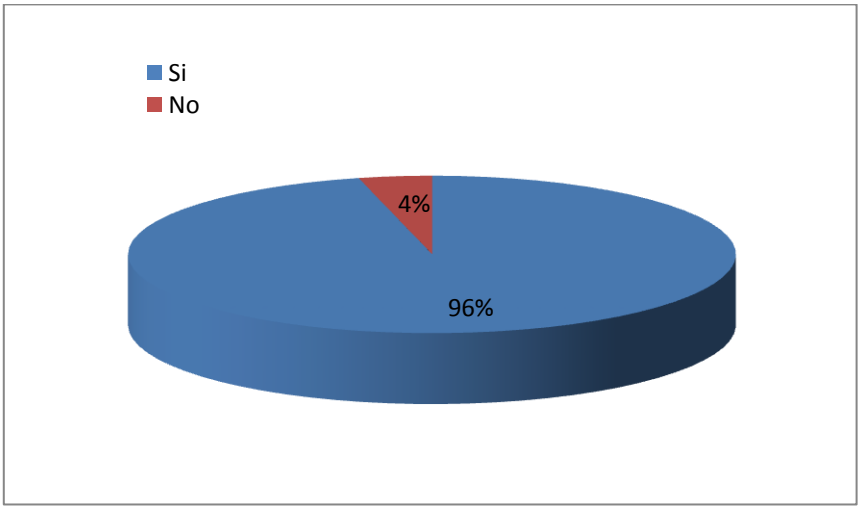
Tabla 2.10. Resultado de la pregunta N° 7

Respuesta	Frecuencia	Porcentaje
SI	**72**	**96 %**
NO	**3**	**4%**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.7. El aprendizaje mejorara con la implementación del laboratorio de redes



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

La calidad del aprendizaje es buena siempre y cuando se implemente herramientas que ayuden a adquirir conocimientos nuevos, para esto la Universidad ha implementado muchos componentes para que los estudiantes y docentes sigan aprendiendo y sigan aumentando sus conocimientos para competir en el campo profesional.

8.- ¿Cree que el laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná debe cumplir con normas y necesidades en cuanto a seguridad en redes?

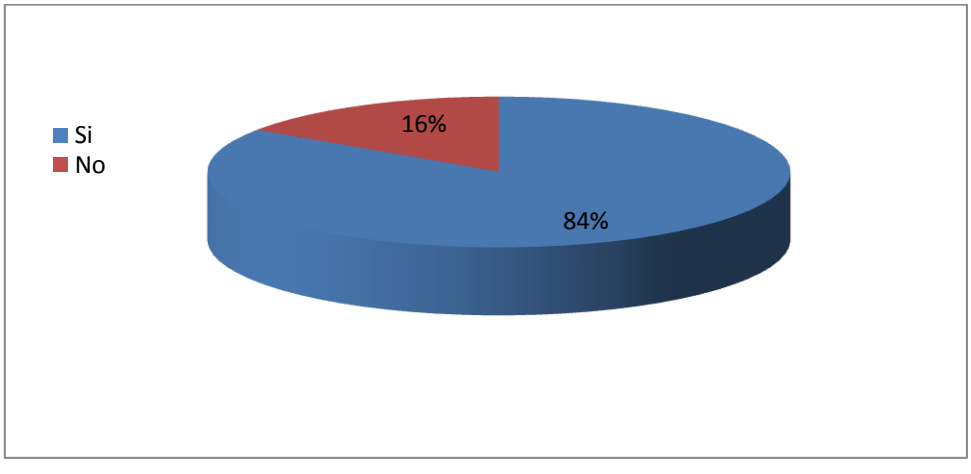
Tabla 2.11. Resultado de la pregunta N° 8

Respuesta	Frecuencia	Porcentaje
SI	**63**	**84 %**
NO	**12**	**16 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.8. El laboratorio debe cumplir con normas y necesidades en cuanto a seguridad en redes



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

En la implementación de un laboratorio debe cumplir con normas y basarse a las necesidades que la requieran para su buen funcionamiento, por lo que se propone aplicar métodos y técnicas para que el funcionamiento del mismo sea seguro eficaz y confiable.

9.- ¿Conoce cuáles son los beneficios de implementación de seguridad en el laboratorio de redes de comunicaciones de la Universidad Técnica de Cotopaxi Extensión La Maná?

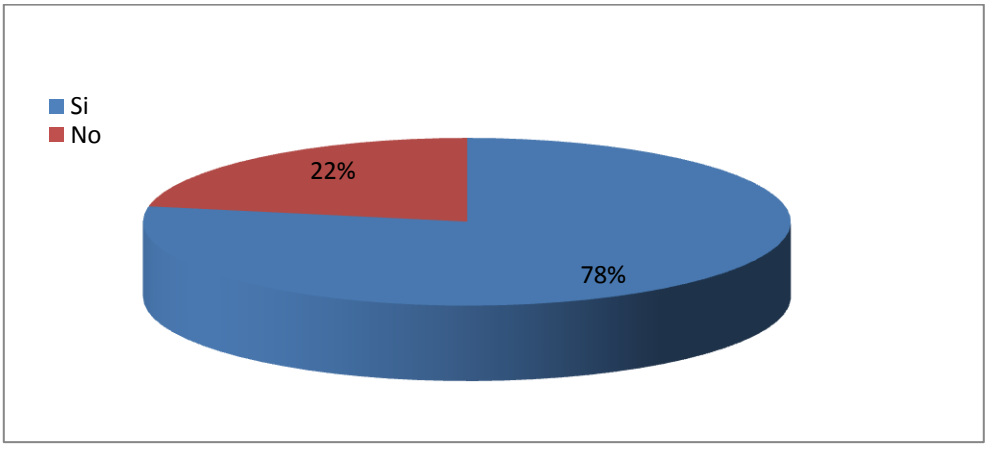
Tabla 2.12. Resultado de la pregunta N° 9

Respuesta	Frecuencia	Porcentaje
SI	**58**	**78 %**
NO	**17**	**22 %**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.9. Conoce los beneficios de implementación de seguridad en el laboratorio



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

No toda la población encuestada sabe o conoce los beneficios de seguridad del laboratorio de redes de comunicación, por lo que se ve necesario llegar de una forma muy clara para que entiendan los usuarios de los beneficios que obtendrán con la implementación de seguridad en el laboratorio de redes de comunicación.

10.- ¿Considera que la implementación de seguridad es un aspecto vital para un servidor?

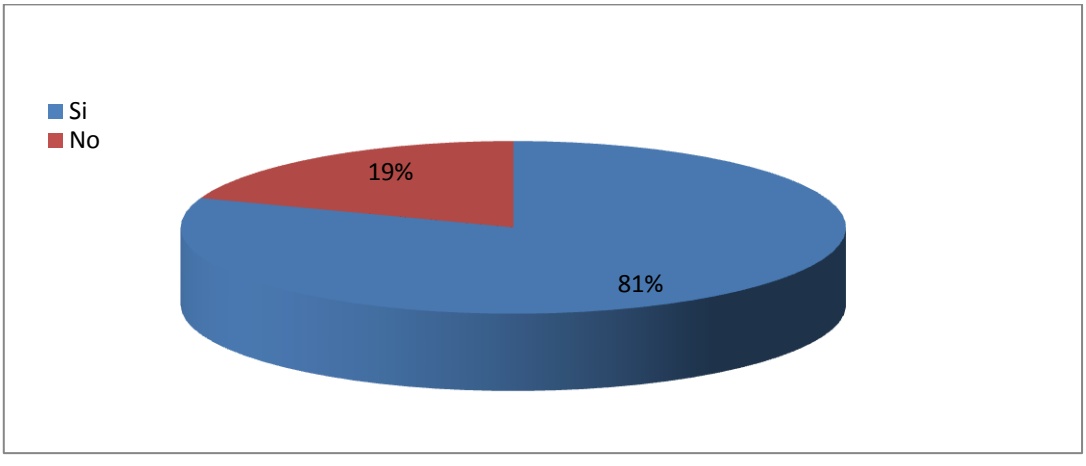
Tabla 2.13. Resultado de la pregunta N° 10

Respuesta	Frecuencia	Porcentaje
SI	**60**	**81%**
NO	**15**	**19%**
TOTAL	**75**	**100 %**

Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Grafico 2.10. Conoce los beneficios de implementación de seguridad en el laboratorio



Fuente: *Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Interpretación de Resultados

Los beneficios de la seguridad se los podrá palpar luego de la implementación para esto utilizaremos las herramientas y servicios que el servidor analizaremos métodos y técnicas de seguridad para la implementación las mismas que estén catalogadas en la actualidad como necesarias veremos cuál de ellos sean las necesarias.

2.7. Hipótesis

La hipótesis planteada en nuestro trabajo de investigación fue la siguiente: **“ IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD QUE PERMITIRÁ UN EFICAZ Y BUEN CONTROL DE SEGURIDAD EN EL INTERCAMBIO DE INFORMACIÓN POR PARTE DE LOS ESTUDIANTES COMO DOCENTES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI. EXTENSIÓN LA MANÁ”**

Con miras a comprobar la hipótesis se realizó la técnica mediante encuesta y se elaboró los respectivos cuestionarios. Los resultados obtenidos fueron analizados interpretados, tal manera que:

El 100% del personal Docente como el estudiantil consideran que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasmitir su información, el 100% tanto del personal docente como del estudiantil piensa que la infraestructura de red del laboratorio de redes de la Universidad Técnica de Cotopaxi extensión La Manà debería tener mecanismos de seguridad que beneficia la protección de la información y el 100% del personal docente está de acuerdo con la implementación de mecanismos de seguridad para fortalecer la confidencialidad e integridad de la información, con dichos resultados se pudo verificar que la hipótesis es verdadera, lo que hace necesario Implementar mecanismos de seguridad para contrarrestar los problemas y vulnerabilidades dentro del laboratorio de redes de la Universidad Técnica De Cotopaxi Extensión La Maná.

CAPITULO III

3. PROPUESTA

EVALUACIÒN DE LOS ATAQUES DE NAVEGACION DE SERVICIOS Y FORMAS DE PROTECCIÒN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÈCNICA DE COTOPAXI EXTENSIÒN LA MANÀ.

3.1. Presentación

Las organizaciones cada vez se encuentran expuestas a ataques desde el interior por parte de los usuarios como también del exterior, lo que permiten es determinar cuáles de los ataques son los más peligrosos. Toda vez que los usuarios de la información buscan beneficio personal o a su vez perjudicar a alguien, estos son los considerados ataques de afectación a terceros, que en muchos de los casos dañan a personas o instituciones

Por otro lado se tiene los que son externos aquellos que lo hacen personas que buscan en cambio perjudicar a la empresa ya sea por alterar la información o eliminarla directamente, estos casos son los casos que hay que en lo posible prevenir mediante Software y Hardware de seguridad, que a su vez ayuden a limitar a los intrusos en su intento de ofensiva dañina de información que en ocasiones puede ser incluso de equipos informáticos.

Como parte de la investigación a efectuarse en la Universidad Técnica de Cotopaxi Extensión La Maná se plantea la presentación de ataques y sus posibles defensas siendo estas las que podrían abarcar la mayoría del caso de estudio, ya que se puede aplicar muchas técnicas de seguridad pero como es de conocimiento hay que determinar cuáles son los ataques y con qué herramientas nos podemos defender y si es posible atacar como medio de disuasión a los posibles hackers.

Las vulnerabilidades informáticas desde siempre han sido un dolor de cabeza en toda institución, sea está pública o privada y lo único que se ha podido hacer es instalar y configurar varios mecanismos de seguridad como medida preventiva.

Basados en esta presentación se tratara de demostrar que los ataques pueden ser prevenidos con métodos y herramientas que en la actualidad no cuenta en el laboratorio de redes de comunicación de la Universidad Técnica de Cotopaxi Extensión La Maná.

3.2. Objetivos

3.2.1. Objetivo General

Implementar mecanismos de seguridad para contrarrestar los problemas y vulnerabilidades lógicas dentro del laboratorio de redes de la Universidad Técnica De Cotopaxi Extensión La Maná.

3.2.2. Objetivos Específicos

- Recopilar la información bibliográfica para determinar los tipos de ataques informáticos a los que puede estar expuesto laboratorio de redes y comunicación de la Universidad Técnica De Cotopaxi Extensión La Maná.

- Analizar la documentación relacionada con los mecanismos de seguridad para saber los problemas y necesidades que tienen en el laboratorio de redes y comunicación de la Universidad Técnica de Cotopaxi Extensión La Maná.

- Aplicar mecanismos de seguridad que permitan asegurar la confiabilidad e integridad de un buen manejo del laboratorio de redes y comunicación de la Universidad Técnica de Cotopaxi Extensión La Maná.

3.3. Análisis de factibilidad

Las factibilidades se las miden de acuerdo al grado de cumplimiento o no que tenga un proyecto razón por la cual se plantea la creación de una análisis minucioso de posibles ataques y sus mecanismos de defensa dentro de la realidad que tiene los laboratorios de Redes y Mantenimiento de la Universidad Técnica de Cotopaxi Extensión La Mana, al tener equipamiento de última tecnología, y que estas puedan tener un nivel de control de seguridades a nivel de redes y servidores, tanto para equipos con software propietario como de software libre.

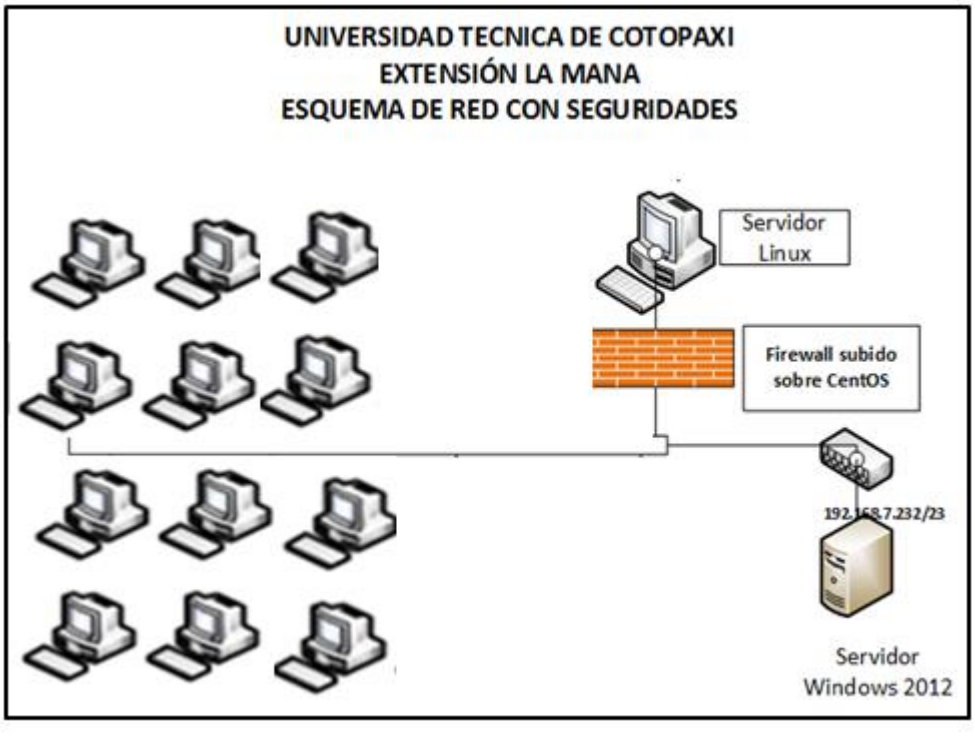
Como se ha podido observar en los primeros capítulos de la investigación se trató de algunas formas de ataque entre otros los virus informáticos que son los que en la actualidad son de mayor divulgación, pero que al tener un control como los contratados un buen sistema de control de virus o llamados también Antivirus, este licenciamiento ayuda al control de las seguridades tanto a nivel de dispositivos de almacenamiento como de páginas web de dudosa procedencia.

3.3.1. Factibilidad Técnica

El proyecto es considerado como factible técnicamente toda vez que se cuenta con equipos de última generación los mismos que se pueden tornar en ocasiones como equipos servidores como es el caso de un computador de los laboratorios que asume las veces de PC Server y que por sus características y almacenamiento así como rendimiento puede cumplir sin ninguna complicación, es importante notar que nosotros como mecanismos de defensa vamos a tomar en cuenta la implementación de un servidor de Firewall el mismo que ayudaría en la prevención de posibles ataques y de esta misma herramienta podría a su vez administrar toda la información que se envía y se recibe en este servidor de seguridades.

Técnicamente el servidor de Firewall puede ser tanto en software como en hardware y la mayoría de estos equipos están basados en el sistema operativo Unix es decir de una u otra manera el Linux es la mejor de las alternativas ya sea por administración, costos, o por la facilidad que se tiene al momento de su instalación, definición de parámetros, la misma administración es mucho más amigable por la personalización de las reglas del juego, que no es otra cosa que cuando podemos enviar y cuando podemos recibir información a través de que protocolos, cuantos puertos tenemos abiertos, cuantos puertos deben y tienen que estar cerrados , incluso se debería tomar en cuenta los tiempos que se deben estar arriba las comunicaciones para precautelar que el uso de los recursos se lo haga de forma ordenada y siempre apuntando a que se cumpla con la optimización de los recursos materiales y económicos.

GRAFICO 3.1.Esquema del laboratorio de redes



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

En la imagen se puede observar que el laboratorio se encuentra equipado con dos servidores, los mismos que por administración de recursos tecnológicos se tiene configurados los sistemas operativos Windows 2012 Server, en el cual se tiene las configuraciones necesarias para la administración del Active Directory, se tiene el concentrador que es el que distribuye el flujo de la red desde los equipos servidores hacia los clientes.

Se tiene un enrutador cisco que tiene la capacidad de administrar por sí mismo la información que se genera a través de una red para pasarla a otra y que estas puedan a su vez tener el servicio que dispone la extensión y que está dado por las configuraciones desde Latacunga (Universidad Técnica de Cotopaxi sede Matriz).

3.3.2. Factibilidad Operativa

Operativamente las seguridades en los servidores y las redes de comunicaciones deben ser dadas por un equipo que sirva de administrador ya que este debería servir de filtro entre los hackers, crackers, piratas informáticos, que son los que desarrollan algunas técnicas avanzadas para evadir cualquier sistema de detección de intrusos e intrusiones.

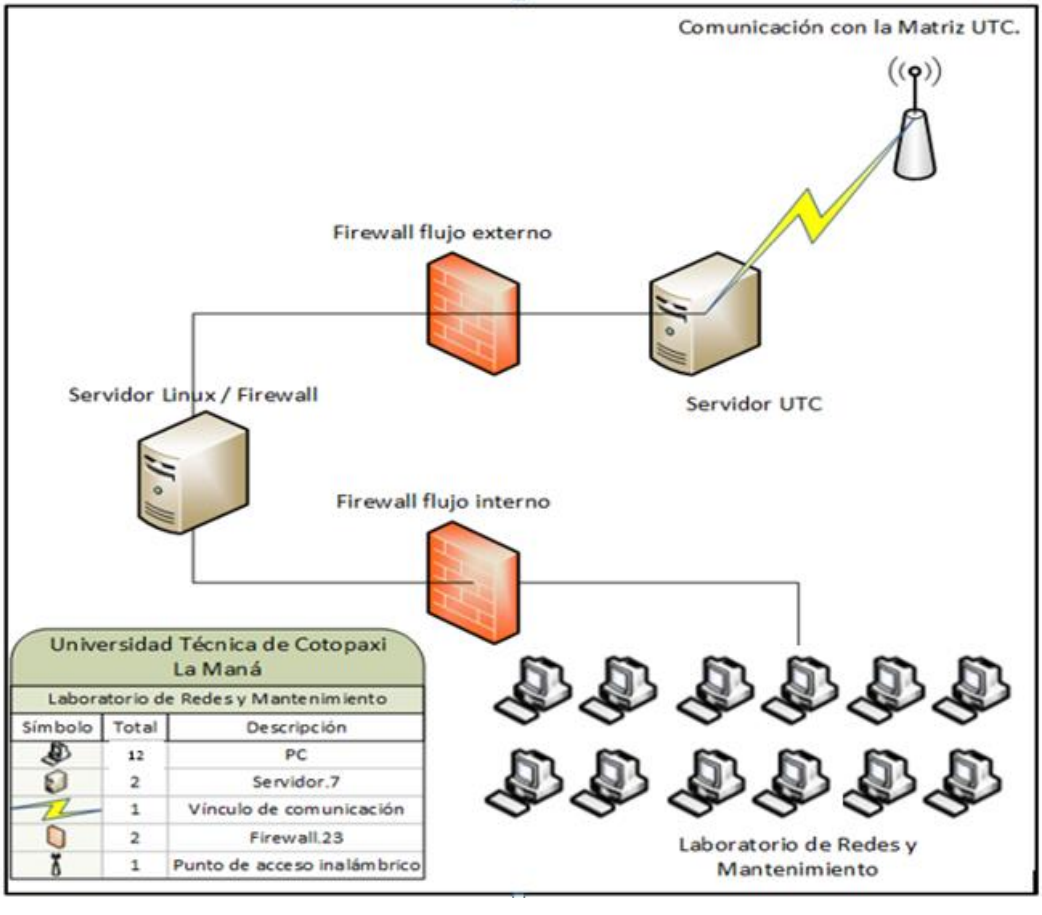
Se tomó como caso de estudio el laboratorio de redes y mantenimiento de la Universidad Técnica de Cotopaxi extensión La Maná, para poder realizar la implementación de herramientas de seguridad que ayuden en la administración para la detección y control de los recursos de la red particularmente de los servidores que son los más vulnerables en un ataque informático, y de igual manera que se pueda controlar si existe algún tipo de tráfico en la red que tenga un patrón de ataque.

El principal objetivo de este proyecto es brindar al laboratorio de redes y mantenimiento un análisis a las seguridades y recomendar el diseño de seguridades que incluyen los servidores y clientes que se tienen y que pueden ser utilizados por los estudiantes de la carrera de Ingeniería en informática y Sistemas

Computacionales, para que en un futuro cercano puedan diseñar seguridades en las topologías que estén incluidos equipos y herramientas que protejan de posibles ataques informáticos no solo para prevenir ataques externos desde el internet o los internos que también son de gran aplicación.

Entonces al plantearnos un firewall que es el medio que sirve para regular el acceso a la red, y que este nos sirva para controlar y registrar los intentos de acceso, y con este se tiene en cuenta la dirección IP del cual origina el intento. Entonces el firewall decide si acepta o no la solicitud pone las reglas y políticas de configuración del firewall.

GRAFICO 3.2. Comunicación con la Matriz de la Universidad técnica de Cotopaxi - Latacunga



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Dentro del laboratorio para la aplicación de la investigación se tiene equipos que conforman este diseño que es planteado por la Universidad y que desarrollamos para poder precautelar la información, y que esta sirva de alternativa para las futuras generaciones dentro de la carrera de Ingeniería en Informática y Sistemas Computacionales.

3.3.3.. Factibilidad Económica

El firewall actual como un filtro entre el servidor y los clientes; entre el servidor y el internet; bloquea los intentos malintencionados para el acceso a la información de la institución y permite el paso solo al tráfico legítimo.

Al tener en cuenta que la Universidad es una institución pública y según el mandato 1014 de la presidencia de la República del Ecuador en la cual se pide se fomente la aplicación de software libre, se planteó la configuración de un servidor de Firewall. Con la utilización de software libre y utilizando los recursos que se tiene en el laboratorio de redes y mantenimiento utilizando sus recursos materiales, con la finalidad de optimizar el recurso económico, hay que notar que los equipos que aquí se tiene son de la más alta calidad tecnológica, y que pueden cumplir con normalidad cualquier actividad que se lo requiera.

Para el desarrollo del proyecto se usó equipos para administración de redes que cumplen con la función que se requiera y que estos pueden formar parte de las necesidades que tiene la Universidad en su camino a la excelencia educativa.

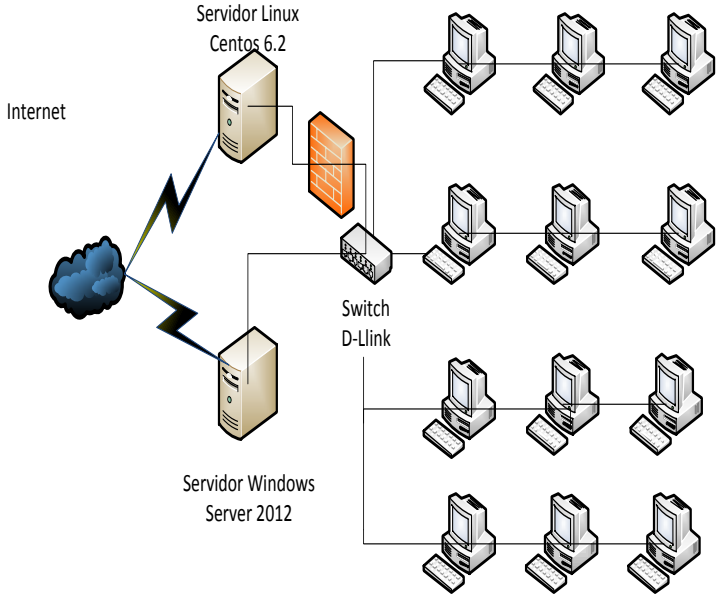
Por lo tanto el proyecto es viable económicamente ya que no se requiere de licencia alguna para el software que se va a utilizar al ser Linux CentOs 6.2, sobre todo que la inversión en el laboratorio se lo realizo para muchas otras actividades.

3.4. Diseño de la Propuesta

Para la implementación de la propuesta detallamos los equipos que se van a tener y como estos pueden afectar al momento de generar la información, pero es importante notar que para nuestro caso se desarrollara un diseño que partirá de que la investigación es en base a la realidad de un laboratorio que forma parte de una institución educativa y que las comunicaciones y las reglas de comunicación los van a dar los administradores de la red de la institución.

Según la planificación el equipo Firewall planteado tendrá que servir de filtro entre las comunicaciones entrantes desde la red de la matriz de la Universidad que es la que conecta con el internet y las redes WAN para los otros servicios, y la red que comunica entre el ruteador de la Universidad con el del laboratorio de redes y mantenimiento de la extensión de la Maná

GRAFICO 3.3. Planificación de Firewall planteado



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

3.4.1. Requerimientos de la propuesta

Para la elaboración del firewall se utilizara todo el recurso existente en los laboratorios de redes y mantenimiento de la Universidad Técnica de Cotopaxi extensión La Maná.

- El cableado estructurado
- El servidor de dominios sobre Windows 2012 server
- Manuales de instalación y administración del mismo
- El servidor de Linux Centos 6.2
- Entre otras actividades.

GRAFICO 3.4. Equipos y Componentes Informáticos

EQUIPOS	CANTIDAD	HARDWARE	SOFTWARE
Servidor HP	1	Intel Xeon, 8 Gb de memoria RAM, 1 Tb en Disco duro, Hot Swap.	Windows 2012 / Virtualización mediante Citrix
Computadores HP / PC Server	1	Modelo Pro Desk con procesador Intel Core i7, 8 Gb de memoria RAM, 1 Tb de disco duro, unidad de DVD RW.	Linux CentOS 6.2., herramientas de seguridad y administración de un servidor..
Router Cisco	1	Cisco serie 2900	IOS de Cisco
Switch D-LINK	1	D – Link	Software base de la empresa D-Link.
Cableado	1	Categoría 6	N/A
RAC	1	48 puertos	
Computadores HP ProDesk	15	Modelo Pro Desk con procesador Intel Core i7, 8 Gb de memoria RAM, 1 Tb de disco duro, unidad de DVD RW.	Windows 7, Ms Office 2010.

Tabla 3.1: *Inventario de equipos del laboratorio de redes y mantenimiento*

Realizado por: *Autores*

3.5. Desarrollo de la propuesta

Para la toma de seguridades en la red de los laboratorios los vamos a tomar el firewall para lo que es el IPv4 mientras que el IPSec para la encriptación de la información en lo protocolos de comunicación de internet IPv6.

Ya que la identificación de los riesgos de seguridad para la red interna de la Universidad, tal como se expuso en las factibilidades, proporcionan un punto de partida para tomar decisiones que si es o no necesario configurar un Firewall, y si este se conectara a una red pública como sería el caso de la red de la Universidad que a través de esta se sale al internet.

Dirección IP: 192.168.7.232

Mascara de Subred: 255.255.240.0

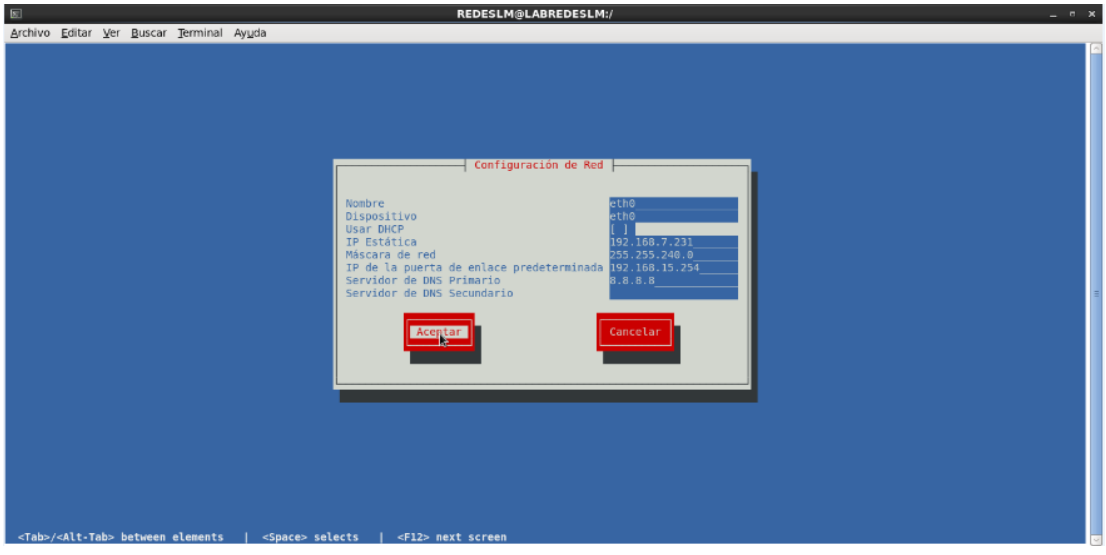
Gateway: 192.168.15.254

DNS Primario: 8.8.8.8

DNS Secundario: 201.107.10.62

Y según desprende la configuración del servidor de administración de la red de la plataforma Linux que va a ser la que se tomara en cuenta para la elaboración del firewall.

GRAFICO 3.5. Configuración de Red en Centos 6.2

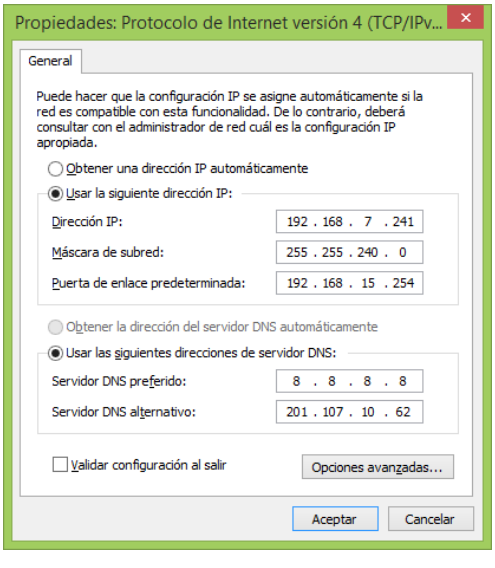


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez configurada la red y teniendo en cuenta que se sabe cómo se quiere encaminar la red dentro del sistema de red de la Universidad y que se tiene las configuraciones dadas de la siguiente manera:

GRAFICO 3.6.Configuración de la red en Windows 7



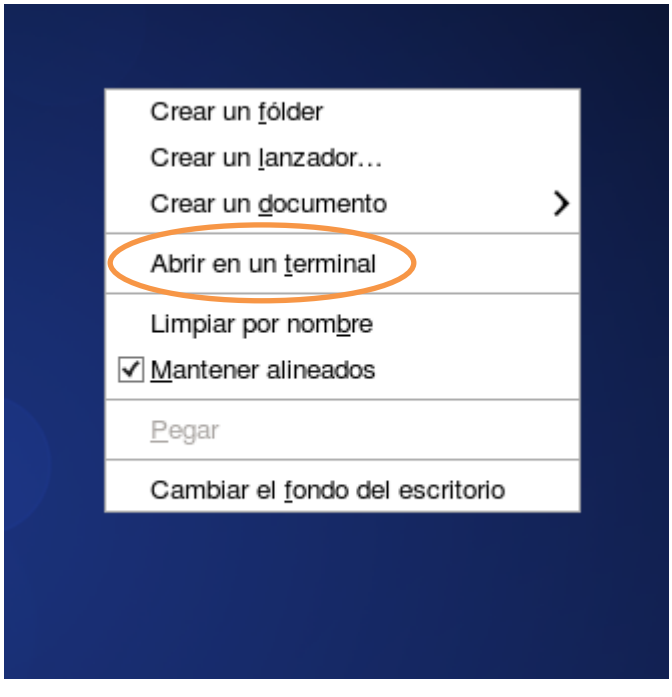
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Las configuraciones estuvieron dados por el parámetro indicado por la Universidad para el laboratorio, no se permitió el enrutamiento con una red distinta por lo que las reglas del firewall serian dadas de acuerdo a lo que se requiera de parte de los asesores del laboratorio y de la configuración de las redes de datos en el sentido que se permitirá solamente lo que se considere necesario para estas actividades.

Todos los firewall sean estos basados en Linux de cualquiera de sus versiones, tiene que estar dados básicamente a reglas que las debe dar el iptable, que es en donde se configurara todas las reglas para que se puedan restringir o permitir según sea el caso de cada uno de los administradores, o por considerarlo o no pertinente el docente a cargo de llevar a cabo una clase demostrativa que es para lo que se está diseñando.

GRAFICO 3.7. Abrir terminal en Centos 6.2

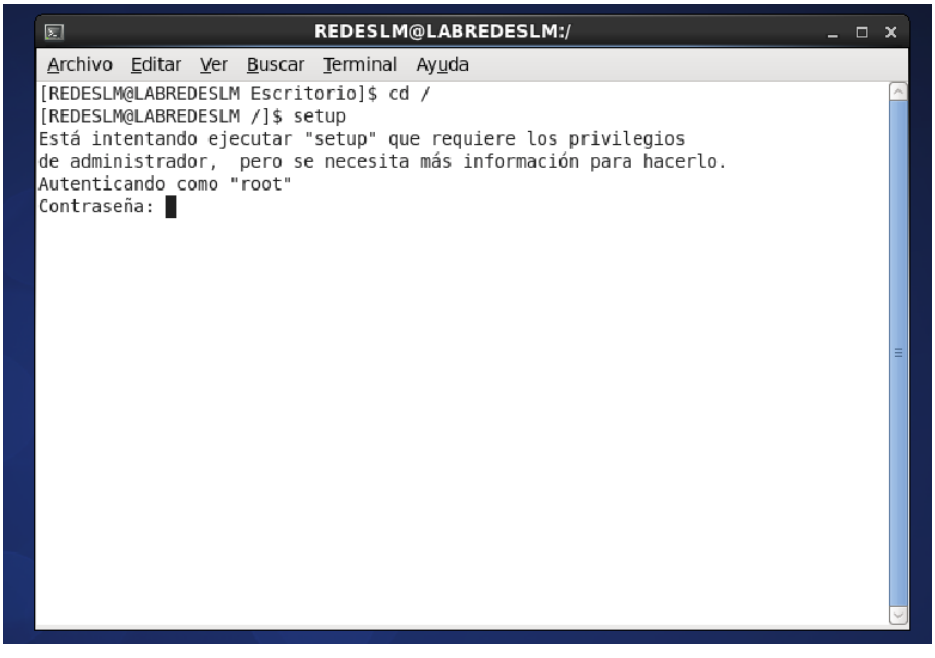


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Linux es una plataforma que tiene su parte grafica que más adelante veremos cómo funciona pero que una de sus fortalezas es la administración mediante comando dentro de terminal de comandos que tienen algunos comandos que son fáciles de aplicarlos y que son concretos para cada trabajo que hay que realizar, aquí podemos ver como ingresar al menú de herramientas con los siguientes comandos (cd , setup) luego pedirá el ingreso de contraseña.

GRAFICO 3.8. Pantalla principal comando cd e ingreso al setup



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Luego de configurar bien las redes de los equipos y el servidor se procede con la seguridad de la red que no es otra cosa más que el nivel de seguridad que garantiza el funcionamiento de todas las computadores y sus equipos electrónicos que estén en una red sea optimo y que todos los usuarios posean los privilegios necesarios para realizar las actividades que correspondan.

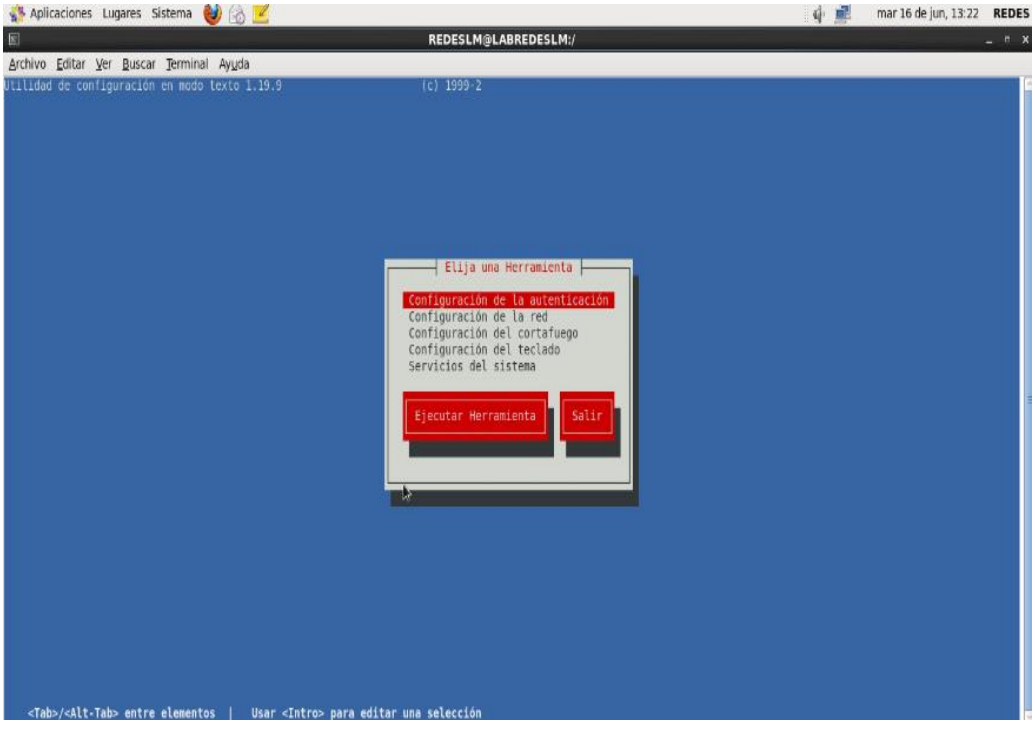
Para la seguridad y porque debemos tener activado el firewall se tiene las siguientes actividades:

- Evitar que personas que no tiene autorización intervenga en el sistema con fines de alterar o eliminar la información
- Evitar que los usuarios por desconocimiento realicen actividades u operaciones involuntarias que puedan dañar al sistema.

- Asegurar los datos ante potenciales fallos de sistema, o de problemas alternativos y que por fuerza mayor puedan causar daños

- Garantizar que no se interrumpan los servicios.

GRAFICO3.9. Menú de herramientas



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Por tema de investigación y como alternativa de seguridades dentro de la planificación se tuvo en cuenta las configuraciones del IPSec para asegurar las comunicaciones mediante encriptación de la información en la red de datos, es decir cuando sale de un host y hasta llegar a otro.

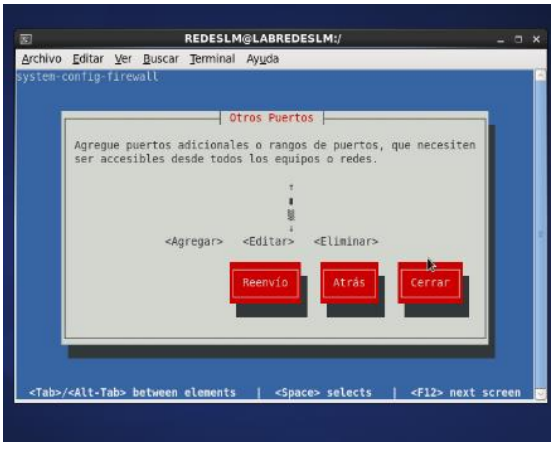
GRAFICO3.10.Activación de Ipsec

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Luego de las configuraciones generales del IPSec se requiere la asignación de los puertos mediante configuraciones personalizadas.

GRAFICO3.11. Servicios de firewall



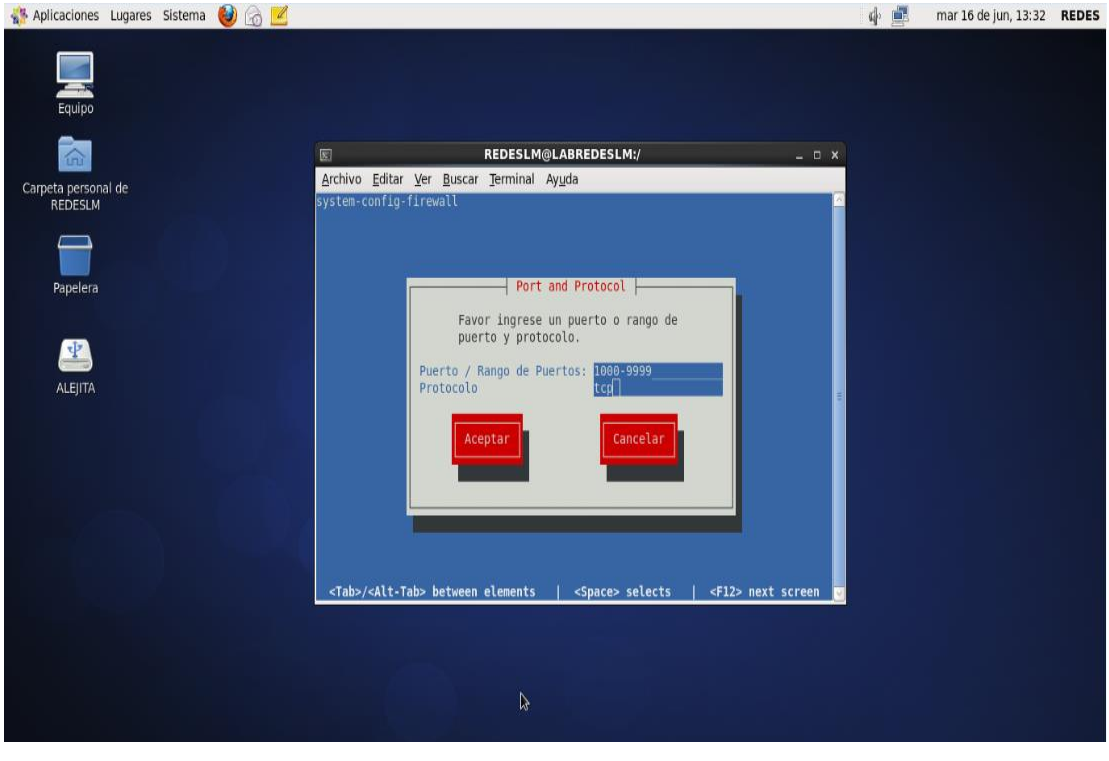
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Dentro de los puertos que se van a proceder a cerrar se decidió tomar en cuenta las actividades que se desarrollaran en este laboratorio y entre otras estas las siguientes:

- Cableado estructurado
- Mantenimiento preventivo de computadores
- Instalación de servidores Windows
- Instalación de servidores Linux
- Administración de servidores de las dos plataformas
- Configuraciones de concentradores y enrutadores
- Administración de concentradores y enrutadores

GRAFICO 3.12. Puertos y Protocolo



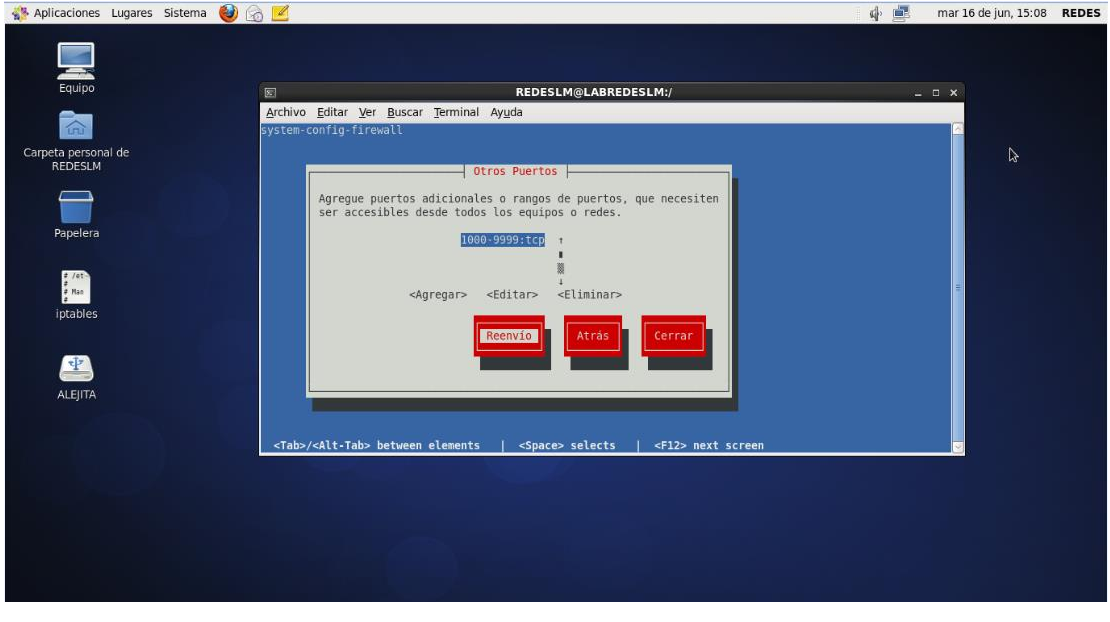
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Para el caso de la Universidad se deciden habilitar los puertos del 1000 en adelante para que se pueda realizar prácticas de los estudiantes como páginas web a través del apache y su puerto 80, o de las páginas web seguras como es el caso del 443, entre otras actividades, que son las más necesarias.

Se debe tomar en cuenta que esto solamente se lo realizo en lo que tiene que ver con el protocolo tcp y mas no con el udp para la transmisión de datagramas pero como se explicó en los puertos no sería necesario al no tener aplicativos aun dentro de este laboratorio o pensar en un futuro cercano en fusionar con otro laboratorio donde se lleve a cabo aplicativos que tengan características de ser cliente servidor y que se considere la apertura de puertos de comunicación.

GRAFICO 3.13. Agregados los Puertos y Protocolos



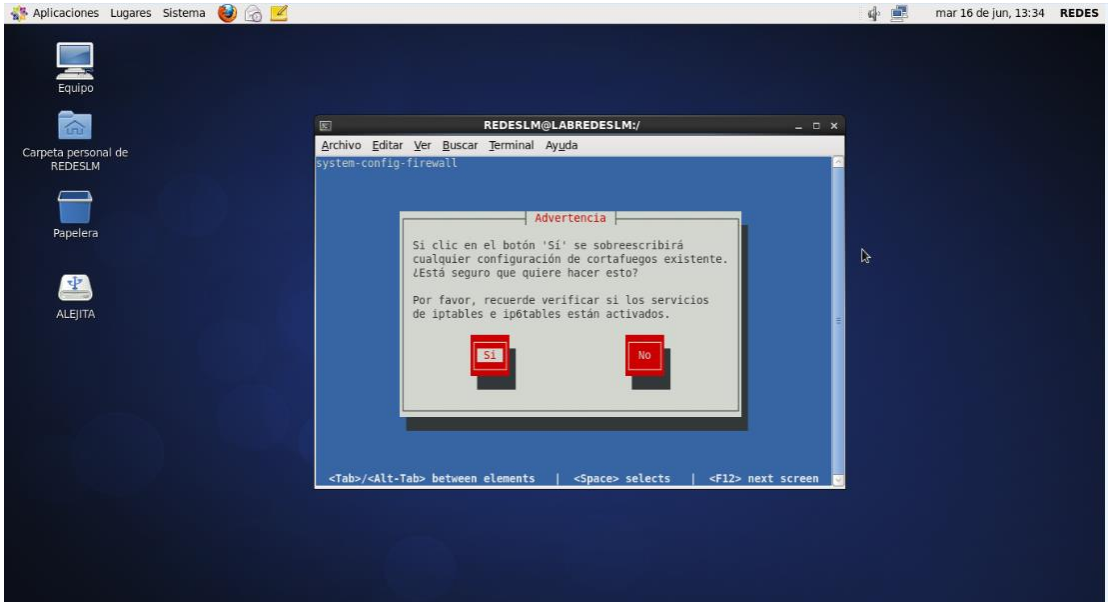
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Luego de que se selecciona las características del firewall se toma en cuenta si las configuraciones realizadas pueden o no afectar al firewall, si es el caso este debería ser activado.

Dentro de los servicios del ntsysv del Linux para que se pueda subir y entre en funcionamiento el firewall del Linux con todas las reglas que se pusieron para garantizar la información.

GRAFICO3.14. Verificación de activación de Iptables



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

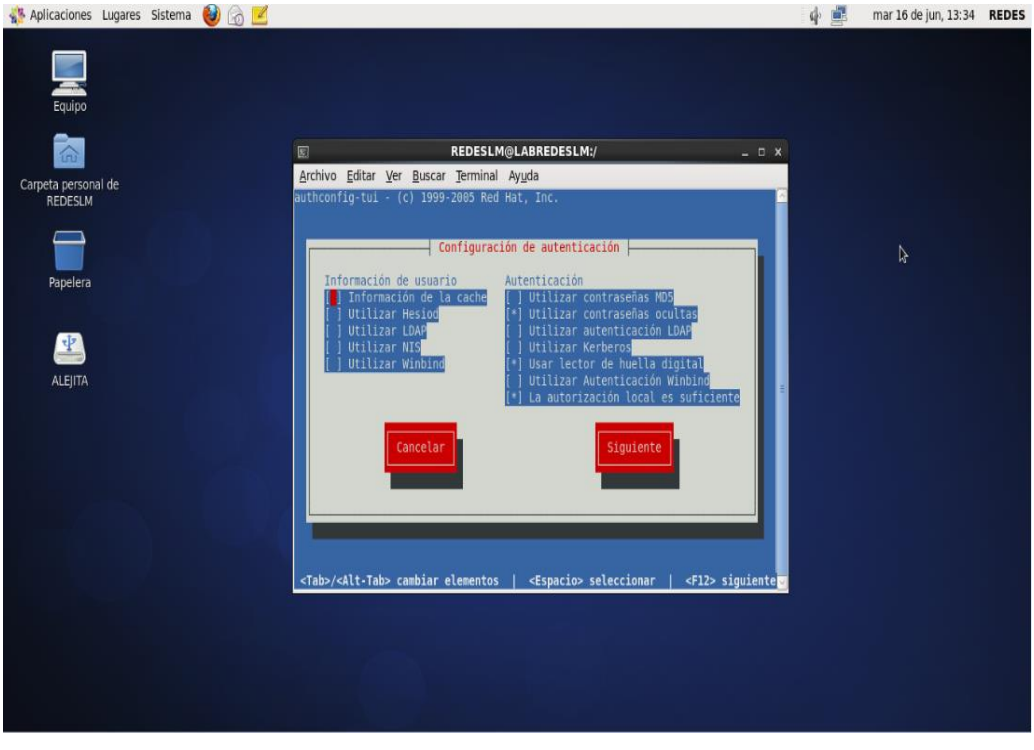
Un aspecto muy importante dentro de las configuraciones que se tienen dentro del firewall, es la encriptación, y como Linux es un software de código abierto siempre se realiza actualizaciones que estas pueden ser utilizadas cuando se lo requiera, cuidado siempre que se haga lo correcto.

Para el caso de la investigación se decidió tomar en cuenta que la encriptación de las contraseñas se lo haga mediante el algoritmo denominada MD5.

El algoritmo MD5 es una función de cifrado fijo tipo hash que acepta una cadena de texto como entrada, y devuelve un número de 128 bits. Las ventajas de este tipo de algoritmos son la imposibilidad de reconstruir la cadena original a partir del resultado.

Esto ayudaría para que todo lo que se genere dentro del sistema ayude en las seguridades que se tengan a todo nivel dentro de la plataforma de seguridades.

GRAFICO 3.15.Activación de Algoritmo para Firewall

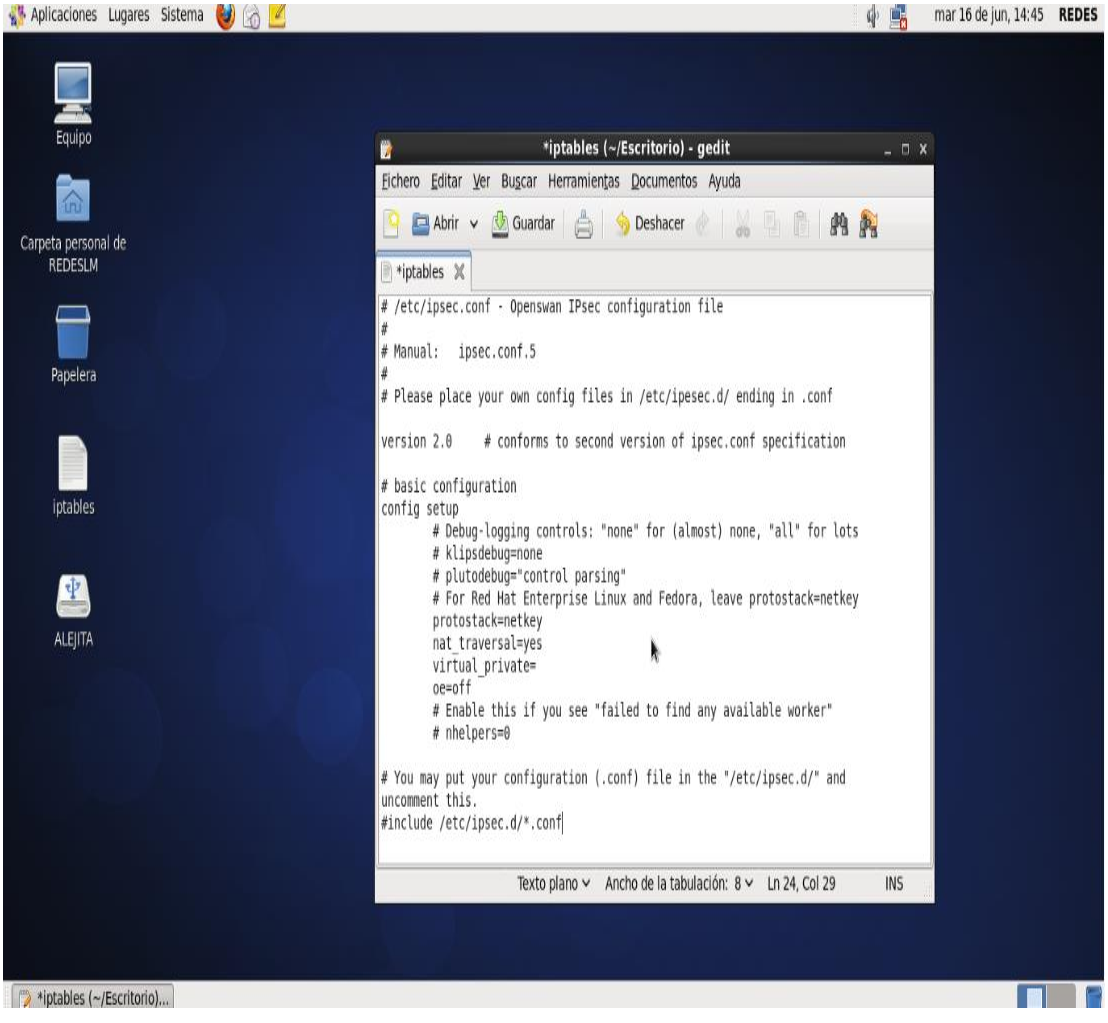


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Configuraciones del IPSec para la encriptación de las seguridades de trasmisión de la información dentro del laboratorio como medida de ataques de denegación de servicio.

GRAFICO 3.16.Código en HTML



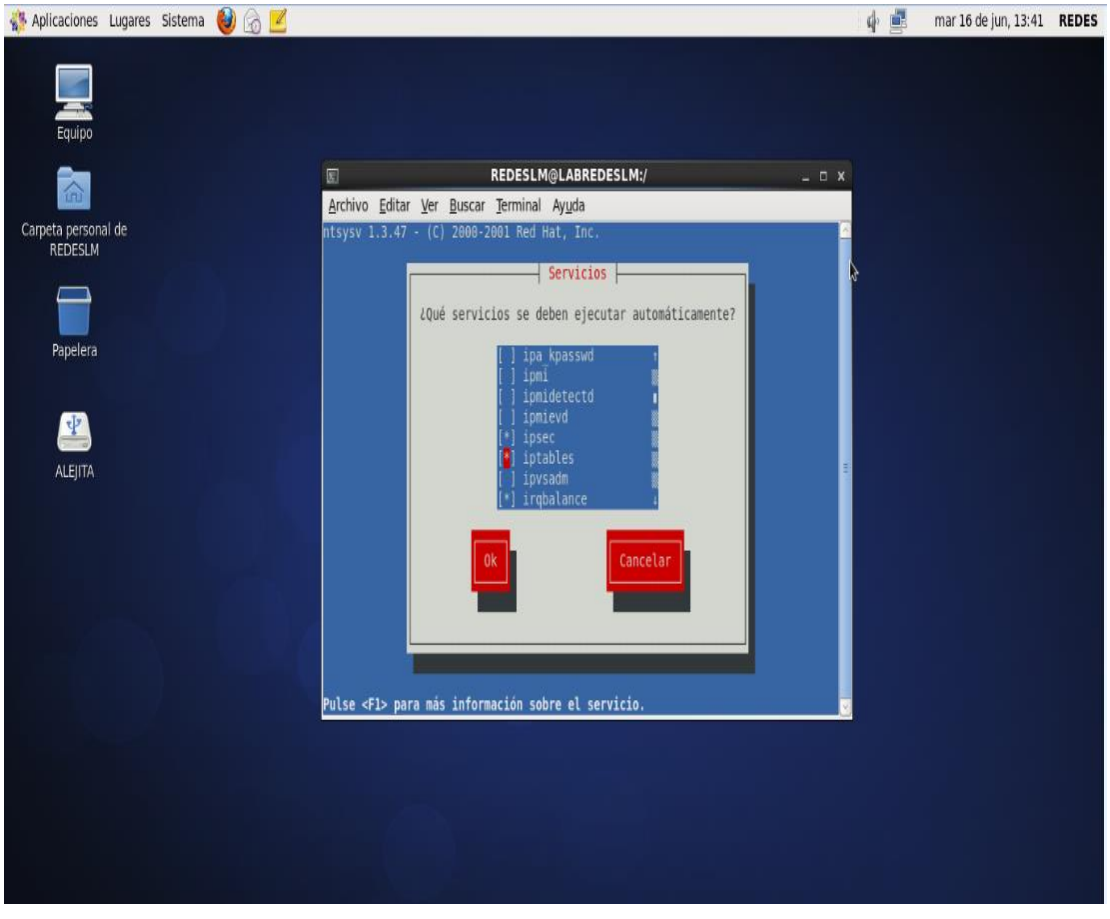
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez diseñadas las direcciones y puestas dentro del script de la IPSec se deberá tomar en cuenta para la adjudicación de los demás servicios.

El servicio del IPTable es diferenciado tanto para el protocolo IPv4 como para el IPv6, ya que a ningún momento estos se entrelazan.

GRAFICO 3.17.Activación de Servicios de IpTables



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Como se tomó en cuenta las configuraciones del IPSec, al momento de definir qué sistemas entraban en el firewall de igual manera hay que subir el servicio de IPSec dentro del ntsysv.

Ya que este es el que ayudara a que la información que se envié a través de la red vaya segura y que no pueda sufrir alteración alguna.

GRAFICO 3.18. Activación de Ipsec

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Luego de activado el servicio y definidas las reglas para el IPSec se procede a subir el servicio, si existen novedades debería darnos un error caso contrario este debería estar arriba es decir todo OK.

GRAFICO 3.19.Reseteando servicios

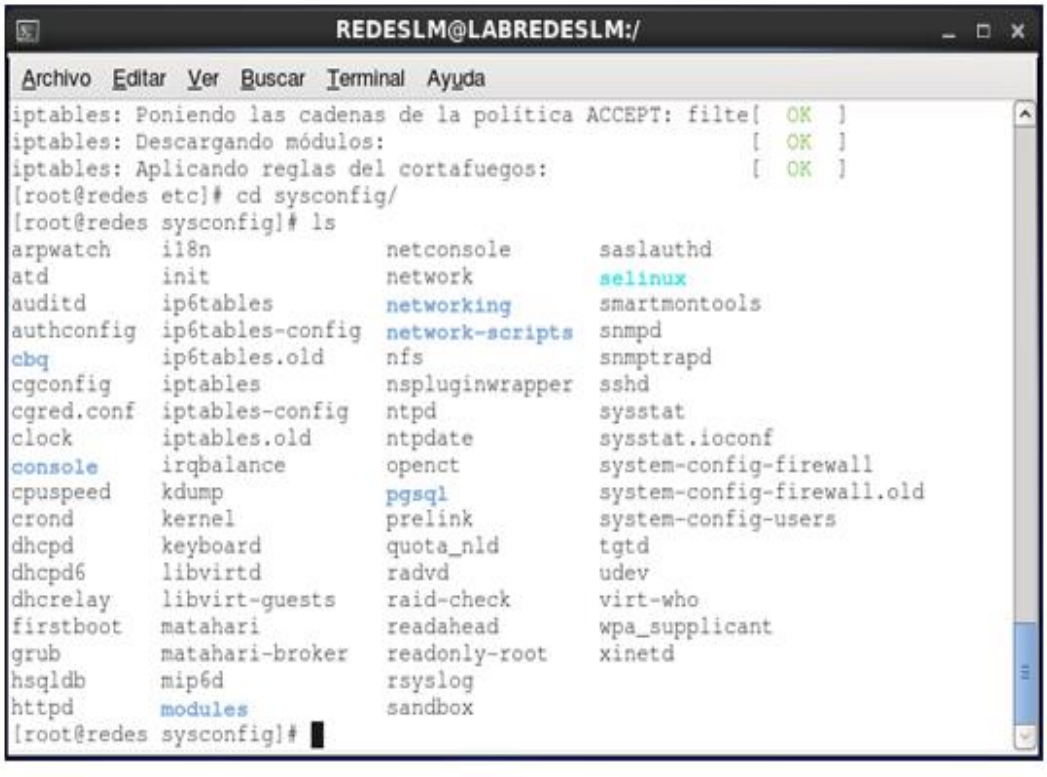
```
idmapd.conf                profile                    yum.repos.d
[root@redes etc]# cd ipsec.conf
bash: cd: ipsec.conf: No es un directorio
[root@redes etc]# gedit ipsec.conf
[root@redes etc]# ntsysv
[root@redes etc]# ntsysv
[root@redes etc]# service ipsec restart
ipsec_setup: Stopping Openswan IPsec...
ipsec_setup: stop ordered, but IPsec appears to be already stopped!
ipsec_setup: doing cleanup anyway...
ipsec_setup: Starting Openswan IPsec U2.6.32/K2.6.32-220.el6.i686...
```

Fuente: Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná

Realizado por: Autores

Seleccionar la carpeta correspondiente a los IPTables para que se puedan configurar las reglas para definir los requerimientos necesarios dentro de la investigación que se tiene dentro de las propuestas realizadas durante toda la investigación.

GRAFICO 3.20. Reseteando Servicios



Fuente: Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná

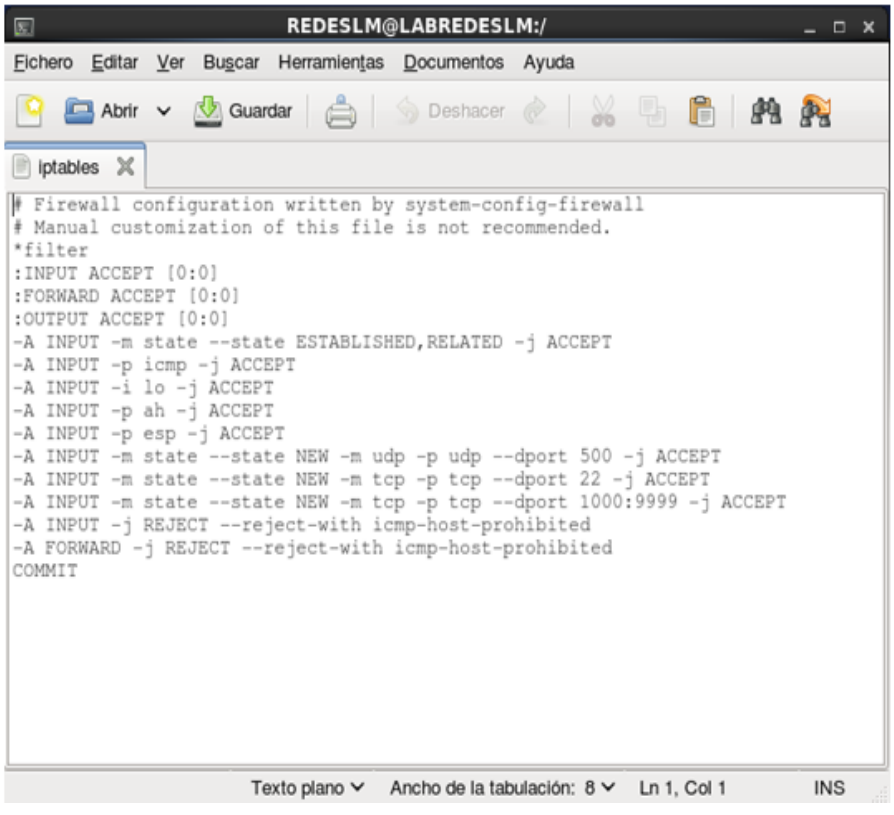
Realizado por: Autores

El Firewall dentro de la institución de educación superior está limitando como se dijo desde un inicio a los potenciales intrusos los mismos que deben tener en cuenta que un rango de puertos son los que se deben tener abiertos.

Y como se escribió dentro de las configuraciones del Firewall se ve reflejada dentro de los archivos del script del servicio.

En donde se puede observar que se tiene los intervalos de los puertos que están abiertos es decir desde el 1000 hasta el 9999, además de que solo se permita realizar ping(ICMP), como protocolo de comunicaciones y pruebas de la validez de las configuraciones. Se pude además anotar que se tiene habilitado el puerto 500 para lo que son envio/recepción de datagramas a través de UDP.

GRAFICO 3.21.Códigos En Script

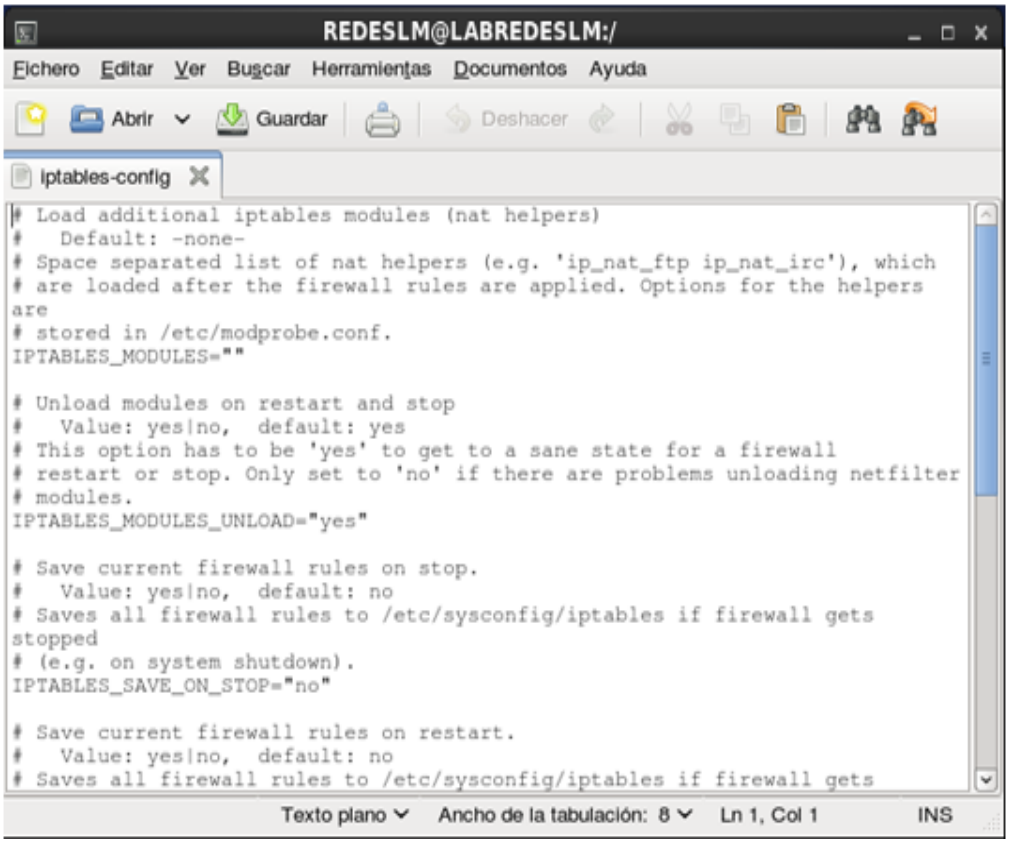


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez definidas las reglas del firewall se procede a configurar los módulos de acuerdo a las necesidades de las actividades que se requiere hacer dentro del servidor de seguridades y del tipo de condicionamiento que se requiere hacer.

GRAFICO 3.22.Codificación de IpTables



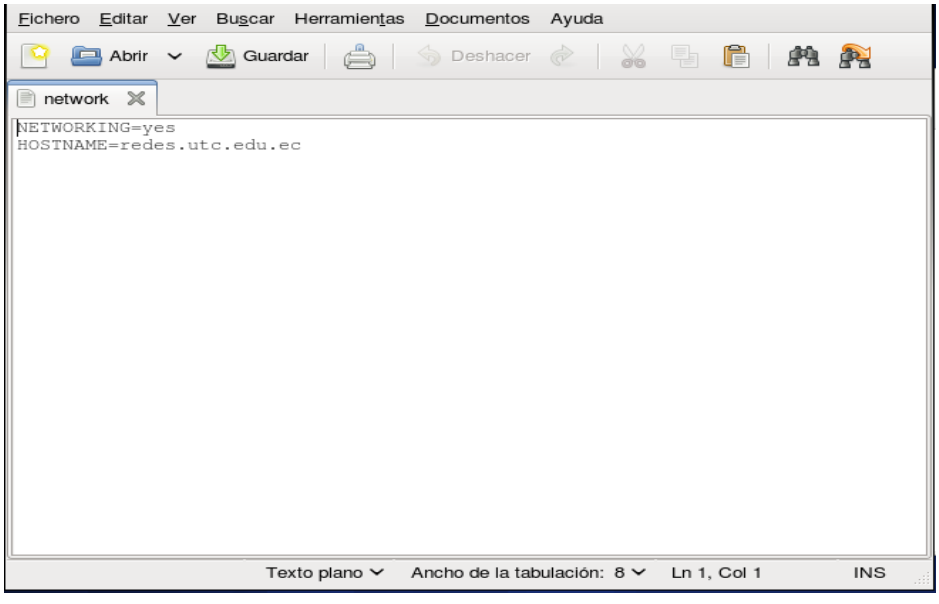
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez configurada las seguridades a nivel de iptables y de ipsec se procede a configurar a la configuración de la red en el ámbito del Servidor de Nombre de Dominios, y que este guarde relación con el dominio de la Universidad, y que solamente sea para las prácticas de los estudiantes luego de implementada las configuraciones dentro de lo que se requiere para el efecto.

Es necesario notar que las redes solamente obedecen al dns y mas no a la dirección física que para este caso se tenía tanto para redes en IPv4 como en IPv6.

GRAFICO3.23.Fin de configuración



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Dadas las reglas que se pusieron en la investigación se procede a desactivar las directivas del sistema que tienen que ver con las IPTABLES ya que estas producirían conflictos con las que se encuentran el Linux por defecto.

GRAFICO 3.24.Menú de herramientas

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Cuando ya se tiene seleccionado todas las opciones, reglas y las configuraciones del firewall dentro del iptable se tiene que desactivar al firewall para que las funciones del iptable puedan surtir efecto y que a su vez estos no se molesten entre sí.

GRAFICO 3.25. Deshabilitar Configuraciones

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

GRAFICO 3.26. Aceptar Cambio de Configuración

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

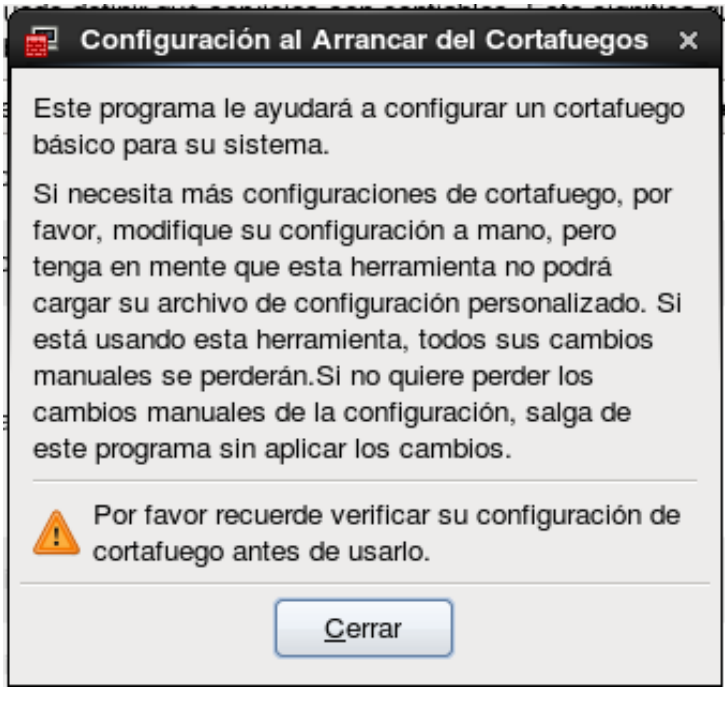
Realizado por: *Autores*

3.6. Verificación de configuraciones mediante modo grafico en las opciones del Firewall de Linux CentOS 6.2.

Cuando el firewall se encuentra activo y funcionando se debe verificar su funcionamiento y que las configuraciones reflejen en el modo gráfico todas las configuraciones que se realizaron dentro del modo texto el cual es más seguro y se puede garantizar de que las configuraciones se las hicieron de buena manera.

Y como se puede ver en la figura se debe tener en claro que es lo que se quiere hacer y cómo se puede realizar las configuraciones dentro del iptables, y comprobar que este desactivado dentro de los servicios del sistema Linux.

GRAFICO 3.27. Configuración en modo grafico del Firewall

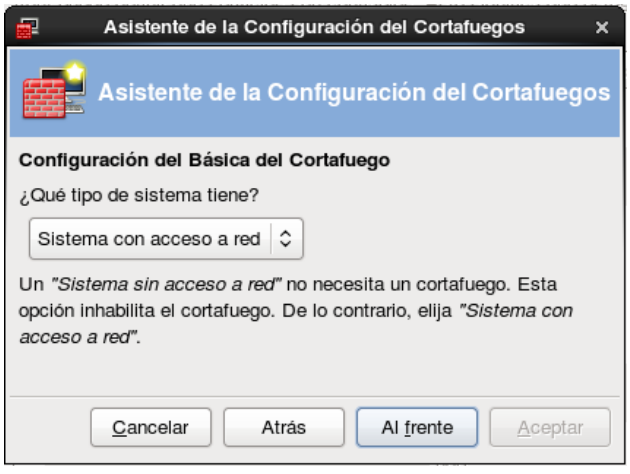


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Revisaremos las configuraciones mediante un asistente para poder comprobar que todas las configuraciones hechas se estén reflejando y sobre todo que asegure las comunicaciones que se tienen dentro del firewall de plataforma Linux.

GRAFICO 3.28. Asistente de configuración de Firewall

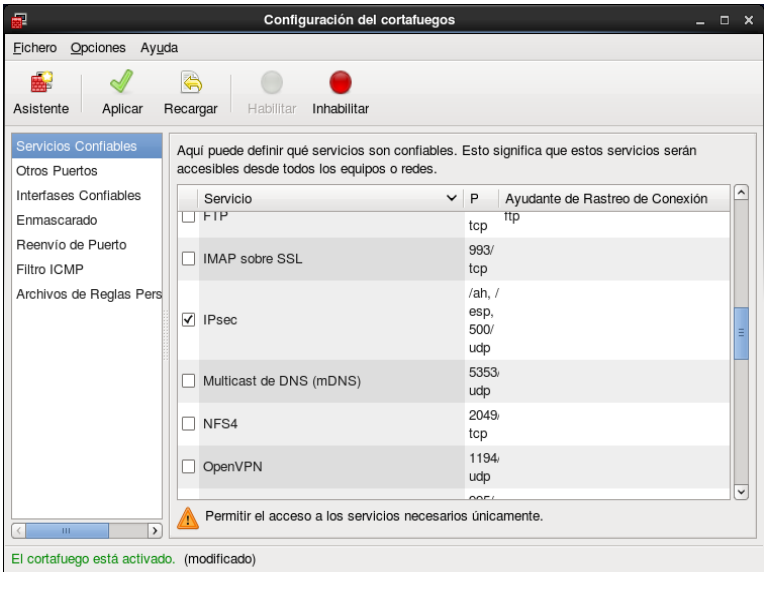


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

En las configuraciones del asistente se pueden ver reflejado los servicios que se encuentran activos y que pueden ser utilizados esta es la mejor manera de ver cómo funciona un firewall y que es lo que tiene bloqueado y que es lo que permite realizar mediante las comunicaciones.

GRAFICO 3.29. Revisión de servicios de firewall



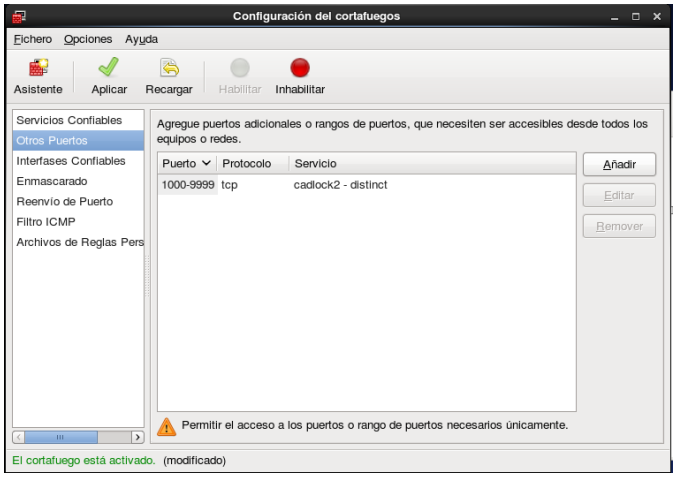
Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Además de poner los servicios se puede observar de igual manera cuales son los puertos que permiten la configuración y que fueron los que primero se activaron en uno de los scripts que se lo hizo en el modo texto.

Es por estas cosas que las configuraciones se les hacen mediante texto y scripts ya que son los que ayudan a garantizar la información que se va generando dentro de la plataforma y que son importantes al momento de restringir y de permitir el paso de la información.

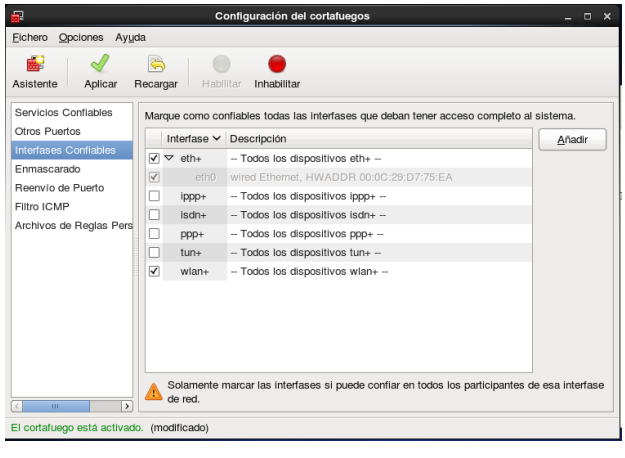
GRAFICO 3.30. Verificación de puertos en Firewall



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

GRAFICO 3.31. Tarjetas de red y hardware de Firewall

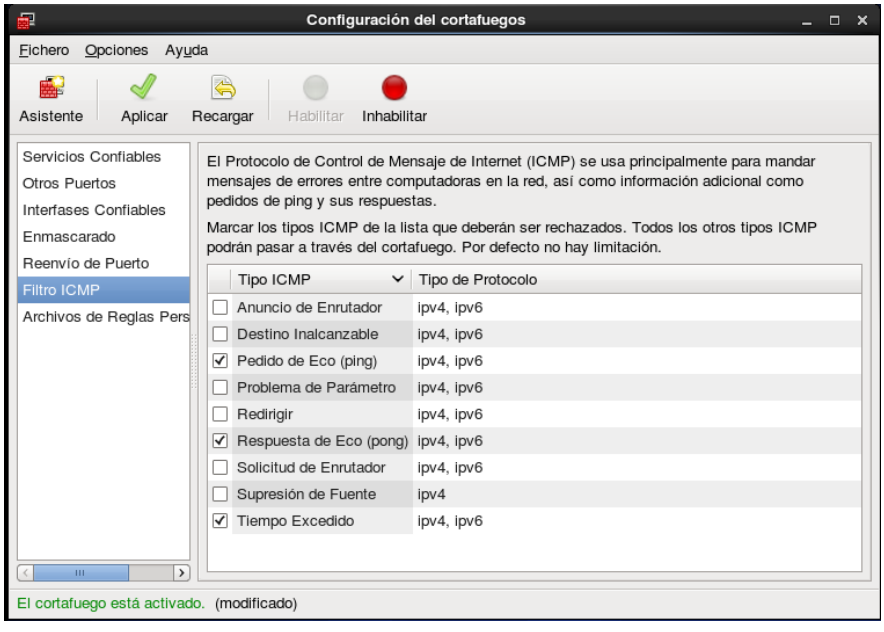


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Luego de todas las configuraciones que se hizo a nivel de tarjetas de red del servidor de Linux, los scripts, puertos y enmascarados podemos habilitar los protocolos permitidos dentro del firewall y que en el modo texto se nos pudo pasar por alto y que a veces son necesarios como el ICMP.

GRAFICO 3.32. ICMP (Ping) según protocolos levantados



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

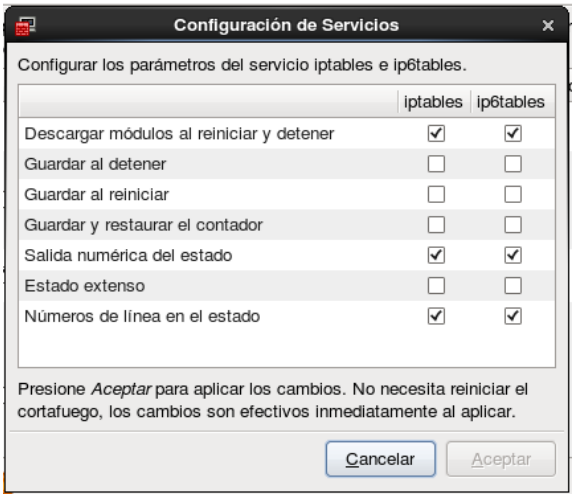
GRAFICO 3.33. Verificación de puertos en Firewall

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Las configuraciones del Iptable tanto para la versión 4 y 6, en donde se determina los servicios finales que debe tener un firewall.

GRAFICO 3.34. Finalmente los servicios de iptables



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

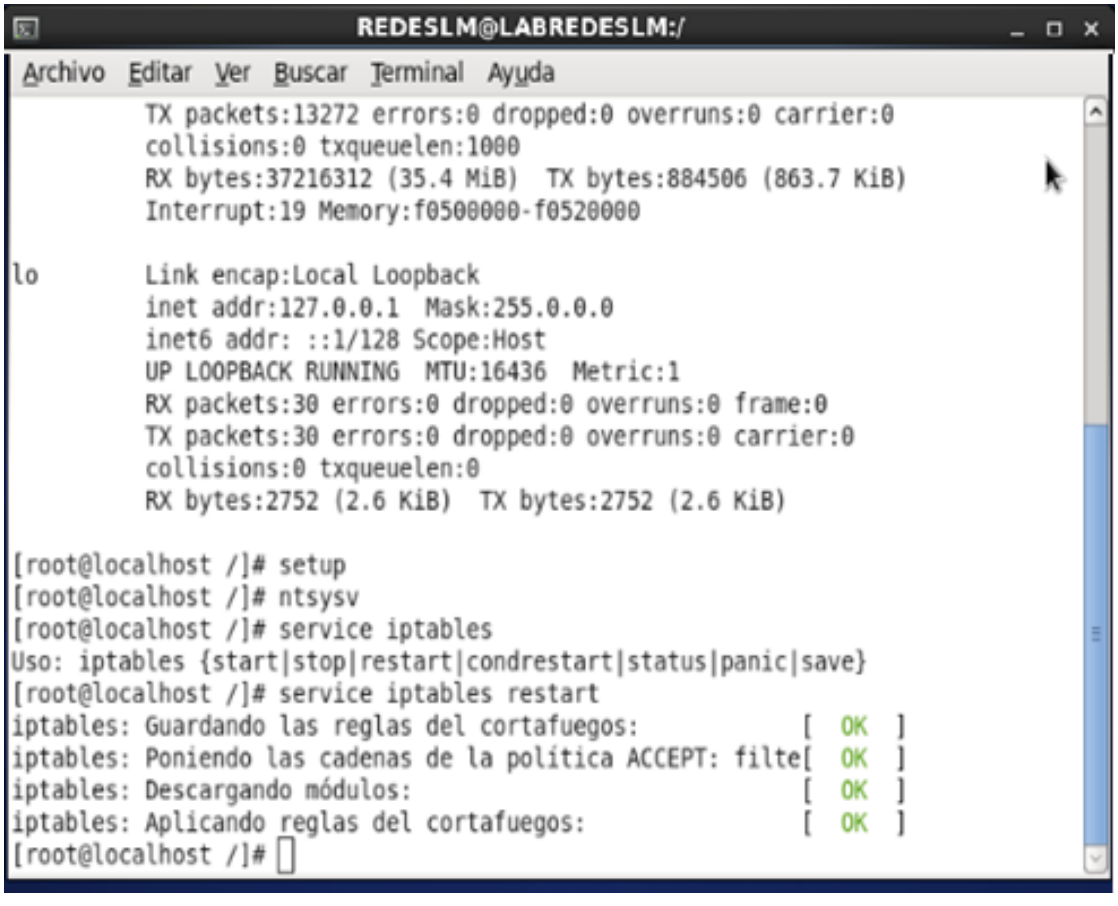
Una vez comprobada las configuraciones y que se puede revisar que los servicios se suban y que estos no boten ningún error a ningún nivel, este es de los procesos más críticos que se presentan en la puesta a punto de firewall.

GRAFICO 3.35. Reiniciar el servicio del ipsec

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

GRAFICO 3.36. Reiniciar el servicio de IPTABLE



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

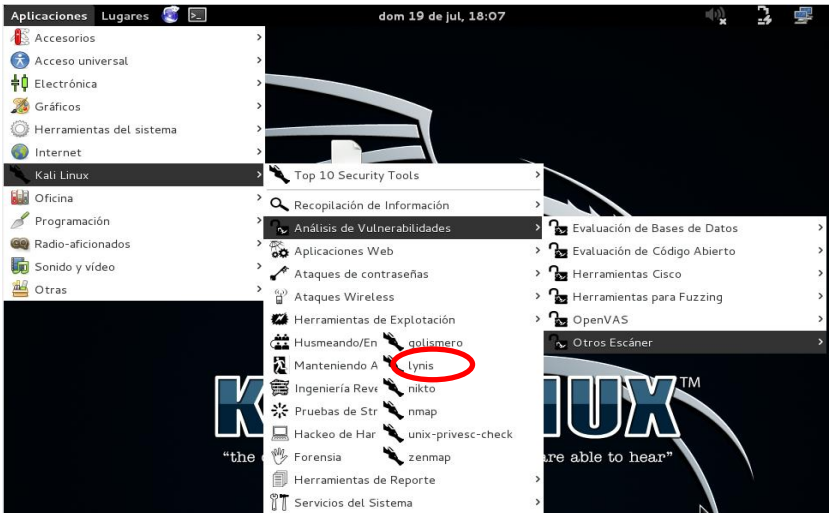
Realizado por: *Autores*

3.6. Escaneo de Vulnerabilidades

Lynis es una herramienta que puede ser de gran utilidad si usas Linux o cualquier sistema UNIX. Basta solo llamar a la herramienta con un comando para que automáticamente comience su trabajo.

El comando a usar es el **lynis** esto previamente al abrir un terminal. O sino seguimos la Secuencia de como abrir la aplicación muestra en la siguiente gráfica, Una vez hecho este proceso damos a ejecutarla.

GRAFICO 3.37. Grafico como abrir lynis en kali linux



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez abierta la aplicación podemos ver cuáles son todos sus servicios en escaneo de vulnerabilidades, entre ellos las opciones más importante.

- Auditar
- Chequeo y escáner vulnerabilidades
- Pruebas de usuarios, registros entre otros

GRAFICO 3.38. Interfaz de inicio de lynis

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Una vez ejecutado el comando **lynis -c** mostrado, la herramienta comenzara a trabajar automáticamente, revisando todas las configuraciones en el sistema operativo. A medida que va analizando la información irá presentándola al usuario de la siguiente manera:

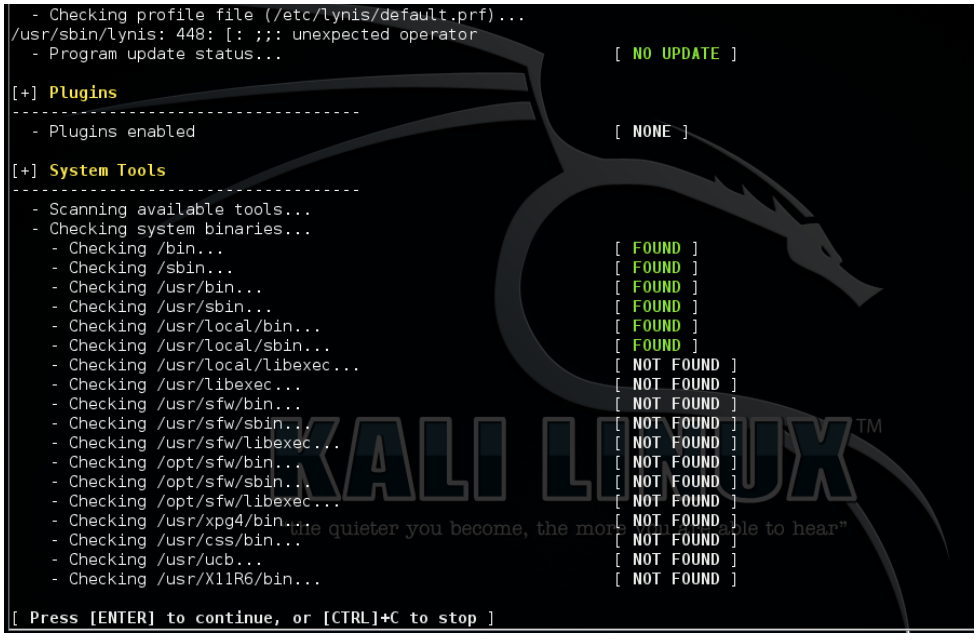
GRAFICO 3.39. Inicialización del comando lynis –c

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Donde podemos ver que arranco la evaluación, primero se ejecuta la evaluación a si mismo, mostrando la toda la información igual podemos observar en letras verdes cuando se realizó correctamente la evaluación igual podemos observar que nos da una opción al final de la pantalla la cual es que si presionamos la tecla **Enter** continuamos con la evaluación mas no si damos a CTRL + C nosotros continuaremos así que ejecutaremos **Enter**

GRAFICO 3.40. De Herramientas del sistema



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

El cual podemos ver que se hizo el escaneo de todos los sistemas binarios en el grafico se ve los encontrados claramente de color verde los encontrados y los de blanco que no fueron encontrados

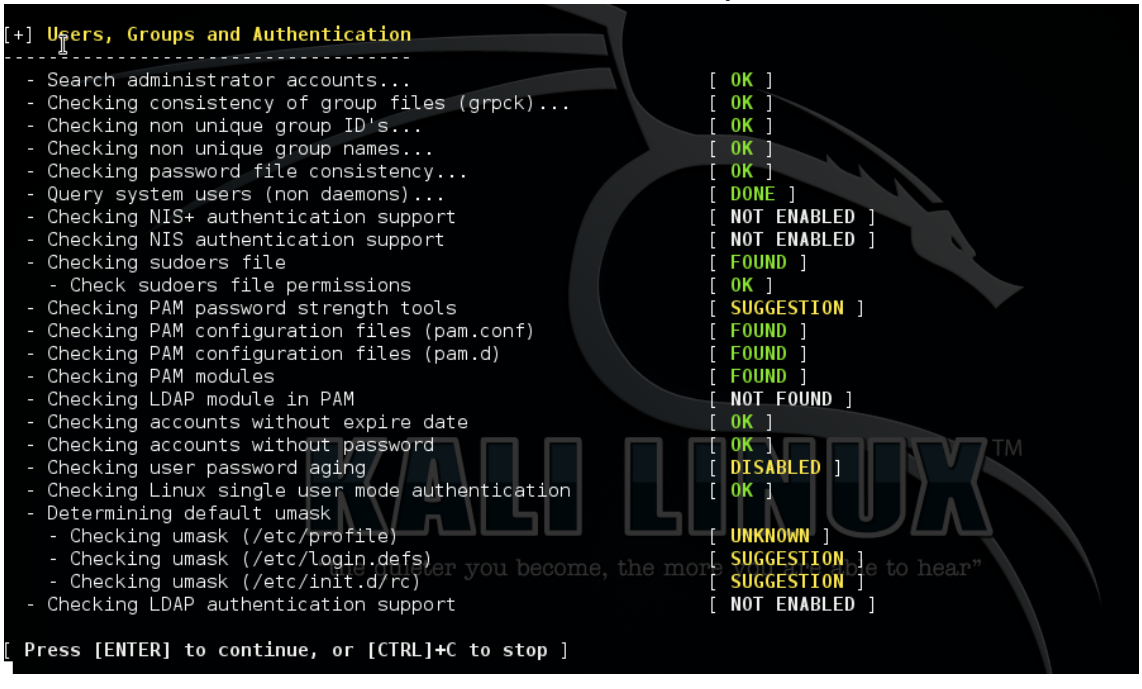
Vale recalcar que es también capaz de encontrar vulnerabilidades y configuraciones por defecto; para ello emplea colores algo llamativos, tal como los que utiliza un semáforo de tránsito. Esta captura de pantalla que colocamos a continuación muestra un claro ejemplo de cómo se ve cuando encuentra alguna falla o potencial vulnerabilidad

GRAFICO 3.41. De arranque y servicios

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

GRAFICO 3.42. Evaluación de autentificación



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

En la gráfica podemos ver que se efectuó el escaneo a todos los grupos de autenticación en la cual vemos existen muchos que se encuentran en buen estado y otros que sugieren que sean mejorados como cambio de clave por falta de fuerza o de confiabilidad

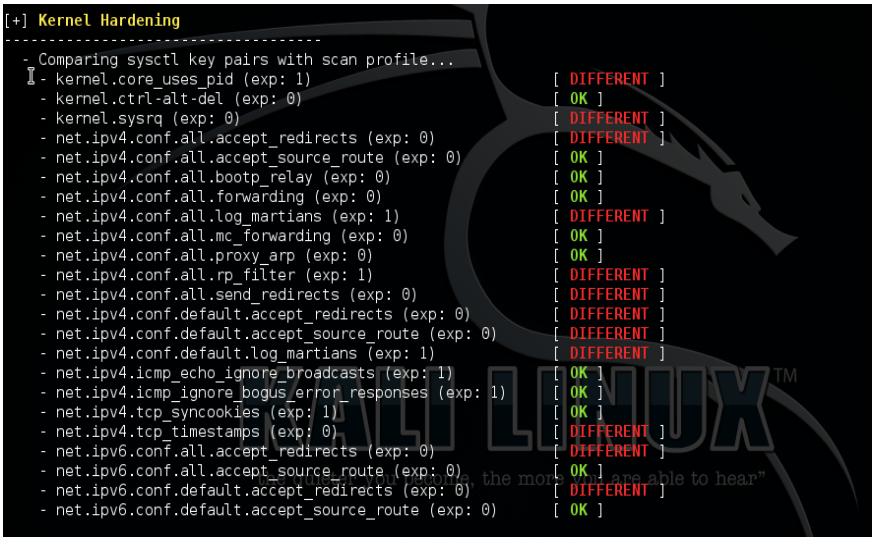
GRAFICO 3.43. De puertos, paquetes y red

Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Hemos llegado al punto más importante de nuestra evaluación donde podemos ver que se analizo los puertos y la red podemos ver que nos sugieren implementar mecanismos de seguridad que posteriormente lo efectuaremos

GRAFICO 3.44. De núcleo de Kernel

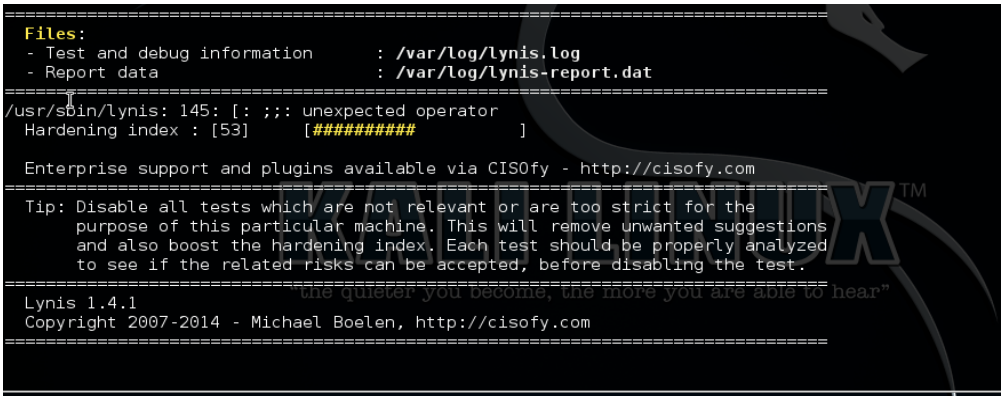


Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

Algo muy interesante es que también informa la configuración que posee el kernel o núcleo de este sistema operativo. Esto es muy importante ya que configuraciones por defecto podrían llevar a establecer vías de acceso para un cibercriminal. Veamos qué información nos brinda

GRAFICO 3.45. Final del escáner



Fuente: *Laboratorio De Redes Universidad Técnica De Cotopaxi Extensión La Maná*

Realizado por: *Autores*

3.7. Conclusiones y Recomendaciones

3.7.1 Conclusiones

El proyecto de investigación reunió todos los factores que impactan en trabajos de seguridades al hablar de prevenir los ataques a la información de cualquier institución, y mediante la implementación de un firewall que reúne todos los requisitos de seguridad que se puede pensar al momento de reunir los requisitos de garantías de seguridades.

En toda institución debe existir un programa de gestión y de evaluación de todas las posibles amenazas a las que pueden estar expuesta todos los componentes e información, este facilitara el buen y eficaz manejo de los mismos.

Todas las empresas e instituciones requieren de un firewall y de seguridades mediante IPSec, para garantizar el flujo de la información con toda la seguridad del caso y que estos puedan ayudar a cumplir con los objetivos de engrandecer sus activos y recursos.

Existe mucha información bibliográfica sobre las alternativas de seguridad y todas estas se pueden encontrar en libros, pero sobre todo en lo que son artículos científicos de personas que investigan alternativas de seguridades a todo nivel.

La plataforma de Linux es muy amigable, de fácil uso para trabajar en actividades de gestión y seguridades Se usó los Sistemas Operativos CentOS 6.2. y Kali en plataforma Linux ya que este es de mucha importancia en el factor económico dándonos facilidades de descarga libres así como su uso para obtener nuevos conocimientos

3.7.2. Recomendaciones

La recomendación principal sería poner más énfasis en la detención de vulnerabilidades ya que de esto depende el uso correcto y el buen funcionamiento del laboratorio, se recomienda según la evaluación poner contraseñas de un descifrado más extenso ya que la actual se encuentra en un estado débil, hay que verificar el intercambio de ficheros e información mediante los protocolos TCP, al igual que no es recomendable dejar el funcionamiento de los protocolos de internet defaul mas bien hacer uso de una secuencia lógica para la configuración.

Se recomienda el uso constante de un programa de evaluación ya que en la actualidad este es un problema que constantemente vienen aquejando, el cual se puede corregir previamente sabiéndolo detectar de una forma oportuna.

Para poder realizar implementaciones de seguridades en una empresa o institución hay que definir claramente que se tiene y que se necesita cuidar para poder empezar con las implementaciones de las seguridades de los equipos de cómputo.

La fomentación de software libre es la mejor alternativa tecnológica ya que se puede garantizar que la información puede fluir de una muy buena manera, todo lo propietario tiene lo libre es decir no hay nada que el software propietario tenga que el software libre no lo pueda hacer.

En cuanto a costos este tipo de implementaciones ayudan a la generación de ahorro en cuanto tiene que ver a las licencias y sobre todo a la administración de recursos con costos bajos.

Fomentar la aplicación de más y mejores proyectos de investigación en el laboratorio que queda implementado en un 90% considerando que existe el potencial necesario para que los estudiantes puedan explotarlo.

BIBLIOGRAFIA

- Matías, Katz.2013.Redes Y Seguridad.2013. Alfa Omega. Pág. 2

- Jose, Manuel Huidobro Y Ramón Jesús Millán Tejedor. 2009

- Vieites, Álvaro Gómez. Enciclopedia De La Seguridad Informática. 2011.Alfaomega. Pág. 62.

- Http://Www.Ecured.Cu/Index.Php/Red_En_%C3%A1rbol

- Álvaro, Gómez Vieites.2013.Seguridad En Equipos Informáticos. 2013. Starbook. Pág. 16

- Julio, Gómez López.2011.Administracion De Sistemas Operativos. 2011. Ra-Ma. Pág. 76

- Serpa Paz, Guillermo Adan. Noviembre 17, 2014, Pag.2

- Chavez Flores, Alejandra T. Octubre 2009

- Douglas Comer, Redes Globales De Informacion Tcp/Ip, Segunda Ediacion, Prentice Hill, Pág. 19,

- Windows Server Administration Fundamentals. Microsoft Official Academic Course. 111 River Street, Hoboken, Nj 07030: John Wiley & Sons. 2011. P. 21. Isbn 978-0-470-90182-3

- Gabriel Verdejo, Álvarez: Seguridad En Redes Ip: Ids 2011. Pag 72.

- Moll Monrreal, Pedro. Seguridad Informática, 2014. Pag,18.

- Charte Ojeda Francisco, Microsoft Windows Server 2012 Anaya Multimedia. Pag 448. Isbn 9788441533202

- Roca, M. "Empresa Y Administración En España Y Cataluña": (2007). España: Uoc. Pag. 21,

- Reed, Jeremy. The Openbsd Pf Packet Filter Book, Ee Uu, Reed Media Services, 2006 . 196 P Isbn 978-0979034206

- International Organization Of Estandardization). Iso/Iec 27001:2005.

- Ramon, Ruiz. Historia Y Evolución Del Pensamiento Científico Sinaloa México 2006 P.182 Isbn-13: 978-84-690-6369-9

- Arosemena, Rafaella. Metodología De La Investigación.(Material Graficoproyectable). Ecuador: Guayaquil, (2009). 83 Diapositivas.
- Eyssautier De La Mora, Maurice. Metodología De La Investigación: Desarrollo De La Inteligencia. Thomson: 2006. 319 P. Isbn: 9706863842, 9789706863843.
- Willie Pritchett, Kali Linux Cookbook, Año 2013 Pág. 52.
- Roderick Smith, Lpic-1: Linux Professional Institute Certification (3ª Ed.) Título. Anaya Multimedia, 2013 Año Pag 92.
- Joel Barrios Dueñas, 2012. Introducción A Ip Versión 4. Pág. 18.
- Ariganello Ernesto, Redes Cisco. Guía De Estudio Para La Certificación Ccna Routing Y Switching, Ra-Ma, Año 2014. Pág. 12.
- Philippe Freddi. Windows Server 2008: Los Servicios De Red Tcp/Ip Año2010 Pág. 42.
- Pérez Ignacio, Aprende A Auditar La Seguridad, Año 2014. Pág. 7.
- Martínez Lorenzo , Herramienta De Auditoría Para Hardening *Nix Año 2010 Pág. 5.