UNIVERSIDAD TECNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

"IMPLEMENTACIÓN DE SEGURIDADES BASADAS EN CAPAS CON TECNOLOGÍA CISCO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN Y PRODUCTIVIDAD DE LA EMPRESA PRODEMCO. S. A. EN LA PROVINCIA DEL AZUAY, CAPITAL CUENCA EN LA CALLE NICANOR AGUILAR Y LUIS MORENO MORA EN EL PERÍODO 2014 - 2015"

Tesis presentada previa a la obtención del Título de Ingeniería en Informática y Sistemas Computacionales.

Autora:

Carolina Elizabeth Vinocunga Viracocha

. **Director:**

Ing. M.Sc. Jorge Bladimir Rubio Peñaherrera.

LATACUNGA- ECUADOR.

2015

AVAL DEL TRIBUNAL DE GRADO

AUTORÍA

La autora certifica que la investigación, redacción y propuesta del presente trabajo son de su exclusiva autoría de Carolina Elizabeth Vinocunga Viracocha.

A través de la presente declaración cede los 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.

Carolina Elizabeth Vinocunga Viracocha

C.I: 050343635-4

AVAL DEL DIRECTOR DE TESIS

En calidad de Directo de Trabajo de Investigación sobre el tema: **"IMPLEMENTACIÓN DE SEGURIDADES BASADAS EN CAPAS CON TECNOLOGÍA CISCO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN Y PRODUCTIVIDAD DE LA EMPRESA PRODEMCO. S. A. EN LA PROVINCIA DEL AZUAY, CAPITAL CUENCA EN LA CALLE NICANOR AGUILAR Y LUIS MORENO MORA EN EL PERIODO 2014 - 2015".** De la señorita estudiante Carolina Elizabeth Vinocunga Viracocha, postulante de la Carrera de Ingeniería en Informática Y Sistemas Computacionales.

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.

Latacunga, a 24 de Septiembre del 2015.

Atentamente.,

……..

DIRECTOR DE TESIS

Ing. Jorge Bladimir Rubio Peñaherrera.

C.I: 050222229-2

CERTIFICADO

Por medio del presente tengo a bien CERTIFICAR .señores de la Universidad Técnica de Cotopaxi, que la Srta. Carolina Vinocunga realizo su trabajo de investigación en nuestra empresa, obteniendo resultados favorables para nosotros

Autorizamos a la señorita antes mencionada, pueda presentar el presente para su monografía.

Paute, 18 de septiembre del 2015

Atentamente

……

Ing. Pablo Urgiles Torres

AGRADECIMIENTO

A dios por haberme permitido llegar hasta este punto, brindándome la fortaleza, amor y sabiduría necesaria para cumplir mi objetivo.

A Mis padres por haberme ayudado con todos los recursos necesarios para poder estudiar, también por su apoyo, comprensión y buenos consejos, ensenándome a ser una mujer luchadora a pesar de las adversidades que se nos presenten.

A mi esposo por ser mi compañero de lucha en el diario vivir, ayudándome a cumplir mi sueño.

A mi director de tesis, M.Sc. Jorge Rubio por brindarme sus conocimientos y experiencias, para poder cumplir con mi reto académico.

Y todas las personas que me brindaron su apoyo económico y moral en el trascurso de mi vida Universitaria.

Vinocunga Viracocha Carolina Elizabeth

DEDICATORIA

A mi hija, por ser el motor de mi vida, ya que tan solo basta una sonrisa en tu rostro para tener la fuerza y valentía necesaria para vencer todas las adversidades que se me presenten. Tú me impulsas cada día a superarme para poder brindarte siempre lo mejor. Gracias mi pequeño ángel por llegar a mi vida.

A mis padres por haberme dado la vida y llenarme de amor a pesar de mis errores.

A todas las personas quienes hicieron posible que este sueño se cumpliera.

Vinocunga Viracocha Carolina Elizabeth.

ÍNDICE GENERAL

CAPITILO II

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPITULO III

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

TEMA: "Implementación de seguridades basadas en capas con tecnología cisco para mejorar la seguridad de la información y productividad de la empresa Prodemco. S. A. En la provincia del Azuay, capital cuenca en la calle Nicanor Aguilar y Luis Moreno Mora en el periodo 2014 - 2015"

Autora: Vinocunga Carolina

Tutor: Ing. Ms. C. Rubio Jorge

RESUMEN

La presente investigación trata de una de las alternativas de enrutar las comunicaciones dentro de la empresa Prodemco con configuraciones alternativas, las mismas que ayudaran tanto en la fidelidad de las comunicaciones como en las seguridades, esto hace que la información que por éstas circule con agiles e integras. El enrutamiento entre las redes de datos que confirman el grupo maderero ha hecho que mejoren los procesos de otras áreas, para este caso se lo ha realizado a través de tecnológica CISCO que es mejor en la actualidad en el mercado de las telecomunicaciones, se tomó en cuenta las seguridades para enrutar con el subneteo de la red en subredes para realizar una comunicación casi de punto a punto por su cálculo mediante la aritmética de redes, entonces la seguridad de redes es el control de acceso, es la capacidad de limitar y controlar el acceso a sistemas host y aplicaciones por medio de enlaces de comunicaciones. Para poder determinar cuáles son los usuarios que quieren acceder deberán antes ser identificados o autentificados, de forma que los derechos de acceso pueden adaptarse de manera individual.

La investigación se complementa con la configuración e implementación de un servidor proxy para la distribución del recursos de internet y que este se encuentre controlado en la utilización de páginas de acuerdo a los perfiles de los usuarios de puntos de red, dentro de las reglas a tomar en cuenta también se tiene que pueden utilizar la red y el proxy los usuarios de lunes a viernes en horarios de oficina, salvo en un segmento de red que se lo realiza a cualquier hora sin importar el día.

Estas actividades están completas con la implementación del firewall mediante la utilización de reglas del IPTABLES, que se encarga de abrir y cerrar los puertos que son y no necesarios para poder tener acceso a la red administrativa de la empresa.

Descriptores: Cisco, securities,proxy.

THE TOPIC: "Implementation of securities based on Cisco technology layers to improve information security and business productivity at Prodemco. SA. in the Azuay province, Cuenca capital city at Nicanor Aguilar and Luis Moreno Mora street during 2014 - 2015 period."

Author: Vinocunga Carolina

Tutor: Ing. Ms. C. Rubio Jorge

ABSTRACT

This research is about an alternative of routing communications at Prodemco SA. with alternative configurations, which will help both: the fidelity of communications and securities, this create a nimble and entire information cycle. Routing data between networks that form the timber group has made possible the improvement of processes in other areas, in this case it has been realized through CISCO technology which is the best one currently on the telecommunications market; it took into account the securities for routing with network subnetting into subnets for getting a communication almost point by point arithmetic calculation network, then the network security is access control, the ability to limit and control access to host applications and systems through communications links. To determine which users are seeking access, they should be identified and authenticated before, so that the access rights can be adapted individually.

The research was complemented by the configuration and implementation of a proxy server for internet distribution of resources, and it is controlled by the use of pages according to user profiles of network points; within the rules to take into account users can use the network and proxy users on weekdays during office hours, too; except in a network segment that is performed at any time regardless of the day.

These activities are complemented by the implementation of the firewall using iptables rules, which is responsible for opening and closing ports that are not needed to access the corporate network administration.

Descriptor: Cisco, securities, proxy.

Aval de traducción

INTRODUCCIÓN

En la actualidad las instituciones y empresas buscan interconectar tanto los procesos como personas e información con la propia organización y de esta manera buscar garantizar que todos los datos sean un bien común dentro de las mismas. La falta de una red de datos estable, ocasiona que se pierda información importante y que esto derive en pérdida de tiempo al momento de estar trabajando a través de ella.

Con el crecimiento poblacional y el aparecimiento de nuevas tecnologías van generando nuevos requerimientos y por ende personal para tratar de mover al mundo, esto ha hecho que las actividades o jornadas de trabajo duren las 24 horas al día y los siete días de la semana para sus redes informáticas y los equipos informáticos.

En los sistemas de información actuales se tienen diversidad de componentes que son necesarios para que estos puedan desarrollar de forma adecuada sus actividades. Todos estos problemas pueden ocurrir a nivel de usuarios o en el propio servidor por lo que siempre se debe tener algunos dispositivos que ayuden a los respaldos de la información. En la infraestructura que son necesarias para garantizar la información se requiere de equipos tales como los servidores, dispositivos de redes locales y extendidas en las que se pueden mencionar a los routers y los switchs que deben estar interconectados para que puedan cumplir con su función de comunicar a todos los usuarios.

En base a lo expuesto todo el departamento de sistemas debe estar proveído de un administrador de las redes y las comunicaciones el que ayudaría en la generación de proyectos de interconexión.

El administrador de la red debe estar pendiente del funcionamiento de las conexiones para que estas no tengan fallos en su estructura interna, que la red externa este funcional todos los días del año que tengan redundancia en las

comunicaciones desde y hacia el internet y las comunicaciones corporativas dentro de la empresa.

En la actualidad la empresa tiene en funcionamiento un sistema ERP (Planificador de Recursos Empresariales) que se encuentra centralizado en la ciudad de Quito, pero que debe ingresar información desde la planta y las oficinas de la ciudad de Cuenca, y está actividad se la debe realizar las 24 horas del día durante todo el año, para que lo datos que arrojen siempre sean los adecuados para que los entes decidores tomen decisiones oportunas.

Se conoce que las seguridades en las redes en la actualidad son de mucho provecho ya que les permite ser más productivas y con esto garantizar el correcto desempeño de todos sus roles. Hay que tomar en cuenta que en la actualidad la información es considerada como un activo muy valioso ara cualquier empresa moderna y eso se ve reflejado a diario en la creciente dependencia en los procesos computarizados para procesar su información y tomar decisiones estrategias y técnicas.

Debido a que las seguridades en la última parte tecnológica es lo más importante dentro de la informática se ha considerado conveniente dividir la investigación en 3 capítulos además de sus respectivas conclusiones y recomendaciones:

En el capítulo I, se hace un análisis a los temas bibliográficos que se trataran dentro del proyecto de investigación, de igual manera se conceptualiza todas las herramientas y lenguaje de configuración de los equipos de comunicaciones.
En el segundo capítulo se realiza el estudio de campo partiendo siempre de la realidad de la empresa y su posicionamiento en el mercado local de la madera, así como también su relación con la empresa matriz, luego las entrevistas partiendo de las guías de entrevistas para las autoridades de la empresa Prodemco S.A. de la ciudad de Cuenca personal de apoyo del departamento de sistemas y después los empleados serán tomados en cuenta para la realización de una encuesta los

mismos que serán los datos para poder comprobar la realización de una hipótesis y su impacto dentro de la investigación.

El tercer capítulo se realizara la propuesta de la investigación, en la que está compuesto por una análisis de las seguridades que tiene la empresa y las que necesita para poder alcanzar la excelencia dentro de sus actividades, luego se diseñara alguna alternativa de la red LAN y WAN que se sujete al equipo adquirido para poder alcanzar todo su potencial y de esta manera asegurar la información que es lo que más se quiere dentro de las necesidades de la empresa.

Como resultado de la investigación se obtendrán las conclusiones que son las que arrojaran las variables diseñadas dentro de la investigación tanto las independientes como las dependientes que van a ser las que ayuden a la implementación de todas las seguridades, una vez obtenidas estas conclusiones se deberán tener las recomendaciones que van a ser un aporte técnico para mejorar las actividades dentro del departamento de sistemas y por ende de toda la empresa.

CAPÍTULO I

FUNDAMENTO TEÓRICA SOBRE USO DE HERRAMIENTAS PARA SEGURIDAD EN LAS REDES Y LAS COMUNICACIONES

1.1 Seguridad de la Información

Todas las empresas en la actualidad buscan precautelar su bien más preciado que es la información que se va generando dentro de las distintas actividades dentro de la empresa y como esta ayuda a que se genere mejoras dentro de la misma.

Los sistemas de información requieren estar siempre protegidos tanto de usuarios maliciosos como de entes externos que puedan afectar al normal desempeño de las actividades, hay que tomar en cuenta que lo más importante es mantener la integridad de la información así como la confidencialidad que no es más que la protección de los datos que son transmitidos a través de la red y que estos sean transmitidos por medio de ataques pasivos. Otra característica que hay que tomar en cuenta es el flujo de tráfico frente del tráfico para lo cual los atacantes no deberían poder ver la fuente o el destino, la frecuencia ni la longitud ni otras características del tráfico en una comunicación.

1.1.1 Antecedentes

La seguridad de la información se basa principalmente en la confidencialidad, integridad y la disponibilidad de los datos, sin embargo existen más requisitos como pueden ser la autenticidad. Sin embargo debemos tener en claro que una cosa es la seguridad de la información y otra muy importante es la protección de los datos, que son algunos motivos de y obligación de las actividades de seguridad, y las medidas de protección aplicadas serán las mismas.

Es asi que en 1986, los virus para PCs IBM entraron a escena. Similar a Elk Cloner, los adolescentes que buscaban fama entre la población de hackers crearon estos primeros virus no destructivos y los transmitían a través de discos flexibles. Durante gran parte de la década de los 80, los virus cumplieron con estas características: el daño era mínimo y los brotes eran raros. En 1988, sin embargo, el dócil panorama de los virus comenzó a cambiar. Luego se propagó "Morris Worm" a través de Internet y provocó daños considerables en todo el mundo. El virus Michelangelo provocó uno de los primeros pánicos mediáticos alrededor de los virus de computadora. Los reportes afirmaban que Michelangelo, programado para activarse cada año el 6 de marzo a partir de 2007, el cumpleaños número 517 del artista, podría borrar los discos duros de miles, incluso millones, de PCs infectadas.

En la actualidad la seguridad de la información es lo más importante ya que es el activo que se debe cuidar en todas las empresas, de tal manera que lo que se busca es precautelar toda la información que se generan aquí mediante la adquisición de equipos informáticos. Se puede concluir que la seguridad de la información es el motor que le mueve la protección de los datos y también el tratar de evitar su perdida y la modificación o alteración no autorizada que son temas que cada vez están más a la orden del día. Esta investigación tiene como objetivo la implementación de medidas de protección de los datos en la empresa garantizando de esta manera el trabajo de los usuarios de la red que alimentan la información de la empresa, y también con esto jurídicamente mantenemos la ética del personal, ya que evitamos alteración de la información.

1.1.2 Definición de seguridad informática.

Según: (Capella & Garcia, 2011) “Es el conjunto de medidas de protección que garantiza la confidencialidad, la integridad y la disponibilidad de la información, autenticidad, el no repudio tanto en origen como en destino así como el sellado de tiempo”

Según (Aguilera, 2010; Aguilera, 2010)“Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos”

En base a los conceptos dados se puede concluir que la seguridad de la Ainformación es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información tratando siempre de mantener la máxima confidencialidad y la disponibilidad y la integridad de la información.

Este concepto de seguridad de la información dista mucho de lo que puede ser considerado como seguridad informática, que la seguridad informática se encarga de lo que son seguridades en el medio informático (Hardware y Software), y en cambio en la seguridad de la información puede encontrarse en cualquier ámbito de la vida y no necesariamente en medios que tengan que ver con la informática.

1.1.3 Confidencialidad

Según: it ISMF International The IT Service Managemnet Forum, 2012 “Fundamentos de gestión de Servicios TL basado en ITIL”. Concepto de Confidencialidad. “Proteger información contra el acceso y uso no autorizado”
Según: (Aguilera, 2010) Concepto de Confidencialidad. “El hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada”

En conclusión la confidencialidad es una condición que asegura a la información no pueda estar disponible para varias personas o entes para acceso a procesos no autorizados.

También puede ser tomado en cuenta como una cualidad de un sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él y alterarla o borrarla, esta cualidad es muy importante porque la consecución de información no autorizada puede ser desastrosa para cualquier empresa que tenga información importante para desarrollar sus actividades.

1.1.4 Integridad

Según: (Aguilera, 2010). Concepto de Integridad. "Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuando se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto".

Según: it ISMF International The IT Service Managemnet Forum, 2012 "Fundamentos de gestión de Servicios TL basado en ITIL". Concepto de Integridad "Tener la Información exacta, completa y a tiempo".

1.1.5 Disponibilidad

Según: El programa MAGERIT define a la Disponibilidad "Grado en el un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información."

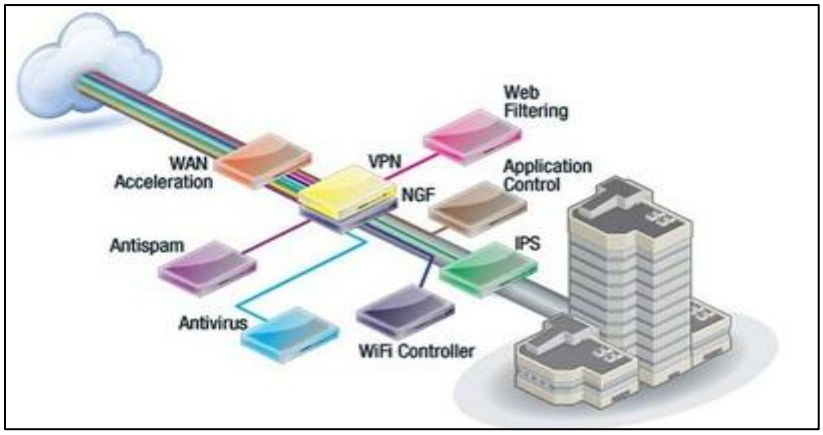
Según (Aguilera, 2010). Concepto de Disponibilidad. “La información ha de estar disponible para los usuarios cuando la necesiten”.

En conclusión en las Tecnologías de la información y las comunicaciones este término disponibilidad es una característica de las arquitecturas de servidores y redes que miden el grado de accesibilidad para la utilización por el usuario final a lo largo de un tiempo dado. Esto se relaciona mucho con la caída del sistema.

1.2 UTM

Según: (Aguilera, 2010) Concepto de Unified Threat Management. “Es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo”.

Ilustración 0-1: Modelo UTM



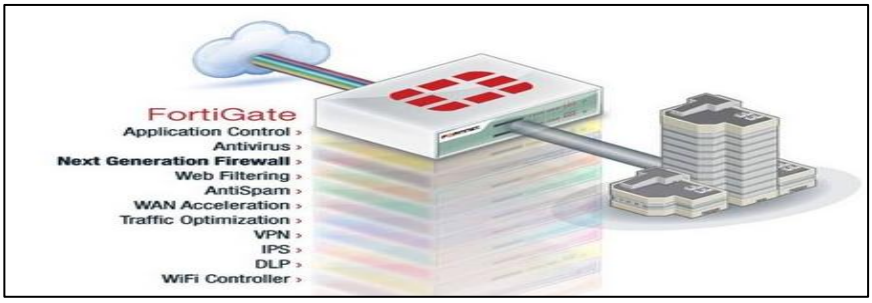
Fuente: http://www.etcomunicaciones.net/sociosestrategicos/fortinet.html/04-03-2015.

Según: Cyberoam a Sophos Company Por su seguridad. Definición de UTM “Son dispositivos que integran en una sola plataforma diversas funciones de seguridad tales como cortafuegos, VPN, sistemas de prevención contra intrusiones, antivirus y antispyware, antispam, filtrado web, control y visibilidad de capa 7, gestión de ancho de banda, gestión de vínculos múltiples y mucho más. La arquitectura de seguridad extensible junto a los procesadores multinucleo les

permiten ofrecer un procesamiento más rápido y seguridad ya preparada para el futuro”

Lo que se puede concluir es que un UTM (Gestión Unificada de Amenazas), es un equipo que cumple muchas actividades de seguridad en una empresa pero particularmente este término partió de la implementación de un firewall pero eso no es todo ya que engloba muchas funcionalidades más de seguridad y sobre todo de administración en las que se pueden mencionar a los VPN(redes privadas virtuales), el UDP (Protocolo de transferencias de datagramas), los antispam para lo que son correos no deseados o que no cumplan con las políticas de seguridad de las empresas, el Antiphising para evitar la adquisición de contraseñas por usuarios incorrectos ya sea estos dentro de la misma empresa o por fuera de ellos, antispyware que ayudar a cuidar de potenciales peligros y ataques de usuarios externos de la red de área local lo que hace que se vuelva más lenta la red y los usuarios internos puedan perder los potenciales creados por y para ellos, obviamente una herramienta de administración y seguridades lo que se necesita es un medidor de ancho de banda mismo que puede servir para que los usuarios no se vean perjudicados en sus actividades que se los realice en el internet.

Ilustración 0-2: Estructura UTM



Fuente: http://www.etcomunicaciones.net/sociosestrategicos/fortinet.html/05-03-2015.

1.3 Servidores de seguridades.

Según: (Garcia, Hurtado, & Alegre Ramos, 2010). Concepto de Servidores de Seguridad. “Para ser considerado como un servidor de seguridad a pesar de que

parezca muy evidente, comienza por la seguridad física. No sirve de nada proteger todo el sistema informático contra todo tipo de ataques por la red si es muy sencillo llegar a los servidores físicamente."

Según: Purificación Aguilera, 2008 "SEGURIDAD INFORMATICA. Informática y Comunicaciones", pág. 108. Concepto de Servidores de Seguridad. "Los servidores tienen un IP fija. Por lo tanto son fácilmente localizables. Pero conscientes del peligro, aplican protección de alto nivel. Los particulares son menos visibles, ya que recién una direcciones que atribuyen a sus abonados en cada solicitud de conexión."

Basándose en los conceptos anteriores se puede concluir que un servidor de seguridad es un sistema diseñado para controlar e impedir el acceso no autorizado o el acceso desde una red privada. La característica principal de este tipo de servidores es que pueden ser instalados tanto en hardware como en software o a su vez de las dos formas en conjunto ya que son parte fundamental en una red bien estructurada.

Se conocen de muchos tipos de servidores de seguridad y estos a su vez utilizan diversa técnicas entre las que se pueden mencionar están las siguientes:

El filtrado de paquetes que se encarga de examinar cada paquete que entre o que salga de la red y acepte paquetes según las reglas definidas por el usuario, esta técnica es muy eficaz y transparente y que es muy difícil de configurar y en la actualidad es muy susceptible a la suplantación de direccionamiento IP.

Como puerta de enlace a las aplicaciones, aplica mecanismos de seguridad a determinados programas que requieren el manejo de protocolos de transportación de paquetes como son el FTP o el Telnet, esta es una de las técnicas que más se utilizan pero puede reducir el rendimiento del servidor ya que consume muchos recursos tecnológicos al momento de su instalación.

En cambio la puerta de enlace a capas, está técnica aplica muchos mecanismos de seguridad cuando se utiliza un protocolo de seguridad tales como los TCP o los UDP. Una vez que haya sido establecida la conexión los paquetes pueden fluir entre los computadores sin que se necesite de ninguna comprobación para tales efectos.

Un servidor proxy es el que se encarga de distribuir los recursos tales como el internet y de igual manera ayuda con las seguridades dentro de la red ya que es muy importante para la intercepción de mensajes de acuerdo a la configuración que se le quiera dar, de otra manera el proxy ayuda de igual manera a controlar los mensajes que salen de la red interna hacia el exterior para garantizar toda la información que se pueda generar.

Un proxy de aplicaciones es aquel que tiene control sobre todas las seguridades de la red de área local. Esto ayuda para que este tipo de servidores puedan tomar decisiones basadas en las autorizaciones básicas del origen y el destino con los protocolos y filtrara comandos ofensivos o no permitidos por los datos.

1.4 Firewall

Según: (Frahim & Santos, 2014). Concepto de Firewall. “El firewall (cortafuegos) es un sistema de seguridad que protege el equipo y que controla los datos que se transmiten desde el equipo a internet y viceversa. De esta manera, le sirve de defensa contra personas o programas (virus y gusanos) que intentan acceder al equipo, sin tener autorización. El firewall se encuentra activado por defecto. Si un programa debe recibir datos provenientes de internet, le aparecerá una alerta y podrá indicar si autoriza o no la conexión”

Según: (Aguilera, 2010). Concepto de Firewall. “Impide la entrada de intrusos y de programas maliciosos a través de la red o de internet. Del mismo modo controla que no pueda salir malware hacia otros equipos. En caso de tenerlo activado y para evitar que el Firewall emita avisos o impida la ejecución de

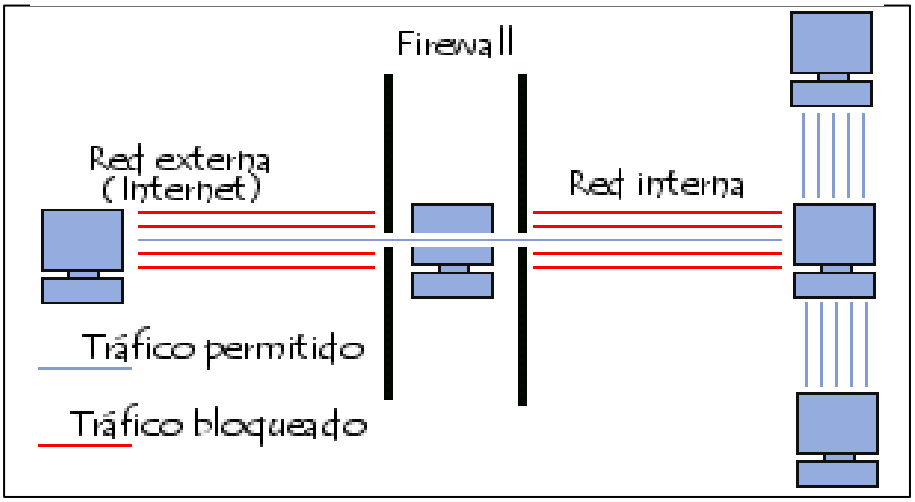
programas que considera maliciosos y que, sin embargo, tienen la confianza del usuario, puede permitirse expresamente la ejecución de determinados programas”De los conceptos adquiridos se puede determinar que los firewall para cada ordenador se conectan a internet que puede ser víctima del ataque de un hacker que es un usuario malicioso en búsqueda de asacar provecho personal. Estos sujetos lo que hacen es buscar en la red usuarios de computadores que se encuentren conectados con la finalidad de obtener esa información mediante el envío de paquetes disfrazados con cosas que puedan ser llamativos para este tipo de usuarios. Una vez que se encuentra estos usuarios el hacker busca alguna puerta por donde entrar y de esta manera tener a disposición toda la información y hacer con ella lo que más les parezca.

Es necesario hacer notar que la máquina que puede estar dentro de las elegidas esté conectada pero no tengan los controles necesarios para poder mantener a la raya a los intrusos.

Hay que tomar precauciones siempre con las maquinas que mayor ancho de banda tienen en la transmisión de la información ya que estos son los blancos favoritos de los intrusos, ya que se piensa que los que más ancho de banda asignados tienen es porque las funciones más delicadas son.

En conclusión se puede manifestar que es necesario que todas las redes de las empresas/instituciones como todos los usuarios de internet con conexión mediante cable o ADSL siempre deben estar cubiertos o resguardados por posibles intrusiones en su red ya que son blanco potenciales de los intrusos que buscan alterar información en su bien personal.

Ilustración 1-0-3: Esquema de un Firewall



Fuente: http:// es.kioskea.net/contents/590-firewall/06-03-2015.

1.5 Antivirus

Según: (Iñigo Griera, y otros, 2009). Concepto de Antivirus. "Para combatir la avalancha de virus informático se creó el software antivirus. Un antivirus no es más que la herramienta (programa o aplicación de software) utilizada para la prevención, detección, y erradicación de virus informáticos.

Los antivirus residentes, también llamados vigilantes, son antivirus residentes en memoria que se cargan automáticamente durante el inicio del sistema y se mantienen activos en memoria hasta que la sesión de trabajo finaliza y el ordenador se apaga, alertando al usuario de cualquier acceso no autorizado o sospechoso a la memoria o unidad de disco.

Los antivirus no residentes, también llamados exploradores, son aquellos que no se encuentran activos durante la sesión de trabajo o el periodo durante el cual el ordenados permanece encendido y que debemos poner en ejecución, es decir manualmente, para hacer uso de él y pode explorar el soporte de datos deseado."

Basado en: (Aguilera, 2010) Concepto de Antivirus "El antivirus tiene funciones como escanear los discos de su ordenador para buscar archivos infectados por un

virus informático. Para realizar esta operación, el antivirus emplea diferentes técnicas como la de comparación de una firma con un fragmento de virus conocidos, una especie de huella. Elimina los virus encontrados, cuando el antivirus descubre un archivo infectado, trata de quitar o neutralizar el virus. Si no lo consigue, puede o bien no ponerlo en cuarentena o bien eliminarlo.

La acción exacta que se lleva a cabo cuando se descubre un virus dependerá de la configuración del programa. Impedir la activación de un virus, el antivirus sigue activo permanentemente en su ordenador y analiza en tiempo real los archivos que maneja. Un antivirus debe estar actualizado ya que compara con la lista de firma de virus con la secuencia de bits de su ordenador".

Ilustración 1-0-4: Antivirus

Fuente: http://www.channelbiz.es/2013/03/15/antivirus-fin-cerca/06-03-2015.

Los antivirus en consecuencia son aplicaciones o grupo de aplicaciones que están dedicados a la prevención, búsqueda, detección y eliminación de programas malignos en los sistemas informáticos. Dentro de estos programas maliciosos podemos encontrar a los virus, los troyanos, gusanos, spyware entre otros malware que son los principales programas que se encargan de causar daño en los computadores, servidores y otros equipos que poseen información o que pueden ser los que ingresas ésta a las bases de datos de los servidores de aplicaciones o de bases de datos.

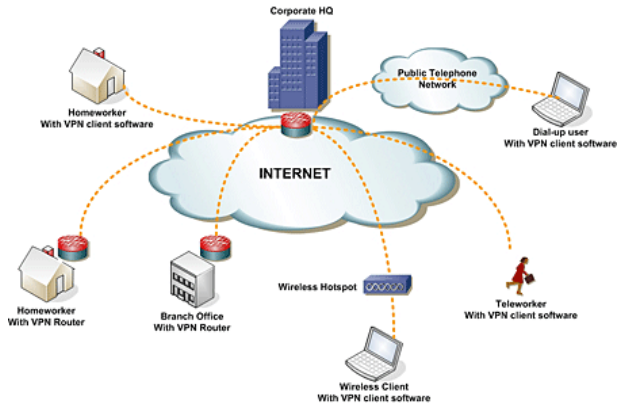
Para ser considerado como un antivirus es necesario que cumplan con muchos requisitos y de esta manera ser considerado como efectivo o eficiente:

- Deberán ser siempre activos,
- Tienen que tener una constante actualización ya que los intrusos generan a diario nuevas técnicas de ataques.
- Una completa bases de datos.

1.6 Vpn (virtual private network)

(Ditech, 2013).Definición de VPN (Red Privada Virtual). “es una conexión segura a través de Internet, que permite interconectar sedes remotas de forma segura pues utiliza protocolos de seguridad y encriptación de datos para mantener la confidencialidad y autenticidad de la información.”

Ilustración 1-0-5: Esquema VPN



Fuente:http://securitcrs.wordpress.com/knowledge-base/vpn-virtual-private-network/06-03-2015.

Basado en (Gil, Pomores, & Condelas, 2010). Concepto de VPN. “La red privada virtual permite simular una red de área local sobre una red pública. Una vez establecidas la conexión de la red privada virtual los datos viajan encriptados de forma que solo el emisor y el receptor son capaces de leerlos. Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad, confidencialidad y no repudio.

Las VPN son una salida al costo que puede significar el pagar una conexión de alto coste, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a internet".

Entonces las VPN's son redes privadas virtuales construidas dentro de una infraestructura de red pública, como por ejemplo internet. Toda empresa puede tener una VPN dentro de su propia red incluso ya sea para conectar directamente el departamento financiero con el área de tecnologías con la finalidad de evitar posibles ataques en la red de datos y de esta manera salir hacia el internet que siempre son los ISP los que dan el servicio y son ajenos a cualquier suministro de el mismo.

Existen también alternativas que pueden ser usadas como una red VPN para bajar costos y que son la utilización del ancho de banda de la red WAN, a la vez que se aumentan las velocidades al tratarse de canales dedicados y que van a través de la red Ethernet de una empresa.

Una VPN está en la capacidad de proporcionar una red VPN, ya que posee el máximo nivel de seguridad, ya que se encarga de cifrar las direcciones IP mediante el IPSEC y mediante los túneles del Secure Sockets Layer(SSL), y las diversas tecnologías de autenticación. Estas redes protegen todos los datos que se transmiten por VPN de un acceso no autorizado. Es importante que toda empresa aproveche los recursos con la finalidad de ganar velocidad en el internet y de esta manera añadir rápidamente nuevos emplazamientos y usuarios.

1.7. Sistema De Prevención De Intrusos

Según: (Ditech, 2013). Definición de IPS (Sistema de Prevención de Intrusos). "El Sistema de Prevención de Intrusos (IPS) es una tecnología de software más hardware que ejerce el control de acceso en una red de computadores para protegerla de ataques y abusos. La tecnología de Prevención de Intrusos (IPS) es considerada por algunos como una extensión de los Sistemas de Detección de

Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías de firewalls; incluso los complementan.

Los Sistemas de Detección de Intrusos (IPS) tienen como ventaja respecto de los Firewalls tradicionales (Cortafuegos), el que toman decisiones de control de acceso basados en los contenidos del tráfico, en lugar de hacerlo basados en direcciones o puertos IP.

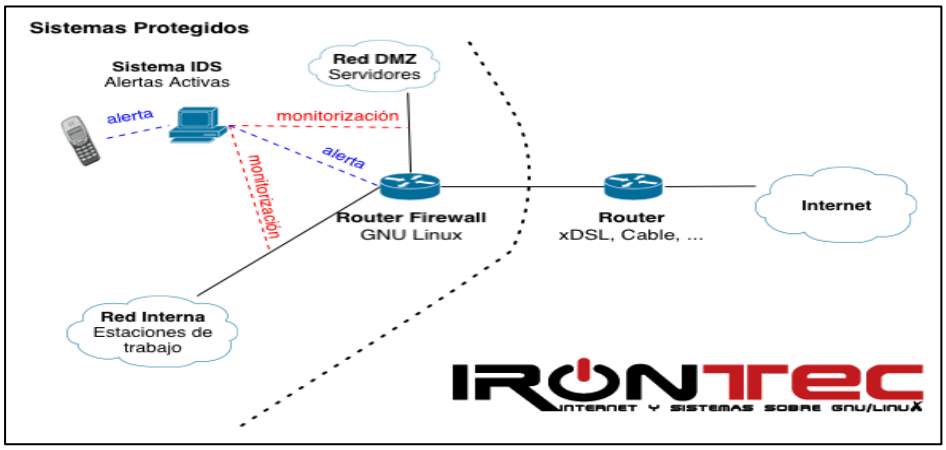
La diferencia entre un Sistema de Prevención de Intrusos (IPS) frente a un Sistema de Detección de Intrusos (IDS), es que este último es reactivo pues alerta al administrador ante la detección de un posible intruso (usuario que activó algún sensor), mientras que un Sistema de Prevención de Intrusos (IPS) es proactivo, pues establece políticas de seguridad para proteger el equipo o la red de un posible ataque".

1.8 Sistemas De Detección De Intrusos.

Basado en: Julio Gómez López, 2008 "Optimización de Sistemas de Detección de Intrusos en Red utilizando Técnicas Computacionales Avanzadas", pág. 3. Concepto de Sistemas de Detección de Intrusos. "Uno de los mecanismos de defensa más usados para reducir el riesgo de las compañías ante ataques dirigidos hacia los bienes informáticos han sido los sistemas de detección de intrusos o IDS (Intrusion Detection Systems).

Un IDS es un elemento que escucha y analiza toda la información que circula por una red de datos e identifica posibles ataques. Cuando aparece un ataque, el sistema reaccionara informando el administrador y cerrara las puertas al posible intruso reconfigurando elementos de la red como firewalls y routers."

Ilustración 1-0-6 Sistema de detección de intrusos



Fuente: http://www.irontec.com/ids.html/06-04-2015.

Según (Frahim & Santos, 2014). Definición de Sistemas de Detección de Intrusos. "Es el proceso de monitorización de eventos que suceden en un sistema informático o red y el análisis de dichos eventos en busca de signos de intrusiones. Estos sistemas están continuamente supervisando los componentes de la red y las personas o intrusos que están continuamente supervisando los componentes de la red y las personas que realizan individuos o sistemas no autorizados sobre elementos de la red. Los IDS (Sistemas de Detección de Intrusos) ayudan a entender el ataque, estimar los daños causados y tratan de prevenir otros ataques similares."

Dentro de este gran mundo de las seguridades informáticas apareció un nuevo tema como son los Sistemas de Detección de Intrusos los mismos que como la gran mayoría de UTM se encarga de controlar las intromisiones en una red de área local, la diferencia entre estas y el firewall es que esta apenas las detecta envía señales a los administradores pero solo cumple la función de detectar y no realizar otra opción que no sea la de comunicar y ahí termina el asunto en lo que tienen que ver con estas seguridades.

Entonces un IDS es un tipo de detección que es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuara como un usuario comprometido, su comportamiento se alejara del de un usuario normal.

1.9 Cisco Systems

En la actualidad existen muchas empresas que se dedican a la fabricación y comercialización de equipos de telecomunicaciones, pero según varias firmas internacionales CISCO son los mejores de largo en el mundo.

Cisco cuenta con su propio lenguaje de configuraciones hecho que lo hace ser más fuerte que la de sus principales contrincantes, dentro de su portafolio de productos se tienen hub, switch, routers, firewalls, teléfonos IP, centrales telefónicas, etc.

1.10 Tipos De Routers

Para la determinación de tipos de routers se tiene que remitir a cada autor por lo que se haría muy larga la precisión, por lo que se ha tomado a dos autores que coinciden con la definición de tipos de routers.

Según: (Bollaprogado, Murphy, & White, 2009)"Internal Router (IR) Routers Internos: Son los encargados de mantener la base de datos del área actualizada y optimizada de cada subred del área. Todos sus interfaces se encuentran en la misma área. El otro router que funciona en una única área es el ASBR.
Backbone Router (BR): OSPF requiere que todas las áreas estén conectadas al área 0 o de backbone. Un router en esta área es un BR. En un Área 0 también pueden estar IR, ABR y ASBR.

Area Border Router (ABR): Este router es el responsable de unir varias áreas. Mantiene una base de datos topológica de cada área. Realiza la suma del área y es el responsable de reenviar los LSAs entre áreas.

Autonomous System Boundary Router (ASBR): Es el responsable de conectar la red OSPF con una red externa con un protocolo EGP."

Según: (Gil, Pomores, & Condelas, 2010)“Router Neutros: Que son para la conexión de cable modem, este dispone de una comunicación WAN, que sirve para conectar con modem y el router XDSL.

Módem Router xDSL (Normalmente basados en ADSL, ADSL2 y ADSL2+ en el caso de España), se emplean en conexiones de banda ancha xDSL como ADSL, ADSL2 y ADSL2+, es decir que con un único router tenemos acceso a la red local y a internet. Y a esto hay que tomar en cuenta que se tiene ora subclasificación que se define de acuerdo a las necesidades empresariales.

Monopuerto (Router xDSL), tienen un sólo puerto Ethernet (Normalmente suele ser de 10 ó 100 Mbps (Fast Ethernet), no tienen Wifi) y en algunos casos pueden incluso funcionar por USB cosa poco aconsejable salvo que no haya otra opción, normalmente son los modelos más sencillos y que suelen “regalar” los ISP (Internet Services Provider, Proveedores de Acceso a Internet) al darte de alta en una conexión xDSL”

Entonces se puede concluir que se tienen tipos de clasificaciones de routers pero en los que más se acercan a la realidad tecnológica, pero dentro de estos tipos aparte de controlar el tráfico entran en distintas redes de área local y a su vez tienen la capacidad de trasmitir información desde adentro hacia fuera de la institución.

Se tiene Routers Internos que son los que están dentro de la misma área y que on tienen la capacidad de enrutar a otras redes.

- Routers de respaldo que son los que se encargan de trancalizar las redes, por lo que en general se configura como área 0.

- Router de área perimetral, sus comunicaciones e interfaces están en la capacidad de conectar a varias areas.

- Router limítrofe de los sistemas autónomo que es un router que al menos tiene una salida hacia una red externa a la red de área local.

1.11 Cisco Asa Serie 5500

Dentro de la familia de equipos de seguridad salta al ojo de los usuarios el cisco asa 5500 como los favoritos en el mercado de la tecnología, es por eso que la empresa Prodemco decide la adquisición de un equipo con estas características la misma que va a ser de gran apoyo por al gran cantidad de fortalezas que este tiene.

Este equipo es el encargado de ayudar a las organizaciones a encontrar un equilibrio entre lo que son las seguridades y la productividad, ya que combina las fortalezas de un Firewall en lo que son seguridades y las redes de última generación y dentro de esta combinación de utilidades se destacan la visibilidad y el control de las aplicaciones basadas en el comportamiento de sus aplicaciones.

Este equipo dispone de un robusto control de seguridades en línea para lo que son protección de intrusiones, cuenta con un sistema de protección avanzada contra amenazas con un sistema de prevención de intrusiones completo y de gran efectividad, administración remota de gran seguridad, protecciones contra los botnets, protecciones contra las amenazas procedentes de internet preventivas y casi en tiempo real.

Este equipo fue diseñado para todo tamaño de red dependiendo de su rendimiento y de acuerdo a su MultiScale y de una gran variedad de formatos.

Estos equipos están disponibles en módulos y en dispositivos autónomos que son escalables para una mejor actualización entre los módulos y el software para que garantice sus seguridades. Es un dispositivo blade de alto rendimiento que se integra particularmente con equipos de la misma marca logrando una gran conexión con otros equipos dentro de una misma red.

CAPÍTULO II

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

2.1 PRODEMCO S.A. Cuenca – Azuay

2.1.1 Reseña Histórica

Prodemco forma parte de la empresa Aglomerados Cotopaxi S.A. (ACOSA) fue fundada en el año de 1978 por un grupo de empresarios visionarios liderados por el Sr. Juan Manuel Durini Palacios, quien había incursionado en la industria forestal y maderera 30 años antes. En el año 1979, Aglomerados Cotopaxi S.A. inicia su producción introduciendo en el Ecuador el tablero de partículas aglomeradas con una moderna línea de tecnología de punta, importada desde Alemania.

A fines del mismo año incorpora la primera línea para recubrimiento de tableros del país, dando así mayor valor agregado a sus productos y expandiendo la gama de colores según los requerimientos del mercado nacional e internacional. En el año 2012 decide abrir sus puertas en la ciudad de Cuenca provincia del Azuay con capital Ecuatoriano – Peruano, ya que resultaba muy caro transportar desde la zona sur del país por lo que se abre primero como empresa de captación maderera para más luego convertirse en una empresa maderera anexa a Aglomerados Cotopaxi.

En la actualidad, Aglomerados Cotopaxi y sus aliados cumplen 30 años de vida y consolida su liderazgo como la industria forestal más grande del Ecuador, con una producción anual que supera los 140.000 metros cúbicos. Cuenta con un patrimonio forestal de 12.500 hectáreas, de las cuales 11.000 hectáreas se encuentran plantadas con pino radiata y pátula, y más del 30% restante está destinado a áreas protegidas para la conservación de ecosistemas propios de la zona, conservación de bosque nativo, protección de cuencas hidrográficas y otros beneficios ambientales.

2.1.2 Misión.

Somos una industria forestal líder en el establecimiento de plantaciones, producción y comercialización de tableros de madera, comprometida con el desarrollo sostenible.

2.1.3 Visión

Ser líderes en la industria maderera regional, la mejor opción para nuestros clientes y sinónimo de excelencia empresarial.

2.1.4 Objetivos

- Facilitar y fomentar buenas relaciones con nuestras comunidades vecinas.
- Ser un referente de buenas prácticas empresariales(especialmente ambiental y social,) en el sector forestal
- Incorporar un modelo de gestión propio y coherente con estándares internacionales
- Establecer una cultura de responsabilidad social empresarial (RSE) en todos los escenarios de la organización.

2.2 Métodos de Investigación

La utilización de los métodos de investigación nos ayuda a seguir procedimientos de una manera lógica, lo que nos permite la adquisición de nuevos conocimientos.

Método Analítico

Método Analítico. (2011). Recuperado el 31 de Julio de 2014. Disponible en http://es.scribd.com/doc/71345489/Unidad-1-Metodologia-de-La-Investigacion

> Este método es un proceso cognoscitivo que consiste en descomponer un objeto de estudio, separando cada una de las partes del todo para estudiarlas en forma individual.

El método analítico interactúa con los problemas y necesidades encontrados en la empresa Prodemco S.A ya que deben ser analizados en su totalidad es decir se los descompone en partes las cuales son estudiadas de manera aguda para poder hallar las causas y efectos que producen.

Es así como luego de aplicar este método minuciosamente se llegó a la conclusión de que el problema principal que tiene la empresa Prodemco S.A es la perdida de información y a su vez la falta de seguridades en la misma, además el análisis permitió identificar otros factores como la pérdida de tiempo y la baja en el área de producción.

Método Deductivo

Método deductivo. (2011). Recuperado el 31 de Julio de 2014. Disponible en http://es.scribd.com/doc/71345489/Unidad-1-Metodologia-de-La-Investigacion

> Es un método de razonamiento que consiste en tomar conclusiones generales para explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes, principios, etc., de aplicación universal y de comprobada validez para aplicarlos a soluciones o hechos particulares.

En base a la aplicación de este metodo se tuvo que tomar en cuenta algunos puntos de vista los mismos que van a ser plasmadas en el resto de la investigación:

Platear la presente investigación partiendo desde falta de una metodología que ayude a determinar la falta de seguridades y que el equipo adquirido sea la solución adecuada para la empresa.

Se definió algunos objetivos, entre los que se deban cumplir para poder alcanzar la garantía de la información dentro de la empresa, todo esto basado en el equipo CISCO ASA que es el más fiable del mercado y que constituye una garantía dentro del proceso de innovación tecnológica de la empresa se encuentra inmersa.

Justificar adecuadamente la investigación toda vez que se requiere la implementación de seguridades dentro de la empresa.

Conformar un marco teórico que sea un aporte para las fuentes bibliográficas de las futuras generaciones de investigadores de la institución y del país en general. La hipótesis de la investigación que será la que ayude a tener un termómetro del

trabajo realizado ya sea que se cumpla en su totalidad o parcialmente, pero siempre tratando de que sus objetivos hayan sido satisfechos adecuadamente.

Cumplir con la operacionalización de las variables que son parte importante de la hipótesis que como dato adicional son fuente fundamental de la investigación.

Se debe verificar la hipótesis con las fuentes que se obtuvieron de la aplicación de las entrevistas y encuestas al personal técnico y a las personas que se beneficiaran de la investigación.

Se obtendrán las conclusiones que serían la parte culminante de la investigación de forma que sean un aporte para las personas que quieran realizar un trabajo de este tipo sea en este empresa o en alguna otra.

Las recomendaciones serán obtenidas de las conclusiones como un aporte a los investigadores.

Método Hipotético-Deductivo

Método hipotético-deductivo. (2011). Recuperado el 31 de Julio de 2013. Disponible en http://es.scribd.com/doc/71345489/Unidad-1-Metodologia-de-La-Investigacion

> Es un método de razonamiento que consiste en tomar conclusiones generales para explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes, principios, etc., de aplicación universal y de comprobada validez para aplicarlos a soluciones o hechos particulares.

El método Hipotético-Deductivo permitió formular la **hipótesis** en el presente trabajo investigativo, luego de realizar el análisis pertinente de la información

recopilada, arrojando como resultado factores que inciden en la problemática dentro de la empresa.

En el presente caso se formuló la siguiente hipótesis: **La implementación de seguridades basadas en capas con tecnología CISCO permitirá el mejoramiento en la productividad de la empresa PRODEMCO. S.A** se planteó esta hipótesis tomando en cuenta todos los factores encontrados en los problemas formulados anteriormente, esta hipótesis debe ser deducida y verificada mediante la recopilación de información

2.3 Población y Muestra

A continuacion se detalla el numero de involucrados en la realizacion del presente trabajp investigativo.

INVOLUCRADOS	CANTIDAD
Personal administrativo	8
Area de sistemas	4
Area de produccion	25
Total	37

Elaborado por: Vinocunga Carolina

Para el caso de esta investigación se decidió tomar al universo completo de la empresa PRODEMCO ya que no es un número que requiera de ser tomado como muestra por ser inferior a 100.

2.4 Operacionalización de las Variables

Para la operacionalización de las variables se tuvo que la variable independiente es la que deberá influir mediante indicadores los mismos que servirán para poder obtener una variable dependiente con sus respectivos indicadores y que estos dos o la conjunción de estos podrán ser la propuesta de hipótesis. La misma que se tratara de comprobar a lo largo de este trabajo de investigación.

Variables Independientes

El análisis de seguridades basadas en Cisco para la conectividad de la red de la empresa Prodemco.

Variables Dependientes

Mejorar las seguridades de la empresa tanto en tráfico interno como externo.

2.5 Análisis e interpretación de resultados.

1.- ¿Qué tan importante es la tecnología en la actualidad?

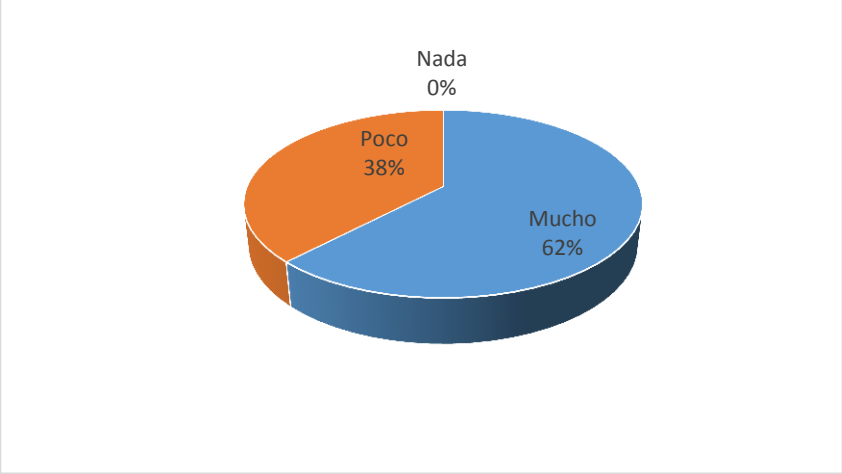
Tabla 1-0-1: La tecnología en la actualidad

RESULTADO		
Mucho	23	62%
Poco	14	38 %
Nada	0	0 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-1: La tecnología en la actualidad



Realizado por: Vinocunga Carolina

Análisis

El personal que labora en la empresa Prodemco considera importante contar con la tecnología de punta, ya que son parte de las actividades diarias que se deben realizar en la actualidad, y como era de esperarse todos coincidieron en esta respuesta.

2.- ¿Para sus actividades se requiere de internet?

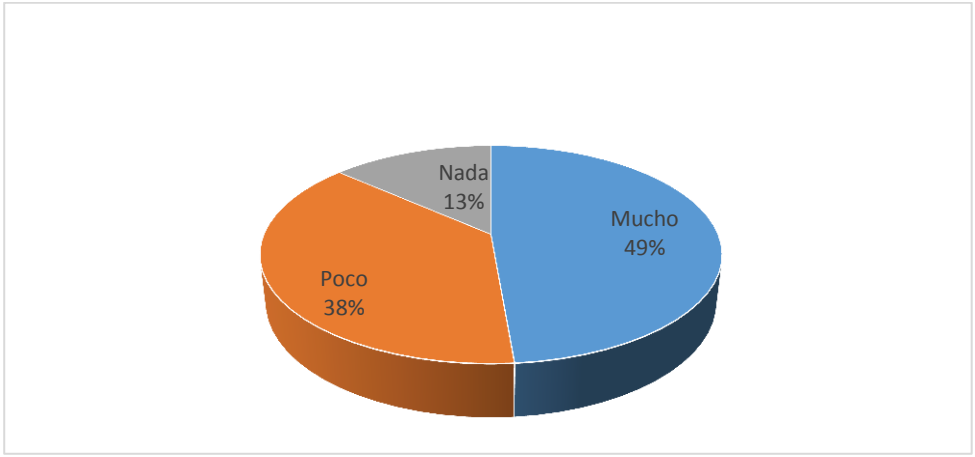
Tabla 1-0-2: Internet

RESULTADO		
Mucho	18	49 %
Poco	14	38 %
Nada	5	13 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-2: Internet



Realizado por: Vinocunga Carolina

Análisis

Casi el 50% de los encuestados coinciden que para sus actividades cotidianas se requiere del internet, un 38% manifiesta que se requiere pero que no es tan importante para su trabajo diario, y un 13% manifestó que no es necesario tener este servicio para sus labores.

3.- ¿Requiere de seguridades para su trabajo en el computador?

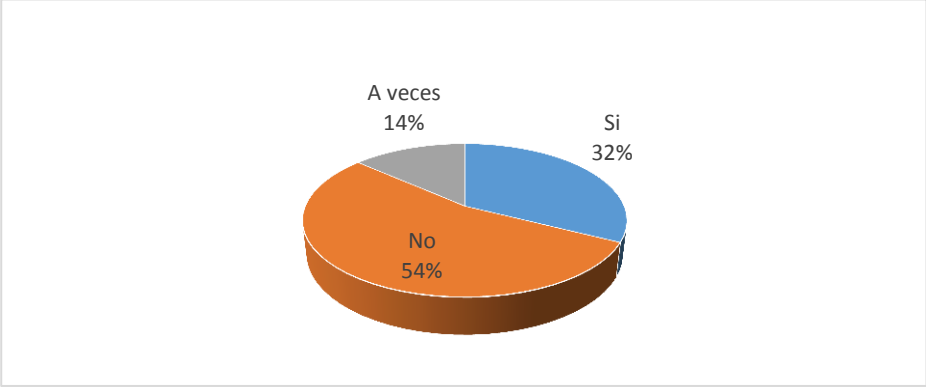
Tabla 2-0-3: Seguridad al trabajo

RESULTADO		
Si	12	32 %
No	20	54 %
A veces	5	14 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-3: Seguridad al trabajo



Realizado por: Carolina Vinocunga

Análisis

Un alto porcentaje que es del 54% considera que no requiere de seguridades para desempeñar su trabajo ya que manifiestan que no se maneja información de alto riesgo, un 14% está de acuerdo que en ocasiones se requiere de algún tipo de seguridades, un 32% que son áreas de riesgo de la información manifiesta que si se requiere de algún tipo de seguridad para garantizar los datos.

4.- ¿Es necesario cumplir con normas internacionales en su trabajo?

Tabla 2-0-4: Normas Internacionales

RESULTADO		
Siempre	15	40 %
A veces	14	38 %
Nunca	8	22 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-4: Normas internacionales

Realizado por: Vinocunga Carolina

Análisis

En un 40% considera que es importante alcanzar normas internacionales que garanticen ciertas actividades que se encuentran inmersas, un 38% no esta tan de acuerdo en que se deba tener ningún tipo de norma internacional para llevar la información, y un 22% no está de acuerdo con las normas internacionales para este tipo de procesos.

5.- ¿Conoce de equipos denominados Firewall?

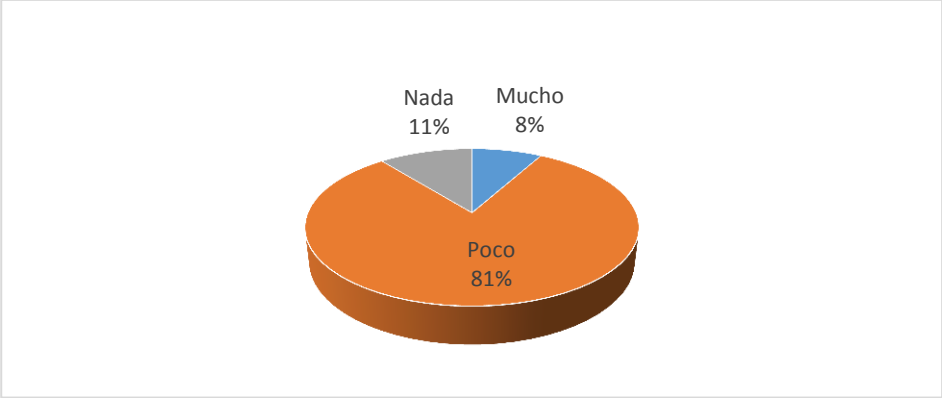
Tabla 2-0-5: Firewall

RESULTADO		
Mucho	8	8 %
Poco	30	81 %
Nada	4	11 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-5: Firewall



Realizado por: Vinocunga Carolina

Análisis

Un 8% de los encuestados manifiestan conocer sobre los firewall, mientras que un 81% dicen que alguna vez escucharon pero a ciencia cierta jamás supieron ni que son, peor aún de que se trata, y finalmente un 11% manifestó que desconoce totalmente de lo que se trata.

6.- ¿Qué conoce de los equipos de la marca Cisco?

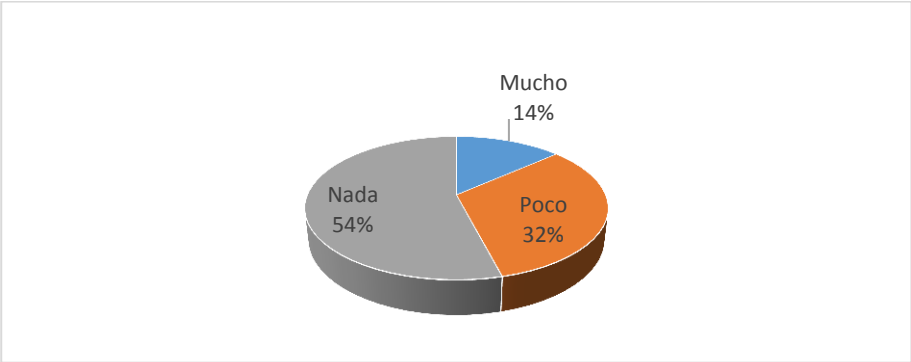
Tabla 2-0-6: Cisco

RESULTADO		
Mucho	5	14 %
Poco	12	32 %
Nada	20	54 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina.

Ilustración 2-0-6: CISCO



Realizado por: Vinocunga Carolina

Análisis

Hoy en día todas las empresas e instituciones necesitan de un adecuado soporte para mejorar sus procesos pero siempre hace falta una adecuada capacitación para que se puedan defender los usuarios de forma adecuada, fue casi total la aceptación al desenvolvimiento de la persona que maneja las tecnologías en la institución.

7.- ¿Considera importante invertir en un equipo de alta tecnología en seguridades?

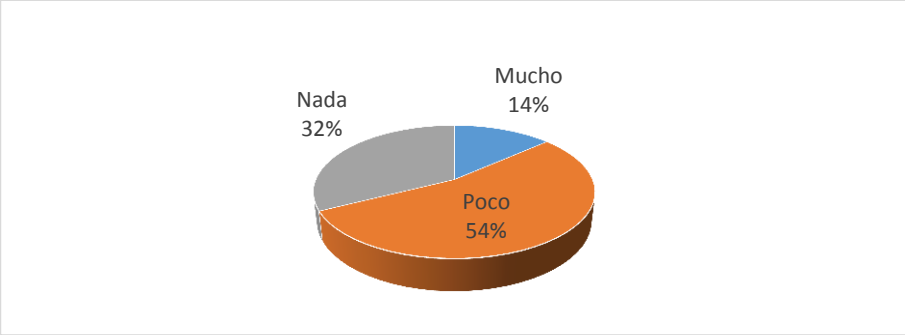
Tabla 2-0-7: Alta Tecnología

RESULTADO		
Mucho	5	14 %
Poco	20	54 %
Nada	12	32 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-7: Alta tecnología



Realizado por: Vinocunga Carolina

Análisis

En la actualidad se dispone de conexiones por lo que se garantiza una buena comunicación por lo que casi es imperceptible el servicio de CNT pero por el ancho de banda que se asignara desde Quito todos los procesos y funciones deberían mejorar ostensiblemente, y para eso se requiere de equipos de alta tecnología.

8.- ¿El internet es rápido para sus actividades?

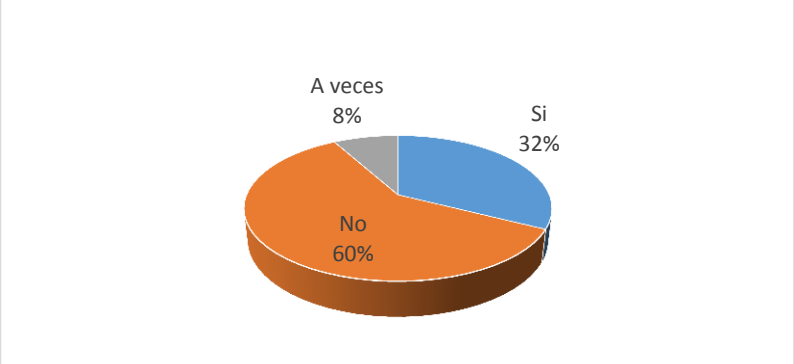
Tabla 2-0-8: El internet es rápido

RESULTADO		
Si	12	32 %
No	22	60 %
A veces	3	8 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-8: El internet es rápido



Realizado por: Vinocunga Carolina

Análisis

Esta pregunta genera mucha resistencia ya que se piensa que puede haber un mejor ancho de banda, todos requieren de más velocidad aunque no se sabe para qué, pero todos quieren, es así que el 60% no está de acuerdo en que el internet es rápido, un 32% piensa que la velocidad del internet es la adecuada para las actividades que se realizan.

9.- ¿Tienen restricciones en algunas páginas del internet?

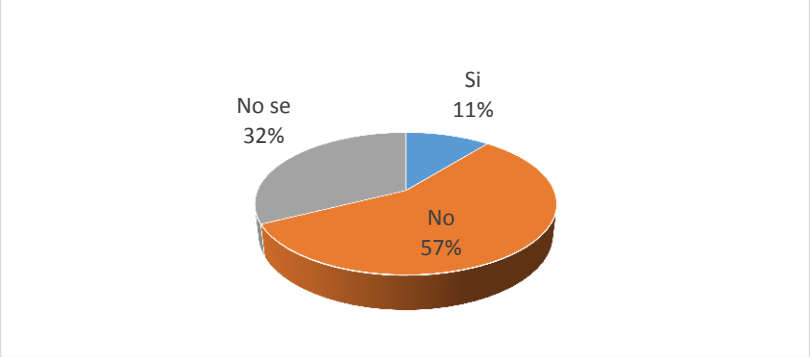
Tabla 2-0-9: Restricciones

RESULTADO		
Si	4	11 %
No	21	57 %
No se	12	32 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-9: Restricciones



Realizado por: Vinocunga Carolina

Análisis

Lo más sorprendente de esta pregunta es que muchos usuarios no saben cómo tienen el servicio del internet, mientras un 57% dice que no hay control de ciertas páginas de internet, un 32% desconoce si tienen o no las restricciones, y apenas un 11% sabe que tiene las restricciones.

10.- ¿Con nuevos equipos mejoraría las comunicaciones y las seguridades?

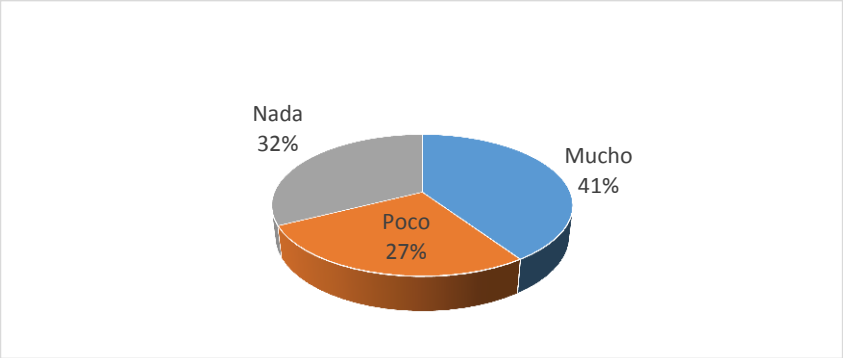
Tabla 2-0-10: Comunicaciones y seguridades

RESULTADO		
Mucho	15	41 %
Poco	10	27 %
Nada	12	32 %

Fuente: Personal de PRODEMCO S.A

Realizado por: Vinocunga Carolina

Ilustración 2-0-10: Comunicación y seguridades



Realizado por: Vinocunga Carolina

Análisis

La tecnología en la actualidad va cumpliendo un papel muy importante en el que hacer de toda empresa y más cuando se trata de prestación de servicios profesionales, es por esto que un 41% considera que es muy importante, un 27% manifiesta que es poco importante, y un 32% coincide que no es importante para nada estas actividades.

2.6 Comprobación de la Hipótesis

En el trabajo de investigación se plantea muchas inquietudes que tienen que irse develando en el transcurrir del proyecto, es por esto que se planteó como idea original:

"Analizar los seguridades basadas en tecnología Cisco ASA en la interconectividad LAN/WAN aplicada al diseño de la red de la empresa Prodemco de la ciudad de Cuenca provincia del Azuay"

En lo que va del proyecto de implementación de las seguridades basados en estos equipos se ha planteado efectos colaterales los mismos que no han podido ser subsanados de forma adecuada siendo estos principalmente por incompatibilidad de los otros equipos con que contaba la empresa, los equipos que nos daban empresas externas que fueron las que proporcionan uno que otro servicio, como es el caso del internet.

Cisco en la actualidad es la mejor empresa en interconexión y por defecto en las seguridades de la información, más sin embargo no son lo suficiente para poder alcanzar la satisfacción de los procesos de acuerdo a la necesidad de la empresa, dejando algunas partes por fuera de la implementación.

CAPÍTULO III

IMPLEMENTACIÓN DE SEGURIDADES BASADAS EN CAPAS CON TECNOLOGÍA CISCO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN Y PRODUCTIVIDAD DE LA EMPRESA PRODEMCO. S. A.

3. Propuesta

Las comunicaciones en la actualidad han ganado más relevancia que cualquier otra área tecnológica ya que todo gira en torno a un celular o una computadora, y que estos tengan comunicación con el Internet. Basada en esta singular característica y percepción tecnológica todas las empresas e instituciones realizan bastas inversiones en la adquisición de equipo que ayuden a la generación de información dentro de las instituciones y empresas y sobre todo que estas estén cuidadas y puedan garantizar su autenticidad.

Acosa empresa matriz de prodemco siempre en búsqueda de que su información permanezca intacta ha realizado inversiones en la adquisición de equipos tecnológicos de punta y que puedan resolver algunos de sus problemas de fidelidad de información y de integridad de los datos, ha creído conveniente la adquisición de equipos CISCO en todos sus niveles operativos de la infraestructura de red partiendo desde la capa física hasta su capa de administración y seguridades por lo que se considera toda la tecnología con que posee en la actualidad la empresa.

3.1 Objetivos.

3.1.1 Objetivo General

Mejorar las seguridades basadas en capas del modelo OSI con tecnología Cisco para proteger la información y la productividad de la empresa Prodemco. S. A. en la provincia del Azuay.

3.1.2 Objetivos Específicos

- Optimizar la información transmitida en tiempo real asegurando los datos enviados.

- Brindar seguridades a la cadena transmitida para que no sean alterados o modificados sin autorización.

- Incorporar un análisis en los routers de la empresa Prodemco S.A para precautelar la información que transmite.

3.1.3 Justificación

El uso de los sistemas tecnológicos a través de redes de computadores, y específicamente con el Internet, están creando un nuevo modelo de presentación y accesibilidad para empresas, industrias e instituciones, redefiniendo su papel como empresas dedicadas a aumentar el grado de percepción pública de la ciencia y de la tecnología en industrias. Surgen, por lo tanto, el interés de conectar los distintos sitios alejados de alguna ciudades y sitios remotos los cuáles son los tipos de aprendizaje más adecuados para desarrollarlos, especialmente en lo que toca el ámbito empresarial e institucional.

Teniendo en cuenta lo expuesto anteriormente el presente proyecto está respaldado por el suficiente aporte bibliográfico a usarse que permitirá el

desarrollo de la investigación, como también en la web hoy en día se puede encontrar información de manejo de distintas herramientas tecnológicas incluido guías de aprendizaje o cursos rápidos del mismo, permitiendo interpretar fácilmente el manejo del lenguaje de configuraciones de los equipos y accesorios de redes y comunicaciones que como toda la empresa está basado en CISCO, para que la empresa pueda desarrollar de mejor manera todos sus procesos y a la vez brindar un servicio óptimo a todos sus usuarios de computadores tanto a nivel local como en comunicaciones empresariales con otras ciudades a través de las redes e internet.

Es así que se llevó a exponer el tema a los directivos representantes de la empresa con la idea de que se mejore la situación tecnológica actual y que se pueda brindar un mejor servicio a nivel de comunicaciones, garantizando de esta manera que la empresa Prodemco pueda tener una administración directa hacia Cuenca y que de igual manera Quito pueda beneficiarse con el servicio que tiene Prodemco a nivel nacional.

El tema planteado la investigadora pretende realizar un enrutamiento rápido, ágil y seguro sobre plataformas Linux en lo que tiene que ver a sistemas operativos el sistema operativo IOS el cual es el propio de los dispositivos CISCO para lo que tiene que ver a él enrutamiento y encaminamiento de las redes de área extensa siempre precautelando que la última milla proporcionada por la empresa estatal, así como Telconet cumpla de manera eficiente.

La Prodemco y su empresa matriz Acosa al ser una empresa que se encuentra en la misma provincia será un nexo para que la Carrera de Ingeniería en Informática y Sistemas Computacionales siga creciendo en su afán de vincular hacia nuevas tendencias tecnológicas y poder brindar una alternativa de cómo mejorar procesos en todos los sectores del país.

La investigación se encuentra costeada en un 80% al tener Prodemco un equipo con las características planteadas para el desarrollo de las configuraciones que se

han planteado y que serán motivo de trabajo. El restante 20% será una inversión que la realice la investigadora ya que forma parte de los gastos que se van a tener en la investigación y que se pueden observar dentro del presupuesto planteado para el trabajo.

En fin por todas las razones enunciadas anteriormente las mismas que mediante el análisis que se lo ha realizado a cada una, indica que cumple con todas las especificaciones y requerimientos que solicita la investigación, por lo cual permite anunciar que el proyecto es factible llevarlo a cabo para así cumplir con lo expuesto al iniciar con el planteamiento del tema.

3.2 Análisis de Factibilidad

3.2.1 Factibilidad Técnica.

Para la ejecución del proyecto se conoce que el departamento de sistemas de la empresa cuenta con tecnología de última generación, toda vez que se tiene equipos con una gran capacidad de almacenamiento así como de procesamiento.

Se detalla a continuación los equipos tanto de administración como de ejecución del proyecto, que son equipos que generan las seguridades y las comunicaciones dentro de la empresa.

Tabla 3-0-1: Equipos Informáticos

PRODEMCO S.A. MIEMBRO DE LA CADENA ACOSA S. A. PARQUE INFORMATICO ACTUALIZADO AL 30/12/2014

CANTIDAD	DESCRIPCIÓN	GRÁFICO
4	• Servidor HP Proliant DL320e, Gen 8 v2 , Intel Xeon E3-1220v3, 3,11 Ghz, 4GB DDR3, 1U, Controlador de almacenamiento HP Dynamics Smart Array B120i, controlador de red Ethernet NC332i • Soporta 2 discos en bahías LFF Hot plug. • puertos de red HP Ethernet 1Gb 2 port Nc3220i • 300W de potencia de la fuente • Slot PCI-E X16:1 • Slot PCI-E X8: 1	**Fuente:** www.hp.com  **Realizado por:** Vinocunga Carolina.
32	Computadores HP ProDesk 400 G1 desktop PC 3.60 Ghz - Intel Core i7-4790, 8 GB DDR3 Memory, 1 TB HDD, DVDRW Windows 7 Pro 64 B	**Fuente:**http://www.solutekcolombia.com  **Realizado por:** Vinocunga Carolina

32	Computadores AcerAspire AXC-605-MO21 DT.SRPAL.020. Windows 8.1Intel Core i3-4150 Dual-core 3.50 GHz6 GB, DDR3 SDRAM1 TB HDD	**Fuente:** https://pcel.com  **Realizado por:** Vinocunga Carolina
3	• puertos integrados de 10/100/1000 Ethernet • 1 modulo slot libre • interfaces de alta velocidad de redes WAN • 2 slots de tarjetas de procesamiento digital • Modulo DSP de voz de alta densidad	**Fuente:** http://www.atec.ro  **Realizado por:** Vinocunga Carolina
2	El Cisco ® Catalizador ® 2960-SF Serie de switches Fast Ethernet Clase empresarial Conmutación de nivel 2 para aplicaciones de sucursales y acceso del campus de tamaño medio. Permiten a las operaciones comerciales fiables y seguras y menor costo total de propiedad a través de una serie de características innovadoras, incluyendo FlexStack, Power over Ethernet Plus (PoE +), y Cisco Catalyst SmartOperations.	**Fuente:** www.aliexpress.com  **Realizado por:** Vinocunga Carolina

	• 2 o 4 factor de forma pequeño conectable (SFP) para enlaces ascendentes Gigabit rendimiento y continuidad del negocio • 24 o 48 puertos Fast Ethernet • Cisco FlexStack para la gestión simplificada con 20 Gbps de rendimiento de la pila, cuando se despliegan con el módulo de apilamiento FlexStack • IEEE 802.1ab (LLDP), IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad (LACP), IEEE 802.3ah, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z • Modelos 370W o 740W oferta de combinado presupuesto POE / POE +	

Realizado por: Vinocunga Carolina

3.2.2 Factibilidad Económica

La investigación está plenamente garantizada en el ámbito económico, ya que la empresa colabora con el equipamiento tecnológico el mismo que permite o da las facilidades para las configuraciones, de parte de la investigación la tesista cubre lo que son traslados y asistencias técnicas cada vez que se requiera como parte de la elaboración de la investigación

En virtud de estos tres procesos se cumplen la investigación es plenamente factible para su análisis, diseño, desarrollo y ejecución.

3.2.3 Factibilidad Operacional

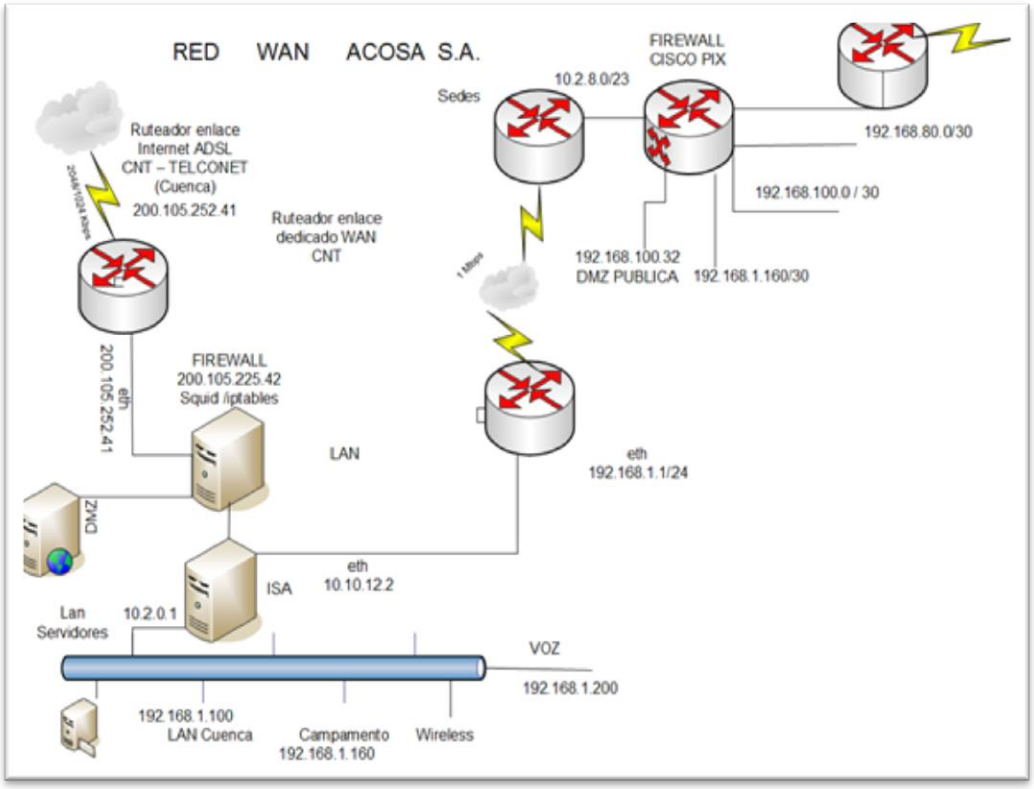
El proyecto es operativo, en virtud que es posible conectar un conjunto de computadoras entre si y que estas puedan tener seguridades dentro de la misma empresa y que puedan ser aún más con el exterior de ésta misma.

La empresa cuenta con muy buen equipamiento y todos de la mejor gama tecnológica actual en el mercado, y que pueden ser parte de la red de redes de ACOSA empresa matriz del grupo al que forma parte Prodemco S. A.

3.3 Diseño de la Propuesta

3.3.1 Diseño Esquemátic o del Sistema O Implementación De La Propuesta.

Ilustración 3-0-1: Diseño de Firewall



Realizado por: Carolina Vinocunga.

3.3.2 Requerimientos de la Propuesta.

Para desarrollar esta propuesta necesito hardware y software.
En un computador escritorio será instalado Centos 6.2 de Linux.

Hardware

- Marca: HP Prodesk
- Disco Duro: 400Gb
- Memoria Ram: 8 Gb DDR3
- Mainboard: Intel Core i7-4790
- Unidad de DVD-RW

Software

- Centos 6.2 de Linux.
- Squid.
- IPTABLES

3.4 Desarrollo De La Propuesta

Para la ejecución de la propuesta debemos partir de los comandos que se requieren para las configuraciones de los equipos cisco, ya que esta plataforma dispone de su propio sistema operativo que ayuda en el enrutamiento y el switching de los equipos de esta marca.

Tabla 3-1: Comandos básicos de IOS de Cisco

COMANDO	DESCRIPCIÓN
connect {dirección_ip|nombre}	Permite conectarse remotamente a un host

disconnect conexión	Desconecta una sesión telnet establecida desde el router
Enable	Ingresa al modo EXEC Privilegiado
Logout	Sale del modo EXEC
ping {dirección_ip|nombre}	Envía una petición de eco para diagnosticar la conectividad básica de red
resume conexión	Resume una sesión telnet interrumpida con la secuencia CTRL+SHIFT+6 y X
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación
show cdp entry [*|nombre_dispositivo] [protocol|version]}	Muestra información acerca de un dispositivo vecino registrado en una tabla CDP
show cdp interfaces [tipo número]	Muestra información acerca de las interfaces en las que CDP está habilitado
show cdp neighbors [tipo número] [detail]	Muestra los resultados del proceso de descubrimiento de CDP
show clock	Muestra la hora y fecha del router
Show history	Muestra el historial de comandos ingresados
show hosts	Muestra una lista en caché de los nombres de host y direcciones
show ip interface brief	Muestra un breve resumen de la información y

	del estado de una dirección IP
show ip rip database	Muestra el contenido de la base de datos privada de RIP
show ip route [dirección |protocolo]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro dirección permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro protocolo permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo rip, igrp, static y connected
show sessions	Muestra las conexiones Telnet establecidas en el router
show versión	Muestra información sobre el Cisco IOS y la plataforma
telnet {dirección_ip|nombre}	Permite conectarse remotamente a un host
terminal editing	Reactiva las funciones de edición avanzada
terminal history size numero_líneas	Establece el tamaño del buffer del historial de comandos
terminal no editing	Deshabilita las funciones de edición avanzada
traceroute dirección_ip	Muestra la ruta tomada por los paquetes hacia un destino.

Fuente: www.cisco.com

Elaborado por: Carolina Vinocunga

Con la revisión de los comandos básicos de Cisco podemos adentrarnos un poco más en la configuración del área local de la red así como de la red de área extensa, la misma que puede contar con muchos routers pero que la base fundamental van a ser los intervalos de las subredes que se pueden dar dentro de la empresa para poder cumplir con lo que se requiere en la empresa.

3.4.1 Fase De Planificación

- En este escenario empiezo a realizar la configuración de los routers de nuestro esquema de red ya que todos deberán realizar el mismo procedimiento.

- También doy a conocer las direcciones IP a cada una de las maquinas, así como su respectiva puerta de enlace para la comunicación entre maquinas, ya q esta me servirá para comunicarme con el router.

    1. Cuando ingresemos al router entramos en la pestaña CLI nos aparecerá una ventana de dialogo en la cual escribimos “no”.

    2. Para entrar al modo de administración ponemos enable.

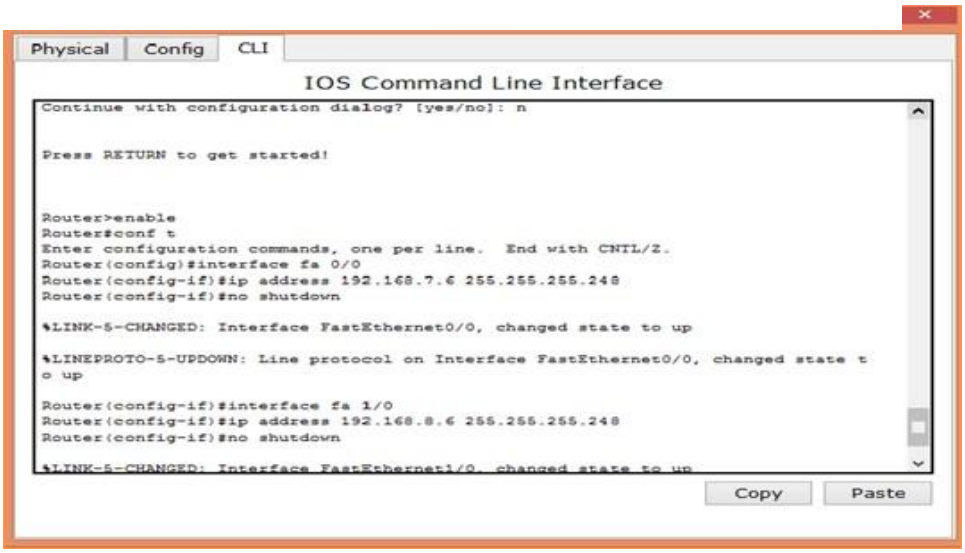
    3. Una vez que nos encontremos aquí en cambio tenemos que entrar al modo de configuración tecleando “conf t”.

    4. A partir de esto empezamos a configurar las interfaces que están conectadas al switch para la conexión de la pc con el router con el comando interface fa0/0 y fa 1/0 (este también varía de acuerdo con las interfaces q estén conectadas)

    5. Luego ingresamos las direcciones de las redes con su máscara de red con el comando “ ip address”.

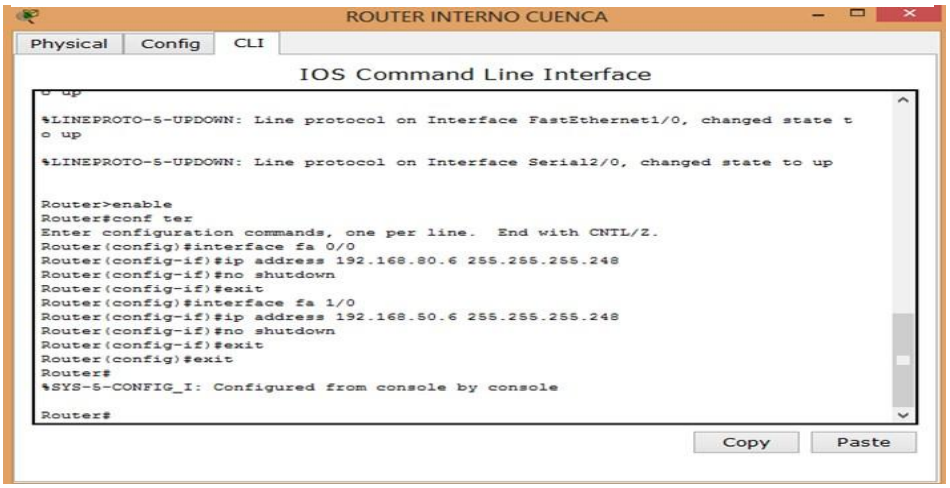
    6. Finalmente digitamos “no shutdown”, “exit”.

Ilustración 3-0-1: Configuración FastEthernet



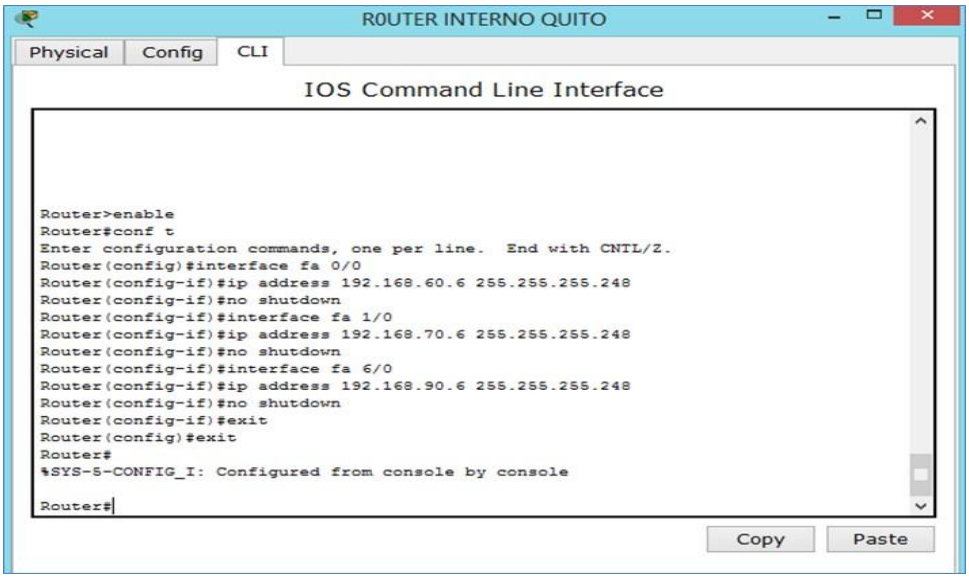
Realizado por: Vinocunga Carolina

Ilustración 3-0-2: Configuración FastEthernet



Realizado por: Vinocunga Carolina

Ilustración 3-0-3: Configuración FastEthernet



Realizado por: Vinocunga Carolina

Ahora les mencionare como realizar las comunicaciones entre routers mediante interfaces seriales. Para esto hemos creado VLMS con la finalidad de brindar seguridad perimetral.

Tabla 3.2: Seguridad Perimetral

Dirección de red	Host Utilizables	Dirección de broadcast	Mascara de red	Conectividad
192.168.4.0	**192.168.4.1 - 192.168.4.2**	**192.168.4.3**	**255.255.255.252**	**Lasso-Quito Quito-Lasso**
192.168.4.4	**192.168.4.5 - 192.168.4.6**	**192.168.4.7**	**255.255.255.252**	**Cuenca-Quito Quito-Cuenca**

192.168.4.8	**192.168.4.9 - 192.168.4.10**	**192.168.4.11**	**255.255.255.252**	**Lasso-Cuenca Cuenca-Lasso**
192.168.4.12	**192.168.4.13 - 192.168.4.14**	**192.168.4.15**	**255.255.255.252**	**Quito/R-Interno Quito R-Interno Quito/Quito**
192.168.4.16	**192.168.4.17 - 192.168.4.18**	**192.168.4.19**	**255.255.255.252**	**Cuenca/R-Interno Cuenca R-Interno Cuenca/Cuenca**

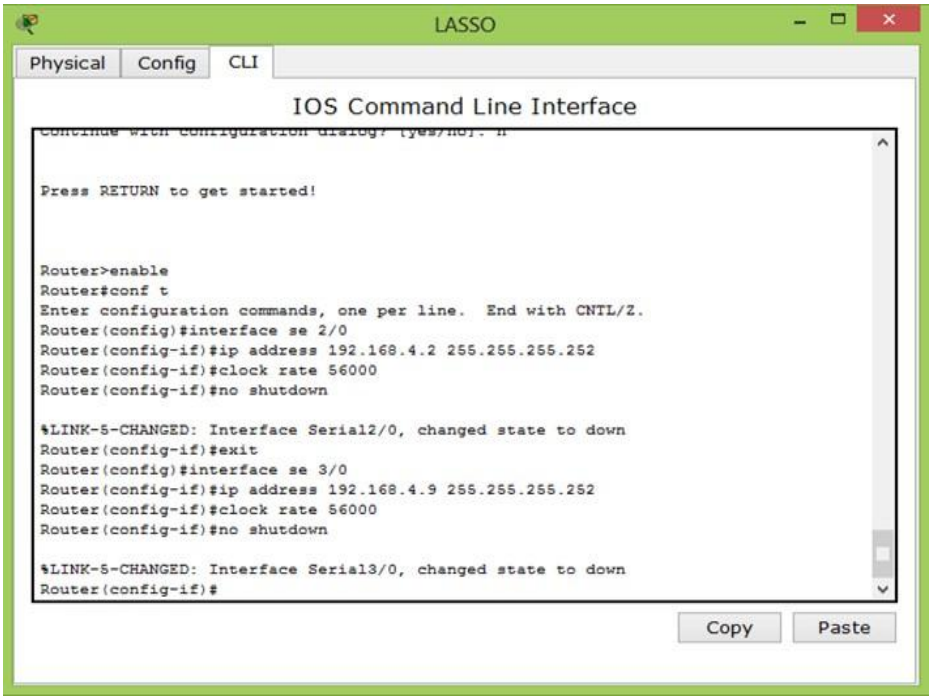
Realizado por: Vinocunga Carolina

3.4.2 Fase De Configuración.

Para las configuraciones de los equipos de enrutamiento se decidió la división como se pudo observar en el segmento anterior el mismo que ayudara en la agilidad de la información como punto de partida, y para esto hay que configurar los puertos que se consideran importantes dentro de los equipos de enrutamiento.

- Lasso se conecta a Quito por la serial 2/0
- Lasso se conecta a Cuenca por la serial 3/0

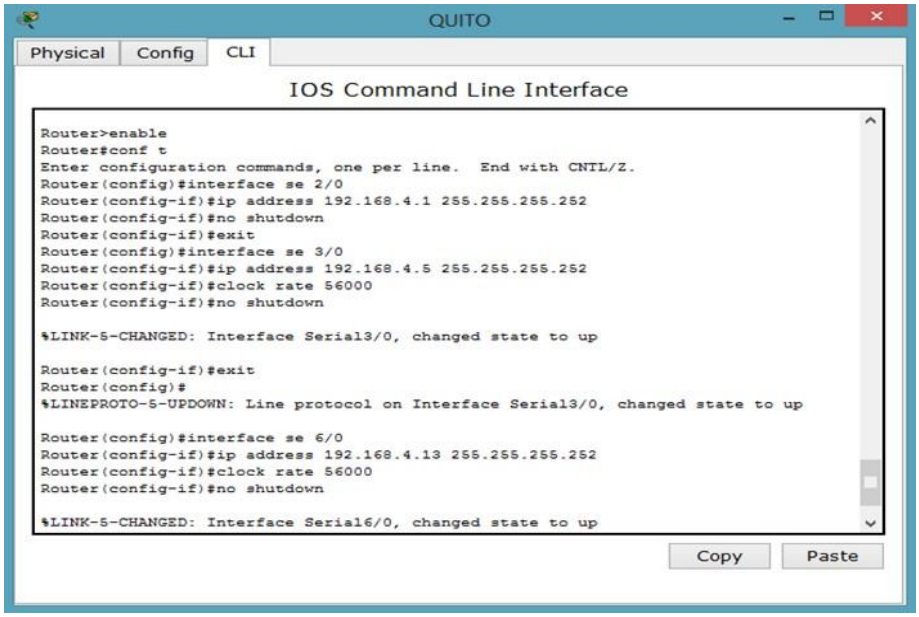
Ilustración 1-0-4: Configuración Interface Serial



Realizado por: Vinocunga Carolina

- Quito se conecta a Lasso por la serial 2/0
- Quito se conecta a Cuenca por la serial 3/0
- Quito se conecta a su router interno de Quito serial 6/0

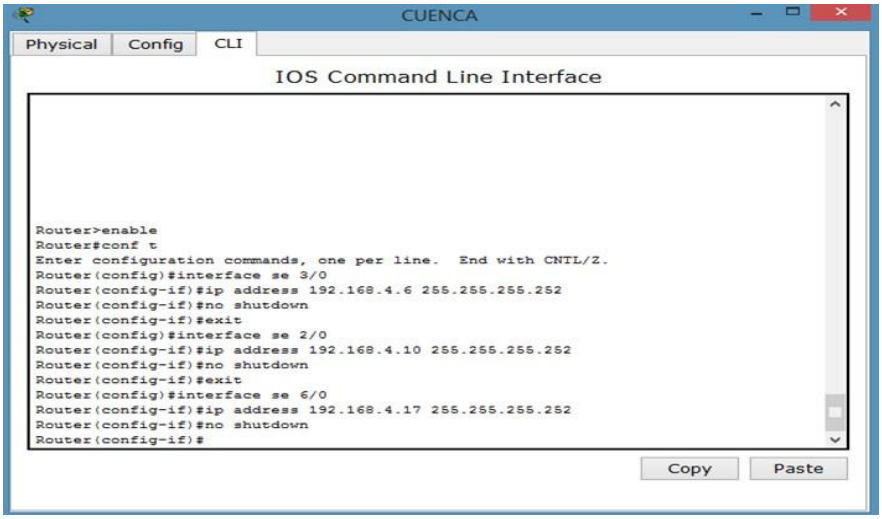
Ilustración 3-0-5: Configuración Interface Serial



Realizado por: Vinocunga Carolina

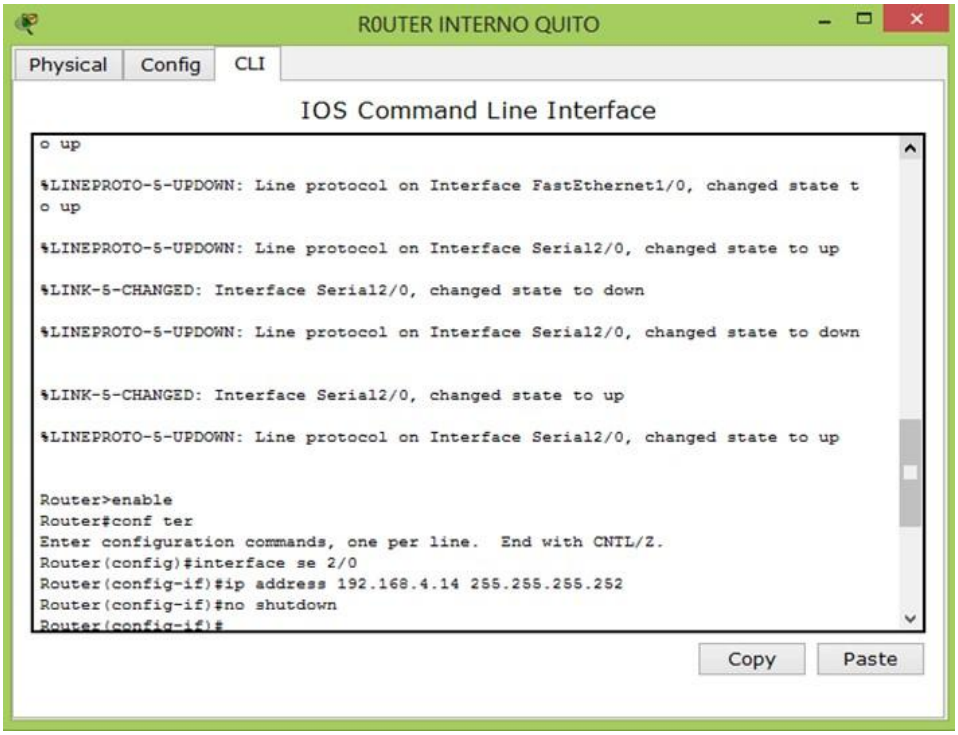
- Cuenca se conecta con Quito por la serial 3/0
- Cuenca se conecta con Lasso por la serial 2/0
- Cuenca se conecta a su router interno por la serial 6/0

Ilustración 3-0-6: Configuración Interface Serial



Realizado por: Vinocunga Carolina

Ilustración 3-0-7: Configuración Interface Serial

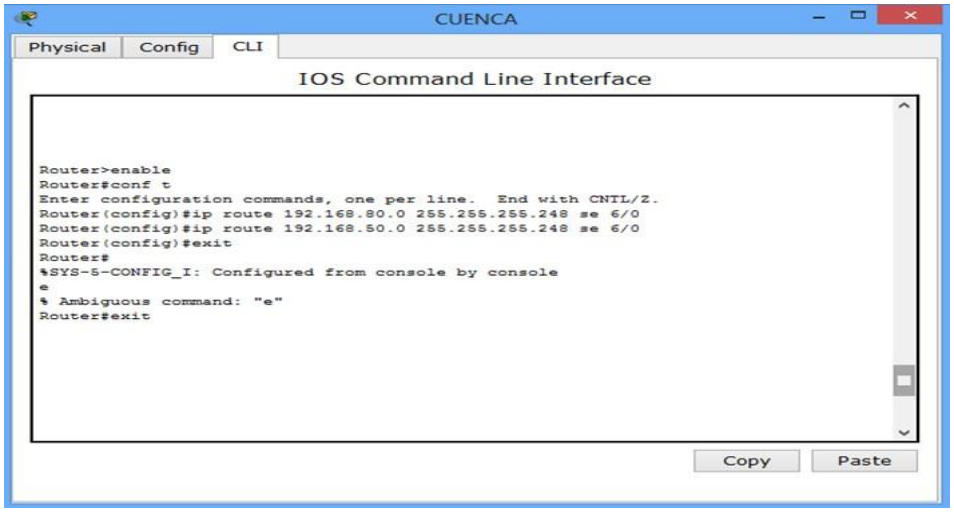


Realizado por: Vinocunga Carolina

- Hasta el momento se tiene configurado pero esto no es suficiente ya q si deseamos enrutar desde una pc de Lasso a Quito no será posible ya q solo saldrá hacia el router más cercano y regresara.

- Para ello se debe realizar el enrutamiento estático y se utiliza el comando "ip route + dirección de red y mascara + la serial q se encuentra más cerca al router ", que para el caso de nuestras configuraciones es la 6/0.

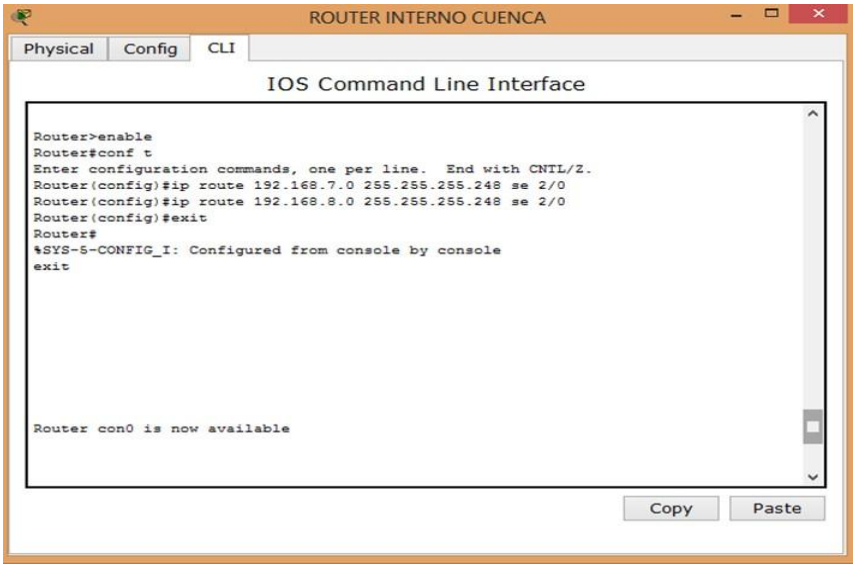
Ilustración 3-0-8: Enrutamiento



Realizado por: Vinocunga Carolina

Para las configuraciones internas entre las seguridades y la planta, con las oficinas en el centro de cuenca se debe tomar en cuenta los puertos que deben cumplir con las mismas características que se tienen en la ciudad de Quito y que estos puedas realizar las mismas actividades como se lo hace entre Lasso y Quito

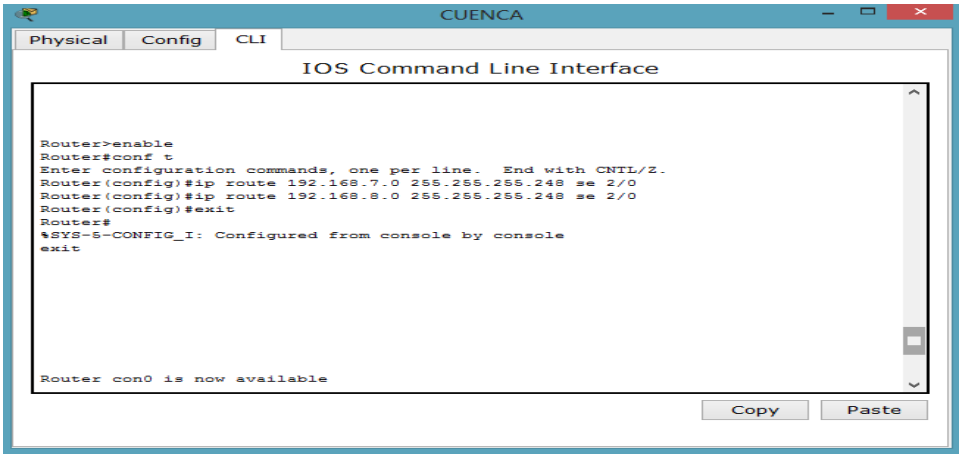
Ilustración 3-0-9: Enrutamiento



Realizado por: Vinocunga Carolina

Tomamos en cuenta los puertos del 2 y 3 para los segmentos de la red que están basados según las subredes 7 y 8 es decir quedarían en dos segmentos de red que no se pueden ver entre sí.

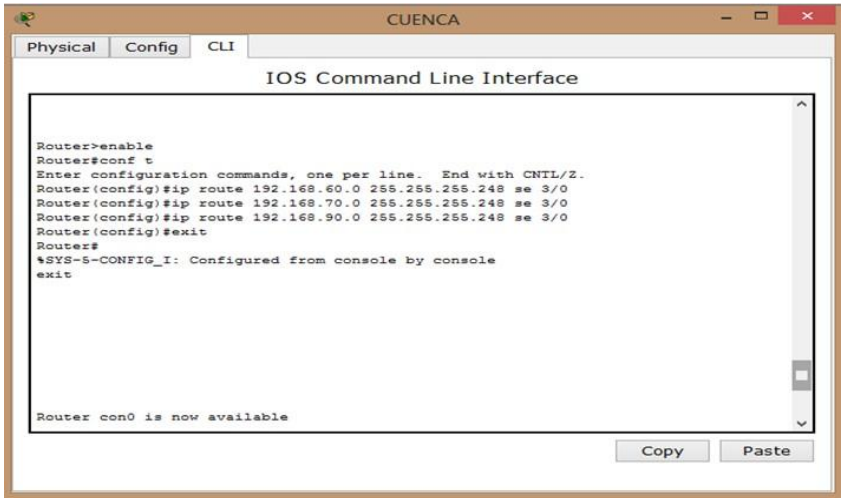
Ilustración 3-0-10: Enrutamiento



Realizado por: Vinocunga Carolina

Del otro router tomamos en cuenta 2l puerto 3 únicamente pero enruta tres direcciones para diferenciar las señales que se envían con otras ciudades como es el caso de Lasso y Quito que fue explicado en este segmento.

Ilustración 3-0-11: Enrutamiento



Realizado por: Vinocunga Carolina

3.4.3 Fase de Aplicación

Para completar la implementación de seguridades dentro de la empresa se tomó en cuenta la utilización del SQUID como proxy el mismo que aparte de repartir el recurso de internet, y sus seguridades para poder filtrar ciertas páginas web y poder administrar este recurso de acuerdo a las necesidades de los administradores de la red.

De igual manera se ha tomado en cuenta la implementación de un IPTABLE en calidad de Firewall con la idea de bloquear ciertos puertos tanto de entrada como de salida de información desde y hacia el exterior de la empresa y que utilizan el internet como medio de comunicación externa.

La idea de realizar un squid en la empresa es la de aprovechar el cache que tiene este servicio en Linux, y obviamente mejorar los servicios que tienen en la actualidad al conectarse desde el exterior hacia el interior mediante peticiones recurrentes que se los hace a los distintos protocolos de comunicación y seguridad, esto estaría complementado por las seguridades que puede ofrecer el firewall basado en iptables para cerrar los puertos que se quedan abiertos en el sistema operativo.

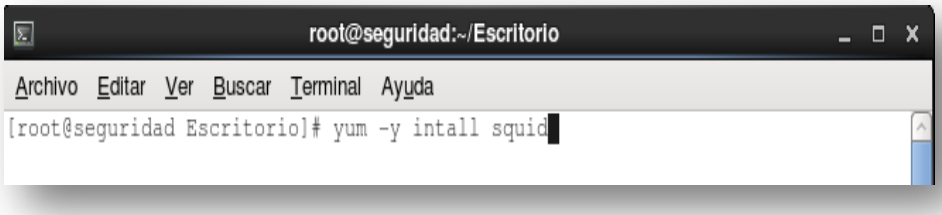
De las funciones importantes se tienen el que está orientado a las páginas web tanto normales como las seguras o que cuentan con encriptación de código y que son utilizadas para páginas que disponen de contraseñas y en la mayoría de páginas que tienen que ver con el sector financiero. Ademas que siempre se debe considerar al FTP e incluso al GOPHER que son protocolos propios de las redes de datos y que en algún momento se los requiere pero como en todo consumen recursos y abren puertos.

Se consideró para la empresa tomar en cuenta al puerto 3128 que es el puerto por defecto de esta plataforma para atender ciertas peticiones a pesar que se lo puede realizar en cualquier puerto y que pude funcionar de igual manera que con este puerto, considerando que se tienen reglas que son utilizadas para el control de acceso mediante políticas que se encuentran en el servidor y que sirven para administrar cualquier equipo de la red.

Instalación de SQUID

Para instalar el SQUID se ejecuta el siguiente comando

Ilustración 3-0-12: Configuración SQUID



Realizado por: **Vinocunga Carolina**

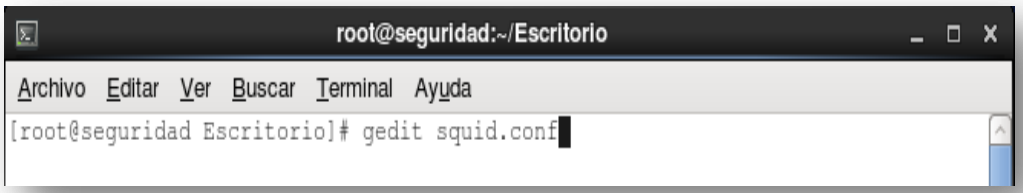
Archivo de configuración de SQUID.

Una vez realizado la instalación de este servicio con el que cuenta Linux , tenemos el archivo más importante de este servidor es el **squid.conf** ya q aquí se encontraran las configuraciones q realizaremos para la seguridad en la red. La ubicación de este archivo esta en /etc/squid/.

Configuración de SQUID

Empiezo con la configuración del squid con el siguiente comando.

Ilustración 3-0-13: Configuración SQUID



Realizado por: **Vinocunga Carolina**

Una vez q he ingresado al archivo establezco una lista de control de acceso q abarca a la red 192.168.1.0/24, que seria las direcciones que por defecto trabaja la empresa de telecomunicaciones públicas nacionales, las mismas que están consideradas dentro de este archivo.

Ilustración 3-0-14: Configuración SQUID

Realizado por: Vinocunga Carolina

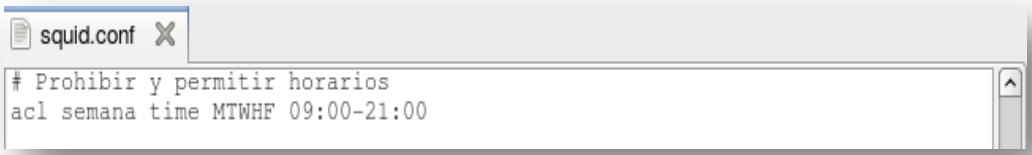
También se creara una lista de control de acceso para denegar páginas que se desean bloquear por tratarse de contenido no permitido para los usuarios de los puntos de acceso al servidor por ser información que pueda atentar con la integridad de la empresa.

Ilustración 1-0-15: Configuración SQUID

Realizado por: Vinocunga Carolina

La siguiente lista de control de acceso será para permitir el acceso de acuerdo a los requerimientos de días y horas que tendrán los usuarios.

Ilustración 1-0-16: Configuración SQUID

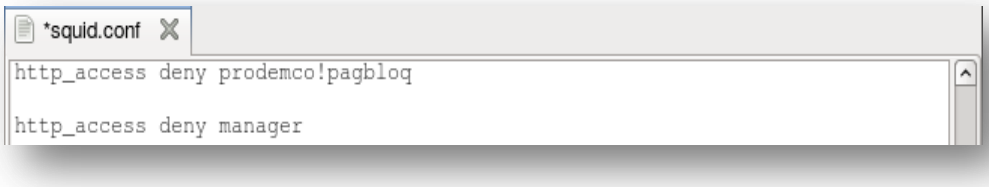


Realizado por: **Vinocunga Carolina**

La última regla de control de acceso q me permitirá ejecutar las seguridades realizadas en el squid.

En esta sección deniego el acceso a ciertas páginas web.

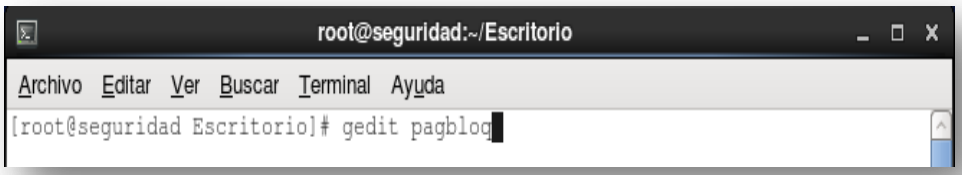
Ilustración 3-0-17: Configuración SQUID



Realizado por: Vinocunga Carolina

Una vez realizadas las configuraciones en **squid.conf,** regresamos al terminal y procedemos a constatar que se haya creado la carpeta **pagbloq** que habíamos generado.

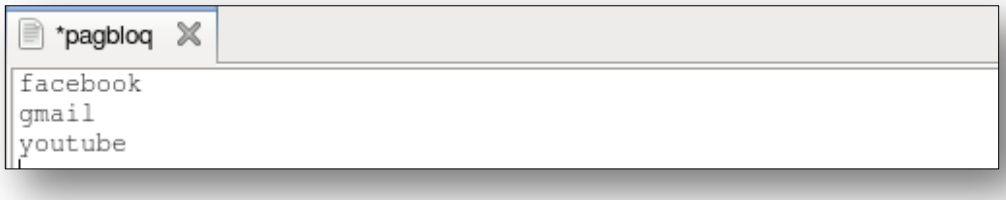
Ilustración 3-0-18: Configuración SQUID



Realizado por: Vinocunga Carolina

Si esta carpeta fue creada correctamente ingresara a la misma, en donde procedemos a ingresar las páginas que deben ser bloqueadas.

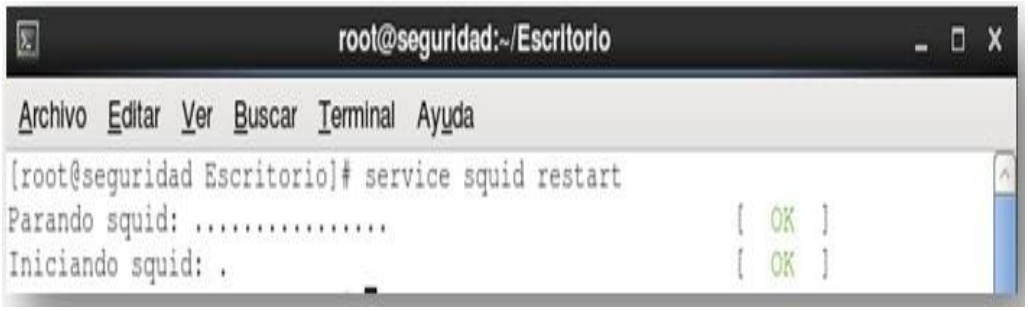
Ilustración 3-0-19: Configuración SQUID



Realizado por: **Vinocunga Carolina**

Una vez que realice todas las configuraciones deseadas procedo reiniciar los servicios para que surtan el efecto deseado dentro de la plataforma tecnológica.

Ilustración 3-0-20: Configuración SQUID

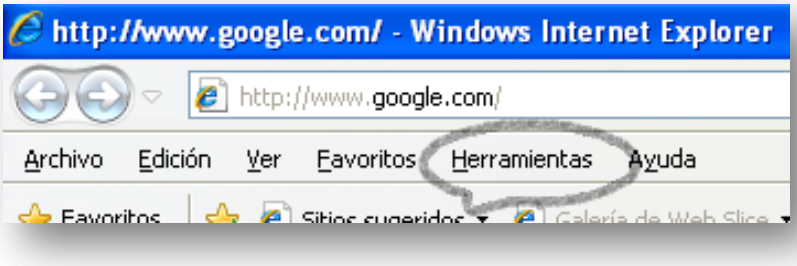


Realizado por: Vinocunga Carolina

Configuración proxy en Windows 7

Para la configuración del proxy debemos acceder a cualquier navegador ya sea Internet Explorer, Google Crome, Firefox, etc, y los personalizamos, pero para que los cambios surtan efectos en todos los navegadores se brinda alternativa que se lo haga a través de Internet explorer ya que este trabaja directamente con la plataforma de Windows, por lo tanto entrega las configuraciones a los otros navegadores.

Ilustración 3-0-21: Configuración Proxy

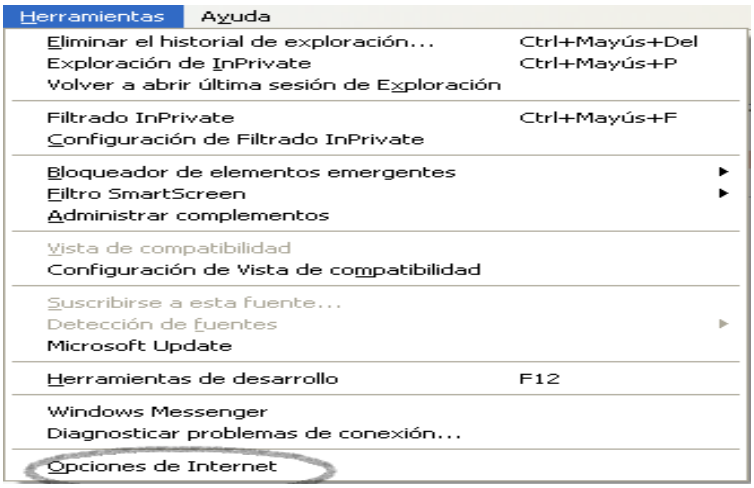


Fuente: Internet Explorer

Realizado por: Vinocunga Carolina

Se despliega un menú y escogemos la siguiente opción.

Ilustración 3-0-22: Configuración Proxy

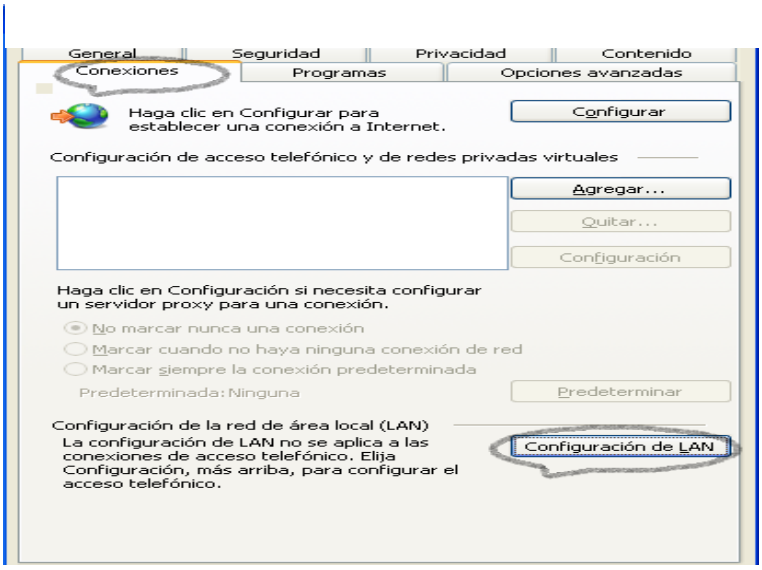


Fuente: Internet Explorer

Realizado por: Vinocunga Carolina

Se desplegará una nueva pantalla en donde se debe elegir las opciones.

Ilustración 3-0-23: Configuración Proxy



Fuente: Internet Explorer

Realizado por: Vinocunga Carolina

Aquí asignaremos la dirección 192.168.1.0 y el puerto 3128 y damos click en aceptar.

Ilustración 3-0-24: Configuración Proxy

Fuente: Internet Explorer

Realizado por: Vinocunga Carolina

Por lo que las direcciones y los puertos quedan activos, para que se puedan ejecutar las opciones de compartir los recursos.

IPTABLES

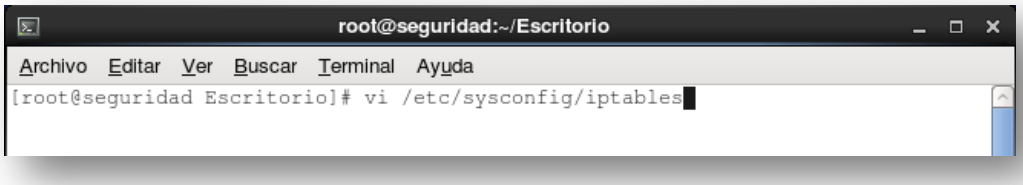
La segunda parte de la investigaciones la asignación de puertos de entrada y salida para todas las actividades de un servidor que servirá de pared de fuego(firewall), el mismo que puede tener las alternativas de negar o aprobar el trafico externo – interno.

Creación de iptables para la restringir el acceso desde los puertos de Linux de manera que ningún usuario pueda ingresar a realizar cambios.

```
echo "1" >/proc/sys/net/ipv4/ip_forward

iptables -F

iptables -t nat -F

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -d 0/0 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT

iptables -t nat -A PREROUTING -s 193.168.0.20 -p tcp --dport 80 -j ACCEPT

iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3128

iptables -A FORWARD -s 192.168.1.0/24 -p UDP --dport 21 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24 -p TCP --dport 21 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p UDP --dport 22 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p TCP --dport 22 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p TCP --dport 53 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p UDP --dport 53 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p TCP --dport 80 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p UDP --dport 80 -j ACCEPT

iptables -A FORWARD -s 192.168.1.0/24  -p TCP --dport 3128 -j ACCEPT

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -j DROP
```

Para acceder a verificar si las reglas iptables están creadas ingresamos lo siguiente en el terminal.

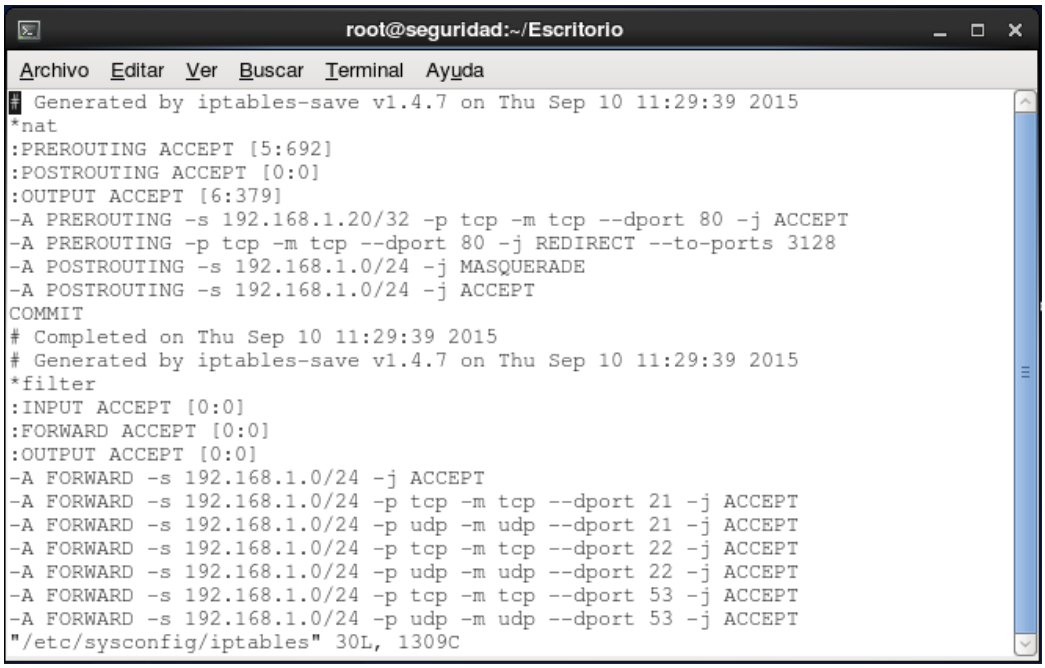
Ilustración 3-0-25 IPTABLES



Realizado por: Vinocunga Carolina

Al ingresar este comando se desplegara todas las reglas iptables q se han realizado para las seguridades de la red de datos empresarial que será la que se encarga de las comunicaciones.

Ilustración 3-26: IPTABLES



Realizado por: Vinocunga Carolina

Con estas configuraciones La mayoría de las formas de comandos de iptables requieren que se les indiquen una especificación de reglas, que es usada para comparar un subconjunto particular del tráfico de paquetes de red procesados por una cadena. La especificación de regla incluye también un destino que determina qué hacer con paquetes que son comparados por la regla.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La red de datos en la actualidad cuenta con seguridades físicas que van dentro de la empresa pero que puede tener ataques de denegación de servicios cuando no se tiene activado el iptables dentro del servidor, por muchos recursos que este pueda consumir.

- Un proxy de datos ayuda a compartir recursos y a brindar seguridades blandas a través de las reglas pero claramente se puede ver que desnuda otras muchas vulnerabilidades sobre todo en protocolos como el DTU al envió/recepción de los datagramas.

- El proxy es considerado como un firewall transparente por lo que siempre representara un atentado tenerlo como herramienta de control de tráfico dentro de una red empresarial

- Los IPTABLES garantizan la comunicación dentro de una empresa, lo que ayuda a que no se invierta mayor cantidad de dinero en más clusters de seguridad que los que ya se tienen, cuando con investigación se tienen este tipo de alternativas a las ya existentes en el mercado.

- Se debe platear planes de contingencia en caso de ataques cibernéticos dentro de las comunicaciones teniendo en cuenta que este campo siempre está en constante crecimiento, de acuerdo a las necesidades empresariales.

Recomendaciones

- Generar un plan de contingencias ante posibles ataques que se tengan a los equipos de comunicación de la empresa, para poder tener capacidad de reacción ante posibles hechos aislados de alteración de información.

- Migración de las otras plataformas hacia el open source para poder tener una misma plataforma, esto hará que los servicios de los otros servidores hablen en un mismo idioma dentro de la red y ayudara a que se puedan desarrollar de mejor manera.

- El squid es la mejor alternativa en Proxy pero siempre es bueno que este complementado con el IPTABLES para cuidar de las posibles amenazas, y que estas puedan ser mitigadas a tiempo y que los costos beneficio sean mínimos.

- Las comunicaciones entre sedes de ACOSA deberán garantizar que la información que entre pase por un mismo filtro y no como se lo realiza en la actualidad de forma aislada.

- El subneteo de redes se lo debe realizar en base a las necesidades de la empresa basada en actividades, y más no a departamentos ya que esto genera retraso en las comunicaciones.

Glosario De Siglas

B

BIT: Binary Digit O Dígito Binario

C

CPU: Central Processing Unit o Unidad de Procesamiento Central.

CIDR: Classless Inter-Domain Routing o Enrutamiento Entre Dominios sin Clases

D

DHCP: Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host.

DNS: Domain Name System o Sistema de Nombres de Dominio.

DOS: Disk Operating Syistem o Sistema Operativo de Disco.

E

EIA: Electronic Industries Association o Asociación de Industrias Electrónicas.

F

FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos

G

GUI: graphical user interface o interfaz gráfica de usuario

H

HTTP: Hiper Text Transfer Protocol o Protocolo de Transferencia de Hipertexto.

I

IEEE: Instituteof Electrical and Electronics Engineers o Institutos de Ingenieros Eléctricos y Electrónicos.

IETF: Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet.

IP: Internet Protocol o Protocolo de Internet.

IPV4: Internet Portocol v. 4 o Protocolo de Internet versión 4.

IPV6: Internet Portocol v. 6 o Protocolo de Internet versión 6.

ISP: Internet Service Provider o Proveedor de Servicios de Internet.

L

LAN: Local Área Network o Red de Área Local.

M

MAC: Media Access Control o Control de Acceso al medio.

N

NAT: Network Address Traslation o Traducción de Dirección de Red.

P

PDA: Personal Digital Assistant o Asistente Digital Personal

Q

QoS: Quality of Service o Calidad de Servicio.

R

RAM: Random-Access Memory o Memoria de Acceso Aleatorio.

RCF: Requests for Comments o Peticiones de Comentarios.

T

TCP: Transmission Control Protocol o Protocolo de Control de Transmisión.

TIA: Telecommunications Industry Association o Asociación de la Industria de las Telecominicaciones.

U

UDP: User Datagram Protocol o Protocolo de Datagrama de Usuario

V

VPN: Redes Privadas Virtuales

Glosario De Términos

A

AUTHENTICATION: En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

B

BYTE: Un byte es la unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos.

C

CABLE UTP: Es un tipo de cable que se utiliza en las telecomunicaciones y redes informáticas para la trasmisión de datos.

CISCO: Es una empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones, es el líder mundial en redes para internet.

CENTOS: Es una distribución del sistema operativo GNU/Linux que es desarrollado por la empresa Red Hat Enterprise Linux.

D

DOMINIO: Es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

DHCP: El protocolo de configuración dinámica de host, es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Dirección IP: Viene a ser una estructura numérica que identifica principalmente a un computador, de manera lógica y jerárquica dentro de la red informática e internet.

E

ETHERNET: Es un estándar de redes de área local para computadores

F

FIBRA ÓPTICA: La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Firmware: Es un programa que está grabado en la memoria ROM y establece la lógica de más nivel que controla los circuitos electrónicos de un dispositivo.

H

HOME BANKING: Banca en Línea es el servicio por el cual se pueden ejecutar transacciones bancarias por medios electrónicos específicamente vía redes privadas o públicas como el internet.

HUB: Es un dispositivo que tiene la función de interconectar las computadoras de una red local.

HARDWARE: Es la parte física del computador, se refiere a todas las parte tangibles (que puedes tocar) de un sistema informático en general.

M

MICROSOFT: es una empresa multinacional de origen estadounidense. Microsoft, desarrolla, fabrica, licencia y produce software y equipos electrónicos.

MIDDLEWARE: es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, software, redes, hardware y/o sistemas operativos.

P

PATCH PANEL: Un panel de conexiones, también denominado bahía de rutas o patch panel, es el elemento encargado de recibir todos los cables del cableado estructurado.

R

RED HAT: Es la compañía responsable de la creación y mantenimiento de una distribución del sistema operativoGNU/Linux que lleva el mismo nombre: Red Hat Enterprise Linux.

REDES: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

ROUTERS: Un dispositivo dedicado a la tarea de administrar el tráfico de información que circula por una red de computadoras.

S

SISTEMA OPERATIVO: Es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación.

SOFTWARE: Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

T

TARJETA DE RED: es un periférico que permite la comunicación con aparatos conectados entre sí, también permite compartir recursos entre dos o más computadores.

BIBLIOGRAFIAS

Bibliografía Citada:

RAMOS, Alegre, M d C y GARCIA-Cervigón Hurtado, A. *Sistemas Operativos en Res.* Madrid : Parainifo, 2010.

ESPAÑA, Maria. *Sistemas Avanzados de Telecomunicaciones.* Mexico D.F. : Diaz de Santos, 2010.

ESPAÑA, Boquera. *Sistemas Avanzados de Telecomunicaciones* . Mexico : Diaz de Santos, 2010.

KUROSE, F y KEITH, R.W. *Redes de Computadoras.* Madrid : Pearson, 2010.

Lazarano, J. *Fundamentos de Telemàtica.* Valencia : Universidad Politecnica de Valencia , 2012.

M, Eduardo. 2011. *Sistemas Operativos de Red.* Madrid : Aditex, 2011.

Moro Vallina, M. *infraestructura de Redes de Datos.* Madrid : Paraninfo, 2013.

Ortiz Pavon , H.J. *Sistemas Operativos modernos* . Madrid : Sello Editorial, 2011.

Romero , M.D. *Redes Locales* . Madrid : s.n., 2009.

Systems, Cisco. Pagina Principal de Cisco. [En línea] 04 de 2002. [Citado el: 23 de 07 de 2015.] http://www.cisco.com.

Tanembaum, Andrew S. *Redes de Computadores.* Mexico D.F. : Prentice Hall, 2009.
Valencia Arribas, F. *Manual Basico de Configuraciòn de redes Cisco.* España : s.n., 2011.

CAPELLA. GARCIA, *Seguridad informática*. España : s.n., 2011.

AGUILERA. A, *Seguridad informatica.* Madrid : Sello Editorial, 2010.

FRAHIM, Y SANTOS. *conceptos de firewall.* Madrid : Paraninfo, 2014.

GRIERA, I. Y Otros, *Antivirus.* Madrid : Pearson, 2009.

DITECH, *Vpn (Vrtual private network).* España : s.n., 2013.

POMORES, G. y CONDELAS. *Red privada virtual.* Madrid : Paraninfo, 2010.

GOMES, J. *optimizacion de sistemas de deteccion de intrusos.* Madrid : Pearson, 2008.

Bibliografía Virtual:

ACOSTA, S. *Metodología de la investigación* [en línea]. Quito, Ecuador.: Universidad Central del Ecuador. 2011. <http: //es.scribd.com/doc/71345489/Unidad-1-Metodologia-de-La-Investigacion. [Consultada: 09-05-2015].

BOHÓRQUEZ, L. BERNAL, A. *Componente Para La Visualización De Resultados De Búsqueda Multidominio*[web en línea]. Bucaramanga, Colombia.: Universidad

GIMSON, L. VPN [documento en línea]. Buenos Aires, argentina.: Universidad Nacional de la Plata.2012. <http://sedici.unlp.edu.ar/bitstream/handle/10915/24942/Documento_completo__.pdf?sequence

INDUSTRIAL de Santander. 2012.<http://repositorio.uis.edu.co/jspui/handle/123456789/2817. [Consultada: 27-03-2015]

LUCÍAN, T. *Diseño de seguridades en redes* [documento en línea]. Navarra, España.: Universidad Pública de Navarra. 2013. <http: //academica-e.unavarra.es/bitstream/handle/2454/7544/578081.pdf?sequence=1.[Consultada: 28-04-2015].

MOSQUERA, N. *Sistema operativos* [documento en línea]. Pereira, Colombia.: Universidad Tecnológica de Pereira. 2009. < http://repositorio.utp.edu.co/dspace/handle/11059/1325. [Consultada 06-04-2015].

NEXOLINUX. [En línea] 24 de agosto de 2006. [Citado el: Miercoles de Diciembre de 2014.] http://www.nexolinux.com/comandos-mas-usados-para-gestionar-iptables/.

SEAVTEC. [En línea] 10 de Enero de 2014. [Citado el: 6 de marzo de 2015.] http://www.seavtec.com/es/content/soporte/documentacion/iptables-howto-ejemplos-de-iptables-para-sysadmins.