UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniera e Ingeniero de Sistemas

TEMA:
ANÁLISIS DE LOS MECANISMOS DE SEGURIDAD EN UN ISP DE NIVEL TRES Y PROPUESTA DE IMPLEMENTACIÓN DE IPSEC EN UN ENTORNO IPV6

AUTORES:
BELÉN MARCELA GALLEGOS ALTAMIRANO
ISMAEL ALEXANDER ROMÁN GONZÁLEZ

TUTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, julio del 2018

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Belén Marcela Gallegos Altamirano con documento de identificación N°.1723532311 e Ismael Alexander Román González, con documento de identificación N°.1721034799, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores de titulación con el tema **"ANÁLISIS DE LOS MECANISMOS DE SEGURIDAD EN UN ISP DE NIVEL TRES Y PROPUESTA DE IMPLEMENTACIÓN DE IPSEC EN UN ENTORNO IPV6"**, mismo que ha sido desarrollado para optar por el título de INGENIEROS DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada.

En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

BELÉN MARCELA
GALLEGOS ALTAMIRANO

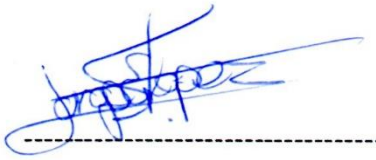
ISMAEL ALEXANDER
ROMÁN GONZÁLEZ

Quito, julio del 2018

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: "ANÁLISIS DE LOS MECANISMOS DE SEGURIDAD EN UN ISP DE NIVEL TRES Y PROPUESTA DE IMPLEMENTACIÓN DE IPSEC EN UN ENTORNO IPV6", realizado por Belén Marcela Gallegos Altamirano e Ismael Alexander Román González, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, julio del 2018



JORGE ENRIQUE LÓPEZ LOGACHO
CI: 1712082484

DEDICATORIA

Los esfuerzos nunca llegan solos, la motivación, la preocupación de cada una de las personas que me acompañaron en este caminar fue fundamental y por lo cual quiero dedicar este trabajo a mis padres Sandra y Marcelo, quienes, con imperecedero amor, paciencia, esfuerzo supieron guiar mi camino.

A mis hermanas Evelyn y Celine que con todo su amor me llenan de fuerza para afrontar el día a día. A mi abuelita por enseñarme que todo esfuerzo con dedicación y disciplina tiene su recompensa.

A mi tía, mis adoradas sobrinas, primos, mi hermosa familia, por estar pendientes de mí durante toda mi carrera, y quienes en los momentos difíciles dibujaron una sonrisa en mí para seguir y lograr este objetivo.

A mis amigos incondicionales, por brindarme su apoyo en cada momento y permitir que nuestra amistad trascienda más allá de las aulas.

Finalmente, a mis pequeños Gabriel y Valentina por ser el motivo de superación, felicidad y alegría diaria desde que llegaron a mi vida.

A esa persona, que nunca dejo de creer en mí…

MARCELA

DEDICATORIA

Dedico este proyecto, a mi madre, esa persona que siempre creyó en mi de manera incondicional, para la que siempre fui el hijo perfecto a pesar de que no sea así, la que tuvo que esforzarse de manera muy especial para poder darme este regalo tan grande que es la educación, para ti madre querida, aunque sé que en ocasiones no demuestro todo lo que siento, este logro va dedicado especialmente para ti.

A mi abuelita querida, la que siempre me enseño que la derrota no es una opción y que hay que salir adelante a como dé lugar, la que tiene la capacidad de soportar todos mis errores y conductas equivocadas, gracias a su constante apoyo, paciencia y formación, siempre he sabido superar cualquier obstáculo y he podido cumplir todos los objetivos que me he trazado. Sin ti no sería nada viejita querida.

A mi tío, mejor dicho, a mi ñaño y a mi padre, el que siempre estuvo conmigo, el que para mí representa una figura paterna y para el que soy su prioridad ante cualquier circunstancia de su vida, el que siempre tiene un consejo adecuado en el momento indicado, al que admiro, respeto y quiero con todo mi corazón por todo su sacrificio, esfuerzo y perseverancia. Para ti también va dedicado este logro ñaño.

A ti Fer, gracias por todo el apoyo recibido y sobre todo la confianza incondicional puesta en mí. También significas una parte importante de mi vida, este logro es una muestra de mi agradecimiento infinito hacia ti.

ISMAEL

AGRADECIMIENTO

Agradecemos, en primer lugar, a Dios, el creador de la vida, por permitirnos gozar de todos los momentos hermosos de la vida.

A la Universidad Politécnica Salesiana por abrirnos las puertas de una educación basada en amor y valores, por formarnos como seres humanos con excelencia académica y profesional.

A todos los docentes y amigos, en especial a Viviana, Daniel y Walter, quienes fueron parte de esta hermosa experiencia, guiando nuestros caminos, para alcanzar tan anhelado objetivo.

Al ingeniero Jorge López, en su calidad de tutor de este proyecto de titulación y aún más, un verdadero amigo, que nos brindó su amistad incondicional durante nuestra vida universitaria. Gracias por la confianza puesta en nosotros, por todo su tiempo y apoyo incondicional.

MARCELA E ISMAEL

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En el presente documento, en primer lugar, se desarrolla un estudio integral de los procedimientos de seguridad con los que cuenta un ISP de nivel tres, para esto, se estudia algunos principios relacionados con Internet como historia, características básicas y datos estadísticos, luego se describe cual es el funcionamiento general de un ISP, así como su estructura y algunos protocolos que se desarrollan en este entorno, además se explica detalladamente la clasificación de los ISP's.

Se desarrolla un análisis completo de los paradigmas de seguridad que se manejan dentro de los ISP. En este estudio se incluyen los requerimientos de seguridad que presentan estas organizaciones, tanto desde la perspectiva del proveedor de servicios de Internet como de la perspectiva del cliente. También se describe un prototipo de seguridad generado mediante la norma ISO/IEC 27001, el mismo que puede ser adoptado por organizaciones que se dedican a la comercialización de acceso a Internet.

Como parte fundamental de este documento, se presenta una propuesta de implementación del protocolo de seguridad IPSec dentro de un entorno IPv6. Dicha propuesta se la maneja bajo el modo de una simulación de red realizada sobre el programa Riverbed Modeler en su versión académica. Los datos estadísticos arrojados por este prototipo de red son analizados y posteriormente presentados como muestra de la viabilidad de la propuesta mencionada.

Abstract

In this paper, in the first instance, a complete analysis of the security mechanisms of a level three Internet service provider is carried out. For this, we first study some principles related to the Internet such as history, basic characteristics and statistical data, then describe what is the full operation of an ISP, as well as its structure and some protocols that are developed in this environment, also detailing the different types of ISPs that currently exist.

The study of security criteria that are handled in Internet service providers is developed. This study includes the security requirements presented by this type of organization, both from the ISP point of view and from the point of view of the end user. It also describes a security model based on the computer security standard ISO / IEC 27001, which can be adopted by organizations that are dedicated to the commercialization of Internet access.

As a fundamental part of this document, a proposal for the implementation of the IPSec security protocol is presented within an IPv6 environment. This proposal is managed under the mode of a network simulation performed on the Riverbed Modeler program in its academic version. The statistical data produced by this network prototype are analyzed and later presented as a sample of the viability of the proposal.

INTRODUCCIÓN

La seguridad dentro de las últimas décadas ha cobrado gran importancia dentro de las grandes redes informáticas. Hoy en día existe gran variedad de medidas de prevención contra incidentes informáticos, pero así mismo cada día aparecen nuevas amenazas cibernéticas que buscan romper las características esenciales de la información. Es por dicho motivo que la seguridad dentro de las redes informáticas debe ser la característica principal que se maneje en este tipo de entornos y a partir de ella se construya un adecuado modelo de funcionamiento.

El establecimiento de mecanismos y medidas de seguridad dentro de los ISP's aporta al fortalecimiento de del entorno en el que se desarrollan este tipo de organizaciones. Dichas reglas deben ser establecidas en base a las necesidades y actuales requerimientos de la organización, además deben apoyarse en normas internacionales que busquen resguardar el principio de seguridad, como el conjunto de normas ISO/IEC 27000. Así, todo intento por vulnerar las medidas de seguridad impuestas por el ISP mediante acciones físicas, o porciones de código mal intencionado podrá ser identificado, gestionado y tratado para reducir los niveles de riesgos hasta que estos sean aceptables para la organización.

La implementación de un mecanismo de seguridad lo suficientemente robusto en la red de un ISP de nivel tres, resulta siendo una alternativa que evidentemente incrementa los niveles de seguridad dentro de la organización, garantizando la disponibilidad de los recursos que se ofrece y además resguardando la información que es el principal activo de un ISP. IPSec provee protección al camino por el cual se trasporta la información que ha sido generada por el usuario y que se debe transportar hacia Internet. Además, la red donde se implementa IPSec debe estar diseñada bajo

direccionamiento IPv6, esto complementara las características de seguridad que ofrece el protocolo de seguridad mencionado.

PROBLEMA DE ESTUDIO

La principal característica de los proveedores de servicio de Internet como su nombre lo indica es abastecer de este servicio a usuarios finales, pero para lograr esto, el escenario sobre el que se debe implementar todo esto debe contar con características que ofrezcan calidad de servicio, confiabilidad, disponibilidad de servicio y sobre todo seguridad.

Aquí es justamente donde se pueden evidenciar algunas debilidades las cuales se pueden mejorar utilizando técnicas que hagan más robusto a esta prestación de servicios. Las debilidades se pueden ver expresadas en la poca seguridad informática con la que cuentan algunos ISP, con esto se hace referencia a que la infraestructura de red no está protegida contra ataques que se pueden generar. Esto se produce por diferentes motivos, uno de ellos y el que más sobresaliente es la carencia de protocolos de seguridad, que obligatoriamente se deben configurar sobre la infraestructura de red perteneciente a organizaciones de este tipo. La seguridad a más de proteger al usuario se debe enfocar en implementar mecanismos como IPSec o MPLS. Estos mecanismos pueden aportar en la generación de un canal seguro mediante el cual los datos puedan circular sin que se afecten sus características y principios generales.

El termino seguridad dentro del ambiente de las telecomunicaciones y de redes, puede abarcar muchos conceptos, debido a esto la implementación de este conjunto de reglas, denominas protocolos de seguridad de debe manejar a nivel de capa tres que es justamente donde los ISP carecen de una seguridad robusta. La seguridad de nivel tres de un ISP, también se puede ver potenciada con la utilización de IPv6. La mayoría de ISP’s no cuentan con esta versión del protocolo de Internet. Por estos motivos se

considera que los ISP necesitan fortalecer o mejorar la seguridad en cuanto al trasporte de tráfico se refiere.

JUSTIFICACIÓN

En el presente proyecto, se describen las principales características, comportamiento y retos de un ISP de nivel tres, este es el encargado de ofrecer conexión a Internet a usuarios finales, manejando una gran cantidad de datos y procesamiento. Al administrar un gran volumen de datos, es importante que, además de la observación acerca de su comportamiento se deba poner énfasis en la seguridad; la cual se la referencia desde dos puntos de estudio: por un lado, la seguridad que se debe manejar y administrar dentro de la estructura propia de un Proveedor de Servicios de Internet, y por otro, la seguridad que se debe brindar a usuarios finales.

Para realizar un estudio completo de los procedimientos de seguridad con los que cuenta un ISP se debe manejar aspectos como su infraestructura, servicios que ofrecen y por su puesto cuales son las funciones por desempeñar. En este estudio se ha tomado como referencia a la ISO/IEC 27000, la cual es una norma internacional que asegura que las características esenciales de la información no sean vulneradas. Esta norma describe ciertos mecanismos y procedimientos relacionados con la seguridad que se puede manejar dentro de organizaciones que deseen manejar un ambiente de seguridad integro, en este caso en un ISP. Los procesos a seguir para conseguir un entorno de seguridad integro son planificación y operación, que se han considerado los de mayor relevancia ya que esta información resulta útil, al realizar el análisis de los mecanismos de seguridad.

IPSec es un mecanismo que ayuda a resguardar los datos que se trasmiten por un canal de comunicación, combina algoritmos de autenticación y cifrado de los paquetes IP. En base a la utilización de este protocolo, se puede llevar a cabo un estudio relacionado

con en el rendimiento y comportamiento de la red, los parámetros que se pueden utilizar para obtener los resultados deseados son el throughput y la latencia. Es importante mencionar que el escenario propuesto y el análisis, está basado en el Protocolo IPv6, ya que IPSec fue creado propiamente para trabajar con este protocolo.

OBJETIVOS

Objetivo General

Analizar los mecanismos de seguridad en un ISP de nivel tres y propuesta de modelo de IPSec en un entorno IPv6.

Objetivos Específicos:

Identificar la arquitectura de un ISP de nivel 3, con la finalidad de conocer más a fondo las principales funciones y retos propios de su naturaleza.

Analizar los mecanismos de seguridad de un ISP de nivel 3, con el fin de establecer los criterios de seguridad que se deben manejar, para satisfacer estándares que se manejan hoy en día.

Proponer un protocolo de seguridad, usando IPSec, dentro de un escenario IPv6, con la finalidad de brindar seguridad extremo a extremo dentro de la red, eliminado así posibles amenazas que afecten al comportamiento de la red.

Modelar la simulación propuesta de seguridad (IPSec), mediante una herramienta de simulación.

CAPÍTULO 1

1. PROVEEDOR DE SERVICIOS DE INTERNET

1.1 Antecedentes de la investigación

1.1.1 Internet

Internet se define como la red de redes, es decir la unión de varias redes de computadoras pequeñas que conforman entre si una gran red y debido a esto, no posee un único propietario y puede ser accesible para todo el mundo.

Internet, fue desarrollada por los Estados Unidos de Norteamérica como una iniciativa de uso militar bajo el nombre de ARPANET en el año de 1969, con el propósito de que la información que se manejaba durante el periodo de la guerra fría sea accesible desde cualquier parte del país en caso de un ataque centralizado. En principio eran pocas computadoras conectadas entre sí distribuidas a lo largo de todo el país y a las cuales solo tenían acceso personal militar debidamente autorizado.

Después de un corto tiempo, ARPANET empezó a tomar un nuevo rumbo, no solo estaba dirigida para propósitos militares, sino que se expandió hacia otras áreas de conocimiento y con esto el número de hosts conectados entre sí también creció, ya no eran unos pocos ordenadores, sino que eran cientos o miles. Pero con este crecimiento también se presentaron inconvenientes, uno de ellos y el más importante era la estandarización de la transmisión de los datos. De esta manera y en base a dicha necesidad es como nace el protocolo de control de transmisión basado en redes IP (TCP/IP). En realidad, TCP/IP, no es un solo protocolo, sino es una pila o conjunto de protocolos que se encargan de controlar y estandarizar todas las comunicaciones y transmisiones que se dan en redes basadas en paquetes IP como Internet. Dentro de los protocolos más conocidos e importantes dentro de todo este conjunto se pueden encontrar, HTTP, SMTP, ARP, FTP, etc.

Después de algunos años la Fundación Nacional de Ciencia (NSF) de los Estados Unidos de Norteamérica decide crear la NSFNET con el propósito de dar un espacio a temas académicos y de investigación, es así como después de algún tiempo ARPANET se une a la NSFNET debido a que comparten los mismos objetivos y junto con otras redes de libre acceso creadas, forman los cimientos de Internet bajo el nombre de NSFNET.

"En Ecuador la primera institución en proveer acceso al Internet fue Ecuanex, un nodo de Internet establecido en 1991 por la Corporación Interinstitucional de Comunicación Electrónica, Intercom. En el año 1992 se estableció el segundo nodo de Internet (Ecuanet) por medio de la Corporación Ecuatoriana de información, una entidad sin fines de lucro auspiciada por el Banco del Pacífico, la ESPOL, la Universidad Católica de Guayaquil, entre otras. Sin embargo, fue en el año del 1995 que diario el Hoy publicará el primer boletín informativo en formato digital tratando sobre el conflicto fronterizo con Perú." (Fierro, 1995).

1.1.2 Características Básicas de Internet

En esta era digital, es conocido para todos que el medio de comunicación principal y más importante a lo largo de todo el mundo es el Internet. Esta manera de interconectar a todo el mundo ha alcanzado su popularidad, debido básicamente a las características que posee.

Simplicidad: Hace referencia a la facilidad de uso que proporciona esta forma de comunicación, debido a que cuando una persona desea hacer uso de este servicio, no debe tener conocimientos profundos acerca del funcionamiento. La característica principal de este principio es ocultar el usuario final aspectos técnicos y funcionales.

Universal: Este servicio se puede considerar universal, debido a que está extendido a lo largo del planeta tierra y desde cualquier punto se puede acceder a él y disfrutar de todos los beneficios que proporciona en esta era digital. También se puede considerar universal ya que todo el entorno en el que se desarrolla esta estandarizado.

Anónimo: Internet puede brindar al usuario la sensación de anonimato, debido a que puede navegar por distintos sitios web sin que nadie sepa lo que está haciendo, o publicar cualquier tipo de información en lugares especializados resguardando su identidad. No obstante, dentro de Internet todos los pasos que se den dejan una huella que puede ser rastreada por algún software especializado.

Accesibilidad: Este principio se basa generalmente, en como el servicio de Internet dentro de los últimos años ha llegado a ser muy factible económicamente hablando para el común de la población. Los ISP que son quienes llevan a cabo y hacen posible que el Internet sea accesible al usuario final bajo ciertas condiciones. Estas organizaciones por lo general brindan planes muy económicos que pueden ser adquiridos por la mayor parte de la población.

Libre: Esta es la característica más notoria de Internet. No existe organización alguna que sea propietaria de todo este sistema de comunicación. Si bien es cierto que algunos protocolos que trabajan sobre Internet son propietarios de algunas organizaciones, la realidad de la mayoría de los estándares y contenidos es que son totalmente libres.

1.1.3 Datos estadísticos acerca de Internet

Los usuarios de Internet han empezado a crecer año tras año y esto se debe a distintos factores, uno de ellos es la accesibilidad que este servicio ofrece a través de grandes o medianas empresas que se dedican a la distribución de este.

Existen en la actualidad algunos datos bastante interesantes acerca del crecimiento que está teniendo este medio de comunicación. Según We Are Social y Hootsuite, importantes empresas estadísticas y de marketing de los Estados Unidos de Norteamérica, y a través de su estudio titulado "Digital in 2018" que fue realizado en enero del presente año, se revela que más de 4 billones de personas están conectadas a Internet en el 2018, considerando que la población mundial es de 7.593 billones de personas, se puede decir que más del 50% de la población mundial hoy en día tiene acceso a Internet. La tasa de crecimiento anual para personas que se conectan a Internet ha sido del 7% año tras año. El número de usuarios que utilizan redes sociales también ha crecido en los últimos años. En el 2018 se tiene 3.196 mil millones de usuarios, con una tasa de crecimiento anual del 13%. En la figura No. 1, se puede observar detalladamente, cual es el porcentaje de penetración de Internet alrededor de todo el mundo, tomando en cuanto todos los continentes y sus principales subdivisiones. (We Are Social, Hootsuite, 2018).

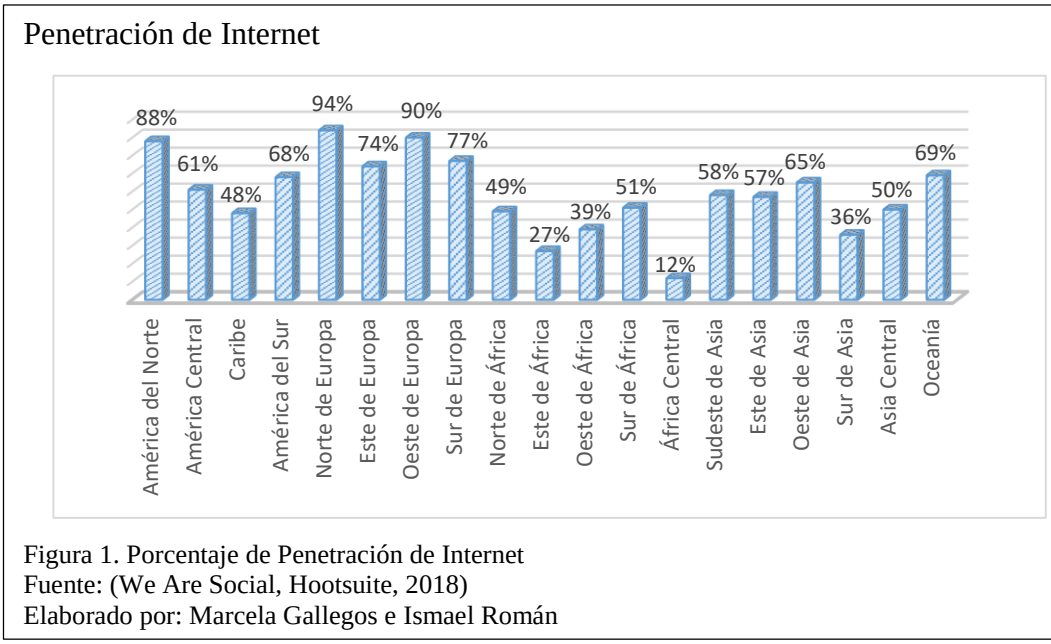


Figura 1. Porcentaje de Penetración de Internet
Fuente: (We Are Social, Hootsuite, 2018)
Elaborado por: Marcela Gallegos e Ismael Román

Otra estadística bastante interesante que presenta el estudio antes mencionado es desde que dispositivos se está accediendo al tráfico web (Internet). Las Laptops y

computadoras de escritorio poseen un 43% de este valor, aunque año tras año presenta una disminución del 3%, mientras tanto que los teléfonos móviles poseen un 52%, con un crecimiento anual del 4%. Los dispositivos móviles como los teléfonos son los que están predominando en el ranking de acceso a Internet.

Dentro del ámbito nacional, también se tiene algunas estadísticas interesantes relacionadas a esta nueva generación tecnológica que está viviendo el país. Según la Encuesta Nacional de Empleo, Desempleo y Subempleo realizada por el INEC, "el 36,0% de los hogares a nivel nacional tienen acceso a Internet, 13,5 puntos más que hace cinco años. En el área urbana el crecimiento es de 13,2 puntos, mientras que en la rural de 11,6 puntos." (INEC, 2016). Por otra parte, según el boletin estadístico del II trimestre del año 2017 publicado por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), el servicio de acceso a Internet fijo, ascendio del 3.35% en el año 2010, al 10.61% en el año 2017. En la figura No. 2 muestra el crecimiento porcentual de suscripciones a Internet fijo por cada 100 habitantes en el pais dentro de los ultimos 8 años. (Agencia de Regulación y Control de las Telecomunicaciones, 2017).

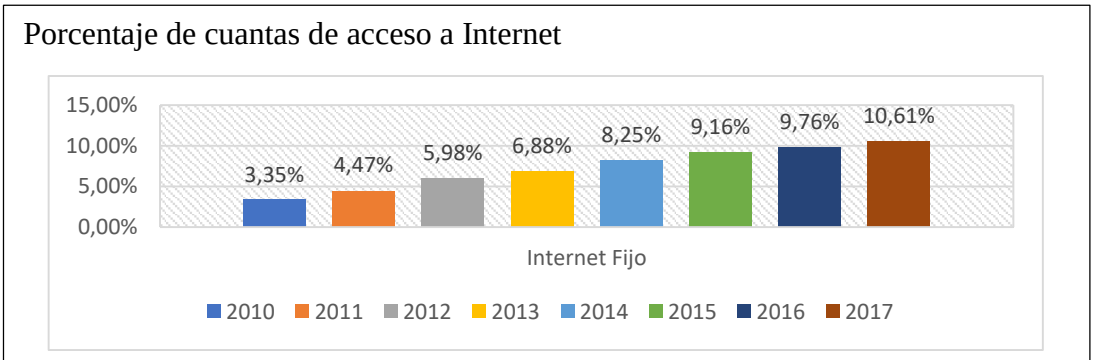


Figura 2. Cuentas de acceso a Internet fijo por cada 100 habitantes
Fuente: (Agencia de Regulación y Control de las Telecomunicaciones, 2017)
Elaborado por: Marcela Gallegos e Ismael Román.

Como dato adicional la ARCOTEL asegura que "la Estadística de participación de mercado para el servicio de acceso a Internet fijo, permite observar que la CNT EP,

operador público ecuatoriano, mantiene el 55,15% del mercado seguido por el prestador SETEL S.A. opera bajo la marca comercial de GRUPO TV CABLE; le siguen el prestador MEGADATOS y CONECEL S.A. (ex ECUADORTELECOM S.A.) con el 10,09% y 8,27% respectivamente de participación cada uno, información para el segundo trimestre del año 2017." (Agencia de Regulación y Control de las Telecomunicaciones, 2017).

1.2 Descripción de un ISP

Un proveedor de servicio de Internet (ISP), básicamente es una organización de tipo privada o gubernamental que tiene como fin principal brindar y comercializar el acceso al servicio de Internet, ya sea a clientes HOME o Corporativos.

El acceso a Internet que brinda un ISP se puede efectuar mediante diferentes medios de conexión con respecto al usuario final, uno de los medios de conexión más comunes y utilizados dentro del ámbito nacional es la utilización de tecnologías xDSL, las cuales una línea de teléfono convencional como medio físico de conexión. FTTH (Fiber To The Home) es otro método de acceso a Internet que ha tomado fuerza y se ha popularizado en los últimos años dentro del país, este se trata de la conexión a Internet mediante fibra óptica, este tipo de tecnología brinda características bastante especiales en cuanto a máximo rendimiento, disponibilidad y velocidad básicamente. Existen muchos más métodos de conexión que brindan los ISP, pero los más populares y comercializados dentro de la nación han sido los expuestos anteriormente.

La seguridad dentro de un ISP debe ser la característica más importante que se debe manejar. Los ISP deben poseer mecanismos de seguridad físicos y lógicos que garanticen que la información transmitida por el usuario no se vea comprometida de alguna manera.

El mantenimiento y soporte técnico cumplen también un rol importante dentro del funcionamiento de la conexión hacia Internet. Los ISP no solo deben preocuparse por brindar el servicio, sino también por monitorear constantemente el funcionamiento de este. Si se produce un incidente dentro de todo este escenario, la organización debe tener la capacidad de solucionar el problema dentro de los niveles de servicio establecidos en el contrato el ISP y el usuario deben firmar.

El monitoreo remoto también representa una función que debe cumplir un ISP, pero este tipo de servicio se podrían considerar adicional, ya que de esto no depende la funcionalidad y disponibilidad de la conexión a Internet que brinda la organización.

1.3 Funcionamiento básico de un ISP

Internet está formado por distintas redes independientes que colaboran entre sí con un fin en común. La unión de distintas redes crea una red con un alcance mundial a la que se puede acceder desde cualquier punto del planeta, siempre y cuando exista un ISP que proporcione dicho servicio.

La función básica que cumple un ISP es llevar la información que genera el usuario hacia Internet y traer información de Internet hacia el usuario. El destino y origen de toda esta información pueden ser páginas web, aplicaciones web o cualquier otro tipo de plataforma que maneje el protocolo TCP/IP. De esta manera se puede decir que un ISP cumple la función de una pasarela entre el usuario y la red mundial. Para cumplir con este servicio de manera confiable, segura y rápida, el ISP posee una infraestructura de red bastante robusta. Dentro de la infraestructura de red, están servidores, enlaces dedicados, ancho de banda y características de seguridad que sean capaces de cumplir con el principio de accesibilidad hacia internet.

Un ISP puede estar enlazado directamente a un punto de acceso a la red (NAP), que básicamente es un punto donde concurren diferentes ISP para tener acceso directamente al backbone de Internet. Como es un punto donde interactúan diferentes entidades, es necesario establecer políticas o estándares que se deben cumplir por parte de los ISP que se conecten al punto, esto con el fin de no influir con el funcionamiento y desempeño del resto de ISP's.

EL ISP también se puede conectar a ISP de mayor jerarquía, que son organizaciones mucho más grandes y con mejores capacidades de red. Esto quiere decir que el ISP de menor jerarquía va a entregar toda la información al ISP de jerarquía de nivel superior y este va a ser quien se encargue de realizar la conexión hacia Internet. Ante esta situación se debe considerar el método de conexión entre los distintos ISP. El método de conexión más común y utilizada en estos días es utilizar líneas dedicadas con un ancho de banda lo suficientemente grande, para poder efectuar la transmisión de grandes cantidades de datos, sin que la información pueda experimentar fallas, como pérdida de información o retardos.

El punto clave para que la conexión pueda efectuarse entre distintos ISP, es que se maneje un direccionamiento IP común, ya sea IPv4 o IPv6 y también manejar un encaminamiento de paquetes en la frontera de conexión. Esto se lo realiza mediante el protocolo de enrutamiento BGP (Border Gateway Protocol). Este protocolo de enrutamiento sirve para llevar los paquetes de un entorno ISP controlado bajo ciertas políticas, hacia otro completamente distinto en cuanto a políticas. La conexión tiene lugar básicamente entre dos enrutadores o routers que establecen comunicación TCP bajo el puerto 179. "Los dos routers que forman una conexión TCP para intercambiar información de ruteo BGP son peers o vecinos" Los peers BGP intercambian inicialmente las tablas de ruteo BGP completas. Después de este intercambio, los peers

envían actualizaciones graduales como los cambios de tabla de ruteo.” (CISCO, 2008). De esta manera es que los distintos ISP que participan en la conexión pueden conocer la ruta de destino a la que deben reenviar la información que ha sido generada por el usuario, para que esta pueda llegar a Internet.

Funcionamiento de un ISP

Figura 3. Diagrama de procesos - Funcionamiento general de un ISP
Elaborado por: Marcela Gallegos e Ismael Román.

1.4 Estructura de un ISP de nivel tres

Los dispositivos de red que predominan en un ISP son los routers. Estos dispositivos cumplen con la función de conmutar paquetes a través de distintas rutas o caminos para que puedan alcanzar su destino. Este reenvió de paquetes se lo realiza mediante enrutamiento ya sea estático o dinámico y para esto utiliza direccionamiento IP que indica cual es la ruta que debe tomar cada paquete. Cuando se trata de redes simples basta con conectar varios routers mediante enlaces de comunicación y aplicar un protocolo de enrutamiento para que estos realicen su función. Cuando los requerimientos de funcionamiento son mayores y se espera una gran concurrencia de información, como es el caso de los ISP, se necesita aplicar otros criterios al diseño de la arquitectura o infraestructura que soportará esta gran cantidad de datos.

Estructura de un Proveedor de Servicios de Internet de Nivel Tres

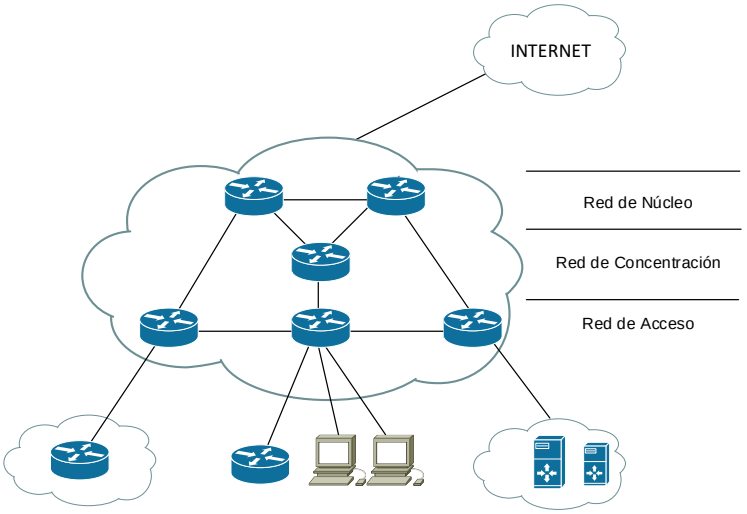


Figura 4. Estructura lógica de un ISP de nivel tres.
Elaborado por: Marcela Gallegos e Ismael Román

La separación o división lógica de los enrutadores, podrá aportar estructura, jerarquización y modularidad a la topología de red. En este mecanismo lo que se busca principalmente es repartir funciones entre distintos grupos de routers. Generalmente los proveedores de servicios de Internet suelen dividir a los routers en dos grandes grupos, los routers de concentración y los routers de núcleo.

- **Routers de concentración:** Estos enrutadores son los encargados de recibir grandes volúmenes de tráfico desde los sistemas finales. Están provisionados un gran número de puertos de baja velocidad. También se los podría considerar enrutadores de acceso, ya que estos son los primeros que toman contacto con datos provenientes de otro dominio
- **Routers de núcleo:** La función principal de este grupo de enrutadores es conmutar a alta velocidad los paquetes que llegan hacia ellos. La conmutación puede tener lugar entre dos ISP o directamente al backbone de Internet. Utilizan enlaces de conmutación de alta velocidad como fibra óptica.

En la tabla No. 1, se pueden apreciar las principales diferencias que existen entre los routers de backbone y los de concentración.

Tabla 1. Diferencias entre routers de backbone y de concentración - ISP

PARÁMETRO	ROUTER DE BACKBONE	ROUTER DE CONCENTRACIÓN
Throughput	Extremadamente alto	Alto
Funcionalidades de procesamiento de paquetes	Muy pocas, se centran en él envió rápido de información	Funcionalidades de alto valor añadido
Tipos de interfaces	Pocas interfaces de muy alta velocidad	Muchas Interfaces de relativa baja velocidad
Patrones de tráfico	Desde y hacia cualquier interfaz	En su mayoría cliente-troncal y troncal-cliente.

Nota: Principales diferencias entre los enrutadores de un ISP. Fuente: (Caicedo & Yánez, 2002).

Cuando los routers se separan de acuerdo a la clasificación previamente descrita, la infraestructura de red de un ISP se divide en 4 segmentos que responden a una organización semi-jerárquica como se puede apreciar en la figura No. 5.

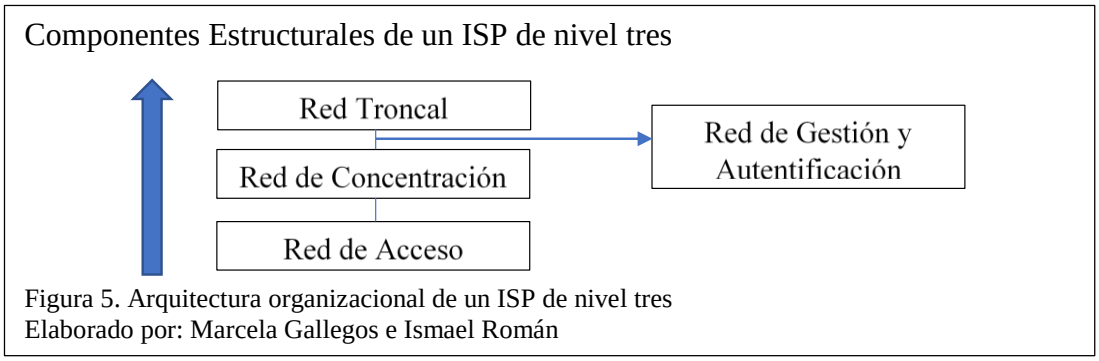


Figura 5. Arquitectura organizacional de un ISP de nivel tres
Elaborado por: Marcela Gallegos e Ismael Román

La estructura general del ISP se divide en varios tipos de redes, esto no quiere decir que sean redes separadas, sino más bien que cumplen roles totalmente diferentes con el fin de segmentar y modularizar funciones. Para manejar la organización jerárquica dentro de la infraestructura física y lógica del ISP, se puede decir que su estructura tiene tres niveles jerárquicos de conexión. **Nivel de acceso, nivel de concentración y nivel de backbone.**

1.4.1 Red de Acceso

El concepto general de la red de acceso es que permite que los usuarios finales puedan conectarse a un proveedor de servicios a través de distintas tecnologías. Cabe mencionar que existen múltiples tecnologías de acceso en la actualidad, pero todas

estas se clasifican en dos grandes grupos, según el tipo de tecnología y según el tipo de usuario.

1.4.1.1 Tecnologías de acceso

1.4.1.1.2 Líneas Conmutadas

Las líneas conmutadas o Dial-up son canales de comunicación que se establecen y una vez terminada la comunicación o trasferencia de datos se cierran. Este tipo de tecnología permite la comunicación desde cualquier parte en la que se tenga acceso a la red telefónica (PSTN). Para este tipo de conexión, necesariamente se debe utilizar un MODEM (Modulador-Demodulador) ya que este transforma las señales digitales producidas por un nodo de red en señales analógicas que puedan ser transportadas por la red de telefonía pública. El uso de líneas conmutadas es muy frecuente en los ISP. Los proveedores de Servicios de Internet utilizan esta tecnología para establecer comunicación con sus clientes o usuarios finales.

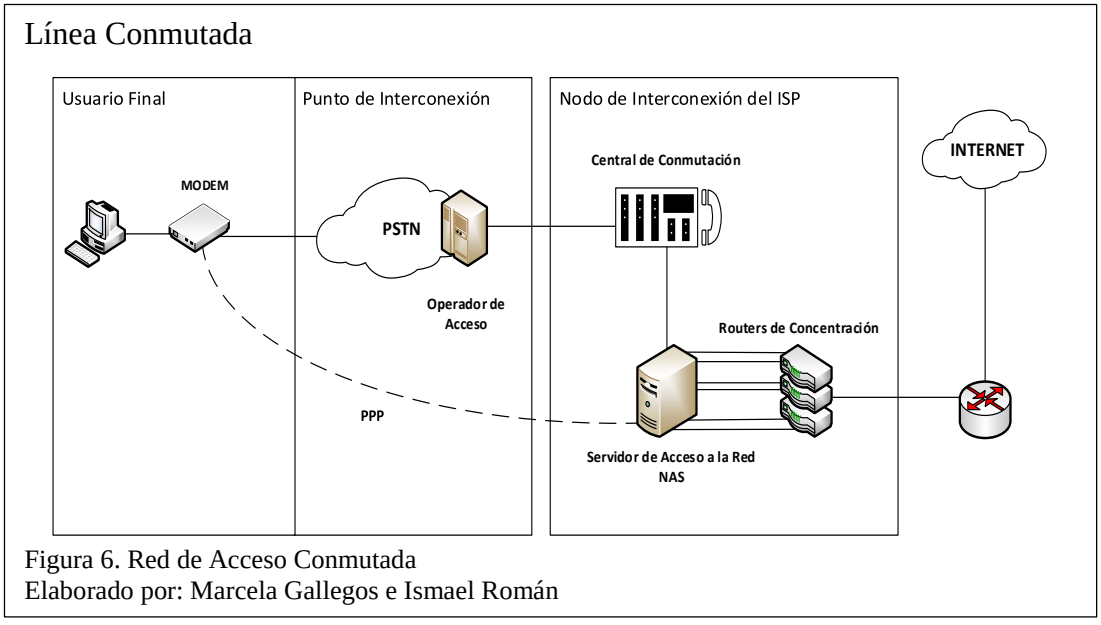


Figura 6. Red de Acceso Conmutada
Elaborado por: Marcela Gallegos e Ismael Román

Cuando el usuario final genera tráfico que debe alcanzar Internet, el MODEM realiza la transformación de estos datos para que puedan viajar a través de la PSTN. El tráfico se envía mediante la red de telefonía pública hasta llegar al nodo de conexión. Este

punto está conformado por el operador de acceso el cual se conecta directamente con la central de conmutación del ISP. La función general de la central de conmutación es extraer los argumentos de destino del tráfico que se está enviando. Esta entidad obtiene el número de destino que servirá para direccionar el tráfico correctamente, además extrae el tráfico de Internet a través de interfaces primarias (ISDN PRI). Seguidamente, entra en funcionamiento el servidor de acceso a la red que mantiene comunicación directa con el modem. El NAS, autentica al usuario y termina la sesión PPP, después de este proceso, el tráfico de Internet es transmitido hacia los routers de concentración mediante enlaces redundantes. De esta manera es como se consigue que el tráfico de Internet procedente de un usuario pueda alcanzar su destino final (Internet), a través de una línea conmutada.

1.4.1.1.1 Líneas Dedicadas

El concepto de una línea dedicada se basa en asegurar recursos para una comunicación, el propósito general de esta tecnología es dedicar recursos para que la transmisión de datos entre dos entidades no presente inconvenientes. Algunas de las líneas dedicadas más conocidas son E1, T1 y SMT-1. En este escenario, el usuario final tiene un router que se conecta al router de concentración del ISP mediante una línea dedicada.

Línea Dedicada

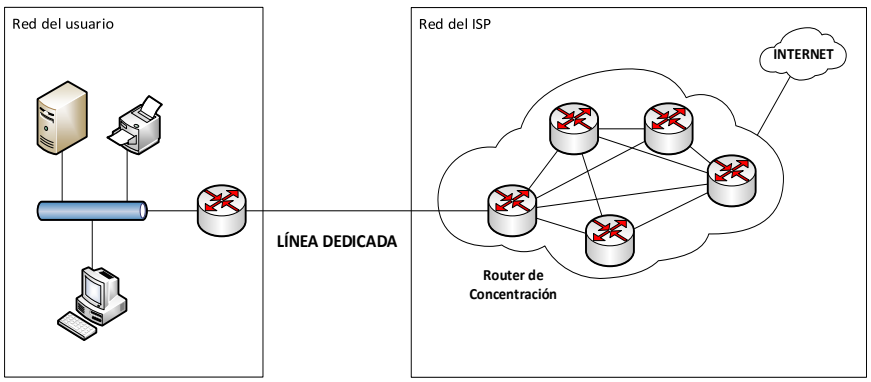


Figura 7. Red de Acceso Dedicada
Elaborado por: Marcela Gallegos e Ismael Román

Las tecnologías más comunes y populares para implementar líneas dedicadas son Metro Ethernet, PDH/SDH y 4G. Estas tecnologías presentan ciertas ventajas con respecto al resto, este es el caso de las redes Metro Ethernet, las cuales están diseñadas bajo infraestructura de fibra óptica, por ende, ofrecen velocidades de transmisión elevadas. La tecnología 4G ofrece ancho de banda simétrico, estable y garantizado, mientras tanto que las tecnologías PDH/SDH ofrecen velocidades de 2 Mbps hasta 155 Mbps.

1.4.1.1.3 Tecnologías Alámbricas

Cuando se utilizan medios guiados se aportan características extra a la transmisión y transporte de tráfico. Una de las principales ventajas es que, al utilizar este tipo de tecnología, se pueden alcanzar velocidades de transmisión mucho más elevadas en comparación con otras tecnologías específicamente con los medios inalámbricos. También se aporta seguridad ya que en el medio físico se pueden emplear mecanismos de control y de seguridad mucho más efectivos. En la actualidad existen múltiples tecnologías de acceso alámbricas, pero algunas sobresalen más que otras. En el ámbito nacional es frecuente el uso de las tecnologías xDSL, HFC y FTTx.

Línea Digital de Suscriptor: La tecnología xDSL (Digital Subscriber Line), se basa en la trasmisión de tráfico de Internet a través de la línea convencional de teléfono, para esto se necesita contar con un MODEM DSL a ambos lados de la red, es decir uno del lado del cliente y otro de lado del ISP. La función del MODEM es, de un lado modular las señales para que puedan ser trasportadas por la PSTN y del otro lado demodular la señal para obtener los daros que serán enviados hacia internet. Es una tecnología de banda ancha basada en cobre. Existen distintas variaciones dentro de la tecnología xDSL, la diferencia fundamental entre estas es la velocidad máxima a la

que pueden trasmitirse datos, tanto de subida como de bajada. En la tabla No.2 se puede apreciar las velocidades que manejan las distintas tecnologías xDSL.

Tabla 2. Velocidades de la tecnología xDSL

Nombre	Significado	Tasas de Tx	Modo
DSL	Digital Subscriber Line	160 kbps	Duplex
HDSL	High data rate DSL	1.544 Mbps 2.048 Mbps	Duplex Duplex
SDSL	Single line DSL	1.544 Mbps 2.048 Mbps	Duplex Duplex
ADSL	Asymmetric DSL	1.5 to 9 Mbps 16 to 640 kbps	Down Up
VDSL	Very high data rate DSL	13 to 52 Mbps 1.5 to 2.3 Mbps	Down Up

Nota: Descripción de las velocidades de la tecnología xDSL
Elaborado por: Marcela Gallegos e Ismael Román

Cable Modem (Hybrid Fiber Coaxial - HFC): Es una tecnología de acceso que como su nombre lo indica es una combinación de fibra óptica con cable coaxial. La unión de estas tecnologías permite superar algunas barreras que por su naturaleza las tecnologías alámbricas tradicionales presentan. La velocidad de transmisión ya no es más un problema, con la implementación de fibra óptica los datos se transmiten a velocidades elevadas, además este tipo de redes son altamente resistentes a la interferencia electromagnética que presentan las tecnologías alámbricas basadas en cobre.

“Estas redes fueron mejoradas y en la actualidad permiten el envío y recepción de información a través del mismo cable sin interferir con la transmisión habitual de contenido de Televisión con los estándares DOCSIS 3.0 y 3.1. Al igual que DSL pueden alcanzar velocidades de varios Mbps, pero se ven afectados por la distancia, es por esto que utilizan tecnología de Fibra Óptica hasta el Headend y los nodos de distribución, y desde este punto utilizan cable coaxial con amplificadores cada cierta distancia, para el acceso a los usuarios.” (Agencia de Control y Regulación de las Telecomunicaciones, 2015).

Redes de Fibra Optica (FTTx): La aparición de las redes PON (Pasive Optical Network) marcó un antes y un después dentro de la utilización de la tecnología de fibra óptica. Estas redes manejan múltiples dispositivos pasivos dentro de su arquitectura y esta es la causa principal por la cual los costos de implementación se reducen considerablemente. Esta es la razón por la cual se puede utilizar este tipo de tecnología en el segmento de acceso que es el que se comunica directamente con el usuario final.

Estructura de una red de fibra óptica

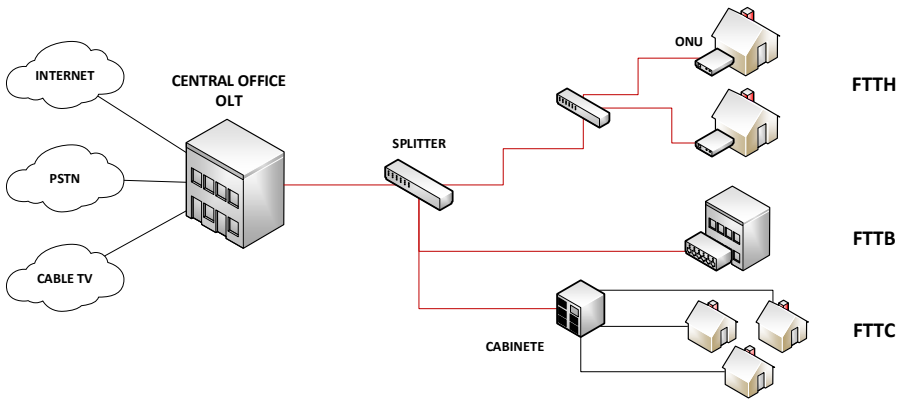


Figura 8. Red de Acceso FTTx
Elaborado por: Marcela Gallegos e Ismael Román

La fibra óptica es muy resistente a la interferencia electromagnética, cubre grandes distancias antes de que la señal se vea degradada y se tenga que realizar splitting (técnica parecida a la multiplexación) y la ventaja más importante que tiene esta tecnología, es la velocidad a la que se pueden transmitir los datos. La tecnología GPON (Gigabit-capable Pasive Optical Network) es la que frecuentemente se utiliza ya que sus velocidades de transmisión son muy elevadas. Las velocidades convencionales y de referencia de esta tecnología son 1.24416 Gbit/s de subida y 2.48832 Gbit/s de bajada, con esto se puede tener una idea general de la tasa de trasmisión que pueden llegar a tener las tecnologías alámbricas basadas en fibra óptica.

FTTC: (Fiber To The Cabinet o Fiber To The Curb). El punto de partida para este tipo de redes generalmente es en la oficina central donde se encuentra el OLT (Optical Line

terminal). En esta tecnología, la fibra óptica llega a gabinetes de conexiones, que se ubican a poca distancia (500m – 1000m) del usuario final. Desde el gabinete se produce la comunicación con el cliente mediante la ONU (Unidad Optica de Red). Esta conexión se la realiza generalmente a través de tecnologías xDSL o mediante la red telefónica.

FTTB (Fiber To The Building): En esta tecnología la fibra óptica llega a módulos de distribución que generalmente se encuentran dentro de los edificios (sótano). Desde este punto, la fibra suba hacia los diferentes pisos del edificio donde se conecta en cajas terminales de acceso y se distribuye a los diferentes usuarios. Las tecnologías más utilizadas para realizar esta última sección de la conexión son xDSL y Ethernet.

FTTH (Fiber To The Home): En esta tecnología, la fibra óptica llega directamente hasta la residencia del usuario final. En el domicilio del cliente se instala la unidad óptica de red (ONU), este se conecta con la línea de fibra que generalmente sale de los postes de alumbrado público. Esta es la tecnología más utilizada en la actualidad por los proveedores de servicio de Internet en el país, ya que es la que presenta más ventajas en cuanto a rendimiento y seguridad.

1.4.2 Red de Concentración

La red de concentración se ubica por encima de la red de acceso (ubicación jerárquica) y su función principal es agregar las conexiones de los clientes en los PoP. En esta capa del ISP se utilizan routers de concentración de dos tipos, los primeros van a ser los encargados de manejar las conexiones de los usuarios de líneas conmutadas y los segundos se encargan de manejar las conexiones de los usuarios de líneas dedicadas.

Los routers de concentración deben tener características adicionales, ya que están diseñados para soportar una gran concurrencia de conexiones y deben estar preparados para ello.

En algunas topologías o arquitecturas de red, el enrutador no solo cumple con la función de encaminar los paquetes hacia su destino, sino que realizan funciones adicionales, este es el caso de los routers de concentración, en ocasiones estos dispositivos también deben funcionar como firewalls, filtrado de paquetes, manejo de listas de acceso entre otras características adicionales, por lo cual este dispositivo debe ser uno de los más robustos de toda la infraestructura de red.

En cuanto al enrutamiento, los routers de concentración no anuncian las rutas completas a los routers de backbone, lo que hacen es sumarizar dichas rutas, de esta manera solo se transmiten grupos de direcciones que abarcan al resto, dando como resultado la reducción del nivel de procesamiento del router debido a que las tablas de enrutamiento disminuyen considerablemente en cuanto a tamaño. Esto es posible ya que en el nivel de acceso se maneja un pool de direcciones las mismas que son transmitidas hacia los routers de concentración y estos realizan la sumarización correspondiente.

1.4.3 Red Troncal

La red troncal de un ISP se ubica en la parte superior jerárquicamente hablando, es la que se encarga de realizar las conexiones directamente con Internet si es que se trata de un ISP de nivel 1, o con otros proveedores de servicios de Internet de menor o de mayor jerarquía. En esta capa también se realiza la interconexión con los puntos de presencia con los que cuanta el proveedor de servicios.

La red troncal, está constituida generalmente de routers de núcleo los cuales cumplen con funciones específicas que permitan que los paquetes se trasmitan de una manera rápida hacia su destino. El throughput, que es un indicativo del correcto funcionamiento de la red, en los routers de backbone debe ser extremadamente alto, además este tipo de enrutadores generalmente cuentan con muy pocas interfaces de conexión pero que son de alta velocidad.

La conectividad hacia Internet es una de las funciones esenciales del segmento de backbone dentro de la red de un ISP. Generalmente los Proveedores de Internet acceden a la gran red de mundial a través de puntos de acceso (NAP). En Ecuador existe un punto de acceso a la red que esta supervisado por AEPROVI (Asociación de empresas proveedoras de Internet, valor agregado, portadores y tecnologías de la información) y se denomina NAP.EC (Network Access Point Ecuador)

NAP.EC es una infraestructura de red que fue diseñada para intercambiar tráfico de Internet que sea generado desde el país o que este destinado hacia el país. Existen dos nodos de interconexión en el país (Quito y Guayaquil). De esta manera cuando un ISP desea acceder al backbone de Internet lo debe hacer a través de este punto de acceso, pero debe cumplir ciertos requisitos para que la interacción con los demás proveedores de servicios de Internet no se vea afectada. “NAP.EC se soporta en un "Acuerdo" para intercambio de tráfico local cuyos términos y condiciones los participantes se comprometen a cumplir.” (AEPROVI, 2018).

Topología de NAP.EC

La figura No. 9 muestra la topología de NAP.EC y cuáles son sus actuales miembros.

Topología del NAP.EC

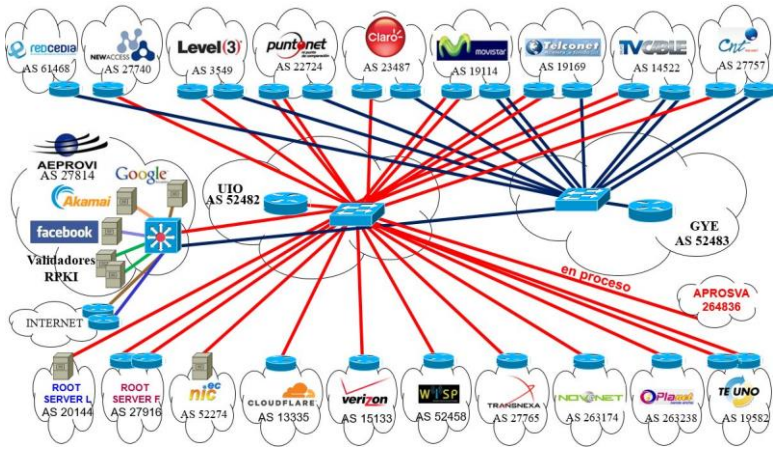


Figura 9. Topología lógica del NAP.EC
Elaborado por: Marcela Gallegos e Ismael Román

1.5 Tipos de ISP

1.5.1 ISP Nacional o Internacional o de Nivel 1

Este tipo de ISP cuentan con su propia red de acceso al backbone de Internet y son el nivel más alto que puede alcanzar un proveedor de Internet, debido a este motivo debe tener una infraestructura bastante robusta para soportar la gran demanda de tráfico y de ancho de banda, cabe mencionar que a este tipo de ISP se conectan los ISP regionales y también los locales.

Su área de cobertura es muy extensa, en el caso de los ISP's nacionales cubren todo un país y en el caso de los internacionales cubren áreas mucho más extensas como continentes enteros. Generalmente los ISP nacionales o internacionales prestan sus servicios a grandes corporaciones mundiales o a proveedores de menor nivel.

Los ISP´s Nacionales o Internaciones se subdividen en tres grupos, ISP's integrados, ISP's de acceso outsourced e ISP's multimodo. **Los ISP's integrados** son básicamente los que en un inicio empezaron siendo ISP regionales y mediante de la implementación de redes veloces lograron posicionarse como entidades de jerarquía superior. Los **ISP's de acceso outsourced** son proveedores que alquilan infraestructura de los ISP's

locales para poder dar acceso a clientes, es decir no cuentan con infraestructura propia. Esto con el fin de reducir costos de implementación y ampliar su cartera de clientes y por su puesto sus ganancias.

Los **ISP´s multimodo** son organizaciones que no se dedican únicamente a proveer servicios de Internet, sino que también brindan otros servicios como telefonía e incursionan en este medio para lograr mayor captación de clientes, cabe mencionar que tienen infraestructura propia y por ello logran una gran cobertura y buen servicio.

1.5.2 ISP Regional o de Nivel 2

Este tipo de ISP tiene una estructura más robusta y completa que el ISP local además cubre un área mucho más grande, una región o una provincia entera. Debido a estas características es que posee más oficinas centrales y locales, la demanda de usuarios es más grande.

Algunos proveedores de Internet de este tipo tienen acceso directamente al backbone de Internet, sin tener la necesidad de conectarse a un ISP de nivel superior ya que cuentan con infraestructura propia para poder realizar esta función. Para asegurar una conectividad total entre los diferentes nodos de un ISP regional, todas sus oficinas locales y centrales están conectadas entre sí.

Las oficinas locales enrutan el tráfico hacia las diferentes oficinas centrales que posea el ISP, o en su defecto dirigen el tráfico hacia Internet.

Estructura de un ISP Regional

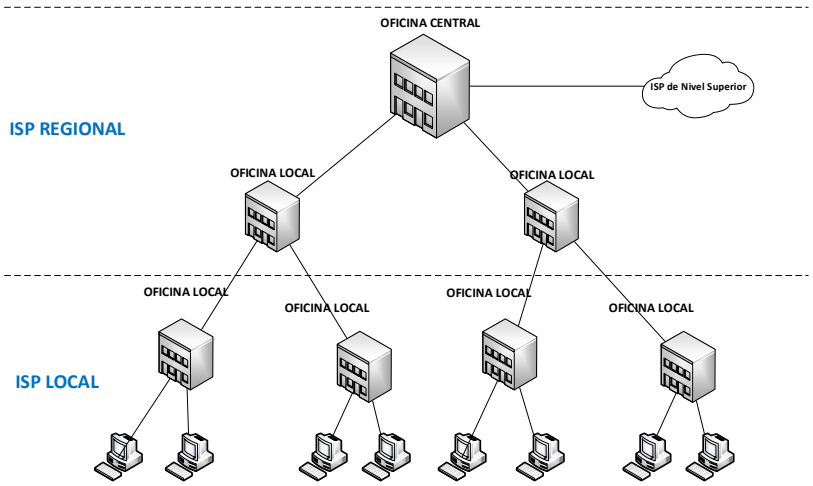


Figura 10. ISP Regional
Elaborado por: Marcela Gallegos e Ismael Román

1.5.3 ISP Local o de Nivel 3

Los proveedores de servicios de Internet locales son organizaciones pequeñas que cubren una determinada área geográfica no muy extensa como una ciudad.

Este tipo de ISP's no posee un acceso directo hacia el backbone de Internet, lo que hacen es conectarse a través de enlaces P2P a ISP más grandes o de nivel superior. Lo clientes acceden hacia el ISP mediante tecnologías como xDSL, broadband o fibra óptica.

Los ISP's locales generalmente cuentan con una oficina central, donde se concentran todos los dispositivos de networking necesarios para conectarse a un ISP más grande, en algunos casos estos ISP's cuentan con oficinas locales que se crean en base a la demanda de suscriptores, es decir que si el ISP cuenta con poca cantidad de suscriptores no hace falta la creación de oficinas locales, sino que la conexión del cliente se hará directamente con una oficina central.

Estructura de un ISP Local

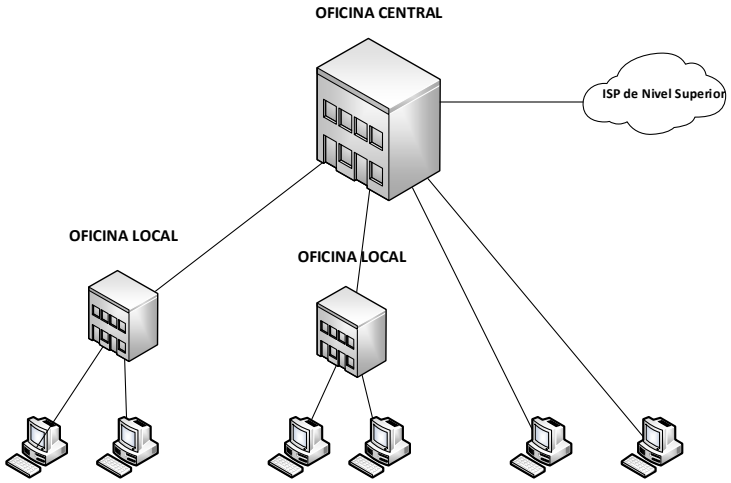


Figura 11. ISP Local
Elaborado por: Marcela Gallegos e Ismael Román

"Los ISP de nivel 3 son clientes de ISP de nivel superior para acceder al resto de Internet. Debido a que el tráfico de los ISP de nivel 3 requiere varios saltos de enrutadores para llegar a una URL, estos ISP tienden a tener una calidad de red y velocidades de acceso relativamente bajas. Las desventajas de los ISP de nivel 2 y nivel 3 son la cantidad de saltos que tiene que realizar el enrutador para llegar a Internet y la sobresuscripción del ancho de banda. Los usuarios de los ISP de nivel inferior comparten una puerta de acceso común a los ISP de nivel más alto, y el ancho de banda de la puerta de enlace puede degradar el ancho de banda de acceso." (Winther, 2006).

CAPÍTULO 2

2. CRITERIOS DE SEGURIDAD

2.1. Definición

Analizar y comprenderlos distintos aspectos mediante los cuales se puede manejar la seguridad dentro de las redes informáticas, es el punto de partida para establecer una definición concreta para seguridad informática. La seguridad física, se centra en utilizar mecanismos o equipos físicos(hardware), para proveer seguridad, mientras tanto que, en la seguridad lógica, los esfuerzos se centran en la creación de distintos protocolos y mecanismos de seguridad que minimicen los riesgos a los cuales se enfrenta la organización.

"En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a **proteger, resguardar y recuperar** dentro de las redes empresariales." (García, 2016).

La seguridad dentro de las redes informáticas es una agrupación de tecnologías que ejecutan ciertas tareas específicas con el objetivo de proveer un nivel extra de seguridad para los datos que se manejan dentro de las mismas. Todas las acciones y mecanismos que se implementen para proteger los datos deben estar bajo el concepto de un plan global de seguridad.

Existen amenazas dentro de las redes de información, que lo que buscan es echar abajo los tres principios básicos y en los que se fundamentas las redes de computadoras. Estos principios son la **confidencialidad, integridad y disponibilidad** de la información.

Confidencialidad. “Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.” (García, 2016).

Integridad: Esta característica se debe cumplir en el proceso de envió de datos o información. Se basa en que la información que se envía entre dos puntos dentro de la red no sea modificada o manipulada por un tercero. La información debe llegar totalmente integra (sin ser modificada) a su destino

Disponibilidad: La disponibilidad es una característica que basa su funcionamiento en que un recurso este habilitado para ser accesible desde cualquier punto y en cualquier momento, es decir, los datos, la información o cualquier otro recurso que posea la red debe estar disponible y ser accesible para quien este autorizado. Dentro de un proveedor de servicios de Internet, esta característica toma real importancia, ya que su modelo de funcionamiento se basa en que la información de Internet siempre esté disponible para los usuarios.

2.2. Seguridad en un ISP

Como se conoce, la seguridad informática es un tema bastante amplio y complejo que no solo preocupa a los usuarios finales sino también a las organizaciones que ofrecen servicios de Internet. Desde el punto de vista del cliente de un ISP, parece que la seguridad es de total responsabilidad del usuario final, esto en cierta parte es correcto, debido a que el usuario es el que debe tomar las debidas precauciones para que su red local (LAN) sea segura, pero por otra parte la seguridad del segmento WAN le corresponde directamente al proveedor de servicios. Es así como este tipo de organizaciones no solo se dedica a proveer servicios de Internet, sino que también se dedican y están comprometidos con proveer un nivel de seguridad bastante robusto para sus clientes.

Los ISP’s además de procurar que toda su infraestructura de red realice todas sus funciones correctamente, también se debe preocupar por generar un entorno seguro y debido a esto es que generalmente contratan empresas externas para que manejen y administren la seguridad dentro de la organización de forma integral para que la organización pueda garantizar las características esenciales de la información que le cliente envía a través del canal de comunicación que le pertenece al ISP.

“Encontrar un equilibrio entre los servicios de seguridad gestionados por el propio ISP y los subcontratados a empresas especializadas del sector es un factor clave de éxito a la hora de ofrecer niveles de seguridad, servicio y precio atractivos para el cliente final.” (ARSYS INTERNET S.L, 2007).

Ya que Internet posee algunas características especiales en cuanto a seguridad (ambiente sin seguridad), los ISP’s deben precautelar que la integridad de la información no se vea comprometida, implementando sistemas o mecanismos que puedan administrar y gestionar dichos problemas de seguridad.

“El punto fundamental de partida para el establecimiento y mantenimiento con garantías de éxito de la seguridad de la información es la definición clara de objetivos a partir de los cuales desarrollar las políticas y procedimientos que definan el marco en el que situar las medidas de seguridad a implantar” (Recio, 2012).

Una vez que se tiene en claro el punto de partida de la seguridad informática, es necesario establecer mecanismos para resguardar la información. Para esto se debe crear un plan de seguridad en el cual es necesario para que se cumpla el propósito general. La primera acción por realizar es identificar lo que se va a proteger, después se debe analizar o determinar las posibles amenazas, una vez realizado esto es

indispensable diseñar e implementar mecanismos para cumplir con el objetivo y por último se debe revisar constantemente el proceso.

Como lo menciona María de Jesús Recio, en su artículo "De la seguridad informática a la seguridad de la información", "proteger la información supone aplicar aquellas medidas destinadas a garantizar la integridad, confidencialidad, disponibilidad, autenticidad y no repudio de la información, por lo que las medidas físicas deben seleccionarse para asegurar estos aspectos". (Recio, 2012). Después de la seguridad física es importante también asegurar de manera lógica la red empresarial, para esto generalmente se utiliza distintas técnicas como la segmentación por niveles, software de detección o prevención de intrusos, sistemas de control de acceso, protocolos seguros, etc.

2.2.1. Problemas de seguridad en un ISP

El entorno de un ISP se ve envuelto en una serie de problemas de seguridad los mismos que son propios del ambiente en el que se desarrolla (Internet). La problemática actual se desarrolla básicamente en que el perímetro o la frontera del ISP es heterogéneo, es decir que se utilizan diferentes tecnologías o servicios y a esto se le añade el hecho de que todo Internet está formado por varias redes interconectadas entre sí y no todas comparten las mismas políticas o protocolos de funcionamiento.

Por otro lado, el crecimiento exponencial que existe en la actualidad en cuanto al acceso a Internet ya sea por banda ancha o por fibra óptica, también puede representar una brecha de seguridad ya que los atacantes pueden verse atraídos para utilizar las máquinas de los usuarios e infectarlas con algún tipo de software malicioso para después atacar a su objetivo, que puede ser el mismo ISP.

Seguridad hacia el usuario final

Existen algunos documentos e investigaciones que sugieren que los proveedores de servicios de Internet deberían tener más injerencia o compromiso en cuanto a la seguridad de usuario final, ya que el usuario es el eslabón más débil y puede ser usado para realizar un ataque de gran magnitud.

Una de las alternativas que se presentan o se recomiendan para solucionar este problema es en primer lugar notificar al usuario final que está siendo víctima de un malware y segundo poner a dicha computadora en cuarentena hasta que el problema esté solucionado completamente, todo este proceso lo tiene que llevar a cabo el ISP.

En algunos países, el modelo de gestión y de funcionamiento de los ISP consideran esta como una alternativa totalmente viable a tal punto que han implementado estos mecanismos dentro de las propias organizaciones. Este es el caso del Reino Unido, la Agencia de Crimen Nacional dice que, “las personas en el Reino Unido pueden recibir notificaciones de sus ISP acerca de si son víctimas de este malware, se les recomienda respaldar información importante como fotos y videos” (Nacional Crime Agency, 2014).

Este modelo de funcionamiento de algunos ISP´s en el mundo se está volviendo común, a tal punto que más y más organizaciones se van sumando di a día a esta importante iniciativa. “Por ejemplo, en Estados Unidos, Comcast introdujo alertas de seguridad para sus clientes del servicio Xfinity en el 2010 mientras que en Alemania el gobierno se asoció con los ISP para notificar a las computadoras que estaban infectadas con software malicioso de manera continua y ayudaban a los dueños a desinfectar sus equipos.” (Universidad Nacional Autonoma de México, 2014).

Mientras que la seguridad informática brindada por parte de los proveedores de servicios de Internet hacia sus usuarios debería ser una obligación, para algunos ISP, generalmente de nivel tres, es una oportunidad de negocio, en la que se establecen costos o tarifas adicionales para brindar este tipo de servicios.

Sistemas Operativos

Por otra parte, existen sistemas operativos que no son completamente seguros ya que presentan bugs o huecos de seguridad por los cuales el software malicioso puede infectar un ordenador, además las aplicaciones que se instalan en un ordenador tampoco pueden ser seguras o confiables de tal manera que el riesgo de sufrir un ataque informático aumenta considerablemente. Una vez que se identifica que el ordenador, el sistema operativo o alguna aplicación poseen alguna vulnerabilidad, se procede a realizar los denominados parches que básicamente "tapan" o cubre en hueco por el cual estaba ingresando software malicioso. Cabe recalcar que el tiempo que trascurre desde que se identifica la vulnerabilidad hasta que el parche se lo implementa completamente, es bastante largo y durante ese periodo se pueden ejecutar un sin número de ataques informáticos, que, si no se cuenta con un software especializado para la detección de los mismos, pueden ocasionar un daño considerable al usuario.

Software malicioso

Cuando se navega a través de Internet el usuario está expuesto a distintos tipos de ataques que generalmente son intentos de robo o de suplantación de identidad (phishing, pharming), virus, spyware, BotNets, e intentos de denegación de servicios. En este punto es importante mencionar cómo funcionan los BotNets, que son un tipo de malware que lo que pretenden es tomar control de un ordenador para realizar acciones ocultas sin consentimiento del usuario, por lo general los BotNets realizan envíos de spam hacia otras redes.

1. El atacante infecta el ordenador de la víctima con BotNets, a través de algún software portador.
2. Los BotNets (porciones de código) se conectan a una red denomina IRC (Internet Relay Chat), que es un protocolo de comunicación en tiempo real basado en texto, con el cual dos o más usuarios pueden comunicarse a través de Internet.
3. Un usuario mal intencionado (Spammer) compra al atacante el acceso a los BotNets que previamente fueron instalados en el ordenador infectado.
4. El Spammer envía comandos o segmentos de código malicioso hacia otros sistemas vía IRC.
5. Finalmente, el spam llega a su objetivo, que pueden ser otros sistemas de comunicación o computadoras dispersas geográficamente.

BotNets – Modo de operación

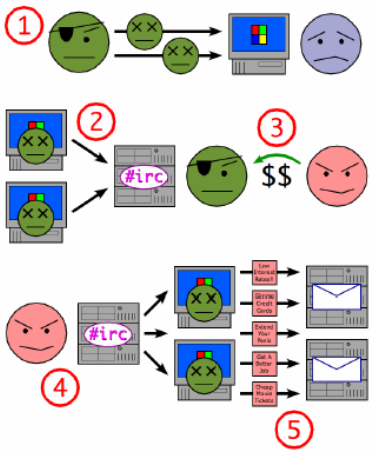


Figura 12. Funcionamiento de los BotNets
Fuente: (Martinez & Vidal, 2006)

Ataques de Denegación de Servicios.

Este tipo de ataques son los que ocurren con más frecuencia dentro de Internet. El objetivo de este tipo de ataques es imposibilitar que algunos o todos los recursos alojados en un servidor no estén disponibles cuando se lo requiera. Cuando este tipo de ataque está dirigido hacia un proveedor de servicios como un ISP, se puede hablar

de denegación de servicios por flooding, que básicamente es inundar la red o sobrecargar un servidor con algún tipo de petición, generalmente las peticiones son a través de los protocolos ICMP o UDP.

Este tipo de ataques cuanta con una variante, en lugar de realizar el ataque desde una única fuente, lo hace desde varias fuentes o nodos produciendo un ataque de tipo distribuido **(DDoS).** El objetivo de este tipo de ataques es producir un daño mucho mayor y que sea difícil detectar desde que nodo se ha producido el mismo.

Spoofing

Esta clase de ataque informático se basa en la suplantación de identidad. La técnica más utilizada para llevar a cabo estos ataques es cambiar la dirección IP de origen por otra totalmente diferente ubicada en alguna ubicación geográficamente alejada. De esta manera se pueden perpetrar actos informáticos maliciosos con una identidad que no corresponde al atacante.

Protocolos de Enrutamiento

Los protocolos de enrutamiento generalmente pueden representar un problema de seguridad para los ISP's. Los ISP utilizan dos tipos de enrutamiento, protocolos de enrutamiento interiores y exteriores.

El enrutamiento interior cumple con la función de encaminar o dirigir los paquetes de datos originados por los clientes, hacia la red del ISP (RIP, OSPF, EIGRP). Mientras tanto el enrutamiento exterior se encarga de redirigir los paquetes de datos generados en la red del ISP, hacia otra red distinta. El protocolo BGP (Border Gateway Protocol) es el más utilizado en el enrutamiento externo.

La principal amenaza a la que se enfrentan los protocolos de ruteo es al envenenamiento de sus tablas de redireccionamiento. Si se logra infectar dichas tablas,

la información se enviará a un destino incorrecto y los atacantes podrán hacer uso de la información que originalmente debía ser dirigida hacia Internet.

Mientras que el problema fundamental de los protocolos de enrutamiento exteriores se centra en la **caída de enlaces**. En caso de ocurrir esto el usuario puede experimentar problemas de accesibilidad, el destino será inalcanzable.

Ataques a DNS

En los últimos tiempos otro objetivo bastante apetecido por los atacantes es el DNS (Domain Name System). Este en servicio bastante importante y crítico que ofrecen la mayoría de ISP, su función principal es traducir las direcciones IP de las páginas web, a nombres que sean fáciles de recordad para los usuarios.

El servicio de DNS es crítico dentro de la navegación web, es por eso que se ha convertido en el principal objetivo de varios atacantes en esta era. De esta manera este servicio que ofrece el ISP se puede convertir en un problema de seguridad bastante grave si es que no se lo configura adecuadamente y además si no se implementan mecanismos de seguridad para que este no se pueda ver afectado por ataques informáticos.

En la actualidad no existe una solución específica para resolver este problema, pero se pueden considerar una serie de acciones que endurezcan la seguridad de este servicio crítico. Como lo mencionan Martínez y Vidal en su documento titulado “Seguridad en un Proveedor de Servicios de Internet”, “todo parece indicar que lo más adecuado es combinar soluciones, niveles de seguridad, en diferentes capas y tener varias fronteras que nos separen del enemigo.” (Martinez & Vidal, 2006). Un mecanismo de prevención puede ser la utilización de varios firewalls para que atacante no pueda ingresar fácilmente a la red. Otro mecanismo bastante importante es la utilización

redes LAN virtuales (VLAN). La función principal de las VLAN's es dividir a la red en segmentos y aislar en cierta forma algunos recursos importantes para la organización, generalmente se debe crear una VLAN para toda la granja de servidores que es donde se encuentran alojados todos los servicios críticos.

Utilización de Firewalls

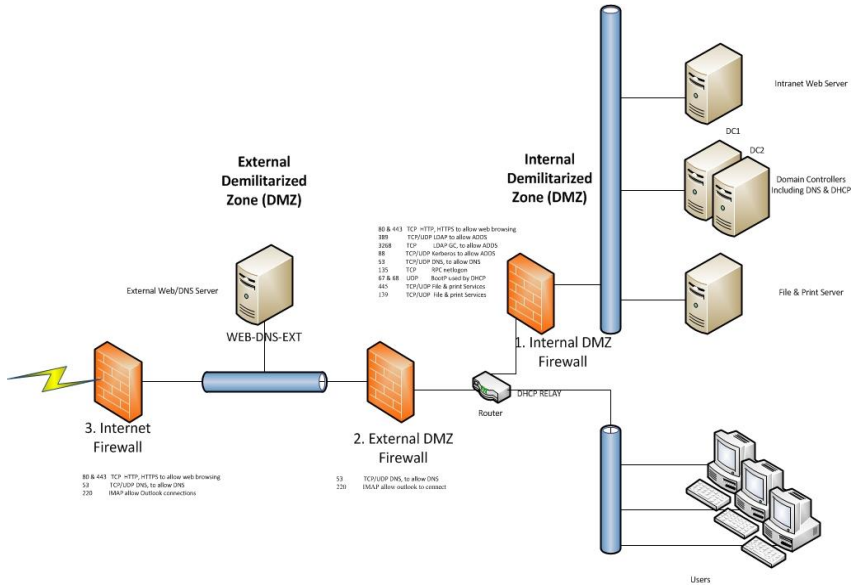


Figura 13. Distribución de Firewalls
Fuente: (McCherry, 2014).

En la figura No. 13, se puede apreciar una adecuada distribución de dispositivos de seguridad (Firewalls). Se puede observar que existe un Firewall que protege directamente a los servidores de la zona desmilitarizada externa, que es justamente donde se encuentra un servidor DNS. También se puede apreciar que no solo se protege la red con dispositivos físicos, sino también con mecanismos de seguridad lógicos como redes LAN virtuales que aíslan ciertos segmentos de la red del ISP.

También se debe tener especial cuidado con respecto a los puertos que se encuentren abiertos en el Firewall, la práctica más recomendable es únicamente abrir los puertos que las aplicaciones o los servicios vayan a utilizar. En la figura No. 13 se puede observar que en el Firewall de Internet únicamente se encuentran abiertos los puertos que corresponden a los servicios Web y DNS.

Problemas de Seguridad en las capas de Internet

Los proveedores de Internet, además de presentar problemas de seguridad por parte de algunos ataques informáticos, también presentan otros problemas de seguridad que se relacionan directamente con los protocolos y servicios que manejan para poder ofrecer el servicio de acceso a Internet.

Modelo de Red TCP/IP

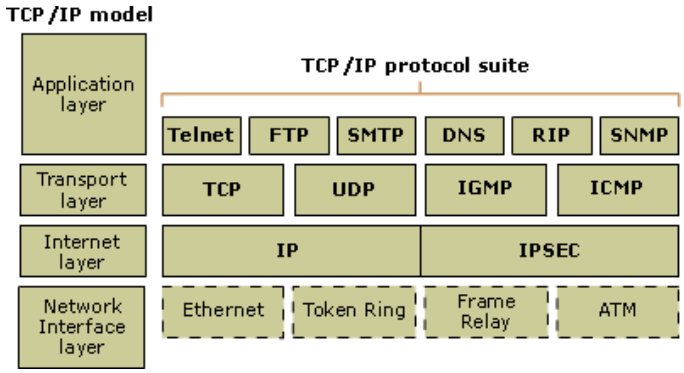


Figura 14. Modelo TCP/IP
Fuente: (Microsoft, 2009).

Bajo el modelo TCP/IP que se muestra en la figura No. 14, se representa todo el funcionamiento de la trasmisión de datos a través de Internet. En la figura anterior también se muestran los principales protocolos que trabajan en cada capa del modelo TCP/IP. Estas capas y protocolos son los que presentan vulnerabilidades que pueden ser aprovechadas por los atacantes para causar grave daño a la estructura en general de un ISP.

2.3. Requerimientos de seguridad en un ISP

Generalmente los requisitos de seguridad de un ISP se basan en la prevención, detección y recuperación de los ataques a los que comúnmente se enfrentan. Es decir que los requisitos de seguridad serán la manera en el proveedor de servicios se proteja ante dichos ataques. Los ataques informáticos por lo general están dirigidos casi siempre al usuario final ya que es el último eslabón en la cadena que conforma una red

de datos y por lo general es el más débil e indefenso, no obstante, los proveedores de servicios también enfrentan sus propios problemas en cuanto a seguridad, algunos de los ataques informáticos, dentro de los últimos tiempos, están dirigidos exclusivamente a este tipo de organizaciones. De estos ataques se pueden extraer los requisitos de seguridad que necesita un ISP para funcionar de manera correcta A continuación, se listan los principales requisitos de seguridad que posee un ISP.

Resistencia a los ataques de denegación de servicios (DoS, DDoS). Este tipo de ataques buscan deshabilitar ciertos servicios de Internet a los cuales el usuario tiene acceso legítimamente. El ISP debe implementar mecanismos y acciones para ser resistente a este tipo de ataques informáticos.

Evitar excesivo tráfico y escasez de recursos. Generalmente este tipo de problemas se presentan por la mala utilización del host dentro de la propia organización (Descarga de contenido innecesario). Este problema también se debe a que en ocasiones los hosts de la organización pueden estar infectados causando de esta manera el consumo excesivo de recursos de los servidores que posee el ISP.

Prevenir ataques al protocolo de enrutamiento BGP (Border Gateway Protocol). Este tipo de ataques se basan en insertar rutas defectuosas en la tabla de enrutamiento del protocolo para redireccionar el tráfico hacia otro destino**.** Después de obtener los datos, los atacantes filtran el tráfico que es de su interés.

Fortalecer el Sistema de Nombres de Dominio (DNS). Por lo general, se suele atacar el servidor DNS con el fin de redirigir o redireccionar el tráfico de Internet hacia destinos que no están debidamente autentificados y que obviamente pertenecen a los atacantes.

Endurecer la seguridad de los dispositivos de Networking. Uno de los principales ataques que llevan a cabo los delincuentes cibernéticos es el compromiso de la

infraestructura de red del ISP. La acción que frecuentemente usan después de comprometer el dispositivo es modificar su configuración para que no funcione como se debería. Dos de los factores más importantes para que existan amenazas en las redes de los ISP's son:

- **Seguridad de los canales y medios de trasmisión.** La seguridad que debe ofrecer un ISP no puede ser granular sino integral, tampoco puede centrar su seguridad en la utilización únicamente de firewalls y de sistemas de detección o de prevención (IDS/IPS). Un ISP debe crear un nuevo modelo de seguridad que se ajuste a sus propios requisitos y necesidades, entre estas necesidades están la seguridad de los canales y los medios por los cuales se trasmite la información.

2.3.1. Mecanismos de seguridad

Existen diferentes métodos que pueden aportar en la generación de un entorno seguro dentro de un ISP. Estos se clasifican de la siguiente manera.

De prevención:

- Mecanismos de autenticación e identificación
- Mecanismos de control de acceso
- Mecanismos de separación física, temporal, lógica.
- Mecanismos de seguridad en las comunicaciones (cifrado de la información)
- IPS (Intrusion Prevention System)

De detección:

- IDS (Intrusion Detection System)

De recuperación:

- Copias de seguridad (backup)
- Mecanismos de análisis forense. (ARSYS INTERNET S.L, 2007).

A continuación, se detallan las acciones más importantes que se pueden aplicar en un ISP.

Actualización y parcheo de sistemas

Mantener actualizados todos los sistemas que maneja el ISP, es un mecanismo de seguridad muy importante, ya que de esta manera se pueden estar corrigiendo bugs de seguridad que pueden presentar los mismos. Las actualizaciones de las aplicaciones o sistemas buscan dar mantenimiento y parchar ciertos "huecos" que posean las mismas.

Redes y seguridad perimetral

Algunos ISP's requieren la colaboración de empresas especializadas en seguridad para cumplir con este tipo de tareas. El objetivo de la organización es mantener gestionada y bajo control a esta zona de la red.

Infraestructuras y seguridad física

Una de las acciones más importantes y críticas al momento de resguardar la seguridad informática de un ISP, es la implementación de Infraestructura de red que garantice este principio y además contar con mecanismos de seguridad física que generen un ambiente totalmente controlado.

Algunos de los sistemas de seguridad física más utilizados son, acceso autorizados mediante biométricos, sistemas integrados de video vigilancia, sistemas de climatización, sistemas contra incendios, etc. Además, se debe contar con infraestructura especializada como son IDS, IPS, Firewalls, ASA, Routers de Frontera, etc.

Desarrollo de aplicaciones

La organización además de necesitar hardware que aporte en la seguridad de la organización, también necesita desarrollas aplicaciones o sistemas que incrementen el nivel de seguridad de la misma.

EL incidente de seguridad más común dentro de un ISP es la intrusión de código malicioso en su infraestructura de red. Es por este motivo que resulta siendo necesario la utilización de aplicaciones que prevengan, detecten y den tratamiento a este tipo de incidencias. Las aplicaciones que se usen dentro de este tipo de organizaciones deben estar diseñadas bajo metodologías de desarrollo que aseguren la integridad de la información que se esté manejando.

2.4. Requerimientos de seguridad hacia el usuario final

En la actualidad existen muchos riesgos de seguridad que en cierta parte se desconocen por parte del usuario, ya que este asume que la organización que le provee de acceso a Internet se encargará de velar por su seguridad. Lastimosamente esto no es así, los ISP no están obligados a garantizar la seguridad del usuario final, ya que no existe una ley que les obligue a realizarlo. Esta es exactamente la situación actual dentro del ámbito nacional, no obstante, algunas de estas organizaciones proveen mecanismos de seguridad hacia sus clientes ya que desde el usuario final se pueden generar ataques que dañen la infraestructura del proveedor de servicios.

Privacidad. Generalmente se centra en que los datos de navegación o de transito sean confidenciales, es decir que los organismos encargados de llevar y traer tráfico (ISP's) no tengan acceso a los mismo.

Transmisión confiable de datos. EL ISP, debe asegurar que la información proveniente del cliente que viaja por su canal de comunicación será integra en su totalidad, es decir la organización prestará e implementará funciones para asegurar sus canales de comunicación, con el objetivo de que los datos no sean manipulados por terceros. Las medidas que comúnmente se toman para asegurar el circuito de trasmisión son VPN's o el protocolo IPSec.

Protección contra ataques cibernéticos. Este concepto se relaciona a lo ya mencionado anteriormente, el ISP debe tomar el control de cierta forma de los hosts de los usuarios finales, esto con el fin, primero de informar a los usuarios que están siendo víctimas de un ataque informático y segundo para aislar a dichos hosts de la red en general con el fin de impedir que el ataque se propague. Este tipo de medidas generarían gastos adicionales para el ISP, pero se mejoraría de manera considerable el entorno de seguridad del ISP.

2.5. Gestionar la seguridad de un ISP

Gestionar la seguridad de toda la red de un ISP es en realidad una tarea bastante grande, ya que se debe controlar una serie de servicios y protocolos. Existe un conjunto de acciones que permite administrar de manera integral toda la seguridad de la organización, esta alternativa es utilizar mecanismos de monitoreo, control y seguimiento.

Mecanismos de monitoreo, control y seguimiento.

La utilización de estos mecanismos permite conocer si algún recurso de red está funcionando de manera inusual o si está funcionando correctamente. Existen diferentes dispositivos y protocolos que se pueden utilizar para ejecutar estas tareas (monitoreo, control y seguimiento), entre los más importantes, destacan IDS's, network appliance, husmeadores de paquetes (sniffers), protocolos de monitoreo como el Simple Network Management Protocol (SNMP) y protocolos de monitoreo remoto (RMON).

Además de los protocolos ya mencionados, existe un mecanismo sumamente eficiente para analizar el tráfico que está cruzando por un dispositivo de seguridad, esta característica se denomina puerto espejo, su modo de funcionamiento consiste en trasmitir el tráfico de un puerto a otro con la finalidad de analizar el tráfico.

Auditoria, monitoreo y detección de intrusos.

Utilizar mecanismos de auditoria y detección de intrusos permite administrar de mejor manera la seguridad en un ISP. Este tipo de acciones pueden analizar todo el sistema de red en tiempo real y generar alertas en base a patrones de comportamiento. Con esto se puede detectar comportamientos extraños en la red, por ejemplo, si el ancho de banda incrementa sin razón alguna es un indicio que puede significar que en la red se encuentra un intruso (malware o programa).

La auditoría informática es una herramienta bastantéate importante dentro del correcto funcionamiento de la seguridad de un ISP. La auditoría debería utilizarse como mecanismo de prevención para evaluar estándares y políticas de seguridad que posea la organización. La auditoría informática debería realizarse por una empresa externa que no tenga en juego intereses, esto con el fin de que proporcione un enfoque bastante claro e imparcial de los resultados de este proceso.

Actividades de Fortalecimiento (Hardening)

Si bien es cierto no es una acción prioritaria parapara asegurar que los datos sean íntegros, es una actividad que se puede desempeñar conjuntamente con otros procedimientos para ofrecer robustez a la seguridad de la organización.

Una de las acciones principales cuando se habla de fortalecimiento o hardening, es configurar de manera adecuado todos los dispositivos de red. Por lo general los profesionales de TI, no se preocupan por cambiar las configuraciones por default que viene en los dispositivos, esto representa una brecha de seguridad dentro de la organización, ya que los atacantes pueden aprovechar esta vulnerabilidad y afectar la red de la organización. A continuación, se listan las acciones de fortalecimiento que generalmente se utilizan en un ISP.

- Desinstalar programas innecesarios o de fuentes desconocidas en los hosts que pertenecen a la organización, esto podría representar una brecha de seguridad.
- Configurar únicamente los servicios de red necesarios para la organización.
- Considerar el acceso remoto exclusivamente a equipos que realmente necesiten supervisión y monitoreo remoto.
- Deshabilitar el protocolo telnet dentro de los equipos de red que lo tengan instalado. Se conoce que este protocolo no aporta la seguridad necesaria y se debe optar por la configuración del protocolo SSH (Secure Shell).
- Manejar listas negras, en las que se puede agregar direcciones IP que tengan comportamiento sospechoso.
- Deshabilitar o eliminar cuentas de usuarios que ya no pertenezcan a la compañía.
- Establecer permisos a los usuarios en base a las actividades que realizan en la organización. Utilizar criterio de mínimos permisos.
- Generar políticas de seguridad, que sustenten la utilización de contraseñas robustas para todos los usuarios que pertenecen a la organización.
- Crear grupos de usuarios y de equipos que cumplan funciones similares, para poder administrar y gestionar los permisos de una manera centralizada y general.

Por lo general a los dispositivos que se les presta mayor atención dentro del proceso de fortalecimiento son los switch y routers, ya que son estos dispositivos los que más pueden presentar brechas de seguridad.

- Mantener al día las actualizaciones del firmware de los equipos de networking.
- Eliminar todas las preconfiguraciones de la infraestructura de red, esto incluye deshabilitar servicios innecesarios.

- Realizar un estudio, para determinar el tipo de permiso que se otorgará a cada usuario, especialmente a los administradores de red.
- Realizar auditorías regularmente y revisar las bitácoras o los registros de actividades de los dispositivos.
- Adecuar el espacio físico para que los dispositivos sean de fácil acceso, pero a la vez estén en una ubicación segura.

2.6. Modelo de seguridad para un ISP de nivel 3

Planificar estrategias de seguridad es el paso intermedio que permite interconectar los equipos y aplicaciones de seguridad con las personas que interactúan directamente con la infraestructura de red.

El modelo de seguridad que puede adoptar un ISP de nivel tres, basa su funcionamiento en la estructuración de seis capas, donde se segmentan y se dividen las funciones de toda la red de la organización Cada capa trabaja para garantizar la seguridad del segmento al que ha sido asignada.

Modelo de Seguridad para un ISP de nivel 3

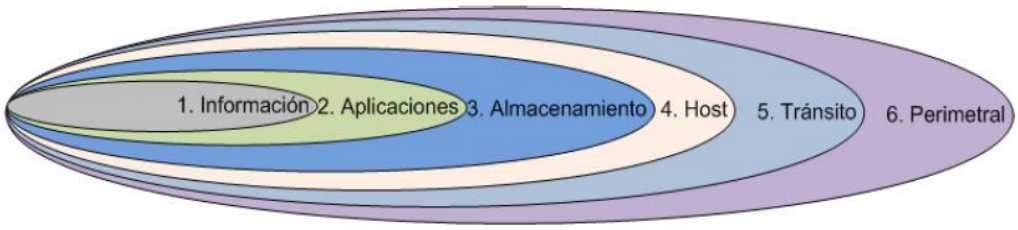


Figura 15. Modelo de seguridad para un ISP de nivel 3
Fuente: (BALTAZAR GÁLVEZ & CAMPUZANO RAMÍREZ, 2011).

La característica que diferencia a este modelo es que se pueden añadir o quitar capas de acuerdos a las necesidades o requerimientos de la organización, de esta manera se puede decir que este modelo es completamente apto para poder utilizarlo en un ISP de nivel 3.

Capa de Información. El objetivo general de este segmento es generar, monitorear y actualizar las políticas de seguridad que se relacionan directamente con la información que maneja la organización. Entre las acciones las frecuentes que se definen en las políticas están, definir quien tiene acceso a la información, que tipo de información va a ser pública, establecer mecanismos lógicos y físicos que resguarden la información.

Capa de Aplicaciones. Esta capa se encarga generalmente de la administración de las aplicaciones y servicios que el proveedor de servicios va a ofrecer. Generalmente se encarga de estructurar un plan de implementación de cada uno de los servicios y con esto todo lo que conlleva, asignación de recursos, privilegios, accesibilidad, administración de puertos, análisis de seguridad, mantenimiento y actualización de las aplicaciones, etc.

Capa de Almacenamiento. El objetivo de este segmento es llevar a cabo un análisis completo de las aplicaciones, servicios y procedimientos que se ejecutan en el ISP, esto con el fin de determinar de manera correcta la cantidad de recursos de almacenamiento que necesitaran. Esta capa toma en cuenta los recursos de almacenamiento y también de procesamiento. Si no se realiza el análisis de requerimientos de manera adecuada, se pueden sobredimensionar los recursos que una aplicación necesita y esto puede producir congestionamiento la red de la organización.

Capa de Host. Esta capa es la que se encarga de gestionar y administrar toda la seguridad concerniente a los hosts que pertenecen a la organización. Es aquí donde se establecen mecanismos de acceso, control de usuarios, designación de privilegios, implementación de software antivirus, generación de políticas relacionadas con la utilización de dispositivos de almacenamiento extraíbles, agregación al dominio de la organización a todos los hosts, soporte técnico (helpdesk), etc.

Capa de Transito. La capa de transito cumple con la función de resguardar el canal de comunicación por el cual se envía toda la información, esto comprende desde que el usuario genera un flujo de datos, hasta que los datos llegan a su destino (Internet). Los profesionales que se encargan de esta área tienen la responsabilidad de utilizar protocolos de seguridad que garanticen que le canal de comunicación va a ser totalmente seguro, por lo general se suelen utilizar técnicas como VPN o IPSec para fortalecer la seguridad del canal.

Capa Perimetral. Este segmento centrará todos sus esfuerzos en implementar seguridad de los bordes de la topología de red del ISP. Se recomienda utilizar Firewalls, IDS, y Appliance ya que estos son algunos de los mecanismos más utilizados y de mejor desempeño. También se suelen aplicar conceptos como la estructuración de DMZ's para resguardar los recursos de red.

Además de la implementación del modelo de seguridad de seis capas, existen otras técnicas de seguridad que se pueden ejecutar, para de esta manera obtener un entorno mucho más seguro.

Seguridad en profundidad. El concepto de seguridad en profundidad se basa en ubicar múltiples barreras de seguridad, de tal manera que si una barrera es superada el atacante se encontrar con características de seguridad superiores.

Eslabón más débil. Este concepto se centra en realizar un estudio completo para conocer cuál es la parte más débil y por donde pueden ingresar atacantes cibernéticos. Generalmente, las configuraciones por defecto de los equipos de red, las contraseñas poco robustas y por supuesto los hosts que pertenecen a los clientes suelen ser las partes más débiles. Una vez identificado el eslabón más débil se procede a establecer mecanismos de seguridad para fortalecer al mismo.

Seguridad basada en red. Este mecanismo implementa alarmas que se disparan el momento en que la seguridad haya sido vulnerada. Por lo general, junto con el concepto de seguridad basada en red, se maneja la seguridad perimetral.

Principio de menor privilegio. Este concepto se basa en la asignación de los privilegios estrictamente necesarios a un usuario de la organización, esto con el fin de evitar conflictos de seguridad con usuarios inexpertos que intenten cambiar las configuraciones de los dispositivos de red. Este principio no solo se basa en usuarios, sino que también se aplica a programas, sistemas y demás mecanismos que se desempeñen dentro de la red de datos de la organización.

Seguridad por oscuridad. Este mecanismo de seguridad busca mantener en total resguardo el funcionamiento de la red del ISP, así como también las aplicaciones, servicios y procedimientos que se ejecutan en la organización. Se mantiene la idea de que, si no se conoce como está estructurado un sistema, la red no estará susceptible a ataques.

Punto de ahogo. Esta técnica busca generar y establecer un único punto en la red por el cual entre y salga la información, esto con la finalidad de centrar todos los esfuerzos de seguridad en una sola ubicación y no en toda la red de la organización. Se recomienda utilizar esta técnica en conjunto con otras estrategias de seguridad, por ejemplo, redundancia de servicios y aplicaciones, seguridad perimetral, entre otras.

2.7. Introducción IPv6

En 1991, el IETF – Internet Engineering Task Force, cuya funcional principal es la investigación y creación de tecnologías, quien también tiene como objetivo analizar propuestas y regulación de estándares, (MIKROWAYS, 2010) ; se planteó dar solución a la escasez de disponibilidad de direcciones IPv4, con la creación del

protocolo IPv6 definido en el RFC 2460, el cual viene acompañado de distintas funcionalidades y protocolos para poder reforzar la seguridad e infraestructura de red.

La disponibilidad de direcciones, es evidente la diferencia entre la versión 4 y la versión 6, por un lado, con la creación de IPv4 se alcanzó un rango de $2^{32} = 4.294.967.296$ direcciones posibles (representadas en formato decimal, 4 grupos de 8 bits, separados por puntos) mientras que con IPv6 se obtiene un total de $2^{128} = 240\ sextillones$ direcciones posibles (representadas en formato hexadecimal, 8 grupos de 16 bits, separados por dos puntos), información obtenida de la publicación del medio de prensa electrónico "END – El Negocio Digital" en el 2015, (EL Negocio Digital, 2015).

El impacto generado por el protocolo ipv6 ha sido tan grande, que su llegada se puede percibir en distintos ámbitos de desarrollo, como lo es el IOT o Internet de las cosas, como se puede apreciar en lo siguiente: "En febrero de 2010, se agotaron las direcciones IPv4 del mundo. Si bien el público en general no ha observado un impacto real, esta situación podría lentificar el progreso de IOT, ya que los posibles miles de millones de sensores y/o dispositivos inteligentes necesitarán direcciones IP exclusivas. Además, IPv6 facilita la administración de las redes gracias a las capacidades de autoconfiguración y ofrece características de seguridad mejoradas", (Evans, 2011). El contenido citado hace referencia a la escalabilidad y adaptabilidad del protocolo Ipv6, es decir, no es necesaria ninguna implementación o consideración extra, para que este protocolo pueda trabajar sobre su antecesor IPv4.

Todas las funcionalidades del protocolo IPV6, componentes y demás son analizadas a detalle en los apartados siguientes.

2.8. Arquitectura IPv6

La arquitectura de IPv6 contempla dentro de su desarrollo permitir a los host y usuarios de IPv4, la facilidad de una migración o transición hacia el nuevo protocolo, incorporando servicios como seguridad, calidad de servicio y un nuevo direccionamiento, todas estas implementaciones son implementadas en el encabezado del protocolo. Por ejemplo, dentro de esta arquitectura se reduce de 12 a 8 campos en la cabecera, adicionalmente la nueva versión IPv6 soporta una amplia variedad de protocolos de enrutamiento como RIPng (RIP para IPv4), EIGRP, OSPFv6, IS-ISv6, entre otros.

2.8.1. Paquete IPv6

La versatilidad y e increíble funcionalidad de IPv6 radica en el encabezado, si bien es cierto una dirección IPv6 es más grande (longitud) que una IPv4, los campos del primero se reducen, haciendo de este protocolo una verdadera sorpresa, ya que desaparecen campos innecesarios, pero el protocolo ofrece una mayor seguridad.

Cabecera IPv6

La cabecera con una longitud de 40 bytes comprende 8 campos, los cuales son: versión, clase de tráfico, etiqueta de flujo, longitud de la carga útil, cabecera siguiente, límite de saltos, dirección origen y dirección destino, (Deering & Hinden, 1998).

Tabla 3. Encabezado IPv6

N°	CAMPO	LONGITUD (BITS)	DESCRIPCIÓN
1	Versión	4 bits	Versión del Protocolo IP (0110 en hexadecimal: 6)
2	Clase de tráfico	8 bits	Prioridad del paquete
3	Identificador de flujo	20 bits	Calidad de servicio
4	Longitud de carga útil o contenido	16 bits	Indica la cantidad de información útil del paquete
5	Cabecera siguiente	8 bits	Identifica el tipo de cabecera siguiente, similar al campo “Protocolo” de IPv4.

			0x01 – ICMP – Internet Group Management Protocol
6	Límite de saltos	8 bits	Campo utilizado para evitar que un paquete caiga en un bucle de red infinito, similar al campo "TTL" de IPv4. Cada vez que el paquete pasa a través de un enlace este campo decrementa en 1, al llegar a 0 el paquete de descarta.
7	Dirección IP de origen	128 bits	Este campo indica la dirección origen del paquete
8	Dirección IP de destino	128 bits	Este campo indica la dirección destino del paquete

Nota: Descripción del encabezado IPv6
Elaborado por: Marcela Gallegos e Ismael Román

Estructura del encabezado IPv6

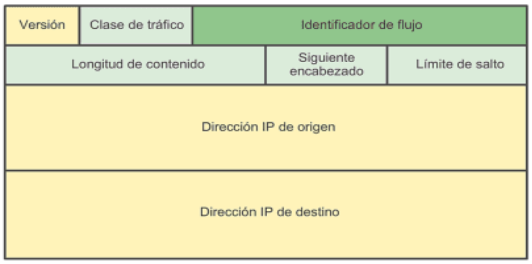


Figura 16. Encabezado IPv6
Fuente: (Walton, 2017).

Encabezado IPv6 vs IPv4

Estructura del encabezado IPv4

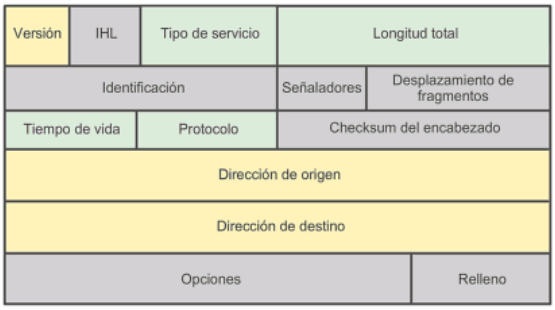


Figura 17. Encabezado IPv4
Fuente: (Walton, 2017)

El encabezado de IPv4 con una longitud variable de 20 bytes, está compuesto por 12 campos con información importante sobre los protocolos, aun así; una de las mejoras del paquete IPv6 con respecto a la versión 4.

2.8.2. Tipos de direcciones

El protocolo IPv6 en cuanto a difusión se refiere no ha cambiado mucho, por un lado, IPv4 maneja direcciones de difusión unicast, multicast y broadcast, mientras que en la versión 6 desaparece la dirección de broadcast, pero aparece “anycast”.

Tabla 4. Direcciones de difusión

TIPO DE DIRECCIÓN	DESCRIPCIÓN
Unicast	La comunicación e intercambio de paquetes es uno a uno, en el cual intervienen una dirección de origen y una de destino.
Multicast	La comunicación e intercambio de paquetes es de uno a varios, en el cual para poder transmitir o recibir se debe pertenecer a un grupo multicast
Anycast	La comunicación es uno al más cercano.

Nota: Descripción de las direcciones de difusión.
Elaborado por: Marcela Gallegos e Ismael Román

Por otro lado, existen ciertas direcciones de IPv6 que son necesarias analizarlas y compararlas en ciertos casos con las direcciones IPv4 las cuales se presentan a continuación:

Tabla 5. Direcciones IPv6

IPV6	LONGITUD PREFIJO	**DESCRIPCIÓN**	IPV4
::	128 bits	Sin especificar	0.0.0.0
::1	128 bits	Loopback	127.0.0.1
::00:xx:xx:xx:xx	96 bits 64 bits - IPv6 32 bits - IPv4	Direcciones IPv6 compatibles con IPv4 – Direcciones empotradas	NA
::ff	96 bits 64 bits - IPv6 32 bits - IPv4	Representar direccionesIPv4 mediante direcciones IPv6	NA
fe80:: - feb::	10 bits	Direcciones de link-local	Loopback
fec0:: - fef::	10 bits	Direcciones site-local	Direcciones IP privadas
ff::	8 bits	Direcciones multicast	NA
001	3 bits	Las direcciones unicast globales empiezan con “001”	NA

Nota: Descripción de las direcciones IPv6
Elaborado por: Marcela Gallegos e Ismael Román

2.9. Introducción IPSec

El protocolo de seguridad IPSec, definido por la IETF, como estándar opcional para IPv4 y obligatorio para IPv6, abarca la unión de protocolos cuya función es brindar un alto nivel de seguridad a los paquetes que viajan a través de la red, protegiendo las comunicaciones al incluir características de autenticación y cifrado de extremo a extremo, haciendo que las comunicaciones en redes públicas y privadas sean más estables y confiables. Este protocolo definido bajo el RFC 6071 (Frankel & Krishnan, 2011), y bajo el RFC 2401 (Kent & Atkinson, 1998); proporciona diferentes servicios de seguridad, al ser un estándar abierto que permite seleccionar que servicios implementar, brinda la capacidad de realizar un hardening (proceso de asegurar un sistema reduciendo sus vulnerabilidades o puntos en los cuales existen riesgos) de seguridad capaz de adaptarse al modelo de negocio de una infraestructura de red.

Los beneficios que trae la implementación de este protocolo son numerosos y para poder comprender su funcionamiento es necesario un análisis de su arquitectura y componentes los cuales son detallados en apartados siguientes.

El protocolo IPSec abarca las siguientes cuestiones de seguridad:

- **Autenticación.** La autenticación se la realiza para verificar que la persona u usuario que envía la información sea quien dice ser.
- **Integridad.** La integridad ayuda a verificar que el contenido no se ha cambiado o alterado en el camino.
- **Confidencialidad.** Oculta el contenido del mensaje, con esto, solo el remitente / destinatario autorizados y autenticados accedan a él.
- **Gestión de claves.** El protocolo IPSec maneja una gestión automatizada de claves criptografías y asociaciones de seguridad, mediante la AH -Cabecera de

Autenticación y ESP - Carga Útil de Seguridad Encapsulada, protocolos que se analizan más adelantes.

- **Protección.** IPSec puede ser implementado y empleado para proteger diferentes trayectos o caminos, por ejemplo: entre un par de host (del Host A al Host B), entre host y una puerta de enlace (Host A al Gateway de seguridad) o entre pares de puertas de enlace (Gateway de seguridad), (Vazquez Clavijo, 2011).

2.9.1. Funcionamiento IPSec

El funcionamiento del protocolo de seguridad IPSec, se basa en dos configuraciones modo transporte y modo túnel, dependiendo del tipo de conexión establecida.

a) Modo Trasporte

En el modo transporte proporciona una seguridad punto a punto, IPSec, puede aplicar diferentes directivas basándose en los campos del paquete IPv6 como "siguiente encabezado", esta implementación contempla que solo la "carga útil" es protegida por el proceso de cifrado y autenticación. (Lopez, 2007).

La dirección de destino no se ve afectada, ya que, la cabecera IP no entra en modificación, como en la imagen siguiente:

IPSec – Modo trasporte

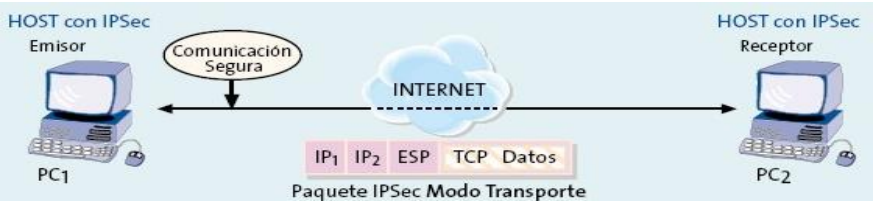


Figura 18. Modo Transporte de IPSec
Fuente: (UNEX, 2006)

b) Modo Túnel

En el funcionamiento del modo túnel, todo el paquete IP es protegido por los procesos de cifrado o autenticación, esto se logra sometiendo todo el paquete a una técnica de

encapsulamiento, con esto proceso cambia la dirección de origen y destino, por las nuevas direcciones del túnel recién creado, como se aprecia a continuación:

IPSec – Modo túnel

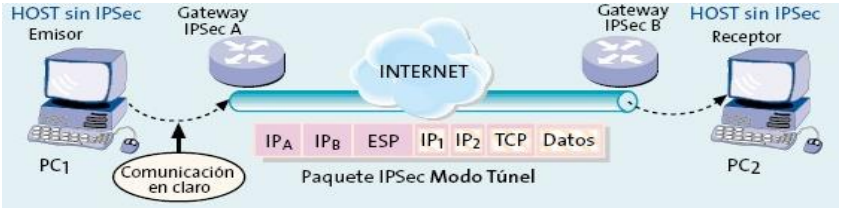


Figura 19. Modo Túnel de IPSec
Fuente: (UNEX, 2006)

2.9.2. Arquitectura IPSec

Una de las consideraciones más importantes del protocolo es que es independiente de la topología manejada, ya que al trabajar a nivel de capa de Red resulta ser totalmente transparente a las aplicaciones. A diferencia de SSL, que solo funciona con HTTP, IPSec puede brindar y establecer conexiones seguras para todos los protocolos de la capa aplicación, (Palet, 2001).

IPSec trabaja autenticando y cifrando los datos que se envían entre el host emisor/receptor en una red, intranet o extranet, también incluye la protección entre terminales finales de trabajo y servidores, y entre servidores, logrando cifrado de extremo a extremo, entendiendo así que los únicos hosts que conocen que su enlace trabaja con IPSec son el emisor y receptor.

Componentes IPSec

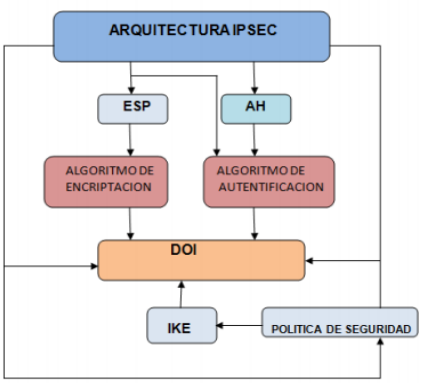


Figura 20. Arquitectura IPSec
Fuente: (Villagra, 2000)

En la ilustración anterior, se contempla la arquitectura básica de IPSEC, el cual proporciona un escenario seguro, para que esto suceda, en necesario que los extremos participantes compartan los dos protocolos de seguridad ESP y AH, incluido el protocolo de gestión e intercambio de calves IKE – Internet Key Exchange.

Finalmente, el dominio de interpretación o DOI, define los parámetros ah negociar en las políticas de seguridad y poder establecer canales seguros, esto incluye identificadores para los algoritmos de autenticación, cifrado y encriptación a lo largo del proceso de comunicación, también incluye los parámetros en los cuales IKE – Intercambio de Claves, por ejemplo: el tiempo de vigencia de las claves.

Con toda esta información se puede establecer una Política de Seguridad, para la protección del tráfico, (Lopez, 2007).

2.10. Componentes IPSec

Esta suite de protocolos trabajan como un engranaje bajo el mismo modelo de seguridad, cada uno de ellos cumpliendo una funciona especifica dentro de IPSec; estos los componentes son: SA – Asociación de Seguridad, HA – Cabecera de Autenticación, ESP – Cabecera de Seguridad Encapsulada, IKE – Protocolo de Intercambio de Calves en Internet, y por ultimo esta ISAKMP – Protocolo de Gestión

de Calves y Asociación de Seguridad en Internet, a continuación una descripción y funcionamiento de cada uno.

2.10.1. Asociación de Seguridad (SA)

Las asociaciones de seguridad especifican los parámetros a negociar en cada trayectoria segura del Protocolo IP, en la cual a cada trayectoria o enlace le corresponde una única SA, esta protección es en una sola dirección (para un solo host o para un grupo multidifusión), de modo que para poder establecer una comunicación entre dos canales es necesario dos SA para proteger el tráfico de datos en ambos sentidos.

Las SA están compuestas por tres elementos: el protocolo de seguridad, la dirección de destino y el índice de parámetros de seguridad.

- **Protocolo de seguridad.** Comprende: la Cabecera de Autenticación y la Cabecera de Seguridad Encapsulada.
- **Dirección de destino.** La dirección IP de destino con la cual se establecerá la otra SA
- **Índice de parámetros de seguridad.** El SPI es un valor de 32 bits, que genera el número de secuencia de transmisión en las cabeceras. (ORACLE, 2012)

2.10.2. Cabecera de Autentificación (HA)

El protocolo HA - Cabecera de Autenticación proporciona los servicios de autenticación en IPSec, permitiendo que el destinatario del mensaje verifique la autenticidad del remitente, es decir “que sea quien dice ser”, con lo cual se pretende que los participantes tengan la seguridad de que los datos sean correctos y que no haya sufrido algún tipo de corrupción, como, por ejemplo, con un ataque de hombre en el medio, en el cual existe un interceptor en la comunicación.

Este protocolo puede ser utilizado solo o en ayuda del protocolo ESP, con la observación de al trabajar de forma independiente los datos viajan en texto plano (no cifrado), haciéndolo poco eficaz.

2.10.3. Cabecera de Seguridad Encapsulada (ESP)

La Cabecera de Seguridad Encapsulada, proporciona los criterios de autenticación y confidencialidad de los datos cifrando al paquete IP. ESP y AH son protocolos no muy diferentes, ya que ambos trabajan como cabeceras dentro del protocolo de seguridad IPSec, estos pueden ser implementados conjuntamente para hacer un hardening de seguridad otorgando autenticación y privacidad.

Estructura ESP

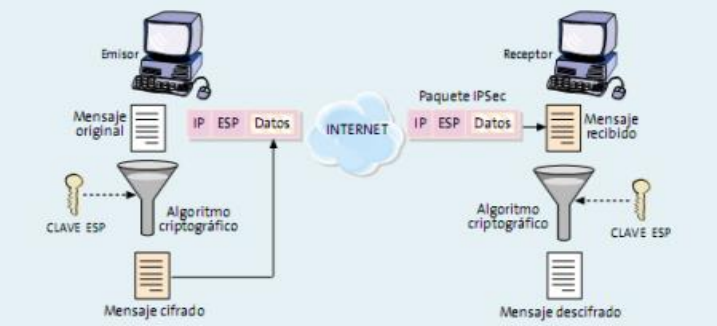


Figura 21. Cabecera de Seguridad Encapsulada
Fuente: (Telefónica , s.f.)

Como se pude apreciar en la ilustración anterior, ESP permite que el tráfico viaje de forma confidencial, en el proceso el emisor cifra el mensaje original, utiliza una clave determinada y lo adjunta al paquete IP (a continuación de la Cabecera de Autenticación ESP); cuando el destinatario recibe el paquete IP utiliza un algoritmo con la misma clave del remitente accediendo de esta forma a los datos, este protocolo es bastante seguro y robusto ya que la clave para acceder a los datos únicamente es conocida por el remitente y destinatario, (Vazquez Clavijo, 2011) .

2.10.4. Protocolo de Intercambio de Claves en Internet (IKE)

El Protocolo de intercambio de Claves - IKE o Internet Key Exchange, por sus siglas en inglés; establece un vínculo cifrado en los dos nodos (origen y destino), en ese punto se negocian las Asociaciones de Seguridad (SA), empleando algoritmos de cifrado y encriptación en ambos extremos de la conexión.

Para este proceso, IKE utiliza algoritmos de encriptación como Hash o MD5; estos algoritmos que trabajan mediante el cálculo de una fórmula llamada hash o resumen, ya que esta basados en la información de los datos de entrada y una clave; que intercambian las claves entre los nodos, quedando así el remitente y destinatario involucrados en todo el proceso de autenticación y cifrado, (López Logacho, 2014).

2.10.5. Protocolo de Gestión de Claves y Asociación de Seguridad en Internet (ISAKMP)

Finalmente, el protocolo ISAKMP, define los pasos a seguir para el establecimiento de las Asociaciones de Seguridad (SA), así como la administración de claves utilizadas en una conexión TCP (orientada a conexión), dando como resultado que el paquete sea sometido a procesos de negociación, modificación e incluso eliminación de las SA, con la finalidad de generar las claves de autenticación entre los hosts participantes. (López Logacho, 2014).

CAPÍTULO 3

3. PROPUESTA DE IMPLEMENTACIÓN

3.1 Políticas de seguridad

3.1.1 Introducción

Todas las organizaciones en la actualidad manejan información sensible y que representa su activo más importante, es por este motivo que la seguridad informática es un aspecto bastante importante que considerar dentro del ámbito empresarial. Para cumplir con este propósito, la organización debe centrar la mayor parte de sus esfuerzos en generar, implementar y mantener mecanismos que permitan que la información y todos sus recursos valiosos permanezcan seguros.

En el caso de un ISP la información es el activo más importante que posee. Esta información es la que el usuario final envía y es trasportada a través de la red del ISP, de aquí nace la necesidad de implementar acciones que protejan tanto los recursos físicos y lógicos que hacen posible la transmisión de datos, como la información en sí.

Las reglas de seguridad (políticas) que se establecen dentro de la organización, básicamente son la agrupación de objetivos, mecanismos y metodologías que se llevaran a cabo para generar un ambiente seguro dentro del ISP. Es necesario mencionar que esta agrupación, no solo rige a los clientes o usuarios, también incluye a toda la infraestructura de red con la que cuenta la organización. En las políticas se establece lineamientos de utilización, acceso, reproducción y demás consideraciones que sean necesarias o indispensables para la organización.

Formalmente, las políticas de seguridad son un artefacto legal donde se establecen reglas que pretenden asegurar y garantizar las características esenciales de la información.

3.1.2 Características de las políticas de seguridad

Es un concepto erróneo pensar que las políticas de seguridad son estáticas y que solo se crean una vez. Las políticas de seguridad son un documento que va sufriendo cambios de acuerdo a la evolución organizacional que tiene el ISP. Existen diferentes aspectos por los cuales una política de seguridad debe ser actualizada, por ejemplo, la adquisición de nuevos recursos tecnológicos, un nuevo modelo de negocio, entrada y salida de personal, desarrollo de nuevos sistemas, implementación de nuevos servicios, etc.

Para que la política de seguridad sea correctamente implementada, se deben tener en cuenta varios aspectos, a continuación, se listan los elementos que son necesarios a considerar dentro de la elaboración de una bien estructurada política de seguridad.

- Identificar y considerar los activos más importantes para la organización.
- Delimitar el alcance y competencias que va a poseer la política de seguridad (Sistemas, servicios, procedimientos, recursos, etc.)
- Definir responsabilidades para los diferentes entes que interactúan con la información y los recursos tecnológicos.
- Definir claramente cuáles van a ser los objetivos que busca cumplir la política de seguridad.
- Establecer reglas, que describan los requerimientos técnicos en cuanto y a seguridad se refiere, analizando todas las situaciones de riesgo que se puedan presentar.
- Considerar el modelo organizacional de la compañía y definir órganos encargados de gestionar y administrar el establecimiento y operación de las reglas de seguridad.

- Tomar en cuanta como principal actor al usuario interno de la compañía, puesto que en base a esta entidad se establecerán varias estrategias de seguridad.
- Definir las acciones permitidas dentro de la organización y establecer sanciones para quienes no las cumplan.
- Establecer mecanismos de seguridad que se ajusten con normas y estándares que estrictamente deba cumplir la organización (Normas Gubernamentales).

Además de los elementas a considerar, las políticas de seguridad se deben basar en parámetros para establecer su alcance y delinear su modo de funcionamiento, a continuación, se exponen los principales parámetros que se deben tomar en cuenta.

- Identificar los riesgos que actualmente tiene la organización, para establecer una política de seguridad adecuada.
- Mantener entrevistas con los principales actores dentro del funcionamiento de los recursos informáticos (administradores de red, desarrolladores) para establecer el alcance de las políticas y establecer sanciones.
- Socializar las políticas de seguridad desarrolladas e implementadas con todos los miembros de la organización.
- Delegar responsabilidades a ciertos profesionales, para que esta persona se encargue de la seguridad del segmento que se le será asignado.
- Monitorear y analizar la aplicación de las normas de seguridad establecidas con el fin de identificar si los objetivos de estas se están cumpliendo.
- Describir de forma clara y precisa el alcance de las políticas, para que todos los usuarios pueden comprenderlas.
- Establecer políticas de seguridad basándose en estándares internacionales que se ajusten a los requerimientos y necesidades de la organización.

3.2.3 Generalidades de las políticas de seguridad

Las políticas de seguridad se establecen y se definen para crear posturas con respecto a lo que esta explícitamente permitido y a lo que no. Generalmente la definición de este tipo de reglas se las hace en dos grupos, las políticas de seguridad permisivas y las prohibitivas.

Las **políticas permisivas**, centran su concepto en permitir todo lo que no está explícitamente prohibido. Mientras que las **políticas prohibitivas** dicen que todo está prohibido excepto lo que esta explícitamente permitido. En base a estas definiciones y tomando en cuenta las buenas prácticas de seguridad informática, se puede decir que la mejor opción para establecer políticas de seguridad es implementar políticas prohibitivas, ya que de esta manera se estará permitiendo únicamente lo necesario y no se estará corriendo riesgos innecesarios.

El objetivo principal de la generación de políticas de seguridad es fortalecer la seguridad de la organización. A continuación, se muestran los aspectos más comunes que suene cubrir las políticas de seguridad.

- De acceso
- De seguridad física
- De backups
- De contingencia
- De almacenamiento
- De cuentas de usuario
- De seguridad lógica
- De uso de la infraestructura
- De extracción de información
- De procedimientos

Es recomendable que aparte de generar políticas de seguridad bien estructuradas, se establece y defina un plan de contingencia. En todo proceso de seguridad informática el plan de contingencia resulta siendo parte fundamental del mismo, ya que, frente a algún incidente de seguridad, este plan presenta medidas y acciones a tomar durante y

después del incidente de seguridad. Si se cuenta con un plan de contingencia, se pueden evitar pérdidas importantes para la organización en cuento a presupuesto económico y disponibilidad de recursos, servicios y aplicaciones.

3.2.4 Ciclo de vida de las políticas de seguridad

Como ya se ha mencionado las políticas no son un producto estático, sino que más bien responden al concepto de proceso en el cual se distinguen varias etapas por las cuales cruza una política de seguridad. El ciclo de vida de las políticas de seguridad generalmente consta de 4 etapas.

1. Definición
2. Implementación
3. Verificación
4. Renovación o Revocación.

La definición de la política de seguridad tiene lugar al inicio del proceso y es donde se establecen varias reglas para reforzar algún aspecto de la organización**. La implementación de la política de seguridad** es desarrollar formalmente un documento y empezar a poner en prácticas las reglas definidas en la etapa número uno. Después de que las reglas ya están en funcionamiento, **la verificación** de las mismas significa realizar estudios para determinar si los objetivos que buscan cumplir las políticas se están cumpliendo. La última etapa por la cual atraviesa una política de seguridad es la **revocación o renovación.** En esta etapa se analizan los resultados de la etapa anterior y se determinar si la política llego a su fin, o si se puede modificar para conseguir cubrir más o nuevos requisitos de seguridad.

3.2 Estándar ISO 27001

3.2.1 Aspectos básicos

La norma ISO/IEC 27001, es una agrupación de estándares, fue normalizada y publicada por la Organización Internacional de Normalización conjuntamente con la

Comisión Electrotécnica Internacional. Esta norma específica cómo manejar y gestionar la seguridad de la información dentro de una organización sin importar de qué tipo sea esta y tampoco el modelo de negocio. Este estándar fue publicado por primera vez en el año 2005, estuvo basado en el estándar británico BS 7799-2 y en al año 2013 tuvo una revisión que se conoce como la norma ISO/IEC 27001:2013, esta versión de la norma es una actualización y mejora de la primera que fue publicada en el año 2005.

La implementación de esta norma dentro de una organización trae consigo algunas ventajas competitivas. Una gran ventaja es que, si se cumple todas las reglas que implica la correcta utilización de esta norma, la organización puede certificarse a nivel mundial.

3.2.2 Estructura de la norma ISO/IEC 27001

La estructura de la norma ISO/IEC 27001 consiste en 11 secciones que determinan como se debe manejar y administrar la seguridad informática dentro de la organización.

Como se puede apreciar en la tabla No. 6, la norma ISO/IEC 27001:2013 presenta algunos cambios respecto a la versión diseñada en el 2005. A continuación de explicaran cada una de las secciones con las que cuenta la norma actualizada (ISO/IEC 27001:2013).

0. Introducción – Explica los objetivos que busca alcanzar la norma ISO/EIC 27001.

1. Alcance – Este apartado describe cual es la cobertura de la norma. Explica claramente que este estándar puede implementarse en cualquier organización.

2. Referencias Normativas – Cita la norma ISP/IEC 27000 que es donde se generan estándares o reglas que pueden ser aplicadas en esta norma (ISO/IEC 27001:2013).

3. Términos y Definiciones - Cita la norma ISP/IEC 27000 que es donde se generan términos y definiciones que pueden ser aplicadas en esta norma (ISO/IEC 27001:2013).

4. Contexto de la Organización – En esta sección se establecen las necesidades y requerimientos que posee la organización para después establecer el alcance del SGSI.

5. Liderazgo – Esta sección se enfoca en la designación de responsabilidades que tendrá cada elemento de la seguridad informática en la empresa. También menciona a la alta dirección de la compañía y que rol es el que va a desempeñar para implementar las políticas de seguridad.

6. Planificación – Esta sección se encarga de definir la manera en cómo la organización va a actuar para solventar los problemas de seguridad.

7. Soporte – Esta sección se encargada de definir los recursos que necesita el SGSI para cumplir con la norma. Se contemplan disponibilidad de recursos, control de documentos, gestión y administración de registros.

8. Operación – Define la planificación, implementación y monitoreo de todos los mecanismos implementados para satisfacer las necesidades de la compañía en cuanto a seguridad. Estos mecanismos son definidos y establecidos en el SGSI.

9. Evaluación de Desempeño – En esta sección se establecer mecanismos para el control y monitoreo de los procesos de seguridad, medición, análisis, auditorías internas, evaluación, son algunos de las acciones utilizadas.

10. Mejora – Después de la evaluación de desempeño se obtienen resultados, los cuales son analizados y se extrae de ellos las mejoras que se necesitan implementar en los mecanismos de seguridad, a este proceso se lo denomina actualización de procesos.

Anexo A – Esta sección proporciona un listado de 114 controles de seguridad.

Tabla 6. Evolución de la norma ISO/IEC 27001

ISO/IEC 27001:2005	1. Alcance
	2. Referencias normativas
	3. Términos y definiciones
	4. Sistema de Gestión de Seguridad de la información
	5. Responsabilidad de la Gerencia
	6. Auditorías internas SGSI
	7. Revisión General del SGSI
	8. Mejoramiento del SGSI
	Anexo A - Anexo B - Anexo C
ISO/IEC 27001:2013	1. Alcance
	2. Referencias normativas
	3. Términos y definiciones
	4. Contexto de la Organización
	5. Liderazgo
	6. Planificación
	7. Soporte
	8. Operación
	9. Evaluación del Desempeño
	10. Mejora
	Anexo A

Nota: Actualizaciones de la norma ISO/IEC 27001
Fuente: (ISO/IEC 27001:2005; ISO/IEC 27001:2013, 2013)

3.3 Políticas de seguridad para un ISP

3.3.1 Propuesta

De acuerdo a todos los requerimientos y necesidades de seguridad con las que cuenta un ISP de nivel tres, se detalla un modelo de propuesta de seguridad que está basado en la norma ISO/IEC 27001:2013.

3.3.1.1 Objetivos generales del ISP

- Garantizar las características básicas que posee la información que se maneja dentro de la organización.
- Generar procedimientos de seguridad de calidad, a través de metodologías bien estructuradas y detalladas. De tal modo que los empleados se comprometan con garantizar el principio de seguridad.

- Minimizar considerablemente los niveles de riesgo en la organización mediante la utilización de análisis de vulnerabilidades y mitigación de riesgos.
- Garantizar que todos los servicios que se ofertan en el ISP se mantengan en funcionamiento ante cualquier incidencia de seguridad. Esto se logra con el establecimiento de un plan de contingencia bien estructurado y definido.

3.3.1.2 Objetivos generales del SGSI

Una vez definidos los objetivos instituciones, es momento de definir los objetivos que buscara cumplir el SGSI. Es necesario mencionar que los objetivos tanto institucionales como los del SGSI deben estar alineados.

- Proteger el activo más importante para el ISP (la información), mediante la aplicación de mecanismos de seguridad.
- Fortalecer procesos y procedimientos ya existentes en la organización mediante la estructuración de políticas de seguridad.
- Capacitar a todos los colaboradores del ISP con la finalidad de generar conciencia con respecto a eventos relacionados con la seguridad de la red, los cuales pueden ser evitados.
- Proteger de manera integral el activo más importante que tiene un ISP (información.)

3.3.1.3 Alcance del SGSI

Generar un ambiente de seguridad dentro del ISP, tanto fisco como lógico, el cual involucre a todos los elementos que interactúan en la red de la organización, especialmente el canal de comunicación por el cual transita la información del cliente final.

Proteger el segmento perimetral de la red de la organización, mediante la utilización de protocolos de red, los cuales garanticen el correcto desempeño de esta parte de la red. Implementar mecanismos de control para administrar y gestionar los RR.HH. del ISP.

Generar y establecer mecanismos o reglas de seguridad que se preocupen de la seguridad de la organización de manera integral, desde el almacenamiento de datos en dispositivos extraíbles, hasta la generación de procedimientos que se encarguen de proteger la información manejada en el ISP.

3.3.1.4 Fases de la implementación del SGSI

Fase 1: Situación Actual: Descripción de la situación inicial en la que se encuentra la organización a través de la norma ISO/IEC 270001:2013.

Fase 2: Sistema de Gestión Documental: En esta fase la organización se encarga de satisfacer todos los recursos documentales que requiere la norma ISO/IEC 27001:2013.

Fase 3: Análisis de Riesgos: Identificar cueles son los activos de la organización que están expuestos a riesgos y son vulnerables a ataques. Determinar el nivel de riesgo que estas amenazas representan ara la organización.

Fase 4: Propuestas de Proyectos: Elaborar modelos de implementación, donde se consideren y se estables los responsables de ejecutar este proceso, además se debe considerar los recursos económicos que se tiene para alcanzar el objetivo del SGSI (seguridad informática integral).

Fase 5: Auditoria de Cumplimento: Realizar análisis que permitan conocer si las normas y reglas establecidas en el SGSI se cumplir y como estas beneficiaron a la organización.

3.3.2 Metodología de implementación

Para tomar como válida y funcional una metodología de seguridad, se debe consideras las buenas prácticas que han sido documentadas. De esta manera es como se puede adoptar el ciclo de Deming como una metodología funcional. Esta estrategia basa su funcionamiento en un proceso denominado PDCA por sus siglas en inglés (Plan, Do, Check, Act). Las fases por las que atravieso este ciclo son las siguientes.

Plan: En esta fase se analizan los requerimientos iniciales de la organización, se conoce su estructura organizacional y se establece una planificación general de cómo proceder.

Do: Se establecen y generan los procedimientos de seguridad que posteriormente serán implementados para minimizar las amenazas con las que cuenta un ISP.

Check: Después de implementar ciertos mecanismos de seguridad es indispensable monitorear su desempeño para determinar si se están cumpliendo los requisitos establecidos. Generalmente esta fase debe realizarse por lo menos una vez por año.

Act: Es la fase que esta inmediatamente después de la fase de monitoreo. En base a esta fase previa se obtiene resultados que indican si es que se debe realizar mejorar o actualizaciones de las políticas de seguridad, también una política puede ser modificada de modo preventivo.

3.3.3 Análisis e interpretación de resultados

El análisis de resultados e interpretación es la fase final de la implementación de un SGSI, donde se debe verificar que los objetivos que fueron establecidos al iniciar el proceso se pudieron cumplir. Para verificar esto es necesario considerar dos escenarios, el primer escenario será la situación inicial en la que se encontraba la organización y el segundo será la auditoria de cumplimiento. Se recomienda comparar

los dos escenarios porque así se podrá identificar claramente cueles fueron las mejoras y nuevos procesos que se implementaron.

3.3.4 Auditoria de cumplimiento

Cuando se implementa un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001, se establecen diversos requisitos que se deben cumplir obligatoriamente. Uno de estos requisitos es la realización de auditorías de cumplimiento o auditorías internas como también se conocen, esto con el fin de controlar el cumplimiento de los requisitos que se establecieron en la fase de situación inicial del SGSI. Esta técnica de control también sirve para evaluar y analizar la consistencia de los sistemas que posea la organización. Es importante realizar auditorías internas, ya que, para la certificación de la norma, se realizarán auditorías externas y para esa ocasión todos los requisitos de seguridad deben estar cubiertos. A continuación, se describen algunas características de este proceso.

- Este proceso busca identificar y corregir algún problema antes de que tenga lugar la auditoria de certificación.
- Proporciona una visión general de cuáles son los aspectos de seguridad en los cuales se puede mejorar.
- Se recomienda realizar auditorías internas de manera regular y no solo al finalizar el proceso de implementación del SGSI, esto servirá para encontrar oportunidades de mejora tempranamente y no esperar al fin del proceso para identificarlas y corregirlas.

Dentro de la realización de una auditoria interna se establecen ciertos procesos se deben cumplir. A continuación, se listan las etapas más importantes de este procedimiento.

1. Documentación existente.
2. Planificación de la auditoria
3. Realización de la auditoria
4. Emisión del informe de la auditoria

3.3.5 Buenas prácticas de seguridad en servidores

- Mantener actualizadas las versiones del software de los servidores.
- Identificar cuáles son los procesos habilitados para correr en los servidores, de esta manera se puede evitar que servicios desconocidos actúen sobre ellos.
- Establecer un área adecuada para el funcionamiento de los servidores. Se recomienda la creación de un Data Center que cumpla normas internacionales.
- Seguridad física y acceso autorizado para ingresar al área donde se ubican los servidores.
- Administrar y verificar los puertos abiertos en cada servidor, para evitar instrucciones indebidas.
- Evitar la habilitación de usuarios remotos que posean privilegios de administradores.
- Dar mantenimiento preventivo periódico a los servidores para evitar fallas inesperadas.

CAPÍTULO 4

4. IMPLEMENTACIÓN Y PRUEBAS

El presente capitulo tiene como objetivo principal demostrar la viabilidad de la implementación del protocolo de seguridad IPSec sobre una simulación de red estructurada bajo direccionamiento IPv6. Para esto, se consideran diferentes aspectos como la herramienta de simulación a utilizar, criterios de diseño de red, la creación de diferentes escenarios de pruebas, recolección de datos estadísticos y el análisis de los resultados obtenidos.

4.1 Simulación de Red

Para comprobar la validez de la propuesta desarrollada en este documento, es indispensable simular, tanto el funcionamiento como la estructura de la red de un proveedor de servicios de Internet. Dentro de este prototipo (simulación), se toma en cuanta principalmente la arquitectura que posee un ISP, aplicando los criterios de diseño que han sido expuestos en capítulos anteriores, además se debe considerar y analizar los protocolos y servicios que se configuraran en el entorno de red. Para llevar a cabo este procedimiento, es necesario definir que herramienta de simulación se puede utilizar.

4.1.1 Aspectos a considerar

Herramienta de Simulación

El punto de partida es elegir adecuadamente la herramienta de simulación a utilizar. En este caso se ha decidido utilizar Riverber Modeler Academic Edition, ya que es un simulador basado en eventos discretos (DES) el cual permite recolectar estadísticas generales/especificas acerca del funcionamiento de la red y el comportamiento de ciertos protocolos. Es necesario mencionar que la versión académica de este simulador

solo permite simular un número determinado de eventos, es por esto que el diseño de red considera este aspecto al momento de configurar protocolos y servicios.

Diseño de la topología de red

El diseño de la topología de red del ISP se basa en los criterios arquitectónicos y estructurales descritos en el primer capítulo de este documento. Básicamente la arquitectura red de un ISP está compuesta por diferentes tipos de red, por lo cual se puede decir que su topología es hibrida. Esta red está formada por una red de tipo anillo en su núcleo y una red de tipo malla en el segmento de concentración, además en el segmento de acceso se pueden implementar diferentes tecnologías de acceso y servicios de última milla.

4.1.1.1 Diseño topológico de la Red

Simulación de Red

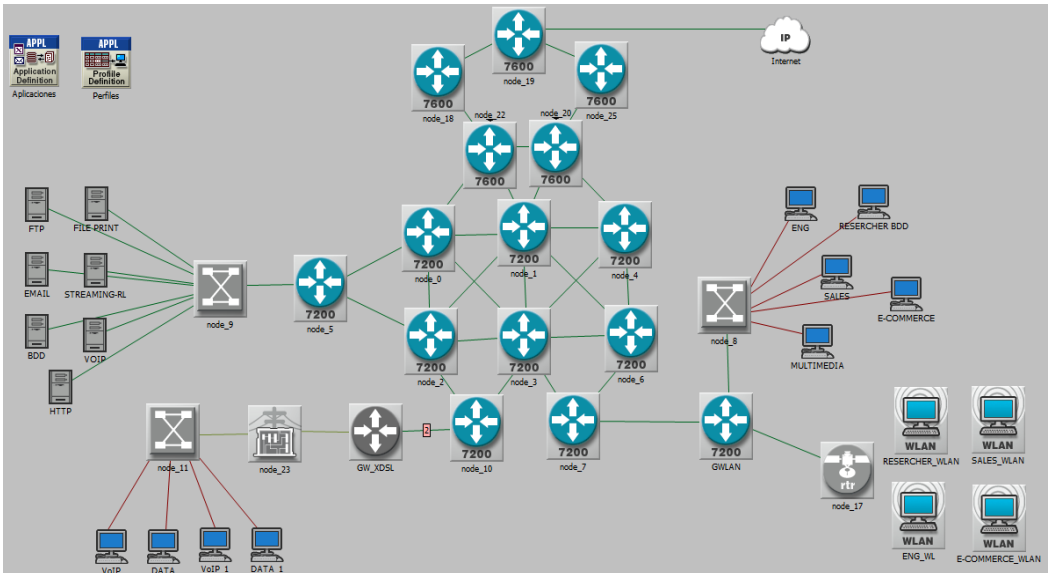


Figura 22. Topología de red de un ISP de nivel 3
Elaborado por: Marcela Gallegos e Ismael Román.

Como se aprecia en la figura No. 22, la topología de red que se utilizará en la simulación, ha sido estructurada bajo criterios de diseño explicados en capítulos pasados. Además de estar compuesta por distintos tipos de red (anillo y malla), esta

topología, posee diferentes segmentos. El **segmento de acceso** brinda acceso a diferentes equipos terminales a través de tecnologías vanguardistas, en este caso se está simulando el acceso mediante tecnologías xDSL y FTTx. **La red de concentración** se encarga de conmutar los paquetes provenientes de los usuarios hacia la red troncal, en este caso los routers de concentración, además de conmutar paquetes, se utilizan interconectar a un PoP que es donde se encuentra la granja de servidores. **La red troncal** está compuesta por una red de tipo anillo cuya función es conmutar los paquetes de manera veloz hacia el backbone de Internet. El acceso a la red de Internet en el territorio nacional se lo consigue mediante NAP.EC (Network Access Point Ecuador) tal como se lo ha explicado en el Capítulo 1.

4.1.1.2 Infraestructura de Red

Enrutadores

Los routers que se ocupan en la simulación, se ajustan a las necesidades de un proveedor de servicios. En las siguientes tablas se detallan sus principales características.

Tabla 7. Router Cisco 7600 Series

Router Cisco 7600 Series
• Módulos de servicios Ethernet de alta densidad: 10/100 Mbps, Gigabit Ethernet y 10 Gigabit Ethernet • Módulos de servicios: seguridad IP (IPSec), cortafuegos, denegación de servicio distribuida, sistemas de detección de intrusos, análisis de red. • Módulo FlexWAN mejorado: compatible con los adaptadores de puerto WAN Cisco 7200 y 7500 de DS-0 a OC-3 para interfaces canalizadas y ATM y también adaptadores de puerto Fast Ethernet.

Nota: Características generales del Router Cisco 7600 Series. Fuente: (CISCO, 2006).

Tabla 8. Router Cisco 7200 Series

Router Cisco 7200 Series
• Agregación de banda ancha: hasta 16,000 sesiones de punto a punto por chasis. • VPN de seguridad IP (IPSec VPN): disponible para 5.000 túneles por chasis. • Integración de voz, video, datos: multiplexor por división de tiempo (TDM), chasis VXR habilitado y adaptadores de puerto de voz.

Nota: Características generales y más destacadas del Router Cisco 7200 Series. Fuente: (CISCO, 2006).

Enlaces

Los enlaces que se utilizaron en la simulación corresponden a los enlaces físicos que se utilizan en una red jerárquica de un ISP de nivel 3. Básicamente los enlaces utilizados son, enlaces de fibra óptica para interconectar los routers de los distintos segmentos de la red, enlaces ethernet 100BaseT para interconectar las estaciones de trabajo y equipos finales y enlaces ATM para dar acceso a los usuarios finales a través de la tecnología XDSL.

Tecnologías/Servicios de Acceso

Las tecnologías de acceso y los servicios de última milla que han sido configurados en la simulación son xDSL, FTTx mediante acceso inalámbrico (WLAN) y acceso móvil mediante GSM. Se ha decidido configurar estos servicios, ya que son los más representativos y utilizados en la actualidad a nivel nacional.

Servicios de Red

El diseño, contempla los servicios más representativos que el proveedor de servicios de Internet puede ofrecer. Entre estos están: FTP, E-MAIL, BDD, VoIP, HTTP, STREAMING y FILE PRINT.

4.2 Pruebas realizadas

Una vez realizada la explicación de la topología, enlaces y servicios implementados, se procede a realizar el escenario de pruebas, en el cual se capturan datos estadísticos y gráficas, para realizar un análisis comparativo entre las topologías implementadas.

4.2.1 Escenario de Pruebas

Para el escenario de pruebas se creó dos topologías idénticas, la primera “Escenario A” y la segunda “Escenario B”; es en esta última que se implementó el protocolo de seguridad IPSec. Para realizar el análisis ente ambas, se procedió a tomar datos estadísticos de parámetros de la red, como son: Throughput o rendimiento de la red,

Data Dropped o datos descartados - eliminados o perdidos, y servicios; con esto, analizar el comportamiento de la red frente a la configuración del protocolo.

A continuación, se presenta las gráficas y datos estadísticos tomados las topologías (por separado), en base a los parámetros mencionados anteriormente; para lo cual se estableció un tiempo de 2 horas (de simulación), puesto que en ese lapso de tiempo se producen la suficiente cantidad de eventos y paquetes globales (toda la simulación) y de nodo (módulos) para proceder con el respectivo análisis.

4.2.1.1 Escenario A (Sin IPSec)

En el primer escenario de red, no se configuro IPSec, razón por la cual no existe afección al rendimiento de la misma, o al paso de paquetes desde un nodo origen a un nodo destino, lo cual puede ser comprobado y verificado en base a las capturas realizadas con la herramienta de simulación Riverber Modeler.

Throughput

El rendimiento de la red o Throughput puede ser observado en la figura No. 23.

Datos Estadísticos - Throughput

```
-------------------------------------------------
zone               : 0
statistic          : 'Simulacion_ISP_IPSEC-SERVICES_NO_IPSEC-DES-1: Wireless LAN.Throughput (bits/sec)'
length             : 101
number of values   : 101
horizontal, min    : 0
            max    : 7200
vertical,   min    : 663.111111111
            max    : 132,591.509803922
initial value      : 663.111111111
final value        : 109,527.643333333
expected value     : 114,367.607254581
sample mean        : 114,367.607254581
```

Figura 23. Throughput Escenario A
Elaborado por: Marcela Gallegos e Ismael Román.

Los parámetros relevantes que se contemplan a continuación en la tabla No. 9, hacen referencia a los datos estadísticos capturados de Throughput del Escenario A, como son el tiempo de ejecución (medida en segundos), así como, los valores máximos y mínimos que alcanza la simulación en cuanto a rendimiento.

Tabla 9. Inicio - Throughput - Escenario A

Eje	Parámetro	Valor	Descripción
Horizontal	Min	0	Tiempo en el cual empezó a correr la simulación (segundos).
	Max	7200	Tiempo en el cual finalizó la simulación (segundos).
Vertical	Min	663.111111111	Valor inicial del rendimiento de la red (bits).
	Max	132,591.509803922	Valor máximo que alcanza el rendimiento de la red (bits).

Nota: Datos estadísticos de inicio correspondientes al Throughput del Escenario A.
Elaborado por: Marcela Gallegos e Ismael Román

En la tabla No. 10, se especifican los valores arrojados por la simulación, en los cuales se puede observar la longitud del paquete, el valor inicial en el cual empieza la ejecución de la simulación, el valor final y valor esperado son parámetros que arrojan los resultados de rendimiento de la red.

Tabla 10. Fin - Throughput - Escenario A

Parámetro	Valor	Descripción
Longitud	101	Total de eventos capturados por la simulación
Valor Inicial	663.111111111	Valor con la cual empieza la simulación (bits).
Valor Final	109,527.643333333	Valor con la cual termina la simulación (bits), este es el punto más alto que alcanza la simulación.
Valor Esperado	114,367.607254581	Valor esperado en la ejecución de la simulación (bits).

Nota: Datos estadísticos de finalización correspondientes al Throughput del Escenario A.
Elaborado por: Marcela Gallegos e Ismael Román

Para una mejor apreciación de los parámetros anteriores, se obtiene la gráfica generada desde la herramienta de simulación en la figura No. 24, la cual representa el rendimiento del escenario de red, sin la implementación del protocolo IPSec.

Gráfica Throughput

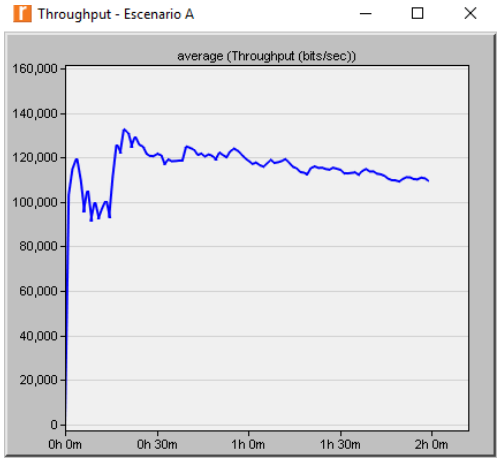


Figura 24. Grafica Throughput – Escenario A
Elaborado por: Marcela Gallegos e Ismael Román.

Data Dropped

Data Dropped o datos descartados, son capturados para medir la cantidad de paquetes perdidos o abandonados, esto ocurre cuando: un paquete o su contenido esta corrupto o cuando no cumple con las políticas de seguridad establecidas. Para lo cual se puede observar en la figura No. 25, los datos estadísticos obtenidos, con su correspondiente explicación más adelante.

Datos Estadísticos – Data Dropped

```
-------------------------------------------------
zone                : 0
statistic           : 'Simulacion_ISP_IPSEC-SERVICES_NO_IPSEC-DES-1: Wireless LAN.Data Dropped (Buffer Overflow) (bits/sec)
length              : 101
number of values    : 101
horizontal, min     : 0
            max     : 7200
vertical,   min     : 0.0
            max     : 5,264.62745098
initial value       : 0.0
final value         : 4,422.38666667
expected value      : 4,559.16757233
sample mean         : 4,559.16757233
```

Figura 25. Data Dropped - Escenario A
Elaborado por: Marcela Gallegos e Ismael Román.

Los parámetros relevantes que se contemplan a continuación en la tabla No. 11, hacen referencia a los datos estadísticos capturados de Data Dropped del Escenario A, como son el tiempo de ejecución (medida en segundos), así como los valores máximos y mininos de perdida de paquetes.

Tabla 11. Inicio - Data Dropped - Escenario A

Eje	Parámetro	Valor	Descripción
Horizontal	Min	0	Tiempo en el cual empezó a correr la simulación (segundos).
	Max	7200	Tiempo en el cual finalizó la simulación (segundos).
Vertical	Min	663.111111111	Valor al iniciar la simulación (bits).
	Max	5,264.62745098	Valor máximo de bits que se pueden perder en la simulación, para que esta no se cierre abruptamente (bits).

Nota: Datos estadísticos de inicio correspondientes a Dropped del Escenario A.
Elaborado por: Marcela Gallegos e Ismael Román

En la tabla No. 12, se especifican los valores arrojados por la simulación, en los cuales se puede observar la longitud del paquete, el valor inicial de la cantidad de datos descartados, (al empezar la simulación es 0), el valor final y valor esperado son parámetros que definen la cantidad de datos descartados en la topología de red.

Tabla 12. Fin – Data Dropped- Escenario A

Parámetro	Valor	Descripción
Longitud	101	Total de eventos capturados por la simulación
Valor Inicial	0	Cantidad de datos perdidos al iniciar la simulación (bits).
Valor Final	4,422.38666667	Cantidad de datos perdidos al finalizar la simulación (bits).
Valor Esperado	4,559.16757233	Cantidad esperada de datos perdidos al finalizar la simulación (bits).

Nota: Datos estadísticos de finalización correspondientes a data Dropped del Escenario A.
Elaborado por: Marcela Gallegos e Ismael Román

Para una mejor apreciación de los parámetros anteriores, se obtiene la gráfica generada desde la herramienta de simulación en la figura No. 26, la cual representa los paquetes perdidos o descartados del escenario de red, sin la implementación del protocolo IPSec.

Grafica Data Dropped

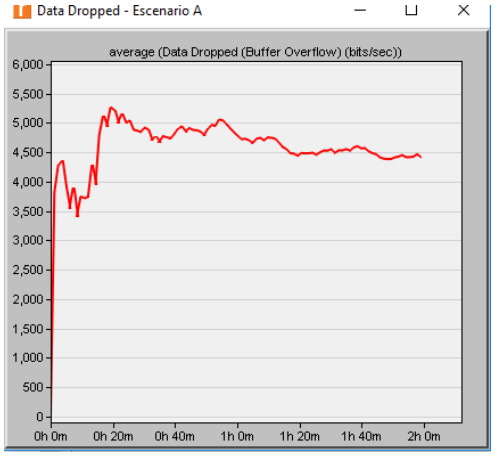


Figura 26. Grafica Data Dropped – Escenario A
Elaborado por: Marcela Gallegos e Ismael Román.

4.2.1.2 Escenario B (Con IPSec)

En el segundo escenario de red se configuro IPSec, por consiguiente, existe afección al rendimiento de la misma y al paso de paquetes desde un nodo origen a un nodo destino, ya que con la implementación de IPSec se crean túneles para el asegurar el transporte de los datos; lo cual puede ser comprobado y verificado en base a las capturas realizadas con la herramienta de simulación Riverber Modeler.

Throughput

El rendimiento de la red con la implementación de IPSec, se observa a continuación.

Datos Estadísticos - Throughput

```
-------------------------------------------------
zone                : 0
statistic           : 'Simulacion_ISP_IPSEC-SERVICES_IPSEC-DES-1: Wireless LAN.Throughput (bits/sec)'
length              : 101
number of values    : 101
horizontal, min     : 0
            max     : 7200
vertical,   min     : 663.111111111
            max     : 76,298.5092593
initial value       : 663.111111111
final value         : 62,279.9455556
expected value      : 59,965.1921565
sample mean         : 59,965.1921565
```

Figura 27. Throughput Escenario B
Elaborado por: Marcela Gallegos e Ismael Román.

Los parámetros relevantes que se contemplan a continuación en la tabla No. 13, hacen referencia a los datos estadísticos capturados de Throughput del Escenario B, como son el tiempo de ejecución (medida en segundos), así como, los valores máximos y mínimos que alcanza la simulación en cuanto a rendimiento.

Tabla 13. Inicio - Throughput - Escenario B - IPSec

Eje	Parámetro	Valor	Descripción
Horizontal	Min	0	Tiempo en el cual empezó a correr la simulación (segundos)
	Max	7200	Tiempo en el cual finalizó la simulación (segundos)
Vertical	Min	663.111111111	Valor inicial del rendimiento de la red (bits).
	Max	76,298.5092593	Valor máximo del rendimiento de la red (bits).

Nota: Datos estadísticos de inicio correspondientes al Throughput del Escenario B.
Elaborado por: Marcela Gallegos e Ismael Román

En la tabla No. 14, se especifican los valores arrojados por la simulación, en los cuales se puede observar la longitud del paquete, el valor inicial en el cual empieza la ejecución de la simulación, el valor final y valor esperado son parámetros que arrojan los resultados de rendimiento de la red.

Tabla 14. Fin - Throughput - Escenario B - IPSec

Parámetro	Valor	Descripción
Longitud	101	Total de eventos capturados por la simulación
Valor Inicial	663.111111111	Valor inicial con la cual empieza la simulación (bits).
Valor Final	62,279.9455556	Valor con el cual termina la simulación (bits), este es el punto más alto que alcanza la simulación.
Valor Esperado	59,965.1921565	Valor esperado en la ejecución de la simulación (bits).

Nota: Datos estadísticos de finalización correspondientes al Throughput del Escenario B.
Elaborado por: Marcela Gallegos e Ismael Román

Para una mejor apreciación de los parámetros anteriores, se obtiene la gráfica generada desde la herramienta de simulación en la figura No. 28, la cual representa el rendimiento del escenario de red, con la implementación del protocolo IPSec.

Grafica Throughput

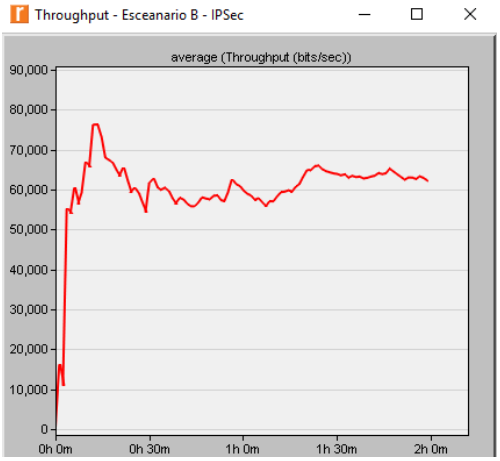


Figura 28. Grafica Throughput – Escenario B
Elaborado por: Marcela Gallegos e Ismael Román.

Data Dropped

Para el Escenario B con la configuración del protocolo de seguridad IPSec los valores se reducen, análisis que se lo realiza más adelante, por lo pronto se puede observar en la figura No. 29, los datos estadísticos obtenidos, con su correspondiente explicación.

Datos Estadísticos – Data Dropped

```
------------------------------------------------
zone                : 0
statistic           : 'Simulacion_ISP_IPSEC-SERVICES_IPSEC-DES-1: Wireless LAN.Data Dropped (Buffer Overflow) (bits/sec)'
length              : 101
number of values    : 101
horizontal, min     : 0
            max     : 7200
vertical,   min     : 0.0
            max     : 2,744.7654321
initial value       : 0.0
final value         : 2,591.37777778
expected value      : 2,341.71606895
sample mean         : 2,341.71606895
```

Figura 29. Data Dropped Escenario B
Elaborado por: Marcela Gallegos e Ismael Román.

Los parámetros relevantes que se contemplan a continuación en la tabla No. 15, hacen referencia a los datos capturados de Data Dropped del Escenario B configurado con IPSec, como son el tiempo de ejecución (medida en segundos), así como los valores máximos y mininos de perdida de paquetes.

Tabla 15. Inicio – Data Dropped - Escenario B - IPSec

Eje	Parámetro	Valor	Descripción
Horizontal	Min	0	Tiempo en el cual empezó a correr la simulación (segundos).
	Max	7200	Tiempo en el cual finalizó la simulación (segundos).

Vertical	Min	0	Cantidad de bits perdidos al iniciar la simulación (bits).
	Max	2.744,7654321	Cantidad máxima de bits que se pueden perder en la simulación, para que esta no se cierre abruptamente (bits).

Nota: Datos estadísticos de inicio correspondientes a data Dropped del Escenario B.
Elaborado por: Marcela Gallegos e Ismael Román

En la tabla No. 16, se especifican los valores arrojados por la simulación, en los cuales se puede observar la longitud del paquete, el valor inicial de la cantidad de datos descartados, (al empezar la simulación es 0), el valor final y valor esperado son parámetros que definen la cantidad de datos descartados o perdidos en la topología de red.

Tabla 16. Fin – Data Dropped- Escenario B - IPSec

Parámetro	Valor	Descripción
Longitud	101	Total de eventos capturados por la simulación
Valor Inicial	0	Cantidad de datos perdidos al iniciar la simulación (bits)
Valor Final	2,591.3777778	Cantidad de datos perdidos al finalizar la simulación (bits)
Valor Esperado	2,341.71606895	Cantidad esperada de datos perdidos al finalizar la simulación (bits)

Nota: Datos estadísticos de finalización correspondientes a data Dropped del Escenario B.
Elaborado por: Marcela Gallegos e Ismael Román

4.3 Análisis de Resultados

El análisis de los resultados comprende dos instancias, en la primera se contempla el análisis de las gráficas del comportamiento de la red y en la segunda los datos estadísticos. La decisión de realizar el análisis en dos módulos surge de la necesidad de poder interpretar las gráficas, que se obtiene desde una herramienta de simulación y realizar un análisis comparativo con los datos estadísticos, para finalmente emitir un juicio acerca del comportamiento de los distintos escenarios de red.

4.3.1 Análisis Gráfico

Lo que a análisis gráfico comprende, se realizó la comparativa del Escenario A y el Escenario B – IPSec, en cuanto a rendimiento de la red y datos perdidos.

En la figura No. 30, se puede apreciar el rendimiento de la red de ambos escenarios de red, la línea de color rojo representa al Escenario A (sin configuración IPSec), mientras que la línea de color azul al Escenario B (configurado con IPSec).

Notablemente el rendimiento del Escenario A (línea roja) es superior con un alcance máximo de alrededor de 132,591 bits/sec, mientras que el Escenario B (línea azul) llega a un máximo de 76,298 bits/sec, es importante recalcar que el tiempo de la simulación para ambos casos es de 2 horas; se debe tener en cuenta que al implementar el protocolo de seguridad IPSec, se realiza el encapsulamiento de los paquetes dos veces, haciendo que estos tengan un mayor tamaño, lo que recae en que se tenga que procesar datos de mayor volumen, degradando el rendimiento de la red.

Comparación Throughput

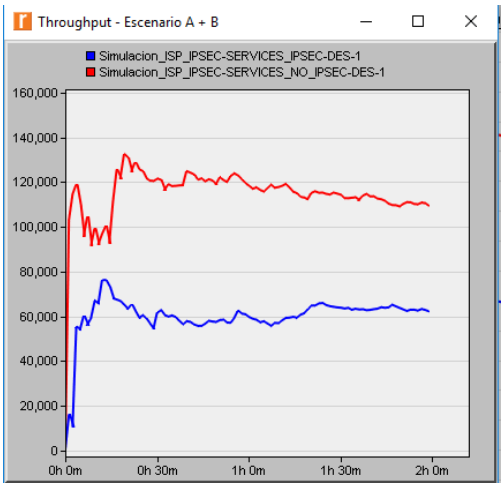


Figura 30. Gráfica Comparativa Throughput
Elaborado por: Marcela Gallegos e Ismael Román.

En el caso de los datos perdidos o descartados como se observa en la figura No. 31, la tasa de descarte en el Escenario A (línea roja) es más alta con un máximo de 4,422 bits/sec, por otro lado en el Escenario B con la implementación del protocolo de seguridad este valor se reduce a casi la mitad en comparación al primer escenario, con un máximo de pérdida de 2,591 bits/sec; para entender esta situación, se considera que en la configuración del protocolo de seguridad IPSec se implementan túneles de un

nodo emisor a un receptor, lo que hace que los paquetes o datos enviados conozcan una ruta de salida y de llegada, reduciendo así la cantidad de tráfico descartado o perdido.

Comparación Data Dropped

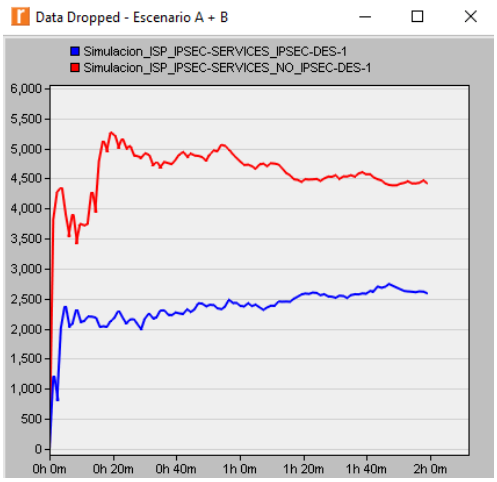


Figura 31. Gráfica Comparativa Data Dropped
Elaborado por: Marcela Gallegos e Ismael Román.

4.3.2 Análisis Estadístico

Para el análisis estadístico, se optó por calcular los valores de varianza y desviación estándar; la varianza representa a la desviación promedio de la media de los datos tomados, mientras que la desviación media es una medida estadística que se utiliza para determinar cuánto tienden los valores a alejarse del rango normal obtenido. La diferencia entre los dos es la segmentación de los datos, la varianza trabaja con todos los datos en función de la media obtenida, mientras que la desviación trabaja con los datos sin que la media obtenida influya en el resultado; en otras palabras, con la desviación media se obtiene el comportamiento de los datos a analizar, que tan estables son y cómo estos afectan en el rendimiento de la red (para entender mejor estos conceptos se realiza el análisis respectivo más adelante).

Para obtener la varianza y la desviación media de los datos, se utilizan las siguientes ecuaciones:

Tabla 17. Ecuación de la Varianza

VARIANZA	
$$s^2 = \sum_{i=1}^{n} \frac{(x_i - \bar{x})^2}{n-1}$$	
$\mathbf{s^2}$	Varianza
$\mathbf{n}$	Total de eventos de la simulacion – o datos a procesar
$\mathbf{x_i}$	Representa a los datos de la muestra
$\bar{\mathbf{x}}$	Media de lo datos
$\sum()$	Sumatoria de los datos

Nota: Ecuación para obtener la varianza de los datos estadísticos de la simulación.
Elaborado por: (Walpole, Myers, Myers, & Ye, 2012)

Tabla 18. Ecuación de la Desviación Media

DESVIACIÓN MEDIA	
$$s = \sqrt{s^2}$$	
$\mathbf{s}$	Desviación media
$\mathbf{s^2}$	Varianza

Nota: Ecuación para obtener la desviación media de los datos estadísticos de la simulación.
Elaborado por: (Walpole, Myers, Myers, & Ye, 2012)

Para el cálculo de estos valores, se tomó los datos de la simulación en el tiempo de ejecución de 7200 segundos.

Los resultados de la varianza y desviación media se encuentran en la tabla No. 19, los cuales fueron obtenidos al procesar los 101 eventos de la simulación, deduciendo lo. siguiente: los valores del Escenario A son visiblemente altos en comparación del Escenario B en ambos parámetros, uno de los principios básicos de la desviación media es analizar el comportamiento de los datos, partiendo del hecho que mayor dispersión mayor variabilidad y a menor valor más homogeneidad.

Por consiguiente, se puede decir que en el Escenario B con la implementación de IPSec, si bien es cierto, el rendimiento tiende a disminuir por el volumen del tráfico y doble encapsulado, los datos presentan una mayor homogeneidad, con el establecimiento de parámetros y políticas de seguridad, logrando así que el comportamiento de los datos y de la red sea más estable.

Tabla 19. Varianza y Desviación Estándar

		ESCENARIO A	ESCENARIO B
THROUGHTPUT	Varianza	187,206,246.217	96,256,359.925
	Desviación Media	13,682.333	9,811.033

Nota: Resultados de la varianza y desviación media de los datos de ambos escenarios
Elaborado por: Marcela Gallegos e Ismael Román

En el apartado “Anexos” se puede encontrar los datos y resultados de los parámetros de varianza y desviación media.

CONCLUSIONES

- El entorno de red en el que se desarrolla un ISP es inseguro por naturaleza, debido a todas las amenazas informáticas que en la actualidad existen. Debido a esta razón, se puede decir que la implementación de procedimientos o alternativas de seguridad tradicionales como VPN, SSH, ACL, VLAN o TLS no bastan para garantizar la integridad de la información. La utilización de IPSec aporta en la generación de un entorno de red seguro.
- Los mecanismos de seguridad que se manejan en un ISP con respecto al usuario final son casi nulos o ineficientes. La seguridad informática dirigida hacia el usuario es un criterio que debe manejar un proveedor de servicios. El ISP debe implementar mecanismos de alerta cuando el host del usuario final está infectado o es víctima de un ataque informático, de esa manera se podrá aislar el problema y darle el tratamiento correspondiente.
- El rendimiento de la red se ve afectado con la implementación del protocolo IPSec, ya que realiza un hardening de seguridad (con la creación de políticas para el transporte de información), añadiendo doble encapsulado a los paquetes, lo que con lleva a que la red tenga que procesar volúmenes de datos más altos.
- Para comprobar que IPSec es ampliamente eficiente, se realizó el cálculo de la desviación estándar, con los resultados obtenidos se puede concluir que la implementación de este protocolo, además de incorporar seguridad al escenario de red, se logra una mayor estabilidad en la simulación.
- El modelo de seguridad de un ISP debe contemplar todas las necesidades de la organización, a través de la implementación de normas que brinden una guía de cómo llevar este proceso de una manera estructurada y funcional. La utilización de la norma ISO/IEC 27001 permite generar un modelo de seguridad integral.

RECOMENDACIONES

- Para mejorar el modelo de investigación, se propone estructurar un plan general de desarrollo, donde se defina objetivos y metas a alcanzar, además se establezcan acciones a tomar, como entrevistas directas con un proveedor de servicios, esto con el fin de conocer más a fondo algunos aspectos relacionados con el funcionamiento de un ISP.
- Los ISP, a más de proveer los servicios tradicionales, como acceso a Internet o hosting, deberían incluir en sus planes y por su puesto en sus contratos, servicios de seguridad orientados a proteger al usuario en caso de un ataque informático. De esta manera se puede generar un nuevo modelo de funcionamiento por parte de este tipo de organizaciones, además el usuario estaría protegido legalmente si su información se ve comprometida de alguna manera.
- En el presente proyecto, la simulación fue ejecuta en un tiempo de 2 horas, en el cual, se tomaron datos estadísticos para realizar cálculos matemáticos y así poder emitir el respectivo análisis, por ello, se recomienda que en cuanto a escenarios con la implementación de IPSec, se mantenga el tiempo de simulación por el gran número de datos obtenidos.
- En base a la herramienta de simulación, se recomienda realizar un análisis de los módulos y escenarios que se pueden implementar, ya que, al ser un software de simulación en base a eventos, se pueden realizar varias configuraciones y obtener información importante como gráficas y datos estadísticos, que muchas veces por la falta de investigación se desconoce.

LISTA DE REFERENCIAS

AEPROVI. (2018). *Asociación de empresas proveedoras de Internet, valor agregado, portadores y tecnologías de la información.* Obtenido de http://aeprovi.org.ec/es/napec

Agencia de Control y Regulación de las Telecomunicaciones. (2015). Internet - Boletín Estadístico del Sector de las Telecomunicaciones. Quito. Obtenido de www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf

Agencia de Regulación y Control de las Telecomunicaciones. (Diciembre de 2017). *ARCOTEL.* Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2015/09/3.1.1-Cuentas-internet-fijos-y-moviles_dic2017-Rev-2.xlsx

Agencia de Regulación y Control de las Telecomunicaciones. (2017). *ARCOTEL.* Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2015/01/BOLETIN-ESTADISTICOIITRIMESTRE-Septiembre-2017_def.pdf

Amaro, G. (22 de Marzo de 2017). Obtenido de https://sites.google.com/site/wikiuptxti/5-1-2-8-practica-de-laboratorio-visualizacion-de-direcciones-mac-de-dispositivos-de-red/6-5-1-2-armado-de-una-red-de-switch-y-router/7-1-2-8-uso-de-la-calculadora-de-windows-con-direcciones-de-red/7-1-2-9-conversio

ARSYS INTERNET S.L. (11 de Diciembre de 2007). *ARSYS.* Obtenido de https://www.arsys.es/blog/soluciones/cloud/la-seguridad-gestionada-desde-la-perspectiva-del-isp/

BALTAZAR GÁLVEZ, J. M., & CAMPUZANO RAMÍREZ, J. C. (2011). *DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PERIMETRAL PARA REDES DE DATOS. CASO PRÁCTICO: DIRECCIÓN GENERAL DEL COLEGIO DE CIENCIAS Y HUMANIDADES.* México, D.F.: UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/174/Version%20Final.pdf

Caicedo, M., & Yánez, F. (2002). *Planificación de un proveedor de servicios de internet y diseño de su sistema de seguridad.* Quito: Quito : EPN, 2002.

CISCO. (04 de Mayo de 2006). *CISCO*. Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/7609-router/product_data_sheet09186a0080169ead.html

CISCO. (25 de Abril de 2006). *CISCO*. Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/7200-series-routers/product_data_sheet09186a008008872b.html

CISCO. (30 de Octubre de 2008). *CISCO.* Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Cisco Networking Academy. (s.f.). Obtenido de http://www.itesa.edu.mx/netacad/introduccion/course/module8/8.2.2.2/8.2.2.2.html

CISCO. (s.f.). *Service Provider Security.* Obtenido de https://www.cisco.com/c/en/us/about/security-center/service-provider-infrastructure-security.html

Corral, B. (29 de Junio de 2010). *IPv6.* Obtenido de https://sites.google.com/site/tknikaipv6/5-mecanismos-de-transicion/5-3-teredo

Deering, S., & Hinden, R. (Diciembre de 1998). *Especificación Protocolo Internet, Versión 6 (IPv6)*. https://tools.ietf.org/html/rfc2460.

Delgado, C., & Lara, J. (28 de Febrero de 2016). Obtenido de http://tesis.ipn.mx/bitstream/handle/123456789/22858/Transici%C3%B3n%20de%20IPv4%20a%20IPv6.pdf?sequence=1&isAllowed=y

EL Negocio Digital. (17 de Noviembre de 2015). Obtenido de http://elnegociodigital.com/post/cuantas-direcciones-ip-hay-disponibles-ipv4-vs-ipv6-el-futuro-esta-aqui

Evans, D. (2011). *Intenet de las cosas: Cómo la próxima evolución de Internet lo cambia todo.* Obtenido de https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Fierro, L. (1995). Presencia del Ecuador en Internet. Obtenido de https://interred.wordpress.com/1995/02/12/presencia-del-ecuador-en-el-internet/

Frankel, S., & Krishnan, S. (Febrero de 2011). *Internet Engineering Task Force*. Obtenido de https://tools.ietf.org/html/rfc6071

García Alfaro, J. (s.f.). *Ataques contra redes TCP/IP.* Obtenido de www.deic.uab.es/material/26118-atacs.pdf

García, M. A. (2016). Adopción de pautas de seguridad informática - Seguridad y Alta Disponibilidad. Obtenido de https://mgarciafelipe.files.wordpress.com/2011/10/ud-1-adopcic3b3n-de-pautas-de-seguridad-informc3a1tica-miguelangelgarcia1.pdf

IBM. (2013). Resolución de problemas de TCP/IP. Obtenido de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_71/com.ibm.aix.networkcomm/tcpip_troublesh.htm

INEC. (Diciembre de 2016). *Ecuador en cifras.* Obtenido de http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf

ISO/IEC 27001:2005; ISO/IEC 27001:2013. (2013). *Information technology - Security techniques - Information security management systems - Requirements.*

Kent, S., & Atkinson, R. (Noviembre de 1998). *Security Architecture for the Internet Protocol*. Obtenido de https://tools.ietf.org/html/rfc2401

López Logacho, J. E. (Agosto de 2014). Obtenido de http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/9690/AC-MRIC-ESPE-048317.pdf?sequence=1&isAllowed=y

Lopez, J. (Julio de 2007).

Martinez, C., & Vidal, L. (11 de Septiembre de 2006). *ANTEL Telecomunicaciones.* Obtenido de https://iie.fing.edu.uy/eventos/telcom2006/conferencias/Seguridad_en_un_ISP.pdf

McCherry, P. (31 de Noviembre de 2014). *Cloud9 IT Services*. Obtenido de https://icloud9.co.uk/network-report/

Microsoft. (10 de Agosto de 2009). *Microsoft Docs*. Obtenido de https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786900(v=ws.10)

MIKROWAYS. (1 de Enero de 2010). Obtenido de https://www.mikroways.net/2010/01/01/ietf-internet-engineering-task-force/

Nacional Crime Agency. (02 de Junio de 2014). *NCA*. Obtenido de http://www.nationalcrimeagency.gov.uk/news/news-listings/386-two-week-opportunity-for-uk-to-reduce-threat-from-powerful-computer-attack

ORACLE. (Marzo de 2012). Obtenido de https://docs.oracle.com/cd/E26921_01/pdf/E25871.pdf

Oracle Corporation. (2010). Obtenido de https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html

Palet, J. (1 de Octubre de 2001). *NETWORK WORLD*. Obtenido de http://www.networkworld.es/archive/seguridad-con-ipsec

Recio, M. J. (2012). De la seguridad informática a la seguridad de la información . *SEGURIDAD Y SALUD*, 1-2. Obtenido de https://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128

Siles Peláez, R. (2002). *Análisis de seguridad de la familia de protocolos TCP/IP.* Obtenido de http://www.rediris.es/cert/doc/segtcpip/#_Toc12260170

Telefónica . (s.f.). Obtenido de http://www.telefonica.es/on/io/es/atencion/tutoriales_articulos/pdf/IPSec.pdf

UNEX. (2006).

Universidad Nacional Autonoma de México. (Junio de 04 de 2014). *Cordinación de Segiridad de la Información de la UNAM*. Obtenido de https://www.seguridad.unam.mx/historico/noticia/index.html-noti=1749

Vazquez Clavijo, J. E. (Abril de 2011). *Análisis de las funcionalidades de los protocolos de seguridad IPSEC, IKE, ISAKMP, sobre IPV6 e implementación en una red prototipo bajo infraestructura CISCO*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/1683/8/UPS-ST000292.pdf

Velasco, R. (21 de Abril de 2016). *Redes Zone*. Obtenido de https://www.redeszone.net/2016/04/21/los-isp-no-protegen-correctamente-los-usuarios-los-ataques-ddos/

Viguera, A. P. (s.f.). *INFRAESTRUCTURA DE UN ISP*. Obtenido de http://web.dit.upm.es/~david/TAR/trabajos2002/10-Infraestructura-ISP-Andoni-Perez-res.pdf

Villagra, V. (2000).

Walpole, R. E., Myers, R. H., Myers, S. L., & Ye, K. (2012). *Probabilidad y estadística para ingeniería y ciencias.* México: Pearson Educación. Obtenido de https://vereniciafunez94hotmail.files.wordpress.com/2014/08/8va-probabilidad-y-estadistica-para-ingenier-walpole_8.pdf

Walton, A. (20 de Noviembre de 2017). *CCNA DESDE CERO*. Obtenido de https://ccnadesdecero.es/encabezado-paquete-ipv4-paquete-ipv6/#21Encabezado_de_paquetes_IPv6

We Are Social, Hootsuite. (30 de 01 de 2018). *We Are Social.* Obtenido de https://wearesocial.com/blog/2018/01/global-digital-report-2018

Winther, M. (2006). Tier 1 ISPs: What They Are and Why They Are Important. *IDC - Analize the Future*. Obtenido de https://www.us.ntt.net/downloads/papers/IDC_Tier1_ISPs.pdf

ANEXOS

Anexo 1

Cálculo de la varianza y desviación media - Escenario A

THROUGHPUT - ESCENARIO A						
VARIANZA						DESVIACIÓN MEDIA
X_i	n	$\overline{x}$	$x_i - \overline{x}$	$(x_i - \overline{x})^2$	$s^2 = \sum_{i=1}^{n} \frac{(x_i - \overline{x})^2}{n-1}$	$s = \sqrt{s^2}$
663.111111111	101	113,235.254707505	-112,572.143596394	12,672,487,513.887200000	**187,206,246.217**	**13,682.333**
103,400.777777778			-9,834.476929727	96,716,936.481340000		
114,899.629629630			1,664.374922125	2,770,143.881397350		
119,433.388888889			6,198.134181384	38,416,867.330436200		
109,958.933333333			-3,276.321374172	10,734,281.746858800		
95,781.833333300			-17,453.421374205	304,621,917.665569000		
104,898.777777778			-8,336.476929727	69,496,847.599876700		
91,841.708333300			-21,393.546374205	457,683,826.465276000		
99,762.617284000			-13,472.637423505	181,511,959.145237000		
92,450.944444400			-20,784.310263105	431,987,553.113028000		
96,936.444444400			-16,298.810263105	265,651,215.992709000		
100,651.388888889			-12,583.865818616	158,353,678.940941000		
92,945.760683800			-20,289.494023705	411,663,567.737976000		
111,428.674603175			-1,806.580104330	3,263,731.673362370		
125,715.874074074			12,480.619366569	155,765,859.773168000		
122,012.625000000			8,777.370292495	77,042,229.251567200		
132,591.509803922			19,356.255096417	374,664,611.357555000		
131,128.117283951			17,892.862576446	320,154,531.179568000		
125,006.450292398			11,771.195584893	138,561,045.497796000		
129,271.688888889			16,036.434181384	257,167,221.253849000		
125,710.169312169			12,474.914604664	155,623,494.393650000		
125,034.752525253			11,799.497817748	139,228,148.751031000		
121,681.719806763			8,446.465099258	71,342,772.672977000		
120,690.240740741			7,454.986033236	55,576,816.755738400		
120,613.226666667			7,377.971959162	54,434,470.230175300		
121,565.132478633			8,329.877771128	69,386,863.681926000		
121,075.876543210			7,840.621835705	61,475,350.770528300		
116,766.087301587			3,530.832594082	12,466,778.807429200		
119,101.501915709			5,866.247208204	34,412,856.307756800		
118,274.922222222			5,039.667514717	25,398,248.658890000		
118,395.000000000			5,159.745292495	26,622,971.483420500		
118,578.427083333			5,343.172375828	28,549,491.037807400		
118,682.666666667			5,447.411959162	29,674,297.052817200		
124,957.029411765			11,721.774704260	137,400,002.217421000		
124,244.431746032			11,009.177038527	121,201,979.065622000		
123,532.453703704			10,297.198996199	106,032,307.167314000		
121,098.216216216			7,862.961508711	61,826,163.687464800		
121,713.418128655			8,478.163421150	71,879,254.995719600		
120,444.242165242			7,208.987457737	51,969,500.165804000		
121,302.213888889			8,066.959181384	65,075,830.434109700		
120,830.322493225			7,595.067785720	57,685,054.669676100		
119,116.917989418			5,881.663281913	34,593,962.961799200		
122,151.224806202			8,915.970098697	79,494,522.800852200		
120,986.954545455			7,751.699837950	60,088,850.377668200		
120,044.207407407			6,808.952699902	46,361,836.869497600		
122,883.553140097			9,648.298432592	93,089,662.644350200		
123,940.990543735			10,705.735836230	114,612,779.795131000		
122,959.219907407			9,723.965199902	94,555,499.208897800		
121,394.691609977			8,159.436902472	66,576,410.565415800		
119,546.260000000			6,311.005292495	39,828,787.801895100		

118,394.745098039			5,159.490390534	26,620,341.090008800		
117,098.474358974			3,863.219651469	14,924,466.075493300		
117,644.867924528			4,409.613217023	19,444,688.723740600		
116,533.012345679			3,297.757638174	10,875,205.440132500		
115,840.070707071			2,604.815999566	6,785,066.391593100		
117,383.176587302			4,147.921879797	17,205,255.920895600		
118,884.656920078			5,649.402212573	31,915,745.359420600		
117,541.095785441			4,305.841077936	18,540,267.388437800		
117,850.250470810			4,614.995763305	21,298,185.895319700		
118,406.733333333			5,171.478625828	26,744,191.177392000		
119,291.194899818			6,055.940192313	36,674,411.612867500		
117,600.897849462			4,365.643141957	19,058,840.042912900		
115,741.130511464			2,505.875803959	6,279,413.544865280		
115,212.909722222			1,977.655014717	3,911,119.357233820		
113,446.666666667			211.411959162	44,695.016476560		
113,155.843434343			-79.411273162	6,306.150305269		
112,423.366500829			-811.888206676	659,162.460140182		
115,297.104575163			2,061.849867658	4,251,224.876759770		
115,922.784219002			2,687.529511497	7,222,814.875165310		
115,305.811111111			2,070.556403606	4,287,203.820512290		
115,354.837245696			2,119.582538191	4,492,630.136202640		
114,804.228395062			1,568.973687557	2,461,678.432245050		
114,510.774733638			1,275.520026133	1,626,951.337065370		
115,357.492492492			2,122.237784987	4,503,893.216024960		
114,912.549629630			1,677.294922125	2,813,318.255785050		
114,407.915204678			1,172.660497173	1,375,132.641629130		
112,928.323232323			-306.931475182	94,206.930457626		
112,855.831908832			-379.422798673	143,961.660153136		
113,061.189873418			-174.064834087	30,298.566465865		
113,246.709722222			11.455014717	131.217362158		
112,213.838134431			-1,021.416573074	1,043,291.815750990		
114,065.956639566			830.701932061	690,065.699929246		
114,751.394912985			1,516.140205480	2,298,681.122671780		
113,674.988095238			439.733387733	193,365.452286816		
113,689.977777778			454.723070273	206,773.070638161		
112,688.297157623			-546.957549882	299,162.561373324		
112,390.839080460			-844.415627045	713,037.751198422		
111,720.829545455			-1,514.425162050	2,293,483.571451310		
110,470.916354557			-2,764.338352948	7,641,566.529581300		
109,797.514814815			-3,437.739892690	11,818,055.569794800		
109,705.653235653			-3,529.601471852	12,458,086.550102500		
109,204.667874396			-4,030.586833109	16,245,630.219234700		
110,294.789725209			-2,940.464982296	8,646,334.312111190		
111,093.828605201			-2,141.426102304	4,585,705.751630530		
111,007.114619883			-2,228.140087622	4,964,608.250069860		
110,281.746527778			-2,953.508179727	8,723,210.567716510		
110,160.631156930			-3,074.623550575	9,453,309.977752710		
110,879.541950113			-2,355.712757392	5,549,382.595341210		
110,629.583613917			-2,605.671093588	6,789,521.847962040		
109,527.643333333			-3,707.611374172	13,746,382.101892300		
0.000000000			-113,235.254707505	12,822,222,908.673600000		

Nota: Datos calculados de la varianza y desviación media en el escenario A.
Elaborado por: Marcela Gallegos e Ismael Román

Anexo 2

Cálculo de la varianza y desviación media - Escenario B

THROUGHPUT - ESCENARIO B - IPSEC						
VARIANZA						DESVIACION MEDIA
X_i	n	$\bar{x}$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$	$s^2 = \sum_{i=1}^{n} \frac{(x_i - \bar{x})^2}{n-1}$	$s = \sqrt{s^2}$
663.111111111	101	59,371.477382626	-58,708.366271515	3,446,672,270.270340000	**96,256,359.925**	**9,811.033**
16,296.944444400			-43,074.532938226	1,855,415,387.846300000		
11,020.481481500			-48,350.995901126	2,337,818,804.630690000		
55,429.083333300			-3,942.394049326	15,542,470.840160000		
54,278.444444400			-5,093.032938226	25,938,984.509853600		
60,502.462963000			1,130.985580374	1,279,128.383014220		
56,513.317460300			-2,858.159922326	8,169,078.141589770		
59,427.694444400			56.217061774	3,160.358034517		
66,975.320987700			7,603.843605074	57,818,437.570427000		
65,848.377777800			6,476.900395174	41,950,238.729006800		
76,253.050505100			16,881.573122474	284,987,511.089441000		
76,298.509259300			16,927.031876674	286,524,408.153942000		
73,266.589743600			13,895.112360974	193,074,147.524096000		
68,075.190476200			8,703.713093574	75,754,621.615254000		
67,488.755555600			8,117.278172974	65,890,204.937442400		
66,860.229166700			7,488.751784074	56,081,403.283473500		
65,040.581699300			5,669.104316674	32,138,743.753333300		
63,492.500000000			4,121.022617374	16,982,827.412909200		
65,606.713450300			6,235.236067674	38,878,168.819624400		
62,363.622222200			2,992.144839574	8,952,930.740990150		
59,424.587301600			53.109918974	2,820.663493439		
60,526.585858600			1,155.108475974	1,334,275.591267310		
59,151.531401000			-219.945981626	48,376.234833363		
56,713.375000000			-2,658.102382626	7,065,508.276521280		
54,469.551111100			-4,901.926271526	24,028,881.171475400		
61,739.602564100			2,368.125181474	5,608,016.875131930		
62,810.415637900			3,438.938255274	11,826,296.323587900		
60,586.837301600			1,215.359918974	1,477,099.732648820		
59,955.766283500			584.288900874	341,393.519684711		
60,436.559259300			1,065.081876674	1,134,399.404019700		
59,728.372759900			356.895377274	127,374.310319649		
57,879.142361100			-1,492.335021526	2,227,063.816472590		
56,555.663299700			-2,815.814082926	7,928,808.949603620		
57,888.189542500			-1,483.287840126	2,200,142.816665250		
57,526.730158700			-1,844.747223926	3,403,092.320182180		
56,396.209876500			-2,975.267506126	8,852,216.733008410		
55,824.528528500			-3,546.948854126	12,580,846.173784800		
55,783.201754400			-3,588.275628226	12,875,721.984119700		
56,774.182336200			-2,597.295046426	6,745,941.558188320		
58,063.022222200			-1,308.455160426	1,712,054.906845060		
57,730.699187000			-1,640.778195626	2,692,153.087241260		
57,568.235449700			-1,803.241932926	3,251,681.468662200		
58,374.284237700			-997.193144926	994,394.168287133		
58,582.646464600			-788.830918026	622,254.217233519		
57,293.844444400			-2,077.632938226	4,316,558.626001030		
57,142.258454100			-2,229.218928526	4,969,417.031297970		
59,417.387706900			45.910324274	2,107.757874957		
62,596.930555600			3,225.453172974	10,403,548.171049000		
61,330.734693900			1,959.257311274	3,838,689.211781160		
60,927.035555600			1,555.558172974	2,419,761.229506640		

59,742.052287600			370.574904974	137,325.760196595		
58,969.574786300			-401.902596326	161,525.696933468		
58,505.171907800			-866.305474826	750,485.175713256		
57,432.633744900			-1,938.843637726	3,759,114.651550050		
57,847.038383800			-1,524.438998826	2,323,914.261141200		
56,824.333333300			-2,547.144049326	6,487,942.808016160		
55,837.814814800			-3,533.662567826	12,486,771.143253700		
57,102.524904200			-2,268.952478426	5,148,145.349354860		
57,029.167608300			-2,342.309774326	5,486,415.078902470		
58,287.638888900			-1,083.838493726	1,174,705.880481940		
59,349.273224000			-22.204158626	493.024660283		
59,475.512544800			104.035162174	10,823.314968600		
59,801.754850100			430.277467474	185,138.699015958		
59,499.248263900			127.770881274	16,325.398101570		
60,765.331623900			1,393.854241274	1,942,829.645917900		
61,426.723905700			2,055.246523074	4,224,038.270608330		
63,252.477611900			3,881.000229274	15,062,162.779625900		
64,869.671568600			5,498.194185974	30,230,139.306679900		
64,910.505636100			5,539.028253474	30,680,833.992784800		
65,793.998412700			6,422.521030074	41,248,776.381744700		
66,015.043818500			6,643.566435874	44,136,974.987873300		
65,105.442901200			5,733.965518574	32,878,360.568197200		
64,607.657534200			5,236.180151574	27,417,582.579739000		
64,313.723723700			4,942.246341074	24,425,798.895860700		
64,047.454814800			4,675.977432174	21,864,764.946201900		
63,895.399122800			4,523.921740174	20,465,867.911220200		
63,565.875901900			4,194.398519274	17,592,978.938489100		
63,805.393162400			4,433.915779774	19,659,609.142130100		
63,003.786216600			3,632.308833974	13,193,667.465366600		
63,418.609722200			4,047.132339574	16,379,280.174026900		
63,128.427983500			3,756.950600874	14,114,677.817408500		
63,215.551490500			3,844.074107874	14,776,905.746828400		
62,790.847389600			3,419.370006974	11,692,091.244594300		
62,929.279100500			3,557.801717874	12,657,953.063708200		
63,237.759477100			3,866.282094474	14,948,137.234051300		
63,482.118863000			4,110.641480374	16,897,373.380172500		
64,107.020434200			4,735.543051574	22,425,367.993312100		
63,874.760101000			4,503.282718374	20,279,555.241607200		
64,065.761548100			4,694.284165474	22,036,303.826221300		
65,224.340740700			5,852.863358074	34,256,009.488286900		
64,513.323565300			5,141.846182674	26,438,582.166280600		
63,817.365942000			4,445.888559374	19,765,925.082373800		
63,138.636798100			3,767.159415474	14,191,490.061595500		
62,473.520094600			3,102.042711974	9,622,668.986911850		
63,002.719298200			3,631.241915574	13,185,917.849422500		
62,989.819444400			3,618.342061774	13,092,399.276003900		
62,649.744559000			3,278.267176374	10,747,035.679692100		
63,295.163265300			3,923.685882674	15,395,310.905896300		
62,903.182940500			3,531.705557874	12,472,944.147519100		
62,279.945555600			2,908.468172974	8,459,187.113203550		
0.000000000			-59,371.477382626	3,524,972,326.595650000		

Nota: Datos calculados de la varianza y desviación media en el escenario B.
Elaborado por: Marcela Gallegos e Ismael Román