UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

Tesis presentada previo a la obtención del título de Ingenieros en Informática y Sistemas Computacionales

Autores:

Jácome Calderón Freddy Paúl

Robayo Granja Manuel Alejandro

Director:

Ing. Corrales Beltrán Segundo Humberto

Latacunga – Ecuador

Abril 2014

AUTORÍA

Los criterios emitidos en el presente trabajo de investigación **"IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013",** son de exclusiva responsabilidad de los autores.

……	……..……
Jácome Calderón Freddy Paúl	Robayo Granja Manuel Alejandro
050305737-4	050338867-0

AVAL DEL DIRECTOR DE TESIS

En calidad de Director del Trabajo de Investigación sobre el tema: **"IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013"** de Jácome Calderón Freddy Paúl con CI 050305737-4 y Robayo Granja Manuel Alejandro con CI 050338867-0; postulantes de la especialidad de Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Tesis que el Honorable Consejo Académico de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga a 10 de abril del 2014

……..

Ing. Segundo Humberto Corrales Beltrán

C.C. # 050240928-7

DIRECTOR DE TESIS

UNIVERSIDAD TÉCNICA DE COTOPAXI
UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
Latacunga Ecuador

APROBACIÓN DEL TRIBUNAL DE GRADO

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

- Jácome Calderón Freddy Paúl
- Robayo Granja Manuel Alejandro

Con el título de tesis: **IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013** han considerado las recomendaciones emitidas oportunamente y reúnen los méritos suficientes para ser sometidos al acto de Defensa de Tesis.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 10 de abril 2014

Para constancia firman:

……..	…….
Ing. Jorge Rubio	Msc. Bolívar Vaca
PRESIDENTE	**MIEMBRO**
……	…….
Ing. Víctor Medina	Ing. Segundo Corrales
OPOSITOR	**DIRECTOR**

UNIVERSIDAD TÉCNICA DE COTOPAXI
UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Latacunga, 10 de abril del 2014

CERTIFICADO

La Carrera de Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi. Certifica que los egresados Jácome Calderón Freddy Paúl con CI 050305737-4 y Robayo Granja Manuel Alejandro con CI 050338867-0, estudiantes de la Universidad Técnica de Cotopaxi de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas, de la carrera de Ingeniería en Informática y Sistemas Computacionales aplicaron la tesis **"IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013",** trabajo que se implementó y se dejó en perfecto funcionamiento.

Es todo cuanto puedo certificar en honor a la verdad, los egresados Jácome Paul y Robayo Manuel, pueden hacer uso del presente certificado de manera que estimen conveniente siempre y cuando esto no perjudique directa o indirectamente a la Institución.

Atentamente,

……..

Ing. Segundo Humberto Corrales Beltrán

C.C. # 050240928-7

Director de la Carrera Ingeniería en Informática y Sistemas Computacionales

CERTIFICACIÓN

En calidad de docente del centro de idiomas de la Universidad Técnica de Cotopaxi, CERTIFICO haber revisado el resumen de la tesis de los estudiantes Jácome Calderón Freddy Paúl y Robayo Granja Manuel Alejandro, egresados de la Carrera de Ingeniería en Informática y Sistemas Computacionales cuyo tema es**:**

"IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013"

Latacunga, 10 de abril del 2014

Por su favorable atención reciba nuestro agradecimiento

Atentamente,

……

Lic. Alison Mena Barthelotty

C.C. # 0501801252

Docente Centro Cultural de Idiomas

AGRADECIMIENTO

Al finalizar mis estudios, quiero agradecer a Dios por haber permitido lograr los objetivos que me he planteado y proporcionarme la capacidad para efectuar la presente investigación.

A la Universidad Técnica de Cotopaxi por darme la oportunidad de culminar mi estudios y obtener mi profesión.

Expreso mi más sincero agradecimiento y reconocimiento a mis padres por los esfuerzos y sacrificios que hicieron para darme una profesión.

A mis hermanos y hermana quienes han confiado y apoyado para seguir adelante.

Al Ing. Jorge Rubio, por la ayuda ofrecida durante la implementación y elaboración de esta investigación.

Al Ing. Segundo Corrales, quien con sus conocimientos y apoyo incondicional supo guiar el desarrollo de la presente tesis.

Paúl

AGRADECIMIENTO

En primer lugar a Dios por haberme guiado por el camino de la felicidad hasta ahora.

A cada uno de los que son parte de mi familia, mi PADRE Jhonny Robayo, mi MADRE Judith Granja, y no menos importante, mi TÍA.

A mis tres hermanas y a toda mi familia en general; por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora.

Por último a mis amigos porque en esta armonía grupal lo hemos logrado y a todos mis profesores quienes contribuyeron día a día en mi formación profesional.

Alejandro

DEDICATORIA

Las páginas que enmarcan esta investigación, fruto de mucho esfuerzo, entrega y sacrificio, está dedicado a Dios por estar presente en cada momento de mi vida concediéndome felicidad, salud y bendición.

A mis padres Nelson Jácome y Susana Calderón por el completo apoyo, y el inmenso esfuerzo que hicieron para poder culminar esta profesión sin dudar que se lograra este éxito.

A mis hermanos Marco, Maryorie y Mauricio por estar a mi lado apoyándome incondicionalmente a lo largo de mi trayecto estudiantil.

Paúl

DEDICATORIA

La concepción de este proyecto de tesis está dedicada a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento, depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ello que soy lo que soy ahora.

Alejandro

ÍNDICE GENERAL

CONTENIDO **Pág.**

CAPÍTULO I

1. FUNDAMENTACIÓN TEÓRICA DE MECANISMOS DE SEGURIDAD

CAPÍTULO II

2. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO III

3. IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

La propuesta "IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI UBICADO EN LA CIUDAD DE LATACUNGA, PROVINCIA DE COTOPAXI, EN EL PERIODO 2013".

Autores: Jácome Calderón Freddy Paúl
Robayo Granja Manuel Alejandro

La implementación de mecanismos de seguridad es un apoyo para el laboratorio de redes de la Universidad Técnica de Cotopaxi, la cual ofrecerá una comunicación segura a los estudiantes alojados en la red de comunicación, brindándoles una guía de cómo proteger una red con autenticidad, integridad y confiabilidad al momento de enviar y recibir información. El presente trabajo de investigación consta de un análisis de los principales mecanismos de seguridad en redes, así como las ventajas y características del mecanismo (IPSec) a implementar, el cual está encargado de proteger la seguridad de la red de comunicación, asegurar el flujo de paquetes de datos y garantizar una autenticación mutua contrarrestando ataques informáticos. Además se contará con una guía simple y flexible que tiene por objetivo el conducir, encaminar y dirigir la implementación de mecanismos de seguridad, protegiendo la red de comunicación de los diferentes ataques informáticos.

UNIVERSIDAD TÉCNICA DE COTOPAXI
UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

ABSTRACT

The proposal "IMPLEMENTATION OF SECURITY MECHANISMS FOR CRITICAL INFRASTRUCTURE TO COUNTER ATTACKS IN COMPUTER NETWORKS LABORATORY TECHNICAL UNIVERSITY OF COTOPAXI, LOCATED IN LATACUNGA CITY, COTOPAXI PROVINCE , IN 2013 PERIOD".

BY: Jácome Calderón Freddy Paúl
Robayo Granja Manuel Alejandro

The implementation of security mechanisms is a support network for the laboratory of Technical University of Cotopaxi, which it provides secure communication to students staying in the communication network, providing guidance, how to protect a network with authenticity, integrity and reliability when sending and receiving information. The present researching consists of an analysis of the main mechanisms for network security, as well as the advantages and features of the mechanism (IPSec) to implement, which is responsible for protecting the security of the communication network, ensure the flow of data packets and ensuring mutual authentication countering attacks. In addition there will be a simple and flexible guide which aims to drive, it will direct and manage the implementation of security mechanisms, protecting the communication network of different attacks.

INTRODUCCIÓN

Con la evolución de la tecnología, y el desarrollo de distintos medios de comunicación surge la necesidad de implementar redes de comunicación con la finalidad de transportar datos, compartir información, recursos y ofrecer servicios, otorgando ventajas tanto en movilidad, flexibilidad y productividad. Sin embargo, a pesar de poseer muchas ventajas la implementación de redes de comunicación, acarrea consigo riesgos de seguridad que es de suma importancia disminuirlos, en su mayoría asociados a la inexistencia de delimitación física, y otros más importantes asociados a la carencia de mecanismos de seguridad que resguarden el acceso a la información y a los recursos tecnológicos.

Los problemas de seguridad en infraestructuras de red cada vez son más notables debido a la confidencialidad de la información utilizada en los mismos, dado que ésta puede ser accesible fuera del límite físico. Por esta razón fue necesario analizar y comparar los diferentes mecanismos de seguridad aplicables a la infraestructura de red de comunicación e implementar un mecanismo de seguridad (IPSec) suficientemente eficaz para preservar la confiabilidad, integridad y disponibilidad de los bienes informáticos, garantizando un nivel adecuado de seguridad de información.

Los principales objetivos que determinaron la investigación son: Implementar mecanismos de seguridad para contrarrestar infraestructuras críticas frente ataques informáticos en el laboratorio de redes de la Universidad Técnica de Cotopaxi, ubicado en la ciudad de Latacunga, provincia de Cotopaxi. Recopilar la información necesaria para conocer las vulnerabilidades y seguridades en la transmisión de datos de los bienes informáticos. Analizar la documentación relacionada con los mecanismos de seguridad para saber las necesidades que tienen los usuarios al momento de intercambiar información. Aplicar mecanismos de seguridad que puedan asegurar la confiabilidad, integridad y autenticidad de la información.

La Hipótesis de esta investigación es que la implementación de mecanismos de seguridad permitirá un adecuado control de seguridad en el intercambio de información por parte de los estudiantes y docentes de la Universidad Técnica de Cotopaxi.

La investigación tuvo una utilidad práctica porque ayudó al desarrollo de la implementación y a la seguridad en el intercambio de información. Los resultados obtenidos permitieron encontrar soluciones concretas a los problemas de compartimiento de recursos informáticos, que afectaban la transmisión de la información y protección de servicios informáticos. Con tales resultados se obtuvo la posibilidad de proponer cambios al proceso investigativo y al compartimiento de información actual, aumentando el nivel de resguardo de los bienes informáticos y evitando vulnerabilidades.

La población para realizar el estudio estuvo conformada por 157 estudiantes y 15 docentes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, quienes fueron encuestados.

La Metodología que se utilizó se centró en la investigación experimental para lo cual se requirió el empleo de métodos de investigación tales como el método analítico, método inductivo y el método hipotético-deductivo. Para la recolección de información se utilizó la técnica de la encuesta la cual facilitó el trabajo de campo. Además se requirió de un instrumento para la recolección de información (cuestionario), que fue aplicado a la población antes mencionada.

La presente tesis costa de tres capítulos. El Capítulo I, detalla la Fundamentación Teórica, en donde se da a conocer los conceptos, características y las herramientas necesarias para análisis e implementación de mecanismos de seguridad, las mismas que están basadas en criterios de varios autores que respaldan la presente investigación.

En el Capítulo II, describe el propósito, misión, visión, organigrama estructural de la Institución, así como el análisis e interpretación de los resultados obtenidos en las encuestas aplicadas y su respectiva tabulación para conocer los criterios emitidos por los usuarios involucrados, permitiendo así conocer las necesidades y factibilidad para la realización de la propuesta.

El Capítulo III, contiene la propuesta de la implementación de mecanismos de seguridad para el laboratorio de redes de la Institución, la misma que dará credibilidad del funcionamiento de la implementación y su aplicación se representa en el Manual Técnico.

Finalmente se presentan conclusiones y recomendaciones, en las que se plasman lineamientos elementales y aspectos fundamentales sugeridos en el desarrollo de la investigación.

CAPÍTULO I

1. FUNDAMENTACIÓN TEÓRICA DE MECANISMOS DE SEGURIDAD

1.1. Seguridad Informática

1.1.1. Definición de Seguridad Informática

Para GARCÍA, Alfonso (2011) en su obra Seguridad Informática expresa: "La seguridad informática es un elemento primordial en los sistemas informáticos actuales cuyo objetivo es asegurar la integridad, disponibilidad y privacidad de la información de un sistema informático e intentar reducir las amenazas" (pág. 10).

Para FUNDACIÓN TELEFÓNICA (2012) en su obra Privacidad y Seguridad en la Red establece:

"Las redes digitales han dado lugar a una aproximación virtual y han planteado nuevos retos tanto para la privacidad como para la seguridad. La porosidad y vulnerabilidad de las redes de comunicación y la facilidad con la que quienes poseen intención maliciosa logran acceder a la información sin el permiso del propietario supone nuevos riesgos para los individuos, empresas y naciones, y al mismo tiempo añade una nueva dimensión a cualquier esfuerzo por preservar la privacidad individual" (pág. 48).

Para CANCELO, Pablo (2007) en su obra Comunicación, Tecnología y su Nomenclatura expresa: “La privacidad siempre estará en peligro sin la seguridad adecuada, pero una mejor seguridad en sí misma no protegerá la privacidad. La información personal puede explotarse sin el permiso o conocimiento del propietario en el nuevo entorno digital” (pág. 133)

De acuerdo a lo anteriormente mencionado se puede decir que la propagación de la información y las redes de comunicación implica que exista un mayor conocimiento de seguridades y por ende una mayor privacidad. Para crear confianza es necesario progresar tanto en la protección de la privacidad como en la información.

1.2. Sistemas Operativos

1.2.1. Windows Server 2012

MICROSOFT CORPORATION (2013). Extraído el 27 de noviembre de 2013, de http://blogs.technet.com/b/ccaitpro/archive/2012/09/04/windows-server-2012.aspx

Windows Server 2012 es el nuevo sistema operativo de Microsoft para servidores. Este sistema ofrece grandes beneficios a proveedores de Hosting y a empresas para realizar sus tareas ya que permite el manejo de escalabilidad y dinamismo.

También para PROYECTO DONO (2008). Extraído el 27 de noviembre de 2013, de http://dono.discapnet.es/contact

Es un sistema operativo de servidor que permite al ordenador manejar funciones de red como servidor de impresión, controlador de dominio, servidor web y servidor de archivos. También es la plataforma para aplicaciones de servidor separado.

Luego de analizar lo establecido anteriormente se puede decir que Windows Server 2012 es la última versión lanzada por Microsoft del sistema operativo Windows server con mejores características de red y grandes capacidades que reduce costos y simplifica tareas de gestión.

1.2.1.1. Características de Windows Server

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

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

Considerando lo anteriormente detallado se puede deducir que Windows Server 2012 ofrece una solución de compatibilidad y rendimiento. Además proporciona interoperabilidad y administración mejorada en eficiencia y calidad.

1.2.2. *Windows Seven*

APRENDE LIBRE (2013). Extraído el 27 de noviembre de 2013, de http://blogs.technet.com/b/ccaitpro/archive/2012/09/04/windows-server-2012.aspx

Es un sistema operativo que le permite al computador administrar los programas y realizar tareas básicas, su Interface Gráfica para el Usuario (GUI) que permite interactuar visualmente con las funciones del equipo de una manera lógica, divertida y fácil.

También para ALEGSA (2013). Extraído el 27 de noviembre de 2013, de http://sistemaoperativowin7.blogspot.com/

Es una actualización incremental del núcleo NT 6.0, lo cual sirve para mantener cierta compatibilidad con las aplicaciones y hardware.

Luego de analizar lo expuesto anteriormente se puede decir que Windows Seven es un sistema operativo que posee una adecuada interface gráfica de usuario para la correcta manipulación y fácil entendimiento.

1.2.2.1. Características de Windows Seven

Las principales características del sistema operativo Windows Seven son las siguientes:

- Incluye mejoras en el reconocimiento de voz
- Mejoras en el reconocimiento de escritura a mano
- Bajo consumo de memoria
- Previsualizaciones interactivas y útiles.
- Detección más rápida de dispositivos USB.

- Mejor desempeño en procesadores multi-nucleo.
- Permite ejecutar aplicaciones que solo están permitidos por el Administrador del Sistema
- Es más rápido el arranque y el sistema en general.
- Se eliminó la cartelería de seguridad de permiso
- Acelera el acceso a imágenes, canciones, sitios web y documentos favoritos

Según lo establecido anteriormente se pude decir que el sistema operativo Windows Seven brinda una mayor flexibilidad a los usuarios, incorpora mayores beneficios, además es más ligero y rápido en comparación a su antecesor.

1.3. Redes Informáticas

LÓPEZ, José (2005) en su obra Informática y Comunicaciones para la Empresa expresa: "Una red informática es un conjunto de máquinas que se interconectan entre si por algún medio físico y cuyo cometido es facilitar el intercambio de información entre diferentes emisores y receptores" (pág. 142).

También BIELER, Juansa (2006), Extraído el 10 de junio del 2013, de http://juansallopis.wordpress.com/2006/01/09/recursos-compartidos

"Las redes informáticas ofrecen a los usuarios acceso a archivos y carpetas. Los usuarios pueden conectar con el recurso compartido por la red y acceder a aplicaciones y datos públicos del usuario".

De acuerdo a lo anteriormente mencionado se puede decir que una red informática es el mejor servicio para el acceso e intercambio de información. Mediante este sistema de comunicación los usuarios alojados pueden compartir archivos, enviar y recibir documentos e información sin importar la cantidad.

1.3.1. Topología Infraestructura

Para ENGLS, Adams (2008) en su obra Introducción a Redes Inalámbricas expresa: “La Topología Infraestructura es aquella en la cual existe un nodo central que sirve de enlace para todos los demás (Tarjetas de Red Wifi)” (pág. 345)

También MOLINER, Francisco (2005) en su obra Informáticos Generalitat Valenciana expresa: “Es aquella que conecta una LAN de cable con una LAN inalámbrica a través de una estación base, denominada punto de acceso. El punto de acceso une la LAN inalámbrica y la LAN de cable y sirve de controlador central de la red LAN inalámbrica” (pág. 77).

De acuerdo a lo expuesto anteriormente se puede decir que una topología infraestructura es la conexión existente entre dos o más computadores con un punto de acceso. Mientras más puntos de acceso obtengan un sistema de recursos compartidos más altos serán los niveles de conectividad entre usuarios.

1.3.2. Redes LAN

Para PÉREZ, María (2005) en su obra La Informática, Presente y Futuro en la Sociedad expresa: “Las redes LAN (Local Area Network) son redes de pocos kilómetros de extensión. Se utilizan para desarrollar un entorno privado extendiéndose por los límites de la propiedad legal constituyéndose en uno de los temas más controvertidos de la industria de comunicaciones” (pág. 165).

También para HERRERA, Enrique (2006) en su obra Tecnologías y Redes de Transmisión de Datos expresa: “Se utilizan para interconectar computadoras que se encuentran dentro de un mismo edificio o campo. Éstas redes operan en la modalidad cliente-servidor” (pág. 121).

De lo expuesto anteriormente se puede decir que una red LAN es la conexión de varias computadoras con el propósito de intercambiar información, capaz de extenderse en un espacio no mayor a 3 kilómetros. Una red LAN prevalece si se trata de varias redes conectadas entre sí, siempre que estas se encuentren colocadas dentro del mismo espacio, edificio o campo.

1.3.2.1. Características Redes LAN

Las principales características de las redes LAN son:

- Cableado específico instalado normalmente a propósito.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Uso de un medio de comunicación privado.
- La simplicidad del medio de transmisión
- Extensión no superior a 3 km
- Gran variedad y número de dispositivos conectados.

Con lo expuesto anteriormente se puede concluir que las redes LAN son medios de comunicación con una simple transmisión de información que alcanzan cortas distancias en comparación a la gran variedad de redes de comunicación.

1.3.3. Redes WLAN

Para RAY, Jimmy (2010) en su obra Acrónimos con la Tecnología Inalámbrica expresa: “Una red de área local inalámbrica WLAN (Wireless Local Area Network) utiliza ondas de radio para conectar dispositivos, como equipos portátiles, a Internet y a la red de su empresa y sus aplicaciones” (pág. 134).

También ZAPATA, Antonio (2011) Extraído el 11 de julio del 2013, de http://antonioza.blogspot.com

Es una red en la que dos o más terminales se pueden comunicar sin la necesidad de una conexión por cable. Es también una red de ordenadores que puede verse en la práctica como un cable Ethernet pero por vía radio.

Conforme el criterio grupal una red inalámbrica, es aquella que conecta a dos o más dispositivos remotos utilizando ondas de radio, permitiendo que se conecten sin dificultad, ya sea que se encuentren a unos metros de distancia como a varios kilómetros. La instalación de redes WLAN no requieren de ningún cambio significativo en la infraestructura.

1.3.3.1. Características redes WLAN

Las principales características de las redes WLAN son las siguientes:

- Red sin cables.
- Ofrecen comodidad y libertad de movimiento
- Red de alta velocidad
- Necesita de una fuerte seguridad para evitar accesos no deseados
- Facilidad y rapidez en la instalación
- Costo de propiedad reducido
- Flexibilidad de trabajar cuándo y dónde lo deseen
- Mayor escalabilidad de la red
- Utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado

Según los fundamentos anteriormente expuestos se puede decir que una red inalámbrica proporciona la mayor comodidad al usuario ya que ofrece un mejor acceso a la red de comunicación estando a una cierta distancia del lugar de trabajo o estudio, brindándole así información rápida y un amplio espacio para el intercambio de datos.

1.4. Ataques Informáticos

1.4.1. Ataques Internos

Para CORRALES, Luis (2006) en su obra Diseño e Implantación de Arquitecturas Informáticas Seguras expresa: “Es un ataque interno si es realizado desde dentro del sistema u organización, son potencialmente devastadores afectando la capa de enlace. Los posibles atacantes son ex empleados o ex administradores” (pág. 18).

También para CARUA, José (2012) Extraído el 18 de noviembre del 2013, de http://www.slideshare.net/sm2099/tipos-de-ataques-informaticos-17557769

Son más comunes y peligrosos. Los ataques internos son iniciados por alguien con acceso autorizado a la red.

Luego de analizar lo establecido anteriormente se puede decir que los ataques internos son provocados por usuarios no autentificados a la red de comunicación generando grandes problemas en la capa de enlace. Los posibles atacantes suelen ser ex usuarios o ex administradores que anteriormente estaban alojados en la red.

1.4.2. Ataques Externos

Para CORRALES, Luis (2006) en su obra Diseño e Implantación de Arquitecturas Informáticas Seguras expresa: “Ataque externo es cuando se tiene por objetivo aprovechar un servicio para el cual no se está autorizado, conseguir el acceso a un sistema para desarrollar un ataque u obtener información privilegiada” (pág. 18).

También para CARUA, José (2012) Extraído el 18 de noviembre del 2013, de http://www.slideshare.net/sm2099/tipos-de-ataques-informaticos-17557769

Son iniciados por un individuo o grupos trabajando desde afuera de una compañía. Ellos no tienen acceso autorizado al sistema o red de computadoras de dicha compañía.

Considerando lo anteriormente detallado se puede decir que los ataques externos son intrusiones en una red informática que operan externamente y son capaces de eliminar o modificar los datos almacenados en los computadores que forman parte de la red de comunicación.

1.4.3. Sniffing

Para CORRALES, Luis (2006) en su obra Diseño e Implantación de Arquitecturas Informáticas Seguras expresa: “Es una pieza de software o hardware que se conecta a una red informática y supervisa todo el tráfico que pasa por el cable. Permite escuchar las conversaciones entre ordenadores” (pág. 19).

También para GUZMÁN, Sacristán (2010) en su obra Informática Segura expresa: “Se refiere al espionaje del tráfico de una red por parte de una máquina que captura la información aunque vaya dirigida a otras máquinas, filtrando esta información aunque esta vaya dirigida a otras máquinas” (pág. 37).

De acuerdo a la información recopilada se puede decir que el sniffing también conocido como un sistema de captura de datos sin etiquetas, filtra información que se envía a los ordenadores provocando tráfico de red y espionaje.

1.4.4. El Spoofing

Para PACHECO, Federico (2008) en su obra Ethical Hacking expresa: "El spoofing es una técnica utilizada para suplantar la identidad de otro sujeto, que puede ser un usuario, un proceso u otro. Consiste en sustituir la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se suplanta la identidad" (pág. 241).

También para PARDO, Beltrán (2006) en su obra Diseño e Implantación de Arquitecturas Informáticas Seguras expresa: "El atacante crea un contexto engañoso para así engañar a la víctima, el atacante crea un mundo falso pero convincente alrededor de la víctima, de este modo el intruso utiliza un sistema para obtener información de otro" (pág. 43).

Considerando lo detallado anteriormente se puede decir que el spoofing es un ataque el cual suplanta la identidad de un usuario, creando un engaño a la víctima obteniendo información valiosa de otro usuario que anteriormente estuvo alojado en la red de comunicación.

1.4.5. Man in the middle

Para ANDREU, Fernando (2006) en su obra Seguridad en Redes WLAN expresa: "Es un ataque basado en el spoofing que consiste en interponerse entre dos sistemas. Un atacante intercepta y selectivamente modifica los datos de la comunicación para suplantar la identidad de las entidades implicadas en la comunicación" (pág. 40).

También para SARUBBI, Juan (2008) en su obra Seguridad Informática expresa: “Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre partes” (pág. 140).

Luego de recopilar la información necesaria se puede decir que el ataque Man in the middle consiste en interponiéndose en medio de dos sistemas de red con el objetivo de interceptar, leer, insertar y modificar datos para suplantar identidades dentro de la red de comunicación.

1.4.6. Hijacking o Secuestro de sesión

Para CORRALES, Luis (2006) en su obra Diseño e Implantación de Arquitecturas Informáticas Seguras expresa: “El Hijacking Supone una intromisión en una comunicación. Suplanta a uno de los extremos de la comunicación una vez realizado el proceso de autentificación para recoger, falsear o insertar información.

También para PELLEJERO, Izaskun (2005) en su obra Fundamentos y Aplicaciones de Seguridad en redes WLAN expresa: “Consiste en tomar una conexión existente entre dos dispositivos de usuario. Tras monitorizar la red el atacante puede generar tráfico que parezca venir de una de las partes envueltas de la comunicación, robando sesión de los individuos envueltos” (pág. 41).

Luego de analizar lo establecido anteriormente se puede decir que el Hijacking o secuestro de secciones es una amenaza de seguridad que se vale del ataque spoofing, toma el control de una conexión permitiendo inyectar comandos o realizar ataques de denegación de servicio DoS.

1.4.7. Denegación de servicio DoS

Para SIMÓN, Abram (2011) en su obra Catholic Prayers establece: “La Denegación de servicio (DoS) es un incidente en el que se ve privado de un usuario u organización de los servicios de un recurso que normalmente se espera tener. La pérdida de servicio es la incapacidad de un servicio de red en particular, la pérdida temporal de toda la conectividad de red y servicios” (pág. 21).

También para STAFF, Users (2011) en su obra Hacking establece: “Es una acción iniciada por un sujeto que busca saturar algún tipo de recurso, ya sea hardware, software o ambos dentro de un determinado sistema. Estos recursos son memoria, capacidad de procesamiento, conexiones de red o disco duro” (pág. 106).

En función de esto se puede decir que la Denegación de Servicio DoS inutiliza la red para que los usuarios no puedan acceder a ella provocando la perdida de la conectividad de la red.

1.5. Mecanismos de Seguridad

1.5.1. Definición de mecanismos de seguridad

Para AGUILERA, Purificación (2010) en su obra Seguridad Informática y Comunicaciones expresa: “Los mecanismos de seguridad se corresponden con un conjunto de mecanismos, estándares, protocolos y recomendaciones orientados a proteger dispositivos, infraestructuras, servicios y recursos de la red de posibles ataques” (pág. 17).

También para STALLINGS, William (2005) en su obra Seguridad Informática y Comunicaciones expresa: “Es una técnica o herramientas que se utilizan para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático” (pág. 9).

De acuerdo a lo anteriormente mencionado se puede decir que los mecanismos de seguridad son herramientas viables que ayudan al control, integridad, confidencialidad, y seguridad de la información transferida en las redes de comunicación.

1.5.2. Mecanismo WEP (Wired Equivalet Piracy)

Para MÉNDEZ, Alyk (2013) Extraído el 17 de julio del 2013, de http://configuracionparametros.blogspot.com/2013_04_01_archive.html

WEP es un mecanismo estándar de cifrado de datos que proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la información.

También para ANDREU, Fernando (2006) en su obra Seguridad en redes WLAN expresa: “Es el primer mecanismo de seguridad que se implementó bajo el estándar de redes inalámbricas IEEE 802.11x para codificar los datos que se transfieren a través de una red inalámbrica” (pág. 12).

De acuerdo a la información consultada se puede decir que WEP es un mecanismo de seguridad para codificar datos, controla y evita que usuarios no registrados accedan a la red de comunicación.

1.5.2.1. Inconvenientes WEP

- El algoritmo de cifrado que emplea ha sido vulnerado.
- El protocolo WEP no fue creado por expertos en seguridad o criptografía.

1.5.2.2. Ventajas de WEP

Las principales ventajas del mecanismo de seguridad WEP son:

- Bajo coste
- Fácil de gestionar (Si no se cambian las claves)
- Se pueden definir perfiles de usuario que permiten el control de acceso para usuarios corporativos e invitados (visitantes).

1.5.2.3. Características de WEP

Las principales características del mecanismo de seguridad WEP son:

- Asegurar la confidencialidad de los datos intercambiados
- Autentificación de clave compartida
- Control de acceso en redes WLAN,
- Utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso.

Luego de haber recopilado la información se puede decir que el mecanismo WEP permite la autenticidad, confidencialidad y control de seguridad en el acceso a la red pero su algoritmo de cifrado ha sido vulnerado por lo que no permite una confidencialidad de seguridad estable.

1.5.3. Mecanismo WPA (Wi-Fi Protected Access)

Para HERNANDO, Roberto (2011) en su obra Seguridad en Redes Inalámbricas expresa: “WPA es un preestándar que utiliza una encriptación mejorada mediante TKIP (Temporal Key Integrity Protocol)” (pág. 18).

También para ANDREU, Fernando (2006) en su obra Seguridad en redes WLAN expresa: “Es un estándar desarrollado por la Wi-Fi Alliance, basado en un borrador del estándar IEEE 802.11i, para mejorar el nivel de codificación existente en WEP así como para incorporar un método de autenticación”. (pág. 12)

Luego de analizar lo establecido anteriormente se puede decir que el WPA es un mecanismo de seguridad desarrollado para corregir falencias del mecanismo existente WEP así como para mejorar los métodos de autenticación y encriptación.

1.5.3.1. Características de WPA

- Distribución dinámica de claves
- Utilización más robusta del vector de inicialización (mejora de la confidencialidad)
- Nuevas técnicas de integridad y autenticación (aplicable en entornos residenciales y empresariales).
- Actualización de equipamiento radio a WPA mediante software.

Considerando lo antes expuesto se puede decir que las características del mecanismo de seguridad WPA permiten la integración de herramientas de autenticación, con un enfoque de facilidad de aplicación y utilización en la red de comunicación. Al igual que el mecanismo de seguridad WEP su algoritmo de cifrado de red ha sido vulnerado, por ello se considera inseguro.

1.5.4. Mecanismo WPA2 (Wi-Fi Protected Access 2)

Para ANDREU, Fernando (2006) en su obra Seguridad en redes WLAN expresa: "Es la Implementación aprobada por Wi-Fi Alliance interoperable con IEEE 802.11i. El grupo WPA2 de la Wi-Fi Alliance es el grupo de certificación del estándar IEEE 802.11, para lo cual se basa en las condiciones obligatorias del estándar". (pág. 18).

También para FALCÓN, Guillermo (2007) Extraído el 13 de diciembre del 2013, de http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa

WPA2 necesita el estándar avanzado de cifrado AES, aporta seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal para el cifrado de los datos.

Luego de analizar lo establecido anteriormente se puede decir que WPA2 es la mejora del WPA ampliando nuevas características y mejoras al control de acceso y autentificación de usuarios.

1.5.4.1. Características de WPA2

El mecanismo WPA2 posee las siguientes características:

- Reemplazo del algoritmo Michael por un código de autenticación considerado criptográficamente seguro.
- Reemplazo del algoritmo RC4 por AES, uno de los más seguros actualmente.

De acuerdo a lo anteriormente mencionado se puede indicar que el mecanismo de seguridad WPA2 consta de un algoritmo de seguridad reemplazado y mejorado en relación al mecanismo WEP y WPA, siendo así un mecanismo más seguro.

1.5.5. EAP (Extensible Authentication Protocol)

Para ANDREU, Fernando (2006) en su obra Seguridad en Redes WLAN expresa: “EAP es el protocolo de autenticación para llevar a cabo tareas de AAA que define las credenciales necesarias para la autenticación de usuarios” (pág. 10).

También para JEAN, Marc (2005) en su obra Seguridad en la Informática de Empresa expresa: “Es una autenticación framework usada habitualmente en redes WLAN. La utilización de EAP es más frecuentemente en WLAN que en LAN”. (pág. 112).

Luego de haber recopilado la información necesaria se puede decir que EAP es un protocolo de seguridad para la conexión en redes WLAN y LAN que permite generar credenciales para la debida autenticación de usuarios. Además puede soportar solamente un paquete en la transmisión de información

1.5.6. Estándar 802.11

Para ANDREU, Fernando (2006) en su obra Seguridad para Redes WLAN expresa: “El IEEE 802.11 se diseñó para sustituir a las capas físicas y MAC. Lo único que se diferencia una WiFi de una red Ethernet es en cómo se tramiten las tramas o paquetes de datos” (pág. 63).

También GARCÍA, Francisco (2011) en su obra Video vigilancia usando Videos IP expresa: “Se utiliza radiofrecuencia en las bandas sin licencia de radiofrecuencia por las capas física y la subcapa MAC de enlaces inalámbricos” (pág. 137).

Luego de analizar lo establecido anteriormente se puede decir que el estándar IEEE 802.11 sirve para el control de acceso a la red, evita el acceso de un ordenador o dispositivos remotos no autorizados, permitiendo a los usuarios registrados en su sistema de red, un mayor servicio y entrega de su información.

1.5.7. IPSec (Internet Protocol Security)

Para ANDREU, Fernando (2006) en su obra Seguridad en Redes WLAN expresa: “IPSec es el marco de estándares abiertos para asegurar comunicaciones privadas sobre redes IP” (pág. 10).

También para MATHON, Philippe (2005) en su obra Windows Server 2003 Network Infrastructures expresa: “Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos” (pág. 501).

Luego de analizar lo expuesto anteriormente se puede decir que IPSec es un conjunto de protocolos que favorecen la seguridad de comunicación en las redes informáticas, controlando el acceso a la información y autenticación de usuarios.

1.5.7.1.Beneficios del IPSec

Los principales beneficios que ofrece el mecanismo de seguridad IPSec son:

- Confidencialidad por autenticación digital y encriptación de paquetes
- Confidencialidad limitada del flujo de trafico
- Prevención contra ataques de repetición de tramas
- Autenticación al inicio y durante la comunicación
- Integridad de direcciones IP
- Buen control de acceso

Según lo antes establecido se puede decir que el mecanismo de seguridad IPSec brinda beneficios a los usuarios mediante su confiabilidad de información al inicio y durante una comunicación a través de la autenticación de usuarios.

1.5.7.2.Características del IPSec

Las principales características del mecanismo de seguridad IPSec son:

- Claves basadas en criptografía
- Administración automática de claves
- Negociación de seguridad automática
- Seguridad a nivel de red
- Autenticación mutua entre los agentes en el comienzo de la sesión
- Carácter de estándar abierto
- Integración de algoritmos criptográficos
- Permite definir diferentes perfiles de usuario.
- Reutilización de la VPN fuera del entorno corporativo

De acuerdo a lo expuesto se puede mencionar que el mecanismo IPSec aporta seguridad a nivel de red por medio de la integración de algoritmos, los mismos que se encuentran formados por una lista específica de filtros y reglas de seguridad.

1.5.7.3.Protocolos IPSec

Está formada por Authentication Header y Encapsulating Segurity Payload.

1.5.7.3.1. Protocolo AH

Para PÉREZ, Santiago (2011) en su obra Análisis del Protocolo IPSec establece: "El protocolo AH es el procedimiento para garantizar la integridad y autenticación de los datagramas IP. Proporciona un medio al receptor de paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados" (pág. 52).

También para ESPAÑA, María (2008) en su obra Servicios Avanzados de Telecomunicación establece: “Este protocolo proporciona integridad de datos, autenticación del origen y, opcionalmente, un servicio destinado a impedir ataques por repetición” (pág. 279).

Luego de analizar lo establecido anteriormente se puede decir que el protocolo AH (Cabecera de Autenticación) proporciona seguridad, garantiza la integridad de datos y su autenticación. Impide que los ataques se realicen por repetición.

1.5.7.3.2. Protocolo ESP

Para ESPAÑA, María (2008) en su obra Servicios Avanzados de Telecomunicación establece: “El protocolo ESP aporta confidencialidad mediante cifrado y ciertas capacidades de protección frente análisis del tráfico. Opcionalmente, ofrece integridad y autenticación del origen” (pág. 280).

También para MARTÍNEZ, Jordi (2011) en su obra IPv6, Aspectos Legales del Nuevo Protocolo Internet establece: “Tiene como fin fundamental proporcionar confidencialidad. A tal fin, especifica el modo de cifrar la información que se desea enviar y como este contenido cifrado se incluye en un datagrama IP” (pág. 281).

Luego de analizar lo establecido anteriormente se puede decir que el protocolo ESP (Carga de seguridad encapsulada) es fundamental por su confidencialidad y cifrado de información al momento de enviarla por la red.

1.5.7.4. Modos de trabajo

Es preciso explicar los dos modos de funcionamiento que admite el mecanismo IPSec como lo son el modo transporte y el modo túnel.

1.5.7.4.1. Modo transporte

Para CORPORACIÓN, ORACLE (2010) Extraído el 17 de octubre del 2013, http://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-13/index.html.

El encabezado exterior determina la directiva IPsec que protege el paquete IP interior. IPsec puede aplicar diferentes directivas de modo de transporte entre dos direcciones IP hasta la granularidad de un único puerto. Se aplica en escenarios en los que la comunicación segura debe hacerse de extremo a extremo.

También para ESPAÑA, María (2008) en su obra Servicios Avanzados de Telecomunicación establece: "Un protocolo que opera en Modo Transporte, proporciona protección a los protocolos de las capas superiores". (pág. 53)

En función a lo anteriormente expuesto se puede decir que el modo transporte da protección a protocolos superiores. Cifra y autentifica la carga útil de IP permitiendo un intercambio de cifrado de datos IP del origen hacia el destino.

1.5.7.4.2. Modo túnel

Para MATHON, Philippe (2004) TCP/IP entorno Windows establece: "El modo túnel permite establecer conexiones seguras entre dos redes, cuando las pasarelas no soportan la tecnología de VPN proporcionando protección al paquete IP". (pág. 291)

También para CORPORACIÓN, ORACLE (2010) Extraído el 17 de octubre del 2013, http://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-13/index.html.

El paquete IP interior determina la directiva IPsec que protege su contenido. El modo túnel sólo funciona para los datagramas de IP en IP. El uso de túneles en modo túnel puede ser útil cuando los usuarios se conecten desde casa a un equipo central.

De acuerdo a lo establecido anteriormente se puede decir que el modo túnel es empleado para asegurar conexiones entre dos redes, es útil para la comunicación entre usuarios y equipos locales protegiendo paquetes IP.

1.6. Funciones de Seguridad

1.6.1. Privacidad

Para GALINDO, Marco (2010) en su obra Escaneando la Informática expresa: "Es garantizar que solo las partes autorizadas podrán acceder a un conjunto de datos, tanto en su origen/destino como durante su tráfico por la red" (pág. 90).

También para GARCÍA, Héctor (2006) en su obra Avances en Informática y Sistemas Computacionales expresa: "La privacidad garantiza que solo los usuarios a los que van destinados los datos trasmitidos los comprendan" (pág. 122).

De acuerdo a la información antes mencionada se puede decir que la privacidad es la manera de controlar el acceso a una red de comunicación a usuarios no autorizados evitando amenazas y peligros.

1.6.2. Autenticidad

Para GARCÍA, Héctor (2006) en su obra Avances en Informática y Sistemas Computacionales expresa: "La autenticidad se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mandó o que el mensaje recibido es el que se esperaba" (pág. 122)

También para GALINDO, Marco (2010) en su obra Escaneando la Informática expresa: "Es garantizar la identidad de las partes implicadas en un intercambio de datos" (pág. 90).

En base a lo expuesto anteriormente se puede decir que la autenticidad es la confirmación de haber recibido la información por parte del destinatario que se esperaba.

Luego de haber recopilado la información necesaria se puede decir que la encriptación es el proceso que se realiza para el envío y entendimiento de un texto plano sin ninguna complicación.

1.6.3. Integridad

Para STALLINGS, William (2005) en su obra Fundamentos de Seguridad en Redes expresa: “La seguridad que los datos recibidos son exactamente como los envío una entidad autorizada, no contienen modificación, inserción, omisión, ni repetición” (pág. 12)

También para MONTERO, Antonio (2008) en su obra Informática para Gestión de Empresas establece: “Garantiza que el mensaje no sea modificado por el camino, alterándose el pedido, el importe, el número de cuenta, entre otros” (pág. 135).

Luego de analizar lo establecido anteriormente se puede decir que la integridad es un servicio que asegura los mensajes protegiéndolos para que estos no sean modificados o cambiados.

1.6.4. Cifrado

Para ANDREU, Fernando (2006) en su obra Seguridad en Redes WLAN expresa: “El cifrado es un tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos” (pág. 8).

También ESPAÑA, María (2008) en su obra Servicios Avanzados de Telecomunicación expresa: “Nos permite ocultar el contenido del mensaje para que solo el destinatario final pueda leerlo” (pág. 61).

En base al criterio de los investigadores se puede decir que el cifrado es un impedimento para que usuarios ajenos puedan tener acceso a la información, poniendo en peligro la información confidencial

CAPÍTULO II

1. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

2.1. Entorno de la Universidad Técnica de Cotopaxi

2.1.1. Antecedentes Históricos

En Cotopaxi el anhelado sueño de tener una institución de Educación Superior se alcanza el 24 de enero de 1995. Las fuerzas vivas de la provincia lo hacen posible, después de innumerables gestiones y teniendo como antecedente la Extensión que creó la Universidad Técnica del Norte.

El local de la UNE-C fue la primera morada administrativa; luego las instalaciones del Colegio Luis Fernando Ruiz que acogió a los entusiastas universitarios; posteriormente el Instituto Agropecuario Simón Rodríguez, fue el escenario de las actividades académicas: para finalmente instalar en casa propia, merced a la adecuación de un edificio a medio construir que estaba destinado a ser Centro de Rehabilitación Social. En la actualidad son cinco hectáreas las que forman el campus universitario y 82 las del Centro de Experimentación, Investigación y Producción Salache.

Se ha definido con claridad la postura institucional ante los dilemas internacionales y locales; somos una entidad que por principio defiende la autodeterminación de los pueblos, respetuosos de la equidad de género.

Se rechaza frontalmente la agresión globalizadora de corte neoliberal que privilegia la acción fracasada economía de libre mercado, que impulsa una propuesta de un modelo basado en la gestión privada, o trata de matizar reformas a la gestión pública, de modo que adopte un estilo de gestión empresarial.

En estos 18 años de vida institucional la madurez ha logrado ese crisol emancipador y de lucha en bien de la colectividad, en especial de la más apartada y urgida en atender sus necesidades. El nuevo reto institucional cuenta con el compromiso constante de sus autoridades hacia la calidad y excelencia educativa.

2.1.2. Filosofía Institucional

2.1.2.1. Propósito

Tener profesionales con un perfil que respondan a la realidad social, económica, política, cultural, científica y tecnológica del país; capaz de proyectar sus experiencias en beneficio nacional; diestro en la utilización de herramientas informáticas; diseña, opera, evalúa proyectos y procesos de desarrollo informático, redes de computadoras; es un eficiente administrador informático, capacitado para resolver grandes avances tecnológicos y ponerlos a disposición de la colectividad.

La aceptación indica fundamentalmente que la Universidad está cumpliendo el papel protagónico y el encargado social para lo que fue creada, esto es entregar profesionales sólidamente preparados dentro del plano científico, técnico y humanístico, encaminados a determinar y solucionar los problemas de diferente índole de la sociedad.

Formar profesionales creativos, críticos y humanistas que utilizan el conocimiento Científico – Técnico, mediante la promoción y ejecución de actividades de investigación y aplicaciones tecnológicas para contribuir en la solución de los problemas de la sociedad.

Promover proyectos de investigación para generar ciencia y tecnología, orientados a solucionar los problemas y satisfacer las necesidades del país.

2.1.2.2. Misión

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

2.1.2.3. Visión

"En el año 2015 la carrera de Ingeniería en Informática y Sistemas Computacionales lidera los procesos de formación profesional en el desarrollo de tecnologías de última generación, que le permite alcanzar un sólido reconocimiento social.".

2.1.2.4. Análisis de la Infraestructura Tecnológica del Laboratorio de Redes de la Universidad Técnica de Cotopaxi

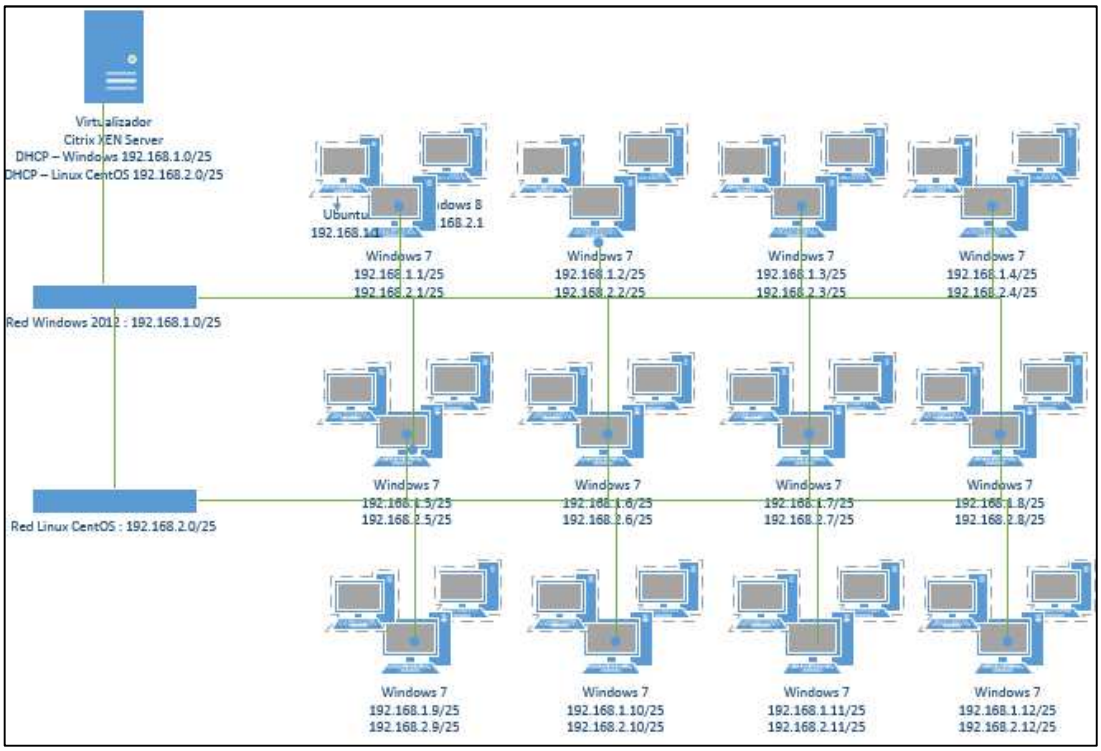
Actualmente el Laboratorio de Redes de la Universidad Técnica de Cotopaxi cuenta con una infraestructura tecnológica suficiente y adecuada para el desarrollo de las actividades de enseñanza; que mediante un sistema integral de gestión le permite garantizar la calidad de sus métodos de aprendizaje y lograr reconocimiento social. Posee una red LAN y WLAN, las mismas que tienen limitaciones tanto para los estudiantes como para los docentes.

Diagrama de la red del Laboratorio de Redes de la Universidad Técnica de Cotopaxi

A continuación se describe en forma general la red LAN existente:

GRÁFICO N° 2.1.

DIAGRAMA DE LA RED LAN Y WLAN



Fuente: Investigadores
Realizado por: Investigadores

2.2 Diseño Metodológico

2.2.1. Métodos de Investigación

2.2.1.1. Método Analítico

HERNÁNDEZ, Santiago (2006) en su obra Metodología de la Investigación manifiesta: “El Método Analítico permite separar alguna de las partes del todo para someterlas a estudio independiente. Posibilita estudiar partes separadas de éste, poner al descubierto las relaciones comunes a todas las partes y, de este modo, captar las particularidades, en la génesis y desarrollo del objeto del todo” (pág. 78).

En esta investigación fue importante utilizar el método analítico ya que se necesitó conocer la naturaleza del fenómeno, y el objeto de que se estudia para comprender la esencia y descomposición de sus elementos.

2.2.1.2. Método Inductivo

Para BERNAL, Augusto (2006) en su obra Metodología de la Investigación argumenta: “El método inductivo es aquel que utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones, cuya aplicación sea de carácter general” (pág. 56).

La utilización del método inductivo fue de suma importancia ya que se partió de razonamientos particulares ya existentes para luego elevarlos a conocimientos generales, obteniendo de esta manera información de gran ayuda para la presente investigación.

2.2.1.3. Método Hipotético Deductivo

Para BERNAL, Augusto (2006) en su obra Metodología de la Investigación argumenta: “El método hipotético deductivo consiste en un procedimiento que parte de unas aseveraciones en calidad de hipótesis y busca refutar o falsear tales hipótesis, deduciendo conclusiones que deben confrontarse con los hechos” (pág. 56).

Cada una de las etapas del mencionado método son aquellas que han permitido desarrollar el tema de investigación ya que se fundamentan en una sola causal, razón por la cual anteriormente se planteó una hipótesis que fue aplicada al desarrollo de la investigación.

2.2.2. Tipos de Investigación

2.2.2.1. Investigación Bibliográfica

Para DE LA MORA, Maurice (2006) en su obra Metodología de la Investigación para el Desarrollo de la Inteligencia argumenta: “La Investigación Bibliográfica es aquella que depende exclusivamente de fuentes de datos secundarios, o sea, aquella información que existe en documentos y material de índole permanente y a la que se puede acudir como fuente de referencia” (pág. 159).

La aplicación de este tipo de investigación facilitó y profundizó los conocimientos adquiridos en el análisis de la investigación, además sirvió como base para fundamentar los datos expuestos otorgándoles confiabilidad y seriedad.

2.2.2.2. Investigación de Campo

Para DE LA MORA, Maurice (2006) en su obra Metodología de la Investigación para el Desarrollo de la Inteligencia argumenta: “La investigación de campo es aquella en la que el mismo objeto de estudio sirve como fuente de información para el investigador, el cual recoge directamente los datos de las conductas observadas” (pág. 96).

La aplicación de la investigación de campo permitió obtener nuevos conocimientos del propio lugar de la investigación, su realidad social y manejar los datos con más seguridad.

2.2.2.3. Investigación Experimental

Para RUIZ, Ramón (2006) en su obra Historia y Evolución del Pensamiento Científico argumenta: “La Investigación Experimental es aquella que se presenta mediante la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas con el fin de descubrir de qué modo o por que causa se produce una situación o fenómeno particular” (pág. 106).

La aplicación de este tipo de investigación permitió realizar pruebas, obtener resultados deseados, confiables y efectivos para el tema de investigación.

2.2.3. Técnicas de Investigación

2.2.3.1. Encuesta

Para VIVALDI, Gonzalo (2006) en su obra Concurso de Redacción Teórica y Práctica manifiesta: “La encuesta es el acopio de datos obtenidos mediante consulta o interrogatorio, sobre cualquier aspecto de la actividad humana” (pág. 409).

Esta técnica de investigación fue dirigida a los estudiantes y docentes de la Universidad Técnica de Cotopaxi para conocer qué tipo de seguridades son utilizadas para aumentar la confiabilidad de la información en una infraestructura de red.

2.2.4. Instrumentos

Se seleccionó un instrumento que ayude a la recolección y manejo de la información y beneficie la realización del tema de investigación por lo que a continuación se menciona el instrumento utilizado.

2.2.4.1. Cuestionario de Encuesta

Para ABASCAL, Elena (2009) en su obra Fundamentos y Técnicas de Investigación argumenta: “El Cuestionario de Encuesta es un conjunto articulado y coherente de preguntas para obtener la información necesaria para poder realizar la investigación que la requiere” (pág. 189).

2.3. Población

La presente investigación se desarrolló tomando en cuenta una muestra de los estudiantes y docentes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

TABLA N° 2.1.

POBLACIÓN

INVOLUCRADOS	CANTIDAD
Docentes	15
Estudiantes	380
TOTAL:	**395**

Fuente: Coordinación de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

Realizado por: Investigadores

2.4. EL MUESTREO

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

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

n= ?

N= Número de población

O= 0.5 varianza

Z= 1.96 nivel de confianza

E= 0.06 error máximo admisible

$$n = \frac{380 * (0.5)^2 * (1.96)^2}{(380-1) * (0.06)^2 + (0.5)^2 * (1.96)^2}$$

$$n = \frac{380 * 0.25 * 3.84}{(380-1) * (0.0036) + (0.25 * 3.84)}$$

$$n = \frac{364.80}{1.3644 + 0.96}$$

$$n = \frac{364.80}{2.3244}$$

$$n = 157$$

TABLA N° 2.2.

MUESTRA

INVOLUCRADOS	POBLACIÓN	MUESTRA
Docentes	15	15
Estudiantes	380	157
TOTAL:	395	172

Fuente: Coordinación de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

Realizado por: Investigadores

2.5. Operacionalización de Variables

TABLA N° 2.3.

OPERACIONALIZACIÓN DE VARIABLES

HIPÓTESIS	VARIABLES	INDICADORES
La implementación de mecanismos de seguridad permitirá un adecuado control de seguridad en el intercambio de información por parte de los estudiantes y docentes de la Universidad Técnica de Cotopaxi.	**V. Dependiente** La implementación de mecanismos de seguridad.	• Confiabilidad • Accesibilidad • Autenticidad • Flexibilidad • Integridad
	V. Independiente Adecuado control de seguridad en el intercambio de información por parte de los estudiantes y docentes de la Universidad Técnica de Cotopaxi.	• Comodidad • Beneficios • Fortificación • Protección • Progreso

Fuente: Investigadores

Realizado por: Investigadores

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

1.- ¿Cree usted que en el laboratorio de redes de la Universidad Técnica de Cotopaxi, exista la debida seguridad en el envío y recepción de información?

TABLA N° 2.4.

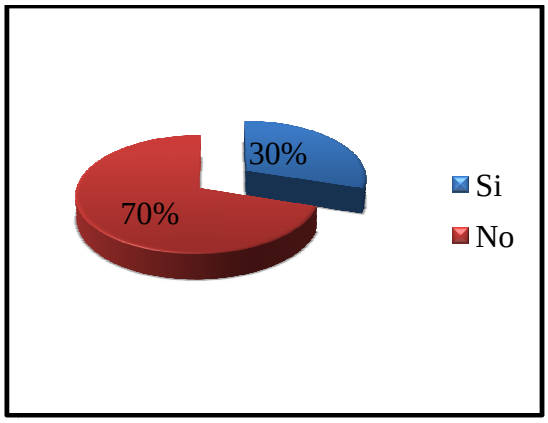
ENVÍO Y RECEPCIÓN DE INFORMACIÓN

OPCIÓN	VALOR	%
Si	47	30
No	110	70
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.2.

ENVÍO Y RECEPCIÓN DE INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 30% que corresponde a 47 encuestados, piensa que en el laboratorio de redes de la Universidad Técnica de Cotopaxi existe la debida seguridad en el envío y recepción de información, mientras que el 70% que corresponde a 110 encuestados opina lo contrario, lo cual sería factible la implementación de seguridades para el envío y recepción de información, beneficiando la comunicación entre los usuarios.

2.- ¿Cómo considera usted la seguridad de información al momento de enviarla o recibirla a través de la red?

TABLA N° 2.5.

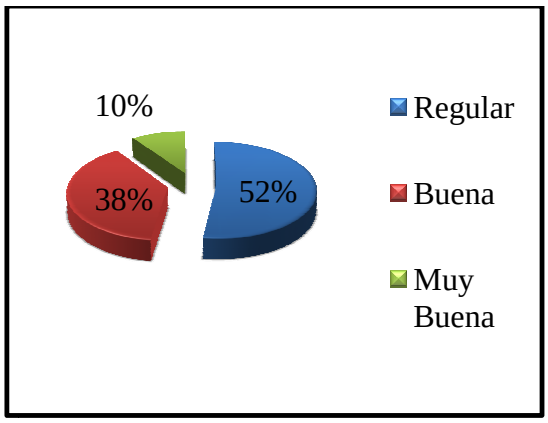
SEGURIDAD DE INFORMACIÓN EN LA RED

OPCIÓN	VALOR	%
Regular	82	52
Buena	60	38
Muy Buena	15	10
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.3.

SEGURIDAD DE INFORMACIÓN EN LA RED



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 52% que corresponde a 82 encuestados, considera que es regular el envío y recepción de información a través de la red, el 38% que corresponde a 60 encuestados considera que es buena, mientras que el 10% que corresponde a 15 encuestados considera que la información enviada y recibida es muy buena, por lo cual es fundamental aumentar la seguridad de información en una red de comunicación.

3.- ¿Conoce usted si el laboratorio de redes de la Universidad Técnica de Cotopaxi posee una herramienta de seguridad que permita la protección de los bienes y servicios informáticos?

TABLA N° 2.6.

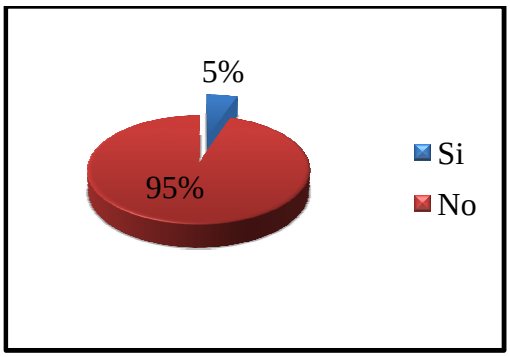
HERRAMIENTA DE SEGURIDAD

OPCIÓN	VALOR	%
Si	8	5
No	149	95
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.4.

HERRAMIENTA DE SEGURIDAD



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 5% que corresponde a 8 encuestados afirma que el laboratorio de redes de la Universidad Técnica de Cotopaxi posee una herramienta de seguridad que permite la protección de los servicios informáticos, mientras que el 95% que corresponde a 149 encuestados opina lo contrario, lo cual sería factible la implementación de una herramienta de seguridad, como lo son los mecanismos de seguridad.

4.- ¿Piensa usted que la información manipulada escrupulosamente puede perjudicar gravemente a la Institución y a los usuarios alojados en la red?

TABLA N° 2.7.

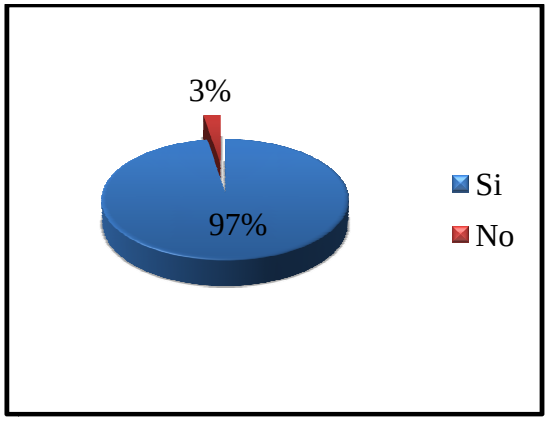
INFORMACIÓN MANIPULADA ESCRUPULOSAMENTE

OPCIÓN	VALOR	%
Si	153	97
No	4	3
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.5.

INFORMACIÓN MANIPULADA ESCRUPULOSAMENTE



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 97% que corresponde a 153 encuestados, piensa que la información manipulada escrupulosamente puede perjudicar a la institución y a los usuarios alojados en la red, mientras que el 3% que corresponde a 4 encuestados piensa lo contrario, lo cual sería necesario la implementación de seguridades para proteger el compartimiento de información.

5.- ¿Considera usted que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasladar información?

TABLA N° 2.8.

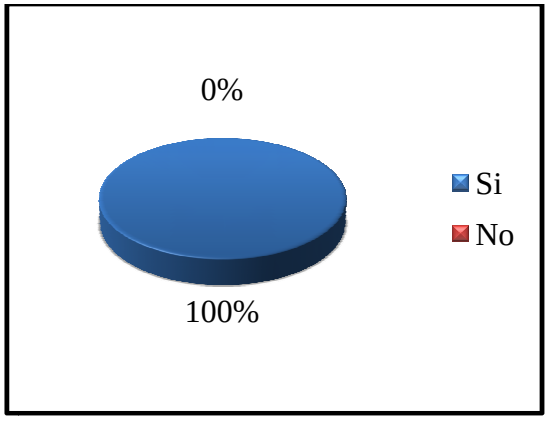
SEGURIDAD Y CONFIABILIDAD DE INFORMACIÓN

OPCIÓN	VALOR	%
Si	157	100
No	0	0
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.6.

SEGURIDAD Y CONFIABILIDAD DE INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 157 encuestados, considera que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasladar información, mientras que el 0% que corresponde a 0 encuestados, considera lo contrario, lo cual sería factible implementar en la infraestructura de red seguridades para prevenirla de daños.

6.- ¿Piensa usted que el laboratorio de redes de la Universidad Técnica de Cotopaxi debería tener mecanismos de seguridad que beneficien la protección de la información?

TABLA N° 2.9.

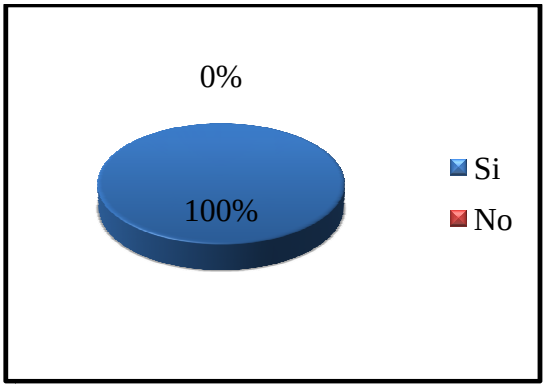
MECANISMOS DE SEGURIDAD

OPCIÓN	VALOR	%
Si	157	100
No	0	0
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.7.

MECANISMOS DE SEGURIDAD



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 157 encuestados, piensa que el laboratorio de redes de la Universidad Técnica de Cotopaxi debería tener mecanismos de seguridad que beneficien la protección de información, mientras que el 0% que corresponde a 0 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad que beneficien la protección de información.

7.- ¿Considera usted que se mejorará la seguridad y confiabilidad de información con la implementación de mecanismos de seguridad en el laboratorio de redes?

TABLA N° 2.10.

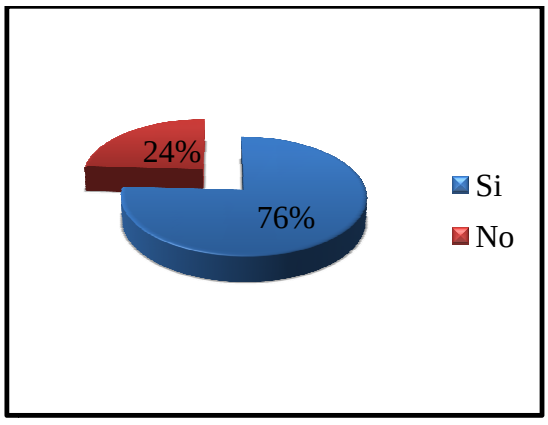
MEJORA DE SEGURIDAD EN LA INFORMACIÓN

OPCIÓN	VALOR	%
Si	119	76
No	38	24
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.8.

MEJORA DE SEGURIDAD EN LA INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 76% que corresponde a 119 encuestados, considera que se mejorará la seguridad y confiabilidad de información con la implementación de mecanismos de seguridad, mientras que el 24% que corresponde a 38 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad para mejorar la seguridad y confiabilidad de información.

8.- ¿Piensa usted que la implementación de mecanismos de seguridad permitirán resguardar la seguridad y evitar vulnerabilidades?

TABLA N° 2.11.

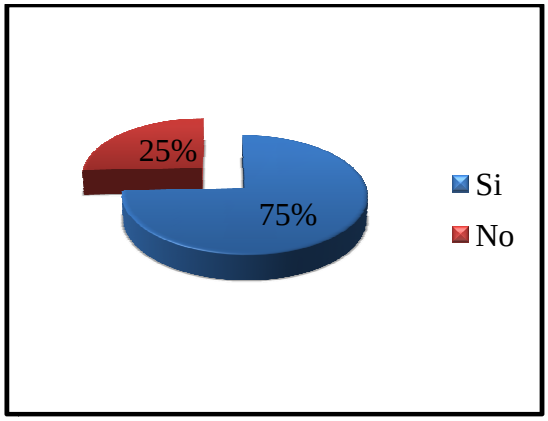
RESGUARDO DE SEGURIDAD

OPCIÓN	VALOR	%
Si	117	75
No	40	25
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.9.

RESGUARDO DE SEGURIDAD



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 75% que corresponde a 117 encuestados, piensa que la implementación de mecanismos de seguridad permitirá resguardar la seguridad y evitar vulnerabilidades, mientras que el 25% que corresponde a 40 encuestados, considera lo contrario, lo cual sería útil implementar mecanismos de seguridad para resguardar la seguridad y evitar vulnerabilidades.

9.- ¿Le gustaría gozar de una comunicación y compartimiento de archivos seguros, sin que dicha información con otro usuario sea vulnerada o alterada?

TABLA N° 2.12.

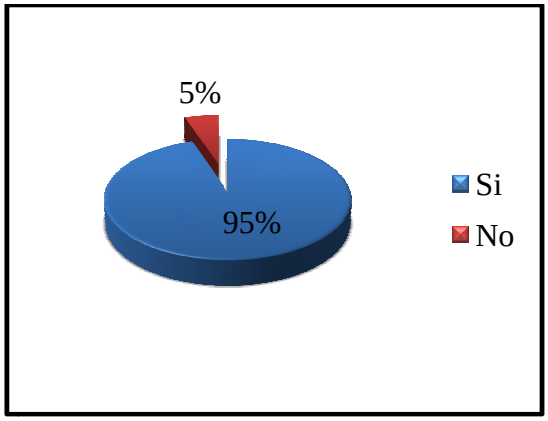
COMUNICACIÓN Y COMPARTIMIENTO SEGURO

OPCIÓN	VALOR	%
Si	149	95
No	8	5
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.10.

COMUNICACIÓN Y COMPARTIMIENTO SEGURO



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 95% que corresponde a 149 encuestados, le gustaría gozar de una comunicación y compartimiento de archivos seguros, mientras que el 5% que corresponde a 8 encuestados considera lo contrario, lo cual sería favorable implementar seguridades para que los usuarios gocen de una comunicación y compartimiento de archivos sin vulneración o alteración.

10.- ¿Estaría usted de acuerdo que se implementen mecanismos de seguridad para fortalecer la confidencialidad e integridad de la información?

TABLA N° 2.13.

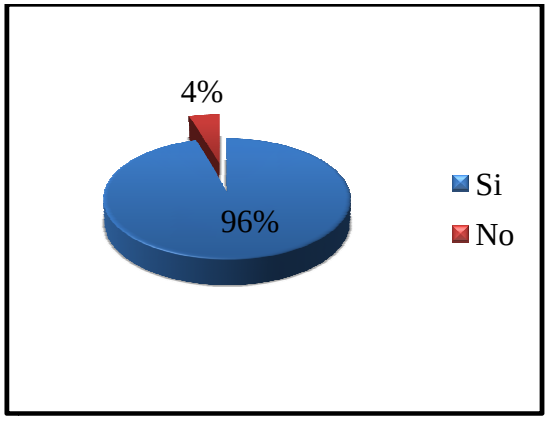
CONFIDENCIALIDAD E INTEGRIDAD

OPCIÓN	VALOR	%
Si	150	96
No	7	4
TOTAL	**157**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.11.

CONFIDENCIALIDAD E INTEGRIDAD



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 96% que corresponde a 150 encuestados, está de acuerdo que se implementen mecanismos de seguridad para fortalecer la confidencialidad, integridad y/o disponibilidad de un sistema informático, mientras que el 4% que corresponde a 7 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad en el laboratorio de redes de la Universidad Técnica de Cotopaxi.

2.7. Análisis e interpretación de resultados de las encuestas dirigidas a los docentes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

1.- ¿Cree usted que en el laboratorio de redes de la Universidad Técnica de Cotopaxi, exista la debida seguridad en el envío y recepción de información?

TABLA N° 2.14.

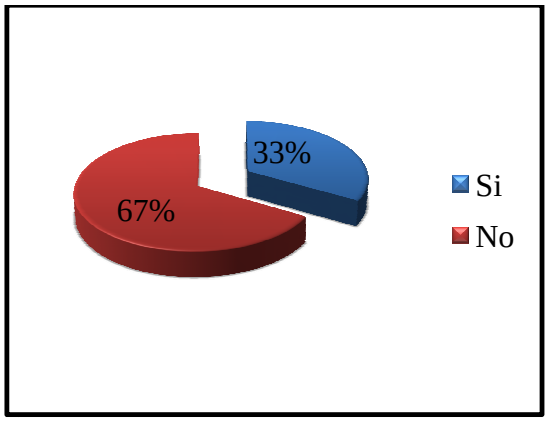
SEGURIDAD EN EL ENVÍO DE INFORMACIÓN

OPCIÓN	VALOR	%
Si	5	33
No	10	67
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.12.

SEGURIDAD EN EL ENVÍO DE INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 33% que corresponde a 5 encuestados, piensa que en el laboratorio de redes de la Universidad Técnica de Cotopaxi existe la debida seguridad en el envío y recepción de información, mientras que el 67% que corresponde a 10 encuestados opina lo contrario, lo cual sería factible la implementación de seguridades para el envío y recepción de información, beneficiando la comunicación entre los usuarios.

2.- ¿Cómo considera usted la seguridad de información al momento de enviarla o recibirla a través de la red?

TABLA N° 2.15.

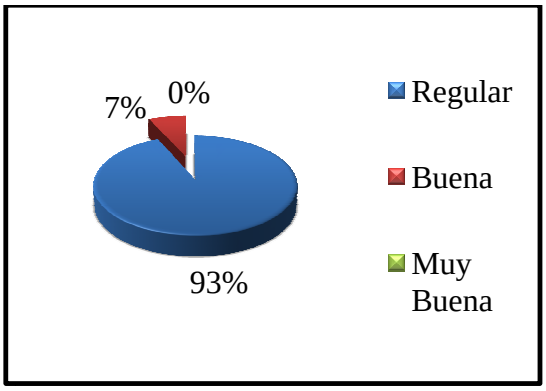
SEGURIDAD DE INFORMACIÓN

OPCIÓN	VALOR	%
Regular	14	93
Buena	1	7
Muy Buena	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.13.

SEGURIDAD DE INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 93% que corresponde a 14 encuestados, considera que es regular el envío y recepción de información a través de la red, el 7% que corresponde a 1 encuestados considera que es buena, mientras que el 0% que corresponde a 0 encuestados considera que la información enviada y recibida es muy buena, por lo cual es fundamental aumentar la seguridad de información en una red de comunicación.

3.- ¿Conoce usted si el laboratorio de redes de la Universidad Técnica de Cotopaxi posee una herramienta de seguridad que permita la protección de los bienes y servicios informáticos?

TABLA N° 2.16.

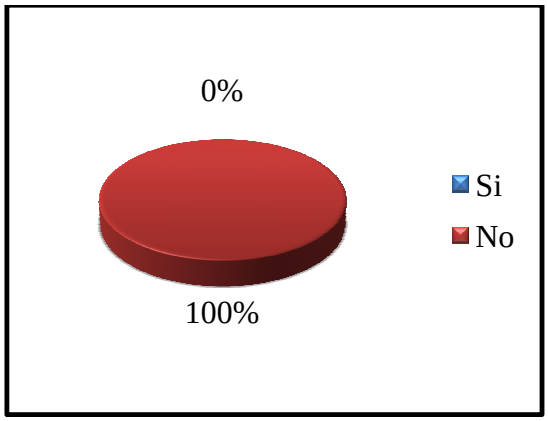
PROTECCIÓN DE SERVICIOS INFORMÁTICOS

OPCIÓN	VALOR	%
Si	0	0
No	15	100
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.14.

PROTECCIÓN DE SERVICIOS INFORMÁTICOS



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 0% que corresponde a 0 encuestados afirma que el laboratorio de redes de la Universidad Técnica de Cotopaxi posee una herramienta de seguridad que permite la protección de los servicios informáticos, mientras que el 100% que corresponde a 15 encuestados opina lo contrario, lo cual sería factible la implementación de una herramienta de seguridad, como lo son los mecanismos de seguridad.

4.- ¿Piensa usted que la información manipulada escrupulosamente puede perjudicar gravemente a la Institución y a los usuarios alojados en la red?

TABLA N° 2.17.

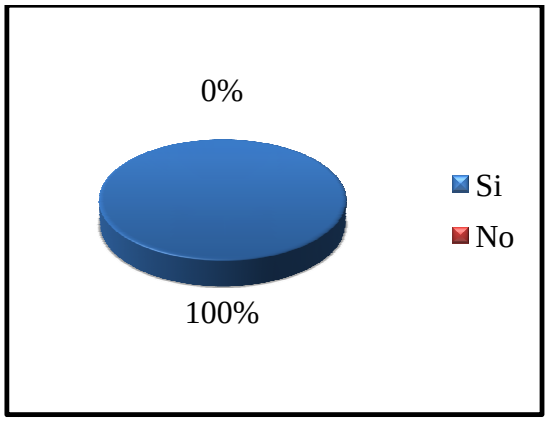
INFORMACIÓN MANIPULADA

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.15.

INFORMACIÓN MANIPULADA



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, piensa que la información manipulada escrupulosamente puede perjudicar a la institución y a los usuarios alojados en la red, mientras que el 0% que corresponde a 0 encuestados piensa lo contrario, lo cual sería necesario la implementación de seguridades para proteger el compartimiento de información.

5.- ¿Considera usted que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasladar información?

TABLA N° 2.18.

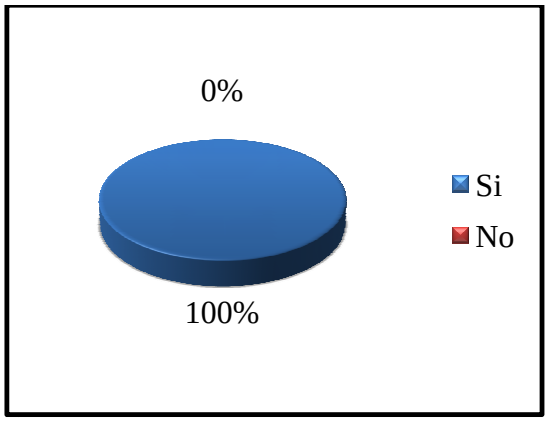
TRASLADO DE INFORMACIÓN

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.16.

TRASLADO DE INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, considera que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasladar información, mientras que el 0% que corresponde a 0 encuestados, considera lo contrario, lo cual sería factible implementar en la infraestructura de red seguridades para prevenirla de daños.

6.- ¿Piensa usted que el laboratorio de redes de la Universidad Técnica de Cotopaxi debería tener mecanismos de seguridad que beneficien la protección de la información?

TABLA N° 2.19.

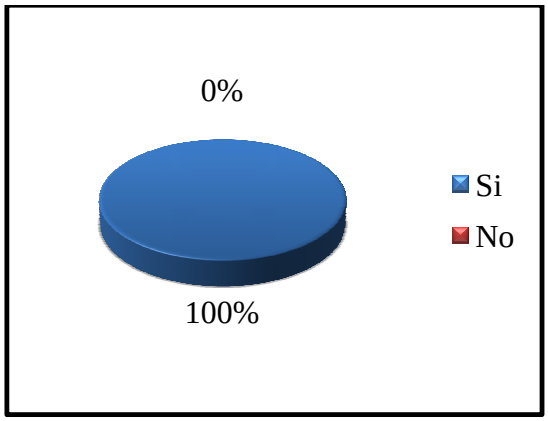
PROTECCIÓN DE LA INFORMACIÓN

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.17.

PROTECCIÓN DE LA INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, piensa que el laboratorio de redes de la Universidad Técnica de Cotopaxi debería tener mecanismos de seguridad que beneficien la protección de información, mientras que el 0% que corresponde a 0 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad que beneficien la protección de información.

7.- ¿Considera usted que se mejorará la seguridad y confiabilidad de información con la implementación de mecanismos de seguridad en el laboratorio de redes?

TABLA N° 2.20.

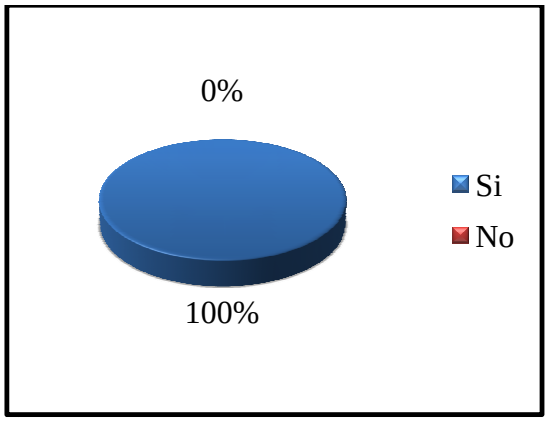
SEGURIDAD EN EL LABORATORIO DE REDES

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.18.

SEGURIDAD EN EL LABORATORIO DE REDES



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, considera que se mejorará la seguridad y confiabilidad de información con la implementación de mecanismos de seguridad, mientras que el 0% que corresponde a 0 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad para mejorar la seguridad y confiabilidad de información.

8.- ¿Piensa usted que la implementación de mecanismos de seguridad permitirán resguardar la seguridad y evitar vulnerabilidades?

TABLA N° 2.21.

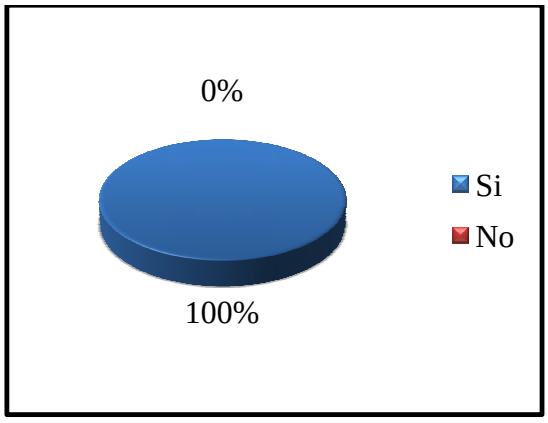
EVITAR VULNERABILIDADES

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.19.

EVITAR VULNERABILIDADES



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, piensa que la implementación de mecanismos de seguridad permitirá resguardar la seguridad y evitar vulnerabilidades, mientras que el 0 que corresponde a 0 encuestados, considera lo contrario, lo cual sería útil implementar mecanismos de seguridad para resguardar la seguridad y evitar vulnerabilidades.

9.- ¿Le gustaría gozar de una comunicación y compartimiento de archivos seguros, sin que dicha información con otro usuario sea vulnerada o alterada?

TABLA N° 2.22.

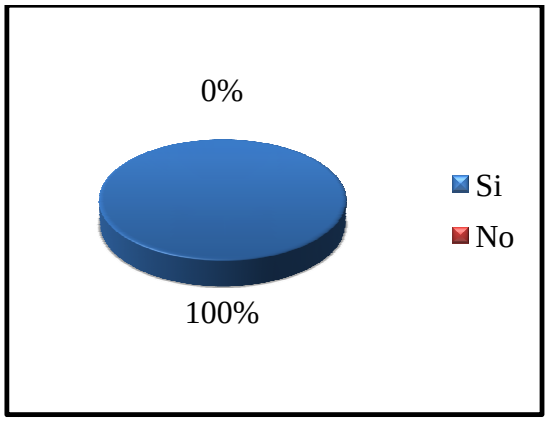
COMUNICACIÓN SEGURA

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.20.

COMUNICACIÓN SEGURA



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, le gustaría gozar de una comunicación y compartimiento de archivos seguros, mientras que el 0% que corresponde a 0 encuestados considera lo contrario, lo cual sería favorable implementar seguridades para que los usuarios gocen de una comunicación y compartimiento de archivos sin vulneración o alteración.

10.- ¿Estaría usted de acuerdo que se implementen mecanismos de seguridad para fortalecer la confidencialidad e integridad de la información?

TABLA N° 2.23.

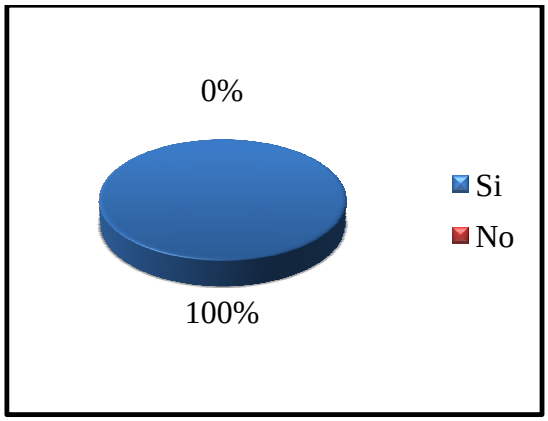
CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN

OPCIÓN	VALOR	%
Si	15	100
No	0	0
TOTAL	**15**	**100**

Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

GRÁFICO N° 2.21.

CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN



Fuente: Técnica de encuesta UTC
Realizado por: Investigadores

ANÁLISIS E INTERPRETACIÓN

De la población encuestada, el 100% que corresponde a 15 encuestados, está de acuerdo que se implementen mecanismos de seguridad para fortalecer la confidencialidad, integridad y/o disponibilidad de un sistema informático, mientras que el 0 % que corresponde a 0 encuestados considera lo contrario, lo cual sería factible implementar mecanismos de seguridad en el laboratorio de redes de la Universidad Técnica de Cotopaxi.

2.8. Verificación de la Hipótesis

La hipótesis planteada en el anteproyecto de tesis fue la siguiente: “La implementación de mecanismos de seguridad permitirá un adecuado control de seguridad en el intercambio de información por parte de los estudiantes y docentes de la Universidad Técnica de Cotopaxi”.

Con miras a comprobar la hipótesis se realizó la técnica de la encuesta y sus respectivos cuestionarios. Los resultados obtenidos fueron analizados e interpretados anteriormente, tomando la tabulación de los datos de la siguiente manera:

El 100% del personal docente como estudiantil consideran que una infraestructura de red debe poseer mayor seguridad y confiabilidad al momento de trasladar información, el 100% tanto del personal docente como del estudiantil piensa que la infraestructura de red del laboratorio de redes de la Universidad Técnica de Cotopaxi debería tener mecanismos de seguridad que beneficien la protección de la información y el 100% del personal docente está de acuerdo con la implementación de mecanismos de seguridad para fortalecer la confidencialidad e integridad de la información, con dichos resultados se pudo verificar que la hipótesis es verdadera, lo que hace necesario la implementación de mecanismos de seguridad para contrarrestar la infraestructura crítica, asegurar la red, proporcionar integridad y brindar confiabilidad de información a los usuarios alojados en la red de comunicación.

CAPÍTULO III

IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR INFRAESTRUCTURAS CRÍTICAS FRENTE ATAQUES INFORMÁTICOS EN EL LABORATORIO DE REDES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

3.1. Presentación

El presente capitulo está destinado a resolver los problemas de seguridad, así como asegurar la información privada de todos los usuarios alojados en la red de comunicación del laboratorio de redes de la Universidad Técnica de Cotopaxi. Además brindar a los usuarios adscritos en dicha red la mayor confiabilidad en el envío y recepción de información.

Se ha procedido a investigar las maneras de proteger los bienes informáticos de ataques realizados por usuarios ajenos a la red de comunicación. Una vez obtenido el estudio de las necesidades que afectan a los usuarios de la red de comunicación y el problema, se analizó los ataques más frecuentes en las redes de comunicación así como las características y beneficios de cada mecanismo de seguridad.

La implementación de mecanismos de seguridad brinda confiabilidad, integridad, confidencialidad, acceso rápido y seguro a las redes de comunicación, y permite a los usuarios que acceden a dicha red aprovechar todos los recursos informativos que poseen sin ninguna limitación y de esta manera pueden gozar de una comunicación directa y segura.

Los mecanismos de seguridad previenen y fortalecen la confiabilidad de información creando un ambiente adecuado para la utilización de todos los bienes informáticos, aumentando el nivel de resguardo evitando vulnerabilidades.

3.2. Objetivos

3.2.1. Objetivo General

Implementar mecanismos de seguridad para contrarrestar infraestructuras críticas frente ataques informáticos en el laboratorio de redes de la Universidad Técnica de Cotopaxi, ubicado en la ciudad de Latacunga, provincia de Cotopaxi.

3.2.2. Objetivos Específicos

- Recopilar la información necesaria para conocer las vulnerabilidades y seguridades en la transmisión de datos de los bienes informáticos.

- Analizar la documentación relacionada con los mecanismos de seguridad para saber las necesidades que tienen los usuarios al momento de intercambiar información.

- Aplicar mecanismos de seguridad que puedan asegurar la confiabilidad, integridad y autenticidad de la información.

3.3. Análisis de Factibilidad

Es conveniente realizar un estudio de factibilidad para determinar la infraestructura tecnológica y la capacidad técnica que involucra la implementación de mecanismos de seguridad, así como los costos, beneficios y el grado de aceptación que la propuesta genera en la Institución. A continuación se describen tres áreas que se tomó en cuenta para el tema de investigación.

3.3.1. Factibilidad Técnica

Las redes informáticas, son consideradas herramientas vitales para la enseñanza de las comunidades, facilitando el acceso a la información y compartimiento de datos de suma importancia. Para esto es necesario que la implementación de dichas redes de comunicación cuenten con la mejor tecnología y seguridad tanto interna como externa, inducida hacia una excelente adecuación y mantenimiento de infraestructura, que contrarreste inseguridades y permitan establecer sus propios servicios y estrategias.

La factibilidad técnica consistió en realizar una evaluación de la tecnología de los bienes informáticos requeridos para el laboratorio de redes de la Universidad Técnica de Cotopaxi, este estudio fue destinado a recolectar información sobre los componentes técnicos adecuados para la implementación de mecanismos de seguridad y poner en marcha la ejecución del proyecto de investigación.

De acuerdo a la tecnología necesaria para la implementación de mecanismos de seguridad en el laboratorio de redes de la Universidad Técnica de Cotopaxi, se evaluó los componentes hardware y software.

Actualmente el Laboratorio de redes cuenta con los siguientes equipos.

TABLA N° 3.1.

FACTIBILIDAD TÉCNICA

HARDWARE	SOFTWARE
Computadoras HP	Sistema operativo Windows Seven
Servidor HP Proliant Gen8	Sistema operativo Windows Server 2012
COMPONENTES DE RED	
Medio de Transmisión (Cableado)	
Switch HP	
Router Cisco	
Tarjetas de red	

Fuente: Investigadores
Realizado por: Investigadores

Con la implementación de mecanismos de seguridad se protege la información, proporcionando confiabilidad e integridad de datos y a la vez se evitan vulnerabilidades. Además permite al administrador de la red corregir errores a tiempo previniendo inconvenientes futuros que puedan agravar la infraestructura y traer consigo grandes costos.

3.3.2. Factibilidad Económica

La información a intercambiar en el laboratorio de redes es de suma importancia y un bien que, como los demás activos, tiene valor para la comunidad universitaria y por ende debe ser propiamente protegida, garantizando la seguridad de los sistemas de información, restando las vulnerabilidades y contribuyendo de este modo, a una mejor gestión en la Universidad.

Los recursos económicos y financieros necesarios para llevar a cabo las actividades son el costo del tiempo, el costo de la realización y el costo de adquirir nuevos recursos.

La responsabilidad de la operación y/o funcionamiento de la implementación no generó inversión debido a que en la Universidad Técnica de Cotopaxi existe el personal docente capacitado, facilitando el desarrollo de la implementación.

3.3.3. Factibilidad Operacional

La visión de la carrera de Ingeniería en Informática y Sistemas Computacionales ha permitido que se implemente un laboratorio de redes cuyo fin es el de mejorar la educación, investigación y servicios. La implementación de mecanismos de seguridad en dicho laboratorio fue en busca de mejorar la calidad de información y la infraestructura tecnológica computacional, con el fin de gozar de una comunicación segura entre usuarios.

Los mecanismos de seguridad cuentan con características que mejoran y facilitan la comunicación, a la ves permiten la manipulación y aprovechamiento por parte de los usuarios, así como la adecuación de la normativa para que los servicios de comunicación ofrecidos a través de esta infraestructura puedan ser suministrados por prestadores no tradicionales, allanando en estos casos los requisitos legales necesarios.

Fue factible operativamente implementar mecanismos de seguridad debido a que estuvieron a disposición los elementos necesarios para el manejo, control de la seguridad y comunicación de equipos. Además existe en la institución el personal técnico capacitado para manejar los equipos que requerirá el sistema.

3.4. Desarrollo de la Propuesta

Para la elaboración e implementación de mecanismos de seguridad se realizó un análisis comparativo de los principales mecanismos de seguridad a implementar en la red de comunicación la cual se presenta a continuación:

3.4.1. Comparación de Mecanismos de Seguridad

Las principales características de mecanismos de seguridad desarrolladas específicamente para dotar de seguridad a redes son:

TABLA N° 3.2.

COMPARACIÓN MECANISMOS DE SEGURIDAD

		WEP	WPA	802.11i	IPsec VPN
Autenticación	Autenticación	WEP	802.1X + EAP	802.1X + EAP	IKE de maquina X-AUTH de usuario
	Pre-autenticación	NO	NO	802.1X (EAPOL)	SI
Cifrado	Negociación del cifrado	NO	SI	SI	SI (DES, 3DES, AES)
	Cifrado	RC4 40-bit o 104-bit	TKIP RC4 128-bit	CCMP AES 128-bit	ESP, DES 56-bit, 3DES 168-bit AES 168, 128, 192.256
	Vector de inicialización	24 bits	48 bits	48 bits	DES-CBC 8 bytes
	Integridad de la cabecera	NO	MIC	CCM	AH
	Integridad de los datos	CRC-32	MIC	CCM	AH/ESP
	Protección de respuesta	NO	Fuerza secuencia de IV	Fuerza secuencia de IV	SI
	Gestión de claves	NO	Basada en EAP	Basada en EAP	IKE (Diffe-Hellman)
	Distribución de clave	Manual	802.1X (EAP)	802.1X (EAP)	Diffe-Hellman
	Clave asignada a:	Red	Paquete, sesión y usuario	Paquete, sesión y usuario	Usuario
	Clave por paquete	Concatenación de IV	Mezclado TKIP	No necesario	ESP
Otros	Seguridad ad-hoc	NO	NO	Si (IBSS)	NO

Fuente: Mecanismos de Seguridad
Realizado por: Investigadores

La comparación de los distintos mecanismos de seguridad se ha realizado con los parámetros de autenticación y cifrado obteniendo varias conclusiones con respecto a su seguridad y vulnerabilidad.

La autenticación WEP se limita a aceptar el tráfico de terminales, en cambio la autenticidad de los demás mecanismos de seguridad es más compleja y robusta.

En cuanto a la autenticación los mecanismos IEEE 802.11i y WPA se asientan en la combinación del estándar IEEE 802.1x con el protocolo EAP, los cuales generan claves de distribución y cifrado.

Los mecanismos de seguridad WEP y WPA utilizan el algoritmo de cifrado RC4, el mismo que ha sido fácilmente vulnerado por ataques informáticos.

La utilización del algoritmo de cifrado diferencia a los mecanismos IEEE 802.11i y WPA ya que el IEEE 802.11i utiliza AES y WPA en cambio el mecanismo WEP utiliza RC4.

IEEE 802.11i y soluciones VPN basadas en IPSec emplean pre-autenticación en diferentes dispositivos para que éstos puedan realizar procesos de autenticación con el punto de acceso seleccionado.

Cuando se emplean mecanismos de seguridad basados en IPSec, la gestión de claves es dinámica, por lo que aumenta la seguridad del sistema y dificulta el descubrimiento de una clave valida.

Luego de hacer un análisis de los principales mecanismos de seguridad se ha optado por implementar el mecanismo IPSec por las siguientes razones:

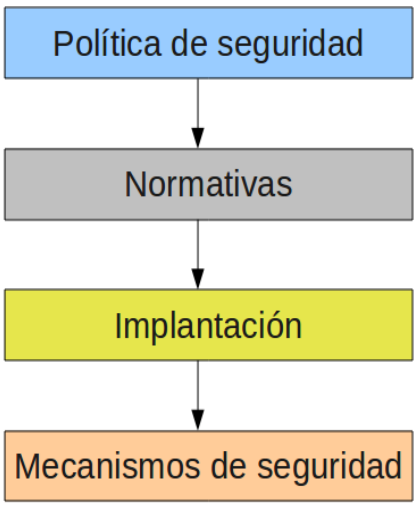
- Brinda una mayor seguridad a los escenarios de movilidad
- Ofrece seguridad que permite acceder a todos los recursos de la red
- Permite construir una red corporativa segura sobre redes publicas
- Proporciona una infraestructura segura para realizar transacciones
- Posibilita nuevas aplicaciones y el acceso seguro y transparente.

3.5. Diseño Esquemático de la Implementación de Mecanismos de Seguridad

De acuerdo al análisis realizado a la infraestructura de la red de comunicación del laboratorio de redes de la Universidad Técnica de Cotopaxi se ha diseñado la implementación del mecanismo de seguridad IPSec, la cual está estructurada en cuatro fases a fin de contar con guías que faciliten la explicación y beneficien el desarrollo de la implementación.

Cada fase desempeñará una función determinada con el fin de cumplir con los requisitos propuestos para mejorar la seguridad y el control de vulnerabilidades en la red. Las fases que conforman la implementación de mecanismos de seguridad así como el esquema se muestran a continuación:

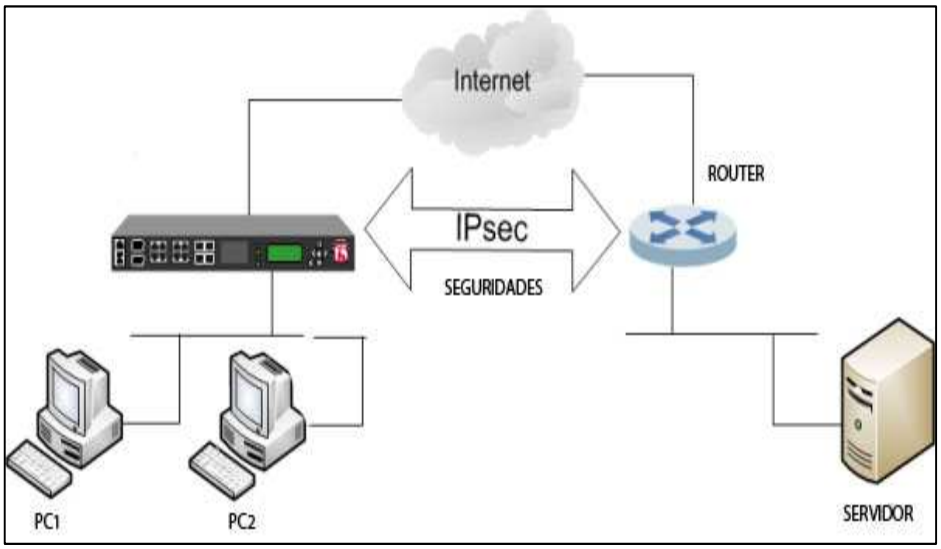
GRÁFICO N° 3.1.
IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD



Fuente: Mecanismos de Seguridad
Realizado por: Investigadores

GRÁFICO N° 3.2.

ESQUEMA DE LA IMPLEMENTACIÓN IPSEC



Fuente: Investigadores
Realizado por: Investigadores

3.6. Etapas para la Implementación del Mecanismo de Seguridad IPSec

Las principales etapas para la implementación del mecanismo de seguridad IPSec son las siguientes:

- Los equipos deben tener una dirección IP (origen y destino)
- Protocolo IPsec (AH o ESP).
- Algoritmo y password empleados por IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index).
- Seguridad para proteger los paquetes de datos.

3.6.1. Servicios de Seguridades

- ***Control de Acceso***

  Se establecen políticas de establecimiento de conexiones IPSec.

- ***Autenticación del originario de los datos***

  El usuario está convincente que proviene del servidor el paquete enviado.

- ***Integridad de mensaje***

  Un atacante no puede modificar ni aceptar un paquete.

- ***Protección contra reenvíos***

  Un atacante no puede reenviar paquetes ni aceptarlos.

- ***Confidencialidad***

  Un atacante no puede leer datos asegurados.

- ***Authentication Header(AH)***

  Proporciona integridad y autenticación del mensaje.

- ***Encapsulating Security Payload (ESP)***

  Provee cifrado y protección limitada contra análisis de flujo de datos.

- ***El establecimiento del túnel IPSec se hace básicamente en dos fases:***

  IKE - Fase 1:

  - Las puertas de enlace negocian un canal bidireccional
  - Algoritmos de cifrado probables
  - Llaves de autenticación para proveer los túneles IPSec.

  IKE - Fase 2:

  - Se establecen direcciones, uno para cada sentido.
  - Método de cifrado, el protocolo a usar es el AH o ESP.

3.6.2. Requerimientos

El mecanismo IPSec puede aplicarse a cualquier computador de escritorio con requerimientos mínimos bajo un sistema operativo XP y un servidor bajo un sistema operativo Windows server los mismos que deben tener una conexión en red ya sea cableada o inalámbrica.

TABLA N° 3.3.

REQUERIMIENTOS PARA LA IMPLEMENTACIÓN

REQUERIMIENTOS
Servidor con Sistema Operativo Windows Server 2003 o superior
Computador con Sistema Operativo Windows XP o Superior
Medios de Transmisión (Cable de red)
Switch
Recursos Compartidos
Estaciones de Trabajo

Fuente: Investigadores

Realizado por: Investigadores

3.7. Creación de Certificado de autenticación (CA) para la implementación IPSec

3.7.1. Servicios de Certificados de Active Directory

Para la implementación IPSec es necesario la creación de un certificado de autenticación, el cual realiza aspectos de seguridad como la autenticación. Se procedió a agregar servicios de certificados de Active Directory los cuales servirán para la creación de un certificado digital que beneficiará la seguridad y la autenticación. **(VER MANUAL DE USUARIO)**

Se agregó características las cuales son instaladas en el Windows Server 2012 las mismas que permiten administrar y supervisar dispositivos de almacenamiento a través de interfaces de administración.

Por medio del asistente para agregar roles y características, se procedió a agregar una Entidad de certificación la cual indica que se desea crear una entidad para administrar e emitir certificados, también se agregó una Inscripción web de entidad de certificación las misma que proporciona una simple interfaz para que los usuarios realicen tareas de solicitud o renovación de certificados.

3.7.2. Configuración de Servicios de Certificados de Active Directory

Para la configuración del certificado de Autenticidad (CA) se procede a seleccionar el nombre del dominio a cual pertenece el servidor, especificando de esta forma que el CA será aplicado al dominio en general. **(VER MANUAL DE USUARIO)**

3.7.2.1. Tipo de Instalación

Se seleccionó un CA independiente que se utiliza para aplicar la autenticación a un dominio o a un grupo de trabajo. Se pueden usar sin conexión a la red. Se utiliza un CA raíz por ser las únicas configuraciones en una jerarquía y debido a su función de ampliar una jerarquía de infraestructura.

3.7.3. Criptografía para CA

Se procede a la selección de un algoritmo Hash para firmar el certificado a crear por CA. El algoritmo seleccionado SHA1 (Secure Hash Algorithm 1) realiza su proceso en base al algoritmo MD5, se utiliza para comprobar la integridad de los datos y es más efectivo que MD5 debido a sus longitudes de Hash que generan mayor seguridad. **(VER MANUAL DE USUARIO)**

3.7.4. Complemento Certificados

Para poder utilizar el CA que fue creado se procede primero a agregarlo mediante una consola MMC. El complemento Certificados permite examinar el contenido de los certificados que son creados o se encuentran predeterminados. El certificado creado se encuentra dentro de la carpeta Personal/Certificados de la ventana Raíz de Consola MMC. **(VER MANUAL DE USUARIO)**

3.7.5. Propiedades de Seguridad

Luego de agregar el Certificado de Autenticación (CA), se cambió las propiedades de seguridad para establecer una mejor comunicación. Se agregó a Usuarios autenticados, equipos que se encuentran en el dominio, Administradores del dominio, controladores de dominio y servicios de red, cada una de ellas con su respectivo permiso y denegación.

Es necesario parar la ejecución del servicio de certificados digitalizando net stop certsvs y volver a iniciar digitalizando certsvs para que todas las modificaciones realizadas sean actualizadas. **(VER MANUAL DE USUARIO)**

3.7.6. Configuración IPSec en Server 2012 y Windows Seven

La configuración de IPSec se centra en obtener una comunicación segura entre los equipos existentes en el Laboratorio de Redes de la Universidad Técnica de Cotopaxi.

Se puede implementar seguridad IPSec mediante:

- Microsoft Management Console + Snap-In de Directivas de Seguridad IP
- Directivas de Grupo (GPO)
- Consola de Firewall Avanzado de Windows

Para la implementación de IPSec, en principio los equipos deben tener conexión entre sí. A continuación se procede a revisar las direcciones IP y establecer un PING continuo en el equipo cliente y servidor.

3.7.6.1. Administrador de directivas de grupo

Se agregó el complemento Administrador de directivas de grupo la cual brinda una única herramienta para la administración de directivas de grupo en sitios, dominios y unidades organizativas de uno o demás bosques.

Además se procede a crear una nueva unidad organizativa dentro del dominio existente lab_redes.com, la cual servirá para establecer una mejor administración de los clientes. **(VER MANUAL DE USUARIO)**

3.7.6.2. Directivas de seguridad IP

Se agregó Directivas de seguridad IPSec tanto a los clientes como al servidor las cuales se aplican para establecer servicios de seguridad de IPSec y proveer niveles de resguardo en la red de comunicación. Al momento de configurar directivas de seguridad IPSec se integra los requisitos de seguridad al equipo local, dominio e infraestructura de red.

Las directivas de seguridad incorporan todas las reglas de seguridad que se van a implementar en el Laboratorio de redes de la Universidad Técnica de Cotopaxi. Al usar el complemento Directivas de seguridad IP, tiene la autorización de crear, editar y asignar directivas IPSec al equipo remitente y receptor. **(VER MANUAL DE USUARIO)**

3.7.6.2.1. Políticas de IPSec

La directiva de grupo en la configuración actual presenta tres políticas predefinidas que determinan diferentes comportamientos del equipo en relación a IPSec las cuales serán utilizadas. **(VER MANUAL DE USUARIO)**

3.7.6.2.1.1. Cliente (sólo responder)

Maneja una comunicación normal sin encriptar a menos que el dispositivo o servidor con el que se vaya a comunicar le exija encriptar su tráfico, en ese momento podrá encriptar el tráfico y los paquetes que se envíen al servidor.

- Establece comunicación sin IPSec
- Modo de sólo respuestas
- Negocia la seguridad si se genera una solicitud de seguridad.
- Sólo inicia conversaciones en claro, no en modo IPSec

3.7.6.2.1.2. Servidor (seguridad de petición)

Permite como primera opción encriptar el tráfico entre dos dispositivos pero si el dispositivo con el que intenta establecer comunicación no puede trabajar en IPSEC, entonces le permite establecer una comunicación no segura.

- Recibe tráfico IPSec y tráfico no IPSec desde los clientes.
- Establece comunicación cifrada y si otro equipo no tiene configurado IPSec establece la comunicación en claro.
- Negocia seguridad IPSec al momento que inicia una conexión.
- Establece reglas IP, ICMP, Trafico dinámico

3.7.6.2.1.3. Servidor seguro (requiere seguridad)

Exige que cualquier dispositivo que se comunique al servidor envíe los paquetes encriptados a través de IPSEC. Si la información no se envía encriptada no se puede establecer comunicación.

- Requiere utilizar IPSec para todo el tráfico entrante y saliente.
- El equipo solamente establece comunicaciones seguras.
- Establece reglas IP, ICMP, Trafico dinámico

3.7.6.2.2. Claves de Seguridad

Luego de haber agregado una Directiva de Seguridad se procede a la asignación de una clave o llave de seguridad de comunicación, la misma que servirá de protección al momento de intercambiar datos. Para eso es necesario asignar una clave de seguridad fuerte o a su vez establecer métodos personalizados de seguridad que beneficien la protección de la información.

3.7.6.2.3. Reglas de seguridad de conexión

Se creó reglas de seguridad de conexión para autentificar los equipos de la red de comunicación y así preservar la información al ser enviada o recibida. Con la creación de nuevas reglas de seguridad se podrá autentificar o cifrar las conexiones entre equipos. **(VER MANUAL DE USUARIO)**

3.7.6.2.4. Supervisión

La opción supervisión permite revisar las reglas de seguridad activas y las reglas de seguridad de conexión en el equipo.

3.7.6.2.4.1. Modo Principal

Con el modo principal se establece una comunicación segura entre el equipo cliente y el servidor la misma que servirá para proteger los datos a intercambiar entre dichos equipos. En este modo solamente hay una asociación de seguridad.

3.7.6.2.4.2. Modo Rápido

Al utilizar el modo rápido se puede generar nuevas claves o simplemente actualizar las llaves de seguridad las cuales son encargadas de proteger el tráfico de datos IP.

A diferencia del modo principal en el modo rápido puede haber muchas asociaciones de seguridad.

Para la supervisión de la Asociación de Seguridad se utiliza el modo rápido ya que proporciona información de los equipos que se encuentran actualmente conectados y el tipo de seguridad que protege la información a intercambiar.

3.7.6.2.5. Asistentes de Configuración

Para la creación de reglas seguridad es necesario seleccionar el tipo y uso de cada una las cuales se encuentran en el Asistente de Configuración.

3.7.6.2.5.1. Aislamiento

Ésta regla será habilitada la cual restringe las conexiones entrantes, la pertenencia al dominio y aísla los equipos de la red de comunicación permitiendo la implementación de una estrategia de incomunicación de servidor.

3.7.6.2.5.2. Exención de autenticación

El objetivo de la regla exención es la de elegir equipos que no requieren autenticación mediante la dirección IP. En esta regla los equipos pertenecientes a un dominio aislado pueden comunicarse con otros equipos aunque estos no sean autenticados.

3.7.6.2.5.3. De servidor a servidor

La regla de servidor a servidor resguarda las conexiones entre equipos y servidores.

3.7.6.2.5.4. Túnel

Al crear la regla túnel se protegen las conexiones entre los equipos de la puerta de enlace. Para utilizar esta regla es necesario especificar los extremos del túnel.

3.7.6.2.5.5. Personalizada

Se utiliza esta regla cuando no se pueda crear ninguna de las demás tipos de reglas. Ésta regla será adaptada a las necesidades del usuario.

3.7.6.2.6. Reglas de IPSec

Con las reglas IPSec se establece el modo de comportamiento del sistema tanto en el envío como en la recepción de la información. Cada regla IPSec creada determina el tráfico que debe examinar, permitir o bloquear. **(VER MANUAL DE USUARIO)**

3.7.6.2.7. Filtros

Se configuró la acción de filtrado para bloquear o restringir la seguridad en la red.

Con la creación de filtros se limita el tráfico que se desea analizar, permiten definir los requisitos de seguridad para el tráfico de la red de comunicación, además se especifica el tráfico inicial no seguro.

Si no se especifica la acción de filtrado correcta la seguridad no será la adecuada, de esta forma no se podrá filtrar todos los paquetes entrantes o salientes. **(VER MANUAL DE USUARIO)**

3.7.6.2.8. Métodos de autenticación

Luego de crear una regla de seguridad y su tipo con el asistente de configuración, se procede a seleccionar el método de autenticación. Se puede utilizar un solo método de autenticación entre el cliente y servidor. A continuación se describen los métodos de autenticación a utilizar.

3.7.6.2.8.1. Certificado de Autenticación

Se empleó un certificado de autenticación que está diseñado para satisfacer todas las necesidades que los usuarios puedan tener proporcionando un medio de comprobación de su identidad. Mediante la implementación de un certificado (CA) con el mecanismo IPSec, se limita la posibilidad de interceptar, modificar o falsificar información enviada a través de la red. **(VER MANUAL DE USUARIO)**

3.7.6.2.8.2. Predeterminado

Se utiliza el método predeterminado cuando se desea tener una configuración de IPSec ya establecida como método de autenticación.

3.7.6.2.8.3. Equipo y usuario (Kerberos V5)

Se aplica para restringir las conexiones desde usuario y equipo el cual debe pertenecer a un dominio de confianza.

3.7.6.2.8.4. Opciones avanzadas

Aplica una configuración personalizada de autenticación

3.7.6.2.9. Configuración de métodos de seguridad

Al configurar métodos de seguridad se especifica la manera de comunicación y protección de intercambio de datos entre el cliente y servidor. A continuación se detalla los métodos de seguridad y su utilidad al momento de utilizarlos. **(VER MANUAL DE USUARIO)**

- Integridad AH (Algoritmos AES, SHA1, MD5).
- Integridad ESP (Algoritmos AES, SHA1, MD5).
- Confidencialidad ESP (Algoritmos AES, DES, 3DES).
- Confidencialidad AH + ESP (No atraviesa NAT)

Tanto el protocolo de seguridad AH (Integridad de direcciones y datos sin cifrado) como el protocolo ESP (Integridad de datos de cifrado) se habilitan para proporcionar seguridad a nivel de paquete. Los algoritmos antes definidos se usan para protección de integridad y confiabilidad.

3.8. Discusión de Resultados Obtenidos de la Implementación de Mecanismos de Seguridad

Con la implementación de mecanismos de seguridad se cubrió de beneficios y se aumentó la seguridad en la infraestructura de red, se identificó, describió y diferenció cada uno de los mecanismos de seguridad en una red de comunicación.

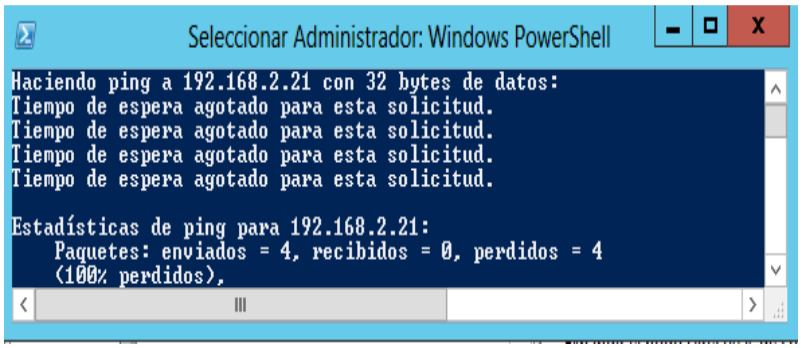
Se pretendió examinar cual es el mecanismo más apropiado, seguro, confiable, flexible y aplicable en la infraestructura de red del Laboratorio de redes de la Universidad Técnica de Cotopaxi.

A continuación se dan a conocer los resultados obtenidos de la implementación del mecanismo de seguridad (IPSec), con el objetivo de explicar y evaluar su protección contra riesgos y vulnerabilidades en la red de comunicación.

Al asignar IPSec, la comunicación se interrumpe y no se puede comunicar con la carpeta compartida, no es posible porque el servidor exige que la comunicación hacia él se dé mediante IPSec, y como el cliente no puede establecer IPSec la comunicación no se realiza.

GRAFICO N° 3.3.

COMUNICACIÓN INTERRUMPIDA

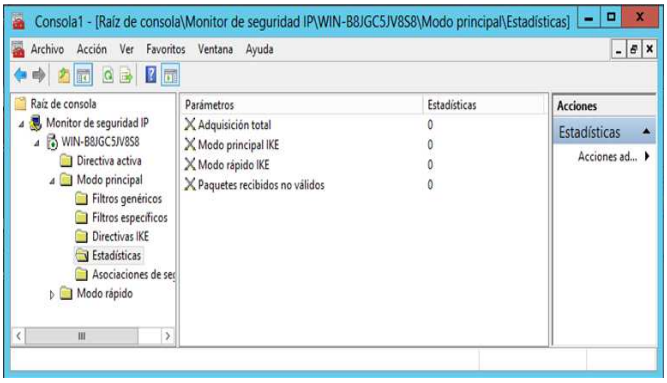


Fuente: WindowsPowerShell (IPSec)
Realizado por: Investigadores

La transmisión de los paquetes de datos fue asegurada con los servicios de autenticación y encriptación que brinda IPSec, por ende al enviar paquetes con la seguridad definida, ya no es posible su extracción.

GRAFICO N° 3.4.

ESTADÍSTICA DE LA TRANSMISIÓN

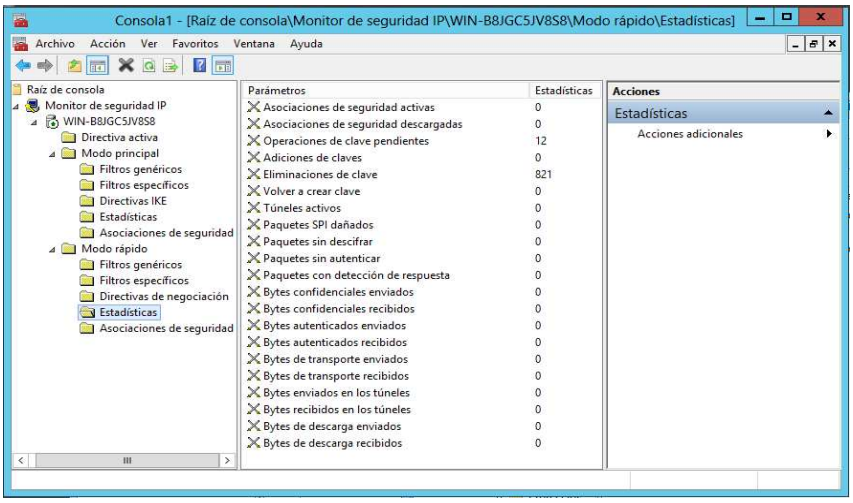


Fuente: Consola de Windows Server 2012
Realizado por: Investigadores

Los ataques informáticos como el sniffing y spoofing que buscan suplantar la identidad de paquetes que son enviados a través de la red, son inhabilitados y protegidos por IPSec, consecuencia de los métodos de autenticación utilizados y aplicados a cada paquete de datos transferido.

GRAFICO N° 3.5.

ESTADÍSTICA IPSEC

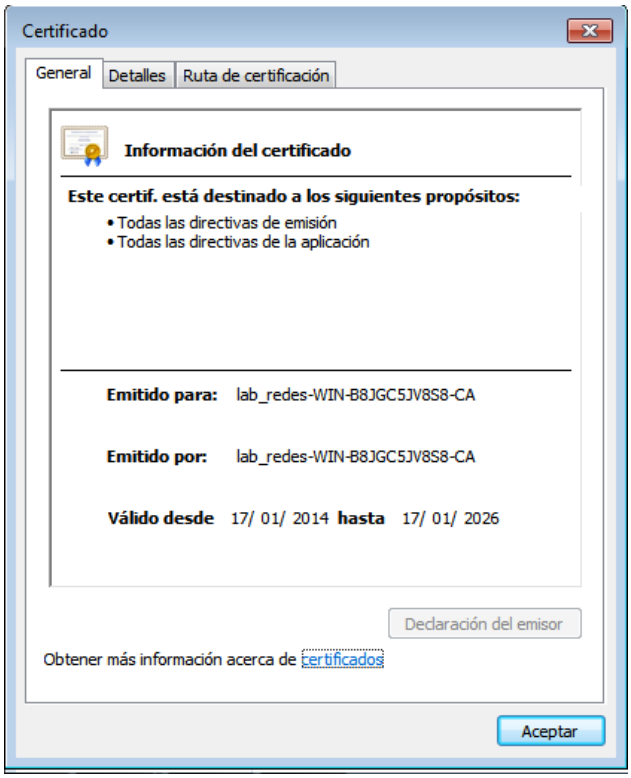


Fuente: Consola de Windows Server 2012
Realizado por: Investigadores

Al implementar la configuración de IPSec con un certificado (CA), se autentifica a un usuario en Internet brindando confianza en línea.

GRAFICO N° 3.6.

INFORMACIÓN DEL CERTIFICADO (CA)



Fuente: Certificado de Autenticidad (CA)
Realizado por: Investigadores

Los resultados obtenidos son solo un modelo que manifiesta el estado de la red en un momento determinado, la transmisión de la información depende de varios factores entre ellos el enrutamiento, la conexión estable entre el equipo cliente y servidor, el nivel de congestionamiento de internet, entre otros.

3.9. Conclusiones y Recomendaciones

CONCLUSIONES

- La implementación del mecanismo de seguridad (IPSec) permitió asegurar la red de comunicación de ataques internos como externos mejorando y garantizando un mejor envío y recepción de información entre los usuarios.

- Con la implementación del mecanismo de seguridad IPSec se garantiza el derecho a acceder a datos seguros, administrar servicios y a escoger necesidades o requerimientos que soliciten los usuarios.

- El mecanismo de seguridad IPSec en comparación con los demás mecanismos de seguridad se utilizó por ser seguro, confiable y fácilmente implementado ya que incluye reglas y filtros a fin de desarrollar una mejor seguridad de comunicación.

- Tanto el mecanismo de seguridad IPSec como los demás mecanismos de seguridad tienen sus ventajas y desventajas, el grado de protección contra vulnerabilidades o ataques informáticos dependerá del escenario en el que fue implementado.

- IPSec se puede considerar un mecanismo de seguridad ideal a implementar en aplicaciones como VPN Acceso remoto, Seguridad VoIP, Seguridad en WLAN y VPN Red a Red.

RECOMENDACIONES

- Es necesario asegurar la integridad, privacidad y disponibilidad de la información contenida en el sistema informático para evitar daños, problemas y vulnerabilidades al momento de transferir la información.

- Capacitar a los usuarios sobre nuevas tecnologías y amenazas que surgen con el pasar del tiempo ya que esta manera estarán a la expectativa de nuevas seguridades para la comunicación y protección de información, además estar en alerta de nuevas y mejoradas técnicas de acceso indebido a las redes de comunicación.

- La seguridad de la información debe ser bien administrada evitando que usuarios externos no autorizados puedan acceder a la misma ya que si lo hicieran la información podría ser utilizada maliciosamente perjudicando a la Institución como a los usuarios autorizados en la red de comunicación.

- Es necesario que la Institución y los usuarios enfoquen su atención a nuevas y mejores herramientas de seguridad para evitar riesgos de posibles ataques informáticos en la red.

- Se sugiere que a futuro se implementen nuevas seguridades en la red de comunicación del laboratorio de redes de la Universidad Técnica de Cotopaxi, concordes a la tecnología y a los beneficios ofrecidos, permitiendo una mejor protección ante vulnerabilidades y peligros que puedan afectar a la red de comunicación.

GLOSARIO DE TÉRMINOS

E

Encriptación: Es el proceso para volver ilegible información considera importante.

F

Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

H

Host: Es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

I

Infraestructura: Modo de conexión en una red wireless que define que el equipo se conectará a un Punto de Acceso.

T

Texto Plano: Son aquellos formados exclusivamente por texto (sólo caracteres), sin ningún formato.

Topología: Se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red.

GLOSARIO DE SIGLAS

A

AAA: Authentication, Authorization and Accounting o Autenticación, Autorización y Contabilización.

ADSL: Asymmetric Digital Subscriber Line o Línea de abonado digital asimétrica.

AES: Advanced Encryption Standard o Estándar de Cifrado Avanzado

AH: Authentication Header o Encabezado de autenticación

D

DES: Data Encryption Standard o estándar de cifrado de datos.

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

E

EAP-TLS: Autentificación extensible Protocolo o Protocolo de autentificación extensible.

ESP: Encapsulated Security Payload o Carga de seguridad encapsulada

F

FTP: File Transfer Protocol o Protocolo de Transferencia de Ficheros.

G

GUI: Graphical User Interface o Interfaz Gráfica de Usuario

H

HTTP: HyperText Transfer Protocol o Protocolo de transferencia de hipertexto.

I

IEEE: Institute of Electrical and Electronics Engineers o Instituto de Ingenieros. Eléctricos y Electrónicos.

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

IKE: Internet Key Exchange o intercambio de claves por Internet.

IPSEC: Internet Protocol Security o Seguridad del protocolo Internet.

L

LAN: Local Área Network o Red de Área Local.

M

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

MD5: Message-Digest Algorithm o Algoritmo de Resumen del Mensaje 5

N

NAT: Network Address Translation o Traducción de Dirección de Red

P

PDA: Personal Digital Assistant o Asistente digital personal.

S

SHA: Secure Hash Algorithmo Algoritmo de Hash Seguro

SMTP: Simple Mail Transfer Protocol o Protocolo para la transferencia simple de correo electrónico.

SPI: Serial Peripheral Interface Bus o Bus serial de interfaz de periféricos.

SSID: Service Set Identifier o Servicio identificador de conjunto.

T

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

TKIP: Temporal Key Integrity Protocol o Protocolo de integridad de claves.

V

VLAN: Virtual Local Area Network o Red de Área Local Virtual.

VPN: Virtual Private Network o Red Privada Virtual.

W

WEP: Wired Equivalent Privacy o Privacidad Equivalente a Cableado.

WLAN: Wireless Local Area Network o Red de Área Local Inalámbrica

WPA: Wi-fi Protected Access o Acceso Wi-Fi Protegido.

WPA2: Wi-fi Protected Access 2 o Acceso Protegido Wi-Fi 2.

REFERENCIAS BIBLIOGRÁFICAS

Básica:

- ABASCAL, Elena (2009). “Fundamentos y Técnicas de Investigación”. San Andrés: México.
- BERNAL, Augusto (2006). “Metodología de la Investigación”. PEARSON: México.
- CEGARRA, Sánchez (2012), “Los Métodos de Investigación”. Díaz de Satos: Madrid. Ecafsa: México.
- DE LA MORA, Maurice (2006), “Metodología de la Investigación para el Desarrollo del Pensamiento”. FEBUAP: México.
- Hernández, Santiago. (2006). Roberto. “Metodología de la Investigación”. Ultra: México.
- RUIZ, Ramón (2006), “Historia y Evolución del Pensamiento Científico”. Trillas: México.

Citada:

- AGUILERA, Purificación (2010). “Seguridad Informática y Comunicaciones”. ENDITEX: Madrid.
- ANDREU, Fernando (2006). “Seguridad en Redes WLAN”. MARCOMBO: Barcelona.
- CANCELO, Pablo (2007). “Comunicación, Tecnología y su Nomenclatura”. GESBIBLO: La Coruña.
- CORRALES, Luis (2006). “Diseño e Implantación de Arquitecturas Informáticas Seguras”. DIKINSON: Madrid.
- ENGLS, Adams (2008). “Introducción a las Redes Inalámbricas”. De laUPV: Valencia.

- ESPAÑA, María (2008). “Servicios Avanzados de Telecomunicación”. Díaz de Santos: Madrid.
- FUNDACIÓN TELEFÓNICA (2012). “Privacidad y Seguridad en la Red”. ENI: Barcelona.
- GALINDO, Marco (2010). “Escaneando la Informática”. UOC: Barcelona.
- GALINDO, Alfonso (2011). “Seguridad Informática”. MAS: Barcelona.
- GARCÍA, Francisco (2011). “Videovigilancia CCTV Usando Videos IP”. AENOR: Malaga.
- GARCÍA, Héctor (2006). “Avances en Informática y Sistemas Computacionales”. USBN: Tabasco.
- GUZMÁN, Sacristán (2010). “Informática”. DKINSON: Madrid.
- HERNANDO, Roberto (2011). “Seguridad en Redes Inalámbricas”. ISBN: Tena.
- HERRERA, Enrique (2006). “Tecnologías y Redes de Transmisión de Datos”. LIMUSA: Balceras
- JEAN, Marc (2005). “Seguridad en la Informática de Empresa”. ENI: Barcelona.
- LÓPEZ, José (2005). “Informática y Comunicaciones para la Empresa”. CIDI: Tarancón.
- MARTINEZ, Jordi (2011). “IPV6 Aspectos Legales del Nuevo Protocolo Internet”. ISOC: Buenos Aires.
- MATHOM, Philippe (2004). “TCP/IP Entorno Windows”. ENI: Barcelona.
- MATHON, Philippe (2005). “Windows Server 2003 Network Infrastructures”. ENI: Barcelona.
- MOLINER, Francisco (2005). “Informáticos Generalitat Valencia”. MAD: Valencia.
- MONTERO, Antonio (2008). “Informática para Gestión de Empresas”. ESIC: Madrid.
- PACHECO, Federico (2008). “Ethical Hacking”. DALAGA: Buenos Aires.

- PARDO, Beltrán (2006). “Diseño E Implementación de Arquitecturas Informáticas Seguras”. PEARSON: Valencia.
- PELLEJERO, Izaskun. (2006). “Fundamentos y Aplicaciones de Seguridad en Redes WLAN”.ENI: Barcelona.
- PÉREZ, María (2005). “La Informática, Presente y Futuro en la Sociedad”. ENI: Barcelona.
- PÉREZ, Santiago (2011). “La Informática, Presente y Futuro en la Sociedad”. MONDADORI: Barcelona.
- RAY, Jimmy (2010). “Acrónimos con la Tecnología Inalámbrica”. UPC: Barcelona
- SARUBBI, Juan (2008). “Seguridad Informática”. LUJAN: Buenos Aires.
- SIMON, Abram (2011). “Catholic Prayers”. KENEDY: Madrid.
- STAFF, Users (2011). “Hackig”. Fox Andina: Buenos Aires.
- STALLINGS, William (2005). “Fundamentos de Seguridad en Redes”. PEARSON: Madrid.
- STALLINGS, William (2005). “Seguridad Informática y Comunicaciones”. PEARSON: Madrid.

Consultada:

- ALTES, Jonah (2005). “Análisis de Redes y Sistemas de Comunicaciones”. UOC: Barcelona.
- GÓMEZ, Vieites. (2011). “Enciclopedia de la Seguridad Informática”. ALFAOMEGA: Mexico.
- HUERTA, Antonio. (2005). “Seguridad en Unix y redes”. Prentice Hall: Mexico.
- JAMRICH, June, (2008). “Conceptos de Computación”. ZENIT: Burgo.
- LIZARRONDO, Magaña. (2005), “Comunicaciones y Redes de Computadores”. LIT: Madrid.

Virtual:

- ALEGSA (2013). Sistema operativo Windows 7 [en línea]. [fecha de consulta: 27 de noviembre 2013]. Disponible en: http://sistemaoperativowin7.blogspot.com/.
- APRENDE LIBRE (2013). Sistema Operativo Windows Server 2012 [en línea]. [fecha de consulta: 27 de noviembre 2013]. Disponible en: http://blogs.technet.com/b/ccaitpro/archive/2012/09/04/windows-server-2012.
- BIELER, Juansa (2006). Recursos Compartidos [en línea]. [fecha de consulta: 10 de junio 2013]. Disponible en: http://juansallopis.wordpress.com/2006/01/09/recursos-compartidos.
- CARUA, José (2012). Ataques Informáticos [en línea]. [fecha de consulta: 18 de noviembre 2013]. Disponible en: http://www.slideshare.net/sm2099/tipos-de-ataques-informaticos-17557769.
- CORPORACIÓN, ORACLE (2010). Seguridad IPSec [en línea]. [fecha de consulta: 17 de octubre 2013.] Disponible en: http://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-13/index.html.
- FALCÓN, Guillermo (2007). Mecanismo WEP y WPA [en línea]. [fecha de consulta: 13 de diciembre 2013]. Disponible en: http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa.
- MENDEZ, Alyk (2013). Configuración de Seguridad [en línea]. [fecha de consulta: 18 de noviembre 2013]. Disponible en: http://configuracionparametros.blogspot.com/2013_04_01_archive.html
- MICROSOFT CORPORATION (2013). Windows Server 2012 [en línea]. [fecha de consulta: 27 de noviembre 2013.]. Disponible en: http://blogs.technet.com/b/ccaitpro/archive/2012/09/04/windows-server-2012.aspx.
- PROYECTO DONO (2008). Seguridad en redes [en línea]. [fecha de consulta: 27 de noviembre 2013]. Disponible en: http://dono.discapnet.es/contact.