UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

Tema: Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la ciudad de Cuenca

Autor: Tlgo. Paúl Guzhñay C.

Tutor: Ing. Pablo Tamayo

2011

CERTIFICA:

Que el presente trabajo de investigación "**Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la ciudad de Cuenca**", realizado por el Tlgo. Paúl Santiago Guzhñay Cordero, egresado de la facultad de Sistemas Informáticos, se ajusta a los requerimientos técnicos, metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación

Cuenca, 1 de diciembre de 2011

_____

Ing. Pablo Tamayo

ACTA DE CESIÓN DE DERECHOS

Yo, Tecnólogo Paúl Santiago Guzhñay Cordero, estudiante de **SISTEMAS INFORMÁTICOS**, declaro conocer y aceptar las disposiciones del programa de Estudios de Ingeniería Informática, que en lo pertinente dice: “Es patrimonio de la Universidad Tecnológica Israel, todos los resultados provenientes de investigaciones, de trabajos artísticos o de creación artística o científicos o técnicos o tecnológicos y de tesis o trabajos de grado que se realicen a través o con el apoyo de cualquier tipo de la Universidad Tecnológica Israel. Esto significa la cesión de los derechos de propiedad intelectual a la Universidad Tecnológica Israel”.

_____

Tlgo. Paúl Santiago Guzhñay Cordero

CERTIFICADO DE AUTORÍA

El documento de tesis con título "**Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la ciudad de Cuenca**", ha sido desarrollado por el Tecnólogo Paúl Santiago Guzhñay Cordero con C.C. No. 0104435086 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Tlgo. Paúl Santiago Guzhñay Cordero

DEDICATORIA

Dedico está presente Tesis de Grado a mi esposa Melania y a mi hijo John Paúl, quien con su apoyo, cariño, paciencia, amor y comprensión, me han dado día a día las fuerzas necesarias para seguir adelante y cumplir con una meta tan importante en mi vida, a mis padres Rubén y Janneth ya que con su apoyo incondicional han sabido guiarme en todo momento de mi vida. Para que todo este sacrificio y esfuerzo sirva de ejemplo para mi esposa e hijo para que cumplan con todas sus objetivos que se propongan y vean en mi a un amigo, un guía y un apoyo incondicional.

AGRADECIMIENTO

Agradezco a Dios ya que me ha sabido guiar por el camino correcto, dándome la sabiduría, entendimiento, comprensión, a todas las personas que han estado siempre a mi lado apoyando guiándome en todo momento para la culminación de este proyecto, en especial a mi tutor Ing. Pablo Tamayo, ya que con sus conocimiento me ha sabido guiar de muy buena manera para la culminación de este propósito.

RESUMEN

Los Dispositivos inalámbricos hoy en día han venido dando pasos muy grandes ganando espacio en cada una de las preferencias de los usuarios y se han convertido en uno de los más utilizados en todo el mundo, tanto para oficinas como para hogares, ya que al no estar conectados por un medio físico (cables) proporciona una alternativa viable a las redes locales cableadas.

Las redes inalámbricas surge como una nueva solución de comunicación en cada una de las organizaciones u hogares, las redes inalámbricas de área local van tomando un papel muy importante en las mismas. Una conexión inalámbrica se ha convertido en una alternativa muy viable para ofrecer conectividad en lugares donde resulta un tanto complicado dar un servicio de red cableada.

Las seguridades que se tiene que dar al momento de utilizar una red inalámbrica son muy importantes ya que con esto se puede asegurar de mejor manera la información que circula dentro del área de cobertura de los dispositivos, para así estar protegido contra cualquier ataque inesperado o robo de información, el cual puede ser muy perjudicial para el usuario que utilice una red inalámbrica no segura.

En la actualidad existen diferentes maneras para poder proteger nuestras redes inalámbricas de ataques, pero en muchas ocasiones no conocemos, ni tenemos noción de estas, no sabemos cómo protegernos, ni que rumbo tomar para poder encaminarnos y así poder tener nuestros dispositivos y redes seguras.

Pensando en cada una de estas debilidades que se presentan en las redes inalámbricas del Colegio Técnico Sudamericano y al saber que no se cuenta con los mejores conocimientos de seguridades que se pueden dar a los dispositivos inalámbricos, se quiere apoyar con una guía de solución, que permita adaptar dichas mejoras a cada uno de sus dispositivos con estándares actuales, protocolos, métodos, que se ajusten a las necesidades de las redes inalámbricas de la institución y así tener configurados de una manera aceptable, previniendo que personas no autorizadas ingresen a nuestros sistemas y minimizando los posibles riesgos que se pueden tener dentro de una red inalámbrica.

SUMMARY

Actually wireless devices have been doing a lot great gain ground in each of the user preferences and have become one of the most widely used worldwide for both enterprises and homes, as not being connected by a physical medium (cable) provides a viable alternative to wired LANs.

Wireless networking is emerging as a new communication solution in each organization; local area wireless networks are gaining an important role in them. A wireless connection has become a very viable alternative to provide connectivity in places where it is somewhat complicated to a wired network service.

The assurances must be given when using a wireless network is very important because with this you can better ensure the information circulating within the coverage area of the devices in order to be protected against any unexpected attack or theft information, which can be very harmful to the user using an unsecured wireless network.

There is some ways to protect our wireless networks from attacks, but often do not know, nor do we have this notion, we know how protect to these, nor what course to take in order to track and so we can have our devices and secure networks.

Thinking about each of these weaknesses are in wireless networks and Sudamericano Technical High school to learn that do not have the best knowledge of assurances can be given to wireless devices, It is to support a

troubleshooting guide, which such improvements may be adapted to each of their devices with current standards, protocols, methods that meet the needs of the institution's wireless network so you have configured and acceptable, preventing unauthorized persons from entering our systems and minimizing the potential risks that can have within a wireless network.

Tabla de Contenido

Lista de Tablas y Gráficos

1. Introducción

1.1 Antecedentes

Una red inalámbrica es un medio que nos permite la comunicación de datos e información, este es muy utilizado por instituciones, personas como una alternativa a una red cableada.

Esta utiliza un medio de radiofrecuencia que permite una mucha mayor movilidad y facilidad para el usuario para estar conectado a sus redes sin necesidad de estar cableada, con la cual nos permite transmitir información en tiempo real y estar conectados y compartiendo el acceso a internet

En la evolución de la informática se ha venido dando muchos casos de personas mal intencionadas que quieres hacer daño a cualquier individuo o sistema de información, para sacar provecho de las cosas realizadas por aquellas personas que han dedicado mucho tiempo y sacrificio a proyectos importante, por lo que se ven muy afectadas con estas situaciones, como todos muy bien sabemos cada día va creciendo la tecnología y los medios para realizar algún ataque o simplemente para hacer daño a personas que conocen poco o nada del tema y se siente muy impotentes para poder protegerse, entonces la consideración que uno debe tomar en cuenta para saber cómo podemos y debemos configurar este dispositivo para que no caigamos en algún ataque que atente contra la información que tenemos en nuestros equipos.

En la actualidad se ha vuelto muy importante saber o utilizar alguna herramienta o simplemente saber cómo defender nuestra información, por

lo que no solo empresas están adoptando cualquier medida cautelar para proteger su información, sino que las personas comunes quieren empaparse del tema, ya que no quisieran llegar a que les hagan daño.

Las redes inalámbricas hoy en día ha tomado gran aceptación para la utilización de un dispositivo inalámbrico y también se ha hecho muy importante en la vida cotidiana de las personas, ya que no solo en instituciones, empresas se ha implementado esto, sino también en cada uno de los hogares de las persona, por lo que las redes inalámbricas están en auge y va creciendo a un ritmo acelerado.

Sabemos que las redes inalámbricas que ahora se utilizan en el medio es una muy buena opción, no solo para empresas sino para cualquier persona que tenga un Access Point en casa o en trabajo, ya que podremos ver como tenemos configurados nuestros dispositivos y sabremos qué es lo que tenemos que corregir para que las redes e información estén mejor protegidas.

En el caso que surgió en nuestro país sobre las personas que con mala intención o por represalias para el gobierno o cualquier persona e ingresan a las bases de datos y modifican la información, con lo cual paso el caso de la página del municipio de Francisco de Orellana en la cual personas hackearon la página web dejando un mensaje: *“somos Anonymous, somos*

legión, no perdonamos, no olvidamos, espéranos, la victoria para Anonymous".[1]

En el caso de nuestro país, no solo es el único implicado con estos problemas de personas malintencionadas, también tenemos el caso de países aledaños al nuestro y como es el caso de Colombia que: *"Bajo la frase el Gobierno quedó goleado, el conocido grupo de hackers Anonymous, dio a conocer su nuevo ataque a las páginas Web del gobierno colombiano. En esta ocasión, los portales afectados fueron los de la Presidencia de la República, el Senado, y los ministerios de Educación y Defensa"*.[2]

Así mismo tenemos el caso de advertencia de ataques, en el cual el más escuchado es el caso de la red social Facebook, el cual está amenazado con *"un ataque masivo el 5 de noviembre y hacer desaparecer a la red social más grande"*.[3]

Así como podemos notar, existen muchos casos de infiltraciones que no solo afecta a nuestro país sino afecta a todo el mundo, con lo que cada una de las empresas y personas buscan una forma de protegerse contra amenazas que surgen en vida actual, por lo que es importante saber por medio de un análisis como están nuestros dispositivos inalámbricos como debemos hacer para proteger nuestra información.

---

[1] Recopilado de: http://www.elmercurio.com.ec/291643-anonymous-anuncia-acciones-para-defender-libertad-de-expresion-en-ecuador.html
[2] Recopilado de: http://www.diariocritico.com/colombia/2011/Agosto/noticias/285076/anonymous-hackea-nuevamente-paginas-gubernamentales.html
[3] Recopilado de: http://ec.globedia.com/descargarte-datos-facebook

1.2 Diagnóstico o planteamiento de la problemática general

1.2.1 Causa

Las personas que utilizan un medio informático y que realizan el proceso de instalación, configuración, etc., no están al tanto si los procesos los realizan de una buena forma.

La gente que utiliza algún medio informático dentro de la institución se siente incómoda con la interacción que realiza con el equipo informático ya que se torna lento y no se puede trabajar con el mismo.

Cuando un estudiante o profesor de la institución se conecta a la red inalámbrica y el equipo no responde como uno lo quisiera, se genera molestias por la utilización de este servicio.

Un dispositivo que no cuente con una configuración deseada tiende a que los usuarios se sientan molestos con el servido dado.

La inversión que debe realizar la institución para adquirir alguna guía para contrarrestar estas molestias, no está contemplada en los presupuestos de la institución.

1.2.2 Efectos

El no realizar un análisis, hace que los procesos llevados por las personas encargadas de los medios informáticos, sigan cayendo en los mismos errores y no se tome correctivos para mejorarlos.

Considerar que las demoras en la interacción con un equipo informático tienden a dar problemas y molestias a los usuarios con los que pierden competitividad, productividad con procesos efectuados en la institución.

Al momento de que un usuario quiera conectarse a la red y no la pueda hacer genera malestar y baja notablemente el desempeño del usuario que utiliza el servicio de una red inalámbrica.

La no generación de una guía para saber cómo dar una buena configuración a un dispositivo disminuya el nivel de productividad del usuario.

La no inversión en una guía para que apoye el proceso en un medio inalámbrico para un buen funcionamiento de un dispositivo disminuirá el nivel de competitividad y productividad de los usuarios que se conectan a las redes inalámbricas.

1.3 Pronóstico y control del pronóstico

1.3.1 Pronostico

Crees usted que se pueden mejorar los procesos que se llevan a cabo en la institución por medio de un análisis que permita ver cuáles son las fallas que están cometiendo las personas encargadas de los medio informáticos.

Con la ayuda de este análisis cree usted que podríamos cambiar los procesos que se deben realizar en las redes Wi-fi de los laboratorios, para mejorar y tomar correctivos.

Con la creación de una guía, podremos dar una solución viable para saber en qué estamos fallando y resolver estas fallas en los procesos que tenemos para así mejorar la utilización de las redes inalámbricas en el Colegio Técnico Sudamericano.

1.3.2 Control del Pronóstico

Por este motivo en el Colegio Técnico Sudamericano se pretende realizar un análisis para ver cómo están manejándose los procesos para la utilización de los dispositivos de redes inalámbricas de los laboratorios, por lo que se realizara una propuesta de una guía de seguridad para redes Wi-Fi requiriendo la implementación si así lo creyeran conveniente, el uso de una guía es para prever o prevenir que los procesos que realiza el personal sea mucho más rápidos y sin inconvenientes, para así tener muchas más productividad, además de esto que se adapte a las necesidades y a la realidad que tiene la institución. Teniendo en cuenta que los procesos que se llevarán a cabo se los realizan en el menor tiempo posible, no habrá demora ni malestar para los usuarios que utilicen el servicio de Wi-Fi y así los usuarios se sentirán mucho mejor con el servicio dado por la institución y las redes inalámbricas estén configuradas confiablemente.

1.4 Formulación de la problemática especifica

1.4.1 Problema Principal

¿Permitirá la realización de un análisis ayudar para la correcta utilización y configuración de un dispositivo inalámbrico para el Colegio Técnico Sudamericano, conociendo puntos importantes en los que la institución y

la persona encargada está teniendo fallas, conociendo sus problemas, dando un propuesta de solución necesaria para las de redes inalámbricas Wi-Fi, para así asegurar el estado de la información de los usuarios que se conecten a una red inalámbrica?

1.4.2 Problemas Secundarios

- ¿Permitirá la creación de un análisis ver los problemas principales que tiene la institución, para así salvaguardar la información de los usuarios?
- ¿Permitirá la presentación de diferentes formas de protección mantener nuestros datos de forma segura y sin comprometer nuestra información?
- ¿Permitirá con la ayuda de la seguridad informática identificar las amenazas, debilidades, vulnerabilidades en los dispositivos Wi-Fi, dar la mejor protección para la conexión de un equipo informático?
- ¿Podrá identificar la utilización de una guía los puntos principales que debemos tomar en cuenta para minimizar los riesgos de amenazas?
- ¿Logrará una guía de seguridad brindar aspectos importantes sobre instalación, configuración y utilización de redes inalámbricas?

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar un análisis para la correcta utilización de un dispositivo inalámbrico, encontrando fallas, vulnerabilidades y riesgos de configuración en los dispositivos, dando una debida propuesta de solución para redes inalámbricas Wi-Fi, asegurando de mejor manera la información del usuario que se conecte a las misma desde los laboratorios del Colegio Técnico Sudamericano de la ciudad de Cuenca provincia del Azuay.

1.5.2 Objetivos Específicos

- Presentar un Cuadro comparativo entre las redes Wi-Fi vs LAN.
- Exponer la situación actual de la institución, indicando los problemas que se encuentra dentro de la misma.
- Identificar las amenazas y debilidades más comunes de los dispositivos inalámbricos.
- Indicar cuáles son los puntos principales que debe tener en cuenta para minimizar los riesgos de amenazas.
- Presentar las configuraciones más recomendables que se deben tomar para la buena configuración de un dispositivo inalámbrico.
- Indicar los aspectos más importantes sobre la instalación, configuración y uso de los dispositivos inalámbricos.
- Diseñar y Desarrollar una guía para la utilización correcta de los dispositivos inalámbricos.

1.6 Justificación

1.6.1 Teórica

Es importante decir que al realizar un análisis se prevé encontrar los errores o fallas que están cometiendo las personas encargadas de las redes inalámbricas, con lo cual si no se lo realiza tiende a seguir cayendo en los mismo errores y esto tiende a que personas mal intencionadas quieran dañar nuestra información y modificar nuestra configuraciones de los dispositivos.

Hoy en día la mayoría de dispositivos cuenta con un punto de acceso a Internet, con lo cual aumenta su exposición ante un sin número de amenazas que ni siquiera las personas que están en constante iteración están al tanto de esto, es por ellos que se ha vuelto muy importante estar protegido contra ataques que intentan aprovechar cualquier vulnerabilidad o falla para cometer el robo de informaron o daños en los sistemas informáticos.

A través de esto se presentará las diferentes formas de protección que la persona encargada de realizar el proceso de configuración de los dispositivos inalámbricos o simplemente una persona común, puede implementar para mantener sus dispositivos inalámbricos configurados muy confiablemente, sin ningún peligro y sin comprometer la información, para esto se debe dedicar mucho esfuerzo durante la instalación, configuración y uso de los dispositivos inalámbricos.

Es también importante mencionar que al momento de realizar esta guía la institución o simplemente las personas podrían adoptarlo y utilizarlo, para así poder tener sus medios seguros y no caer en ningún tipo de daño para su información.

Es muy importante también mencionar que al momento de desarrollar una guía para los dispositivos inalámbricos, no solo el Colegio Técnico Sudamericano se beneficiará con esto, ya que también esto servirá para cada uno de las instituciones y para las personas que necesiten saber cómo deben tener configurados sus dispositivos inalámbricos de una manera confiable y puedan cuidarse de un ataque malicioso, ya que se vieran con los mismos inconvenientes y tuviese una solución inmediata.

1.6.2 Metodológica

Para cada una de las herramientas o pasos que iremos revisando, empezaremos viendo la recolección de información, la cual debemos tener en consideración para poder realizar nuestro proyecto.

La creación de una guía de seguridad para la utilización, configuración de los dispositivos inalámbricos es una innovación para el Colegio Técnico Sudamericano, ya que este no cuenta con esta guía para poder contrarrestar alguna falla de configuración y defenderse de algún ataque malicioso. Así mismo no cuenta con configuraciones que le ayuden para salvaguardas sus datos de personas no autorizadas.

Con la generación de una guía simplemente las personas o instituciones que utilizan un dispositivos inalámbrico, podrían adoptarlo y utilizarlo

para apoyo de cómo deben tener a salvo su información y que no esté comprometida bajo ninguna persona que quiera hacer daño.

Es una gran ventaja tener un guía para la utilización de dispositivos inalámbricos, ya que sin esto no tendríamos seguridad alguna en los sistemas y en la información manejada.

Otra de las grandes ventajas que se tendría es a cuanto la conexión de los usuarios ya que no tendrán inconveniente a conectarse a la red inalámbricas del Colegio Técnico Sudamericano, con esto se llegará a dar una mayor productividad y competencia contra varias instituciones que no tiene desarrollada alguna guía y para tener los dispositivos inalámbricos trabajando correctamente.

También podemos decir que con la creación de una guía será una manera para que los dispositivos inalámbricos que contiene el Colegio Técnico Sudamericano estén mucho más protegidos contra ataques, ya que en la actualidad ningún equipo está 100% seguro de cualquier infiltración o daño.

1.6.3 Práctica

Esto será justificable puesto que el proyecto propuesto en el Colegio Técnico Sudamericano es una solución viable a las circunstancias que se presente en él en cuanto a los dispositivos inalámbricos, ya que al aplicar esta guía resolveremos los problemas planteados.

2. MARCO DE REFERENCIA.

2.1 Generalidades.

"El término red inalámbrica (Wirelessnetwork en inglés) es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos".[4]

La utilización de redes inalámbricas en la actualidad empieza a ser una alternativa muy viable a las redes locales cableadas, ya que con esto se elimina de sobre manera las restricción que reconoce la unión de un equipo a un cable físico.

La tecnología Wireless abarca diferentes puntos que puede ser desde teléfonos inalámbricos, micrófonos, dispositivos infrarrojos, hasta sistemas más complejos como pueden ser las Redes de Área Local Inalámbricas más conocidas como WLAN. Cada una de estas hoy a menudo son muy utilizados tanto en cada uno de los hogares como en empresas y con esto empiezan a sobresalir muchos más ataques y a su vez tenemos que contemplar muchas más medidas de seguridades.

Es importante mencionar una de las principales ventajas que nos proporciona una de ellas los costos, ya que con el simple hecho de eliminar todo el cableado Ethernet empieza con una reducción en los costos, pero así mismo tenemos una considerable desventaja que nos puede afectar

[4] Recopilado de: http://es.wikipedia.org/wiki/Redes_inalámbricas

duramente y es en la seguridad, en la cual tendremos que ser muchos más rígidos y tener mucho más robusto nuestros sistemas para evitar así intrusos no deseados.

Un dispositivo inalámbrico nos ayuda a interconectar dispositivos que nos permite enviar y recibir datos o información, con la interacción del usuario permite que estos dispositivos nos den la facilidad de estar conectados a un red para estar conectados y recibiendo información.

Pero como hoy en día existen muchas interrogantes que debemos conocer el mismo caso del funcionamiento de las tecnologías Wi-Fi, como operan, como trabajan las bandas de radiocomunicación, existen muchas interrogantes que con el transcurso de este proyecto podremos ir analizando y viendo cada uno de estas preguntas que nos hacemos.

2.2 Redes

2.2.1 Tipos de redes Inalámbricas.

En la actualidad existen diferentes tipos de redes inalámbricas, la cuales hoy en día se ven que tiene una acogida significativa en el medio, estas son utilizadas para conexiones sin necesidad de una conexión física (cables), es decir que se dan por medio de ondas electromagnéticas.

2.2.1.1 Wireless Personal Area Network

Una de red inalámbrica de área personal es un tipo de red de conexión personal que realiza la comunicación entre diferentes dispositivos ya sea Internet, teléfonos móviles, PDA, impresoras,

estos siempre estarán cercanos a una central o un punto de acceso, por lo general la misma un funcionan a unos pocos metros y para uso personal.

2.2.1.2 Wireless Local Area Network

Son conocidas como WLAN, son redes de área local que bajo una buena flexibilidad realizan una comunicación de datos inalámbricamente, es muy utilizado como una alternativa a las redes de área local cableadas o también como una extensión de ellas.

Estas redes utilizan tecnología de radio frecuencia que permite mucha mayor movilidad a cada uno de los usuarios, ya que al no contar con una conexión cableada permite un mejor cambio de lugar a lugar, estas redes cada día van adquiriendo mucha importancia en diferentes campos, ya sea hogares, almacenes, empresas, ya que la transmisión de información se la realiza en tiempo real y permite compartir el acceso a internet a varios ordenadores.

Estas también permiten conectar a una serie de equipos para compartir información, archivos, servicios, impresoras y cualquier otro recurso, sabiendo que estas utilizan señales de radio, estas son captadas PCMCIA (Tarjetas para ordenadores personales) conectadas a laptops o PC de escritorio.

Las Wireless LAN ofrecen ventajas sobre las LAN cableadas como son la movilidad, flexibilidad, escalabilidad, velocidad, costos

reducidos de instalación. Son una muy buena solución para cualquier empresa u hogar.

2.2.1.3 WirelessMetropolitanArea Network

Una de las redes que abarca por lo general una ciudad, estas son conocidas por ser redes metropolitanas, se encuentran tecnologías como WIMAX (Banda ancha de largo alcance), estas son por acceso con microondas, son parecidas a las redes Wi-Fi, pero con una mayor cobertura y ancho de banda.

2.2.1.4 Wireless Wide Area Network

Estas redes están encaminadas a abarcar una área geográfica mucho más extensa, esta permite a múltiples organismos como empresas, universidades y otras a conectarse a una misma red pero utilizando conexiones satelitales o por antena de radio de microondas, estas son flexibles, fácil de instalar y económicas.

La manera más común de implementar una red WAN es por medio de satélites, las mismas que se enlazan a una o más estaciones bases para la emisión y recepción. Estas utilizan una banda de frecuencia para recibir la información y luego en diferente frecuencia amplifican y repiten la señal para enviarla.

Para que una comunicación sea efectiva se necesita por lo general que los satélites permanezcan estacionario con respecto a la

posición sobre la tierra, y si no sucede esto cada una de las estacione en tierra perdería su conexión.

2.3 Seguridad

Empezar a definir un concepto de Seguridad no es un modo fácil, pero empezaremos a partir de una frase muy citada por el Dr. Eugene Spafford "El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto y cuidado por guardias muy bien armados, y aun así tengo mis dudas". Esta cita parece que no nos lleva a ningún lado, ni se asemeja a un concepto de seguridad, pero tenemos que notar que nos percata de 3 formas:

- No podemos decir ni hablar que existen sistemas totalmente seguros.
- Lo difícil que es tratar de asegurar un sistema.
- Y este conlleva a un proceso intensamente complejo.

Podemos decir que la seguridad viene dada en que un sistema se comporte como el usuario quiere que lo haga, y así mismo mantenerle libre de amenaza y riesgo. Por más de mucho tiempo se ha venido manejando la seguridad en base a tres parámetros conocidos como la triada de la seguridad: Confidencialidad, Integridad, Disponibilidad.

Figura 1: Triada de Seguridad

En la actualidad esta percepción de triada de seguridad ha sido sustituida por seis elementos de la información: Confidencialidad, posesión o control, integridad, autenticidad, disponibilidad y utilidad.

2.3.1 Elementos de la Seguridad.

2.3.1.1 Confidencialidad

El principio de confidencialidad, viene dado por asegurar que el nivel necesario de secreto se encuentra asegurado en cada instancia del procesamiento de datos, de tal manera de prevenir su divulgación a personas o individuos no autorizados a conocer los mismos.

Para tomar en cuenta este principio es muy importante saber que el nivel de confidencialidad debe prevalecer no solo cuando los datos residen en los sistemas y dispositivos de la red, sino que también en durante su transmisión y almacenamiento.

Para que se pueda garantizar la información existente se utiliza mecanismos de cifrado y de ocultación de las comunicaciones, estos

mecanismos de cifrado garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje, por tal razón, se debe determinar en cuanto tiempo el mensaje debe seguir siendo confidencial. Sabemos que no existe ningún mecanismo de seguridad completamente seguro.

Cuando la información confidencial ha sido accedida, usada, copiada o revelada por una persona no autorizada, se da entendido que se ha presentado un rompimiento de confidencialidad. La confidencialidad es un requisito indispensable para mantener la privacidad de las personas.

La misma es una propiedad de muy difícil recuperación, pudiendo minar la confianza de cada una de las personas de una organización.

2.3.1.2 Integridad

La integridad que se tiene en la información es la característica que hace posible garantizar su exactitud y confiabilidad, viendo para que su contenido permanezca inalterado por medios no autorizados o desconocidos a menos que sea modificado por personal autorizado, de modo autorizado y mediante los procesos autorizados.

Una característica muy importante que se debe dar en el momento de la modificación es que debe ser siempre registrada para luego realizar cualquier control.

2.3.1.3 Disponibilidad.

Esta es la manera de encontrarse siempre disponible, para ser utilizada por personas autorizadas, estos sistemas deben ser capaces de recuperarse de una manera rápida y segura de cada una de las paralizaciones que se den, a fin de que no se vea afectada la productividad.

2.3.1.4 Autenticidad.

Debe ser siempre posible para cada uno de los usuarios establecer el origen de la información, verificando su identidad. Cualquier atacante no debe poseer la capacidad de hacerse pasar por otro usuario.

2.3.1.5 Posesión o Control

Es la capacidad de mantener, controlar y tener destreza de usar la información. La posesión se da cuando la persona realmente posee, controla y usa la información.

2.3.1.6 Utilidad

Este consiste en la utilidad que tiene la información, ya que cada dato o información que se tiene, no sirve y es útil para algún propósito que requerimos utilizar.

2.3.2 Amenazas, Vulnerabilidades y Riesgo.

Dentro de cada uno de los campos de la informática existen riesgos, amenazas y vulnerabilidades que son diferentes.

2.3.2.1 Amenazas

Las amenazas son una causa potencial de algo no deseado, que causa daño a cualquier sistema. Estas se clasifican en naturales, involuntarias e intencionales.

Las amenazas naturales son los que ponen en peligro cada uno de los componentes, dispositivos de la red. Se distinguen por desastres naturales como inundaciones, rayos, terremotos, humedad, presencia de polvo.

Las involuntarias viene dado por el uso descuido de un dispositivo o equipo. Las intencionadas son originadas por usuarios que quieren acceder a la red para poder modificar, borrar, robar la información o simplemente por diversión.

Las amenazas humanas vienen dadas por diferentes aspectos conocidos como personas malintencionadas que pueden hacer daño a nuestros dispositivos de los cuales podemos decir:

- Hacker: usuario que busca superarse que posee conocimientos elevados, pero su trabajo es completamente legal.

- Cracker: personas que busca hacer daño o violar las seguridades de los sistemas o dispositivos.
- Insider: Persona interna que trabaja en una organización, utilizan sus permisos para alterar la información o a los sistemas.

2.3.2.2 Vulnerabilidad

Viene dada por la debilidad de diferentes recursos que son aprovechadas por una o varias amenazas. Esto se da ya que no existen controles que evitan amenazas y que por ende afectan al entorno informático.

En el entorno de las redes inalámbricas las vulnerabilidades se pueden dar por la intercepción de la señal de transmisión de datos.

2.3.2.3 Riesgo

Esta dado por la estimación del grado de exposición a que cualquier amenaza se materialice sobre uno o más de los activos, causando daños a una organización.

Los riesgos indican lo que podrían pasar a cada uno de los activos sino tiene una protección adecuada.

Es siempre muy importante tomar medidas de protección para la seguridad en cada una de las instituciones u organizaciones sin importar si estas son grandes medianas o pequeñas.

2.3.3 Seguridad Informática de redes de Computadoras

2.3.3.1 Intercepción

Esto son accesos a la información por parte de personas no deseadas o no autorizadas, usa privilegios no adquiridos. Su detección se torna muy difícil. Por ejemplo copias ilícitas de programas.

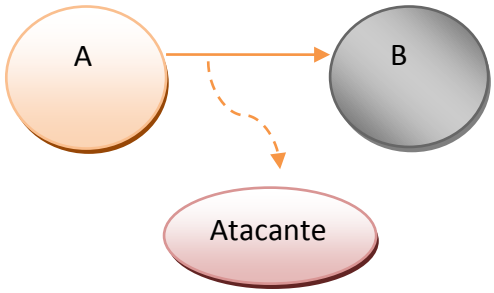

Figura 2: Ataque de Interceptación

2.3.3.2 Interrupción

Se puede señalar que un ataque es una interrupción si se logra que algún elemento se dañe, se pierda o simplemente que deje de funcionar algún punto del sistema. Su detección es inmediata. Por ejemplo borrado de datos, programas destrucción de hardware.

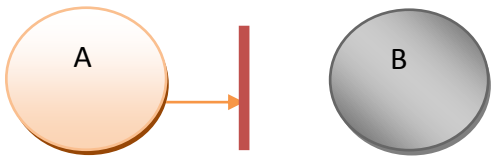

Figura 3: Ataque de Interrupción

2.3.3.3 Modificación

Este ataque se da luego que se realiza la interceptación, logrando modificar y cambiar el entorno para su beneficio. Su detección se torna difícil según las circunstancias que se presenten. Por ejemplo modificación de base de datos.

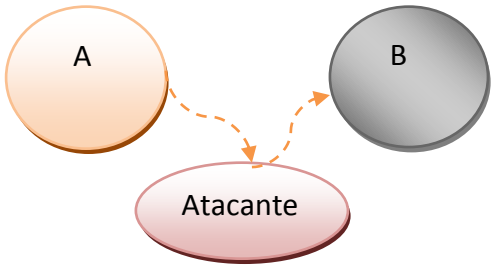

Figura 4: Ataque de modificación

2.3.3.4 Fabricación

Se entiende como fabricación cuando el atacante crea nuevos objetos dentro del sistema, el cual es muy difícil de poder distinguir si es un elemento genuino. Su detección es difícil. Por ejemplo añadir registros a la base de datos.

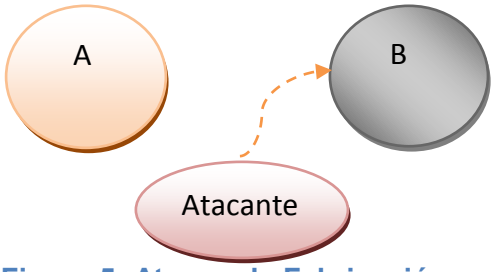

Figura 5: Ataque de Fabricación

2.4 Redes Inalámbricas Wi-Fi de Área Local

Las redes inalámbricas Wi-Fi son comúnmente WLAN, estas son redes que cubren distancias de 10 a 100 metros, esta cobertura permite una pequeña

cobertura y una menor potencia de transmisión pero que en la actualidad se utiliza mucho en instituciones, empresas u hogares.

Entre los dispositivos que usualmente son utilizados para la interconexión inalámbrica se encuentran equipos portátiles, de escritorio, asistente digitales, teléfonos celulares. Las tecnologías inalámbricas tienen muchos usos prácticos. Por ejemplo cuando una persona está con un equipo portátil pueden conectarse a Internet a través de estaciones bases instaladas en diferentes partes ya sea lugares públicos, en casa los usuarios pueden conectarse con su equipo de escritorio y sincronizar datos y transferir archivos.

El estándar IEEE 802.11 o también llamado WI-Fi fue definido por el Instituto de Ingeniero Eléctricos y Electrónicos como un estándar que reemplazaría los cables de conexión alámbrica Ethernet con una conexión inalámbrica.

2.4.1 Topología de red inalámbrica.

Existen diferentes tipos de topologías dependiendo de la disposición lógica o física de una red, las topologías, no centraremos en las lógicas, en cómo se comunican los dispositivos.

2.4.1.1 Ad-hoc

Esta topología se caracteriza por que no tiene ninguna administración central, es decir no hay un nodo central o un punto de

acceso, las estaciones de trabajo se comunican directamente entre sí, estableciendo enlaces punto a punto.

Esta es el modelo más simple de una red inalámbrica, en el cual radica en colocar estaciones de trabajo con una tarjeta de red inalámbrica que estén al alcance y que se encuentren en la misma área.

Figura6: Ad-hoc

2.4.1.2 Infraestructura

El objetivo principal es la de centralizar todas las comunicaciones, es decir que se tiene como mínimo un ponto de acceso, ninguna comunicación se lo puede realizar directamente, ya que primero se debe pasar por un punto de acceso.

Un punto de acceso cubre por lo menos 100 metros a la redonda, tomando en cuenta el tipo de antena y los impedimentos que puede haber en el rango de cobertura.

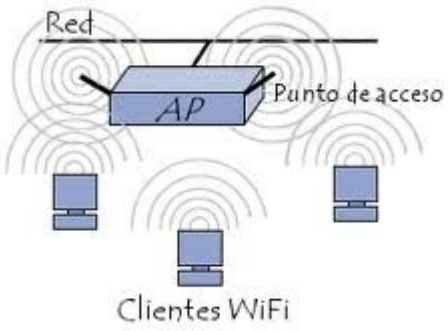

Figura 7: Modo Infraestructura

En este tipo el punto de acceso primero trabaja como una LAN, distribuyendo ya sea datos, internet a cada una de los clientes los cuales se conecta a un punto de acceso.

2.4.1.3 Mesh

Esta es una red en malla implementada sobre una red inalámbrica. Es la unión de la topología Ad-hoc y la topología infraestructura. En estas la comunicación se descentraliza y cada uno de los dispositivos que intervienen en la comunicación puede compartir recursos. Es resistente a fallos, pues la caída de un nodo no afecta ni implica la caída de toda la red.

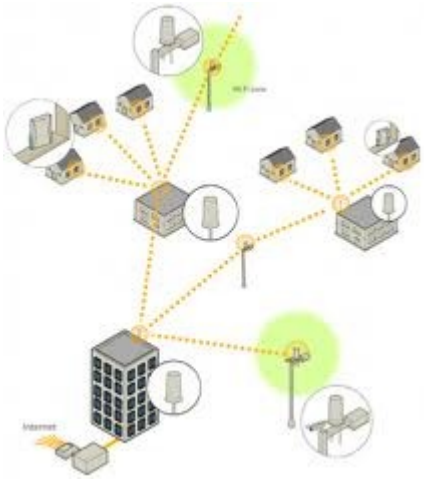

Figura 8: Mesh

2.4.2 Componentes de una red inalámbrica

2.4.2.1 Punto de Acceso.

Es un concentrador inalámbrico central que se encarga de receptar información, ya que cuando el transmisor y receptor se conectan entre sí para recibir datos, se centraliza para su envió o enrutamiento. Es decir que cada uno de los equipos que se conectan están enlazados por un hub o switch para que empiecen a repartir los paquetes.

En las redes Wi-Fi son muy similares, ya que existe un dispositivo que gestiona los paquetes enviados por otras estaciones inalámbricas, haciendo llegar a su destino el paquete. Además de esto podemos añadir que estando conectando hacia una red cableada, la red inalámbrica puede acceder a otros equipos que estuvieran dentro de la red cableada.

2.4.2.2 Clientes inalámbricos.

Esta es cualquier estación inalámbrica que nos proporcione conectividad a una red local inalámbrica para compartir sus recursos. Es decir que se puede definir a una estación inalámbrica como un computador con una tarjeta instalada que transmite y recibe señales.

Las más conocidas son las PCMCIA para portátiles, ya que para PC de escritorio están en formato PCI, USB, etc.

2.4.2.3 Gateway

Es un dispositivo que permite interconectar redes entre protocolo y arquitecturas diferentes. El propósito principal es la de traducir la información del protocolo al protocolo de destino.

2.4.2.4 Router

Este es un dispositivo que permite la interconexión entre redes, el cual permite asegurar el direccionamiento de paquetes de datos o determinar la mejor ruta que debe tomar.

2.4.3 Estándares IEEE 802.11

“El estándar 'IEEE 802.11' define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama

802.x definen la tecnología de redes de área local y redes de área metropolitana".[5]

Este estándar define y gobierna las redes de área local inalámbricas que operan en el espectro de los 2,4 GHz. El estándar original aseguraba la interoperabilidad entre equipos de comunicación dentro de cada una de estas tecnologías inalámbricas, pero no entre las tres tecnologías. Desde entonces, muchos estándares han sido definidos dentro de la especificación IEEE 802.11 que permiten diferentes velocidades de operación.

2.4.3.1 Estándar IEEE 802.11b

La extensión de estándar es la base para la mayoría de las LANs inalámbricas que existen en la actualidad 802.11b opera en una banda de 2.4 GHz y permite velocidades de 1, 2, 5.5 y 11 Mbps utilizando DSSS (Espectro ensanchado por secuencia directa), la cual es un método de modulación en espectro ensanchado para la transmisión de señales digitales sobre ondas radiofónicas, estas generan un patrón de bits redundante para cada uno de los bits que componen la señal. Cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias, y utiliza una modulación CCK (ComplementaryCodeKeying) para dispersar la señal de datos, CCK es utilizada para redes inalámbricas digitales para lograr una mayor velocidad de datos.

[5] Recopilado de: http://es.wikipedia.org/wiki/IEEE_802.11

"El estándar 802.11b define una única técnica de modulación para las velocidades superiores - CCK - al contrario que el estándar original 802.11 que permitía tres técnicas diferentes (DSSS, FHSS e infrarrojos). De este modo, al existir una única técnica de modulación, cualquier equipo de cualquier fabricante podrá conectar con cualquier otro equipo si ambos cumplen con la especificación 802.11b. Esta ventaja se ve reforzada por la creación de la organización llamada WECA (Wireless Ethernet Compatibility Alliance), una organización que dispone de un laboratorio de pruebas para comprobar equipos 802.11b. Cada equipo certificado por la WECA recibe el logo de compatibilidad WI-FI que asegura su compatibilidad con el resto de equipos certificado"[6]

Rango de Frecuencia	De 2.4 a 2.4835 GHz
Acceso	Direct Sequence Spread Spectrum (DSSS) usando Complementary Code Keying (CCK)
Velocidad	Hasta 11 Mbps
Compatibilidad	Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación	Todo tipo de red de datos Ethernet

Figura 9: Tabla Resumen Estándar IEEE 802.11b

[6]Recopilado de: http://www.x-net.es/tecnologia/wireless.pdf

2.4.3.2 Estándar IEEE 802.11b+

"Es una variación del IEEE 802.11b pero que puede operar a 22Mbps contra los 11Mbps de la versión 11b. Su mayor problema es que no es un estándar. Aunque aparece en la mayoría de las documentaciones como IEEE 802.11b+, IEEE nunca lo ha certificado como estándar. Es un sistema propietario diseñado por Texas Instruments y adoptado por algunos fabricantes de dispositivos inalámbricos como D-Link y Global Sun que utilizan estos chipsets. Técnicamente utiliza técnicas que forman parte del estándar 11g. Comparativamente con el resto de estándares no ofrece grandes diferencias, ya que aunque anuncia velocidades de 22Mbps en prestaciones reales se obtiene una discreta mejor".[7]

2.4.3.3 Estándar IEEE 802.11g

La más reciente es la 802.11g, el cual asegura la compatibilidad de los equipos Wi-Fi preexistente. De la misma forma a 802.11b, 802.11g opera en la banda de 2.4GHz. El estándar 802.11g es compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir de hasta los 54Mbits/s para competir con los otros estándares que prometen velocidades mucho más elevadas.

"Para aquellas personas que dispongan de dispositivos inalámbricos de tipo Wi-Fi, 802.11g proporciona una forma sencilla de migración a alta velocidad, extendiendo el período de vida de los dispositivos de

[7] Recopilado de: http://es.wikipedia.org/wiki/IEEE_802.11

11Mbps. El estándar 802.11g se publicó como borrador en Noviembre de 2001 con los siguientes elementos obligatorios y opcionales:

- *El método OFDM (OrthogonalFrecuancyDivisionMultiplexing) es obligatorio y es lo que permite velocidades superiores en la banda de los 2,4GHz.*
- *Los sistemas deben ser totalmente compatibles con las tecnologías anteriores de 2,4GHz Wi-Fi (802.11b). Por lo que el uso del método CCK (ComplementaryCodeKeying) también será obligatorio para asegurar dicha compatibilidad.*
- *El borrador del estándar marca como opcional el uso del método PBCC (PacketBinaryConvolutionCoding) y el OFDM/CCK simultáneo"*[8]

Rango de Frecuencia	De 2.4 a 2.4835 GHz
Acceso	Obligatoriamente ComplementaryCodeKeying (CCK) y OrthogonalFrecuencyDivisionMultiplexing (OFDM), opcionalmente puede incluir PacketBinaryConvolutionCoding (PBCC) y CCK/OFDM
Velocidad	Hasta 54 Mbps

[8] Recopilado de: http://es.wikipedia.org/wiki/IEEE_802.11

Compatibilidad	Compatible con sistemas 802.11b de 11Mbps y 5,5Mbps. Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación	Todo tipo de red de datos Ethernet

Figura 10: Tabla Resumen de Estándar IEEE 802.11g

2.4.3.4 Estándar IEEE 802.11a

Este estándar se aplica a la banda UNII (Infraestructura de Información Nacional sin Licencia) opera en la banda de 5 GHz. El mismo utiliza el método OFDM[9] (Multiplexación por División de Frecuencias Ortogonales), esto lo hace para la transmisión de datos hasta los 54 Mbps. OFDM Es una multiplexacion que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.

Su mayor inconveniente viene dado por la incompatibilidad con los estándares de 2,4 GHz. Por lo demás toda su operación es muy parecida al estándar 802.11g.

[9]Ver: http://es.wikipedia.org/wiki/OFDM

Rango de Frecuencia	De 5,15 a 5,25 GHz De 5,25 a 5,35 GHz De 5,725 a 5,825 GHz
Acceso	Orthogonal Frequency Division Multiplexing (OFDM)
Velocidad	Hasta 54 Mbps
Compatibilidad	No compatible con los sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF
Distancia	Depende de la instalación y de los obstáculos
Aplicación	Todo tipo de red de datos Ethernet

Figura 11: Tabla Resumen de estándar IEEE 802.11a

2.4.3.5 Estándar IEEE 802.11n

Es un sistema muy novedoso que se basa en tecnología MIMO (Multiple input Multiple output), que es una forma de manejo de las ondas de transmisión y recepción, usa múltiples antenas transmisoras y receptoras para mejorar el desempeño, permitiendo más información pero siempre cuidado la coherencia. Esta tecnología es multi-señal con lo que existen una onda primaria y varias ondas secundarias.

Esta tiene un incremento significativo en la velocidad máxima de transmisión de 54 Mbsp a un máximo de 600 Mbsp. Actualmente

soporta una velocidad de 300 Mbps en la capa física, con el uso de dos flujos espaciales en un canal de 40 MHz.

2.4.3.6 HiperLAN2

Es desarrollada bajo el proyecto BRAN (Redes de acceso radioeléctrico de banda ancha) del Instituto Europeo de Estandarización de las Telecomunicaciones.

Este es muy similar al estándar IEEE 802.11a, ya que estos usan una banda de 5 GHz y también utilizan el mismo método OFDM el cual obtiene velocidades de hasta 54Mbps.

La diferencia fundamental de estas está el control de acceso a medio (MAC), ya que HiperLAN2 se orienta más a la conexión. Debido a las características, HiperLAN2 será usado inicialmente pasa interconexiones WAN entre nodos. Actualmente IEEE 802.11a no ofrece diversidad de canales con QoS variables, por lo que se le compara con Wireless Ethernet, mientras que a HiperLAN2 es más parecida a un ATM inalámbrico.

Rango de Frecuencias	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso	Orthogonal Frequency Division Multiplexing (OFDM)
Velocidad	Hasta 54 Mbps

Compatibilidad	No compatible con los sistemas 802.11g, 802.11b, 802.11, ni con HomeRF
Distancia	Depende de la instalación y de los obstáculos, máximo 150m
Aplicación	WAN/LAN, voz encapsulada, vídeo, dato

Figura 12: Tabla Resumen de estándar HiperLAN2

2.4.4 Protocolo en redes inalámbricas.

Existen diferentes protocolos que se utilizan para la encriptación de datos de red inalámbrica.

2.4.4.1 WEP

Se encuentra en basado en algoritmo RC4 (Sistema de Cifrado de Flujo), el WEP es un algoritmo de seguridad que está en la norma IEEE 802.11. Este fue el primer protocolo de encriptación.

Los objetivos de este son proporcionar confidencialidad, autentificación y control de acceso en rede WLAN, las características que incorpora este protocolo es la de utilizar una misma clave simétrica y estática en las estaciones y el punto de acceso.

Esta también no contempla mecanismos de distribución automáticas de claves, lo que es obligado a escribir la contraseña manualmente, con esto conlleva a varios inconvenientes. Por un lado la contraseña se almacena en todas las estaciones y por otro lado provoca el

mantenimiento de parte del administrador de la red, con lo que la contraseña se cambia poco o nunca.

El algoritmo utiliza una clave secreta de 40 bits que se combina con un vector de inicialización de 24 bits para encriptar el mensaje. El vector de inicialización es la clave de seguridad WEP, en donde para poder mantener el nivel de seguridad y minimizar la difusión el vector de inicialización debe ser aplicado a cada paquete.

Este protocolo actualmente se ha comprobado que es vulnerable ante problemas de RC4, ya que en este existen dos vulnerabilidades en el algoritmo de encriptación, las cuales son de no-variación y ataques de vector de inicialización conocidos. Es importante también mencionar que en la etapa de comprobación de integridad también sufre de serias debilidades por razones del algoritmo CRC32, este algoritmo es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida.

2.4.4.2 WAP

WPA soluciona las debilidades conocidas de WEP y se considera que este es suficientemente seguro. WPA utiliza el protocolo de integridad temporal el cual es diseñado para re direccionar todos los ataques de las direcciones conocidas y deficiencias del algoritmo WEP.

Con la ayuda de TKIP defiende contra ataques débiles e insistentes, este descubre que ha existido una modificación del mensaje y evita el uso continuo de una misma llave, TKIP es un protocolo de seguridad para mejorar el cifrado de datos.

Para tener un mejor control de acceso y autenticación de usuarios, WPA lleva a cabo el control de autenticación extensible y el estándar IEEE 802.1x para el control de acceso al puerto. Este escudo usa la autenticación remota dial en el servicio de usuario, sabiendo que si se utiliza un servidor de autenticación, este puede autenticar a cada usuario en la red.

WPA trabaja obteniendo los 128 bits de clave temporal de escudo EAP durante la autenticación y entradas, conjuntamente con una función de password junto con la dirección del transmisor de 48 bits y el vector de inicialización de 48 bits.

Es importante saber que el EAP es un protocolo de transporte entallado a las necesidades de protocolos de autenticación de capa superior, permite un mayor rango de tamaño de bloques y longitud de claves.

2.4.4.3 WPA2

WPA2 introdujo diversos cambios fundamentales, como es el caso de la separación de la autenticación de usuario de la integridad y privacidad de los mensajes proporcionando una arquitectura mucho

más robusta y sobre todo escalable, este sirve para toda red doméstica como para redes corporativas.

La nueva arquitectura se llama RSN (Robust Security Network) y utiliza una autenticación 802.1x, distribución de claves robustas y nuevos mecanismos de integridad privacidad.

Además de que esta tiene una arquitectura más completa, RSN proporciona soluciones escalables y seguras para las comunicaciones inalámbricas, pero solo aceptara maquinas con capacidades para la misma.

IEEE 802.11i que es la llamada WPA2 define una red transicional de seguridad TSN (Transitional Security Network), en los que esta arquitectura podrá incursionar sistemas RSN y WEP, permitiendo que los usuarios puedan actualizar sus equipos a futuro.

Existen 4 fases importantes para el establecimiento seguro de comunicación, los cuales podemos mencionar los siguientes:

- Acuerdo sobre la política de seguridad.
- Autenticación 802.1x.
- Derivación y distribución de las claves.
- Confidencialidad e Integridad de los datos RSNA.

Todas estas claves que se generan se usan en protocolos que soportan la confidencialidad integrada de datos RSNA.

2.4.4.4 IPSec

Es un protocolo de comunicación (Internet Protocol Security), el cual es un conjunto de protocolos, que provee opciones avanzadas de seguridades tales como algoritmo de encriptación de la información más avanzadas en una autenticación de usuarios más exhaustiva.

En IPSec tiene dos modos de autenticación, dependiendo del nivel sobre el que se actué, los mismos que son:

- Modo Transporte, el cual solo encripta el transporte de los paquetes.
- Modo Túnel, este encripta la cabecera de cada paquete de información

IPSec proporciona protección de retiro y repitiendo la protección con la autenticación mutua a través del uso de cliente de servidores certificados. Para poder utilizar este protocolo seguro solo dispositivos certificados lo pueden hacer.

2.4.5 Encriptación

Es la manera de asegurar la información para que sea ilegible y no la pueda modificar la información importante, esta funciona con algoritmos en los cuales de una pequeña información se transforma a una muy extensa y difícil de descifrar.

La encriptación tiene como propósito evitar que personas no autorizadas puedan modificar la información, dotado cada vez de más tecnología y utilizando algoritmos cada vez más seguros.

2.4.5.1 Encriptación Simétrica

Con esta encriptación nos permite que la información almacenada y que es crítica pueda ser cifrada y descifrada por una misma persona, y a esta nadie podrá tener acceso, ya que la persona que la cifro es la única que podrá tener acceso a la misma.

Existen algunos algoritmos que son más seguros que otros. La llave Key es unas de las principales maneras para encriptar y desencriptar la información, ya que toda seguridad depende de esta llave, como está compuesta y quien tiene acceso a ella.

2.4.5.2 Encriptación Asimétrica

Con referencia a la Simétrica esta permite que 2 personas puedan enviar información encriptada, sin entregar la llave de seguridad, esta utiliza dos llaves, la primera para encriptar todo el texto y la otra para desencriptarla, ya que no se puede desencriptar con una misma llave pública, entonces para desencriptarla se necesita tener una llave privada.

2.5 Marco Temporal/Espacial

2.5.1 Marco Temporal

El tiempo que nos tome realizar este proyecto en base a todos los objetivos que nos hemos planteado y se estudiaran, será aproximadamente en unas 6 semanas para la culminación del mismo.

2.5.2 Marco Espacial

El proyecto en el cual contendrá una investigación y desarrollo de una guía de seguridad para la correcta utilización, configuración de dispositivos inalámbricos se realizará en el Colegio Técnico Sudamericano, los cuales proveerán de toda la información y equipos necesarios para realizar este proyecto.

3. METODOLOGÍA Y ANALISIS DEL ENTORNO

3.1 Generalidades

El Colegio Técnico Sudamericano se encuentra ubicado en las afueras de la ciudad en las calles 25 de marzo y vía San Miguel, con un espacio muy cómodo para el trabajo de los estudiantes y docentes del colegio.

En este capítulo definiremos la situación actual de la institución, dando a conocer los procesos que se están realizando en cuanto a la utilización de los dispositivos inalámbricos, realizando un análisis de los mismos, con lo cual esto se realiza con recursos materiales que pertenecen a la institución.

Para poder realizar todo este análisis deberemos recoger, agrupar y avaluar evidencias para determinar si la información esta salvaguardad en la institución, manteniendo la integridad de los datos, utilizar eficientemente los recursos y cumpliendo con las leyes y regulaciones establecidas.

Es este caso estudiaremos los mecanismos de control que están implantados en la institución u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

En los últimos tiempos las redes inalámbricas han ganado un espacio muy significativo y se ha ganado mucha popularidad en todo mercado hogares, hospitales, áreas de negocios, instituciones, organizaciones, etc.

El uso de las redes inalámbricas permite el uso de recursos y acceso a la información en tiempo real, sin la necesidad de estar conectados físicamente a un lugar de trabajo. Con la ayuda de WLAN se elimina la necesidad de usar cables y establecer una mayor flexibilidad a la red, y los que es importante para cada organización que la de elevar su productividad y eficiencia en cada una de las actividades diarias que se realizan.

3.2 Metodología de Investigación.

3.2.1 Unidad de Análisis.

En la investigación y desarrollo para la creación de una guía de seguridad para dispositivos inalámbricos se lo realizará en las redes inalámbricas de los laboratorios del Colegio Técnico Sudamericano de la ciudad de Cuenca, provincia del Azuay, ubicado en las calles 25 de Marzo y Vía a Ricaurte.

3.2.2 Tipo de Investigación.

Se utilizará la investigación aplicada, en la cual se podrán todos los conocimientos adquiridos para recolectar información que ayude a realizar el proyecto, ya que está dirigida a la aplicación de teorías, con la finalidad de resolver los problemas que se suscitan.

Existen características principales que podemos mencionar como:

- Recoger, registrar y analizar los datos obtenidos.

3.2.3 Método.

El método escogido y a utilizar es el inductivo-deductivo, en el cual se parte de la realidad de la obtención de datos mediante un proceso llamado inducción, luego mediante un proceso llamado deducción organizar los datos en forma de leyes, teorías y modelos para finalmente ser contrastados con la realidad.

3.2.4 Técnicas.

Sera necesario la utilización de técnicas como la Observación, en la cual se deberá observar atentamente los hechos, fenómenos o casos, la cual detectará y asimilará, la información utilizando los sentidos como instrumento, para registrarla para posteriormente poder analizarla.

A su vez se utilizara la técnica de la entrevista, la misma que nos ayuda para obtener información, la cual consiste en un dialogo entre dos personas, acerca de cómo funcionan los procesos de la institución, con el objetivo de obtener datos exactos e información valiosa. Existen características que tenemos que tomar muy en cuenta:

- Debe ser planificada previamente. Redactar con tiempo las preguntas, asegurar con tiempo la entrevista.
- Cuando se hace entrevistas a varias personas las preguntas tienen que ser las mismas para todos, para facilitar la tabulación.

- El entrevistador tiene que ser consecuente con el entrevistado y no pensar nunca que es más, cuando es el que entrevista el que se beneficia del entrevistado.

3.3 Análisis del Entorno.

3.3.1 Levantamiento de la información.

En el Colegio Técnico Sudamericano cuenta con diferentes Áreas en las que se encuentran interconectadas las mismas, las cuales están en contante uso y están siempre disponibles los recursos que proporciona la red interna, las mismas que están definidas de la siguiente manera:

- Departamento IT
- Área Administrativa
- Laboratorios

3.3.2 Definición de la Arquitectura Actual

La arquitectura con la que cuenta el Colegio Técnico Sudamericano la definiremos en base a un diagrama, en la cual obtendremos información de cómo está estructurada cada una de las áreas de la institución, con esta información sabremos cómo está distribuida y las aéreas a las que nos vamos a encaminar.

En el grafico que nos proporciona el Departamento IT notamos la estructura con la cual cuenta el Colegio Técnico Sudamericano, en la cual podemos ver que existe diferentes áreas como es el caso del Área de Laboratorios, Área Administrativa y Área de IT, con lo cual

empezaremos definiendo cada uno de ellos para ver qué es lo que tenemos en los mismos.

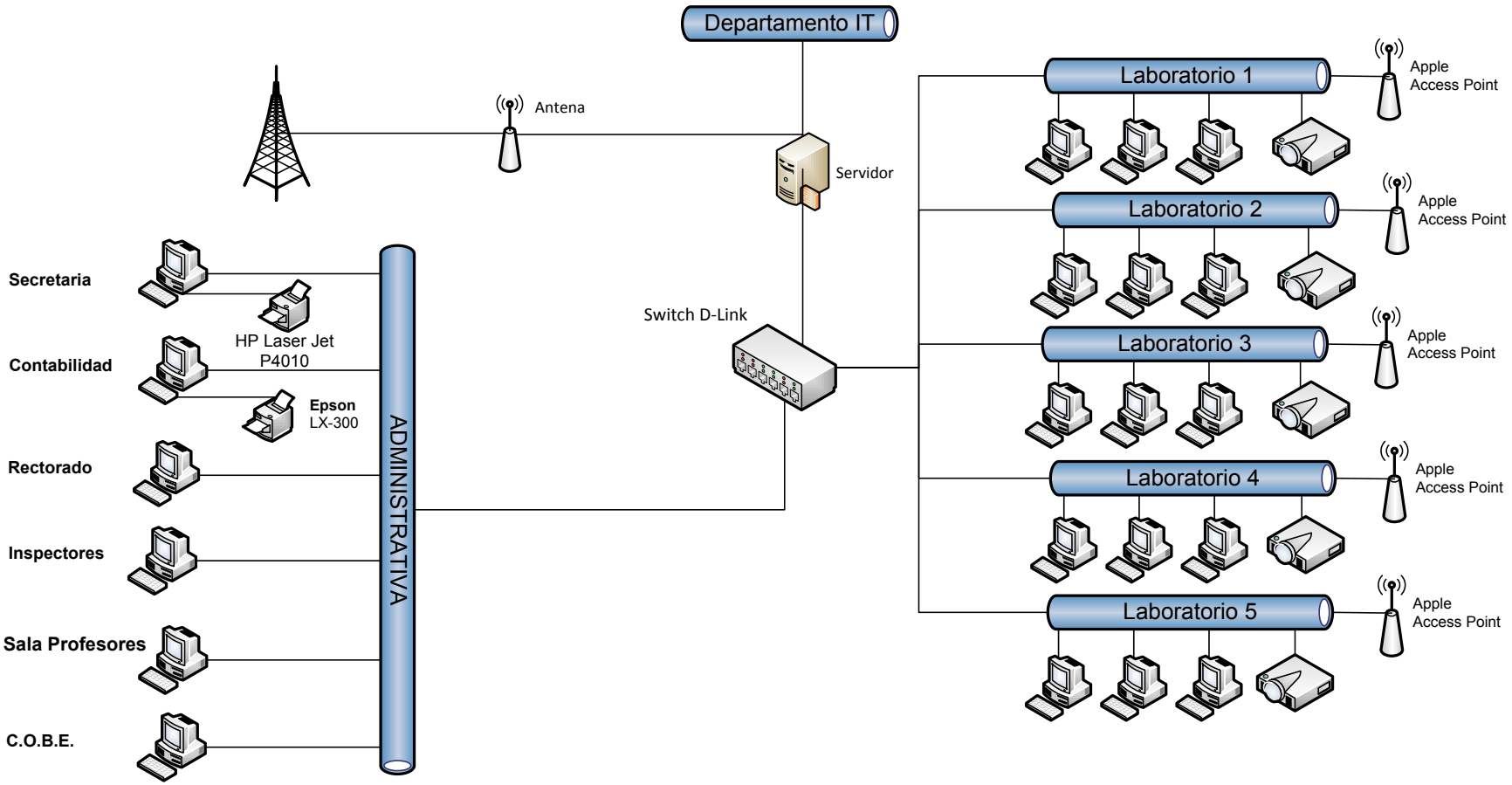

Figura 13: Arquitectura Colegio Técnico Sudamericano

3.3.3 Área IT

En esta área consta de todas las conexiones y las distribuciones para toda la institución, la cual está definida de la siguiente manera, en primer lugar se tiene un enlace de internet que es proporcionado por la empresa Punto NET, la misma que es la encargada de dar soporto y conexión empresarial de internet, la compresión del ancho de banda es de Dos a Uno.

Este enlace se conecta a una Antena en la parte superior de la edificación del colegio, la misma señal que es transferida a un equipo servidor que es el firewall, donde este va a realizar el re-direccionamiento a los diferentes equipos de toda la red interna de la institución.

En el área de IT, se encuentran los diferentes Switch que permiten la distribución del internet y los datos para toda la red interna del colegio.

3.3.4 Área Administrativa

En esta área comprende la parte administrativa y académica del colegio, la misma que cuenta con los siguientes usuarios:

- Rectorado
- Vicerrectorado
- Secretaria
- Colecturía
- Contabilidad
- DOBE

- Inspección General
- Inspecciones por bloque
- Sala de Profesores

Cada uno de estas oficinas cuenta con equipos que están conectados a la red interna del colegio, con lo cual toda esta parte comprende un número total de 19 equipos, los mismos que están instalados con un sistema operativo Windows XP SP3, el cual es un sistema que en la actualidad las empresas están utilizando.

Cada uno de los equipos están conectando con una tarjeta de red Ethernet de 10/100Mb, y estas están siempre conectado en un horario de 07H00 de la mañana a 16h00 de la tarde, teniendo internet y enlace de datos en todo momento.

3.3.5 Área de Laboratorios.

En esta área el Colegio Técnico Sudamericano cuenta con 5 laboratorios para la instrucción de la educación a estudiantes de secundaria, son laboratorios que cuenta con varios equipos informáticos para el aprendizaje de los mismos, con lo que en la tabla a continuación mostrada detallamos todo lo que tienen estos laboratorios.

	#Pc	Monitores	Teclados	Mouse	Proyector	Access Point
Laboratorio 1	11	41	41	41	1	1

Laboratorio 2	11	41	41	41	1	1
Laboratorio 3	11	41	41	41	1	1
Laboratorio 4	11	41	41	41	1	1
Laboratorio 5	35	35	25	25	1	1

Figura 14: Tabla de Equipos de Laboratorios

Aquí como podemos notar los laboratorios cuentan cada uno con 11 equipos de los cuales trabajan con dispositivos Ncomputing X300 y X350, estos son dispositivos que ayudan al trabajo en multiusuario, que nos permiten compartir una PC para varios usuarios, por lo que con ellos se logra abarcar a 41 usuarios en los laboratorios, cada uno de estos cuentan con sus monitores, teclados, mouse, y en cada laboratorios cuenta con un proyector para mejorar el aprendizaje de los estudiantes.

En cada uno de los equipos de los laboratorios del Colegio Técnico Sudamericano cuenta también con una tarjeta de red inalámbrica, la cual permite la conexión a Internet con un Access Point, la tarjeta inalámbrica utilizada para la conexión entre dispositivos es una D-link, 10/100Mb, esta tarjeta es una PCI que se encuentra en cada una los equipos que siempre estará conectada con el Access Point del laboratorios.

El Access Point es un dispositivo que transmite la señal inalámbrica a cada uno de los equipos, el cual estará dando conexión a la red, y estos estarán conectados y navegando en el Internet, por lo que en todo momento se tendrá una conexión con los recursos que tiene la institución.

También podemos mencionar que cada uno de los equipos informáticos cuenta con un sistema operativo Windows XP Service Pack 3, el mismo que esta instalo en cada uno de los 4 laboratorios, y el quinto laboratorio está instalado Ubuntu 10.04, ya que la educación que se transmite a cada uno de los estudiantes se trabaja en diferentes plataforma para así lograr hacerlos conocer los diferentes sistemas que existen en la actualidad.

Los laboratorios cuentan con un espacio suficiente para cada uno de los usuarios se conecten a la red, dando comodidad para que el usuario se sienta de lo mejor para que su estudio sea mucho más productivo estos empezaran a funcionar desde el inicio de clases de los alumnos.

Como vemos en el Cuadro 4, existen en cada uno de ellos un Access Point o punto de acceso, el cual estará dando la conexión a Internet y a la red interna del colegio, estos Access Point siempre pasaran encendido las 24 horas del día.

3.3.6 Usuarios Conectados.

Es muy importe saber de dónde ingresa el tráfico de red o de donde se genera todo este tráfico, por lo que se ha pedido al administrador de sistemas del Colegio Técnico Sudamericano nos proporcione donde existe el número más alto de accesos a los recursos de la red, con lo cual teniendo un análisis de donde ingresan más personas a la red sabremos que es el punto principal donde tenemos que encaminarnos, por lo que nos proporciona cifras importantes.

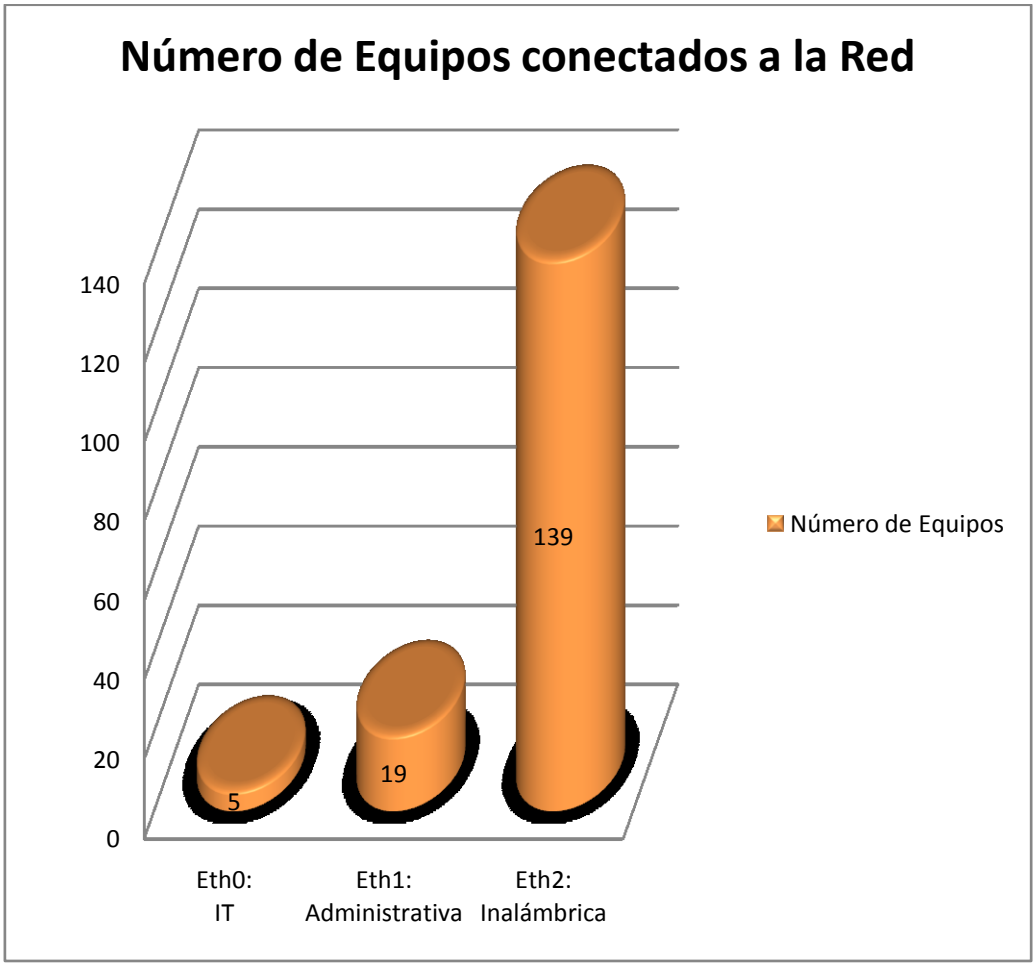

Figura 15: Numero de Equipos conectados a la Red

En la Figura 15, son datos proporcionados por el administrador de las redes, con lo cual en la parte de ETH0, que es el área de IT, nos dice que el número de equipos conectados a la red es de 5, por lo que se genera un tráfico de red que no influye para el uso de recursos de la red como es el internet.

En la parte Administrativa que es la llamada ETH1, podemos notar que se cuenta con un número de 19 equipos que se conectan a la red, por lo que se empieza a ver un mayor número para la utilización de recursos, ya sea

para internet, impresoras, datos. En el mismo podemos mencionar que se encuentra toda la parte Académica.

Como podemos notar en la parte de la ETH2, se encuentra lo que son las redes inalámbricas de cada uno de los laboratorios y el número de equipos que se conectan a la red, por lo que podemos decir que es un número muy elevado de equipos, entre ellos podemos mencionar que son:

- PC de Escritorio
- Portátiles
- Teléfonos Móviles

Podemos decir que en cuanto a lo que se ha observado y a la información proporcionada por las personas encargadas de las redes de Colegio Técnico Sudamericano, hemos podido deducir que el mayor número de tráfico que se genera en toda la red de colegio, proviene de las redes inalámbricas, las misma que se encuentran en cada uno de los laboratorios.

Cabe señalar también que los equipos y personas que se conectan a la red se encuentran mezclados entre sí, es decir que en cada red inalámbrica se conectan profesores, alumnos, teléfonos móviles, personas varias, con lo que esto se debe tomar muy en cuenta para la propuesta.

3.3.7 LAN vs Wi-fi

Existen algunas diferencias entre redes Ethernet LAN y redes Inalámbricas Wi-Fi, pero para la utilización de cada una de estas se debe saber, en que

las vamos a utilizar y si lo que necesitamos se adapta a las necesidades que tenemos.

Si bien es cierto, cada una de estas, son redes de área local, pero con ciertas diferencias que denotaremos en el siguiente cuadro comparativo:

Características	**LAN**	**Wi-Fi**
Estabilidad	SI	Puede Variar
Conectividad	Siempre conectado	Siempre Conectado
Movilidad	Siempre tiene que estar en un solo lugar	Tiene Libertad de movimiento
Desplazamiento	Se accede desde un punto especifico	Se puede acceder desde cualquier parte de la oficina o casa
Flexibilidad	No se puede desplazar de un lugar a otro y hay que desconectarse cuando se quiera hacer eso.	Nos permite estar conectados mientras nos movemos de un lugar a otro.
Escalabilidad	Requiere instalar un nuevo cable y	Conectar otro equipo es sumamente

	esperar hasta que el cable esté listo	sencillo
Robustez	Se puede tropezar con cables, o hasta pequeños terremotos se puede desconectar el cable	Puede aguantar bastante mejor estos percances inesperados
Diseño		Los receptores son pequeños y pueden integrarse dentro de un dispositivo que se puede llevar en bolsillo
Poca Planificación	Se debe pensar mucho en la distribución física	Solo se preocupa de que los equipos estén dentro de la cobertura de la red.
Seguridad	Existe más seguridad	Se implementan varias seguridad para la redes
Costos	Mucho más costoso	Menor costo

Figura 16: Tabla comparativa entre LAN y Wi-Fi

Como podemos ver en nuestro cuadro comparativo notamos que las redes inalámbricas tienen muchos beneficios que nos ayudan para optar por instalar una red inalámbrica en nuestra oficina u hogar

Entre cada una de estas características que son muy importantes para poder adoptar uno de estos dispositivos, es el caso de la movilidad ya que las redes Wi-Fi pueden, los equipos que se conectan a ellas tiene la facilidad de movimiento y que en las redes Ethernet no te permiten realizar esto.

Un factor también hay que mencionarlo es el desplazamiento que podemos realizar, ya que esta se puede conectar desde cualquier parte de la oficina o la casa, sabiendo que en la redes cableadas no puede hacer esto ya que necesita tender cable para poder llegar al lugar indicado.

En el caso de la flexibilidad, siempre nos permitirá estar conectado a nuestra red, así nos movamos de un lado a otro en cualquier parte de la casa u oficina.

La escalabilidad es otro aspecto muy importante en las redes inalámbricas, ya que este se puede conectar otro equipo muy fácilmente, en cambio en las redes Ethernet, requieres instalar un nuevo cable y esperar hasta que realices la implementación de ese cable y así poder conectarte.

La robustez que pueden llegar a tener estos dispositivos es muy bueno ya que te permiten aguantar percances tales como tropezar con el cable o

hasta cuando se ocasiona un pequeño terremoto y se pueden desconectar los cables.

En el diseño de cada uno de estos dispositivos para la conexión son tan pequeños que pueden integrarse fácilmente dentro de un dispositivo que se puede llevar en el bolsillo.

La planificación que se da para las redes wi-fi, es muy poca, por lo que la única preocupación que debe tomar es la de estar dentro del área de cobertura, en cambio en red LAN se debe pensar mucho para poder implementar una red física.

La seguridad que se da en torno a estas redes, se torna importante, ya que el hecho de estar protegido contra cualquier ataque, el usuario se beneficia para estar seguro en sus redes inalámbricas y que ningún usuario no autorizado ingrese a nuestra red.

Una característica muy fundamental que a todas las personas les interesa es el costo de instalación, ya que este es muy importante para poder tomar una decisión en lo que se quiere hacer, y es que las redes Wi-Fi son mucho más baratas poder implementarla, como no es el caso de las redes Ethernet, ya que se necesita mucho más dinero para implementarlo.

Entonces podemos decir que las redes inalámbricas tienen muchos puntos positivos para poder ser implementadas, ya que con esto se ahorra tiempo, esfuerzo y sobre todo dinero.

3.3.8 Dispositivos Inalámbrico

En cada uno de los laboratorios vienen equipados a más de los PC's, tiene sus Access Point conectados a las red Ethernet de la Institución, para dar conexión inalámbrica a cada uno de esto equipos.

Los dispositivos inalámbricos instalados en cada uno de los laboratorios de la institución son los conocidos Airport Extreme, estos cumplen una muy buena cobertura y velocidad.

Los Airport Extreme trabaja en doble banda simultánea, es decir que se puede tener dos redes inalámbrica al mismo tiempo saliendo de un solo dispositivo inalámbrico, este emplea una banda inalámbrica de 2.4 GHz. Este dispositivo inalámbrico cumple con el estándar 802.11n y este utiliza tecnología MIMO (Multiple input Multiple output). Estos dispositivos son compatibles con diferentes estándares podemos mencionar los 802.11a, 802.11b y 802.11g que son los más utilizados hoy en día por otros dispositivos inalámbricos, los mismo que pueden enlazar a cualquier PC, portátil, teléfonos inteligente que sean compatible con cualquier estándar antes mencionado.

3.3.9 Análisis de las Redes Inalámbricas.

Como hemos detallado anteriormente, pudimos notar que las redes inalámbricas son las más utilizadas por los usuarios en la institución, los usuarios que se conectan a la red están entre los profesores, estudiantes que por lo general utilizan el servicio de Internet.

En cada uno de los laboratorios se tiene instalado un Access Point para la navegación en Internet, por lo que no solo equipos de los laboratorios, estudiante, profesores se enlazan a las redes inalámbricas, sino también usuarios que tienen teléfonos como se les conoce hoy en día los teléfonos inteligentes.

3.3.9.1 Topología utilizada por la Institución.

En el siguiente cuadro que mostraremos a continuación podremos ver cómo están estructuradas las topologías lógicas y en los cuales lograremos sacar una conclusión de cuál es la que utilizan en las redes inalámbricas del Colegio Técnico Sudamericano.

Características	**Ad-hoc**	**Infraestructura**	**Mesh**
Infraestructura e integración	Depende de sus dispositivos	Tiene un punto de acceso	Contiene toda una red de router's
Routing y configuración	Realiza cada dispositivo	Se lo realiza en el punto de acceso	Realiza en mayor parte de la red de router
Cobertura y movilidad	Pequeña	Cubre por lo menos 100 metros a la redonda	Mucho más grande
Redes:	Puede conectar una	Puede conectar redes LAN	Puede conectar redes Wimax

	red pequeña		

Figura 17: Tabla comparativa de Topologías

Como podemos ver en el cuadro comparativo entre cada uno de las topologías Ad-hoc, Infraestructura, Mesh, podemos notar que entre cada una de las características que tienen, la que más se adapta a las circunstancias que se encuentran las redes inalámbricas de la institución, es la topología infraestructura, ya que esta cuenta con un punto de acceso para dar una conexión de internet a diferentes equipos, sabiendo que este se conecta a un punto Ethernet para la conexión a la red. Como también podemos mencionar que la topología infraestructura alcanza hasta unos 100 metros a la redonda, por lo que cada una de las características mencionadas en el cuadro 5, se adapta para las redes inalámbricas de la institución.

3.3.9.2 Estándar utilizado en WLAN

Como sabemos existen diferentes estándares en la actualidad, en los cuales podemos discutir cual es el estándar que utiliza la institución, mediante una cuadro comparativo el mismo que podremos observar las características que nos permita determinar cuál es el estándar que utiliza la institución, para así poder sacar una conclusión que nos ayudara a guiarnos y encaminarnos mucho mejor.

Características	Estándar 802.11a	Estándar 802.11b	Estándar 802.11g	Estándar 802.11n	HiperLan2
Acceso	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS) usando Complementary Code Keying (CCK)	Complementary Code Keying (CCK) y Orthogonal Frequency Division Multiplexing (OFDM), CCK	Complementary Code Keying (CCK) y Orthogonal Frequency Division Multiplexing (OFDM), CCK	Orthogonal Frequency Division Multiplexing (OFDM)
Compatibilidad	No compatible con sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF	Compatible con sistemas 802.11 DSSS. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF	Compatible con sistemas 802.11b, 802.11 DSSS No compatible con sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF	Compatible con sistemas 802.11b 802.11g y 802.11a	No compatible con los sistemas 802.11g, 802.11b, 802.11, ni con HomeRF
Aplicación	Todo tipo de red de datos Ethernet	Todo tipo de red de datos Ethernet	Todo tipo de red de datos Ethernet	Todo tipo de red de datos Ethernet	WAN/LAN, voz encapsulada, vídeo, dato

Figura 18: Tabla comparativa entre estándares 802.11

Para la institución las configuraciones que se realizan no están dadas en base a ningún análisis que determine que estándar es el más factible y el que se debería utilizar para cada una de los laboratorios.

El estándar 802.11g, es el que están utilizando por el momento los administradores de red, ya que cumplían con la compatibilidad del estándar 802.11b, y les permitía tener una mejor compatibilidad con diferentes dispositivos inalámbricos que se conectaban al Acceso Point.

Como podemos ver en nuestro cuadro comparativo de estándares aprobados por el IEEE, ya que sabemos de estándares que no fueron aprobados como es el caso de 802.11b+, podemos notar que el estándar mejor diseñado en este momento es el 802.11n, ya que es el que mejora significativamente el rendimiento de la red, más allá de los estándares 802.11b y 802.11g.

La ventaja de 802.11n y uno de los más importantes es el componente MIMO (Multiple Entrada Múltiple Salida). Esta es una tecnología que permite mediante el empleo de varias antenas ofrecer varias rutas de señales mediante varias antenas.

3.3.9.3 Velocidad y Frecuencia

La velocidad y la frecuencia son unos de los aspectos también muy importantes cuando se hablan de estándares 802.11, ya que cada uno de los estándares trabaja bajo cierta velocidad y frecuencia.

Características	Estándar 802.11a	Estándar 802.11b	Estándar 802.11g	Estándar 802.11n	HiperLan2
Rango de Frecuencia	De 5,15 a 5,25 GHz	De 2.4 a 2.4835 GHz	De 2.4 a 2.4835	De 2.4 GHz De 5.4 GHz	De 5,15 a 5,25 GHz

	De 5,25 a 5,35 GHz De 5,725 a 5,825 GHz		GHz		De 5,25 a 5,35 GHz De 5,725 a 5,825 GHz
Velocidad	Hasta 54 Mbps	Hasta 11 Mbps	Hasta 54 Mbps	Hasta los 600 Mbps	Hasta 54 Mbps

Figura 19: Tabla comparativa entre Velocidades y Frecuencias

Como podemos notar en nuestro cuadro comparativo por cada estándar viene definido su rango de frecuencia y su velocidad, lo cual al momento de utilizar cualquier estándar es importante definir porque vamos a utilizar estos rangos y velocidades.

Hablando con relación al rango de frecuencia, como sabemos cada uno de los estándares viene definido, desde un cierto inicio hasta un cierto límite, lo que nos limita a definir un estándar a escoger.

Con relación a la Velocidad, los estándar viene dado por su propia característica de velocidad, con lo que dependiendo de lo que se necesite realizar y la velocidad que necesitamos en nuestras redes inalámbricas tomaremos una decisión acertada para utilizar cualquier estándar.

Para tener una mejor conclusión de estos estándares de frecuencia y velocidad, vemos que el estándar 802.11n, es el estándar que mejor trabaja y que mejor compatibilidad tiene con otros estándares, ya que

este puede funcionar en rango de frecuencia de 2.4Ghz y 5.4Ghz, con lo cual hablaría que este estándar es compatible con los estándares 802.11a que ocupa hasta el 5.4Ghz, el estándares 802.11b y estándares 802.11g, que ocupa hasta el 2.4Ghz de rango de frecuencia.

Ahora para definir la velocidad que uno quiera es lo que uno vaya a realizar y las necesidades que tengamos, por lo que la mejor velocidad que tenga va a ser la que elija, como es el caso del estándar 802.11n, que este es el que llega a tener una mejor velocidad. Tenemos que saber que esta velocidad alcanza los 600Mbps teóricamente, pero todavía no está llegando a su verdadera velocidad, ya que por el momento se llega hasta los 300 Mbps.

Con lo cual, cada una de estas característica nos pueden ayudar a tener una conclusión más clara entre cual estándar utilizar y que cual nos va a dar un mejor trabajo para lo que uno necesita.

3.3.9.4 Canales

Cada uno de los estándares viene dados por los canales que utilizan, pero es muy importante saber y conocer cuando se adquiere un equipo en que canal puede trabajar estos.

Características	Estándar 802.11a	Estándar 802.11b	Estándar 802.11g	Estándar 802.11n
Canal	20 MHz	20 MHz	20 MHz	20 MHz

				40 MHz

Figura 20: Tabla comparativa entre canales

Como resultado de estos canales tenemos que todos los canales en los estándares 802.11a, 802.11b y 802.11g trabaja sobre un canal de 20Mhz y el único que trabaja bajo diferentes canales es el estándares 802.11n, ya que este implementa tecnología MIMO, porque se puede realizar esto, porque trabaja bajo varias antenas, y como se puede trabajar con varias frecuencias, con lo que permite que el canal para este estándar se vea una buena opción.

Hay que tomar muy en cuenta que el estándar 802.11n, es compatible con los demás estándares, con lo cual al momento de ver los canales en los cuales trabajan, este estándar se adapta con otros estándares.

Cabe notar como hablamos anteriormente sobre cuando se adquiere un equipo es importante saber e informarse muy bien sobre los equipos que se quiere adquirir, las prestaciones que este va a tener, con lo que tenemos que revisar todas las especificaciones del fabricante y tomar una clara conclusión de lo que se desea.

3.3.9.5 Perdidas de Señal

Es muy importante saber cómo esta nuestra señal de transmisión, ya que esta utilizamos a cada momento y necesitamos estar conectados a la red. Existe diferentes motivos por lo que se da la perdida de la señal, entonces se da uno de los casos, el cual es por el canal elegido en el

dispositivo inalámbrico para emitir y recibir la señal inalámbrica, ya que este si no se configura un canal apropiado vamos seguramente a tener una pérdida de señal.

Otro de los factores de las perdida de la señal que influye en la calidad y fuerza de la señal son las interferencias que son causadas ya sea por diferentes equipos, distancia del punto de acceso, hardware, pero los más importantes son obstáculos o ruidos que se dan, con lo cual cuando se transmite energía y esta es absorbida y reducida.

En las edificaciones que se construyen, y la ubicación de los puntos de acceso son otras de las maneras en las cuales se tiende a una pérdida de señal, ya que al momento de tener edificaciones que tengan muchas paredes tiende a que la señal disminuya, y así mismo la ubicación de los puntos de acceso que estén ubicados donde haya muchas interferencia de electricidad, se va a ver reflejada una baja notable en la señal de la red.

3.3.9.6 Protocolos en Redes Inalámbricas

Como sabemos muy bien la seguridad de red es extremadamente importante, en especial cuando tenemos información valiosa que no queremos que nos roben personas mal intencionadas. Es muy importante considerar en el estudio de los dispositivos inalámbricos la encriptación que nos proporciona cada uno de los protocolos, con lo

cual si no tomamos las debidas precauciones nos podremos ver envuelto en muchos problemas.

Características	**WEP**	**WPA**	**WPA2**
Cifrado	Utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Utiliza claves de 64, 128 e incluso 152 bits. Utiliza clave simétrica y estática en las estaciones y puntos de acceso	Creado para corregir deficiencias de WEP. clave previamente compartida: PSK (Pre-Shared Key) - TKIP (Temporal Key IntegrityProtocol) para la gestión de claves dinámicas	Versión mejorada. Basa en el sistema de cifrado TKIP. WPA-2 garantiza el cifrado así como la integridad de los datos incorpora seguridad como “Key Caching” y la “Pre-Autenticación” y AES (AdvancedEncryption Standard)
Algoritmo de encriptación	RC4 de RSA Data Security.	RC4	-AES (AdvancedEncryption Standard)

Sistema de autenticación	Controla el acceso mediante clave compartida y evita accesos no autorizados a la red.	Necesita un servidor central que cataloga a los usuarios, Eje: servidor RADIUS.	WPA2 versión con Autenticación 802.1x/EAP

Figura 21: Tabla comparativa entre Protocolos de Encriptación

Es sumamente importante la seguridad de red ya que esta es un pilar indispensable para no tener problemas de instrucciones en nuestras redes.

Como podemos observar en nuestro cuadro comparativo notamos cada una de sus características de encriptación que existe hoy en día, empezaremos diciendo que WEP no ofrece una seguridad alta de cifrado para los datos, ya que en esta se notaron vulnerabilidades que eran fácilmente explotadas. WEP no cumple con las características para poder optar por una encriptación sumamente confiable, por sus debilidades que presenta.

WPA ofrece una mayor seguridad que WEP, ya que este fue creado para mejorar las deficiencias que este presenta. La autenticación y el cifrado mejora la seguridad de la información cifrada, este es un sistema que va asignando claves dinámicas diferentes a cada equipo a medida que WPA es utilizado. Este también ofrece una protección

contra ataques de repetición, ya que incluye un contador de tramas. También cabe destacar que tiene un código de integridad llamado MIC (MessageIntegrityCode), que permite verificar la integridad del paquete, tiene 8 octetos.

WPA también tiene sus vulnerabilidades y esta se da en TKIP ya que si realizan un ataque de recuperación Keystream, es decir que vuelve a inyectar tráfico en una red, se crea una brecha de vulnerabilidad para los usuarios no autorizados.

En el caso de WPA2, es el método más seguro, ya que maneja un sistema de cifrado AES en lugar de RC4, ya que este es mucho más seguro en cuanto al cifrado de datos, así mismo permite al usuario conservar una clave primaria el PMK que es una variante de PSK (Previamente compartida), que es cambio de fase de codificación, el mismo que es un esquema de modulación digital que transmite datos mediante el cambio o la modulación de la fase de una señal de referencia, esto le permite que el usuario se identifique una sola vez al momento de acceder a la red.

WPA2 también ofrece mayor eficiencia en cuanto a seguridad y movilidad, gracias a la autentificación del cliente desde cualquier lugar que se desee conectar. Nos da flexibilidad ya que realiza una re-autenticación rápida y segura, y se torna mucho más segura gracias a un mecanismo de distribución dinámica de claves.

La comparación que se hace en torno a los tres protocolos de encriptación, hace denotar que el WPA2, es el método de encriptación mucho más seguro, confiable, eficiente, y con una muy buena flexibilidad, que se adapta para mantener mucho más seguro las encriptaciones de las claves para nuestras redes inalámbricas, sabiendo también que no todos los sistemas son 100% seguros, ya que en algún momento podrán explotar alguna vulnerabilidad que tenga este método de encriptación.

En la información proporcionada por la persona encargada de administrar las redes inalámbricas se pudo recoger que la encriptación que se la realiza para los dispositivos inalámbricos esta dado con una WAP, con la cual esta se ha venido dando solución a las debilidades de WEP, esta es una encriptación mucho más segura.

Las seguridades que se den a las contraseñas que están asignadas para las redes inalámbricas están dadas por la combinación de número y letras y en cada una de las redes inalámbricas las contraseñas son similares con cambios poco seguros.

3.3.9.7 Vulnerabilidades de la Red

Las vulnerabilidades que se pueden dar en las redes inalámbricas del Colegio Técnico Sudamericano son las siguientes:

- Las contraseñas definidas no son correctas, ya que existen indicios para saber fácilmente cuál podría ser la contraseña, ya

que esta cuenta con iniciales del mismo dispositivo y también nombre del colegio.

- Las contraseñas no son solo configurada por el administrador de red, sino que también por los estudiantes, ya que las contraseñas nunca has sido cambiadas y ya conocen cada uno de los usuarios las contraseñas.
- Todos los usuarios de las redes inalámbricas, ya sean estudiantes, profesores, teléfonos, personas particulares se conectan a una misma red.

3.3.10 Ventajas y desventajas de una red inalámbrica

3.3.10.1 Ventajas

Las principales ventajas que se da en una red inalámbrica son:

- Movilidad
- Desplazamiento
- Flexibilidad
- Escalabilidad
- Ahorro de costos

La libertad que se tiene al momento de tener movilidad es unos de los beneficios más evidentes dentro de las redes inalámbricas. Cualquier dispositivo puede situarse en cualquier punto dentro del área de cobertura de la red, sin necesidad exclusiva de depender de que si es o no posible hacer llegar el cable hasta el sitio específico.

Ya no es indispensable estar conectado a un cable para navegar en internet o el simple hecho de imprimir documentos o acceder a los recursos de la red.

El desplazamiento ya que al tener un equipo portátil no solo podemos acceder a internet sino que también a cualquier recurso de la red desde cualquier parte de la oficina o casa, sin perder la conexión ni la comunicación al desplazarse de un lugar a otro. Esto da cierta comodidad, pero también facilita en mucho el trabajo en determinadas tareas.

En el caso de la flexibilidad, no solo nos permite estar conectados mientras nos desplazamos de un lugar a otro con una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que realizar ninguna configuración o cambio mínimo en la configuración de red. En ocasiones extender una red cableada no es una tarea fácil ni mucho menos barata. En muchas ocasiones acabamos con instalar peligros cables que están regados por el suelo para evitarnos realizar e instalar enchufes de red. Las redes inalámbricas nos evitan muchos de estos problemas.

La escalabilidad o la facilidad de expandir la red después de una instalación inicial es una de las ventajas muy buenas en las redes inalámbricas. Conectar un nuevo equipo cuando disponemos de una red inalámbrica es algo tan sencillo como instalar una tarjeta y listo. Con

las redes cableadas esto se ve muy afectado, ya que requiere instalar un nuevo cableado o lo que es peor esperar hasta que el nuevo cableado quede instalado.

El ahorro de costos debido a que diseñar e instalar una red cableada puede llegar a adquirir un alto costo, no solamente en la parte económica sino en la parte de tiempo y molestas que surjan al momento de realizar este trabajo. En determinados entornos donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica hace que permita ahorra cotos al permitir compartir recursos como acceso a internet, impresoras, etc.

Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.

La Wi-Fi asegura que la compatibilidad entre dispositivos con la marca *Wi-Fi* es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total.

3.3.10.2 Desventajas

Entre las desventajas de tener una red inalámbrica podemos mencionar que existe:

- Menor velocidad.
- Seguridad

- Interferencia
- Tecnología en proceso

Entorno a la velocidad, las redes actuales de cable trabajan a 100 Mbps mientras que las redes Wi-Fi lo haces a 11 Mbps, es cierto que existen estándares que llegan a los 54Mbps y soluciones propietarias que llegan a los 100 Mbps, pero estos estándares están es su comienzo de su comercialización, por ende tiene un precio superior al de los dispositivos actuales Wi-Fi.

La seguridad debido a que estos dispositivos tienen la particularidad de no necesitar un medio físico para funcionar. Esto se puede decir que fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona o computador portátil solo necesita estar cerca de la cobertura de la red para poder intentar acceder a ella. A los intrusos no les hace falta estar conectados mediante una red cableada o a un edificio o casa para poder realizar sus ataques. Es muy importante saber que el sistema que incorpora las redes inalámbricas Wi-Fi no es tan bueno y no son tan fiables. A pesar de que las redes Wi-Fi no proporcionan tanta fiabilidad estas tienen incorporadas seguridades que les haces más confiables para poder utilizarlas.

Entre las interferencias que se puede dar dentro de las redes inalámbricas tenemos que si en una red se cuenta con diferentes redes Wi-Fi puede ocasionar un mal funcionamiento por tener un radio

electrónico que puede ocasionar interferencias ya que todas trabajarían bajo una misma frecuencia y no se podrías garantizar que la red inalámbrica funcionen en su totalidad. Cada vez que empiecen a existir muchas más interferencias que se producirían por otros equipos, el rendimiento de nuestra red se verá afectada.

En la parte tecnológica cada día se va creando nuevas y mejores velocidades de transmisión y mayores niveles de seguridad, con esto las redes Wi-Fi empezaran a bajar su popularidad, ya que existieran nuevas y mejoradas tecnologías.

3.3.10.3 Riesgos de las redes Inalámbricas

La utilización de redes inalámbricas sin la debida seguridad, puede ocasionar que personas no autorizadas o hacker, que poseen equipos sofisticados se introduzcan fácilmente a una red inalámbrica. Una vez dentro, una persona no autorizada puede tener acceso a contraseñas, introducirse a servidores y robar todo tipo de información, cambiar modificar o hacer que simplemente deje de funcionar toda la red o cualquier sistema que se tenga.

Es muy elevado el porcentaje de redes inalámbricas que se instalan sin tener en consideración la seguridad, convirtiendo las mismas en redes abiertas o vulnerables, sin proteger la información que circulan por ellas.

Los riesgos que se pueden dar en torno a las redes que no tiene seguridad es la de no tener un cifrado seguro, una autenticación no definida, por lo que se puede dar:

- Exposición de datos a intrusos.
- Ataque de inserción: usuarios no autorizados
- Ubicación de un punto de acceso ilegal.
- Creación de interferencias y posibles denegaciones de servicio.
- Ataque directo a una estación cliente
- Duplicación de direcciones Mac o IP.

3.3.10.4 Problema de las redes Inalámbricas

Uno de los problemas fundamentales que tienen las redes inalámbricas se basa en la seguridad que deben tener estas, debido a que desde cualquier laptop se podría ingresar a la red, si no se toman las medidas necesarias y existe alguna brecha de seguridad en la red es un grave problema para cualquier institución.

La seguridad debe ser prioridad para cualquier persona que administre o utilice las redes, así mismo la dificultad que se tiene para mantener segura una red cableada se multiplica en una red inalámbrica.

Una WLAN está abierta a cualquiera dentro del alcance de un punto de acceso y de las credenciales apropiadas para asociarse a él.

Con un NIC inalámbrico (Tarjeta de interfaz de red) y los conocimientos necesarios de técnicas de decodificación, un atacante no tendrá que

entrar físicamente al espacio de trabajo para obtener acceso a una WLAN.

Existen 3 categorías que son muy importantes en cuanto a las amenazas que conllevan el acceso no autorizado, los cuales podemos describir:

- Empleados: Pueden enchufar un Gateway de calidad comercial a los puntos de acceso Ethernet de las instituciones para crear sus propias redes inalámbricas.
- Piratas Informáticos: Explotan medida de privacidad débiles para ver información de WLAN sensible e incluso ingresar sin autorización a las WLAN.
- Buscadores de redes inalámbricas abiertas: buscan redes abiertas para conseguir y utilizar acceso a internet gratis.

4 Guía de Seguridades para Dispositivos Inalámbricos

4.1 Generalidades

La utilización de redes inalámbricas hoy en día se ha vistos como una alternativa factible a redes de área local cableadas, ya que se elimina la restricción que existe con la unión de equipos por medio de un cable físico.

La tecnología inalámbrica abarca diferentes dispositivos o equipos, ya sea desde un teléfono celular hasta las redes de área local WLAN. Las redes WLAN son cada vez más frecuentes en hogares como en empresas y con su incorporación aparecen nuevas maneras de ataque y cada vez más se debe considerar y tomar nuevas medidas de seguridad, ya que en la actualidad nos vemos perjudicados por intrusiones de personas no autorizadas a nuestros sistemas por lo que es importante saber cómo protegerse de todos estos problemas para así ver que nuestros sistemas no se vean comprometidos y no tener ningún inconveniente en los mismo.

En nuestro capitulo hablaremos de la propuesta que se realiza al Colegio Técnico Sudamericano para que sus dispositivos inalámbricos brinde la seguridad necesaria y no tengan inconvenientes al momento de utilizar las redes inalámbricas.

4.2 Diseño y Construcción de Propuesta

4.2.1 Distribución de las Redes Inalámbricas

Como pudimos notar en nuestro estudio de levantamiento de información, el número más alto de acceso que se da en el Colegio Técnico Sudamericano es en la parte de la red inalámbrica (Véase Figura 13).

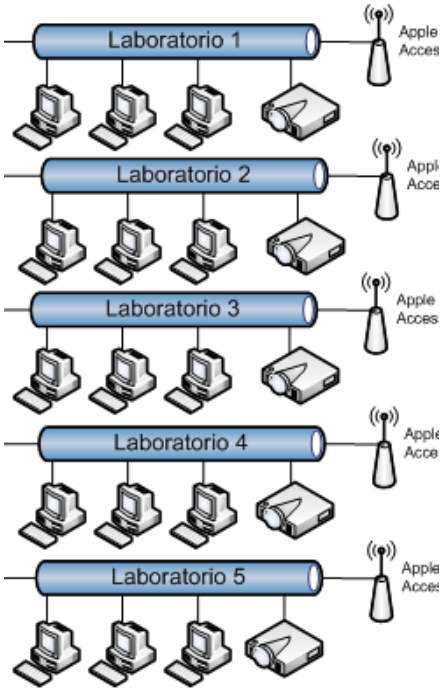

Figura 22: Redes de Laboratorios Colegio Sudamericano

Como podemos observar en la figura 22, Aquí tenemos que todos los equipos de los laboratorios, estudiantes, profesores, teléfonos inalámbricos se conectan a cada una de las redes inalámbricas de cada laboratorio, por lo que esto no debería pasar ya que se tiene que dividir las redes y dejar segmentadas todas estas.

Lo que se recomienda que las redes de los laboratorios deban estar independientemente de las redes de los profesores, estudiantes y otros dispositivos. Por lo que se recomienda lo siguiente:

- Los dispositivos inalámbricos para los laboratorios, deben estar solo configurados para estos, ya que aquí se gana una segmentación de redes y se daría una seguridad para no tener a todos los usuarios conectados a una misma red.
- Se deberá crear otras redes inalámbricas distintas para Profesores, Estudiantes.
- Se deberá adquirir otro dispositivo inalámbrico para las nuevas redes de Profesores y Estudiantes.

4.2.2 Amenazas, Vulnerabilidades y Riesgos

Estas también son una de los factores importantes que tenemos que tomar en cuenta. Cabe destacar que el Colegio Técnico Sudamericano no cuenta con un plan de contingencia que le permita actuar en estos problemas, con lo que se recomienda que se cree un plan de contingencia para salvaguardar los dispositivos inalámbricos, en base a las amenazas, vulnerabilidades y riesgos que pueden tener los mismos.

4.2.2.1 Amenazas

En las amenazas que se podrían dar las podemos dividir en 3 grupos:

- Naturales, estas se pueden dar en caso de que existe desastres naturales, terremotos, humedad, polvo. Para estos se

recomienda que los dispositivos inalámbricos deben tener protección contra el polvo, humedad, sol, ya que al momento de observar la ubicación del dispositivo inalámbrico, se puedo notar que este no tiene la debida limpieza, ni la protección correcta para mantener en perfectas condiciones al mismo.

- Las amenazas involuntarias que se pueden dar, son por descuido de un dispositivo, esto se puede dar por que la persona sin autorización quieren entrar a nuestras redes, por lo que se recomiendo, que las configuraciones que se las realice se las hagan conscientemente y con conocimiento de lo que se está haciendo, ya que podría ingresar a la red, modificar y borrar la información.
- Otro de los aspectos importantes que se deben tomar en cuenta es el hecho de las amenazas humanas, ya que existen personas que quieran infiltrase en nuestra red.

4.2.2.2 Vulnerabilidades

Esta de aquí se pueden dar cuando un dispositivo no está bien configurado, y tiende a que personas no autorizadas exploten las vulnerabilidades que tiene el dispositivo inalámbrico, por lo que se recomienda que cada uno de los dispositivos inalámbricos sea correctamente configurado, para no tener inconvenientes contra ataques de personas no autorizadas, se puede utilizar programas que nos permitan encontrar vulnerabilidades como por ejemplo podemos

encontrar en la Web diferentes software que nos ayuden con esto, podría ser Nesuss, Ethereal, que va analizando las vulnerabilidades que podemos tener, estos se pueden instalar en Linux y lo bueno es que estos son gratuitos. Estas vulnerabilidades se pueden dar por una intercepción de señal cuando se transmiten datos de un lugar a otro.

4.2.2.3 Riesgos

Los riesgos se dan por el grado de exposición que tienen a cualquier amenaza por lo que se recomienda lo siguiente.

- Cuando se instale un nuevo dispositivo inalámbrico no se debe dejar con los valores por defecto, ya que la primera manera de ver alguna vulnerabilidad es en base a los valores predeterminados que existen en un dispositivo inalámbrico

4.2.3 Topología a utilizar.

Si bien es cierto existen diferentes topologías que se puede utilizar y adaptar dependiendo de nuestros requerimientos como es el caso de las topologías lógicas Ad-hoc, Infraestructura, Mesh, cada una de estas cumple diferente puntos importantes, pero como hemos estudiado en los capítulos anteriores (Ver Pag.24), existe una topología en la cual se adapta a las necesidades de que tenemos para las redes inalámbricas.

La topología que se debe utilizar para el Colegio Técnico Sudamericano es la topología llamada Infraestructura. Ya que está en base a una de sus

características que es la integración e infraestructura sabemos que se tiene que conectar a un punto de acceso.

Es muy importante saber también que en la topología infraestructura para realizar el routing y configuración se tiene que realizarlo en el mismo punto de acceso.

La misma también nos proporciona una cobertura de 100 metros a la redonda dependiendo del dispositivo inalámbrico que adquiramos, estos dispositivos inalámbricos sabemos también que se conecta desde una red Ethernet para dar recursos y servicio de internet, impresora, etc.

4.2.4 Instalación, Configuración y uso del Dispositivo Inalámbrico

4.2.4.1 Instalación.

Para poder realizar una muy buena instalación de un Airport Extreme, se la puede realizar la instalación en cualquier sistema operativo MacOS 10.4 o superior, en Windows se lo puede hacer desde cualquier Windows XP o Superior.

La instalación en MacOS es muy sencilla por lo que solo se necesita seguir los pasos correctamente para una buena instalación.

En Windows se tiene que ver que el equipo este sin virus, ya que el software podría comportarse extraño al momento de instalarlo y ejecutarlo, igualmente que en MacOS solo necesita seguir leyendo cuidadosamente para poder tener una muy buena instalación.

Al momento de la instalación, se debe considerar que exista el espacio suficiente para poder instalar el software, a su vez elegir la unidad correcta para instalarlo.

4.2.4.2 Estándar a Utilizar

Como hemos estudiando los diferentes estándares que existen en la actualidad (Véase Pág. 14), y además de estos el estándar que utilizan los dispositivos inalámbricos en la institución, podemos recomendar lo siguiente:

Los dispositivos inalámbricos deben estar muy bien configurados y tener un estándar 802.11n, ya que este es el estándar más actual de hoy en día, la elección de este estándar se da por lo siguiente.

- Utiliza un acceso CCK que es un esquema de modulación, con el cual se puede lograr mayor velocidad y OFDM que tiene una multiplexación que nos sirve para llevar un conjunto de ondas portadoras de diferentes frecuencias.
- Son compatibles con los diferentes estándares 802.11b, 802.11g y 802.11a.
- Se puede conectar a todo tipo de red de datos Ethernet
- También podemos mencionar que el estándar 802.11n, utiliza tecnología MIMO que es entrada múltiple y salida múltiple, para transmitir múltiples cadenas de datos simultáneamente

Ya que cuenta con todas estas características hace que el estándar 802.11n sea el mejor estándar que existe en la actualidad.

4.2.4.3 Velocidad y Frecuencia.

Debido a que el estándar recomendado es el 802.11n, también por ende, su velocidad y frecuencia son uno de los aspectos muy importantes en la propuesta.

Como sabemos el estándar 802.11n nos proporciona una frecuencia de 2.4Ghz y 5.4Ghz, es decir que trabaja con doble banda y que es compatible y puede correr con estándares 802.11b, 802.11g y 802.11a. Podemos concluir que si trabajamos con esto se obtendrá una mejor compatibilidad con varios equipos que están en estos estándares y además de esto que la velocidad que llegaría es de 600 Mbps, pero esto por el momento es solo teórico, lo que hoy en día se alcanzar es a los 300Mbps, que es muy superior a los estándares antes mencionados.

4.2.4.4 Canales

El canal es otro aspecto importante que hay que tomar en cuenta, los canales en los que trabajan vienen definidos por cada uno de los estándares, por lo que al tener un estándar 802.11n, trabajaría sobre dos diferentes canales los cuales son de 20Mhz y 40Mhz, con lo cual podemos decir que este al momento de utilizar un canal mucho más

amplio, podremos llegar a tener una mejor señal, ya que si se incrementa el canal se logrará mucha más cobertura.

4.2.4.5 Perdida de Señal

La pérdida de señal que se da en el Colegio Técnico Sudamericano se da por circunstancias, de su infraestructura, las cuales están compuestas de hormigón y ladrillo, ya que estas provocan un alto índice de interferencia de señal.

4.2.4.6 Protocolo de Red

Los protocolos de red es uno de los aspectos muy importantes en la configuración del dispositivo inalámbrico, por lo que en esto se recomienda lo siguiente:

- Se debe utilizar un método de encriptación WPA2, ya que este cuenta con sistema mejorado de cifrado TKIP que es un mecanismo utilizado para crear encriptación de clave dinámica y autenticación mutua, ofrecen un nivel de protección bien alto, ya que las claves cambian permanentemente. EAP, ya que este utiliza un mecanismo de autenticación extensible para intercambiar mensajes durante el proceso de autenticación.
- Utiliza un algoritmo de encriptación AES que es un esquema de cifrado por bloques y el más seguro de hoy en día.

El protocolo WPA2, es el más seguro hasta la actualidad, ya que sabemos que todo sistema no es 100% seguro.

4.2.4.7 Seguridad en la Contraseña.

Al momento de definir una contraseña, es indispensable saber que contraseña vamos a poner y la seguridad que se le debe dar a esta, por esta razón las contraseñas debe ser:

- Las contraseñas que se crean deben tener por lo mínimo 8 caracteres.
- Estas no deben tener una palabra concreta.
- Debe ser diferente a contraseñas creadas anteriormente.
- Combinación de letras en mayúsculas y minúsculas
- Utilización de números
- Utilización de símbolos

También así mismo debemos tomar muy en cuenta, que las contraseñas no deben ser definidas en base a un nombre de la persona, fecha de nacimiento, nombre de la institución, ya que al momento de realizar esto, las personas no autorizadas empezaran por buscar desde estos parámetros, ya que se les haría mucho más fácil deducir la contraseña puesta por el administrador de la red.

Tenemos que tomar en cuenta que el administrador de la red debe ser el único que configure los equipos clientes, ya que al no proporcionar la contraseña para otras personas en un papel se logra tener más seguridad para las infiltraciones de personas no autorizadas.

4.2.4.8 Ocultación y Modificación del SSID

El SSID se conoce comúnmente que es el nombre de la red inalámbrica, cuando un usuario quiere ingresar a la red necesita conocer el SSID de la red, la ocultación de la red es un buen método para evitar intrusiones a la red, ya que al ocultar el SSID las personas no autorizadas tiene muchas más dificultades para poder ingresar a la red.

Es importante también mencionar que al momento de adquirir un dispositivo inalámbrico, los fabricantes dejan su mismo nombre de SSID, por lo que si no se modificación de esto los intrusos pueden adivinar fácilmente el nombre y conectarse a ella, y cambiar datos inmediatamente, con lo que es recomendable no dejar los valores por defecto en los dispositivos inalámbricos.

4.2.4.9 Filtrado por Direcciones MAC's

Una de las opciones de seguridad para poder protegerse de personas no autorizadas es activar el filtrado por direcciones MAC donde podremos indicar solo las direcciones MAC que vamos a permitir conectarse a nuestra red inalámbrica.

4.2.4.10 Actualización del Dispositivo Inalámbrico

Cabe anotar que un dispositivo inalámbrico que viene de fábrica siempre tiene actualizaciones para los dispositivos, por lo que las empresas publican actualizaciones de firmware, de manera que estos

dispositivos deben ser actualizados regularmente, con lo cual se genera un incremento en el desempeño y permite el acceso a nuevos recursos.

5 Conclusiones y Recomendaciones

5.1 Conclusiones

Con esta tecnología de redes inalámbricas hoy en día se abre un nuevo camino lleno de posibilidades de conexión sin la utilización de cables, proporcionando una gran flexibilidad, movilidad, desplazamiento, escalabilidad, robustez y comodidad, sin precedentes en la conectividad entre computadoras o cualquier dispositivo.

Uno de los puntos muy importantes es que esta tecnología tiene como su mayor inconveniente la seguridad, ya que hay que tener y poner mucho empeño en ella.

La aplicación de la propuesta es muy sencilla, práctica y fácil de implementar, estas puede ser utilizada no solo en el Colegio Técnico Sudamericano, sino también en otras instituciones y en hogares que tengan una red inalámbrica montada.

La propuesta realizada debe ser aplicada para mejorar la seguridad de los dispositivos inalámbricos, se debe tener en cuenta que para aplicar estas seguridades se debe tener el apoyo necesario y compromiso del Administrador de la red.

La seguridad total de los dispositivos inalámbricos no existe, lo que se trata es de reducir el riesgo a niveles aceptables. Las seguridades es una continua actividad de cada día.

Como podemos notar cumplimos con los objetivos específicos propuestos en nuestro tema de tesis, en donde cubrimos los aspectos de Análisis, riegos, vulnerabilidades, amenazas, funcionamiento, estándares, configuraciones, arquitecturas de las redes inalámbricas.

5.2 Recomendaciones

La propuesta que se realiza deberá ser aplicada, para suplir muchas deficiencias de las configuraciones que se tienen en las redes inalámbricas de la institución.

Se debe tener un mayor control en la seguridad de las redes inalámbricas.

Dar capacitación técnica al Administrador de la red inalámbrica dentro y fuera de la institución para que este pueda dar un mejor mantenimiento a las redes inalámbricas y un mejor soporte a los estudiantes.

Desarrollar un plan de contingencia que contenga los procedimiento necesarios que se deben tomar cuando exista alguna falla en la red inalámbrica,

Crear políticas de seguridad, ya que la institución no cuenta con una de ellas.

Se debe dar mantenimiento constante a los dispositivos inalámbricos y revisar las seguridades y contraseñas de cada red.

Bibliografía

- http://www.elmercurio.com.ec/291643-anonymous-anuncia-acciones-para-defender-libertad-de-expresion-en-ecuador.html
- http://www.diariocritico.com/colombia/2011/Agosto/noticias/285076/anonymous-hackea-nuevamente-paginas-gubernamentales.html
- http://ec.globedia.com/descargarte-datos-facebook
- http://guias.bicgalicia.es/v2/nuevo/asp/individual/plantilla.asp?pagina=QueE
- http://es.wiktionary.org/wiki/an%C3%A1lisis
- http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
- http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html
- http://es.wikibooks.org/wiki/Seguridad_inform%C3%A1tica/Vulnerabilidad
- http://es.wikipedia.org/wiki/Wi-Fi
- http://es.wikipedia.org/wiki/Investigación
- http://es.wikipedia.org/wiki/Observación
- http://es.wikipedia.org/wiki/Entrevista_period%C3%ADstica
- http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Como-proteger-red-Wi-Fi-intrusos.php
- http://enredado.wordpress.com/2007/01/25/proteger-una-red-wireless/
- http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica_Mesh
- http://es.wikipedia.org/wiki/Extensible_Authentication_Protocol
- http://www.slideshare.net/iaraoz/la-triada

- http://es.wikipedia.org/wiki/IEEE_802.11
- http://www.x-net.es/tecnologia/wireless.pdf
- http://www.taringa.net/posts/linux/7124430.R/Como-anadir-mas-seguridad-a-tu-red-Wireless-_WIFI_.html
- http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
- http://www.alegsa.com.ar/Dic/tkip.php
- http://support.apple.com/kb/HT1365?viewlocale=es_ES&locale=es_ES

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Alberto Valencia
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que el pregradistaPaúl Santiago Guzhñay Cordero con CI No.0104435086 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la Ciudad de Cuenca**, del título de ingenieros en sistemas informáticos

Atentamente

_____
Ing. Alberto Valencia

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Esteban Cáceres
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que el pregradistaPaúl Santiago Guzhñay Cordero con CI No.0104435086 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la Ciudad de Cuenca**, del título de ingenieros en sistemas informáticos

Atentamente

_____
Ing. Esteban Cáceres

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Carlos Bautista
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que el pregradistaPaúl Santiago Guzhñay Cordero con CI No.0104435086 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la Ciudad de Cuenca**, del título de ingenieros en sistemas informáticos

Atentamente

_____
Ing. Carlos Bautista