PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

SERÉIS MIS TESTIGOS

ESCUELA DE INGENIERÍA DE SISTEMAS

TEMA:

Implementación de un HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad y la Provincia, ubicada en Ambato – Tungurahua

DISERTACIÓN DE GRADO PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR:

Bolívar Xavier Paredes Calero

DIRECTOR:

Ing. MSc. Darío Robayo

AMBATO – ECUADOR

Mayo – 2010

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

Implementación de un HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad y la Provincia, ubicada en Ambato – Tungurahua

Autor:

BOLÍVAR XAVIER PAREDES CALERO

Darío Robayo, Ing. MSc. f. _____

DIRECTOR DE TESIS

Galo López, Ing. MSc. f. _____

CALIFICADOR

Verónica Pailiacho, Ing. MSc. f. _____

CALIFICADOR

Santiago Acurio, Ing. Msc. f. _____

DIRECTOR UNIDAD ACADÉMICA

Pablo Poveda, Dr. f. _____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Mayo 2010

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Bolívar Xavier Paredes Calero portador de la cédula de ciudadanía No. 050316393-3 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniero de Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Bolívar Xavier Paredes Calero

CI. 050316393-3

AGRADECIMIENTO

Un agradecimiento especial al Honorable Gobierno Provincial de Tungurahua por autorizar la implementación del proyecto en la Biblioteca de la Ciudad y la Provincia, y a la Pontificia Universidad Católica del Ecuador Sede – Ambato, por la formación profesional que ha brindado a sus estudiantes.

DEDICATORIA

Este proyecto va dedicado a mis padres, que siempre me han brindado su apoyo, sin ellos nada de esto hubiera sido posible, también a todas la personas que han confiado en mí. A todos ustedes, mil gracias.

RESUMEN

En este proyecto se detalla la implementación de un HOTSPOT con servidor RADIUS en la Biblioteca Virtual de la Ciudad y la Provincia, ubicada en Ambato – Tungurahua, en donde se ofrece servicio de Internet gratuito a la ciudadanía, pero, el número de usuarios ha incrementado en los últimos meses y después de haber realizado encuestas a los usuarios, se notó que varios desean acceder al servicio de internet en sus propias computadoras portátiles o dispositivos móviles con tecnología inalámbrica, servicio con el que no cuenta la institución, por lo tanto, se implementó este sistema para incrementar el nivel de satisfacción de los usuarios que recurren a la institución. Debido a las políticas de la Biblioteca, el software utilizado para implementar este sistema es totalmente gratuito, por lo que simplemente se lo puede descargar desde el Internet. El software utilizado fue: sistema operativo Ubuntu 9.04, en donde están instalados los programas necesarios. Servidor Freeradius 2, el cual se encarga de administrar los usuarios y controlar el tiempo de acceso a Internet. Chillispot, un portal cautivo por el que pasan todos los usuarios que se conectan a la red para ingresar un nombre de usuario y una contraseña antes de tener acceso a Internet. Apache, en donde se aloja la interfaz de administración de todos los servicios. MySQL, como gestor de bases de datos. PHP como lenguaje de programación. EasyHotspot, una interfaz web que administra el HOTSPOT. Así la red está asegurada contra usuarios no autorizados que intenten acceder a la misma de manera ilícita y la necesidad de los usuarios será cubierta con un sistema eficaz.

ABSTRACT

This project details the implementation of a RADIUS server HotSpot at the Virtual Library of the City and the Province, located in Ambato - Tungurahua, where Internet service is offered free to the citizens. However, the number of users has increased in recent months and after performing user surveys, it was noticed that several of them request access to internet service in their own laptops or mobile devices with wireless technology. This service is not available in the institution, therefore, this system was implemented to increase the level of satisfaction of users making use of the institution. Due to the policies of the Library, the software used to implement this system is completely free; consequently, it can be simply downloaded from the Internet. The software applied was: Ubuntu 9.04 operating system, where the necessary programs are installed. Freeradius server 2, which is responsible for managing users and controlling Internet access time. Chillispot, a captive portal all users connecting to the network to enter a user name and password go before gaining access to the Internet. Apache, where the management interface for all the services is held. MySQL as a database manager, PHP as programming language. EasyHotspot, a web interface that manages HOTSPOT. As a result, the network is secured against unauthorized users attempting to access it illegally and the need for users will be covered with an efficient system.

TABLA DE CONTENIDOS

TABLA DE GRÁFICOS

CAPÍTULO I

1.1 Tema

Implementación de un HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad y la Provincia, ubicada en Ambato – Tungurahua

1.2 Antecedentes

Hoy en día el Internet es una herramienta indispensable tanto para estudiantes como para profesionales en el desarrollo investigativo en la provincia de Tungurahua, el país y el mundo entero, debido a esto el Honorable Gobierno Provincial de Tungurahua ha implementado desde hace más de tres años un servicio de Internet gratuito en una Biblioteca Virtual abierta a todo el público en general para que puedan realizar investigaciones. Esta inició sus labores para atender a la ciudadanía desde el 26 de marzo del 2007.

La Biblioteca Virtual del Honorable Gobierno Provincial de Tungurahua tiene como objetivo fomentar la formación educativa e investigativa de la ciudadanía de la provincia, por lo tanto el uso del Internet en la Biblioteca Virtual es estrictamente para investigaciones académicas, más no para entretenimiento, por lo que páginas sociales, pornografía, archivos ejecutables, software P2P, etc. están restringidos.

Los horarios de atención son de lunes a viernes de 9:00 a 12:30 y de 15:00 a 18:30, los sábados de 9:00 a 12:00 horas.

Gracias a los avances tecnológicos dentro de la informática que existen en la actualidad, se pude mejorar el servicio de internet para que los usuarios puedan realizar sus investigaciones en la biblioteca y estén satisfechos con el servicio que se ofrece. Debido al incremento de usuarios es urgente implementar un sistema con el que los usuarios puedan realizar sus investigaciones sin tener que esperar que una máquina esté disponible o que el mismo pueda trabajar en una computadora portátil de su propiedad.

1.3 Definición del problema

El problema nace porque el número de usuarios en la Biblioteca Virtual ha incrementado considerablemente, y muchos de los usuarios desean realizar sus investigaciones en sus propias computadoras portátiles o dispositivos móviles con tecnología inalámbrica, pero la Biblioteca Virtual no cuenta con este servicio, por esta razón se implementó un HOTSPOT con un servidor RADIUS el cual autentique los usuarios que se propongan acceder a la red para utilizar el servicio de Internet, para lo cual se investigó como configurar este servidor, el sistema operativo a utilizar y el tipo de seguridad para proteger la red inalámbrica.

Con la implementación de éste sistema el número de usuarios incrementó significativamente aumentando también el nivel de satisfacción de los mismos, al ofrecer un mejor servicio para mejorar el nivel académico e intelectual para un mejor desarrollo de la ciudad, la provincia y sus alrededores.

1.3.1 Delimitación del problema

La implementación del HOTSPOT con servidor RADIUS se realizó para autentificar a los usuarios que deseen acceder al servicio de Internet para realizar sus investigaciones en sus propias computadoras portátiles o dispositivos móviles con tecnología inalámbrica, en la Biblioteca Virtual en la ciudad de Ambato de la provincia de Tungurahua.

1.3.2 Preguntas básicas

- ¿Es necesaria la implementación de este sistema para la comunidad en la Biblioteca Virtual?
- ¿El número de computadores es suficiente para dar abasto a la demanda de servicio?
- ¿Existen en la actualidad indicadores que muestren el real uso que la comunidad le da al servicio de internet?
- ¿Es eficiente la actual política de seguridad de la red inalámbrica?

1.4 Objetivos.

1.5.1 Objetivo general.

Implementar un Hotspot con servidor RADIUS en la Biblioteca Virtual de la Ciudad y la Provincia, para incrementar el número de usuarios y el nivel de satisfacción de los mismos.

1.5.2 Objetivos específicos.

- Satisfacer el requerimiento de los usuarios para utilizar el servicio de internet con sus propios computadores o dispositivos móviles que tengan tecnología WIFI.
- Implementar un método de seguridad eficaz en la red inalámbrica.
- Generar datos estadísticos de concurrencia de los usuarios que ocupan el servicio y analizar el número y nivel de satisfacción de los mismos.

1.5 Metodología.

1.6.1 Fuentes de información.

Para la realización del proyecto la fuente de investigación que se utilizó continuamente fue el Internet, ya que, hoy en día es la herramienta más poderosa para buscar información de cualquier tipo y en éste particular caso es en donde más información se puede obtener.

También se utilizó bibliografía referente a la implementación de redes inalámbricas seguras e implementación de servidores utilizando Linux.

1.6.2 Instrumentos para obtener la información.

En este caso realizó una encuesta a los usuarios para conocer que tan de acuerdo están con la implementación de este sistema, si la concurrencia de usuarios va a aumentar y si

éstos se sentirían más cómodos trabajando en su propia computadora portátil o dispositivo móvil con tecnología inalámbrica.

1.6.3 Métodos de investigación.

Para obtener la información necesaria que va a ayudar a realizar el proyecto se utilizó el método de investigación bibliográfica porque sirvió como referencia algunos artículos ya publicados los cuales fueron muy útiles.

También se utilizó el método de investigación de campo ya que como se mencionó se hizo encuestas a los usuarios para conocer algunos detalles del servicio.

1.7 Justificación.

Desde que la Biblioteca Virtual de la Ciudad y la Provincia abrió sus puertas a la ciudadanía, ha existido mucha concurrencia de usuarios que desean ocupar el servicio de Internet gratuito. El nivel de usuarios ha incrementado significativamente en los últimos meses, habiendo usuarios que desean acceder al servicio de internet gratuito desde sus propias computadoras portátiles o dispositivos móviles con tecnología inalámbrica, pero lamentablemente este servicio no está disponible en esta entidad.

Por esta razón se cree que es necesaria la implementación de un sistema que permita que los usuarios puedan conectarse a internet para realizar sus investigaciones desde sus propias computadoras portátiles o dispositivos con tecnología inalámbrica.

En la actualidad existen varias maneras para acceder inalámbricamente al Internet, pero uno de los problemas más grandes que existen con este tipo de conexión es el nivel de seguridad utilizado para que personas no autorizadas tengan acceso a la red ilícitamente, por lo tanto, la decisión de implementar un HOTSPOT con servidor RADIUS es una de las opciones más seguras para una red inalámbrica, ya que permite la autenticación de usuarios que previamente se configuran en este servidor y al momento que el usuario desee conectarse a la red el sistema le pedirá un nombre de usuario y contraseña, el sistema verifica la existencia de este usuario y le permite o no conectarse a la red.

Así el nivel de seguridad de la red será muy alto y solo las personas que estén registradas en el sistema podrán tener acceso al servicio, con esto se evitará que la red sufra algún tipo de ataque en su configuración.

CAPÍTULO II

A continuación se revisarán varios conceptos fundamentales, los cuales ayudarán comprender la investigación.

2.1 Red informática.

En la actualidad las redes informáticas son una de las partes fundamentales en la comunicación empezando desde el hogar hasta en las grandes empresas que se comunican de un continente a otro. Pero que significa una red de comunicación, no es nada más que varias computadoras conectadas entre sí mediante un dispositivo con la finalidad de compartir varios servicios como datos (archivos), impresoras, correo electrónico, Internet, aplicaciones, etc. Según el tamaño de la red se las puede clasificar en varios tipos, También existen varias formas de conexión de una red según la necesidad de los usuarios, a estos tipos de conexiones se las llama topologías de red, lo cual se describirá más adelante. La siguiente figura muestra un ejemplo de una red informática.

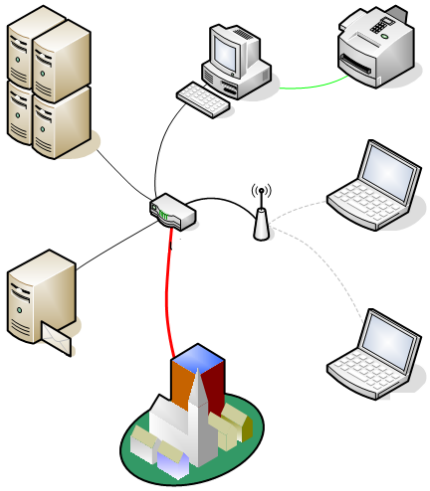

Figura 2.1 Red informática

2.2 Topologías de red.

La topología de red define la manera en la que los dispositivos están conectados entre sí para enviar y recibir la información, existen varios tipos de conexiones las cuales se las define a continuación.

2.2.1 Red de bus.

En este tipo de conexión cada dispositivo comparte el mismo canal de comunicación, es de fácil implementación, pero si se cae cualquier punto de la red, dejará de funcionar.

Figura 2.1: Red informática
http://www.csandoval.net/images/lan.png

Figura 2.2: Red de bus

2.2.2 Red de estrella.

Es la más utilizada en hogares u oficinas, los dispositivos están conectados directamente a un punto central que se encarga de repartir la información a toda la red, si se cae cualquier punto de recepción la red seguirá funcionando, peor si el punto central falla la red dejará de funcionar.

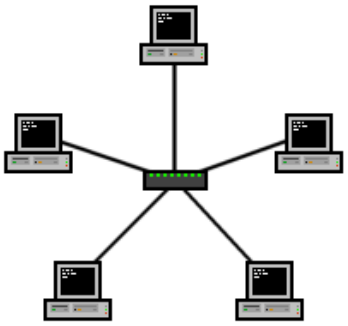

Figura 2.3: Red de estrella

Figura 2.2: Red de bus
http://upload.wikimedia.org/wikipedia/commons/3/32/Netzwerktopologie_Bus.png
Figura 2.3: Red de estrella
http://upload.wikimedia.org/wikipedia/commons/5/53/Netzwerktopologie_Stern.png

2.2.3 Red de anillo.

Aquí cada dispositivo es receptor y emisor, el último punto se conecta al primero formando un anillo, si cualquier punto de la red se cae dejará de funcionar, su desventaja es el mayor costo que de implementación.

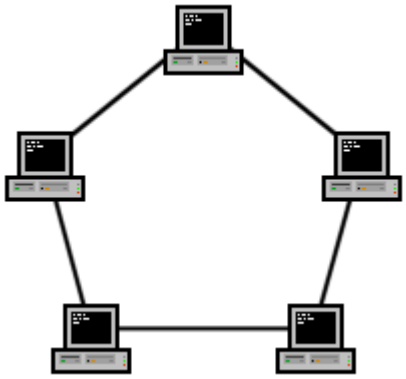

Figura 2.4: Red anillo

2.2.4 Red de doble anillo.

Es una mejora de la red de anillo, se utiliza un segundo anillo para asegurar la transmisión y recepción de los datos, no existe pérdida de datos si uno de los dos anillos se cae.

Figura 2.4 : Red de anillo
http://upload.wikimedia.org/wikipedia/commons/7/71/Netzwerktopologie_Ring.png

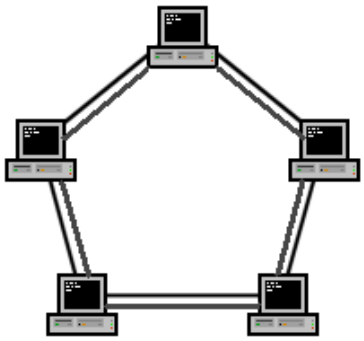

Figura 2.5: Red de doble anillo

2.2.5 Red en malla.

Todos los puntos se conectan entre sí, asegurando así que los datos no se pierdan y que existan varias vías para la transmisión de los mismos, existiendo una baja probabilidad de que los datos se pierdan pero su implementación es costosa.

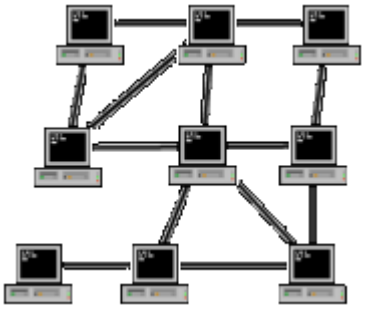

Figura 2.6: Red en malla

Figura2.5: Red de doble anillo
http://es.wikipedia.org/wiki/Red_en_anillo2
Figura 2.6: Red malla
http://upload.wikimedia.org/wikipedia/commons/9/91/Netzwerktopologie_vermascht.png

2.2.6 Red de árbol.

Es una combinación de varias topologías, como la red de bus y la red de estrella, hay varios dispositivos se encargan de repartir los datos. Si se cae algún punto la red seguirá funcionando sin afectar la transmisión de datos. Soporta varios puntos pero resulta costosa su implementación.

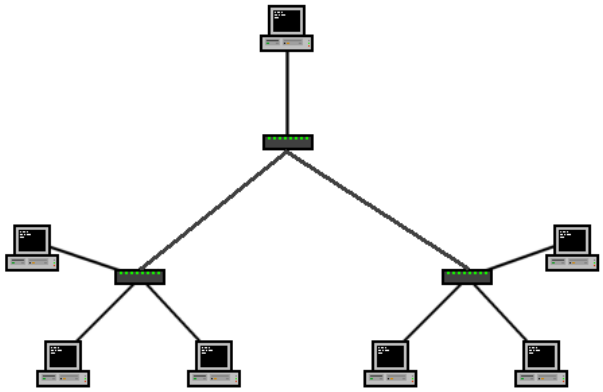

Figura 2.7: Red de árbol

2.3 Clasificación de las redes.

Definidas cada una de las topologías de red, es importante conocer la clasificación de estas, según el tamaño se la puede clasificar en:

Figura 2.7 : Red de árbol
http://upload.wikimedia.org/wikipedia/commons/a/ad/Netzwerktopologie_Baum.PNG

2.3.1 Red LAN.

La red de área local (Local Area Network), permite la conexión de dos o más dispositivos en un área 200 metros, es implementada generalmente en edificios, oficinas, centros educativos etc., permitiendo compartir recursos como datos, impresoras, Internet, etc.

2.3.2 Red MAN.

La red de área metropolitana (Metropolitan Area Network), es una evolución de la red LAN ya que cubre extensas áreas en las que varios dispositivos hacen uso de los recursos de la red, puede llegar a cubrir distancias de hasta 4 kilómetros y combinándola con la red LAN puede dar cobertura a ciudades enteras.

2.3.3 Red WAN.

La red de área amplia (Wide Area Network), es un tipo de red que cubre áreas mucho más extensas que la red MAN, ésta red está diseñada para compartir datos entre dispositivos los cuales se encuentran a varias distancias, puede llegar a cubrir desde 100 kilómetros de área hasta 1000 kilómetros, pudiendo interconectar países o continentes enteros.

2.3.4 Red VLAN.

La red de área local virtual (Virtual Local Area Network), como su nombre lo indica es una red virtual creada como una división de una red de área local, creada para facilitar su

administración, un ejemplo claro de una red de área local virtual es las diferentes subredes que pueden existir en los departamento de una empresa para facilitar el tráfico de los datos y la detección de daños en la red global.

2.3.5 Red WLAN.

La red inalámbrica de área local (Wireless Local Area Network), es una red que se utiliza comúnmente en hogares y oficinas, es una alternativa muy útil para implementarla en hogares u oficinas ya que no hace falta tener un cable para la transmisión de datos realizando este procedimiento por medio de ondas de radio.

2.4 Modelo OSI.

Para que las computadoras puedan comunicarse entre sí y utilizar los servicios que una red ofrece, en 1984 la Organización Internacional de Estándares (ISO), creó un estándar llamado OSI, debido a las diferentes tecnologías que cada fabricante presentaba, lo que dificultaba la comunicación entre dispositivos de diferente marca. Hoy en día todas las redes de información aplican éste estándar, el cual está conformado por siete niveles divididos en dos grupos: de transporte y de aplicación.

Figura 2.8: Modelo OSI

Cada nivel cumple con una función determinada cuando los datos son enviados detallándolos a continuación:

- Nivel físico: Es el medio por el cual se van a transportar los datos ya sea por cable o inalámbricamente.
- Nivel de enlace de datos: Se encarga de verificar que cualquier tipo de transmisión de datos sea confiable, definiendo el direccionamiento físico, topología de la red, control de flujo y detección de errores.
- Nivel de red: Se encarga de que los datos sean recibidos desde su lugar de origen hasta su lugar de destino sin importar que estos puntos estén conectados

Figura 2.8: Modelo OSI
http://48kb.com/wp-content/uploads/2009/03/modelo-osi.png

directamente, llevando un control en la congestión de la red, direccionando lógicamente a los datos (direccionamiento IP) y determinando la mejor ruta para transmisión de datos.

- Nivel de transporte: Se encarga de mantener el control de flujo de los datos, la verificación de errores, y la recuperación de datos entre dispositivos.
- Nivel de sesión: Este nivel está encargado de permitir que el enlace entre dos dispositivos se mantengan, asegurando que los datos se transmitan de principio a fin sin perder la información enviada.
- Nivel de presentación: Este nivel es el que da formato a los datos enviados para que el receptor pueda recibirlos, tomando en cuenta aspectos como la sintaxis y la semántica, ya que cada dispositivo tiene una manera distinta de manejar la información.
- Nivel de aplicación: Este nivel no proporciona información a ningún otro nivel ya que es el último, se encarga de presentar los datos al usuario por medio de una aplicación, navegadores, documentos de texto etc.

2.5 Componentes de una red informática.

Ya revisado el modelo OSI en el cual está basada una red informática, las diferentes topologías que existen y su clasificación, a continuación se revisará los componentes que se requieren para la implementación de una red de información tanto físicamente como lógicamente.

2.5.1 Servidor.

Es una computadora la cual gestiona los servicios que ofrece la red con un sistema operativo creado exclusivamente para desempeñar dicha función (en este caso Linux que

se estudia más adelante). Es capaz de restringir el acceso a la red mediante reglas programadas y se encarga de evitar congestiones en la red. Es importante contar con un servidor cuando la red es de mediano o gran tamaño como las redes MAN o WAN.

2.5.2 Terminales de trabajo.

Las terminales son simplemente las computadoras, ya sean fijas (de escritorio), portátiles o dispositivos que sean capaces de formar parte de una red, y son las que hacen uso de los servicios de la red.

2.5.3 Interfaces o tarjetas de red.

Las interfaces o tarjetas de red es en donde van conectados los diferentes medios de transmisión de datos, deben ser compatibles con la terminal de trabajo para que puedan funcionar, cuentan con un software llamado controlador el cual se encarga de enlazar la tarjeta de red con el sistema operativo. Cuentan con una dirección MAC (Control de Acceso al medio) que es una dirección con la que obligatoriamente cuentan estos dispositivos y es única, es decir no se repite en ningún dispositivo.

2.6 Medios de transmisión de datos.

Los datos deben viajar por algún medio para poder ser transportados de un lugar a otro, a continuación se mencionará alguno de estos medios los cuales hacen posibles que los datos viajen de un punto a otro, estos medios pueden ser físicos o inalámbricos (Más adelante se detallará esta tecnología).

2.6.1 Cable coaxial.

Es un cable que en la actualidad ya no se lo utiliza para las redes informáticas, fue creado en 1930, está conformado por dos cables conductores, un cable central por donde transporta los datos y un cable tubular llamado malla que sirve como tierra.

2.6.2 Cable UTP.

Sus siglas significan par trenzado no pantallado, es el más común en las redes de información por su bajo costo. La siguiente tabla describirá las diferentes categorías de este cable, su velocidad de transmisión y la frecuencia con la que pueden llegar a transmitir los datos.

Categoría	Velocidad de transmisión	Frecuencia
1	4 Mbps	1 Mhz
2	6 Mbps	4 Mhz
3	10 Mbps	16 Mhz
4	20 Mbps	20 Mhz
5	100 Mbps	100 Mhz
6	1 Gbps	250 Mhz
7	10 Gbps	600 Mhz

Tabla 1: Categorías de cable UTP

El cable más utilizado en nuestro medio es el cable de categoría 5, está conformado por cuatro pares trenzados (hilos), los cuales son de colores diferentes.

Figura 2.9: Cable UTP

Este cable es conectado a los puertos Ethernet para que la información que se va a transmitir llegue a sus diferentes puntos de destino. Esto se logra adaptando un conector en los dos extremos del cable llamado RJ-45 (Restricted Jack).

Figura 2.10: Conector RJ-45

2.6.3 Fibra óptica.

La fibra óptica es un hilo muy fino hecho de vidrio o plástico (óxido de silicio y germanio) por el cual se envían pulsos de luz los cuales representan los datos en una red. Es capaz de transportar una gran cantidad de datos a una velocidad mayor o igual a la del cable UTP, es utilizado cuando en la implementación de redes de información se necesita transportar datos entre puntos muy distantes ya que es un material resistente y

Figura 2.9 : Cable UTP
http://tvcenlinea.com/tienda/catalog/images/utp2.gif
Figura 2.10: Conector RJ-45
http://chilenomac.files.wordpress.com/2009/03/rj45.jpg

no es sensible a las interrupciones electromagnéticas que hay en el ambiente, garantizando así que la información enviada no se va a perder.

Figura 2.11: Fibra óptica

2.7 Dispositivos para gestionar paquetes de datos.

Inicialmente se había indicado que en una red informática existen varios dispositivos que están conectados entre sí por medio de algún dispositivo, igualmente en varias de las topologías se notó que para poder tener conexión entre cada punto se utilizaba un dispositivo central el cual se encarga de transmitir la información a cada uno estos puntos. Los dispositivos que se encargan de ésta tarea pueden ser varios y se detallan a continuación.

2.7.1 Hub.

Es un dispositivo que cuenta con varios puertos Ethernet y con un puerto llamado generalmente “Uplink”, en donde se puede conectar otro HUB y a su vez a este mismo

---

Figura 2.11: Fibra óptica
http://cienciaaldia.files.wordpress.com/2009/10/fibra.jpg

se conectarán más puntos consiguiendo así una extensión de la red. En la actualidad ya no se o utiliza.

Figura 2.12: HUB

2.7.2 Switch.

Es un dispositivo con características parecidas a las del HUB, la diferencia entre los dos es que si queremos expandir el tamaño de la red conectando más SWITCHES, estos pueden ser conectados en cualquier puerto Ethernet. Los datos enviados los recibe únicamente el punto destinado sin pasar la información por todos los puntos.

Figura 2.13: SWITCH

Figura 2.12: HUB
http://upload.wikimedia.org/wikipedia/commons/d/d9/4_port_netgear_ethernet_hub.jpg
Figura 2.13: SWITCH
http://www.microalcarria.com/global/php/imagen.php?camino=/uknaaxyhr/&nombre=drtfbtzx/CBY-0755J.oif

2.7.3 Router.

El ROUTER o enrutador cuenta con varios puertos Ethernet a los cuales se puede conectar SWITCHES, HUBS, computadores, impresoras, etc., se encarga de dirigir los paquetes que envía cualquier punto de la red únicamente hacia el punto de destino. Existen varios tipos de enrutadores, la mayoría cuentan con un puerto WAN en donde se sitúa una conexión de Internet, los dispositivos que se conecten a éste compartirán dicho servicio.

Figura 2.14: Router

Existe otro tipo de ROUTER llamado ROUTER ADLS, en nuestro medio se lo conoce como módem ADSL, las empresas que proveen de servicio de Internet son las que trabajan con éste tipo de dispositivo, el cual cuenta con un puerto ADLS que es en donde se conecta la línea telefónica y con uno o varios puertos Ethernet.

Cabe aclarar que una conexión ADSL (Línea de suscripción digital asimétrica), es la transmisión digital de datos (Internet) por medio de la línea telefónica convencional.

Figura 2.14: Router
http://es.wiki2buy.com/images/a/a5/Router.jpg

Figura 2.15: Router ADSL

Por último tenemos otro tipo de enrutador el cual cumple las funciones de los anteriores pero cuenta con son una salida inalámbrica (WLAN), con la que podrán conectarse a la red inalámbricamente varios dispositivos como computadores portátiles o dispositivos móviles (más adelante se hablará de estos dispositivos y la tecnología inalámbrica con más detalle).

Figura 2.16: Router Inalámbrico

Figura 2.15: Router ADSL
http://img.alibaba.com/photo/101281892/Siemens_Cl_110_Router_ADSL_USB_Ethernet_Modem.jpg
Figura 2.16: Router inalámbrico
http://www.pcpartes.cl/catalog/images/1621.jpg

2.8 Familia de protocolos.

Un protocolo es el que permite la transferencia de datos entre computadoras dentro de una red, existen más de cien protocolos pero el estudio se centrará más en el protocolo TCP/IP, que más adelante se lo detallará, en la siguiente tabla se encuentra una lista de los protocolos más importantes y la utilidad de cada uno de ellos:

Protocolo	Utilidad
HTTP	Acceso a páginas web
FTP	Transferencia de archivos
SMTP	Correo electrónico
POP	Correo electrónico
TELNET	Acceso a equipos remotos

Tabla 2: Familia de protocolos

2.8.1 Protocolo TCP/IP.

Este protocolo es el que permite la comunicación entre computadoras en una red sin importar el sistema operativo de cada computadora, es el encargado de transferir los datos mediante paquetes y recibirlos en el orden en el que fueron enviados.

TCP significa Protocolo de Control de Transmisión, garantizando que los datos enviados de un punto hacia otro no se pierdan y sean recibidos tal y como se les envió.

IP significa Protocolo de Internet el cual utiliza direcciones asignadas a cada terminal de la red para conocer el destino de cada paquete enviado dentro de la red por ejemplo 192.168.1.1.

Existen dos versiones del Protocolo de Internet IPv4 e IPv6.

2.8.1.1 IPv4.

Esta es la versión del protocolo IP que más se ha extendido en el mundo y por lo tanto es la más utilizada, el número de direcciones IP que soporta es de 2^{32} o sea 4.294.967.296. Éste protocolo es la base para el funcionamiento del internet, en la actualidad ya no abastece la demanda de direcciones alrededor del mundo existiendo también un desperdicio de direcciones, por esta razón se creó una versión más avanzada.

2.8.1.2 IPv6.

Esta versión del protocolo IP fue creada para sustituir a las versión 4. La versión 6 de este protocolo soporta un número de direcciones de 2^{128} es decir 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones, solucionando así el gran problema de la versión 4 del protocolo IP.

2.9 Direccionamiento IP.

Una dirección IP es la que identifica lógicamente a un dispositivo dentro de una red informática. Al conectar un dispositivo a una red, éste puede recibir una dirección IP automáticamente (Dirección dinámica) o se la puede asignar manualmente (Dirección estática), según la configuración de la red.

Hay 2 tipos de direcciones IP, las privadas y las públicas. Las direcciones IP públicas son las que se manejan dentro del Internet sin existir una igual a otra como en un sistema de telefonía. Las direcciones privadas son las que se manejan dentro de una red en el hogar o en una empresa, asignándolas a cada terminal y tampoco se podrán repetir dentro de la red, pero no existe inconveniente alguno si otra empresa trabaja con el mismo direccionamiento IP ya que son redes diferentes.

También para acceder a un equipo específico con mayor facilidad con facilidad se lo busca a través del nombre asignado a éste, conocido como servidor de nombres de dominio (DNS).

2.9.1 Direcciones IP de la versión del protocolo IPv4.

Es una dirección de 32 bit compuesta por 4 ***octeto***s que van de 0 a 255, cada ***octeto*** es separado por un punto ".", por ejemplo **191.168.2.99**. Aquí encontramos 5 clases de direccionamiento empleadas para diferentes casos, la siguiente Tabla 3 representa las clases de direccionamiento IP:

Las direcciones de la clase A, B y C, están determinadas como privadas, mientras que las direcciones de la clase D y E, tienen otra utilidad que en éste caso de estudio no hace falta indicar.

2.9.2 Direcciones IP de la versión del protocolo IPv6.

Este tipo de direccionamiento IP cumple la misma función que el anterior, la diferencia es que trabaja con el protocolo IPv6, está compuesto por 128 bit representándose con 32

dígitos hexadecimales separados por dos puntos ":", por ejemplo **2001:123:4:ab:cde:3403:1:63.**

Clase	Rango	Número de redes	Número de Hosts	Máscara de red	Broadcast
A	1.0.0.0 - 127.255.255.255	126	16.777.214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	16.384	65.534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	2.097.152	254	255.255.255.0	x.x.x.255
D	224.0.0.0 - 239.255.255.255				
E	240.0.0.0 - 255.255.255.255				

Tabla 3: Clases de direccionamiento IPv4

2.10 Redes inalámbricas.

Hasta ahora se ha tratado conceptos fundamentales los cuales ayudan a tener una idea clara de lo que es una red de comunicación y los proceso que se realizan para transmitir datos de un punto a otro, ahora se estudiará la base de ésta investigación, las redes inalámbricas (también conocidas como Wireless en inglés).

Sus orígenes surgen en año 1979 durante un experimento realizado por un grupo de ingenieros de la empresa IBM, el experimento consistió en enlazarse a una red utilizando señales infrarrojas, observando éste resultado las investigaciones continuaron hasta

llegar a tener una conexión estable a una. Una red inalámbrica cumple la misma función de una red cableada, es decir, transmitir datos de un punto hacia otro, la diferencia es que éste proceso se lo realiza sin necesidad de un cable.

Figura 2.17: Red inalámbrica

En la actualidad las redes inalámbricas se están propagando mucho en nuestro medio, en este tipo de conexión los datos son transportados por medio de ondas electromagnéticas, en donde el dispositivo emisor y el transmisor deben contar con esta tecnología.

Al igual que las redes cableadas, una red inalámbrica se basa en un estándar creado por la ***IEEE*** (Instituto de Ingenieros Electricistas y Electrónicos) conjuntamente con la Alianza Wi-Fi (Wi-Fi Alliance), que es una organización la cual prueba y certifica que los dispositivos inalámbricos cumplan con el estándar 802.11 el cual trabaja sobre los dos primeros niveles del modelo OSI; nivel físico y nivel de datos, especificando sus normas de funcionamiento en una red. También podemos encontrar varias clases de redes inalámbricas las cuales ya se mencionó anteriormente.

Figura 2.17: Red inalámbrica
http://hdo.com.ec/portal/images/stories/red_inalambrica.jpg

2.10.1 Estándar IEEE 802.11.

El estándar 802.11 de la IEEE trabaja sobre los dos primeros niveles del modelo OSI; nivel físico y nivel de datos, especificando sus normas de funcionamiento en una red. Dentro de una red inalámbrica la capa física del modelo OSI es la que define la modulación y características de las ondas electromagnéticas durante la transmisión de los datos, mientras que la capa de enlace es la encargada de controlar que los datos enviados mediante las ondas electromagnéticas no hayan sido alterados durante la transmisión de los datos. En definitiva estas capas cumplen la misma función que la de una red física.

Éste estándar cuenta con varias versiones, cada una de estas cuentan con mejoras con respecto a su versión anterior y cada una de estas fue creada para un determinado uso en algunos casos. En la siguiente tabla se explica rápidamente una pequeña descripción de cada versión de este estándar:

Nombre del estándar	Descripción
802.11 a	Admite un ***ancho de banda*** superior (máximo 54 Mbps), provee ocho canales de radio en la banda de frecuencia de 5 ***GHz***.
802.11 b	Es el más utilizado en nuestro medio. Ofrece un rendimiento total máximo de 11 Mpbs y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 ***GHz*** con tres canales de radio disponibles.
802.11 c	No ofrece ningún interés para el público general, es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11 d	Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11 e	Está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace

	de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ***ancho de banda*** y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11 f	Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Permite a un usuario cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar la marca de los puntos de acceso.
802.11 g	Ofrece un ***ancho de banda*** elevado (54 Mbps) en el rango de frecuencia de 2,4 ***GHz***. Es compatible con el estándar 802.11f y el 802.11b, por lo tanto los dispositivos que admiten el estándar 802.11g también son compatibles con los estándares mencionados.
802.11 h	Regula el uso de las frecuencias y el rendimiento energético de los estándares europeos.
802.11 i	Está destinado a mejorar la seguridad en la transferencia de datos. Éste estándar se basa en el ***AES*** (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11 Ir	Se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11 j	Es equivalente al 802.11h, en la regulación Japonesa
802.11 k	Su objetivo es mejorar la señal electromagnética de los dispositivos facilitando su administración, asegurando un funcionamiento óptimo de la red.
802.11 n	Es el último estándar que presenta la IEEE en la actualidad, alcanza una velocidad de 450 Mbps, razón por la cual no existe pérdida de ***ancho de banda***.
802.11 p	Creado para usarse en sistema de transporte inteligentes, intercambiando información entre vehículos en las vías. Su creación fue impulsado por el ministerios de transporte de Estados Unidos y algunos fabricantes de vehículos, opera en frecuencias de 5.9 ***Ghz***.
802.11 r	La principal función de éste estándar es aumentar la velocidad de conexión el momento en el que un dispositivo traslada su conexión de un punto de acceso a otro, manteniendo así su conexión a la red inalámbrica sin perder los datos.
802.11 s	Creado para redes inalámbricas de topología de malla, apareció en el año 2006 en los Estados Unidos.
802.11 u	El objetivo de éste estándar es facilitar la interoperabilidad de los dispositivos con las redes externas, siendo los proveedores de telefonía celular los más beneficiados con la creación de éste estándar.
802.11 v	Su lanzamiento está previsto para este año, su objetivo es mejorar la gestión y

	configuración de dispositivos y la administración remota en las redes inalámbricas.
802.11 w	Creado para aumentar la seguridad en el nivel 2 del modelo OSI disminuyendo así las vulnerabilidades de las redes inalámbricas.
802.11 y	Creado para los Estados Unidos el cual trabaja en las frecuencias de 3650-3700 MHz, siendo una frecuencia muy alta y de mayor alcance.

Tabla 4: Versiones del estándar IEEE 802.11

Cabe recalcar que varios de estos estándares no se utilizan dentro de nuestro medio debido a la infraestructura de Internet y a la regulación de frecuencias con el que se cuenta. En nuestro país los estándares más utilizados en la actualidad son el 802.11n y el 802.2g, pero no se los aprovecha por completo por la calidad en la velocidad del Internet.

2.10.2 Conceptos importantes dentro de una red inalámbrica.

Para lograr comprender el funcionamiento de una red inalámbrica, a continuación se explicarán algunos conceptos los cuales son importantes conocer.

2.10.2.1 Punto de acceso.

Cuando se estudió el estándar 802.11 varias veces se nombró a éste dispositivo. Un punto de acceso (Access Point en inglés), es un medio de transmisión de datos dentro de una red inalámbrica, cumple la misma función que un SWITCH, la diferencia es que éste dispositivo transmite los datos sin contar con un medio físico, o sea inalámbricamente mediante ondas electromagnéticas. Se utiliza para hacer de intermediario en las redes inalámbricas, entre equipos que cuentan con esta tecnología o para convertir una red

cableada en inalámbrica. No hay que confundir un punto de acceso con un enrutador inalámbrico ya que son dispositivos diferentes, el punto de cuenta con un solo puerto Ethernet en donde se conecta el cable de red.

Existen varios fabricantes de este dispositivo encontrándolo disponible en distintas marcas como Linksys, D-Link, CNet, etc.,

Figura 2.18: Punto de acceso

2.10.2.2 SSID.

Es un código conformado por 32 caracteres alfanuméricos. Este código es el nombre que se le asigna y con el que se le identifica a una red inalámbrica. Tiene dos denominaciones, BSSID si la red es entre equipos y no se cuenta con un punto de acceso o ESSID si se utiliza un punto de acceso para conectarse a una red inalámbrica.

Figura 2.18: Punto de acceso
http://www.linksysbycisco.com/videos/gallery/05,41.png
http://www.xakia.com/img/products/1/12334i1.jpg

2.10.2.3 Canal.

Dependiendo del tipo de red inalámbrica y del estándar que lleve cada dispositivo, las ondas electromagnéticas se dividen en canales. En el caso de redes inalámbricas que trabajen bajo el estándar 802.11b/g, que son las que se utilizan en nuestro medio, las ondas electromagnéticas se dividen en 14 canales y varía según las normativas es cada país. Estos canales fijan las frecuencias de trabajo para los equipos que forman parte de una red.

2.10.2.4 Potencia.

El nivel de potencia de una señal se expresa usualmente en ***dBm*** (decibelios relativos a 1 mW). Cada uno de los componentes en la transmisión de datos en una red aumenta o disminuye la potencia de la señal.

2.10.2.5 Cobertura.

La cobertura de un dispositivo de transmisión en una red inalámbrica depende del tipo de antena que se utilice y también de varios factores externos como la estructura de las construcciones, el clima, interferencia con otras señales, etc. La cobertura de la señal se va perdiendo a medida que el dispositivo receptor se aleja del dispositivo transmisor, dependiendo de la potencia de estos, hasta llegar a perderse.

2.10.2.6 Antenas.

Existen varios tipos de antenas que se utilizan en una red inalámbrica. Esta antena no agrega potencia a la señal, solo la dirige en mayor grado hacia un ángulo deseado para tener mayor recepción de señal.

2.10.2.7 Tarjeta de red inalámbrica.

Una tarjeta de red inalámbrica es un tipo de tarjeta de que se conecta a la tarjeta madre de una computadora o a un puerto como el USB, y que permite conectarse a una red inalámbrica. Prácticamente cumple la misma función que una tarjeta de red cableada.

Figura 2.19: Tarjetas de red inalámbrica

Figura 2.19 : Tarjeta de red inalámbrica
http://v3teknos.com/IMAGENES/tarjeta_de_red_inalambrica.jpg
http://www.corporaciondelco.com/images/zonet.jpg

2.10.3 Seguridad de una red inalámbrica.

Al surgir las redes inalámbricas se expandieron rápidamente por su facilidad para implementarlas, pero poco a poco se encontraba un gran problema con la seguridad ya que era muy fácil que una persona no autorizada en la red se introduzca a utilizar les servicios de la misma e incluso a tener acceso a datos confidenciales. La seguridad en una red inalámbrica consiste en una clave de varios dígitos los cuales el usuario debe conocer e introducirlos el momento en el que esté dispuesto a conectarse a una red. A continuación se describirá los tipos de seguridades más utilizadas en la actualidad.

2.10.3.1 Wep.

Al notar el gran problema de las redes inalámbricas con la seguridad, se implementó un tipo de seguridad llamada WEP que significa privacidad equivalente a redes cableadas (Wire Equivalent Privacy, en inglés) que al parecer solucionaba los problemas de seguridad que existían. En pocos años este tipo de seguridad fue atacada por personas que quería introducirse en las redes ilícitamente demostrando así vulnerabilidades en su seguridad a nivel empresarial, por lo que se notó que no era confiable. Aún así actualmente un gran porcentaje de redes inalámbricas utilizan éste tipo de seguridad por su facilidad de implementación considerándose suficiente para los hogares.

2.10.3.2 Wpa.

Significa Acceso Protegido Wi-Fi, fue creado por la Alianza Wi.Fi para proteger las redes inalámbricas corrigiendo las deficiencias que creó la seguridad WEP.

WPA fue diseñado para utilizar un servidor de autenticación, normalmente un servidor RADIUS (que se estudiará más adelante), distribuyendo claves diferentes a cada usuario de la red. También se puede utilizar a niveles de más baja seguridad pero suficiente para proteger redes inalámbricas domésticas o de pequeña oficinas donde no se necesita un servidor de autenticación, diferenciándolas como WPA Enterprise y WPA Personal respectivamente.

La principal mejora de éste tipo de seguridad es que cuenta con el Protocolo de Integridad de Clave Temporal (***TKIP***) y el Estándar Avanzado de Seguridad (***AES***) , los cuales son algoritmos para cifrar las claves de seguridad. Esta clave cambia dinámicamente a medida que se utiliza, ofreciendo así un alto de nivel de seguridad.

También cuenta con una protección de desconexión contra ataques restringiendo la disponibilidad de conexión durante 60 segundos al detectar dos intentos fallidos durante 1 minuto, limitando el riesgo de ataques.

2.10.3.3 WPA2.

WPA2 fue creado por la IEEE bajo el estándar 802.11i, a diferencia del tipo de seguridad anteriormente mencionado que fue creado por la Alianza Wi-Fi, y en la actualidad todos los dispositivos que cuentan con tecnología inalámbrica deben contar con este tipo de seguridad para poder ser certificados por la Alianza Wi-Fi y así comercializarse.

Como en la seguridad WPA, en WPA2 también se puede utilizar un servidor de autenticación de usuarios en su versión empresarial Enterprise o a nivel de hogares u oficinas pequeñas en su versión Personal.

Otra gran diferencias con WPA, es que WPA2 utiliza los algoritmos de encriptación de claves de red ***TKIP***, ***AES*** o combinarlos para asegurar una red impenetrable para personas no autorizadas. Se dice que es muy eficaz, tanto así que cumple los requerimientos de seguridad del gobierno de los estados Unidos.

2.10.4 Estándar AAA.

Anteriormente estudiando los tipos de seguridades en una red inalámbrica, se había mencionado que WPA y WPA2 en sus versiones Enterprise, trabaja con un servidor de autenticación llamado RADIUS, el cual es un protocolo dedicado a la autenticación de usuarios en las redes de información.

RADIUS trabaja sobre un estándar llamado AAA el cual se explicará primero para entender completamente el funcionamiento de éste protocolo.

Siempre que se habla de sistemas basados en la autenticación de usuarios se habla de RADIUS como la mejor alternativa para realizar esta función. RADIUS es un protocolo que existía antes que el estándar AAA y cumple con todas las normas del mismo, debido a que prácticamente los creadores de este protocolo son los mismos creadores de este estándar.

AAA son las siglas en inglés de Authentication Authorization y Acounting, que a nuestro idioma es traducido como Autenticación Autorización y Registro.

Este estándar fue creado por el ***IETF*** que es un Grupo de Trabajo en Ingeniería de Internet (Internet Engineering Task Force en inglés), encargado de desarrollar un estándar el cual desvincule a RADIUS como una única alternativa de autenticación, dando oportunidad de crear otros productos que mejoren este sistema y regulen su funcionamiento, facilitando el código fuente de RADIUS para que lo tomen como base en su desarrollo y mejoras. Este grupo hasta la actualidad sigue trabajando con el fin de desarrollar productos más seguros y confiables, pero RADIUS ha cumplido con todas las normas del estándar AAA desde el día de su creación hasta hoy, dejando atrás a otros desarrolladores de sistemas de autenticación como TACACS y DIAMENTER, siendo éste último el que actualmente sigue trabajando para superar el nivel de RADIUS sin tener mucho éxito ya que RADIUS se ha extendido alrededor del mundo.

La arquitectura que presenta este estándar es simplemente un modelo Cliente – Servidor, en donde un sistema de cliente solicita los servicios de un sistema servidor, pero el sistema servidor no solicita ningún servicio al sistema cliente, controlando así varios servicios de los que dispone el sistema cliente tales como: velocidad de internet, acceso a diferentes archivos, etc.

A continuación se dará una explicación clara de cada una de las tares que cumple cada “A” de este estándar.

2.10.4.1 Autenticación.

Esta es la base de los sistemas de autenticación siendo la “A” más importante, ya que de ésta dependen las demás. La autenticación es en donde se identifica el sistema de cliente que solicita los servicios del sistema servidor.

En general en los sistemas de autenticación al sistema cliente se le asigna un nombre de usuario y una contraseña, la cual está previamente almacenada en el sistema servidor.

Cuando el sistema cliente quiere acceder a la red, éste no es quien se comunica directamente con el sistema servidor a través de AAA, ya que primeramente se comunica con un dispositivo gestor de paquetes de datos (el cual debe soportar sistemas de autenticación), siendo éste el que traduce y encamina los paquetes hacia el sistemas servidor de autenticación, asegurando así que no exista un camino abierto entre estos dos sistemas garantizando una seguridad de alto nivel contra ataques, ya que para querer alguien infiltrarse en la red ilícitamente previamente deberían pertenecer al sistema.

También es importante mencionar que en esta fase de autenticación se produce un mensaje inicial de acceso a la red desde el dispositivo gestor de paquetes de datos al servidor de autenticación, llamando a esta acción solicitud de acceso.

2.10.4.2 Autorización.

Una vez culminada la fase de autenticación comienza la fase de autorización, en donde el sistema servidor autoriza los servicios a los que va a tener acceso el sistema cliente. Según el tipo de usuario y los atributos con el que este cuenta el servidor concederá detalles como: si el usuario está permitido formar parte de la red en ese momento, que dirección IP se le debe asignar, que velocidad de internet está disponible para este usuario o simplemente el servidor puede negarle el acceso a la red, a estos procesos se los conoce como aceptación de acceso o denegación de acceso respectivamente. También existe otro proceso adicional que se lo conoce como solicitud de información adicional para el acceso en donde el usuario debe alguna información adicional cuando no se lo reconoce por los parámetros mencionados anteriormente.

2.10.4.3 Registro.

Conocido también como Arqueo para mantener el estándar de las tres “aes” pero en nuestro medio es más conocido como registro. Una vez realizado el proceso de autorización se produce la fase de registro la cual es iniciada por el dispositivo gestor de paquetes de datos una vez que el usuario haya sido autorizado a los servicios de la red. En esta fase se producen datos estadísticos los cuales permiten tomar decisiones en cuanto al uso de los servicios de la red por parte de los usuarios, con el fin de denegar conexiones, cambiar la velocidad de internet para determinados usuarios, impedir descargas, etc. Estos datos permiten a un buen administrador de red planificar de mejor manera la estructura y políticas de la red, conociendo también la velocidad de crecimiento de esta y dando una mejor visión de las medidas que se deben tomar en el futuro según su crecimiento. También esta fase indica los usuarios que están en ese momento formando parte de la red y brinda una opción de desconexión la cual permite desvincular a un usuario de la red en cualquier momento.

2.10.5 Servidor de autenticación de usuarios RADIUS.

RADIUS son las siglas de Remote Autentication Dial-Up Server, que significa Servidor de Autenticación Remota para sistemas de Marcado Telefónico a Redes, lleva este nombre debido a sus orígenes donde su uso era únicamente en la telefonía, pero actualmente su funcionalidad es mucho más amplia, está basado en el estándar AAA anteriormente descrito.

Durante los años 90 el crecimiento de las redes de información se fue propagando mucho y el control de acceso a estas se complicaba más y más. Las empresas que trabajaban con varias redes debían tener acceso unas a otras, por lo que era complicado vigilar el acceso de personas no autorizadas a diferentes redes. Una empresa llamada

Merit en California, la cual trabaja con varias redes quería buscar una solución, solicitó a varios de sus proveedores de implementación de redes una solución a este problema. Uno de sus proveedores llamado Livingston Enterprise respondió a esta solicitud dando una clara descripción de su solución la cual posteriormente pasó a llamarse RADIUS. Su solución fue la que más llamo la atención a los empresarios de Merit, la misma que la fue mejorando incorporando nuevas funciones, de esta manera se creó el servidor de autenticación de usuarios RADIUS.

Debido a su gran éxito, varios fabricantes incorporaron RADIUS a sus productos de hardware y software teniendo mayor demanda en el mercado. Y así RADIUS se convirtió en un protocolo de gran importancia para el crecimiento de las redes de información.

2.10.5.1 Especificaciones de RADIUS.

Cumpliendo con el estándar AAA, RADIUS está basado en un modelo cliente-servidor, ya que escucha y espera las solicitudes de un dispositivo gestor de paquetes de datos respondiéndolas inmediatamente. En este modelo el cliente es el responsable del envío y de la correcta recepción de las solicitudes de acceso, y el servidor RADIUS es el responsable de verificar que los datos del usuario son correctos y de indicar cuáles son los servicios de red disponibles para este usuario.

RADIUS utiliza el protocolo UDP el cual proporciona una comunicación muy sencilla entre aplicaciones o computadoras al igual que el protocolo IP, este protocolo es utilizado porque mantiene una copia de seguridad del paquete de una solicitud sobre la capa de transporte del modelo OSI, lo cual permite recuperar dicho paquete si se pierde

durante las diferentes fases de transmisión. También trabaja sobre el puerto 1812 y 1813 para realizar la autenticación.

El protocolo de autenticación RADIUS fue desarrollado en sistemas basados en Unix, por lo tanto los primeros servidores RADIUS fueron compilados para UNIX y funciona de manera excelente en ***GNU***/Linux (se revisará más adelante). También se encuentran protocolos RADIUS que pueden ser utilizados sobre Windows.

En plataformas UNIX como ***GNU***/Linux se poden encontrar soluciones RADIUS ***OpenSource*** (Software desarrollado y distribuido de forma gratuita), las cuales cumplen la misma función que las aplicaciones de alto costo, el problema de las aplicaciones de código abierto para algunos administradores de red es la falta de comodidad en el manejo de estas herramientas ya que en su mayoría no cuentan con un modo gráfico de administración y se lo maneja solo en modo de texto. FreeRadius es una de los programas de código abierto más utilizado hoy en día para una implementación de sistemas de autenticación, pero se lo revisará en el capítulo 3.

2.10.5.2 Métodos de autenticación en RADIUS.

RADIUS cuenta con varios métodos de autenticación. Trabaja con varios módulos los cuales se encargan de realizar el cifrado, descifrado y empaquetado de la información que un usuario envía al servidor para que éste se encargue de verificar y permitir o no el acceso a la red. Cuando RADIUS recibe una solicitud de acceso, va pasando la información del usuario por cada unos de estos módulos hasta que alguno de ellos reconozca la información del usuario y valide su autenticación.

A continuación se detallará varios de estos módulos encargados de manipular la información de un usuario.

2.10.5.2.1 PAP.

El Protocolo de Autenticación por Contraseña, es el modo de autenticación más sencilla y por lo tanto la menos segura, se basa en la transmisión de un nombre se usuario y una contraseña almacenados en un archivo de texto simple.

2.10.5.2.2 CHAP.

El protocolo de desafío mutuo, fue creado como una actualización del método PAP para tratar de incrementar su seguridad. Consiste en el envió de una frase aleatoria, en donde el servidor envía esta frase cifrada al usuario el cual la descifra y la vuelve a enviar al servidor, éste la recibe nuevamente, la compara, y si es correcta permite al usuario formar parte de la red.

2.10.5.2.3 MS-CHAPv1.

Esta versión de protocolo CHAP creada para sistemas operativos Microsoft, cumple la misma, cabe recalcar que Windows Vista no soporta este tipo de autenticación.

2.10.5.2.4 MS-CHAPv2.

Es la versión mejorada del protocolo anterior que tiene soporte en todos los sistemas operativo Windows incluido Vista, Permite soporte para cambiar contraseñas de usuarios.

2.10.5.2.5 Unix.

Se utiliza simplemente los nombres de usuarios y contraseñas existentes en sistemas operativos Unix/Linux para la autenticación.

2.10.5.2.6 HTTP Diagest.

Es un protocolo de autenticación para clientes de servidores web (detallado más adelante) con autenticación RADIUS.

2.10.5.2.7 Métodos EAP.

Es un protocolo encargado del transportar, encapsular y asegurar la autenticación en una red, incluye todos las características de los protocolos descritos anteriormente. Existen más de cuarenta métodos de autenticación sobre EAP convirtiéndolo en el más seguro y se lo puede utilizar a cualquier nivel de seguridad.

En este modelo de autenticación el dispositivo gestor de paquetes de datos solamente inicia el proceso de autenticación reencaminando los datos hacia el servidor RADIUS

sin tener que ser el encargado de la autenticación, de esta manera este dispositivo solo cumple con la función de encapsular la información y el protocolo RADIUS se encarga de transportar la información de forma transparente sin dar opción a que los datos sean atacados.

Existen varios tipos de modelos EAP, se describirán a continuación:

2.10.5.2.7.1 EAP-MD5.

Es el primer método de autenticación de éste tipo, por lo tanto el más inseguro. Como su nombre lo indica utiliza el algoritmo ***MD5*** (algoritmo de reducción criptográfico de 128 bits) para cifrar una contraseña, el cual es un método de seguridad baja de cifrado.

2.10.5.2.7.2 EAP-TLS.

En este método de autenticación se utiliza un método particular, está basado en certificados TLS o SSL (más adelande se explicará con detalle), en donde el usuario envía la petición de conexión al servidor, el servidor recibe la petición del usuario y este envía una serie de paquetes al usuario apoyados con un sistema de certificados de confianza, el usuario recibe los paquetes enviados por el servidor el cual aceptará o no éste certificado, si el usuario lo acepta, el mismo paquete se lo reenvía al servidor al igual que el servidor lo hizo apoyado en un mismo de sistema de certificado de confianza, el cual el servidor comprobará si fue el mismo paquete el enviado anteriormente y posteriormente aceptará o no la entrada a la red al usuario según la verificación de la información. El paquete de datos que se envían es la información del usuario que puede estar cifrado con cualquiera de los métodos antes mencionados, manteniendo así un nivel de alta seguridad en el transporte de datos. Es importante

mencionar que éste método de autenticación tiene un alto nivel de complejidad al momento de implementarlo.

2.10.5.2.7.1.3 EAP-TTLS.

Es un método más sencillo de implementar que el anterior pero mantiene el mismo de nivel de seguridad, la diferencia con el anterior es que el usuario no maneja un sistema de certificados de confianza, el servidor será el único que cuente con este sistema, dificultando así un ataque en la red ya que el usuario sabrá que el certificado que va a aceptar es de confianza.

2.10.5.2.7.4 EAP-PEAP.

Es un método muy similar al anterior, fue desarrollado por Microsoft, Cisco y RSA. Es evidente que fue creado para que los productos de estos fabricantes sean compatibles con este método de autenticación. Maneja el mismo proceso que EAP-TTLS, este modelo es recomendado para utilizarlo en las redes inalámbricas y está soportado por la mayoría de fabricantes que cuentan con tecnología inalámbrica.

Es importante resaltar que si un intruso logra infiltrarse en una red que utiliza los métodos de autenticación EAP, lo cual no es imposible pero necesita tiempo y dedicación extrema, solo logrará conseguir un nombre de usuario y contraseña, la información de los demás usuarios se mantendrá intacta ya que deberá volver a realizar el mismo método que utilizó para conseguir la información de otro usuario, esto no tendrá mayor relevancia dentro de la red, porque simplemente se procederá o eliminar la cuanta violada.

2.10.5.2.8 Autenticación contra archivo de usuarios.

Una de las maneras más clásicas de autenticación es la autenticación de usuario en un simple archivo de texto, en donde se almacena la información de los usuarios, al momento en que un usuario haga una petición de conexión al servidor, este verificará la existencia del usuario en este archivo. Este método es suficiente para implementaciones pequeñas en donde el número de usuario con el que va a contar la red es bajo, para implementaciones más grandes se o deberá realiza de una forma más segura.

2.10.5.2.9 Autenticación contra el sistemas operativo.

Este método también se lo utiliza para gestionar usuarios en una red pequeña, los usuarios que podrán tener acceso a la red serán los mismos que se crean en las cuentas de los sistemas operativos.

2.10.5.2.10 Autenticación contra bases de datos.

Aquí los usuarios y sus atributos se almacenarán en una base de datos, normalmente de tipo SQL, como Oracle, Microsoft SQL Server, MySQL, PostGreSQL, etc., facilitando así la administración de los usuarios si se trata de redes en las que se manejan varias cuentas y teniendo mayor seguridad ya que los datos se los puede respaldar para prevenir una pérdida de datos por cualquier circunstancia. Si se maneja un número grande se usuarios, el servidor de base de datos podría ser implementado por separado sin tener que encontrarse en el mismo servidor RADIUS, pero si se administra un número de usuarios considerable podré encontrarse en el mismo.

2.10.5.2.11 Autenticación contra servicios de directorio.

Es más utilizado en implementaciones de redes de empresas de mediano o gran tamaño, en donde se pretende autenticar a sus empleados. No es apropiado para redes púbicas como lo es en los casos anteriores. Para realizar la autenticación por este método se utiliza Active Directory, LDAP, eDirectory, etc. Realizando la consulta para autenticación a estos sistemas.

Se puede notar que RADIUS es una herramienta poderosa para implementar redes seguras con sistemas basados en la autenticación, se lo puede utilizar tanto en redes cableadas como en redes inalámbricas o una combinación de las dos. Uno de los usos más comunes que se le da a RADIUS dentro de las redes inalámbricas en un HOTSPOT, ya que los usuarios que deseen acceder a los servicios de este, deben primeramente introducir cierta información (generalmente un nombre de usuario y una contraseña) para formar parte de la red y aprovechar sus servicios.

2.10.5.3 Protocolo SSL y TLS

SSL y TLS son protocolos que protegen la información cuando es transportada de un punto hacia otro en una red, actúa sobre el medio de transmisión de los datos cifrando la información. Estos dos protocolos son casi idénticos ya que manejan el mismo método de cifrado de los datos. SSL fue desarrollado por Netscape (navegador de Internet) y utiliza el lenguaje HTTP, garantizando el proceso de autenticación, cifrado y la integridad de la información. Si se utiliza el protocolo SSL sobre HTTP significa que se utilizando un protocolo ***HTTPS***. Este protocolo funciona sobre el nivel de aplicación del modelo OSI, el cifrado de los datos se basa en la emisión de certificados de confianza por parte de una autoridad certificadora.

TLS es un protocolo de uso público, actualmente se encuentra en su versión 1.1 y no está totalmente definido, su funcionamiento es el mismo que el del protocolo SSL, pero su aplicación se basa en el nivel de transporte del modelo OSI.

2.10.5.4 Certificado de confianza y autoridad certificadora.

Un certificado de confianza o certificado digital es un documento que la autoridad certificadora emite a los diferentes usuarios que se disponen a formar parte de la red, en este documento se encuentra la información del usuario la cual es transportada al usuario en forma cifrada.

La autoridad certificadora es la que se encarga de emitir los certificados de confianza a los usuarios luego de haber comprobado su existencia en sus registros, esta entidad debe ser de un alto nivel de confianza para que los usuarios puedan aceptar sus certificados. Existen varias opciones de software para cumplir la función de autoridad certificadora, como es el caso de OpenSSL (Detallado en el capítulo 3).

2.10.6 Hospot.

Un HOTSPOT es una infraestructura de red inalámbrica, en donde uno o varios puntos de acceso o routers inalámbricos conectados entre sí, ofrecen los servicios de una red (generalmente Internet). Un HOTSPOT se encuentran en lugares públicos, como aeropuertos, bibliotecas, cafeterías, hoteles, etc. Este servicio puede brindarse de manera gratuita o pagando una suma de dinero que depende del proveedor del servicio.

Se había mencionado que el protocolo de autenticación RADIUS era también utilizado dentro de un HOTSPOT. Habitualmente los usuarios que deseen tener acceso a los servicios de la red, primeramente deben ingresar cierta información, usualmente un nombre de usuario y una contraseña, la cual es proporcionada por el proveedor del servicio, en el momento en el que usuario ya cuenta con sus credenciales puede utilizar los servicios de la red, siendo el protocolo RADIUS el encargado de verificar si la información que el usuario ha ingresado es legítima, permitiendo o impidiendo al usuario el acceso a la red.

En la mayoría de implementaciones de éste tipo, se trabaja con un interfaz en donde el usuario ingresa su información para acceder a la red y opcionalmente el proveedor puede publicar los términos de uso de la red, describir sus servicios, etc.

2.10.7 Portal cautivo.

El interfaz que se mencionaba anteriormente es llamado portal cautivo (Captive Portal en inglés). Un portal cautivo es una página web por la que obligadamente los usuarios deben pasar antes de utilizar los servicios de una red. El usuario no podrá evitar el paso por esta página ya que aquí es en donde debe ingresar sus credenciales, previamente obtenidas con el proveedor, caso contrario no podrá hacer uso de los servicios de la red. Adicionalmente el proveedor podrá hacer del paso de los usuario por ésta página para presentar publicidad si así lo desea.

Esta página web puede estar implementada dentro de un punto de acceso, o dentro de un servidor. La página web debe estar implementada dentro de un servidor web y generalmente está en escrito en lenguaje PHP (lenguaje de programación para páginas web). Existen varias opciones en cuanto software que ofrece este servicio tanto gratuito

como pagado. El portal cautivo trabaja en junto con el protocolo RADIUS para autenticar usuarios, aumentando así el nivel de seguridad en una red inalámbrica.

2.10.8 Servidor web.

Un servidor web es el lugar en donde se alojan las páginas web, para entender mejor este concepto se va a tomar el siguiente ejemplo:

Cuando una persona navega a través del internet, ésta en su navegador ingresa la dirección de cualquier página, la página web es buscada en línea hasta ser encontrada dentro de su servidor web, el cual envía la página solicitada y mostrará la información de la página en el navegador de la persona que solicitó la página.

Un servidor web también se puede utilizar dentro de una red local en donde sea necesario trabajar sobre cualquier página, este servidor se instalará en la computadora principal de la red y la página se alojará dentro de esta, así los demás usuarios que formen parte de la red local podrán tener acceso a esta página digitando la dirección IP de la computadora principal y seguidamente el nombre de la página.

Todos los servicios anteriormente descritos son utilizados para lograr el objetivo general de la investigación, pero lo que no se ha mencionada es que los estos servicios trabajan dentro de un sistema operativo, pudiendo ser Windows o Linux, éste último es que se ha utilizado para la implementación, a continuación se lo describirá.

2.11 GNU/Linux.

Conocido en nuestro medio simplemente como Linux, es un sistema operativo gratuito el cual simplemente se lo puede descargar de Internet e iniciar su instalación.

Nació de un proyecto universitario realizado por Linus Torvalds en la década de los 90, el objetivo de este proyecto fue crear un sistema operativo totalmente gratuito y de código abierto para que las personas interesadas de todo el mundo puedan cooperar con el mejoramiento del sistema. Se expandió rápidamente por su funcionamiento eficaz y con el tiempo su desempeño fue mejorando hasta llegar a un nivel muy alto, compitiendo con los demás sistemas operativos como Windows.

La principal característica de este sistema operativo es el alto nivel de seguridad que el usuario puede experimentar. Cuenta con versiones de interfaz gráfica y en modo texto para utilizarlo como servidor dentro de una red de información, aunque Linux en su modo gráfico también se lo puede utilizar como servidor sin dificultad. Otra de las grandes ventajas de este sistema operativo es que los requerimientos de hardware son bajos, pudiendo instalarlo en una computadora de bajos recursos de hardware sin tener que contar con una computadora poderosa.

En varias de sus distribuciones cuenta con dos opciones de entorno de escritorio las cuales son ***GNOME*** y ***KDE***, siendo la primera un entorno de fácil manejo para usuarios ordinarios y la segunda es utilizada para usuarios con conocimientos más técnicos.

Además cuenta con varias distribuciones, las cuales fueron creadas para satisfacer diferentes necesidades que los usuarios demandaban, a continuación se detallará brevemente algunas de sus distribuciones.

2.11.1 Distribuciones de Linux.

2.11.1.1 Redhat Enterprise.

Esta es una distribución que tiene muy buena calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye. Es necesario el pago de una licencia de soporte. Enfocada a empresas.

2.11.1.2 Fedora.

Esta es una distribución patrocinada por RedHat y soportada por la comunidad. Fácil de instalar y de buena calidad.

2.11.1.3 Debian.

Otra distribución con muy buena calidad. El proceso de instalación es un poco más complicado, pero sin mayores problemas. Cuenta con gran estabilidad.

2.11.1.4 OpenSuSE.

Otra de las grandes, fácil de instalar, es una versión libre de la distribución comercial SuSE.

2.11.1.5 SuSE Iinux Enterprise.

De muy buena calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye, Novell. Es necesario el pago de una licencia de soporte. Está enfocada a empresas.

2.11.1.6 Slackware.

Esta distribución es una de las primeras que existió. No se actualizó por una largo tiempo y debido a esto desapareció.

2.11.1.7 Kubuntu.

Distribución basada en Ubuntu, cuenta con una gran facilidad de uso. La gran diferencia con Ubuntu es que su entorno de escritorio es ***KDE***.

2.11.1.8 Mandriva.

Esta distribución fue creada en 1998 con el objetivo de acercar el uso de Linux a todos los usuarios, en un principio se llamo Mandrake Linux, y su principal característica es la facilidad de uso para todos los usuarios.

2.11.1.9 CentOS.

CentOS (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise, creado por colaboradores de todo el mundo a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux es un sistema operativo de software libre y código abierto. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser descargado del Internet y usado por todo público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de las fuentes de Red Hat.

CentOS usa ***yum*** para bajar e instalar las actualizaciones, herramienta también utilizada por Fedora.

2.11.1.10 Ubuntu.

Es el sistema operativo que se utilizó para la implementación del proyecto. Es una distribución Linux basada en Debian ***GNU***/Linux, su nombre proviene de la ideología sudafricana Ubuntu que significa humanidad hacia otros.

Integra un sistema operativo actualizado y estable para el usuario con pocos conocimientos en esta distribución o en Linux en general, posee un fuerte enfoque en la facilidad de uso y de instalación del sistema. Al igual que otras distribuciones se compone de múltiples paquetes de software normalmente distribuidos bajo una licencia libre o de código abierto.

Ubuntu está patrocinado por Canonical Ltd., una compañía británica propiedad del empresario sudafricano Mark Shuttleworth, que en vez de vender la distribución con fines lucrativos, se financia por medio de servicios vinculados al sistema operativo y vendiendo soporte técnico. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar el talento de los desarrolladores de la comunidad en mejorar los componentes de su sistema operativo.

Cada seis meses se publica una nueva versión de Ubuntu la cual recibe soporte por parte de Canonical, durante dieciocho meses, por medio de actualizaciones de seguridad, parches para y actualizaciones menores de programas.

Ubuntu y sus derivadas oficiales fueron seleccionadas por los lectores de desktoplinux.com como una de las distribuciones más populares, llegando a alcanzar aproximadamente el 30% de las instalaciones de Linux en computadoras de escritorio tanto en el 2006 como en el 2007.

La versión actual de Ubuntu, 9.10 ("Karmic Koala", nombre clave), se liberó el 29 de octubre de 2009 y la próxima versión, 10.04 (nombre en código: Lucid Lynx), se espera en abril de 2010.

CAPÍTULO III

Para confirmar la necesidad de implementar el HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad y la Provincia, se realizaron encuestas a los usuarios que concurren a utilizar el servicio de Internet, en el Anexo 1 se encuentra el modelo de las encuestas realizadas y en el Anexo 2 la tabulación de éstas, obteniendo una conclusión del cada pregunta.

Revisada la teoría del capítulo anterior, la explicación de la implementación del servidor RADIUS será mucho más sencilla y entendible. Para esto se utilizó una serie de hardware y software los cuales ayudaron a cumplir el objetivo general del proyecto.

El hardware debe cumplir con los siguientes requerimientos mínimos:

- **Servidor:** El servidor debe cumplir con los requerimientos detallados en el punto 3.3.1.
- **Puntos de acceso:** Soporte de estándar IEEE 802.11 g y soporte de seguridad WPA2.
- **Switch:** Mínimo 4 puertos Ethernet, control de flujo de datos y velocidad de transferencia de datos de 10/100 ***Mbps***.

3.1 Hardware.

El hardware utilizado para la implementación del HOTSPOT con servidor RADIUS, fue adquirido por la institución bajo recomendación del ingeniero Luis Bravo, encargado de la administración de la Biblioteca Virtual. Los equipos fueron elegidos por su costo conveniente y sus características de alta calidad, las cuales satisfacen los requerimientos para la implementación del proyecto, a continuación se detallarán las características y especificaciones de estos equipos.

3.1.1 Servidor.

El servidor que se utilizó es un HP ProLiant serie DL320 G5. Se lo detallará a continuación:

“El servidor HP ProLiant DL320 G5 es un servidor empresarial optimizado para bastidor con un precio bajo. El servidor 1 procesador es altamente manejable y resulta ideal para infraestructuras de TI de una sola aplicación, para la web o para aplicaciones de red. La consola remota virtual que se ofrece funciones de administración a nivel empresarial. Es compatible con 1 o 2 unidades Serial ATA de bajo costo, con la posibilidad de actualizarlas opcionalmente a unidades de disco duro SAS de conexión en caliente y de gran fiabilidad. Además, obtiene una solución de bajo costo, como plataforma de un solo procesador y trae la nueva serie de procesadores Intel® Xeon® 3000.

Figura 3.1: Servidor HP ProLiant serie DL320 G5

3.1.1.1 Características.

- **Plataforma de alojamiento masivo en bastidor de bajo costo.**

El chasis para bastidor optimizado minimiza el espacio necesario en un centro de datos, mientras que la arquitectura de un único procesador y el soporte para unidades de disco duro Serial ATA de 3,5" se traduce en un ahorro para el presupuesto.

- **Gestión y supervisión a nivel empresarial.**

El ProLiant DL320 G5, gracias a sus potentes y flexibles herramientas de implantación, supervisión y administración, se convierte en la solución ideal para cualquier entorno.

- **Opciones de almacenamiento flexibles.**

Las tres configuraciones diferentes para las unidades de disco duro internas, además de un gran número de opciones para las tarjetas adaptadoras HBA y RAID, ofrecen una gran variedad de opciones para el almacenamiento. ” [1]

Figura 3.1: Servidor HP ProLiant serie DL320 G5
http://h10010.www1.hp.com/wwpc/es/es/sm/WF06a/15351-15351-3328412-241475-241475-3201178.html
Referencia 1: HP Latinoamérica: Servidor HP ProLiant serie DL320 G5
http://h10010.www1.hp.com/wwpc/es/es/sm/WF06a/15351-15351-3328412-241475-241475-3201178.html

3.1.1.2 Especificaciones técnicas

Especificaciones técnicas	
Número de procesadores	1 procesador Intel® Xeon® 3000
Chipset	Chipset Intel® 3000
Núcleo de procesador disponible	Dual
Ranuras de memoria	4 ranuras Dimm
Memoria	2 GB PC2-5300 (667***MHz***) sin búfer ECC DDR2 SDRAM; Intercalado opcional (activado cuando se instalan DIMM en parejas)
Ranuras de expansión	Dos ranuras: (1) ranura PCI Express x8 (conector x8) de longitud completa - se puede reemplazar por una ranura PCI-X de 64 bits/133***MHz*** de longitud completa; (1) ranura PCI Express x1 de perfil bajo y longitud media (conector x8)
Controlador de red	Adaptador de servidor integrado Gigabit NC324i PCI Express de doble puerto
Tipo de fuente de alimentación	Fuente de alimentación PFC de 420 W con detección automática, cumple con la Marca CE
Controlador de almacenamiento	Controladora de host Intel 82801GR Serial ATA integrada con compatibilidad RAID 0/1. La controladora incorporada de almacenamiento SATA para DL320 no es compatible con la función de conexión en caliente ni con los LED de unidad Para usar la función de conexión en caliente, se necesita un controlador HBA o Smart Array.
Software de gestión	Recuperación automática del servidor (ASR); iLO 2 Advanced Pack (opcional); HP Systems Insight Manager; Registro de gestión integrado; Seguimiento de parámetros de unidades (con controladores Smart Array); Reparación dinámica de sectores (con controladores Smart Array); Garantía de fallo inminente (cubre los procesadores, unidades de disco duro SAS y la memoria); Consola serie para BIOS; Botón/LED de ID de unidad (UID) frontal y posterior
Tipo de unidad óptica	DVD.

Tabla 5: Especificaciones técnicas Servidor HP ProLiant serie DL320 G5

3.1.2 Punto de acceso

El punto de acceso es también uno de los dispositivos que se utilizó en la implementación del proyecto, necesitando tres puntos de acceso Linksys WAP54G versión 1.1, a continuación se presentarán sus características las cuales demuestran la razón por la que se escogió este interesante dispositivo.

Figura 3.2: **Punto de acceso Linksys WAP54G**

3.1.2.1 Características

"Es ideal para agregar funciones inalámbricas a redes con cables y ofrece comodidad que supone eliminar la necesidad de cables.

- **Comodidad inalámbrica**

Ya disponiendo de una red, sólo se la mejora mediante un punto de acceso Wireless-G de hasta 54 Mbps. Se puede ampliar una red añadiéndola más ordenadores, impresoras y otros dispositivos inalámbricos. Ahora es mucho más fácil y no se tendrá que utilizar ni un solo cable. También es compatible con dispositivos Wireless-B. Una conexión de confianza que permite desplazar los ordenadores portátiles o configurar otros dispositivos desde cualquier parte del hogar u oficina.

Figura 3.2: Punto de acceso Linksys WAP54G
http://www.linksysbycisco.com/LATAM/es/products/WAP54G

- **Fácil configuración**

Sólo hay que pulsar un botón para configurarlo, por lo que añadir dispositivos a una nueva red inalámbrica es muy sencillo. Pulsando el botón del punto de acceso y de los demás dispositivos inalámbricos con SecureEasySetup se puede crear automáticamente la conexión inalámbrica. Configurando los parámetros de seguridad y el dispositivo mediante la utilidad de configuración basada en el explorador resulta muy sencillo.

- **Seguridad completa**

Para trabajar con total confianza. La encriptación de seguridad industrial ayuda a mantener protegidas y en privado las comunicaciones. El filtro de acceso permite controlar quién accede a la red inalámbrica. ” [2]

3.1.2.2 Especificaciones técnicas

Especificaciones técnicas	
Modelo	WAP54G
Estándares	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Puertos/botones	Un puerto cruzado automático (MDI/MDI-X) 10/100, puerto de alimentación, botones de reinicio y SES
Tipo de cables	Categoría 5 (con conectores RJ-45)
Luces	Alimentación, Actividad, Enlace
Potencia de transmisión	802.11g: Habitualmente 13,5 +/- 2 ***dBm*** a temperatura normal, 802.11b: Habitualmente 16,5 +/- 2 ***dBm*** a un intervalo de temperatura normal
Funciones de seguridad	WPA, Linksys Wireless Guard (disponible sólo en EE. UU. y Canadá), encriptación WEP, filtrado de direcciones MAC, activación/desactivación de difusión de SSID
Bits de clave WEP	64/128 bits.

Tabla 6: Especificaciones técnicas Punto de acceso Linksys WAP54G

Referencia 2: Linksys Latinoamérica: Punto de acceso Linksys WAP54G
http://www.linksysbycisco.com/LATAM/es/products/WAP54G

3.1.3 Switch

El switch que se utilizó para la implementación del HOTSPOT es un D-Link DES-1008D, ya que su precio es muy cómodo y cumple con los requerimientos para el desarrollo del proyecto, a continuación se detallan las especificaciones técnicas de este dispositivo.

Figura 3.3: **Switch D-Link DES-1008D**

3.1.3.1 Características

"El switch DES-1008D es un switch de alto rendimiento y gran versatilidad. Está diseñado para reforzar el rendimiento en una pequeña empresa, otorgando flexibilidad y manejo a 10/100Mbps. Está provisto de 8 puertos, lo que permite que grupos de trabajo aumenten el rendimiento en la red.

- **8 Puertos 10/100Mbps**

Este switch provee de 8 puertos. Los puertos tienen la capacidad de negociar las velocidades de red, como también el modo de operación en la misma.

Figura 3.3: Switch D-Link DES-1008D
http://www.dlinkla.com/home/productos/producto.jsp?idp=70

- **Control de Flujo**

La arquitectura de operación de éste switch, permite la transferencia de datos en forma directa entre los distintos puntos, eliminando en el tráfico de la red el envío de paquetes incompletos, fragmentados o con errores, salvaguardando de esta forma la integridad de los datos.” [3]

3.1.3.2 Especificaciones técnicas

Especificaciones técnicas	
Puertos	8 (10/100Base-TX)
Estándares	IEEE 802.3 10Base-T Ethernet Repeater, IEEE 802u 100Base-TX class II Fast Ethernet repeater y ANSI/IEEE Std 802.3 Nway auto-negotiation
Conectores	RJ-45
Transferencia	10/100 ***Mbps*** Full Duplex, autodetect
Topología	Estrella
LEDs indicadores	Por puerta: link/activity, velocidad 100***Mbps***, Full-duplex collision. Por switch : Power
Fuente de poder	Externa.
Consumo	8 Watts Máximo Modelo Rev. C2, 12 Watts Máximo Modelo Rev. D1.

Tabla 7: Especificaciones técnicas switch D-Link DES-1008D

El hardware listado anteriormente fue el utilizado para la implementación del proyecto, a continuación se listará el software que se utilizó con sus características y descripción.

Referencia 3: D-Link Latinoamérica: Figura 3.3: Switch D-Link DES-1008D
http://www.dlinkla.com/home/productos/producto.jsp?idp=70

3.2 Software

El software utilizado para la implementación fue elegido por el autor del proyecto. Cumpliendo con una de las políticas de la institución, la cual indica que todo el software con el que la Biblioteca Virtual trabaje debe ser gratuito. Se eligió las herramientas más confiables y estables que existen en la actualidad, a continuación se detallará el software que se utilizó, indicando sus características para demostrar la razón por la que fue elegida cada herramienta.

3.2.1 Freeradius

Freeradius fue creado en 1999, es un proyecto de software libre (gratuito) basado en la autenticación, sus creadores son Alan DeKoK y Miquel van Smoorenburg, los cuales comparten un blog personal en donde los usuarios pueden realizar preguntas y despejar dudas a los usuarios de este famoso servidor, colaborando así con el mejoramiento de este. Existen varias versiones de este servidor, actualmente la última es la 2.1.8.

Freeradius es uno de los servidores de autenticación más utilizado en el mundo, ya que cumple con el estándar AAA, varias son las características de este servidor y una de las más grandes es que es gratuito, por lo que solamente se lo puede descargar desde la página www.freeradius.org. A continuación se detallarán las características más importantes que Freeradius ofrece.

3.2.1.1 Características

Estas son las características de Freeradius.

- Se puede instalar sobre cualquier plataforma Linux, tanto en versiones de 32 y 64 Bit.

- Es compatible con casi cualquier sistema operativo, ya sea Windows, Linux, MacOS, y varios sistemas operativos móviles.

- Soporta una gran variedad de bases de datos y servidores de directorios como Oracle, MySQL, MS SQL, Active Directory, LDAP, etc.

- Trabaja con varias opciones de autenticación como PAP, CHAP, EAP, etc.

- Es compatible con la mayor parte de lenguajes de programación como ***Perl***, ***Phyton***, Java y PHP.

- Es compatible con la mayoría de portales cautivos.

- Es totalmente compatible para trabajar con autoridades certificadoras.

Freeradius en muchos casos se utiliza en implementaciones de redes inalámbricas como en HOTSPOT, para poder controlar a los usuarios que se dispongan a utilizar los servicios de red y que previamente hayan adquirido un nombre de usuario y una contraseña, que es lo que generalmente se le asigna. En este tipo de infraestructura el modelo de autenticación utilizado es PAP o CHAP, ya que es suficiente seguridad debido a la limitación de tiempo que el usuario tiene para acceder a los servicios de la red.

3.2.2 Chillispot

Es el portal cautivo más popular en implementaciones de un HOTSPOT, ya que es gratuito y se lo puede descargar de la página www.chillispot.info/download.html. Cumple con todas las funciones que un portal cautivo debe cumplir, o sea brindar un interfaz a los usuarios de una red en donde puedan ingresar sus credenciales para utilizar

los servicio de de la misma. Es totalmente compatible con el estándar AAA y por lo tanto con freeradius. Así trabajando en conjunto se encargan de asegurar la autenticación, autorización y el registro de los usuarios.

3.2.2.1 Características

- Una de las características con las que cuenta Chillispot es que permite la autenticación a través de un Servidor RADIUS.

- Es totalmente compatible con implementaciones de redes inalámbricas.

- Cuenta con un servidor DHCP, para asignar direcciones IP a los usuarios autorizados a formar parte de una red.

- Permite el control de velocidad de Internet (***Ancho de banda***), asignado a cada usuario de la red.

- Trabaja tanto en redes cableadas como inalámbricas.

Como se ha notado Chillispot es una herramienta sencilla y poderosa, siendo la mejor opción en que a portales cautivos gratuitos se refiere, pero cabe recalcar que Chillispot se logra implementar siempre y cuando se cuente con un servidor web, el cual lo explicaremos a continuación.

3.2.3 Servidor web Apache.

Este servidor web es el más utilizado alrededor del mundo, fue creado en 1995. Está por encima de cualquier servidor por su potencia, ligereza, robustez y seguridad y es

totalmente gratuito, se lo puede descarar de la página www.apache.org., actualmente su última versión es la 2.

3.2.3.1 Características.

- Su principal característica y por la que le hace el servidor web más utilizado es que es multiplataforma, es decir funciona sobre Windows, Linux, MacOS, etc.
- Trabaja sobre el protocolo HTTP, permitiendo así
- Soporte para los lenguajes ***Perl***, python, tcl y PHP.
- Módulos de autenticación: mod_access, mod_auth y mod_digest.
- Soporte para SSL y TLS.

Apache es principalmente usado para alojar páginas web estáticas y dinámicas ya sea en una red local en Internet. Es el servidor web del popular, junto con MySQL y los lenguajes de programación PHP/***Perl***/Python, forman una herramienta poderosa para realizar aplicaciones web de cualquier tipo.

3.2.4 MySQL.

Es un servidor de bases de datos muy poderoso, tan eficiente como las versiones empresariales de Oracle o Microsoft SQL Server. También cuenta con versiones empresariales pero se lo utiliza más en su versión gratuita dentro de nuestro medio, para aplicaciones de pequeño o mediano tamaño, la cual es suficiente para cumplir con las

expectativas de los desarrolladores. También lo convierte en unos de los servidores de bases de datos más utilizado por contar con un manejo sencillo y potencia. Se lo puede descargar de la página www.mysql.com, actualmente se encuentra en la versión 5.1.44.

3.2.4.1 Características.

- La característica que hace de MySQL una herramienta poderosa es que trabaja sobre varios sistemas operativos, o sea es multiplataforma, funciona sobre: Windows, Linux, MacOs, FreeBSD, Solaris, etc. Siendo totalmente compatible y funcionando a la perfección sobre estos.

- Usa todos los procesadores disponibles en una computadora, a diferencia de otros servidores de bases de datos como Oracle Express.

- Trabaja con varias tablas de distintas bases de datos.

- Su nivel de seguridad es muy alto, ya que todas las contraseñas se almacenan cifradas.

- Puede almacenar 60.000 tablas y cerca de 5.000.000.000.000 de registros.

- Los clientes de bases de datos se pueden conectar con el servidor MySQL a través del protocolo TCP/IP desde cualquier sistema operativo.

3.2.5 PHP

Sus siglas significan Hypertext Pre-processor, es un lenguaje de programación gratuito, actualmente se encuentra en la versión 5.3.2 lanzada el 4 de marzo del 2010. Fue creado en 1994 por Rasmus Lerdorf. Se lo puede descargar de la página www.php.net.

PHP es un lenguaje diseñado especialmente para desarrollo de páginas web dinámicas, es capaz de trabajar junto con el código HTML, se ejecuta dentro un servidor web. En la actualidad es utilizado por más 20 millones de páginas web y en un millón de servidores. Uno de los sitios más conocidos y visitados en el mundo; la famosa enciclopedia virtual "Wikipedia", utiliza este lenguaje de programación para publicar su información en la web. Cabe recalcar que el portal cautivo Chillispot mencionado anteriormente también está escrito en este lenguaje de programación.

3.2.5.1 Características.

- Es un lenguaje multiplataforma, por lo que trabaja sobre varios sistemas operativos como Windows, Linux, MacOS, etc., siendo totalmente compatible.

- Está orientado al desarrollo de aplicaciones web dinámicas capaz de manejar información almacenada en una Base de Datos.

- Compatible con varios servidores de bases de datos como MySQL, Oracle, Microsoft SQL Server, etc.

- Trabaja con una serie de módulos los cuales lo convierten en una herramienta de programación poderosa.

- Cuenta con extensa documentación la cual se la puede obtener desde su sitio oficial, haciéndolo así de fácil manejo y comprensión.

- Soporta módulos programación orientada a objetos.

- No requiere definición de tipos de variables haciéndolo más sencillo en su programación.

- Ofrece una solución simple y universal para la programación de páginas web dinámicas.
- Existe gran comunidad de desarrolladores en PHP, permitiendo que los fallos de funcionamiento se encuentren y reparen rápidamente.

- El código se mantiene actualizado, ofreciendo mejoras en el lenguaje para ampliar sus capacidades.

3.2.6 EasyHotspot.

EasyHotspot es una solución muy efectiva al momento de implementar un HOTSPOT, ya que cuenta con varias características y herramientas muy útiles, las cuales satisfacen todos los requerimientos en el desarrollo de este proyecto.

Es un paquete que contiene todo el software anteriormente mencionado, dentro de la muy famosa y utilizada distribución de Linux; Ubuntu, en su versión 9.04. Al ser construido bajo este sistema operativo indica que es totalmente gratuito, por lo que se lo puede descargar de la página www.easyhotspot.sourceforge.net/. A continuación se presenta un esquema de este interesante sistema operativo.

Figura 3.4: EasyHotspot

Como puede notarse en el gráfico, EasyHotspot está instalado dentro de un servidor, el cual está conectado a Internet y también a un switch en donde se conectan varias computadoras y un punto de acceso el cual permite conectarse a más dispositivos a la red de manera inalámbrica, siendo compatible con varios sistemas operativos. Esto demuestra que es una herramienta sencilla y poderosa.

3.2.6.1 Características.

- Construido bajo Linux, en su distribución Ubuntu 9.04.
- Utiliza Freeradius como servidor de autenticación de usuarios.
- El interfaz para la autenticación de usuarios es Chillispot.
- Trabaja con Apache como servidor web, en donde aloja la página web de registro de usuarios, o sea el portal cautivo.

Figura 3.4: EasyHotspot
http://easyhotspot.inov.asia/index.php/documentation

- Como servidor de bases de datos para almacenar los usuarios y sus credenciales en MySQL.

- Su instalación es sencilla, permitiendo que cualquier persona sin conocimientos avanzados de redes lo pueda utilizar.

- Permite la participación de los usuarios en el mejoramiento de esta herramienta, compartiendo un blog, en el cual se puede notificar acerca de errores y requerimientos, los cuales son tomados en cuenta por sus creadores.

- Cuenta con un interfaz web, en donde se administra la creación de usuarios, el tráfico de la red y mucha más información necesaria para que un administrador pueda verificar el buen funcionamiento de la red.

A continuación se detallará el procedimiento que se siguió para implementación del HOTSPOT con servidor RADIUS, indicando paso a paso la instalación de EasyHotspot.

3.3 Instalación de EasyHotspot

Luego de haber descrito las características del software y hardware utilizados para la implementación del HOTSPOT con servidor RADIUS, se explicará la instalación del sistema operativo base, el cual controla y hace posible el funcionamiento del sistema.

3.3.1 Requisitos mínimos de hardware.

El sistema operativo exige los siguientes requerimientos:

- Una computadora con procesador Pentium 3 o equivalente.

- Mínimo 512 MB de memoria RAM.
- Mínimo 5 GB disponibles en el disco duro.
- 2 interfaces o tarjetas de red Ethernet.

Como se puede notar los requerimientos de hardware son mínimos, pudiendo instalar este sistema operativo prácticamente en cualquier computador.

3.3.2 Descarga de EasyHotspot.

Cumpliendo con los requerimientos mínimos con los que debe contar un computador, seguidamente se va a descargar la imagen ISO del sistema operativo, ingresando a la página www.easyhotspot.souerceforge.net y luego dirigiéndose a la sección de descargas.

3.3.3 Grabar EasyHotspot en un disco.

Después de haber descargado la imagen ISO del sistema operativo, se lleva a cabo la grabación en un disco del mismo, utilizando cualquier programa que permita realizar esta acción, tales como Nero, Roxio, Cyberlink, etc. El sistema operativo puede ser grabado en un disco normal con capacidad de 700 MB.

3.3.4 Pasos de instalación.

Ya teniendo el sistema operativo grabado en un disco se seguirán los siguientes pasos de instalación:

- Insertar el disco de instalación del sistema operativo en la bandeja del lector de discos de la computadora y reiniciarla.
- Una vez reiniciada la computadora aparecerá la siguiente pantalla con las siguientes opciones.

Figura 3.5 Opciones de arranque del sistema operativo

En donde se escribe la palabra **"install"** y se presiona la tecla **"Enter"** para llevar a cabo la instalación del sistema operativo.

- Aparecerá la siguiente pantalla la cual indica que se está preparando la instalación del sistema operativo.

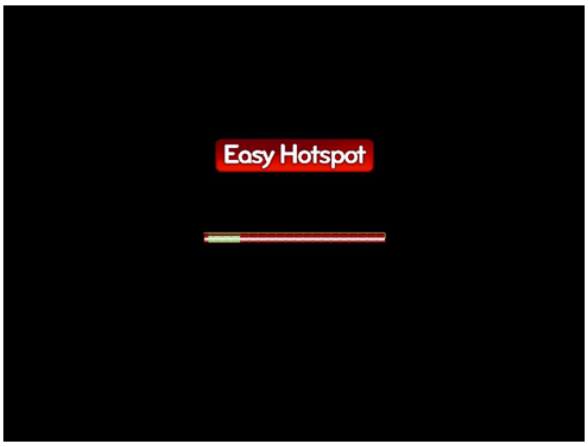

Figura 3.6: Cargando archivos para instalación del sistema operativo

- Ya cargados los archivos necesarios, se presenta la pantalla en donde se debe elegir el idioma de la instalación, en este caso se seleccionará **“Español”** y seguidamente se dará clic en el botón **“Fordward”**.

Figura 3.7: Selección de idioma de instalación del sistema operativo

- Seguidamente aparecerá la pantalla en donde se debe escoger la zona horaria para fijar la hora del sistema operativo, en este caso se seleccionará en la sección **“Región”** escogiendo América, y en **“Ciudad”** se elige Guayaquil. Luego se da un clic en **“Adelante”**.

Figura 3.8: Selección de zona horaria para la instalación del sistema operativo

- A continuación se mostrará la pantalla en donde se debe elegir el idioma del teclado, eligiendo **“Latin American”** y seguidamente se da clic en **“Adelante”**.

Figura 3.9: Selección de distribución del teclado

- En la siguiente pantalla se deberán especificar las particiones del disco duro, en este se utilizará todo el disco duro sin realizar particiones, y se dará un clic en **“Adelante”**.

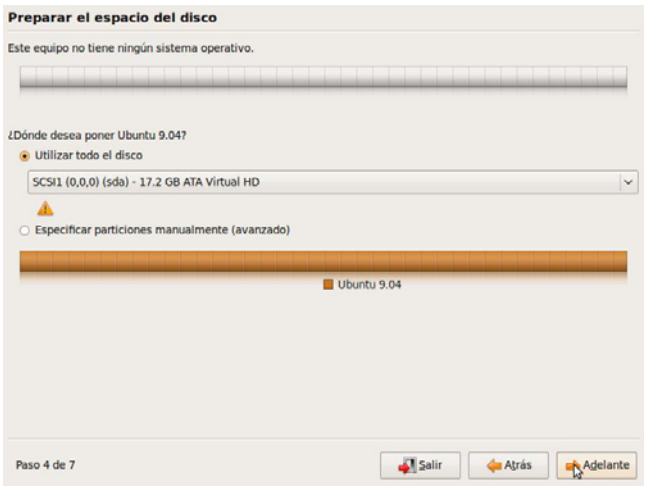

Figura 3.10: Especificación de particiones

- A continuación se mostrará la pantalla en la cual el sistema operativo solicitará un nombre para identificar a la persona que está realizando la instalación, un nombre de usuario, una contraseña la cual se insertará dos veces, el nombre que se desea asignar al equipo y se seleccionará “Solicitar una contraseña para acceder”, para que el sistema operativo pida la contraseña ingresada cada vez que el sistema operativo se inicie, luego se dará clic en “Adelante”. Cabe recalcar que la contraseña ingresada en el segundo cuadro de texto debe ser idéntica a la del primer cuadro de texto.

Figura 3.11: Información del usuario

- En la siguiente pantalla se mostrarán todos los detalles de la instalación que elegimos anteriormente, se revisa que todo esté tal y como lo que se eligió y se selecciona **“Instalar”**.

Figura 3.12: Información de instalación a realizarse

- Una vez dado clic en el botón de instalar en “Instalar”, el sistema comenzará a realizar los procesos de instalación, que durará aproximadamente 15 minutos.

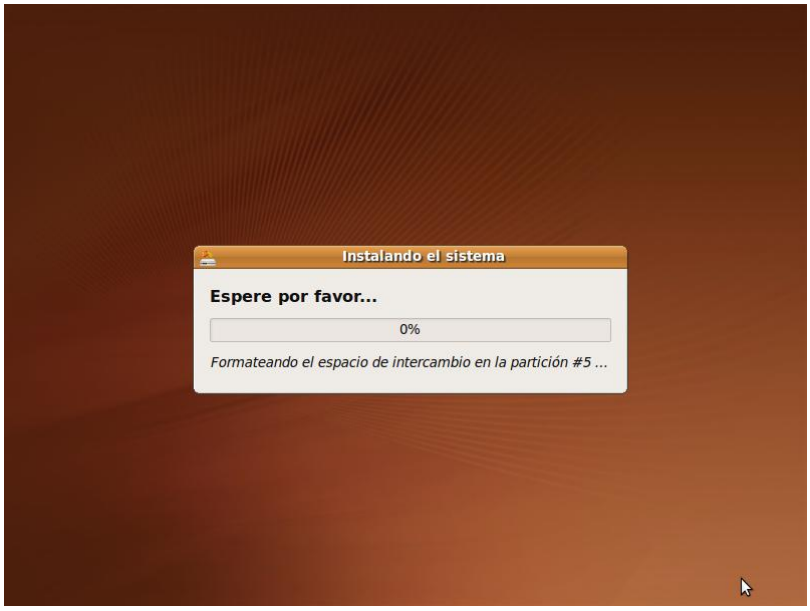

Figura 3.13: Instalación del sistema operativo en curso

- Ya instalado el sistema operativo, aparecerá una ventana notificando que la instalación ha finalizado y se dará clic en “Reiniciar ahora” y retiramos el disco de instalación de la bandeja lectora de discos.

  El equipo se reiniciará y comenzará el proceso de configuración del sistema, que se lo detallará a continuación.

3.4 Configuración de EasyHotspot.

Una vez reiniciada la computadora tras la instalación de sistema operativo, se ingresa al sistema digitando el nombre de usuario que se asignó en la instalación y la contraseña. Se iniciará con la configuración del sistema operativo cumpliendo con los siguientes pasos:

3.4.1 Activación del usuario “root”.

Lo que se hará primeramente es asignar una contraseña al usuario **“root”**, el cual tiene privilegios de administrador y se podrá realizar cualquier modificación en el sistema operativo, mientras no se le asigne una contraseña no se podrá cambiar nada. Este procedimiento se lo puede realizar de dos formas, de manera gráfica o en la consola de comandos, se lo realizará de la segunda forma dando clic en **“Applications”**, luego en **“Accessories”** y finalmente en **“Terminal”**, en donde se abrirá la siguiente ventana:

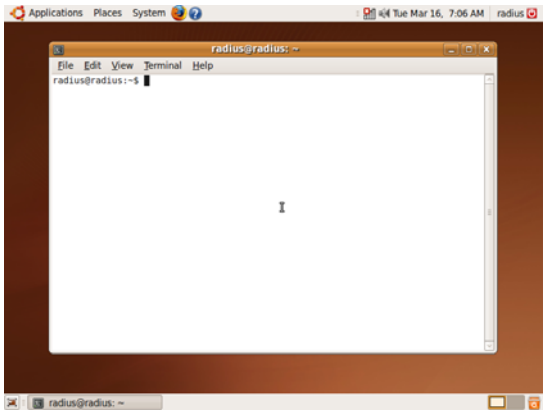

Figura 3.14: Ventana de comandos

Aquí se ingresa el comando: **"sudo passwd root"**, y seguidamente se presiona la tecla **"Enter"**. El sistema operativo solicitará la contraseña del usuario y luego pedirá que ingrese una contraseña para el usuario **"root"**, la cual se deberá introducir dos veces, y si las contraseñas son ingresadas correctamente, saldrá el siguiente mensaje confirmando que la contraseña ha sido actualizada exitosamente.

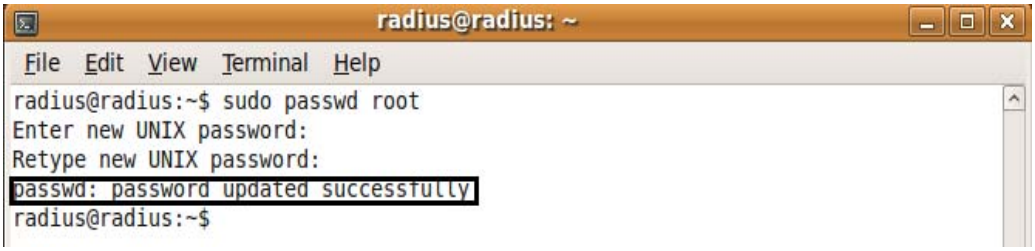

Figura 3.15: Creación de contraseña para usuario "root"

Ya asignada la contraseña al usuario **"root"**, se procederá a cambiar a dicho usuario para seguir con los procedimientos de configuración, esto se lo hace ingresando en la consola el comando: **"su –"** y el sistema operativo solicitará que se ingrese la contraseña

asignada en el paso anterior, obteniendo el siguiente mensaje en donde se nota que el nombre de usuario cambia a **“root”**.

Figura 3.16: Usuario “root” activado

3.4.2 Actualización del sistema operativo.

Hasta el momento ya se ha cambiado al usuario **“root”**, con lo que se podrá realizar el proceso de actualización del sistema operativo para mantener al día todas sus aplicaciones, esto se logra ingresando en la consola de comandos la instrucción **“apt-get update”**. Cabe recalcar que para realizar este procedimiento se debe tener disponible una conexión de Internet a la computadora. El sistema operativo consultará en sus repositorios las actualizaciones que se encuentran disponibles.

Una vez realizado este proceso, se ingresa el comando **“apt-get upgrade”** para confirmar la instalación de las actualizaciones, el sistema operativo informará al usuario el espacio que necesita para realizar las actualizaciones y consultará si está de acuerdo con esta información, la cual se confirma presionando la tecla **“y”** seguidamente por un **“Enter”**, iniciando el proceso de instalación de las actualizaciones. Al finalizar las actualizaciones el sistema operativo, éste pedirá que se reinicie la computadora para completar la configuración.

El mismo procedimiento se la realizara pero con las instrucciones **“aptitude-update”** y **“aptitude-upgrade”**. Así se finalizará con el proceso de actualización del sistema operativo y se podrá continuar con la configuración del HOTSPOT.

3.4.3 Verificación de tarjetas o interfaces de red.

Actualizado ya el sistema operativo, el siguiente paso es verificar que éste haya detectado las tarjetas de red, esto se logra abriendo nuevamente la consola de comandos, cambiando al usuario administrador **“root”** e ingresando la instrucción **“ifconfig”**, en donde hay que observar si a las tarjetas de red han sido detectadas y llamadas **“eth0”** y **“eth1”**, respectivamente, cabe recalcar que la conexión a Internet de estar en la tarjeta **“eth0”**, por lo que ya deberá estar asignada una dirección IP por parte del modem adsl, la segunda tarjeta de red deberá también ser detectada pero no cantará con ninguna direcciona IP, ésta será laque se encargará de proveer de Internet a los usuarios de la red.

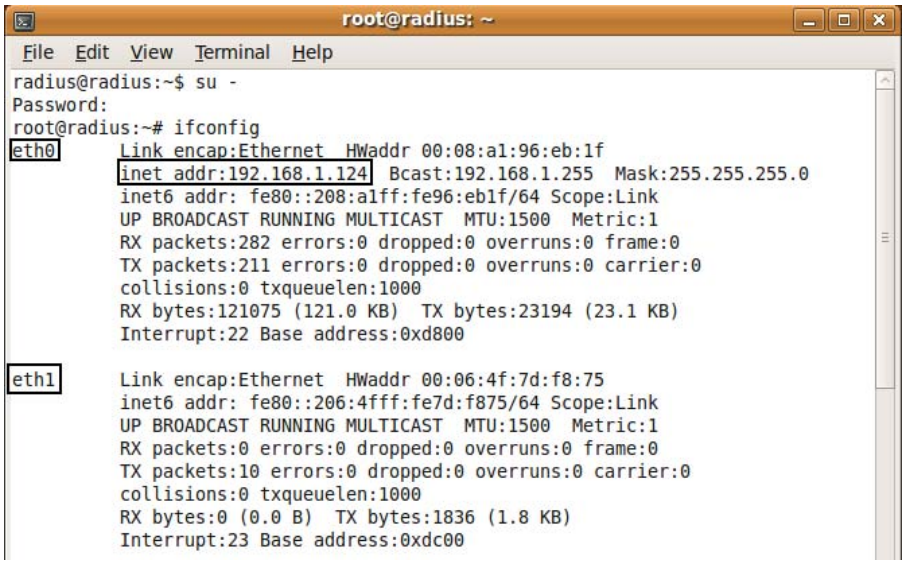

Figura 3.17: Verificación de interfaces de red

Si las tarjetas de red son reconocidas con nombres diferentes por ejemplo como “eth3” y “eth4”, hay que dirigirse en la barra de tareas a **\Places\Computer\Filesystem\etc\udev**, y abrir el archivo llamado “**70-persistent-net.rules**”, en donde se encontrará lo siguiente:

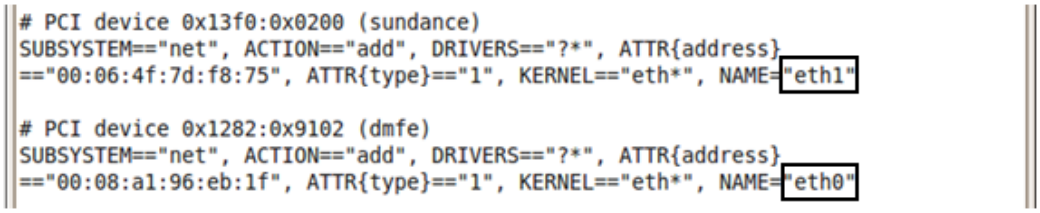

Figura 3.18: Cambio de nombre de interfaces de red

En este archivo se reemplazarán los nombres de las tarjetas de red “eth0” y “eth1” por los nombres que han sido reconocidos con el comando anteriormente ingresado en la consola de comandos, así no existirá ningún problema con los siguientes pasos de configuración.

3.4.4 Ingresando al sistema de administración de EasyHotspot.

Con la verificación de la configuración de las tarjetas de red, el siguiente paso será la configuración del software con los que trabaja el sistema operativo para la implementación del HOTSPOT, esto se logra entrando al navegador Mozilla Firefox ubicado en la barra de tareas.

Ya abierto el navegador, en la barra de direcciones se ingresa la siguiente dirección: http://localhost/easyhotspot, se abrirá la siguiente página:

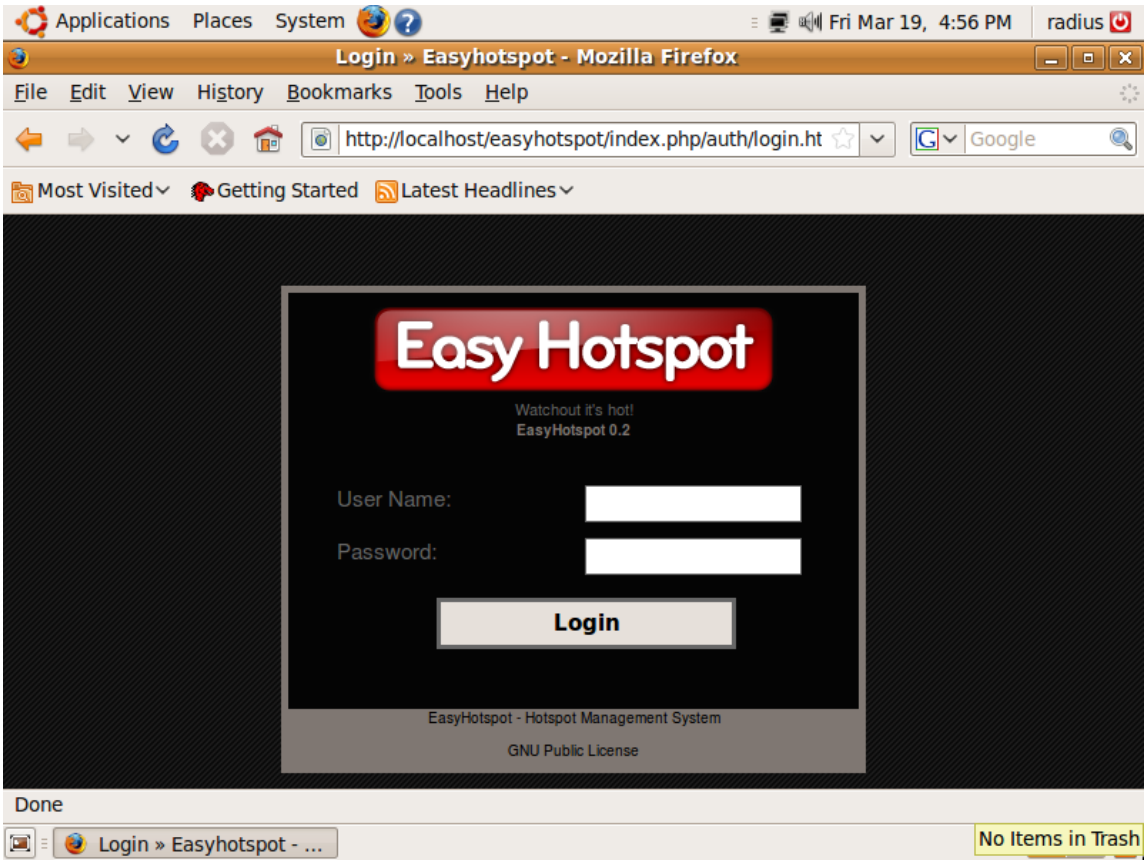

Figura 3.19: Ingresando a EasyHotspot

Esta es la página del sistema Easy Hotspot en donde se debe ingresar el nombre de usuario y la contraseña para entrar a la configuración del HOTSPOT, el nombre de usuario y la contraseña por defecto son:

Nombre de usuario: admin

Contraseña: admin123

Ingresando estas credenciales obtendremos la siguiente página:

Figura 3.20: Página de presentación del sistema de administración

3.4.5 Editando la página web de presentación del sistema de administración de EasyHotspot.

La figura anterior nos indica la página web de presentación del sistema de administración de Easy Hotspot, se puede notar que contiene información que viene por defecto, la cual se puede editar para mostrar la información de la institución. Ingresando en:

\Places\Computer\Filesystem\Opt\Local\web\easyhotspot\htdocs\system\application\config. Se abre el archivo easyhotspot.php, en donde se edita la información de la página de la página web de presentación del sistema, ingresando los datos de la institución:

```
$config['company_name'] = 'Biblioteca de la Ciudad y la Provincia';
$config['company_address_line1'] = 'Honorabe Gobierno Provincial de Tungurahua';
$config['company_address_line2'] = 'Sucre y Catstillo - Esquina';
$config['company_address_line3'] = 'Edificio de Promociones y Servicios - ex Banco Central del Ecuador';
$config['company_phone'] = '032845560';
```

Figura 3.21: Editando la página de presentación del sistema de administración

Quedando de la siguiente forma la página web de presentación del sistema:

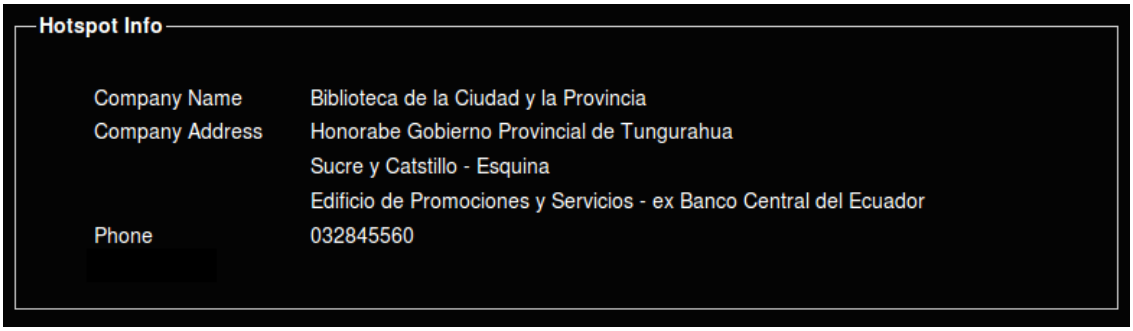

Figura 3.22: Página de presentación del sistema de administración editada

3.4.6 Menús del sistema de administración de EasyHotspot.

Lugo de haber editado la página web de presentación del sistema con la información de la institución, en la parte superior derecha de ésta se puede notar dos enlaces: “Cashier Menu” y “Admin Menu”, estos son los menús que ofrece el sistema, el primero el cual manejarán los empleados y el segundo el administrador de la red.

3.4.6.1 Menú del administrador de red “Admin Menu”.

Dando clic en el segundo enlace, se mostrará un menú con varias opciones, las cuales sirven para configurar las características del HOTSPOT. Cada enlace lleva a una sección

diferente, las cuales se indicarán en el siguiente gráfico y se explicarán una a una más adelante.

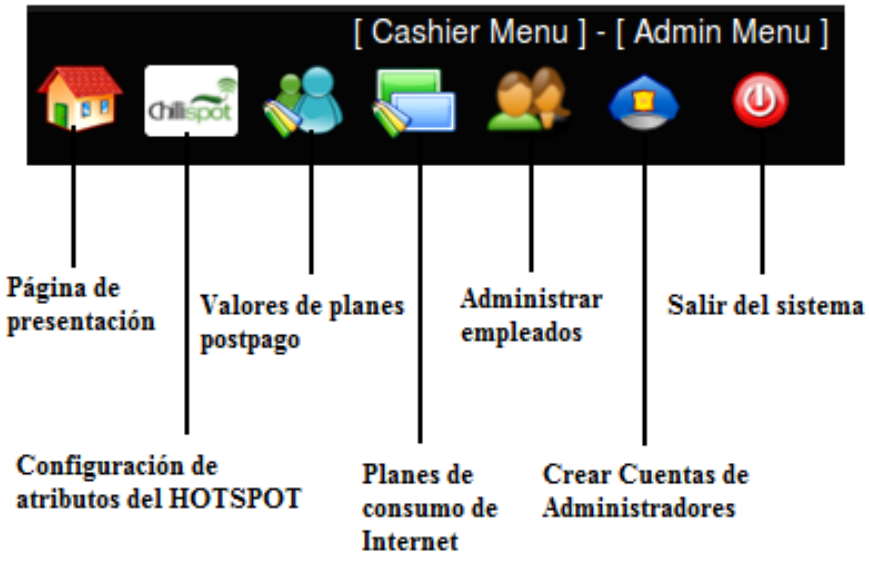

Figura 3.23: Menú del administrador de red

3.4.6.1.1 Página de presentación.

Al dar clic en este enlace el sistema llevará al usuario a la página de presentación del sistema.

3.4.6.1.2 Configuración de atributos del HOTSPOT.

Dando clic en esta sección se presentan las siguientes opciones de configuración del HOTSPOT.

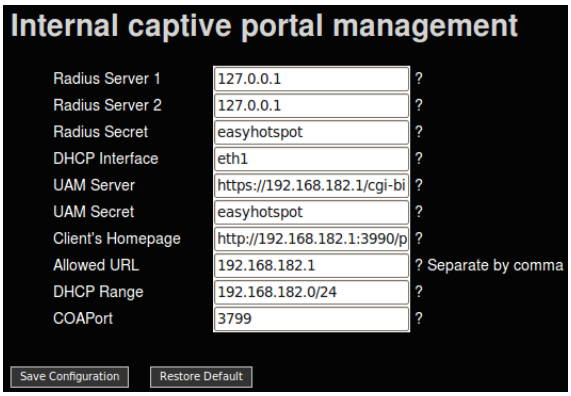

Figura 3.24: Configuración de atributos del HOTSPOT

3.4.6.1.2.1 Opciones de configuración de EasyHotspot.

- **Radius Server 1:** Es la dirección IP del servidor RADIUS
- **Radius Server 1:** Es la dirección IP del servidor RADIUS secundario, que en este caso es la misma del primero. Se utiliza generalmente cuando se trabaja con dos servidores RADIUS.
- **Radius Secret:** Es la contraseña que comparte el servidor RADIUS con el portal cautivo para realizar la autenticación de los usuarios.
- **DHCP Interface:** Es la interfaz o tarjeta de red que usa el HOTSPOT para compartir los servicios de la red, en este caso el Internet.
- **UAM Server:** Es la dirección en donde está almacenada la página web de registro de usuarios del portal cautivo, la cual se encuentra dentro del servidor web Apache.
- **UAM Secret** Es la contraseña que comparte la página web de registro de usuarios con el portal cautivo.
- **Client's Homepage:** Es la página a la que se desea direccionar a un usuario luego de haberse registrado exitosamente en el sistema.

- **Allowed URL:** Son las direcciones IP que se asignan a los usuarios que no pasarán por la página de registro y podrán utilizar los servicios de la red sin autenticarse. Se pueden asignar varias direcciones separándolas con comas “,”.
- **DHCP Range:** Es el rango de direcciones IP que se asignarán a los usuarios de la red. El portal cautivo es el que actúa como servidor de direcciones IP dinámicas y se puede asignar el rango necesario según el número de usuarios que vayan a utilizar los servicios de la red.
- **COAPort:** Es la dirección del puerto que utiliza el sistema para realizar los procesos de autenticación.

Para configurar el HOTSPOT únicamente se debe dar clic en el botón “Save changes”, en este caso se dejará todos los valores por defecto ya que son los correctos para esta implementación.

3.4.6.1.3 Valores de planes postpago.

Este sistema está orientado para negocios, por lo que se puede configurar el precio de consumo de Internet por Mega Bytes consumidos o por minutos y otros atributos. En la siguiente figura se muestra las opciones de configuración.

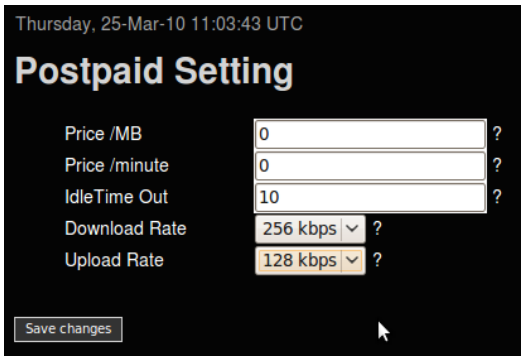

Figura 3.25: Opciones de configuración de planes postpago

3.4.6.1.3.1 Opciones de configuración de los valores de planes postpago.

- **Price /MB:** Se fija el valor del megabyte consumido por cada usuario, como el servicio de internet en la biblioteca se ha configurado el precio en cero.
- **Price /minute:** Se fija el valor del minuto consumido por cada usuario, como el servicio de internet en la biblioteca se ha configurado el precio en cero.
- **IdleTime Out:** Es el tiempo en el que el sistema suspenderá el servicio de Internet al usuario después de haber pasado un tiempo de inactividad, en esta caso se ha configurado 10 minutos, lo que quiere decir que si el usuario ha dejado de utilizar el servicio de Internet por 10 minutos el sistema suspenderá este servicio y para volver a utilizarlo deberá nuevamente ingresar su nombre de usuario y su contraseña.
- **Download Rate:** Es la velocidad de Internet que el usuario dispone para descargar información.
- **Upload Rate:** Es la velocidad de Internet que el usuario dispone para subir información.
- Para guardar estos valores de configuración se debe dar clic en el botón **"Save changes".** Cabe recalcar, que esta opción no es la que se utiliza en la implementación, pero se la configura por seguridad.

3.4.6.1.4 Planes de consumo de Internet.

Esta opción es la que utiliza en la implementación del HOTSPOT, ya que aquí se configura el tiempo que dispone cada usuario para utilizar el servicio de Internet. La siguiente figura muestra las opciones que se deben configurar.

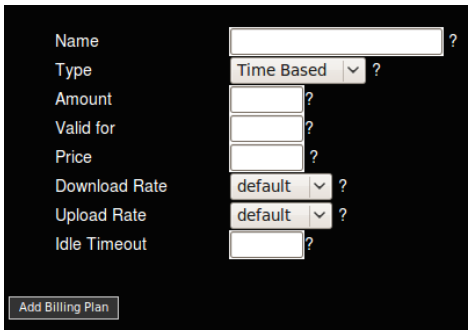

Figura 3.26: Opciones de configuración de planes de consumo de Internet

3.4.6.1.4.1Opciones de configuración de los planes de consumo de Internet.

- **Name:** Es el nombre que se asigna al plan para identificarlo.
- **Type:** En esta opción se elige el tipo de plan con el que se desea trabajar, puede ser basado en minutos consumidos o en megabytes.
- **Amount:** Aquí se asigna el tiempo de duración en la cantidad de megabytes que un usuario tiene disponible para utilizar el servicio de Internet.
- **Valid for:** Es el tiempo en días en el que un usuario es válido para ingresar a la red.
- **Price:** Es el costo que se le asigna al plan, en este caso el valor debe ser cero.
- **Download Rate:** Es la velocidad de Internet que el usuario dispone para descargar información.
- **Upload Rate:** Es la velocidad de Internet que el usuario dispone para subir información.
- **Idle Timeout:** Es el tiempo en el que el sistema suspenderá el servicio de Internet al usuario después de haber pasado un tiempo de inactividad, en esta caso se ha configurado 10 minutos, lo que quiere decir que si el usuario ha dejado de utilizar el servicio de Internet por 10 minutos el sistema suspenderá este servicio y para volver a utilizarlo deberá nuevamente ingresar su nombre de usuario y su contraseña.

Una vez ingresados todos los valores de configuración del plan, se da un clic en el botón **“Add Billing Plan”**. El siguiente gráfico muestra el plan añadido al sistema.

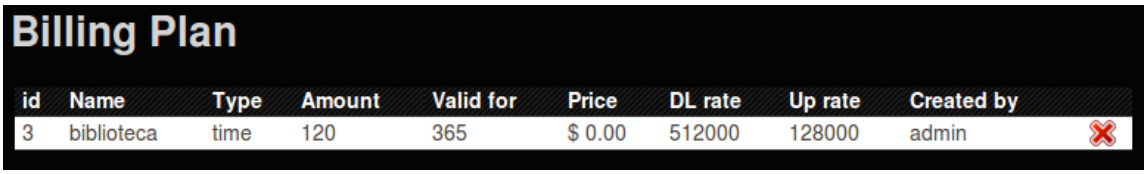

Figura 3.27: Plan de consumo de Internet añadido

Existen planes que vienen por defecto en el sistema, los cuales se los pueden eliminar para que no existan confusiones al momento de crear un nuevo usuario en el plan.

3.4.6.1.5 Administrar empleados.

El sistema ofrece la opción de poder operarlo como administrador, el cual tiene todos los privilegios, y en modo cliente o empleado, el cual se encarga solamente de manejar el sistema únicamente creando usuarios y monitoreando el sistema para verificar que todo marche bien. Esta opción sirve para crear y eliminar los clientes o empleados que manejan el sistema. Para agregar un empleado de debe hacer clic en **"Add Cashier"**, la siguiente figura muestra las opciones para agregar un nuevo empleado.

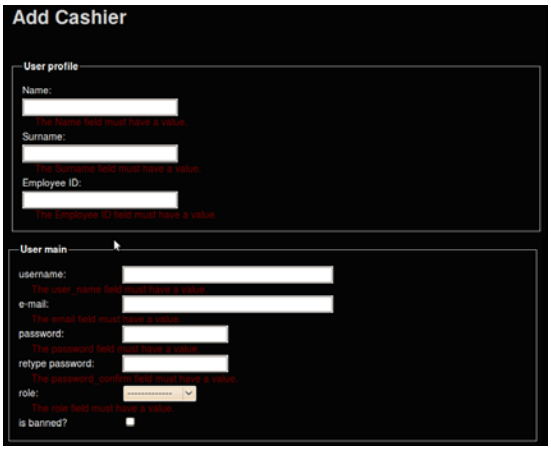

Figura 3.28: Añadiendo un empleado

3.4.6.1.5.1 Opciones de configuración de la administración de empleados.

- **Name:** Se asigna el nombre del empleado.
- **Surname:** Se asigna el apellido del empleado.
- **Employee ID:** Un número de identificación del empleado.
- **Username:** El nombre de usuario del empleado.
- **e-mail:** El correo electrónico del empleado.
- **Password:** La contraseña del empleado.
- **Retype password:** Se ingresa nuevamente la contraseña anterior.
- **Role:** Aquí se asigna si el empleado tendrá privilegios de súper administrador, administrador o simplemente un usuario. En este caso se le da privilegios de usuario ya que solo se va a encargar de crear usuarios para red inalámbrica.
- **Is banned?**: Se activa el cuadro si se desea que el usuario no tenga acceso al sistema.

Finalmente se da clic en el botón **"Add"** para añadir un empleado al sistema, quedando de la siguiente forma:

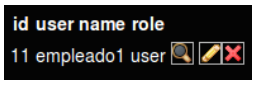

Figura 3.29: Empleado añadido

La información de cada empleado se puede revisar, editar o se lo puede eliminar con los botones que se encuentran en la parte derecha de cada uno.

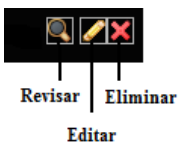

Figura 3.30: Opciones de información de empleado

3.4.6.1.6 Crear cuentas de administradores.

En esta sección el sistema brinda la oportunidad de editar la información de cada cuenta de administrador o añadir una nueva, es similar a la sección anterior, pero aquí solo se toman en cuenta las cuentas con privilegios de administrador. Se debe ingresar la misma información que anteriormente se ingresó en las cuentas de empleados.

3.4.6.1.6 Salir del sistema.

Al dar clic en este botón el usuario saldrá del sistema y se presentará nuevamente la página en la que se tiene que ingresar las credenciales ya sea del administrador o del empleado para poder nuevamente entrar al sistema.

3.4.6.2 Menú de empleados "Cashier Menu".

Ya configurado el HOTSPOT, creado un empleado para que maneje el sistema y creado un plan de consumo de Internet, se procede a ingresar al menú de los empleados para poder crear usuarios los cuales ingresarán al sistema para utilizar el servicio de Internet. Esta sección presenta las siguientes opciones.

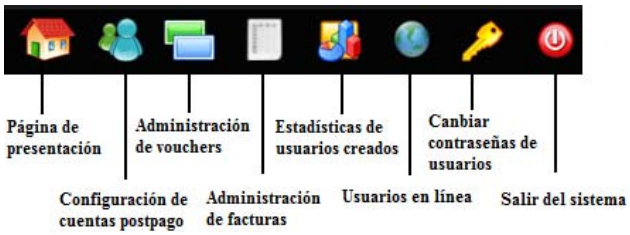

Figura 3.31: Opciones del menú de empleados

3.4.6.2.1 Página de presentación.

Al dar clic en este enlace el sistema llevará al empleado a la página de presentación del sistema.

3.4.6.2.2 Configuración de cuentas postpago.

Como este sistema está orientado a negocios, brinda la opción de crear usuarios postpago, a los cuales se le asigna un nombre de usuario y una contraseña, cuando terminan de utilizar el servicio de Internet, el usuario pagará el valor configurado en la sección de valores postpago, en este caso esta opción no se la utiliza ya que los usuarios creados dentro de este plan caducan mínimo en un día y en este caso lo que se necesita es controlar al usuario en un lapso de tiempo de dos horas, por lo que se utilizará la opción de administración de vouchers, que se la detalla a continuación.

3.4.6.2.3 Administración de vouchers.

Un voucher representa a una cuenta de usuario la cual toma los valores configurados en la sección de planes de consumo de Internet. En la siguiente figura se especifica cuantas cuentas de usuario (vouchers) se desea crear, eligiendo el plan de consumo de Internet, llamado biblioteca, creado anteriormente.

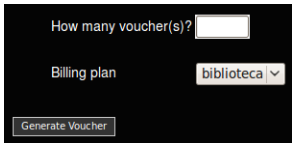

Figura 3.32: Creación de una cuenta de usuario

Al dar clic en el botón **“Generate Voucher”**, el sistema crea una cuneta con nombre de usuario y contraseña asignados aleatoriamente, de esta forma:

Username	Password	Billing plan	Valid until	Time used	Time remain	Packet used	Packet remain	Printed	
tiygup11	megronic	biblioteca	March 26 2011	---	---	---	---	no	

Figura 3.33: Cuenta de usuario creada

En la parte derecha del usuario creado se encuentran 3 botones, los cual dan la opción de: eliminar un usuario, editar la información de un usuario e imprimir en una hoja la información para entregarla al usuario.

En este caso al momento de crear un usuario, se editará la contraseña de éste, asignándole como contraseña su número de cédula, esto se hace como medida de seguridad, por lo que si un usuario pierde o se le olvida su nombre de usuario, será fácil localizarlo en el sistema.

3.4.6.2.4 Administración de facturas.

En sección el sistema ofrece información acerca del valor que cada usuario debe pagar después de haber utilizado el servicio de Internet, pero en este caso no se utiliza esta sección ya que el servicio de Internet es gratuito y no se facturará ningún valor.

3.4.6.2.5 Estadísticas de usuarios creados.

En esta sección el sistema indica toda la información relacionada con las cuentas (vouchers) credos, los que han sido utilizados y los que han expirado. También indica el

número de planes de consumo de Internet creados y las cuentas de usuario creados en la cuenta postpago.

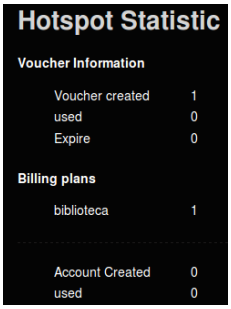

Figura 3.34: Estadísticas de usuarios creados

3.4.6.2.5 Usuarios en línea.

En esta sección el sistema indica todos los usuarios que en ese momento están haciendo uso del servicio de Internet, y da la oportunidad de desconectar a cualquier usuario el momento que sea necesario. También indica la hora en la que inició a utilizar el servicio, y el tiempo o el tamaño de paquetes disponibles con el que cuenta.

3.4.6.2.6 Cambiar contraseñas de usuarios.

En esta sección se pueden cambiar las contraseñas de los usuarios que forman parte del sistema, aquí se debe ingresar el nombre del usuario al que se le va a cambiar la contraseña, la contraseña asignada, la nueva contraseña que se le va a asignar y nuevamente la misma contraseña para confirmar el cambio, finalmente se da un clic en el botón **“submit”**, para confirmar el cambio de contraseña del usuario.

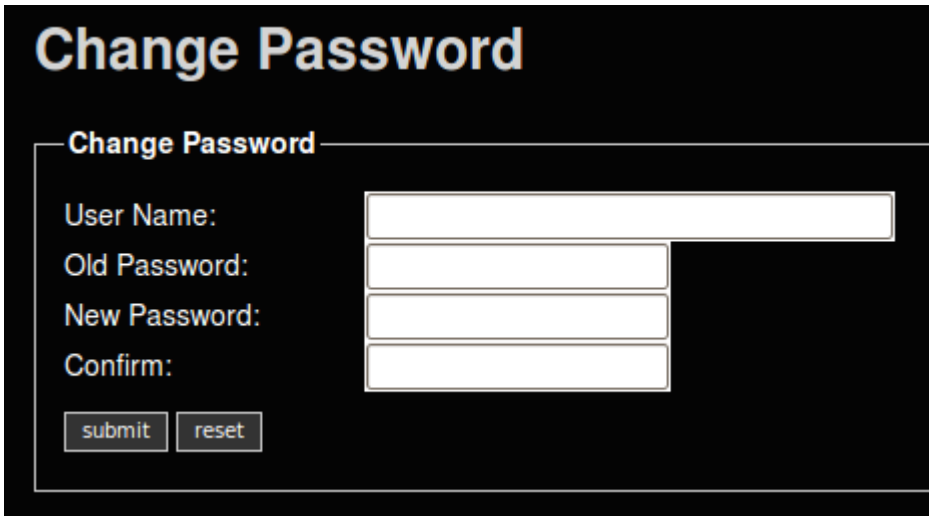

Figura 3.35: Cambiar contraseñas de usuarios

3.4.6.2.7 Salir del sistema.

Al dar clic en este botón el usuario saldrá del sistema y se presentará nuevamente la página en la que se tiene que ingresar las credenciales ya sea del administrador o del empleado para poder nuevamente entrar al sistema.

3.4.6.3 Personalizando la página web del portal cautivo.

Cuando se ha obtenido un nombre de usuario y una contraseña para poder utilizar el servicio de Internet, el momento en el que un usuario abre su navegador el sistema lo redirigirá a la página web de registro del HOTSPOT. El sistema operativo trae una página web de presentación por defecto, la cual se la puede personalizar de acuerdo a la necesidad del caso, esto se logra ingresando a: **\Places\Computer\Filesystem\opt\local\web\easyhotpot\hotspot,** y abriendo el archivo **"hotspotlogin.cgi"**, dentro de este archivo se encuentra todo el código HTML con el que está construida la página web del portal cautivo. Este código se lo puede modificar

para personalizar la página web pero se debe tener mucho cuidado ya que es muy delicado y si no se lo maneja correctamente el sistema puede sufrir daños serios y dejará de funcionar. Más adelante se mostrará la página editada a gusto. En el Anexo 4 se detalla el código editado para personalizar esta página.

3.5 OpenDNS.

Cumpliendo con otra de las políticas de la Biblioteca Virtual, se ha utilizado OpenDNS para bloquear el contenido del Internet no permitido en la institución, tales como pornografía, violencia o cualquier material ofensivo a las personas.

OpenDNS es un servidor de nombres de dominio el que puede utilizar personas y empresas como una alternativa al servidor de DNS en su servicio de Internet gratuitamente. Estos servidores se encuentran en lugares estratégicos, permiten que las consultas de DNS sean generalmente más rápidas, lo que a su vez acelera la velocidad de respuesta de Internet. Los resultados de las consultas son a veces almacenados por los sistemas locales, consiguiendo un aumento de la velocidad en la mayoría de las peticiones, ya que quedan guardadas en un caché local.

Otra característica con la que cuenta este servicio es un filtro de contenido web y corrección de errores ortográficos. Al entrar en sitios clasificados como maliciosos, OpenDNS bloquea el acceso a ese sitio, aunque esto también se puede configurar en el panel de control que cada cuenta dispone para configurarlo.

A continuación se detalla cómo crear una cuenta en este servicio y el manejo básico del mismo.

3.5.1 Creación una cuenta en OpenDNS.

Para poder crear una cuenta en este interesante servidor de nombres de dominio, se debe ingresar desde cualquier computador que integre la red que se desea añadir a este servicio, a la página https://www.opendns.com/, y dar clic en el enlace **"Create account"**, en la parte superior derecha de la página.

Figura 3.36: Creando una cuenta en OpenDns

Ahora se presenta el tipo de cuenta que se desea crear, en este caso se escoge el tipo de cuenta gratuita, ya que es más que suficiente para cumplir con las políticas de la Biblioteca Virtual, y se da clic en **"Sign Up".**

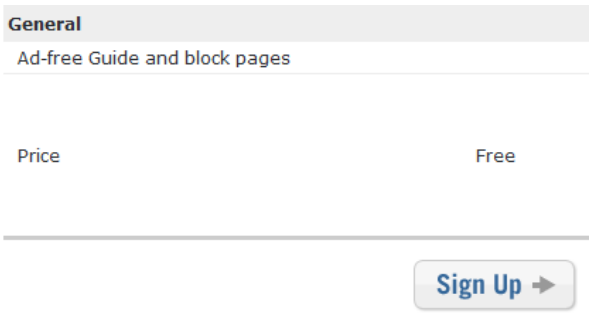

Figura 3.37: Tipo de cuenta en OpenDNS

Escogido el tipo de cuenta que se desea crear, su muestra una página en la que se debe ingresar la información de la persona que está creando la cuenta, al terminar de lleras estos datos de da clic en **"Continue".**

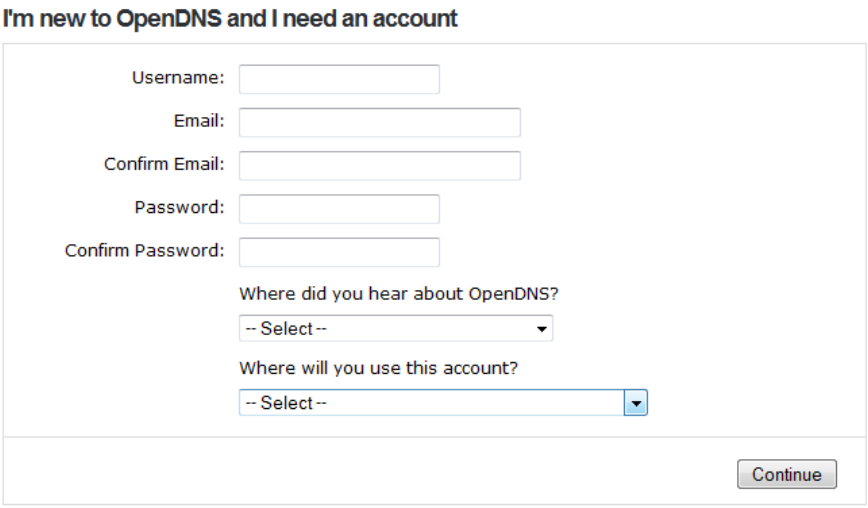

Figura 3.38: Ingresando información de la cuenta a crear

Realizado el paso anterior, se enviará una notificación al correo electrónico introducido, el cual contiene un enlace al que se debe ingresar para confirmar la creación de la cuenta en OpenDNS y la cuenta estará totalmente creada y validada.

3.5.2 Añadiendo la red a OpenDNS.

Ya creada y validada la cuenta en OpenDns, el siguiente paso es agregar a este servicio la red que se está utilizando para poder bloquear el contenido que se desee.

Para agregar la red sobre la que se está trabajando, se debe ingresar en el enlace llamado **"Settings"**, en donde se muestra la dirección IP de la red:

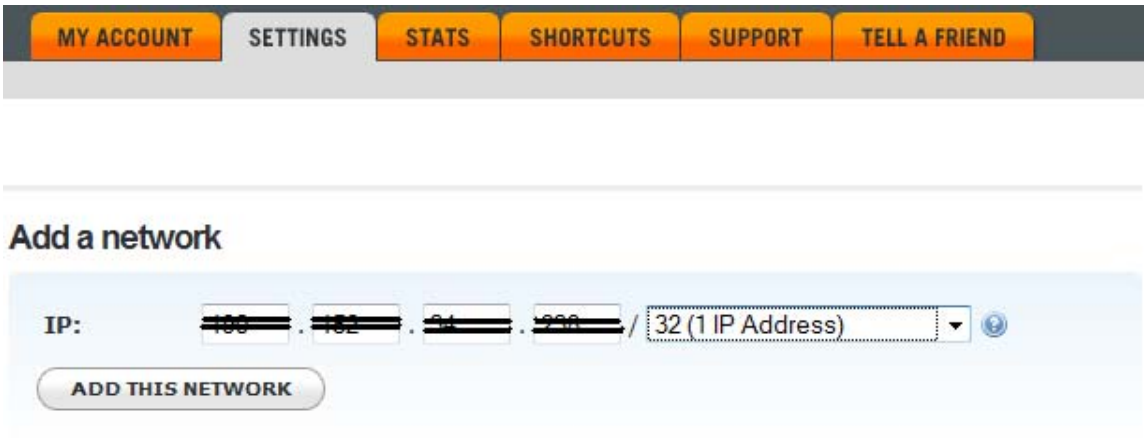

Figura 3.39: Añadiendo la red a OpenDNS

Al dar clic en el botón **"ADD THIS NETWORK"**, aparece una ventana en la cual se le debe dar un nombre a la red para identificarla y se debe especificar si la red cuenta con una dirección IP estática o dinámica:

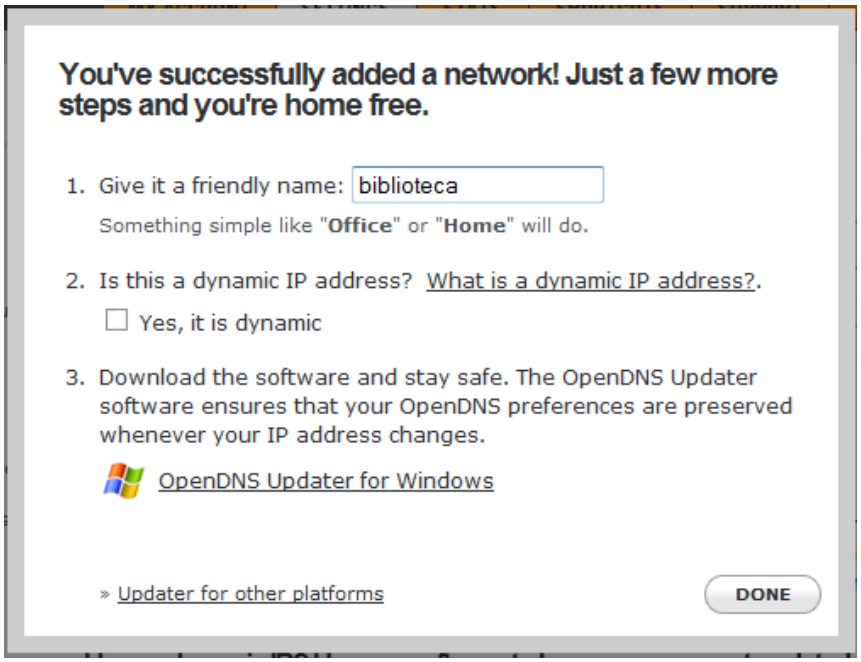

Figura 3.40: Nombre de la red y determinación de dirección IP

Cabe recalcar que la Biblioteca Virtual cuenta con una dirección estática, asignada por el proveedor de servicio de Internet.

Realizado el paso anterior se da clic en el botón **"DONE"** la red será añadida en el sistema:

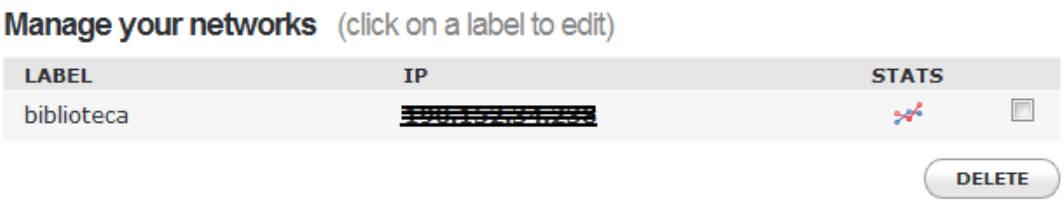

Figura 3.41: Red añadida al OpenDNS

3.5.3 Configuración de OpenDNS en la red.

Para editar la configuración de la red se debe dar en la dirección IP de la misma:

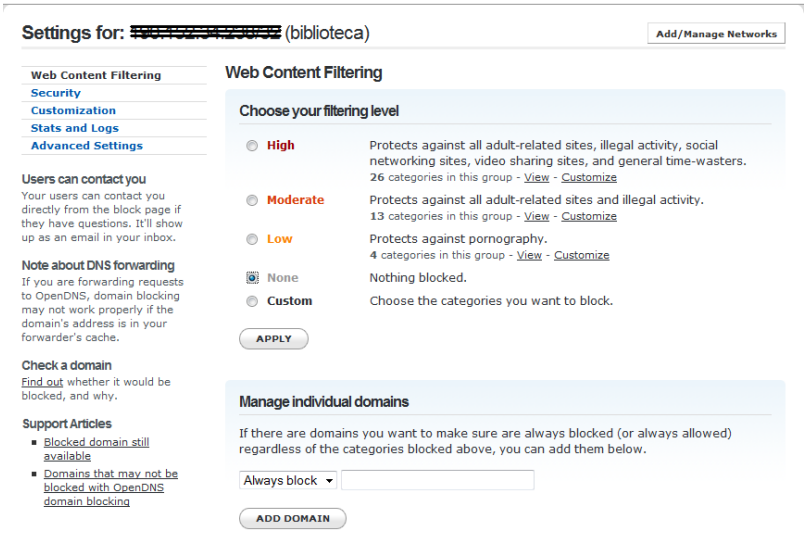

Figura 3.42: Configuración de OpenDNS en la red

En esta sección se puede configurar el nivel de seguridad del contenido web que los usuarios tienen disponible para visitar, cuenta con varios niveles de seguridad los cuales se los puede activar según la necesidad y también cuenta con una opción en la que se puede ingresar individualmente el sitio que se desee bloquear o que no esté bloqueado, en el Anexo 3 se detalla la configuración del nivel de seguridad del sistema.

Este sistema cuenta también con varias opciones interesantes las cuales lo convierten en una herramienta poderosa, a continuación se detalla algunas de estas opciones:

- **Seguridad:** En esta opción se puede configurar que tan segura será la red ya que el sistema da la opción de proteger a los usuarios de la red para no ingresar a sitios que contengan virus o programas maliciosos los cuales dañen el computador del usuario.
- **Personalización:** Aquí se puede editar la página web que indica que algún sitio está bloqueado, se lo puede editar cambiando el logotipo de la institución o lugar en el que se esté trabajando y el mensaje que indica que la página está bloqueada, también se puede editar la página que se muestra cuando el sistema bloque un sitio no confiable.
- **Estadísticas:** En esta opción se puede configurar el sistema para que lleve estadísticas de las diferentes actividades que realiza el usuario realiza, esto se hace para llevar una buena administración del servicio de Internet y controlar que los usuario no esté dando un mal uso al Internet.

También hay configuraciones avanzadas las cuales ofrecen un mejor manejo del sistema y un mayor control en la red para ofrecer un servicio de Internet eficaz.

3.5.4 Configuración de OpenDNS en el servidor.

Las direcciones de OpenDNS son: 208.67.222.222 y 208.67.220.220, estas se deben configurar en el servidor del HOTSPOT para poder utilizar los servicios de restricción del páginas web, esto de logra ingresando en la consola de comandos lo siguiente:

Primero se ingresa a la consola de comandos con privilegios de administrador como ya se explicó anteriormente.

Seguidamente se ingresa el comando: nano "/etc/resolve.conf", y se pulsa **"Enter"**, en donde se abrirá un archivo en donde se encuentra especificado la dirección de nombres de dominio del proveedor de Internet local:

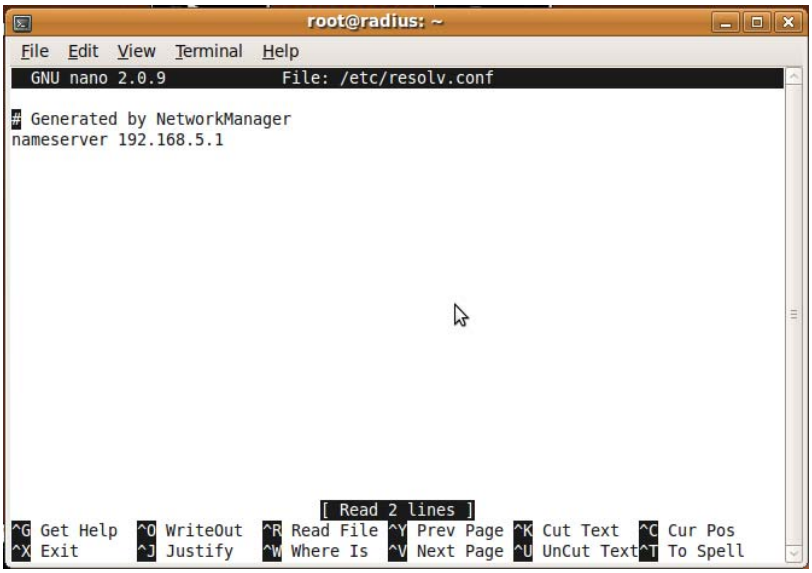

Figura 3.43: Iniciando configuración de OpenDNS en el servidor

Se debe cambiar la dirección de nombres de dominio por las direcciones de OpenDNS, quedando de la siguiente forma.

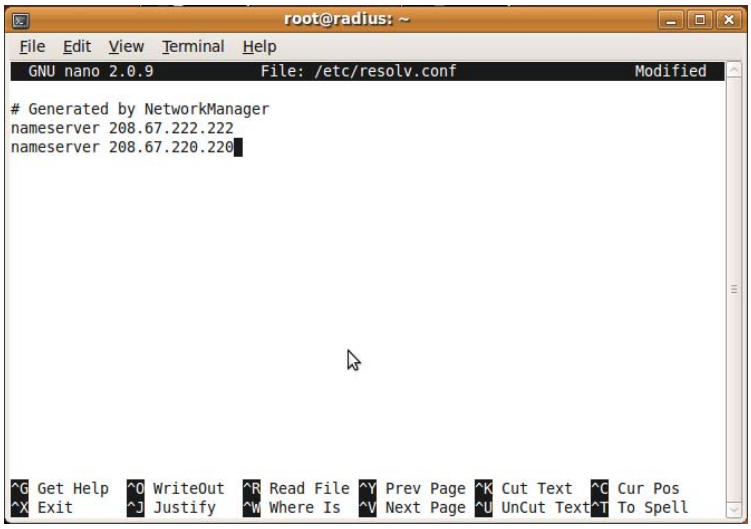

Figura 3.44: Finalizando configuración de OpenDNS en el servidor

Para salir del editor de texto se presiona la tecla **"Ctrl"** + **"x"**, la tecla **"y"** para confirmar los cambios en el archivos y finalmente la tecla **"Enter"** para salir del editor, así ya está configurado el servidor con OpenDNS y todo el contenido web configurado anteriormente estará bloqueado para todos los usuarios.

3.6 Configuración de los Puntos de Acceso.

Ya configurado casi totalmente el servidor, se debe configurar los puntos de acceso, esto se lo puede hacer desde cualquier computadora que cuente con una tarjeta de red y un navegador de Internet como Internet Explorer, Mozilla Firefox, etc. A continuación se explica paso a paso esta configuración.

Primeramente se debe configurar la dirección IP y la máscara de subred de la tarjeta de red de la computadora que se esté utilizando para la configuración del punto de acceso, con los siguientes valores:

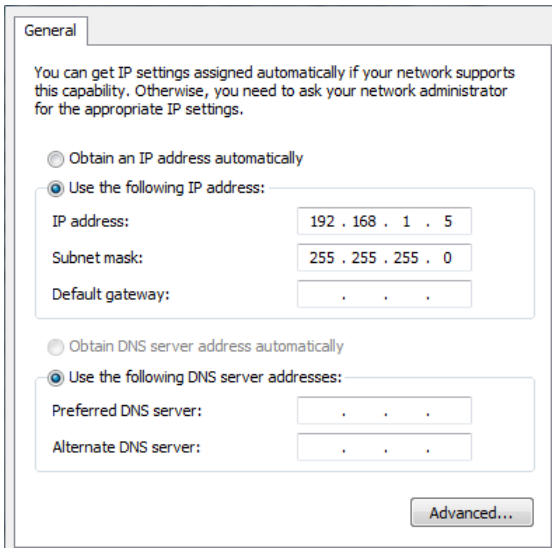

Figura 3.45: Configuración de dirección IP para acceder al punto de acceso

Configurada la tarjeta de red con estos valores, se debe abrir un navegador de Internet, y en la barra de direcciones digitar la dirección IP del punto de acceso que por defecto es: 192.168.1.245 y se mostrará la siguiente imagen.

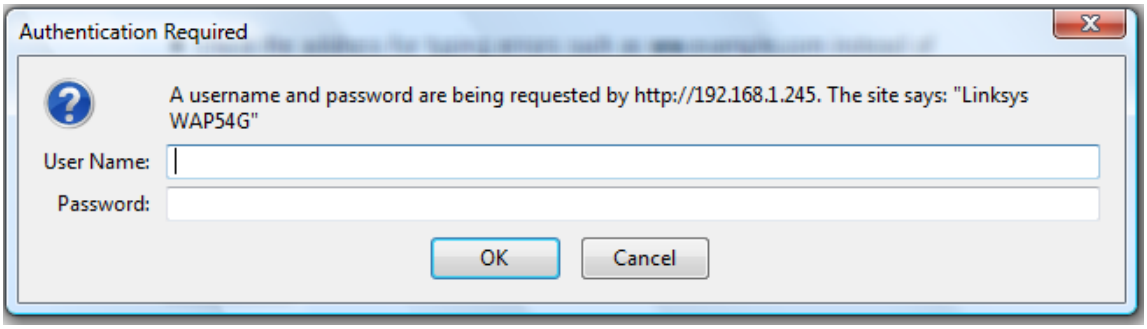

Figura 3.46: Accediendo al punto de acceso

En donde se debe ingresar únicamente una contraseña, la cual por defecto es **“admin”**.

3.6.1 Menú “Setup”.

Dentro de este menú se encuentran las principales configuraciones de acceso y función del punto de acceso.

3.6.1.1 Submenú “Network Setup”.

En esta sección llamada, se debe configurar el nombre que se desee asignar al dispositivo, y la dirección IP de acceso a éste. Para mayor seguridad de la red se configura con cualquier otra dirección IP para no dejar la dirección de fábrica.

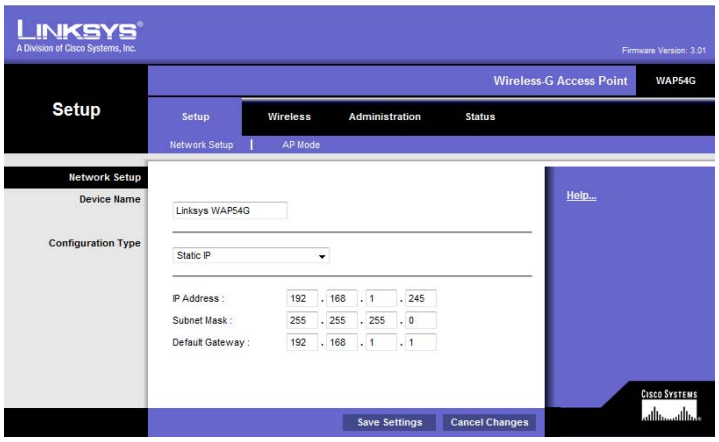

Figura 3.47: Configuración de dirección IP de acceso al dispositivo

3.6.1.2 Submenú “AP Mode”.

En esta sección se configura la función del dispositivo, en este caso se deja el valor por defecto, ya que se lo va a utilizar en modo de punto de acceso.

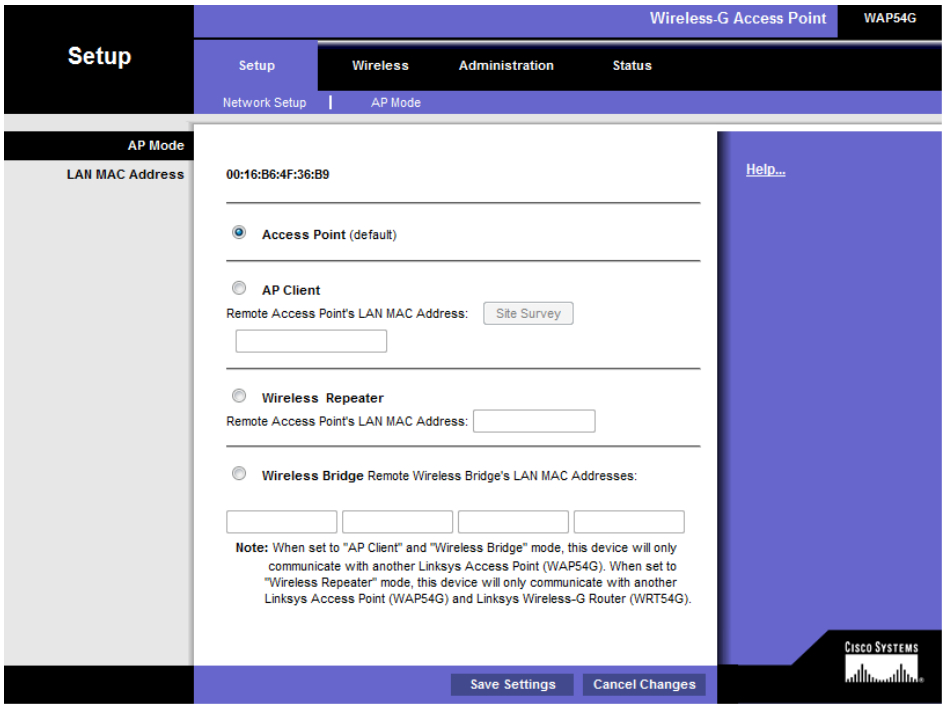

Figura 3.48: Configuración de la función del punto de acceso

3.6.2 Menú "Wireless".

En esta sección se configuran los valores de la red inalámbrica, tales como el nombre de la red y el tipo de seguridad con la que cuenta.

3.6.2.1 Submenú "Basic Wireless Settings".

Aquí se configura el nombre de la red (SSID), y las demás opciones se las deja tal como están.

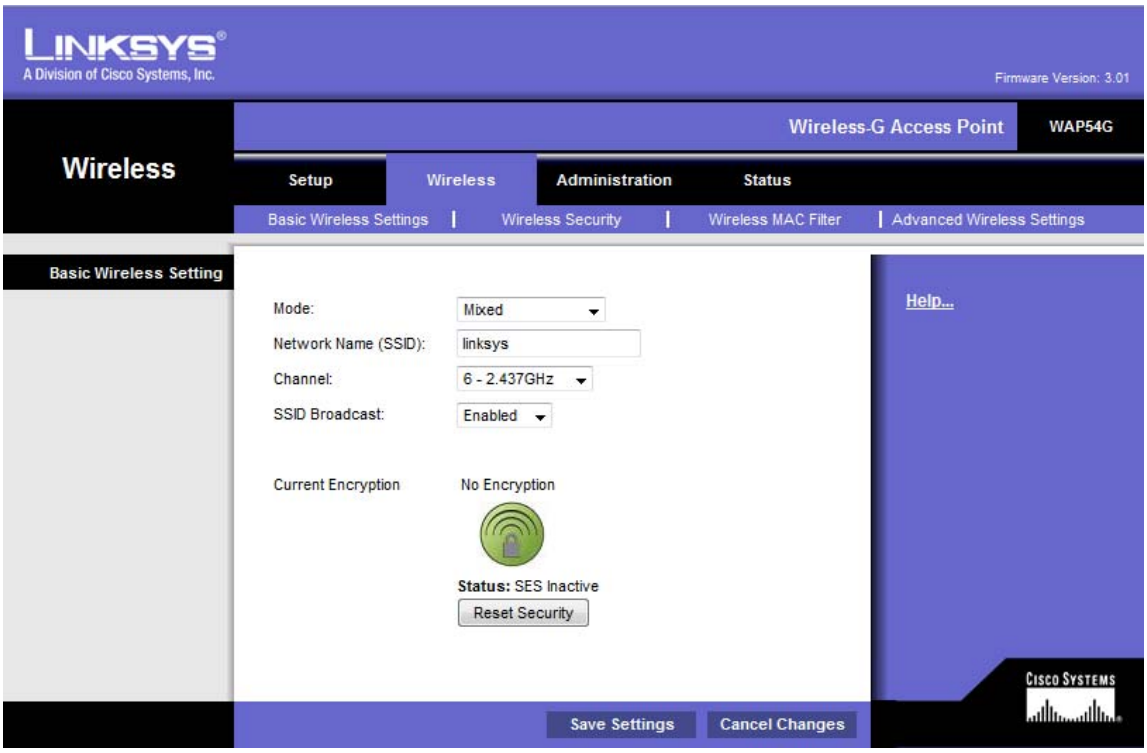

Figura 3.49: Configuración básica de la red inalámbrica

3.6.2.2 Submenú "Wireless Security".

En este submenú se elige el tipo de seguridad que se va a utilizar para red inalámbrica, en este caso se eligió la seguridad "**WPA2-Mixed"**, ya es un nivel de seguridad muy alto y la red se mantendrá protegida de ataques maliciosos. También se especifica el intervalo de tiempo en el que la clave de seguridad va a cambiar, eligiendo 3600 segundos (1 minuto), para dicha acción.

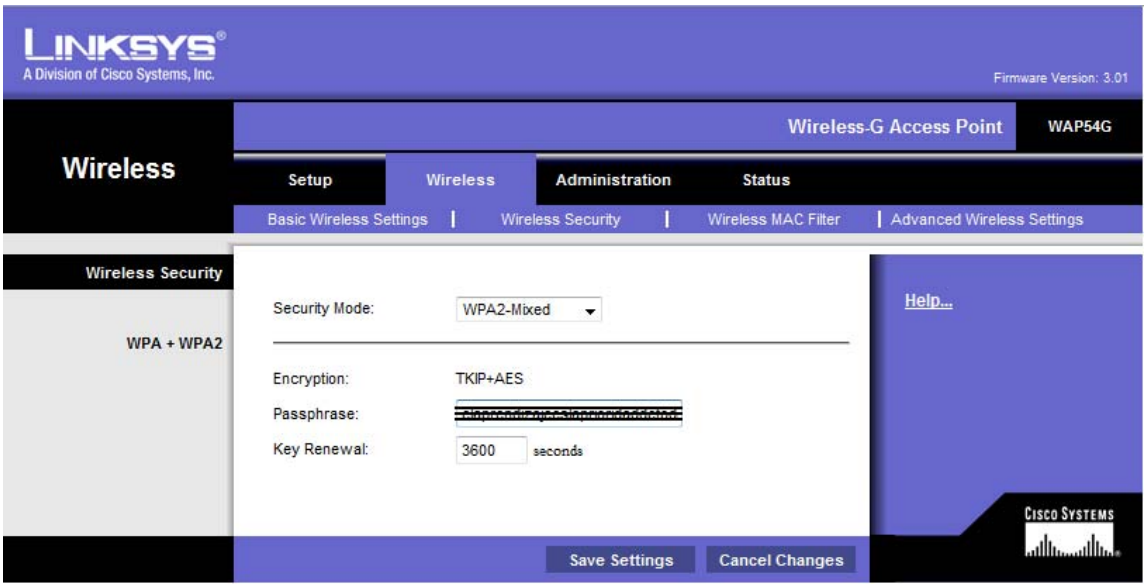

Figura 3.50: Configuración de la seguridad de la red inalámbrica

Todos los cambio realizados se los debe confirmar dando clic en **"Save Settings"**.

Las demás opciones de configuración se las dejará en los valores por defecto ya que en este caso no es necesario configurar ninguna opción adicional.

3.7 Administración remota del sistema.

Ya se ha configurado casi en su totalidad el HOTSPOT, la última configuración que se debe realizar es la habilitación de la administración remota del servidor desde otra computadora que forme parte de la red, con el objetivo de que ninguna persona, aparte del administrador tenga acceso al manejo del servidor en sí, y este se encuentre alejado de todas las personas en un sitio seguro. Para configurar esto, se debe ingresar a: **Places \Computer\Filesystem\opt\local\web\easyhotpot\htdocs\system\application\config** y abrir el archivo **"config.php"**, en este archivo se debe cambiar la siguiente línea de código:

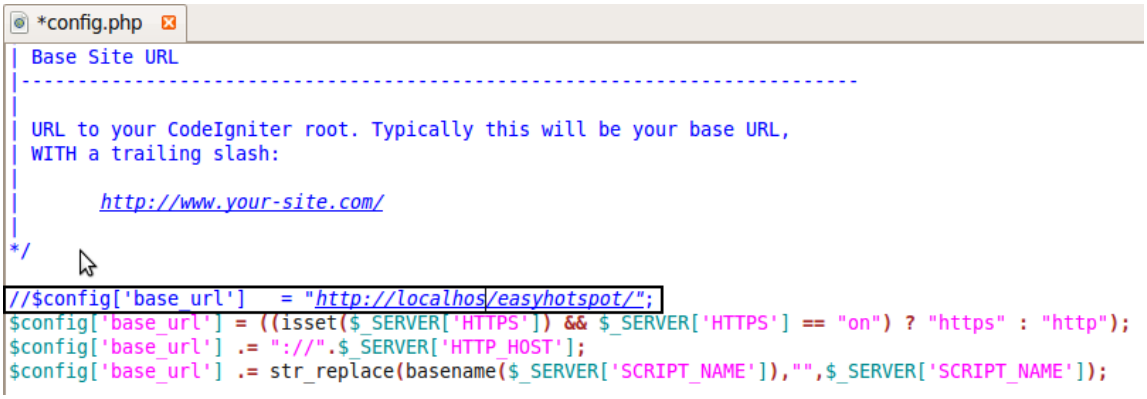

Figura 3.51: Configuración para acceso remoto al servidor

A alguna dirección IP que se encuentre en el rango de direcciones del sistema, en este caso se ha asignado la dirección **192.168.182.1**, y el código debe quedar de la siguiente forma:

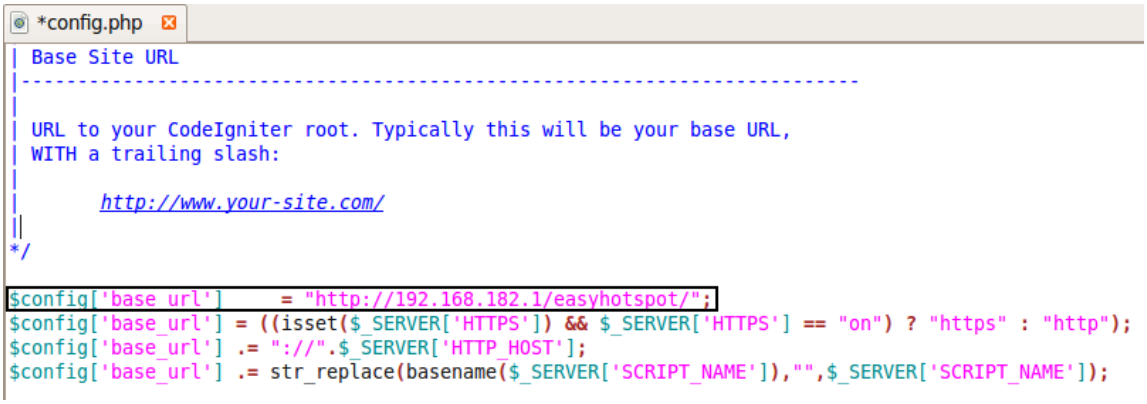

Figura 3.52: Finalizando la configuración para acceso remoto al servidor

Así se puede administrar el HOTSPOT desde cualquier computadora que forme parte de la red digitando en la barra de direcciones del navegador: **http://192.168.182/easyhotspot**, con esto se asegura que ninguna persona no autorizada tenga acceso al manejo del servidor y se evitan daños en el mismo.

3.8 Esquema del HOTSPOT.

Ya configurado el servidor y los puntos de acceso, lo que resta hacer es realizar las conexiones respectivas, la Figura 3.58 muestra el diagrama de la red mostrando la forma de conexión de cada uno de los dispositivos.

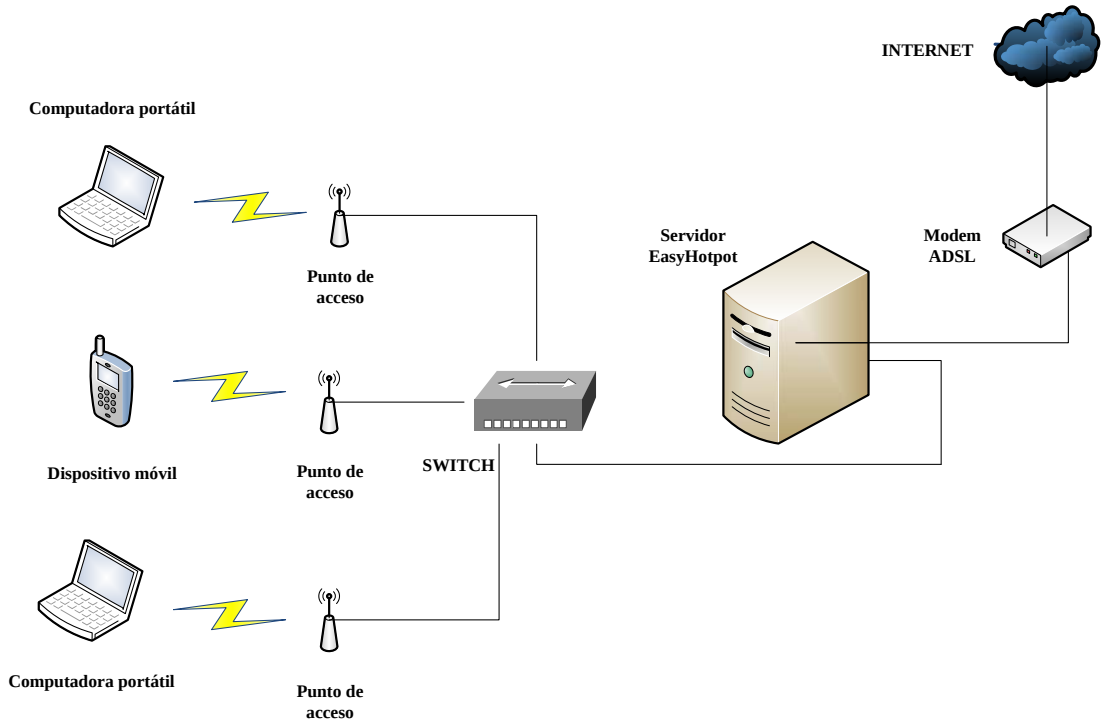

Figura 3.53: Esquema del HOTSPOT

3.9 Configuración de una computadora portátil en el HOTSPOT

Una vez realizadas las conexiones de los equipos, se va a configurar una computadora portátil, únicamente se necesita que ésta cuente con una tarjeta de red inalámbrica y un navegador de Internet y sin importar el sistema operativo.

En este ejemplo se utiliza una computadora portátil HP Pavilion dv4-1220us, con sistema operativo Windows Vista Home Premium, con tarjeta de red inalámbrica Broadcom 4322AG a/b/g y con navegador de Internet Mozilla Firefox en su versión 3.6.

Para realizar la configuración del dispositivo se debe seguir los siguientes pasos, para esto se asume que ya se ha creado un usuario en el sistema como se lo explicó anteriormente:

Primeramente hay que identificar a la red inalámbrica la cual fue llamada "**zona_wi-fi_hgpt".**

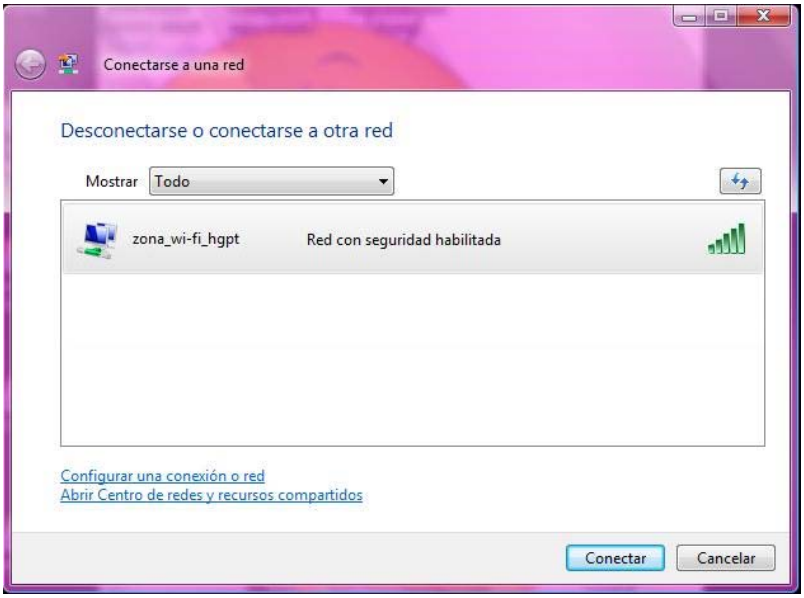

Figura 3.54: Identificando la red inalámbrica

Al dar clic en "**Conectar**" aparecerá la pantalla en donde se debe digitar al clave de red que se configuró anteriormente en el punto de acceso.

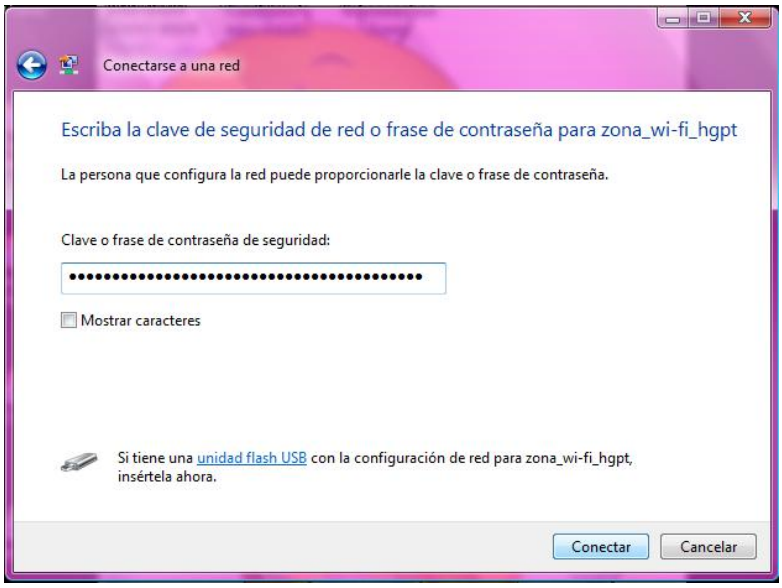

Figura 3.55: Ingresando la contraseña de la red

Ya ingresada la contraseña correctamente se debe dar clic en **"Conectar"** nuevamente y el sistema operativo indica que se está conectando a la red.

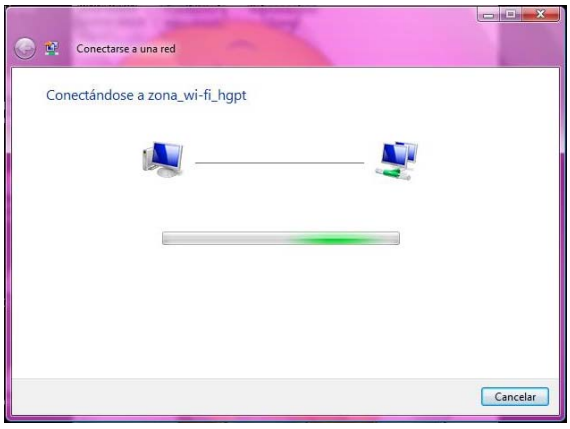

Figura 3.56: Conectándose a la red inalámbrica

Cuando el sistema operativo haya finalizado la conexión con éxito a la red aparecerá el siguiente mensaje.

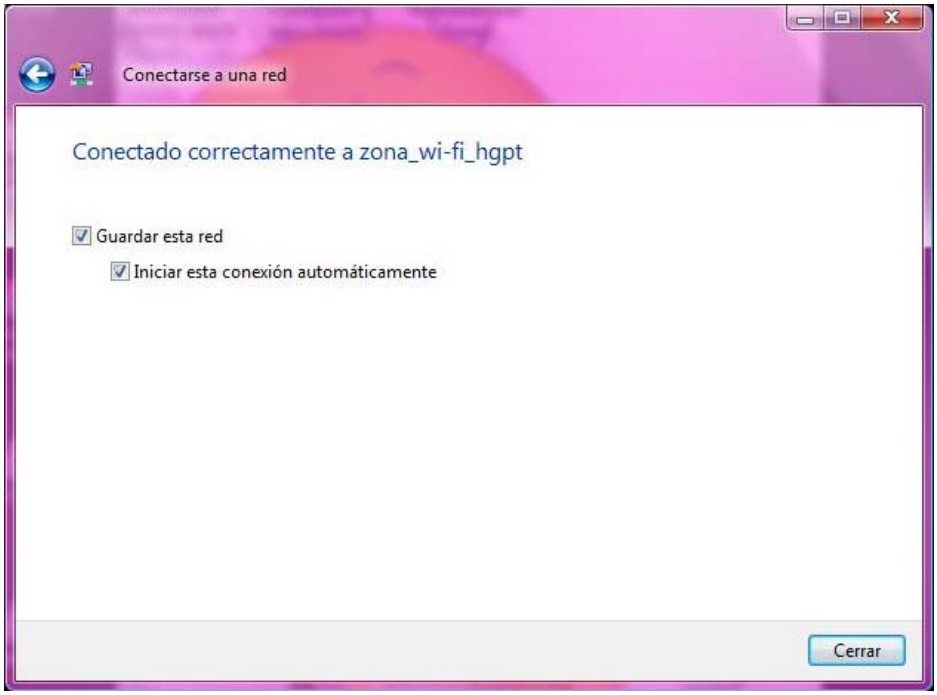

Figura 3.57: Conectándose a la red inalámbrica

Finalmente se da clic en cerrar, quedando almacenada la red y su configuración en el sistema operativo.

Ya conectado a la red, seguidamente se abre el navegador de Internet. Al ser la primera vez que se accede a la red, el navegador advierte al usuario que el certificado emitido por el servidor no es seguro. Esta advertencia es presentada por motivos de seguridad.

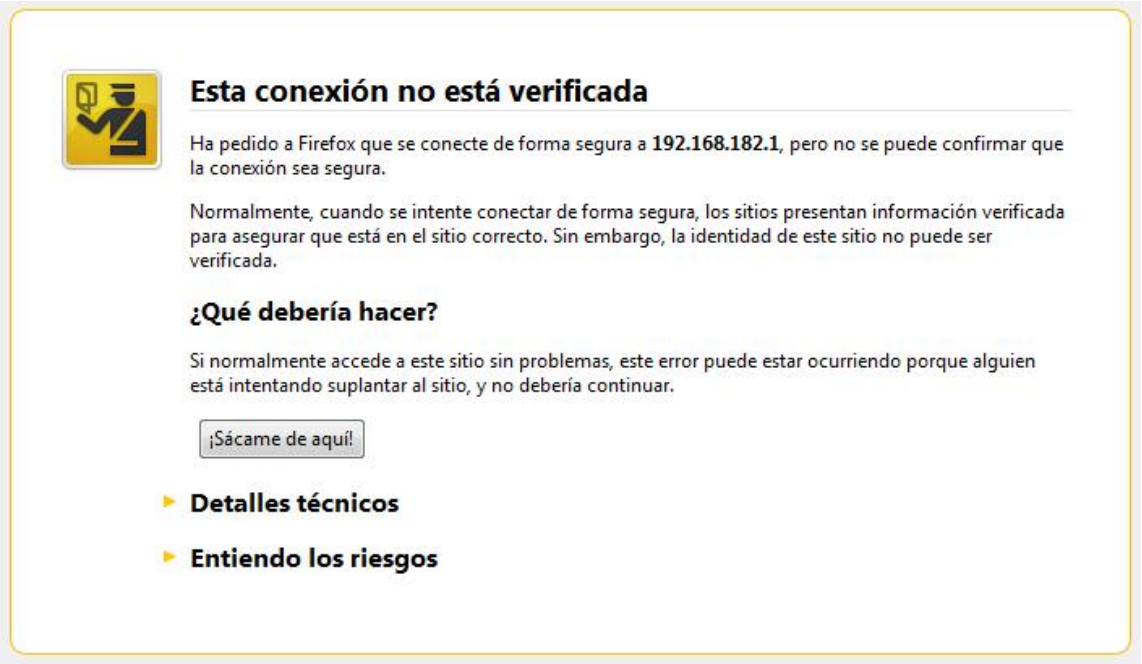

Figura 3.58: Iniciando proceso de configuración de certificado

Como se conoce la procedencia de este certificado, éste se acepta dando clic en **"Entiendo los riesgos"**, y aparecerá otra advertencia más.

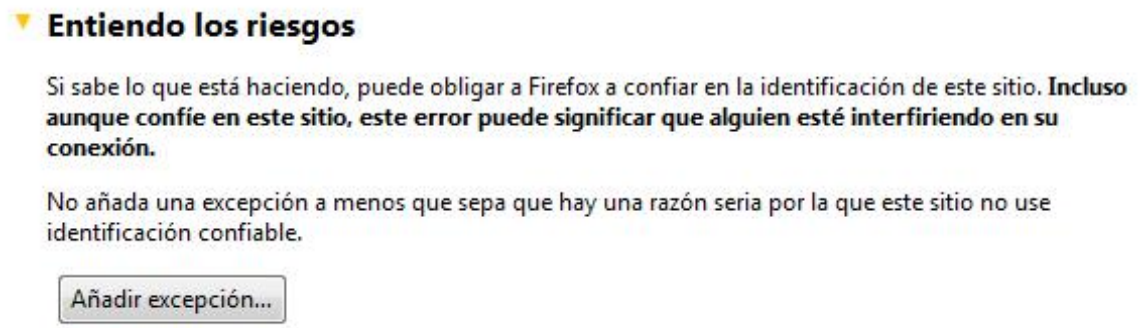

Figura 3.59: Aceptando el certificado

Ahora se da clic en **“Añadir excepción”** para confirmar que se conoce la procedencia del certificado emitido por el servidor.

Seguidamente se presenta la última advertencia de seguridad, la cual se la acepta, verificando que el certificado quede almacenado en el navegador para no volver a realizar este procedimiento las veces que se abra el navegador.

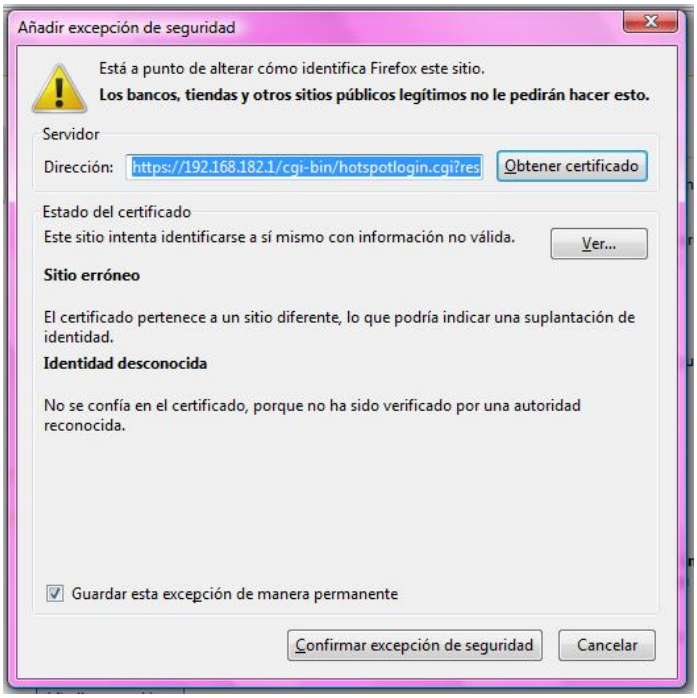

Figura 3.60: Confirmando aceptación del certificado

Al dar clic en **“Confirmar excepción”**, se guardará el certificado y finalmente se presenta la página web de presentación y validación de usuarios del HOTSPOT.

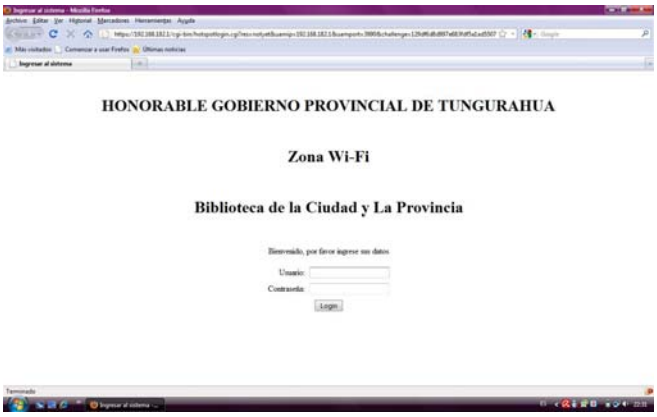

Figura 3.61: Página web de presentación y validación del HOTSPOT

Aquí se ingresa el nombre de usuario y la contraseña obtenidos anteriormente, al se dar clic en **"Login"** el sistema verifica los datos ingresados y decide si las credenciales son correctas o no, permitiendo al usuario hacer uso de los servicios de la red.

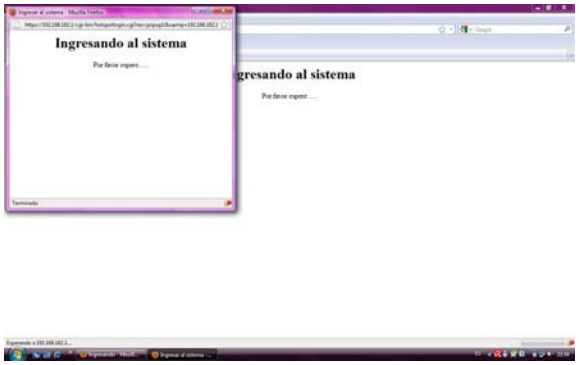

Figura 3.62: Ingresando al sistema

Si las credenciales son correctas, aparecerá una ventana indicando que el usuario se encuentra dentro del sistema indicando el tiempo restante para poder utilizar el servicio de Internet. También se abrirá una segunda ventana con la página configurada anteriormente a abrirse cuando un usuario complete el registro con credenciales válidas.

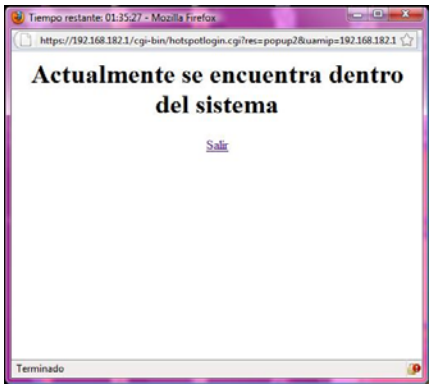

Figura 3.63: Notificación de ingreso al sistema

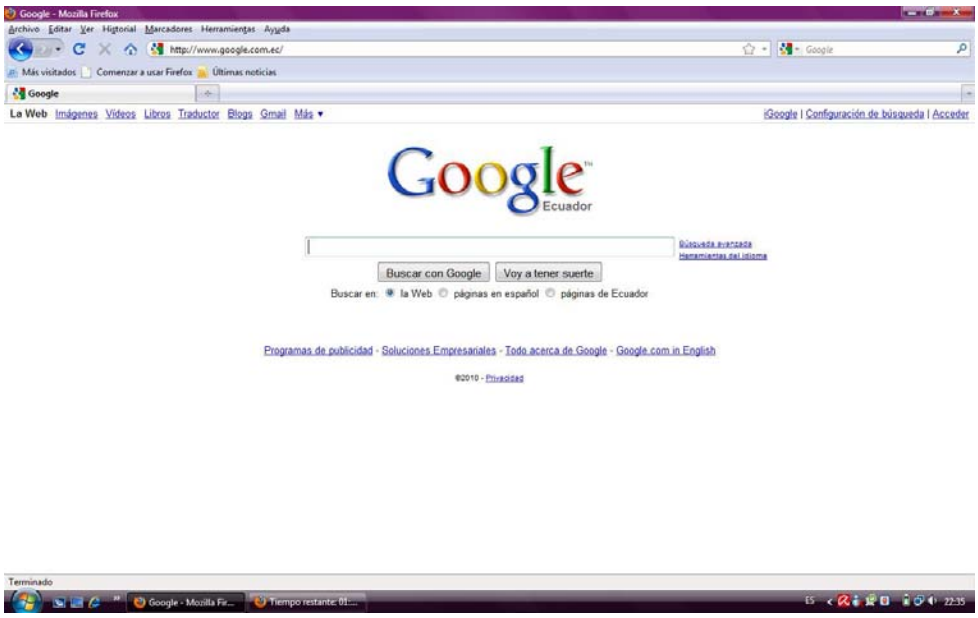

Figura 3.64: Página principal de redirección después del registro

Cuando el nombre de usuario o la contraseña son ingresados incorrectamente, aparecerá la siguiente notificación.

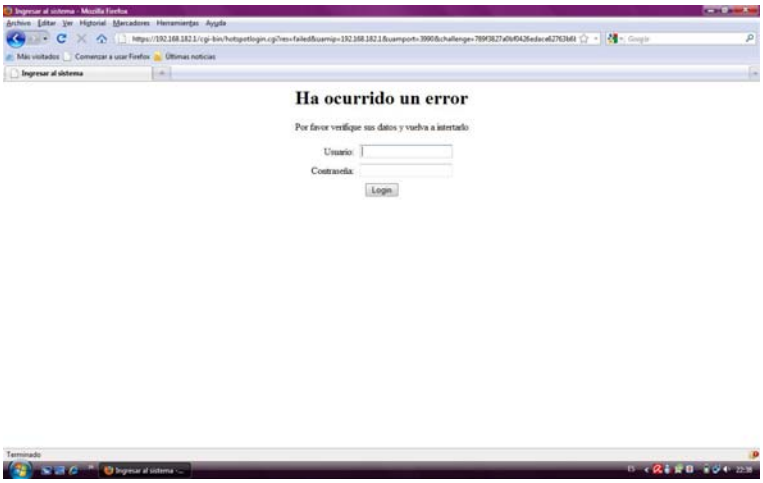

Figura 3.65: Credenciales ingresadas incorrectas

Cuando un usuario ya ha excedido el tiempo límite al que tiene derecho y trata de conectarse al servicio de internet, aparecerá el siguiente mensaje.

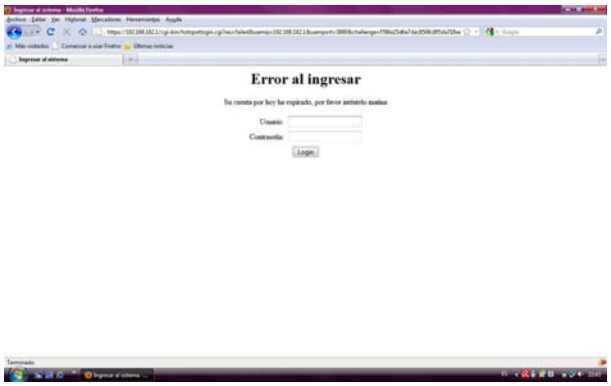

Figura 3.66: Cuenta expirada

Al momento en el que un usuario decida dejar de utilizar el Internet, debe desconectarse del sistema, esto se logra dando clic en salir en la ventana que permanece abierta indicando el tiempo restante.

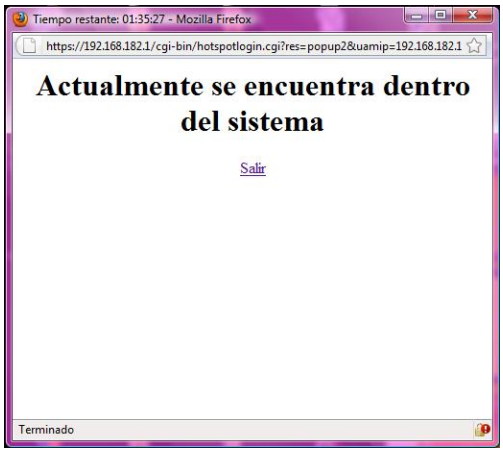

Figura 3.67: Salir del sistema

Al dar clic en **"Salir"**, el sistema alertará al usuario que ha salido del sistema y da la opción de volver a ingresar al sistema.

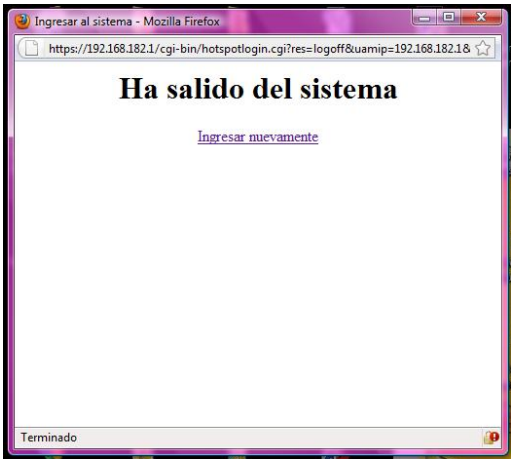

Figura 3.68: Sesión finalizada

Si el usuario decide ingresar nuevamente al sistema, aparecerá nuevamente la página web de presentación y validación de cuentas.

Si por error el usuario ha cerrado la ventana que permanece abierta indicando el tiempo restando, puede desconectarse del sistema, simplemente digitando la palabra **“splush”** en la barra de direcciones del navegador, se abrirá la página mencionada, pudiendo así el usuario desconectarse del sistema.

Cuando el usuario haya consumido el tiempo disponible al que tiene derecho (dos horas), el servicio de Internet se desconectará automáticamente y el usuario no podrá acceder al sistema hasta el siguiente día.

3.10 Configuración de un dispositivo móvil en el HOTSPOT.

Para probar la funcionalidad del HOTSPOT con dispositivos móviles, se realiza un ejemplo de conexión a la red con un iPod Touch, marca Apple, de segunda generación, cuenta con sistema operativo iPhone OS, navegador Safari y conexión a redes inalámbricas. Al igual que en el ejemplo anterior se asume que ya se ha creado un nombre de usuario y una contraseña para acceder al servicio desde este dispositivo. A continuación se detallan los pasos de configuración del dispositivo en el HOTSPOT.

Primeramente se debe identificar la red llamada **“zona_wi-fi_hgpt”**.

Figura 3.69: Identificando la red inalámbrica

Al presionar en la red, el sistema va a solicitar la contraseña de la misma, la cual deberá ser ingresada.

Figura 3.70: Ingresando la contraseña de la red inalámbrica

Ingresada la clave de seguridad de la red, se debe presionar en **"Conectar"** para validar la configuración.

Cuando el sistema haya verificado que la contraseña fue ingresada correctamente, mostrará la siguiente pantalla.

Figura 3.71: Conectado a la red inalámbrica

Para continuar con la configuración, se abre el navegador Safari, presionando su ícono.

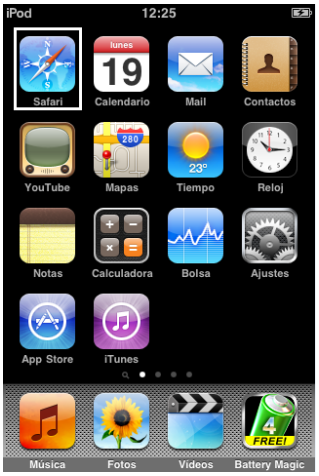

Figura 3.72: Abriendo Safari

Una vez abierto, el navegador consulta con el usuario si desea aceptar el certificado del servidor, en donde se presiona en **"Aceptar"** para continuar la configuración.

Figura 3.73: Aceptando certificado del servidor

Una vez aceptado el certificado del servidor se muestra la página web de presentación y validación del sistema.

Figura 3.74: Página de presentación y validación del sistema

En donde se debe ingresar las credenciales para acceder al servicio de internet. Si el usuario ingresa correctamente los datos, aparecerá una pantalla que indica que se encuentra dentro del sistema y el tiempo que dispone para utilizar el servicio de Internet.

Figura 3.75: Tiempo restante

Y finalmente se abrirá la página configurada en el sistema EasyHotspot, es decir la página que se abrirá cuando un usuario ingrese correctamente los datos.

Figura 3.76: Página principal de redirección después del registro

Al igual que en el ejemplo anterior si el usuario ingresa de manera incorrecta sus credenciales, aparecerá el siguiente mensaje.

Figura 3.77: Error de credenciales

Si el usuario decide dejar de utilizar el servicio de Internet, deberá ingresar en la barra del navegador la palabra **“splush”**, presionar **“Salir del sistema”**, y aparecerá el siguiente mensaje.

Figura 3.78: Sesión finalizada

Hasta aquí se ha indicado el proceso de configuración de la red en una computadora portátil y en un dispositivo móvil, demostrando totalmente el funcionamiento del HOTSPOT.

Cabe recalcar que el administrador del sistema también podrá administrar el sistema desde un dispositivo móvil, ofreciendo así un servicio completo y de cómodo uso.

3.11 Ejemplo de una página restringida por OpenDNS.

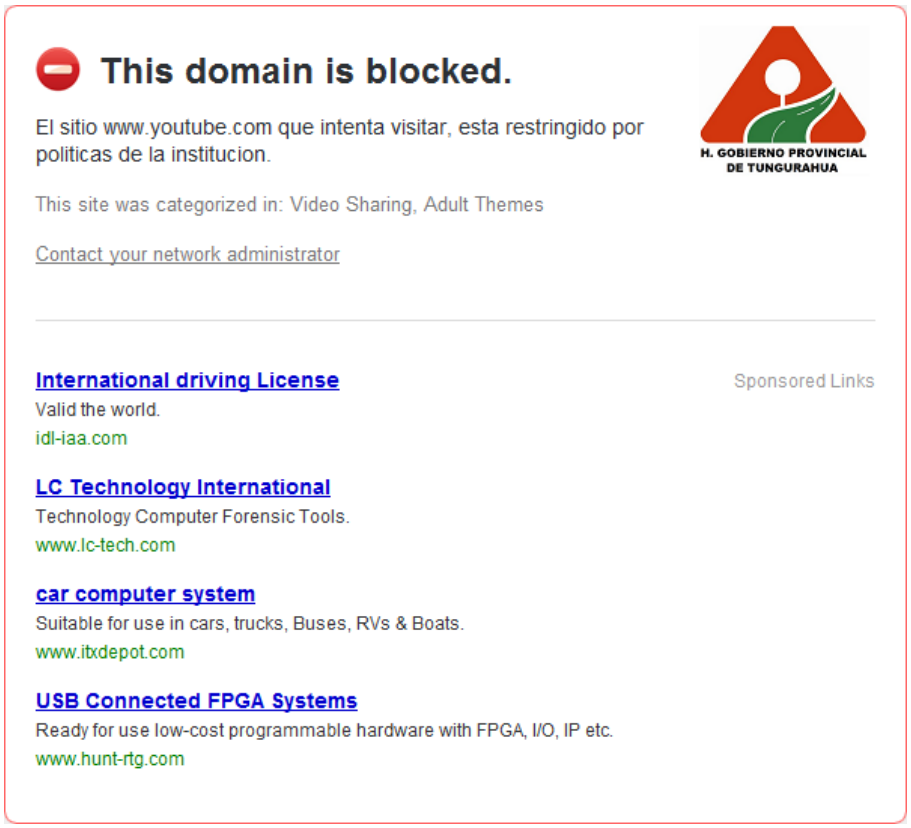

Figura 3.79: Contenido bloqueado

Finalmente se ha demostrado la configuración del sistema EasyHotspot y se ha demostrado con ejemplos prácticos la configuración de una computadora portátil y un dispositivo móvil en este sistema, demostrando su funcionalidad.

CONCLUSIONES

- En el Anexo 2 se encuentra la tabulación de las encuestas realizadas a los usuarios, lo cual indica la importancia de la implementación de este sistema, aumentando el nivel de satisfacción del usuario y confirmando el incremento de concurrencia de los mismos al servicio de Internet.

- La topología de red utiliza para el proyecto fue la red de árbol, ya que se combinan varias topologías, utilizando un servidor el cual se encarga de gestionar la red, un switch y varios puntos de acceso encargados de conectar a los diferentes terminales (computadoras portátiles y dispositivos móviles con tecnología inalámbrica) con el servidor.

- La red implementada, se la puede incluir dentro de la clasificación de redes WLAN, siendo la mejor alternativa para la implementación del HOTSPOT.

- La clase de direccionamiento IP utilizado para la implementación del HOTSPOT fue la C, ya que esta clase de direccionamiento es la suficiente para el buen funcionamiento del sistema. Como se explicó en el Capítulo II esta clase de direccionamiento soporta 254 terminales, número que se estima suficiente para abastecer la cantidad de usuarios que concurran a utilizar el servicio de Internet, existiendo 200 usuarios al día en promedio.

- Los puntos de acceso utilizados para la implementación del HOTSPOT, trabajan sobre el estándar IEEE 802.11 b y g, lo cual indica que no existe ningún problema de compatibilidad con los dispositivos inalámbricos que existen en nuestro medio.
- El sistema EasyHotspot cumple totalmente con el estándar AAA, ya que verifica la información del usuario en el momento en éste trata de acceder a la red, decide si dicho usuario tiene derecho a utilizar los servicios de la red y brinda información y estadísticas al administrador de la red para verificar el buen funcionamiento del sistema.

- El servidor utiliza métodos de autenticación combinados, emitiendo certificados de confianza a través del protocolo SSL y TLS con método de autenticación EAP-PEAP y verificando la existencia de un usuario en una base de datos. También para fortalecer la seguridad de la red, se configuró en los puntos de acceso WPA2 como seguridad de conexión a la red, por lo que el usuario para hacer uso del servicio de Internet primeramente debe conocer la contraseña de seguridad de la red y luego debe contar con un nombre de usuario y una contraseña, por lo tanto si alguien logra ingresar a la red de manera ilícita violando la contraseña de seguridad, no podrá tener acceso al Internet ya que debe contar con un nombre de usuario y una contraseña, esto confirma que el HOTSPOT cuenta con una seguridad eficaz difícil de violar. El Anexo 5 demuestra la inviolabilidad de la red inlámbrica.

RECOMENDACIONES

- Una de las recomendaciones más importantes que se debe tomar en cuenta es la verificación de los nombres que el sistema operativo asigna a las interfaces o tarjetas de red para no tener inconvenientes en la configuración del HOTSPOT.

- Actualizar constantemente el sistema operativo para mejorar su rendimiento, al mantener todas sus aplicaciones al día.

- Cambiar todas las contraseñas por defecto dentro del sistema operativo y de los puntos acceso para evitar que personas no autorizadas entren a la configuración de estos.

- Manipular con extremo cuidado el código de la página web de presentación y validación del HOTSPOT, ya que si es modificado inadecuadamente el sistema sufrirá daños graves y dejará de funcionar.

- En la configuración de los atributos del HOTSPOT, verificar que la interfaz que se encargará de asignar las direcciones IP a los usuarios sea la correcta, como se explico en el punto 3.4.3 del Capítulo III.

- Se recomienda advertir a los usuarios no ingresar información confidencial como números de tarjeta de crédito, cuentas bancarias, etc., ya que se utilizan un DNS externo al de compañía proveedora de Internet, pero por la utilidad ofrecida por

OpenDNS y como la biblioteca es orientada solamente a investigación no existe problema alguno al utilizar este servicio.

BIBLIOGRAFÍA

1. Libros.

- FERNÁNDEZ, Yago; RAMOS, Antonio; GARCÍA-MORAN, Jean.
  AAA RADIUS 802.1x - Sistemas Basados en la autenticación En Windows Y Linux/GNU Seguridad Máxima.
  Editorial: Alfaomega, Ra-Ma, 2009, 640 páginas.

- ANDREU, PELLEJERO, LESTA
  Fundamentos y aplicaciones de seguridad en redes wlan
  Editorial: ARCOMBO, EDICIONES TÉCNICAS, 160 páginas.

- Serrat Olmos, Manuel David
  Ubuntu Linux
  Editorial: Ra-Ma, 468 páginas.

2. Documentos electrónicos.

- Gentoo Lunix Wiki: Chillispot with FreeRadius and MySQL
  http://en.gentoo-wiki.com/wiki/Chillispot_with_FreeRadius_and_MySQL

- Sitio de Soporte de la ECCI: Implementación de una Red Inalámbrica con ChilliSpot, FreeRADIUS y OpenWRT
  http://soporte.ecci.ucr.ac.cr/node/15

- Howtoforge: Install OpenWRT, Chillispot, FreeRadius Based Managed Hotspot(s) Including PayPal Payment Gateway
  http://www.howtoforge.com/openwrt-chillispot-freeradius-chillifire-hotspots-including-paypal-payment-gateway.

3. Direcciones web.

- WIKIPEDIA – La Enciclopedia Libre: GNU/Linux
  http://es.wikipedia.org/wiki/GNU/Linux#Distribuciones
  Fecha de consulta: 14/10/09

- WIKIPEDIA – La Enciclopedia Libre: Distribuciones
  http://es.wikipedia.org/wiki/GNU/Linux#Distribuciones
  Fecha de consulta: 14/10/09

- WIKIPEDIA – La Enciclopedia Libre: Ubuntu
  http://es.wikipedia.org/wiki/Ubuntu
  Fecha de consulta: 14/10/09

- WIKIPEDIA – La Enciclopedia Libre: Red informática
  http://es.wikipedia.org/wiki/Red_de_computadoras
  Fecha de consulta: 20/10/09

- WIKIPEDIA – La Enciclopedia Libre: Topología de redes
  http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red
  Fecha de consulta: 20/10/09

- WIKIPEDIA – La Enciclopedia Libre: Modelo OSI
  http://es.wikipedia.org/wiki/Modelo_OSI
  Fecha de consulta: 27/10/09

- WIKIPEDIA – La Enciclopedia Libre: Cable coaxial
  http://es.wikipedia.org/wiki/Cable_coaxial
  Fecha de consulta: 29/10/09

- WIKIPEDIA – La Enciclopedia Libre: Cable de par trenzado
  http://es.wikipedia.org/wiki/Cable_de_par_trenzado
  Fecha de consulta: 29/10/09

- WIKIPEDIA – La Enciclopedia Libre: Fibra óptica
  http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica
  Fecha de consulta: 29/10/09

- WIKIPEDIA – La Enciclopedia Libre: Concentrador
  http://es.wikipedia.org/wiki/Concentrador
  Fecha de consulta: 03/11/09

- WIKIPEDIA – La Enciclopedia Libre: Conmutador (dispositivo de red)
  http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29
  Fecha de consulta: 03/10/09

- WIKIPEDIA – La Enciclopedia Libre: Enrutador
  http://es.wikipedia.org/wiki/Enrutador
  Fecha de consulta: 04/11/09

- WIKIPEDIA – La Enciclopedia Libre: Familia de protocolos de Internet
  http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet
  Fecha de consulta: 06/11/09

- WIKIPEDIA – La Enciclopedia Libre: Dirección IP
  http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

Fecha de consulta: 07/11/09

- WIKIPEDIA – La Enciclopedia Libre: Red inalámbrica
  http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
  Fecha de consulta: 09/11/09

- WIKIPEDIA – La Enciclopedia Libre: IEEE 802.11
  http://es.wikipedia.org/wiki/IEEE_802.11
  Fecha de consulta: 12/11/09

- WIKIPEDIA – La Enciclopedia Libre: Punto de acceso
  http://es.wikipedia.org/wiki/Punto_de_acceso
  Fecha de consulta: 16/11/09

- WIKIPEDIA – La Enciclopedia Libre: Hotspot
  http://es.wikipedia.org/wiki/Hotspot
  Fecha de consulta: 16/11/09

- WIKIPEDIA – La Enciclopedia Libre: Portal cautivo
  http://es.wikipedia.org/wiki/Portal_cautivo
  Fecha de consulta: 18/11/09

- WIKIPEDIA – La Enciclopedia Libre: Servidor web
  http://es.wikipedia.org/wiki/Servidor_web
  Fecha de consulta: 23/11/09

- HP Latinoamérica: Servidor HP ProLiant serie DL320 G5
  http://h10010.www1.hp.com/wwpc/es/es/sm/WF06a/15351-15351-3328412-241475-241475-3201178.html
  Fecha de consulta: 25/11/09

- Linksys Latinoamérica: Punto de acceso Linksys WAP54G
  http://www.linksysbycisco.com/LATAM/es/products/WAP54G
  Fecha de consulta: 26/11/09

- D-Link Latinoamérica: Switch D-Link DES-1008D
  http://www.dlinkla.com/home/productos/producto.jsp?idp=70
  Fecha de consulta: 27/11/09

- Chillispot: Features
  http://www.chillispot.info/features.html
  Fecha de consulta: 30/11/09

- WIKIPEDIA – La Enciclopedia Libre: Servidor HTTP Apache
  http://es.wikipedia.org/wiki/Servidor_HTTP_Apache
  Fecha de consulta: 03/12/09

- WIKIPEDIA – La Enciclopedia Libre: MySQL
  http://es.wikipedia.org/wiki/MySQL
  Fecha de consulta: 07/12/09

- EasyHotspot: Documentation
  http://easyhotspot.inov.asia/index.php/documentation
  Fecha de consulta: 10/12/09

GLOSARIO DE TÉRMINOS

- ***Aes:*** Es un esquema de cifrado adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.
- ***Ancho de banda:*** Es la transmisión de datos en la cual se envían simultáneamente varias partes de información, con el objeto de incrementar la velocidad de transmisión.
- ***dBm:*** Se define como el nivel de potencia en decibelios en relación a un nivel de referencia de 1 mW.
- ***FTP:*** es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor.
- ***Ghz:*** El gigahercio es un múltiplo de la unidad de medida de frecuencia hercio (Hz) y equivale a 109 (1.000.000.000) Hz.
- ***Gnome:*** Es un entorno de escritorio e infraestructura de desarrollo para sistemas operativos GNU/Linux.
- ***GNU:*** Proyecto iniciado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre (gratuito).
- ***HTTP:*** Protocolo usado para acceder a la Web. Se encarga de procesar y dar respuestas a las peticiones para visualizar una página web.
- ***HTTPS:*** Es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la web, generalmente para transacciones de pagos o cada vez que se intercambie información sensible por ejemplo cintraseñas.
- ***IEEE:*** Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros electricistas, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e Ingenieros en Mecatrónica, dedicada a la estandarización.

- ***IETF:*** Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.
- ***KDE:*** Es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.
- ***Mbps:*** Unidad de medida utilizada para cuantificar el flujo de de datos en relación al tiempo en segundos, representa 1000 kilobits por segundo o 1000000 bits por segundo.
- ***Md5:*** es un algoritmo que toma como entrada una cadena de cualquier longitud y genera una cadena 32 caracteres en notación hexadecimal. Se diseñó para comprobar la integridad de los datos en transmisiones de cualquier tipo.
- ***Mhz:*** Unidad de medida de la frecuencia de trabajo de un dispositivo de hardware, equivale a 10^6 hercios (1 millón).
- ***Octeto:*** Un octeto es una cantidad formada exclusivamente por ocho bits.
- ***Opensource:*** Es el término con el que se conoce al software distribuido y desarrollado libremente.
- ***Perl:*** Lenguaje de programación que toma como base otros lenguajes de programación como C, Shell, AWK, etc.
- ***Phyton:*** Lemguaje de programación mimilar habitualmente comparado con Perl, Java, Ruby, etc.
- ***POP:*** Protocolo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.
- ***SMTP:*** Es un protocolo de la capa de aplicación del modelo OSI utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.
- ***Telnet:*** Protocolo de comunicación que sirve para acceder a una computadora de forma remota, o sea como si se estuviera en ella.
- ***TKIP:*** Es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas.

- ***Yum:*** herramienta libre de gestión de paquetes para sistemas Linux.

ANEXOS

Anexo 1: Modelo de encuesta

Para confirmar la necesidad de implementar un HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad y la Provincia, se realizó encuestas a los usuarios que concurren a utilizar el servicio de Internet, a continuación se indica un modelo de la encuesta realizada a los usuarios:

MODELO DE ENCUESTA

BIBLIOTECA DE LA CUIDAD Y LA PROVINCIA

Por favor responda las siguientes preguntas, las cuales ayudarán a mejorar el servicio de Internet gratuito que ofrece la institución.

Preguntas

1. ¿Cuenta con una computadora portátil o dispositivo móvil con tecnología WIFI (conexión a redes inalámbricas)?

- Si
- No

2. ¿Cree que el número de computadores que la Biblioteca Virtual ofrece es suficiente para la atención a la ciudadanía?

- Si

- No

3. ¿En algún momento ha tenido que esperar para utilizar el servicio de internet porque no hay computadoras disponibles?

- Si Aproximadamente cuánto tiempo:

- No

4. ¿Utiliza el servicio de internet frecuentemente?

- Si

- No

5. Le gustaría trabajar en su propia computadora portátil o dispositivo móvil con tecnología WIFI (Conexión a redes inalámbricas), sin tener que esperar que hayan computadoras disponibles para realizar sus investigaciones.

- Si

- No

6. ¿Le gustaría que la biblioteca virtual cuente con un sistema en el que usted pueda acceder al servicio de Internet en su propia computadora portátil o dispositivo móvil con tecnología inalámbrica, para incrementar su nivel de satisfacción con respecto al servicio?

- Si

- No

7. ¿Si la biblioteca ofrecería este servicio, Ud. acudiría a utilizar sus instalaciones?

- Si

- No

Anexo 2: Tabulación de encuestas

Teniendo en cuenta un promedio de 200 usuarios al día que concurren al servicio gratuito de Internet, se realizó el cálculo de la muestra obteniendo como resultado 29 encuestas a realizarse.

Teniendo las 29 encuestas realizadas a los usuarios, a continuación se describe el estudio de las mismas, detallándolo pregunta por pregunta y obteniendo una conclusión de cada una de ellas.

Pregunta 1

¿Cuenta con una computadora portátil o dispositivo móvil con tecnología inalámbrica?

Los usuarios respondieron:

Si	No
26	3
Total	29

Tabla 1

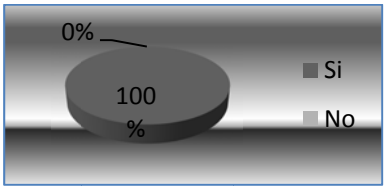

Gráfico 1

Claramente se puede notar que de los 29 usuarios encuestados, un 85% cuenta con una computadora portátil o dispositivo móvil con tecnología inalámbrica, lo que indica que la implementación del HOTSPOT con servidor RADIUS hasta el momento sería un acierto.

Pregunta 2

¿Cree que el número de computadores que la Biblioteca Virtual ofrece es suficiente para la atención a la ciudadanía?

Los usuarios respondieron:

Si	No
1	28
Total	29

Tabla 2

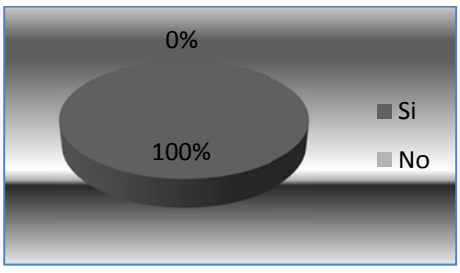

Gráfico 2

Notablemente el 97% de los usuarios encuestados cree que el número de máquinas con el que cuenta la Biblioteca Virtual no es suficiente para la atención a la ciudadanía, confirmando que existe una gran cantidad de usuarios que acuden al servicio de Internet.

Pregunta 3

¿En algún momento ha tenido que esperar para utilizar el servicio de internet porque no hay computadoras disponibles?

Los usuarios respondieron:

Si	**No**
29	0
Total	29
Tiempo Promedio	10 minutos

Tabla 3

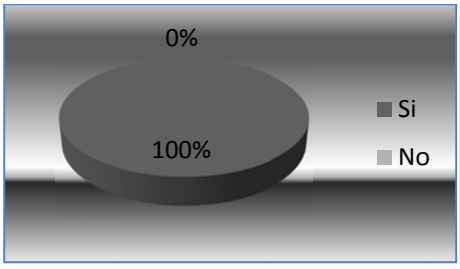

Gráfico 3

Evidentemente el 100% de los usuarios encuestados han tenido que esperar alrededor de 10 minutos para acceder a una máquina, ya que la demanda de usuarios ha incrementado mucho en los últimos meses.

Pregunta 4

¿Utiliza el servicio de internet frecuentemente?

Los usuarios respondieron:

Si	No
28	1
Total	29

Tabla 4

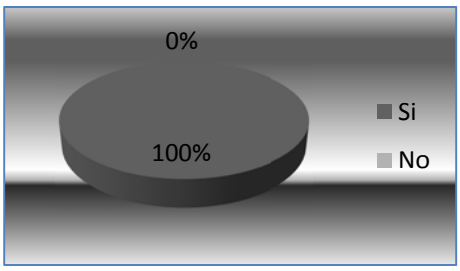

Gráfico 4

De los usuarios encuestados el 97% de estos utiliza el servicio de Internet frecuentemente, verificando una vez más que la demanda de usuarios en la Biblioteca Virtual es alta.

Pregunta 5

Le gustaría trabajar en su propia computadora portátil o dispositivo móvil con tecnología WIFI (Conexión a redes inalámbricas), sin tener que esperar que hayan computadoras disponibles para realizar sus investigaciones.

Los usuarios respondieron:

Si	No
26	3
Total	29

Tabla 5

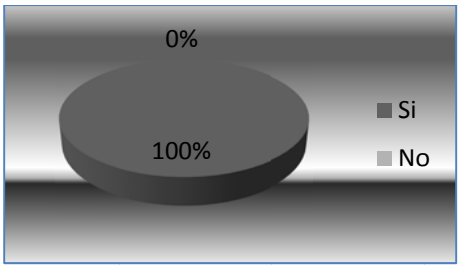

Gráfico 5

Se puede observar que el 90% que los usuarios que cuentan con una computadora portátil o un dispositivo móvil con tecnología inalámbrica desearía poder realizar sus investigaciones en sus propios equipos, lo que confirma la implementación del HOTSPOT con servidor RADIUS en la biblioteca de la ciudad y la Provincia.

Pregunta 6

¿Le gustaría que la biblioteca virtual cuente con un sistema en el que usted pueda acceder al servicio de Internet en su propia computadora portátil o dispositivo móvil con tecnología inalámbrica, incrementando así su nivel de satisfacción con respecto al servicio?

Los usuarios respondieron:

Si	No
26	3
Total	20

Tabla 6

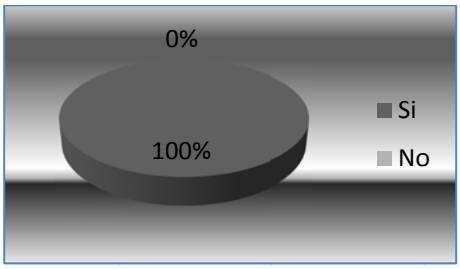

Gráfico 6

Al igual que los resultados de la pregunta anterior, los usuarios que si cuentan con una computadora portátil o un dispositivo con tecnología inalámbrica, le gustaría tener acceso al servicio de Internet en sus propios equipos y el nivel de satisfacción de los usuarios con respecto al servicio, aumentaría al contar con este servicio.

Pregunta 7

¿Si la biblioteca ofrecería este servicio, Ud. acudiría a utilizar sus instalaciones?

Los usuarios respondieron:

Si	No
29	0
Total	20

Tabla 7

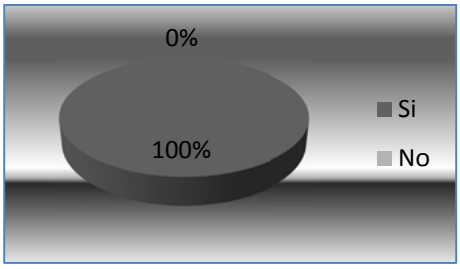

Gráfico 7

Observando estos resultados se nota que, al ofrecer este servicio los usuarios confirman su concurrencia a la institución, lo que muestra que la implementación del HOTSPOT con servidor RADIUS sería un acierto para el incremento académico de los usuarios de la Biblioteca Virtual.

Anexo 3: Configuración de páginas restringidas con OpenDNS

Dentro del capítulo 3 en el punto 3.5.3 se había mencionado que se puede configurar el nivel de seguridad del contenido web que los usuarios tienen disponible para visitar contando con varios niveles de seguridad, los cuales son:

High: Alto nivel de seguridad.

Moderate: Nivel medio de seguridad.

Low: Nivel bajo de seguridad.

None: Ningún nivel de seguridad

Custom: Nivel de seguridad configurado a gusto.

En este caso se ha elegido el nivel de seguridad **Custom**, en donde se presentan varias categorías para restringir el acceso a las páginas web. La siguiente figura indica las diferentes categorías que ofrece el sistema para bloquear el contenido web.

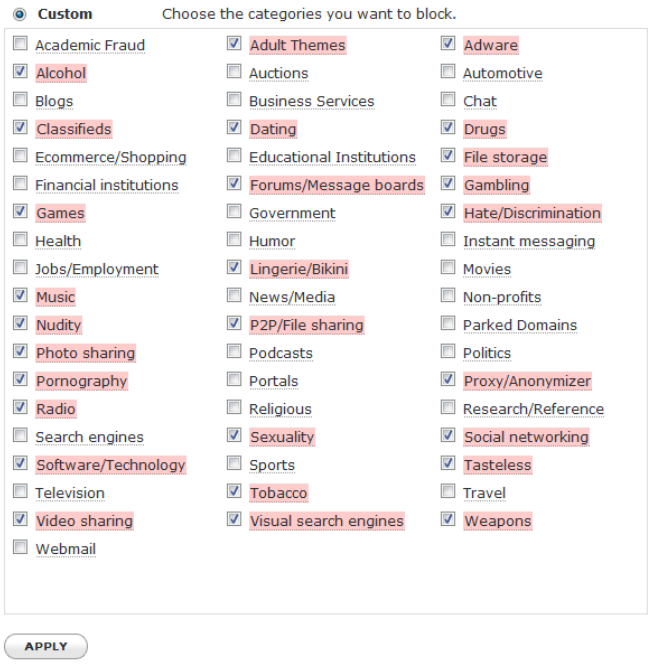

Figura 1: Categorías de restricción de páginas web

Aquí se puede marcar la categoría que se desee bloquear según el contenido que presenten las páginas web. Al dar clic en **“Apply”**, se guardarán los cambios en las restricciones de contenido de las páginas web.

Adicionalmente el sistema también ofrece la opción de mantener o no bloqueada individualmente una página web. Las siguientes figuras muestran un ejemplo.

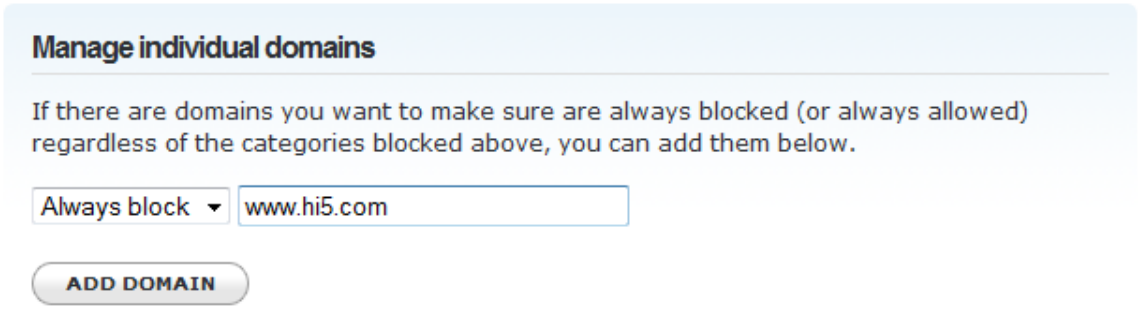

Figura 2: Mantener una página siempre bloqueada

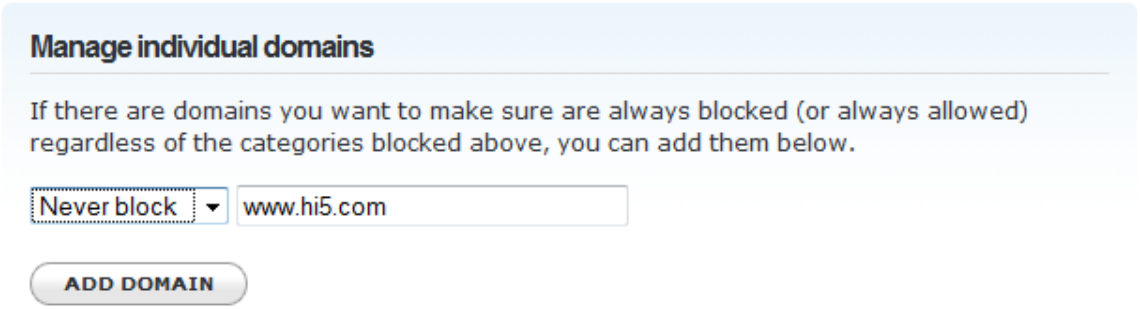

Figura 3: Mantener una página siempre con acceso

Al dar clic en **“ADD DOMAIN”**, se añadirá la configuración de acceso a la página escrita.

Anexo 4: Configuración de la página de presentación

Dentro del capítulo 3 en el punto 3.4.6.3, se indicó que cuando se ha obtenido un nombre de usuario y una contraseña para poder utilizar el servicio de Internet, el momento en el que un usuario abre su navegador el sistema lo redirigirá a la página web de registro del HOTSPOT y que el sistema operativo trae una página web de presentación por defecto, la cual se la puede personalizar de acuerdo a la necesidad del caso, lo cual se logra ingresando a: **Places\Computer\Filesystem\opt\local\web\easyhotpot\hotspot** y abriendo el archivo **"hotspotlogin.cgi"**. A continuación se presenta el código que se ha modificado en este archivo para personalizar la página de presentación.

```
if ($result == 5) {
    print "
  <p> </p>
  <h1 style=\"text-align: center;\">HONORABLE GOBIERNO PROVINCIAL DE
TUNGURAHUA</h1>
  <p> </p>
  <h1 style=\"text-align: center;\">Zona Wi-Fi</h1>
  <p> </p>
  <h1 style=\"text-align: center;\">Biblioteca de la Ciudad y La
Provincia</h1>
  <p> </p>
  <p style=\"text-align: center;\">Bienvenido, por favor ingrese sus
datos</p> ";
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurl\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\"
style=\"width: 217px;\">
    <tbody>
      <tr>
        <td align=\"right\">Usuario:</td>
        <td><input STYLE=\"font-family: Arial\" type=\"text\"
name=\"UserName\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
        <td align=\"right\">Contrase&ntilde;a:</td>
```

```
        <td><input STYLE=\"font-family: Arial\" type=\"password\"
name=\"Password\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input
type=\"submit\" name=\"button\" value=\"Login\"
onClick=\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}
```

El texto resaltado en el código es el que se ha modificado para personalizar la página web de presentación y registro del portal cautivo.

Anexo 5: Pruebas de inviolabilidad de la red inalámbrica

Existen varias distribuciones de Linux como WiFiway 3.1, WiFiSlax 3.1, Russix, etc., las cuales sirven para hacer una auditoria de la seguridad de una red inalámbrica. Para este caso se ha utilizado Wifiway 3.1. Cabe recalcar que este procedimiento se realiza por motivos académicos de aprendizaje, cualquier persona que se proponga a utilizar esta herramienta lo hará bajo su propia responsabilidad.

El funcionamiento de esta herramienta es simple, se comunica con el dispositivo inalámbrico que gestiona el tráfico de los datos (en este caso los puntos de acceso), filtrando los paquetes de datos que se envían entre un terminal y dicho dispositivo, cuando recolecta los datos suficientes descifra la contraseña de la red inalámbrica la cual se encuentra dentro de los paquetes filtrados, esto se logra gracias a unos archivos denominados “diccionarios”, los cuales contienen un gran número de caracteres con los que están construidas las contraseñas de red.

Los puntos de acceso utilizados en la implementación fueron configurados con seguridad WPA2 con encriptación TKIP+AES, este tipo de seguridad es muy confiable y muy difícil de violar, lo cual se demostrará utilizando WiFiway 3.1.

Primeramente se debe descargar la imagen ISO de esta distribución de Linux de la página http://www.wifiway.org/sp/descarga.html, luego se la obtiene en un disco utilizando Nero, Roxio, etc. Para poder manejar la herramienta se necesita una computadora portátil con tarjeta de red inalámbrica de marca Intel o Atheros, garantizando así su funcionamiento ya que la compatibilidad con estas marcas es garantizada.

Lego se introduce el disco obtenido en la unidad óptica de la computadora la cual debe iniciar desde esta unidad. Luego se cargarán los archivos necesarios para ejecutar la herramienta.

Una vez que cargados los archivos se debe ingresar el comando **“kde”**, para iniciar la herramienta.

Ya iniciada la herramienta se da clic en el menú **“K”** ubicado en la parte inferior izquierda de la barra de herramientas, hay que dirigirse al submenú **“WiFiway”**, luego a “**Suite Aircrack-ng”** y finalmente a “**airmon-ng (start mode monitor)”**, aparecerá la siguiente imagen:

Figura 1

Aquí se debe elegir la interfaz de red inalámbrica, llamada generalmente wlan0, al dar clic en aplicar se mostrará la siguiente imagen en donde hay que notar que aparezca **“monitor mode enabled on mon0”**, lo cual confirma que la tarjeta de red ha sido configurada correctamente y se podrá cerrar las dos ventanas.

Figura 2

Ya configurada la tarjeta de red inalámbrica hay que dirigirse nuevamente al menú **“K”**, seguidamente al submenú **“WiFiway”**, luego a **“Wireless”** y finalmente a **“airoscript new (spain)”**, en donde aparecerá una ventana la cual se cerrara automáticamente y luego dará a elegir la resolución de la pantalla, eligiendo la conveniente según el caso.

Figura 3

Ahora la herramienta pregunta cuál es la tarjeta de red con la que se va a trabajar, eligiendo la opción 4 y confirmándolo con la tecla **“Enter”**.

Figura 4

Con esto se obtiene el menú principal de la herramienta en donde se realizará la auditoría de la seguridad de la red, eligiendo la opción 1 para escanear las redes que se encuentran al alcance.

Figura 5

La herramienta pregunta que red se desea escanear según su tipo de seguridad, se elige WPA2 ya que es la seguridad que se utilizó.

Figura 6

Ahora la herramienta pregunta el canal en el que se va a trabajar para encontrar las redes inalámbricas, se elige la opción 1 para que busque redes inalámbricas en todos los canales.

Figura 7

La herramienta comienza a escanear las redes inalámbricas disponibles listándolas como indica la siguiente imagen.

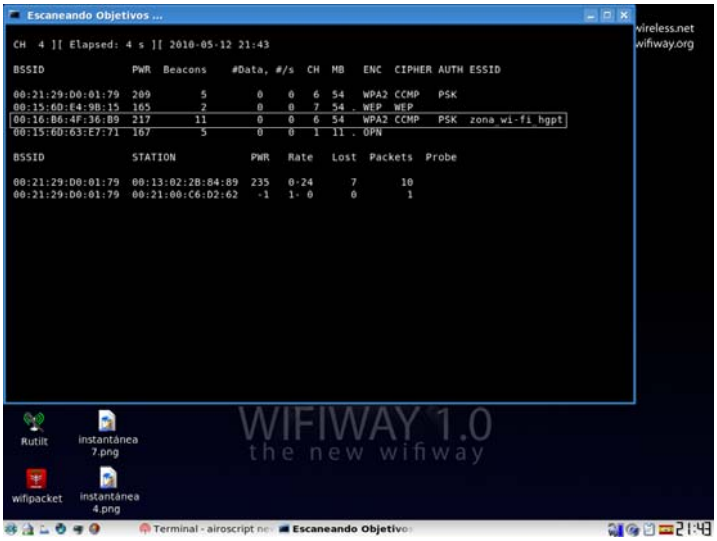

Figura 8

Detectada la red que se desea atacar, se puede cerrar esta ventana y volver al menú principal, en donde se elige la opción 2 que sirve para seleccionar la red a atacar presionando el número que presenta, en este caso la opción 5 y se confirma la acción con **“Enter”**.

Figura 9

Seguidamente la herramienta pregunta si se desea seleccionar un cliente específicp que pertenece a la red para filtrar sus datos, eligiendo la opción 2 **“No”** para que le herramienta elija a un cliente automáticamente.

Figura 10

Elegidas las opciones anteriores se regresa al menú central, en donde se debe elegir la elegir la opción 3 **“Ataques”** y luego la opción 1 para que la herramienta comience a filtrar los paquetes de datos de la red. Aquí se abrirán 3 ventanas e inicia el filtro de datos. Se debe esperar 10 minutos hasta que la herramienta obtenga los datos suficientes, fijándose siempre que en la ventana con título **“Capturando datos del canal”**, en la sección **“Data”**, no marque cero.

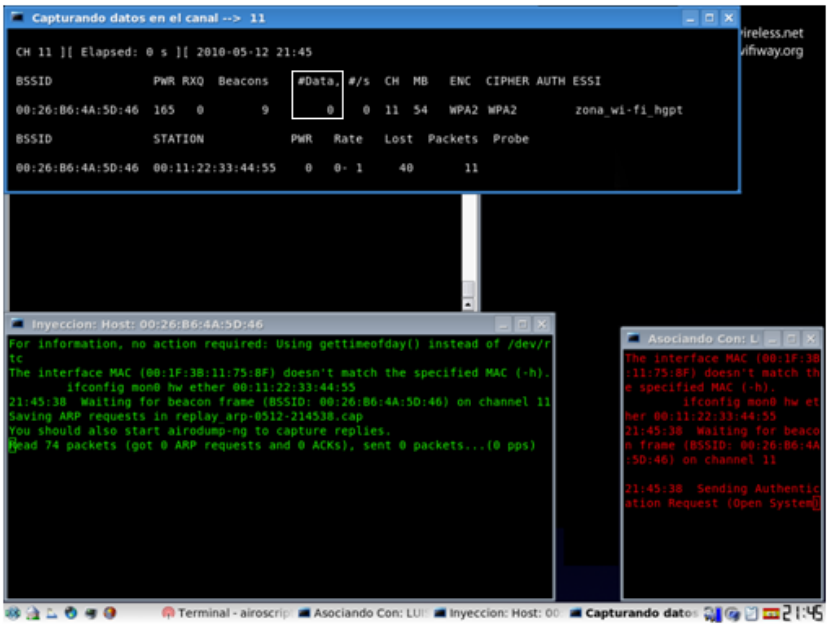

Figura 11

Luego de haber esperado el tiempo indicado, si en el paso anterior en la sección **“Data”** de la ventana **“Capturando datos del canal”** se mantiene en cero, esto quiere decir que la herramienta no ha conseguido filtrar ningún dato, verificando así que la seguridad de la red inalámbrica es eficiente.

Para terminar cabe recalcar que si algún intruso logra ingresar a la red, éste no podrá acceder al servicio de Internet ya que debe contar con un nombre de usuario y una contraseña, para lo cual deberá primero solicitar en la administración.