UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"ESTUDIO COMPARATIVO DE PORTALES CAUTIVOS BASADOS EN SOFTWARE LIBRE PARA AUTENTIFICAR Y CONTROLAR UNA RED INALÁMBRICA DE LA ESCUELA GABRIEL GARCÍA MORENO"

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN SISTEMAS Y COMPUTACIÓN

AUTOR (ES):

CARLOS MAURICIO ESTRADA ARÉVALO

ADRIANO ESCUDERO WILLIAM GEOVANNY

TUTOR:

Ing. Gonzalo Allauca Mgs

RIOBAMBA-ECUADOR

2015

Los miembros del Tribunal de Graduación del proyecto de investigación de título:

"ESTUDIO COMPARATIVO DE PORTALES CAUTIVOS BASADOS EN SOFTWARE LIBRE PARA AUTENTIFICAR Y CONTROLAR UNA RED INALÁMBRICA DE LA ESCUELA GABRIEL GARCÍA MORENO"

Presentado por:

CARLOS MAURICIO ESTRADA ARÉVALO

ADRIANO ESCUDERO WILLIAM GEOVANNY

Y dirigida por:

ING. GONZALO ALLAUCA MGS

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Danny Velasco

Presidente del Tribunal

Firma

Ing. Gonzalo Allauca

Director de Investigación

Firma

Ing. Javier Haro

Miembro del Tribunal

Firma

AGRADECIMIENTO

Mi agradecimiento va para con Dios y la Virgen Dolorosa de los estudiantes quienes me brindaron una nueva oportunidad de vida, para que pueda conseguir este anhelado sueño, también para mis padres quienes supieron cómo llevarme por el camino correcto de los valores, principios y responsabilidades, es su doble rol como padres y amigos, para mi hermana quien sintió mis problemas como los suyos y siempre estuvo allí para cuidarme y para mi hermano quien a pesar de los problemas nunca perdió la fe en mí.

Carlos M. Estrada Arévalo

Agradezco principalmente a Dios por sus bendiciones día a día, a mi madre por estar siempre a mi lado e inculcarme buenos valores, por su cariño, apoyo para seguir adelante y luchar por mis objetivos y metas, a mis hermanos por estar siempre ahí por sus buenos concejos y motivarme a ser cada día una gran persona. De igual manera agradecer a las personas que han formado parte de mi vida universitaria por su amistad, concejos, apoyo y compañía en los momentos difíciles de mi vida, especialmente a mí amigo, compañero, hermano Mauricio quien con su apoyo y ayuda durante este proyecto se ha logrado un gran resultado para ambos.

William Adriano Escudero

DEDICATORIA

Dedico este trabajo a Dios y la virgen Dolorosa de los estudiantes quienes me permitieron llegar a culminar esta meta, a mi padre quien sacrifico tiempo con su familia, la tierra que lo vio nacer y el gran amor de su vida, solo para ayudarnos a construir mi sueño y el de mis hermanos, a mi madre quien me regalo sus lágrimas y me proyecto alegría y confianza además de entregarme sus mejores momentos de la vida, a mi hermana y su único estilo de quererme y apoyarme a mi hermano por su cariño incondicional y humor que alegro mi vida y me llevaron a dar este pequeño paso.

Carlos M. Estrada Arévalo

Dedico este trabajo a mi Dios por haberme dado la vida y permitirme haber llegado hasta una de mis metas, a mi familia quien supieron como guiarme por el buen camino dándome fuerza para seguir adelante en los problemas que se presentaban, a mi madre por ser el pilar principal y demostrarme su apoyo y cariño incondicional, a mis hermanos, tíos, sobrinos quien con sus buenos consejos soy la persona que soy.

William Adriano Escudero

"Nosotros, Carlos Mauricio Estrada Arévalo y William Geovanny Adriano Escudero, somos los responsables del contenido, ideas y resultados planteados en el presente proyecto de tesis, y el patrimonio intelectual del mismo pertenece a la Universidad Nacional de Chimborazo".

Carlos Mauricio Estrada Arévalo

William Geovanny Adriano Escudero

ÍNDICE DE ABREVIATURAS

AP: Access Point**.**

ARP: Address Resolution Protocol.

CGI: Common Gateway Interface.

DHCP: Protocolo de configuración de host dinámico.

EAP: Protocolo Extensible de Autenticación.

HTTP: Protocolo de transferencia de hipertexto.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

IP: Protocolo de internet**.**

LAN: Red de área Local.

MAC: Media Access Control address.

MAN: Red de Área Metropolitana.

MD5: Message-Digest Algorithm 5.

NAS: Network Attached Storage.

PDA: Asistente digital Personal.

RADIUS: Remote Authentication Dial IN.

SSID: Service Set Identifier.

SSL: Secure Socket Layer.

TCP: Protocolo de Control Trasmisión.

TLS: Seguridad de Capa de Trasporte.

TTLS: Tunneled Trasnport Layer Security.

TUN: Dispositivo Virtual Punto Punto.

UDP: Protocolo de Datagrama de Usuario.

VLAN: Red de área local virtual.

VPN: Red Virtual Privada.

WEP: Wired Equivalent Privacy.

WLAN: Red de Area Local Inalambrica

ÍNDICE GENERAL

TABLA DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

La investigación describe el estudio comparativo de portales cautivos más representativos y basados en software libre como son: EasyHotSpot. CoovaChilli, ChilliSpot y Zeroshell, estudio que será plasmado en la implementación de un Sistema de Control de una red WIFI en la Escuela Dr. Gabriel García Moreno, que es una Institución Educativa líder en la formación académica y que pretende mejorar la calidad de sus servicios.

Los avances tecnológicos permiten el uso del internet por medio inalámbrico, en dispositivos personales como celulares, tablets, computadores portátiles, etc. Sin embargo también existen tecnologías que permiten el uso inadecuado de los recursos de internet a terceras personas ajenas a la institución que brinda el servicio.

Lo cual hace necesario la implementación de un sistema de seguridad como es el portal cautivo, el cual será instalado en un sistema operativo Linux de clase empresarial, robusto y bajo licencia GNU/GPL como es Centos 6.4. El sistema del portal cautivo utiliza varios servicios como una base de datos llamada radius elaborada en MySql la cual tendrá comunicación con un servidor de autenticación como es FreeRadius los cuales serán los encargados de aceptar o denegar el servicio de internet por medio de una Cuenta de usuario y una contraseña, adicionalmente se instalaran el servidor apache el cual dará soporte a la página de Login del portal cautivo, y se cuenta con reglas del firewall que aumenta la seguridad tanto de entrada como de salida, al activar solo los puertos necesarios para el funcionamiento del sistema.

Para facilitar la administración del portal cautivo se implementara PhpMyAdmin y DaloRadius, los cuales permiten una gestión ágil y comprensible de todos los procesos del portal cautivo.

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CENTRO DE IDIOMAS

Lic. Geovanny Armas 18 de Marzo del 2015

SUMMARY

This research work describes the comparative study of the most representative captive portals which are based on free software such as: EasyHotSpot, CoovaChilli, ChilliSpot and ZeroShell, this study will be reflected in the implementation of a Control System in a WIFI network at *Dr. Gabriel Garcia Moreno* School, which is a leading educational institution in academic training which aims to improve the quality of its services.

Technological breakthroughs allow the use of wireless internet in personal devices such as cell phones, tablets, laptops, etc. However there are also technologies that allow the inappropriate use of Internet resources to persons outside the institution providing the service.

This makes necessary to implement a security system such as the captive portal. It will be installed on an enterprise type Linux operating system, it is robust and GNU/GPL licensed such as Centos 6.4. The captive portal system uses several services such as a database called radius which is developed in Mysql and it will have communication with an authentication server like FreeRadius. They will be in charge of accepting or refusing the internet service through a user account and password, in addition, the Apache server will be installed, it will provide support for the Login page of the captive portal, and it has firewall rules increasing safety the Input and Output when enabling only the ports required for the operation of the system.

In order to facilitate the administration of the Captive Portal, PhpMyAdmin and DaloRadius are implemented; they allow a swift and comprehensive management for all the processes of the captive portal.

CENTRO DE IDIOMAS

FACULTAD DE INGENIERÍA

C.C. UNACH

CAPÍTULO I

1. MARCO REFERENCIAL

1.1 Antecedentes

La tecnología inalámbrica cobra más fuerza día a día, en el mundo donde la información digital forma parte indispensable de las actividades diarias de todas las personas, al permitir la interconectividad entre computadoras, PDA`s, etc. Sin la necesidad de permanecer en un solo lugar, cada vez son más las instituciones tanto públicas como privadas las que ofrecen disponibilidad de usar una red, como aeropuertos, centros de educación, hoteles, etc.

Ilustración 1 Zona WIFI
Fuente: http://electronics.howstuffworks.com/wifi-phone2.htm

En la Actualidad existen muchas herramientas tanto gratuitas como de paga, para administrar la tecnología inalámbrica, entre las más utilizadas se encuentran los Hotspots, sin embargo estas aplicaciones pueden ser inseguras, y utilizadas por personas maliciosas que solo desean hacer daño a los usuarios de la red inalámbrica o a la misma empresa que presta este servicio.

La Escuela Gabriel García Moreno es una institución educativa Fisco misional con 224 estudiantes, 18 docentes y 3 personas de administración donde la educación interactiva así como la descarga de información digital forma parte de las actividades diarias a realizar. La institución educativa no pudo quedar fuera del avance tecnológico por tal motivo han implantado el servicio WIFI. En sus instalaciones para brindar acceso a

internet a todos los miembros de la institución gracias al ancho de banda de 10MB simétrico.

Uno de los mayores inconvenientes del servicio inalámbrico de la institución es el de poseer una sola contraseña para la autenticación de la red en cualquier dispositivo móvil, lo que facilita el uso del internet inalámbrico a terceras personas que no están relacionadas con la institución educativa de tal manera que pueden consumir recursos de la escuela

La infraestructura que actualmente posee la institución educativa es:

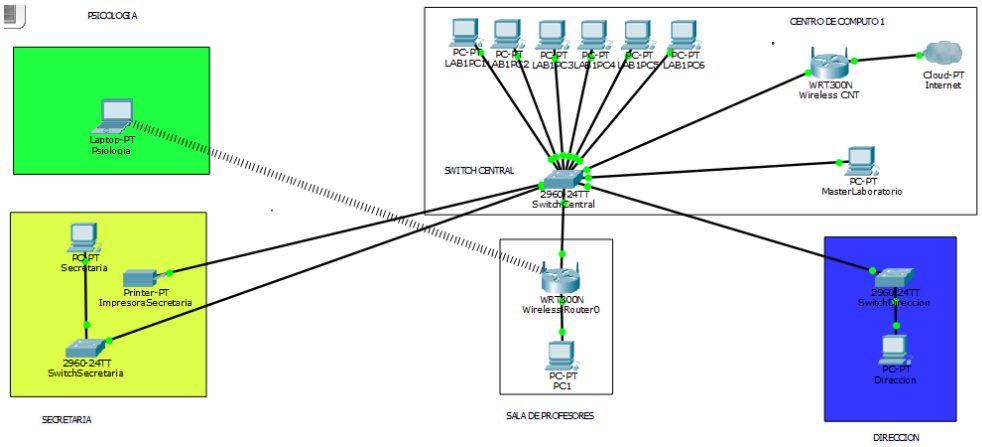


Ilustración 2 Topología Escuela Gabriel García Moreno
Fuente: Mauricio Estrada – William Adriano

La escuela Gabriel García Moreno Posee un Hotspot vulnerable y sin ningún tipo de seguridad, lo que provocaría la perdida de ancho de banda que podría ser utilizada por los miembros de la institución, y podría ser víctima de ataques por personas maliciosas.

Actualmente la institución educativa posee dos Access Point, tres switchs y 25 computadoras los cuales esta ubicados en la sala de profesores y otro en biblioteca, con las siguientes características.

Router Inalámbrico TL-WR841ND

Ilustración 3 AP Escuela Gabriel García Moreno
Fuente: http://www.tp-link.com/ar/products/details/?model=TL-WR841ND

- Velocidad inalámbrica N hasta 300 Mbps es ideal para un ancho de banda que consume o aplicaciones sensibles como el streaming de vídeo sin interrupciones, juegos en línea y VoIP
- Configuración fácilmente con encriptación WPA y una conexión segura con sólo pulsar el botón WPS
- Puente inalámbrico WDS proporciona un enlace o puente para ampliar su red inalámbrica
- La función QoS asegura la calidad de VoIP y multimedia streaming
- Wi-Fi Botón Enc / Apag permite a los usuarios simplemente activar o desactivar el radio inalámbrico
- Soporta servidor virtual, aplicación especial y host DMZ ideal para crear un sitio web dentro de su LAN
- Ofrece la función Auto-mail de registro o bitácora del sistema, adecuado para administrar el router
- Compatible con los productos 802.11b / g
- Las antenas desmontables externas permiten una mejor alineación y actualizaciones de antena más fuertes
- Diseño elegante, se puede montar en una pared o colocarse en posición horizontal sobre una mesa o escritorio

1.2 Justificación

Con el pasar del tiempo la tecnología ha ido evolucionando cada día más y más, en la actualidad tanto como las computadoras portátiles y dispositivos móviles poseen tecnología que le permiten acceder alguna red inalámbrica e incluso tener acceso al internet. Lo cual implica tener un control seguro y fácil de manejar por parte de los administradores de red.

Las instituciones tanto públicas como privadas ofrecen a sus trabajadores un acceso inalámbrico que les permita tener acceso a la red y al internet para realizar su trabajo con calidad y eficiencia. Pero el principal problema de la mayoría de las instituciones que poseen ese servicio a sus trabajadores es la seguridad y el control de autenticación de usuario ya que sus trabajadores para poder tener acceso a dicho servicio en su computadoras personales o dispositivos móviles tiene que acercarse al administrador de la red para que el personal autorizado de acceso al servicio.

Por otra parte, en este proyecto de investigación se trata de analizar y determinar un método factible que ayude al administrador de red tener un mejor control de los usuarios que necesiten del servicio de internet inalámbrico, lo cual determinaremos con la comparación de portales cautivos basados en software libre que son una herramienta segura, gratuita, fácil de implementar , lo que le facilitara al administrador de la red el manejo y control sobre la red, también proporcionara a los usuario tener un registro automatizado para acceder al servicio de internet

1.3 Objetivos

1.3.1 Objetivo General

Determinar un estudio comparativo de portales cautivos basados en software libre para autentificar y controlar la red inalámbrica de la Escuela Gabriel García Moreno.

1.3.2 Objetivos Específicos

- Investigar, comparar los diferentes tipos de portales cautivos basados en software libre que existen en la actualidad.

- Determinar los parámetros necesarios para la correcta comparación de los portales cautivos.

- Analizar el estado en que se encuentra la red inalámbrica de la Escuela Dr. Gabriel García Moreno.

- Implementar el portal cautivo que se adapte a las necesidades de la red de la escuela Dr. Gabriel García Moreno.

1.4 Hipótesis

La implementación del portal cautivo permitirá obtener un mejor control de las redes inalámbricas.

1.5 Delimitación

El tema de esta investigación será analizado, diseñado e implementado de acuerdo a los requerimientos específicos de la escuela Gabriel García Moreno, la cual necesita controlar y aumentar los niveles de seguridad en su topología de red.

Se conoce que existe un amplio ámbito de portales cautivos Open Source, sin embargo se han tomado en cuenta los portales más relevantes y utilizados en el mercado actual entre cuales tenemos:

- CoovaChilli
- ChilliSpot
- EasyHotSpot
- ZeroShell

Los cuales formaran parte del estudio a realizar.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Tecnologías y Seguridades Inalámbricas

2.1.1 Redes inalámbricas

Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías entre ellos:

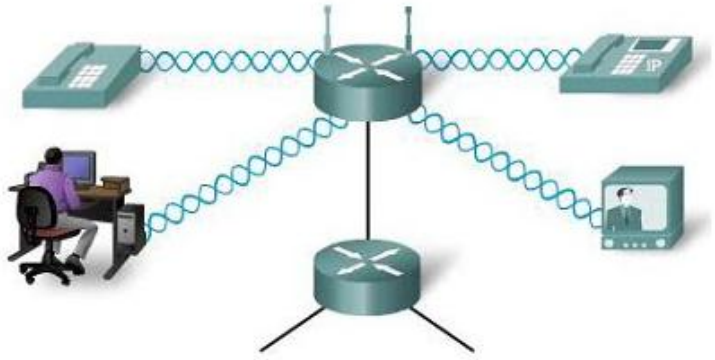


Ilustración 4 Interconexión inalámbrica entre dispositivos
Fuente: http://redytel.info/temp/img/internet_rural.gif

Permite una mayor movilidad y versatilidad en la conexión a la red. Sin embargo, la red inalámbrica no pretende ser nunca un sustituto de la red cableada, y nunca se debe utilizar para puestos de trabajo permanentes.

La infraestructura inalámbrica puede ser construida a muy bajo costo en comparación con las alternativas tradicionales de cableado. Pero construir redes inalámbricas se refiere sólo en parte al ahorro de dinero. Provee a su comunidad con un acceso a la información más sencillo y económico, la misma se va a beneficiar directamente con lo que Internet tiene para ofrecer. (Hacker Friendly LLC, 2008)

2.1.2 Tecnologías actuales para red inalámbrica

a) Wi-Fi ("Wireless Fidelity")

En español significa literalmente fidelidad sin cables. También se les denomina WLAN ("Wireless Local Área Network") o redes de área local inalámbricas, se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m). Este tipo de transmisión se encuentra estandarizado por la IEEE. (Cayufilo, 2014)

Para la transmisión es necesario el uso de antenas integradas en las tarjetas, además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de estar frente a frente el emisor y el receptor.

- Actualmente son 3 estándares básicos:

Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless B	IEEE 802.11b	11 Mbps (Megabits por segundo)	Trabaja en la banda de frecuencia de 2.4 GHz solamente, compatible con velocidades menores.
Wireless G	IEEE 802.11g	11 / 22 / 54 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente.
Wireless N	IEEE 802.11n	300 Mbps	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.

Tabla 1 Estándares Básicos 802.11
Fuente: Mauricio Estrada –William Adriano

Las Redes WiFi pueden tener muchas utilidades prácticas para todo tipo de entidades, empresas o negocios.

- Acceder a una red empresarial desde cualquier punto.
- Acceder a Internet sin necesidad de cables.
- Conectarse sin cables con un pc, un portátil, una PDA, un teléfono móvil o videoconsola con conexión WIFI.

- Servicio de HotSpot para acceso restringido por tiempo o volumen.
- Acceder a servicios de VoIP sin cables.

b) Infrarrojos

Es posible transmitir y recibir información mediante rayos infrarrojos, esta disciplina se engloba dentro de las comunicaciones ópticas no guiadas, IrDA es un estándar que define una forma de implementar el uso de la tecnología infrarroja por los fabricantes. Es una tecnología de transmisión inalámbrica por medio de ondas de calor a corta distancia (hasta 1 m), capaces de traspasar cristales. (Jimenes, 2012)

Esta tecnología, basada en rayos luminosos que se mueven en el espectro infrarrojo. Los estándares IrDA soportan una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y los 4 Mbps. Esta tecnología se encuentra en muchos ordenadores portátiles, y en un creciente número de teléfonos celulares, sobre todo en los de fabricantes líderes como Nokia y Ericsson. (Jimenes, 2012)

c) Bluetooth

Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.

Los principales objetivos son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar los cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

d) Microondas:

Se trata de comunicaciones a gran escala, muy caras y con poco uso doméstico. Las hay de dos tipos:

- **Satelitales:** se realizan a través de bases terrestres con antenas que envían señales al satélite, este se encarga de direccionarlas hacia la estación receptora con la onda amplificada para evitar pérdidas.
- **Terrestres:** se basan en conexiones denominadas punto a punto, ya que sus antenas deben estar sin obstáculos físicos para evitar fallas en la transmisión.

2.1.3 Mecanismos de Seguridad Inalámbricas

a) WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio. (ROYER, 2004)

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama. (ROYER, 2004)

b) OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aun si se activa WEP, por lo tanto es un mecanismo poco fiable. (ROYER, 2004)

c) ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permite el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

d) CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente aquellas estaciones cliente que conozcan el nombre de la red (SSID) de tal manera que este actúa como contraseña.

2.1.4 Estándar IEEE 802.11

El protocolo IEEE802.11 o WI-FI es un estándar de protocolos de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI, habilita el acceso de los dispositivos que se conectan a una red como dispositivos inalámbricos, clientes, puntos de acceso y servidores basado en un marco de autenticación superior que podría ser una pareja de identificados de usuario y contraseña o certificados. (PascuaL, 2007)

Las especificaciones del estándar definido por el IEEE denominado 802.11x comprende letras que definen las variantes de la norma 802.11 a, 802.11 b, 802.11 g, 802.11 n, abarcan las capas física (Capa 1) y la subcapa de acceso al medio (MAC) de la capa de enlace del modelo OSI.

El IEEE 802.11 puede considerarse para “Ethernet inalámbrica”. El estándar original IEEE 802.11 lanzado en 1997, tenía velocidades de 1 hasta 2Mbps y trabaja en la banda de frecuencia de 2.4 GHz con una modulación de señal de espectro expandida por secuencia directa (DSSS) o con espectro expandido por salto de frecuencia FHSS.

2.1.4.1 Elementos que actúan en el estándar 802.11

Para proporcionar una autenticación mutua extremo a extremo los tres elementos que intervienes en un sistema IEEE 802.11 son los siguientes:

- **Autenticador:** generalmente es un punto de acceso y su función es forzar el proceso de autenticación y enrutar el tráfico a las entidades adecuadas de la red.
- **Solicitante:** Generalmente es el usuario inalámbrico de solicita acceso a la red.
- **Servidor de autenticación:** lleva a cabo la autenticación de las credenciales de usuario. Generalmente se suelen emplear como servidores de autenticación remota de usuarios servidores RADIUS, aunque se pueden emplear otros tipos como por ejemplo DIAMETE. El servidor de autenticación puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso como por ejemplo priorizar ciertos tráficos o descartar otro.

No es necesario que el autenticador lleve a cabo la autenticación, en su lugar el autenticador lleva a cabo el intercambio de tráfico de autenticación entre el solicitante y el servidor de autenticación. Entre el solicitante y el autenticador el protocolo empleado es el IEEE 802.11. El protocolo entre el autenticador y el servidor de autenticación no está definido en el estándar IEEE 802.11 aunque generalmente se usa RADIUS.

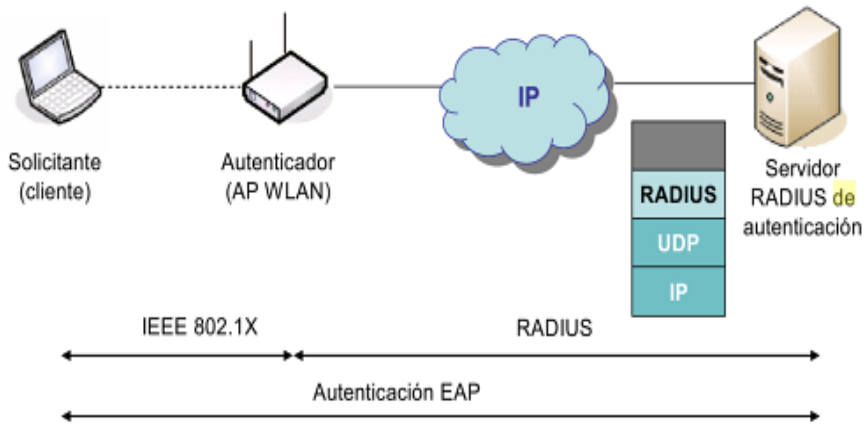


Ilustración 5 Autenticación EAP
Fuente: http://help.globalscape.com/help/eft6-3/mergedProjects/eft/radius_for_user_authentication.htm

Cuando el usuario se conecta a un punto de acceso que soporta IEE802.11 comienza el intercambio de mensajes de autenticación EAP entre ambos para levar a cabo la autenticación de usuario contra el servidor de autenticación.

2.1.5 Protocolo EAP

El estándar 802.11 utiliza un protocolo de autenticación llamado EAP (Extensible Authentication Protocol) Protocolo de autenticación extensible (EAP) que admite distintos métodos de autenticación que utilizan intercambios de credenciales e información de longitudes arbitrarias. EAP se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado. EAP proporciona una arquitectura estándar para aceptar métodos de autenticación adicionales junto con PPP.

El protocolo EAP es un intermediario entre un solicitante (la estación de trabajo inalámbrica) y el servidor de autenticación que permiten la comunicación entre ambos.

Mediante EAP, se pueden admitir esquemas de autenticación adicionales, conocidos como tipos EAP. Entre estos esquemas se incluyen las tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados. EAP, junto con los tipos de EAP seguros, es un componente tecnológico crítico para las conexiones de red privada virtual (VPN) seguras. Los tipos EAP seguros, como los basados en certificados, ofrecen mayor seguridad frente a ataques físicos o de diccionario, y de investigación de contraseñas, que otros métodos de autenticación basados en contraseña, como CHAP o MS-CHAP.

El sistema de autenticación puede ser un servidor RADIUS situado en la red local.

Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que

coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.

- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

De lo que se ha observado, el protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.11, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

2.1.6.1 Tipos de autenticación EAP

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

a) EAP-TLS

Un tipo de método de autenticación que utiliza el protocolo de autenticación ampliable (EAP) y un protocolo de seguridad denominado seguridad del nivel de transporte (TLS). EAP-TLS utiliza certificados que usan contraseñas. La autenticación EAP-TLS admite la gestión de claves WEP dinámicas. El protocolo TLS está diseñado para asegurar y autenticar la comunicación a través de una red pública mediante la codificación de datos. El Protocolo de enlace TLS permite que el servidor y el cliente provean

autenticación mutua y negocien un algoritmo y claves de codificación antes de transmitir los datos.

b) EAP-TTLS

Es una versión simplificada de EAP-TLS. Su principal ventaja es que no requiere la instalación de certificados digitales en cada equipo de usuario, lo que simplifica su despliegue pero conserva su buen nivel de seguridad.

El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. En TTLS (Seguridad del nivel de transporte de túnel), el cliente utiliza EAP-TLS para validar el servidor y crear un canal TLS codificado entre el cliente y el servidor. El cliente puede utilizar otro protocolo de autenticación. Por lo general, los protocolos basados en contraseña desafían un canal TLS codificado no expuesto. En la actualidad, la implementación TTLS admite todos los métodos definidos por EAP, al igual que varios métodos antiguos (PAP, CHAP, MS-CHAP y MS-CHAP-V2).

c) PEAP

PEAP es un nuevo tipo de autenticación bidireccional del Protocolo de autenticación ampliable (EAP), es decir que el AP (punto de acceso) también debe autenticarse en el cliente. IEEE 802.11 diseñado para sacar provecho de la seguridad del nivel de transporte EAP (EAP-TLS) del lado del servidor y para admitir varios métodos de autenticación, los cuales incluyen las contraseñas de usuarios, las contraseñas temporales y las tarjetas de testigo genérico ha creado dos subversiones: PEAP-EAP-MS-CHAPv2 que está basada en una autenticación mediante contraseñas por lo que no requiere ningún certificado digital, y PEAP-EAP-TLS que, está sí, requiere certificados digitales y por tanto del despliegue de una PKI (public key infrastructure). Una PKI representa un conjunto de tecnologías (entre otras un servidor RADIUS y un servidor de certificados) que permiten general, administrar, y autenticar los certificados digitales.

d) LEAP

Es una versión del Protocolo de autenticación ampliable (EAP). El Protocolo de autenticación ampliable ligero (LEAP) es un protocolo de autenticación ampliable

desarrollado por Cisco que proporciona un mecanismo de autenticación desafío-respuesta y permite la asignación de claves dinámica.

Versión apenas más segura que EAP-MD5. También es atacable mediante el método "Man-in-the-middle" ("el reenviador pirata")

e) EAP-MD5

Message Digest EAP son considerados la forma más simple de EAP. Transfiere un hash con el nombre de usuario, su contraseña y una cadena arbitraria. El servidor utiliza la clave en texto claro y la cadena arbitraria para generar su propio hash, el mismo que es comparado con el hash entrante.
Esta versión está basada en el intercambio de una contraseña (Pre-Shared Key). No gestiona la actualización dinámica de las claves WEP y, por este motivo, no resulta mucho más segura que la norma anterior. La identificación se efectúa en sentido único (solo el usuario se identifica en el PA) por lo que es susceptible de ser atacada mediante el método "Man-in-the-middle". Su ventaja es que no requiere de un servidor RADIUS

f) EAP-SIM

El Protocolo de autenticación ampliable para el Módulo de identidad de abonado de GSM (EAP-SIM) es un mecanismo de autenticación y distribución de claves de sesión. Utiliza el Módulo de identidad de abonado (SIM) del Sistema global para las comunicaciones móviles (GSM). EAP-SIM utiliza una clave WEP basada en sesión dinámica, que se deriva del adaptador del cliente y el servidor RADIUS, para codificar datos. EAP-SIM requiere que el usuario escriba un código de verificación del usuario, o PIN, para la comunicación con la tarjeta de Módulo de identidad de abonado (SIM). La tarjeta SIM es una tarjeta inteligente que se utiliza en redes celulares digitales basadas en Global System for Mobile Communications (GSM). RFC 4186 describe EAP-SIM.

g) EAP-AKA

EAP-AKA (Método de protocolo de autenticación ampliable para la concordancia de claves y autenticación UMTS) es un mecanismo de autenticación y distribución de

claves de sesión que utiliza el Módulo de identidad de abonado (USIM) del Sistema universal de telecomunicaciones móviles (UMTS). La tarjeta USIM es una tarjeta inteligente especial utilizada con redes de telefonía móvil que permite validar a un usuario determinado con la red.

2.1.6 Protocolo RADIUS

La gestión de líneas conmutadas para acceso a Internet de un gran número de usuarios requiere un importante soporte administrativo particularmente, se hace necesario gestionar aspectos como la autenticación de los usuarios, la autorización de los accesos y tarificación de los servicios.

Con el fin de desempeñar los cometidos referentes a la gestión, el proveedor de acceso debe disponer de cierta información sobre cada usuario que tenga concertado un servicio de acceso a internet a través de él. En concreto, se precisa registrar:

- Información de autenticación, como el nombre de usuario y la contraseña.
- Información de configuración sobre el tipo de servicio concreto que se ofrece a cada usuario

El protocolo RADIUS (Remote Authentication Dial In User Service) (Dial de autenticación remoto para acceso a servicios) permite transportar dicha información sobre los usuarios desde la base de datos donde se halla almacenada de forma centralizada (servidor de autenticación o servidor RADIUS) hasta los servidores de acceso a la red.

Aunque inicialmente fue desarrollado para llevar a cabo tareas de autenticación, el protocolo RADIUS ha sido ampliado para transportar información sobre contabilidad desde el servidor de acceso a la red a otro servidor (servidor de contabilidad RADIUS).

El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso que se ejecuta en UNIX o una máquina del Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados y a los actos en la respuesta se vuelve qué. Los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el

cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación

Esta figura muestra la interacción entre un usuario de marcación de entrada y el servidor y cliente RADIUS.

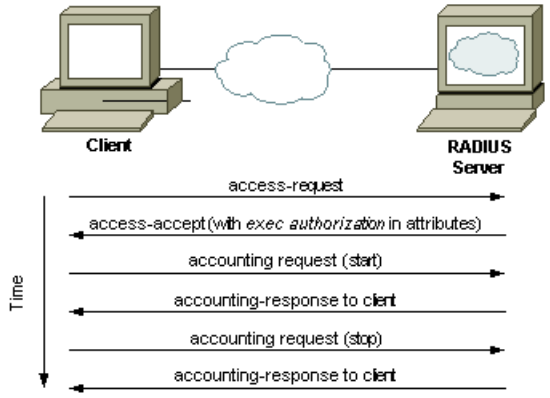


Ilustración 6 Protocolo Radius
Fuente: http://brixtoncat.esdebian.org/27318/comparativa-tacacs-radius

1. El usuario inicia la autenticación PPP al NAS.NAS
2. NAS le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña) o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña).
3. Contestación de usuario
4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.
5. El cliente RADIUS actúa con dependencia de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar.

Las funciones de un servidor RADIUS se resumen con las siglas "AAA" que significan: Autenticación, Autorización y Anotación. Los hacedores de servidores no reciben conexiones directas de los clientes sino que interactúan con las aplicaciones del cliente en otros equipos de la red.

2.1.7.1 Como trabaja RADIUS

RADIUS desempeña tres funciones primarias, éstas son: Autentificación, Autorización y Contabilidad (Accounting).

1. Autenticación

El protocolo RADIUS adopta el modelo cliente/servidor, donde el servidor de acceso actúa como cliente del servidor RADIUS, y suele ejecutarse sobre una conexión UDP (puerto 1812). Las transacciones entre ambos debido a los requisitos de seguridad implícitos en este tipo de servicio, son autenticadas mediante el uso de una clave secreta compartida, que nunca se transfiere a través de la red.

El proceso de autenticación mediante RADIUS de un usuario que desea acceder a una red a través del servidor de acceso se representa en la figura 6 anterior.

Opcionalmente, el procedimiento de autenticar puede incluir comprobar la dirección de red del usuario o el número de teléfono de llamada para verificar si se trata de los detalles esperados para ese usuario. La adición de una dirección en la autenticación sin embargo, restringe el acceso del usuario a una ubicación. El servidor RADIUS tiene un "secreto compartido" que el equipo que intenta conectarse también debería tener almacenado. Esto es por lo general en la forma de un sistema de cifrado. El servidor RADIUS devuelve una frase de comprobación de la RAS, el cual lo reenvía a la computadora del usuario. El usuario entonces encripta la frase, al igual que el servidor RADIUS. Si la respuesta devuelta por el usuario coincide con la frase de cifrado en el servidor RADIUS, el usuario ha demostrado su identidad.

2. Autorización

El servidor RADIUS mantiene una lista de direcciones de protocolo en Internet e instruye al RAS para asignar al cliente como parte del proceso de autorización. ISP no tiene tantas direcciones IP como clientes. Cada computadora conectada a Internet tiene que tener una dirección IP. Todos los paquetes de datos de solicitud que se envían a los servidores deben llevar la dirección IP de ese cliente para que el servidor sepa dónde

enviar la respuesta. Sin embargo, el cliente no tiene que tener la misma dirección IP a perpetuidad, sólo por la duración de una sesión

3. Contabilidad

El protocolo RADIUS ha sido ampliado para posibilitar su uso como medio de transporte de información de contabilidad sobre los usuarios desde el servidor de acceso hasta un servidor centralizado, que se denomina servidor de contabilidad RADIUS.

Las funciones de contabilidad del servidor RADIUS permiten al ISP ofrecer diferentes niveles de servicio a diferentes clientes que pagan diferentes tasas. La función principal de los procedimientos de anotación de RADIUS es para registrar la longitud de tiempo que el cliente está conectado. Una vez completados los procesos de autenticación y autorización, el servidor de acceso envía un mensaje de inicio al servidor RADIUS. Cuando el usuario cierra la sesión, el servidor de acceso envía un mensaje de detención. El servidor RADIUS registra el período de tiempo entre el inicio y detiene los mensajes para cada sesión de cada usuario.

En dicha aplicación del protocolo, se siguen los pasos enumerados a continuación:

1. Cuando se inicia la sesión con un usuario, el servidor de acceso cliente origina un paquete de inicio de contabilidad, proporcionando la identificación del usuario además describe el tipo de servicio que se va a ofrecer.
2. El servidor de contabilidad RADIUS responde con un paquete de confirmación e indica que ha recibido correctamente esa información.
3. Al finalizar la sesión, el cliente genera un paquete de fin de contabilidad, y detalla: el tipo de servicio que se ofreció, la causa de que termine la sesión (a petición de usuario, debido al fin de la temporización de un detector de inactividad en la línea, por error del usuario o del servidor, etc.) y, opcionalmente, estadísticas sobre la misma (tiempo transcurrido, número de octetos enviados y recibidos, números de paquetes enviados y recibidos, etc.)
4. Igual que al inicio del servicio, el servidor devuelve una confirmación, además señala con ellos que el paquete anterior se ha recibido con éxito.

También es posible el envío de actualizaciones de l información de contabilidad intermedias, antes de que concluya la sesión con el usuario. Para ellos se envían

paquetes de fin de contabilidad, pero sin incluir el campo que informa sobre el motivo del cierre de la sesión, con lo cual el servidor RADIUS entiende que la sesión todavía sigue en curso.

2.1.7 FreeRadius

FreeRadius es un servidor RADIUS de código abierto, rápido, flexible, configurable y con soporte de protocolos de autenticación. Es uno de los más populares servidores Radius, y es totalmente software libre (licencia GPL v2).

En la mayoría de los casos, la palabra FreeRadius se refiere al servidor RADIUS.

FreeRadius es un sistema modular, de alto rendimiento y rica en características RADIUS suite con servidor, cliente radio, bibliotecas de desarrollo y numerosos adicional RADIUS utilidades relacionadas.

Como la suite de código abierto estreno RADIUS se incluye como un paquete estándar con numerosos sistemas operativos, tiene paquetes binarios para muchos otros y tiene fuente disponible que es conocido por construir en casi cualquier cosa. Despliegues de producción incluyen instalaciones a gran escala que comprenden múltiples AAA servidores con más de diez millones de usuarios y millones de solicitudes por día. Es compatible con la solicitud de proxy, con conmutación por error y equilibrio de carga, así como la posibilidad de acceder a muchos tipos de bases de datos back-end. Diferentes clases de autenticación solicitudes pueden desencadenar el acceso de diferentes de autenticación y autorización de bases de datos (con caída en cascada de vuelta), y de Contabilidad registros se pueden grabar simultáneamente en varias bases de datos y directorios de almacenamiento diferentes.

2.1.8.1 Características

- FreeRadius viene con soporte para bases de datos LDAP, MySQL, PostgreSQL y Oracle.

- Soporte de protocolos de autenticación como EAP, EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, y Cisco LEAP.
- FreeRadius dispone de muchas características de los servidores de autenticación RADIUS, a continuación se redactan las más relevantes.

1) **FreeRadius ha sido compilado y se ha probado su funcionalidad en las siguientes plataformas**:
   a) Linux (todas las versiones)
   b) FreeBSD
   c) NetBSD
   d) Solaris

2) **Plataformas en las que es soportado pero no ha sido completamente probado**
   a) HP/UX
   b) AIX
   c) MINGW32, CygWin (Unix-style environment under Windows NT)
   d) SFU (or Interix, for Windows XP)

2.2 Portales Cautivos

Un portal cautivo es un software o hardware conectado a una red que vigila y controla el tráfico http y fuerza a los usuarios a pasar por una página especial si quieren navegar por internet. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifique. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede controlar el ancho de banda usado por cada cliente

Generalmente, el sistema portal cautivo utiliza un navegador web como un dispositivo de autenticación que presentan las condiciones de uso y política de la empresa.

Un portal cautivo se suele utilizar en las redes públicas en donde un cliente es obligado a pasar por una página web de autenticación. Los portales cautivos normalmente se encuentran en las redes públicas como hoteles, bibliotecas, aeropuertos entre otras como una manera para que el proveedor fuerce a un usuario a aceptar los términos de servicio, a pagar por el uso, o autenticar antes de acceder a internet.

Un portal cautivo es muy útil a la hora de gestionar una red inalámbrica Wi-Fi, ya que se puede controlar los usuarios que se conectan a nuestra red, asignándoles un nombre de usuario y contraseña, ancho de banda y un tiempo limitado, con lo cual se está brindándole el acceso a internet por el tiempo y forma que nosotros queramos.

2.2.1 Tipos de portales cautivos

a) Por Software

Entre los distintos sistemas de portal cautivo con software libre se puede señalar

- EasyHotSpot
- CoovaChilli
- ChilliSpot
- ZeroShell

b) Por Hardware

Son equipos que se implementa sin necesidad de un ordenador:

- Cisco BBSM-Hotspot
- Nomadix Gateway
- Antamedia Hotspot Gateway
- Aptilo Access Gateway
- Mikrotik RouterOS

CAPÍTULO III

3. ESTUDIO DE LOS PORTALES CAUTIVOS PARA LA IMPLEMENTACIÓN

3.1 Análisis de Aplicaciones

3.1.1 EasyHotspot

EasyHotspot es una solución alternativa para el sistema de facturación hotspot. Contiene software de código abierto en particular que se incluye en un solo paquete. El principal objetivo es ofrecer un sistema tan sencillo, fácil de instalar, usar y modificar. Requiere menos tiempo de configuración para crear un punto de acceso en funcionamiento. Le ahorrará tiempo y energía. (Easyhotspot, 2010)

Ilustración 7 Acceso a internet a través de un servidor EasyHospot
Fuente: http://easyhotspot.inov.asia/index.php

La ilustración representa a EasyHotspot el cual está instalado dentro de un servidor, y este a su vez está conectado a Internet a un switch en donde se conectan redes cableadas 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 (Easyhotspot, 2010)

Utiliza CodeIgniter que es un framework de PHP de fácil uso y resulta muy útil para el desarrollo de aplicaciones web. EasyHotspot se desarrolla en la parte superior de la distribución Ubuntu.

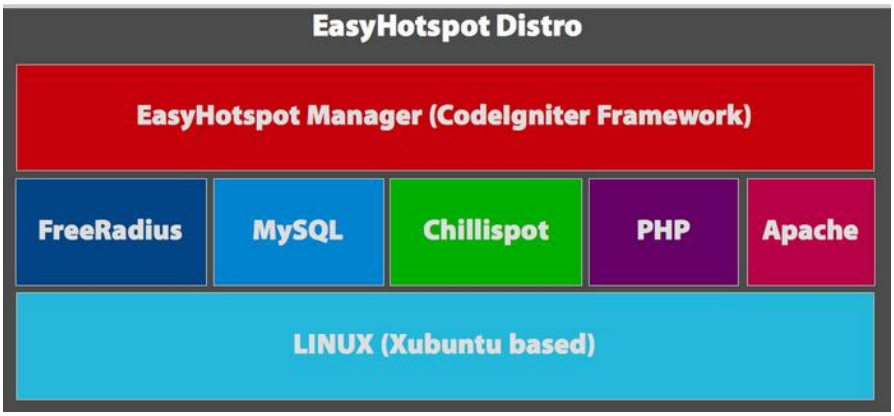


Ilustración 8 EasyHotSpot Componentes
Fuente: http://easyhotspot.inov.asia/index.php

FreeRadius nos ayudará a realizar el proceso del protocolo AAA (Authentication, Authorization and Accounting en inglés). El portal cautivo que se utiliza para la autenticación de usuarios es Chillispot, y la base de datos MySQL, se utiliza para almacenar la información de los usuarios y registros. (Easyhotspot, 2010)

¿Quién lo podría necesitar? Cualquier persona que quiera crear un punto de acceso o de alguien que quiere aprender cómo funciona un hotspot. . Por ejemplo: cafetería, restaurante, hotel, escuela, lugar público, y cualquier otro que requiera conexión a Internet inalámbrica.

3.1.1.1 Características especiales del EasyHotspot

Construido bajo Linux, en su distribución Ubuntu 9.04.

Tiene la garantía del código. Está asegurado por los códigos emitidos durante el proceso de reserva (por SSL). Esos datos no pueden ser utilizados por "espías informáticos" externos.

La plataforma del Punto de Acceso se puede escalar hasta x 1000 usuarios desde una sola radio celular hasta una instalación con varios cientos Puntos de Acceso. Test de resistencia como el del sistema Nomadix se hizo en el CeBit en 2003, donde más de 8000 usuarios pudieron acceder al servicio.

Es la conexión de usuarios más simple ya que el usuario no tiene que llevarse las instalaciones a su ordenador portátil o a su Palm. Incluso los ordenadores portátiles con una dirección IP integrada (no DHCP) o un proxy registrado pueden utilizar el sistema.

Facturas flexibles y centralizadas: el operador puede definir los cargos de su EasyHotSpot.

Asistencia del programa EasyHotspot Roaming con actualmente más de 300.000 usuarios en el mundo.

Servicios: No sólo la facturación se lleva externamente, sino también la asistencia. La línea de supervisión y también de actualizaciones de los programas hace parte de este servicio.

3.1.1.2 Ventajas

Las principales ventajas de la solución EasyHotSpot son:

- Facilidad y rapidez de implantación.
- Acceso a Internet de banda ancha, hasta 54 Mbps nominales.
- Gestión y política comercial independiente de operadores externos; es el propio poseedor del sistema el que pone sus reglas en cuanto al control de acceso y coste de la conexión de los clientes.
- Integración dentro de la red corporativa, diferencia el tráfico generado por los clientes externos del tráfico propio de la empresa.
- Facilidad en la administración y el mantenimiento, no exige la presencia de personal especializado.
- Hasta 20 usuarios simultáneos.

3.1.1.3 Desventajas

- Instalación de Servidores con características por defecto
- No puede ser modificado para ser adaptado a distintas necesidades.

3.1.1.4 Requisitos de Hardware

- Pentium 3 o superior
- 512 MB de RAM
- 5 GB de espacio libre en disco duro
- 2 de interfaz de red (LAN CARD)
- Punto de acceso inalámbrico (no es necesario función router inalámbrico, sino un punto de acceso inalámbrico)
- Switch / Hub (opcional, sólo para usuarios con cable)

3.1.2 CoovaChilli

CoovaChilli es un controlador de acceso de software de código abierto para el portal cautivo (UAM) y el acceso 802.1X aprovisionamiento, basado en Chillispot, y se mantiene activa por un contribuidor original Chillispot. CoovaChilli es liberado bajo la GNU General Public License (GPL). (CoovaChilli, 2012)

CoovaChilli es un controlador de acceso de software rico en característica que proporciona un entorno de portal / jardín-vallado cautivo y utiliza RADIUS o un protocolo HTTP para el acceso de aprovisionamiento y la contabilidad. CoovaChilli es una parte integral de la CoovaAP firmware basado en OpenWRT que está especializada para las zonas activas. (CoovaChilli, 2012)

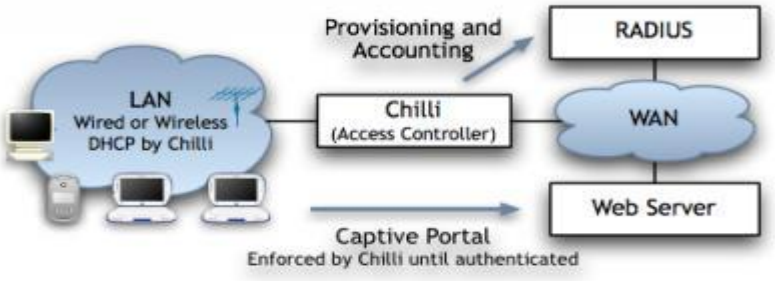


Ilustración 9 Funcionamiento Portal Cautivo CoovaChilli
Fuente: http://coova.org/CoovaChilli

3.1.2.1 Ventajas

- Ideal para facturación de servicios de internet
- Fácil administración
- Servicio de DHCP propio.
- Control del consumo de ancho de banda
- Control del consumo de descarga
- Autenticación UAM con soporte SSL
- Interfaz de Login adaptable para diferentes dispositivos móviles
- Liberado bajo licencia GNU-GPL

3.1.2.2 Desventajas

- Solo admite unos cuantos enrutadores
- Errores de Autenticación en Sistemas operativos de 64-bits

3.1.2.3 Requisitos Hardware

- Dos interfaces de red.
- Pc 32-bits
- Punto de Acceso Inalámbrico

3.1.2.4 Requisitos Software

- Apache-Tomcat
- MySQL
- FreeRadius
- CoovaChilli

3.1.3 ChilliSpot

Ilustración 10 Portal Cautivo ChilliSpot
Fuente: http://www.chillispot.org/

Chillispot es una fuente de portal cautivo de código abierto o controlador de punto de acceso LAN inalámbrico. Se utiliza para la autenticación de usuarios de una LAN inalámbrica. Es compatible con inicio de sesión basado en la web, que es el estándar actual para HotSpots públicos. Autenticación, autorización y contabilidad (AAA) es manejado por el servidor radio favorita. (Chillispot, 2008)

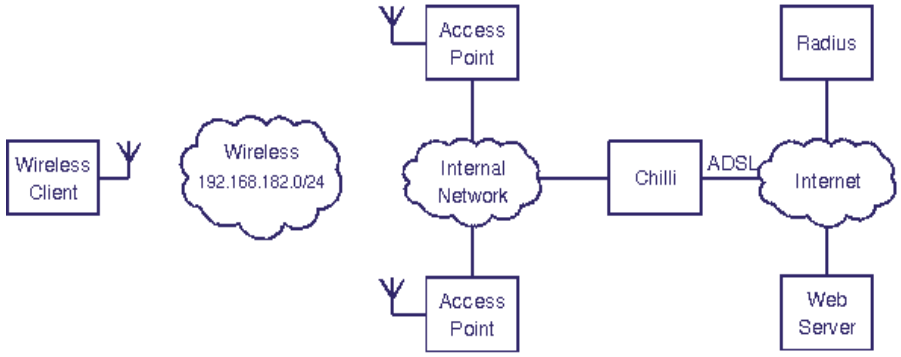


Ilustración 11 Funcionamiento Portal Cautivo ChilliSpot
Fuente: http://www.chillispot.org/

3.1.3.1 Métodos de Autenticación

Chilli Soporta dos métodos de autenticación:

- Método de acceso universal (UAM)
- Acceso Protegido Wi-Fi (WPA)

3.1.3.2 Método UAM

Con UAM el cliente inalámbrico solicita una dirección IP, y se le asigna una dirección IP. Cuando el usuario inicia una web en el navegador chilli capturarán la conexión tcp y redirigirá al navegador a un servidor de autenticación web. El servidor web consulta el

usuario por su nombre de usuario y contraseña. La contraseña se cifra y se envía de vuelta a chilli. (Chillispot, 2008)

3.1.3.3 Método WPA

En este método, el punto de acceso inalámbrico realiza la autenticación del usuario, la misma que es enviada a Chillispot, si es correcta accede a la red, con el método de autenticación WPA/RSN, Chillispot soporta la asignación de IP a través de atributos RADIUS, también funciona como proxy. (Chillispot, 2008)

3.1.3.4 Características

- Chillispot soporta (AAA) Autenticación, Autorización y Registro contra un servidor Radius.
- Es compatible con dos métodos de autenticación UAM (Universal Access Method) y WPA/RSN (Wireless Protected Access)
- Posee un servicio DHCP propio para ambos métodos de autenticación.
- La autenticación con UAM soporta SSL
- Puede utilizarse para la autenticación de usuarios en redes cableadas e inalámbricas.
- Puede actuar como Proxy-RADIUS para otros métodos de autenticación.
- Utiliza NAT o Routing**.**

3.1.3.5 Ventajas

- Liberado bajo licencia GNU-GPL
- Puede ser modificado y adaptado para sus necesidades.
- Plan tarifario para locales
- Facilidad de administración.
- Control de tiempo del servicio
- Filtrado Mac para impedir conexiones de un mismo usuario al mismo tiempo.

3.1.3.5 Desventajas

- Chilli actualmente sólo está disponible para Linux.
- Dependencia de administrador para crear usuarios
- Requiere de Soporte HTTPS
- No es compatible con todos los navegadores.

3.1.3.6 Requisitos

- Conexión a Internet
- Punto de acceso LAN inalámbrico
- Software Chillispot para su PC
- Servidor Radius
- Servidor Apache
- Servidor MySql
- Soporte SSL

3.1.4 Zeroshell

Ilustración 12 Portal Cautivo ZeroShell
Fuente: http://www. ZeroShell.org/

Zeroshell es una distribución Linux para servidores y dispositivos embebidos, que provee de servicios de red. Es un Firewall gratuito que tiene las características de los de los equipos complejos de seguridad. (Zeroshell, 2005)

3.1.4.1 Método de Autenticación

El servidor RADIUS Zeroshell apoya los métodos de autenticación se describen a continuación debido a que incluyen los que ofrecen una mayor garantía de seguridad y con el apoyo de la mayoría de los suplicantes.

- EAP-TLS, que utilizan TLS para la autenticación mutua entre el solicitante y punto de acceso. Tanto el servidor RADIUS y suplicante debe tener un certificado X509 de clave privada y relevante. Aparte de la tarea de tener que dotar a cada usuario con un certificado, éste es sin duda el método de autenticación más seguro y conveniente, ya que no hay ninguna contraseña de usuario debe ser introducido. (Zeroshell, 2005)

- PEAP (Protected EAP), que en su lugar utiliza TLS para autenticar el punto de acceso y establecer un túnel cifrado en MS-CHAPv2 se utiliza para autenticar el suplicante con un nombre de usuario y contraseña. La ventaja de este método es que sólo el servidor RADIUS tiene que tener el certificado de servidor y la clave privada, mientras que el usuario utiliza la misma contraseña para autenticarse con Kerberos 5 en los servicios de la red. (Zeroshell, 2005)

3.1.4.2 Características

- Balanceo de líneas y tolerancia a fallos con conexiones múltiples de internet
- Conexiones UMTS y HSDPA utiliza módems 3G
- Servidor de autentificación radius
- Portal de validación web para redes. El usuario debe validarse antes de poder navegar.
- QoS (Calidad de servicio). Permite configurar el tráfico de la red para garantizar un ancho de banda mínimo.
- HTTP Proxy transparente.
- Punto de acceso wireless
- Host to Lan VPN. VPN cliente
- Lan to Lan VPN. VPN entre servidores
- Router con rutas dinámicas y estáticas
- Soporte de lan Virtual
- Filtro de paquetes, incluido en tráfico P2P
- Traducción de direcciones (NAT)
- TCP/UPD Port Forwarding para la publicación de servidores internos

- Servidor DNS multizona
- Cliente PPPoE para la conexión xDSL
- Cliente DNS dinámico
- Autenticación Kerberos 5
- Autenticación LDAP, NIS y RADIUS
- Sincronización con Active Directory
- Entidad certificadora X509

3.1.4.3 Ventajas

- Filtrado por horas, ancho de banda y protocolos
- Es posible declarar una lista de clientes libres para los que no se requiere autenticación
- Es posible definir una lista de servicios gratuitos proporcionados por servidores externos que los clientes pueden utilizar sin necesidad de autenticación
- La página de acceso web y el lenguaje a utilizar durante la fase de autenticación se puede configurar por el administrador
- Soporte DNS, PROXY, DHCP y Antivirus
- La puerta de enlace pueden trabajar ya sea en modo enrutado o en el modo de bridge
- Encapsulado de datagramas en túneles SSL/TLS
- Configuración por medio de interfaz web

3.1.4.4 Desventajas

- Algunas funciones necesitan donaciones por medio de PayPal
- Suplantación MAC
- Necesidad de seleccionar un medio de almacenamiento para guardar las configuraciones realizadas
- Solo puede ser instalado en una PC con una arquitectura de i386 o 32 bits.

3.1.4.5 Requisitos Software

- Portal Zeroshell
- Clientes Windows Xp o superior, Linux

3.1.4.6 Requisitos Hardware

- Procesador a partir de Pentium II
- Memoria RAM desde 256 MB
- Una tarjeta de red como mínimo
- Tarjeta de Video y Monitor
- Unidad de CD para instalación.
- Router
- Antena Omnidireccional

3.1.5 Resumen Final del Análisis de los Portales Cautivos.

El análisis de los diferentes portales cautivos, se descubrieron funciones únicas y propias de cada portal cautivo, además de la baja demanda en requisitos hardware, en donde se resalta la necesidad de poseer dos interfaces de red de tipo fastEthernet o gigaEthernet con el fin de brindar un correcto funcionamiento de la demanda de internet de la institución y evitar el problema de cuello de botella, cabe resaltar que cada uno de los portales cautivos sujetos a estudio presentan características para un cierto tipo de necesidad donde:

- EasyHotSpot está diseñado como un sistema de control de facturación de un ISP con la facilidad de observar estadísticas de uso por usuario, Ip y ancho de banda y establecer planes de cobranza por tiempo o por ancho de banda.
- CoovaChilli está diseñado para controlar detalladamente a los usuarios de internet que se brinden en hoteles,, restaurantes, aeropuertos, etc. En redes de tipo LAN al no soportar más que dos router para la distribución del servicio de red.
- ChilliSpot está diseñado como un portal cautivo de código abierto con el fin de adaptarse a nuevos servicios o necesidades especiales donde se destaca el control y monitoreo de los usuarios de la red LAN sin la obligación de crear planes tarifarios por el ancho de banda o el tiempo de consumo.

- ZeroShell está diseñado no solo como un sistema de portal cautivo, sino como un complejo sistema de seguridad para instituciones donde la confidencialidad de sus datos requieren más niveles de seguridad, como firewall monitoreo en tiempo real, balanceo de carga, integración con servicios de telecomunicaciones, etc. Sin embargo para adquirir este sistema complejo se requiere de donaciones al proyecto por medio de Paypal, para adquirir todos los módulos de ZeroShell.

3.2 Definición de Parámetros de Comparación

3.2.1 Complementos

Los complementos son cada una de las características tanto en software con en hardware necesarios para el correcto funcionamiento del sistema, como por ejemplo el motor de base de datos del sistema, la versión del sistema operativo, la arquitectura del servidor, etc.

Para cuantificar los complementos de cada portal se utilizara la siguiente tabla:

Cuantitativa	**1**	**2**	**3**	**4**
Cualitativa	Desactualizados	Poco Actual	Actual	Fácil de conseguir
Descripción	Los complementos de cada portal existen pero en versiones antiguas	Los complementos de cada portal se encuentran disponibles pero no todos están actualizados	Los complementos de cada portal se encuentran actualizados	Los complementos de cada portal están actualizados y se encuentran en cualquier Mirror
Valor Porcentual	25%	50%	75%	100%

Tabla 2 tabla de calificación Parámetro Complementos
Fuente: Mauricio Estrada –William Adriano

3.2.2 Tiempo de Respuesta

El tiempo de respuesta se define como el promedio de tiempo en segundos o milisegundos desde el momento de autenticación hasta que el sistema responde autoriza la conexión.

Para cuantificar los tiempos de respuesta de cada portal se utilizara la siguiente tabla:

Cuantitativa	**1**	**2**	**3**	**4**
Cualitativa	Muy Lenta	Lenta	Rápida	Muy Rápida
Descripción	El portal cautivo responde a la autenticación entre de 1 a 1.5 mili segundos	El portal cautivo responde a la autenticación entre 0.50 a 0.99 mili segundos	El portal cautivo responde a la autenticación entre 0.25 a 0.49 mili segundos	El Portal cautivo responde a la autenticación entre 0.10 a 0.24 mili segundos
Valor Porcentual	25%	50%	75%	100%

Tabla 3 Tabla de calificación parámetro Tiempo de Respuesta
Fuente: Mauricio Estrada –William Adriano

3.2.3 Diseño de la Interfaz

Se define el diseño de interfaz como la estructura, Modelo, Diseño, etc. De la página principal de Login de cada portal, además de la capacidad de edición para adaptarla a la institución, así como también la facilidad de publicar políticas de la institución o publicidad.

Para cuantificar el diseño de Interfaz de cada portal se utilizara la siguiente tabla:

Cuantitativa	**1**	**2**	**3**	**4**
Cualitativa	Poco Adaptable	Adaptable	Editable	Fácil de Editar
Descripción	La interfaz de Login del portal cautivo permite ser editada pero solo su diseño no su funcionamiento	La interfaz de Login del portal cautivo permite ser editada pero no	La interfaz de Login del portal cautivo puede ser editada con PHP	La interfaz de Login del portal cautivo puede ser editada en texto plano o php
Valor Porcentual	25%	50%	75%	100%

Tabla 4 Tabla de calificación parámetro Diseño de interfaz
Fuente: Mauricio Estrada –William Adriano

3.2.4 Seguridad

La seguridad se enfoca con la protección tanto en la comunicación como en el almacenamiento de la información y/o datos manejados por el sistema, de tal manera que la edición de la información solo sea realizada por personas acreditadas y con la autorización necesaria.

Entre los tipos de seguridad que se encuentran en la red están:

- **Negociación de claves y Almacenamiento**

  Cada elemento activo en la red debe ser capaz de verificar la identidad de su interlocutor.

- **Integridad**

  La información debe ser consistente y fiable y no propensa a alteraciones no deseadas entre emisor-receptor.

- **Autenticación**

  Se refiere a establecer las entidades que pueden tener acceso a los recursos de cómputo que cierto medio ambiente puede ofrecer.

- **Privacidad**

  La información debe ser vista y/o manipulada solo por quienes tienen el derecho y la autoridad de hacerlo.

- **Auditoria**

  Se refiere a la continua vigilancia del tráfico existente en las peticiones de los usuarios.

Los portales cautivos basan su seguridad en autenticación y cifrado, comúnmente se utiliza el protocolo SSL (Secure Socket layer) la cual proporciona comunicaciones seguras por medio de trasmisiones criptográficas, todo esto es trasparente para el usuario.

Para cuantificar las seguridades de cada portal se utilizara la siguiente tabla:

Cuantitativa	**1**	**2**	**3**	**4**
Cualitativa	Escasamente Segura	Medianamente segura	Segura	Completamente Segura
Descripción	El portal cautivo trasmite los datos en texto plano y no presenta cifrado	El portal cautivo presenta medidas de auditoria pero no cifra la comunicación	El portal cautivo presenta cifrado en la trasmisión de datos	El portal cautivo presenta altas medidas de seguridad tanto en trasmisión de datos (SSL) como en almacenamiento en base de datos
Valor Porcentual	25%	50%	75%	100%

Tabla 5 Tabla de calificación parámetro Seguridad
Fuente: Mauricio Estrada –William Adriano

3.2.5 Control

El control se define como los mecanismos y posibles **configuraciones** que posee cada portal cautivo a cada usuario o grupo de usuarios así como el control de ancho de banda, el tiempo de uso de la red, filtrado web por grupo de usuarios, además de la monitorización de la red en tiempo real entre otros.

- **CONTROL DE USUARIO A NIVEL INDIVIDUAL**

  Para el estudio se establecerá el control respecto al tiempo de conexión, habilitación y des habilitación de acceso, filtrado a través de niveles de privilegio, filtrado en capa de enlace de datos, y capa de red, entre otras medidas de control que puedan presentar los diferentes portales sujetos a estudio.

- **CONTROL DE USUARIOS A NIVEL DE GRUPO**

  Para el estudio a nivel de grupo se establecerá el control respecto a tiempo de conexión, ancho de banda filtrado de privilegio entre otras medidas de control que presente los portales cautivos.

Para cuantificar las medidas de control de cada portal se utilizara la siguiente tabla:

Cuantitativa	**1**	**2**	**3**	**4**
Cualitativa	Poco Control	Medianamente Controlado	Control	Fácil de Controlar
Descripción	El portal cautivo no presenta medidas de control aparte de la autenticación ni por usuario ni por grupo de usuarios	El portal cautivo presenta medidas de control solo a nivel de usuario.	El portal cautivo presenta medidas de control tanto a nivel de usuario como a nivel de grupo de usuarios	El portal cautivo presenta varios niveles de control únicos y fáciles de configurar, adecuándose a la necesidad del usuario
Valor Porcentual	25%	50%	75%	100%

Tabla 6 Tabla de calificación parámetro Control
Fuente: Mauricio Estrada –William Adriano

CAPÍTULO IV

4 ANÁLISIS COMPARATIVO DE LAS APLICACIONES PARA LA IMPLEMENTACIÓN DEL PORTAL CAUTIVO

En este capítulo se analizaran las características de cada uno de los portales cautivos, ChilliSpot, Easyhotspot, CoovaChilli y Zeroshell con el fin de obtener el que mejor se acople de mejor manera a las necesidades de la Escuela "Gabriel García Moreno" de la ciudad de Guano.

4.1 Parámetros de Comparación

Los parámetros que a continuación se mencionan han sido tomados de acuerdo a las principales características de cada uno de los portales cautivos sujetos al estudio, con el objetivo de determinar el que mejor se acople a las necesidades de la Escuela "Gabriel García Moreno" para obtener un mejor control de las redes inalámbricas.

En el estudio se realizara un análisis cuanti-cualitativo de las principales características de los portales antes nombrados.

Los parámetros a tomar en consideración son:

PARÁMETROS	INSTRUMENTOS	TÉCNICAS	VALOR %
Complementos	➢ Laptop ➢ Portales Cautivos ➢ Máquina Virtual	➢ Investigación ➢ Descripción	6,5%
Tiempo de Respuesta	➢ RadLogin ➢ Access Point ➢ Laptop	➢ Monitorización	14,5%
Diseño de la Interfaz	➢ Índex de cada Portal	➢ Encuesta ➢ Entrevista	5,5%
Seguridad	➢ Access Point ➢ Laptop	➢ Wireshark ➢ BackTrack5 r3	32,5%

		➢ Inyección SQL	
Control	➢ Portales Cautivos ➢ Laptop ➢ Access Point	➢ Investigación ➢ Descripción	41%

Tabla 7 Valor porcentual por Parámetro de comparación
Fuente: Mauricio Estrada –William Adriano

Para la obtención de los porcentajes de cada uno de los parámetros a comparar de los portales cautivos se realizaron encuestas tanto a profesionales del tema como a los usuarios finales de la red, Para más detalles ver Anexo 4 (Encuesta) y Anexo 5 (Tabulación de encuestas).

4.1.1 Justificación de Ponderación de Parámetros

- **Control vs Diseño de Interfaz**

Se considera el Control que posee cada uno de los portales cautivos el tema principal de la investigación ya que se relaciona con la hipótesis propuesta, ya que dicho parámetro tendrá una ponderación más alta en cuanto a porcentaje total de la tabla de los parámetros, en comparación al diseño de la interfaz, ya que este último parámetro viene en su mayoría por defecto y no es necesaria su edición para el funcionamiento del portal cautivo.

- **Seguridad vs Tiempo de Respuesta**

Se considera al parámetro Seguridad en una institución educativa como uno de los ejes principales por las siguientes razones:

- Se comparte información confidencial perteneciente a la institución educativa como notas de Estudiantes, Citaciones a Reuniones, Portafolio Estudiantil, etc.
- Para evitar el uso de los recursos de red que deben ser utilizados solo por personal a fin a la institución y no por personas externas.
- Para mantener la integridad de la información trasmitida por la red.
- Para mantener la privacidad de los usuarios de la red.

A demás se considera al tiempo de respuesta con una ponderación más baja respecto a seguridad ya que el número de usuarios de la red es relativamente bajo lo que conlleva a una variación muy insignificante en lo que se refiere al tiempo de respuesta.

- **Complementos vs Diseño de Interfaz**

Se podría considerar a los complementos o software necesario para la implementación del sistema con una ponderación más importante con respecto a Diseño de interfaz, sin embargo tras la investigación realizada se pudo encontrar que dos de los portales sujetos a estudio poseen todos los complementos necesarios en un mismo paquete para su instalación al momento de su descarga, además los dos restantes portales cautivos utilizan paquetes básicos existentes en cualquier mirror de Linux.

Con respecto al Diseño de Interfaz se pudo constatar que los conocimientos necesarios para la edición de la interfaz de Login son de un nivel básico a intermedio, ya que se puede realizar la edición por medio grafico o por lenguaje php.

Por tal motivo se considera al parámetro Complemento y Diseño de Interfaz con una ponderación baja e equivalente con respecto a control y seguridad.

Tiempo de Respuesta vs Complementos y Diseño de Interfaz

Se considera que el tiempo de respuesta tendrá una ponderación más alta con respecto a diseño de interfaz y complementos ya que el número de usuarios podría crecer en la institución educativa lo que llevaría a aumentar los tiempos de autenticación, mientras que los complementos software se mantendrían sin ningún cambio y/o edición por el alto soporte que poseen sus servicios como mysql, FreeRadius, Apache, etc. para un número mayor de usuarios.

4.1.2 Complementos

EasyHotSpot requiere para su correcto desenvolvimiento de una distribución de Linux de preferencia Ubuntu 9.04 o superior estable sus requisitos hardware con un procesador Pentium II, tarjeta de memoria de 512MB, dos Interfaces de red y un Access Point o Router inalámbrico.

CoovaChilli requiere para su correcto desenvolvimiento de una distribución de Linux, se puede trabajar tanto en Ubuntu 9.04 o superior o Centos 6.0 hasta 6.4 además del

servidor Apache o TomCat, MySql, FreeRadius, Portal CoovaChilli y navegador Web con soporte SSL, los requisitos hardware son una pc con arquitectura de 32 bits, dos Interfaces de red, Router Inalámbrico desactivado el servicio de DHCP.

ChilliSpot requiere para su correcto desenvolvimiento una distribución de Linux se puede trabajar en Centos 5.4 en adelante, además de un servidor web, Apache, Mysql, FreeRadius, ChilliSpot, Soporte SSL puede ser complementado para una mejor administración con PhpMyAdmin, DaloRadius, RadiusDesk,, etc sus requisitos hardware son mínimos dos Interfaces de Red (Eth0, Eth1) Access Point inalámbrico o Router inalámbrico desactivado DHCP.

Zeroshell requiere para su correcto desenvolvimiento una distribución GNU/Linux server clientes web tanto Linux, Windows o Mac, además de un live cd con Zeroshell sus requisitos Hardware son dos interfaces de red, una pc con lector de CD-ROM y USB

Para determinar el valor del parámetro se tomó en cuenta el acceso a los complementos, y su facilidad de instalación.

Herramienta	Complementos	Valor
EasyHotSpot	Actual	3
CoovaChilli	Actual	3
ChilliSpot	Fácil de Conseguir	4
ZeroShell	Actual	3

Tabla 8 Calificación Complemento
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 13 se puede observar con mayor detalle el valor de calificación del parámetro Complementos de cada uno de los portales cautivos sujetos a estudio

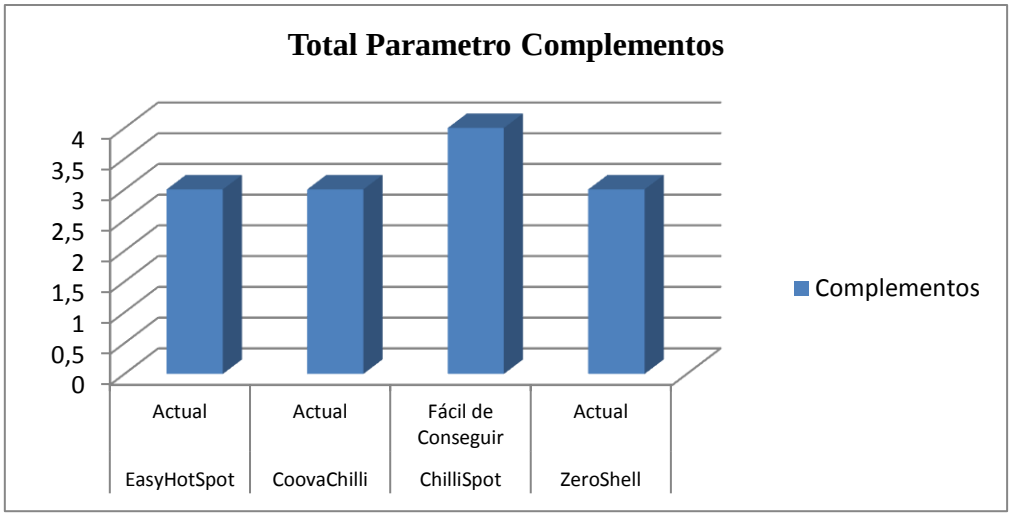


Ilustración 13 Grafica Total Complementos
Fuente: Mauricio Estrada –William Adriano

4.1.3 Tiempo de respuesta

Para determinar el valor de tiempo de respuesta de autenticación, se evaluó el rendimiento del servidor RADIUS frente a cada portal cautivo.

Para el análisis se utilizó la herramienta benchmarking radLogin4 disponible en http://www.iea-software.com/products/radlogin4.cfm el cual permite generar N conexiones al servidor RADIUS además de generar el proceso de autenticación como muestra la ilustración.

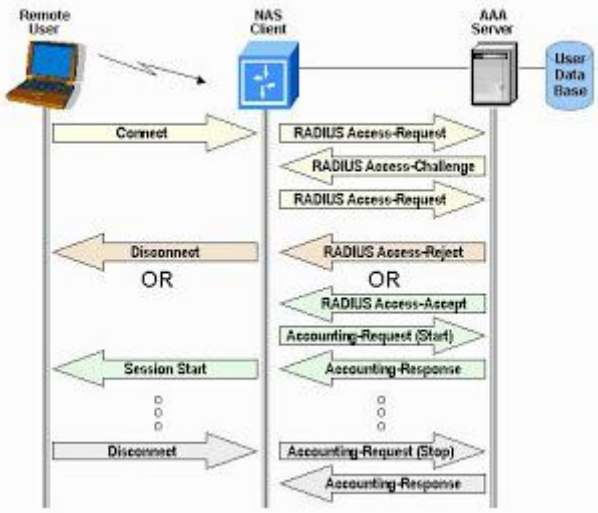


Ilustración 14 Proceso de Autenticación Radius
Fuente: http://trabajotele08.blogspot.com/

El número de conexiones simultáneas estará definido por el tamaño de la muestra de usuarios que utilizan internet inalámbrico la Escuela "Gabriel García Moreno" A continuación se detalla el proceso para el análisis cuantitativo:

Tamaño de la Muestra

N# de conexiones concurrentes esta entre 21 y 30

La Media es:

$$\overline{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$$

x = ½(21+30)

x = 25.5

El tamaño de la muestra se calculó mediante la siguiente formula:

$$n = \frac{Z^2 pqN}{NE^2 + Z^2 pq}$$

Dónde:

n es el tamaño de la muestra.

Z es el nivel de confianza.

P es la variabilidad positiva.

q es la variabilidad negativa.

N es el tamaño de la población.

E es la precisión del error.

$$n = \frac{(0{,}95)\ ^2\ (0.5)\ (0.5)\ (26)}{(26)(0.05)\ ^2 + (0.95)\ ^2\ (0.5)\ (0.5)}$$

$$n = 5.87$$

0.2906

n = 20.1995

El tamaño de la muestra es de 20 conexiones concurrentes las cuales fueron simuladas mediante la herramienta RadLogin simultáneamente como se presenta a continuación:

Simulación de tiempo de respuesta de autenticación del servidor RADIUS frente al portal cautivo.

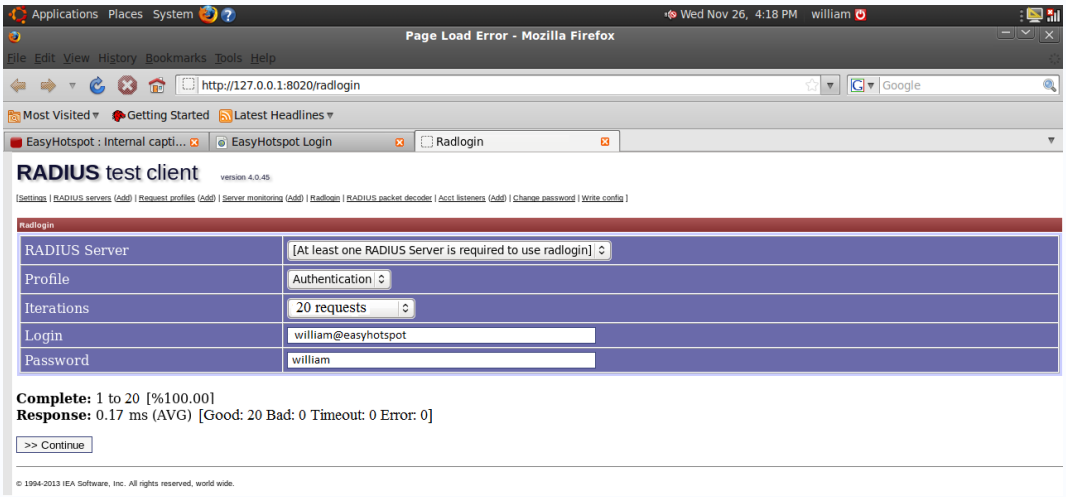


Ilustración 15 Simulación de autenticación RadLogin

Fuente: Mauricio Estrada – William Adriano

El proceso de simulación de autenticación se resume en el anexo 1.

Los tiempos de respuesta de los portales cautivos sujetos a estudio se resumen en la siguiente tabla:

Portal Cautivo	Tiempo de respuesta
EasyHotSpot	0.17
CoovaChilli	0.89
ChilliSpot	0.11
ZeroShell	1.23

Tabla 9 Tiempo de Respuesta

Fuente: Mauricio Estrada –William Adriano

La media de los valores recogidos se tabuló con la ayuda de una hoja de Excel dando el siguiente resultado:

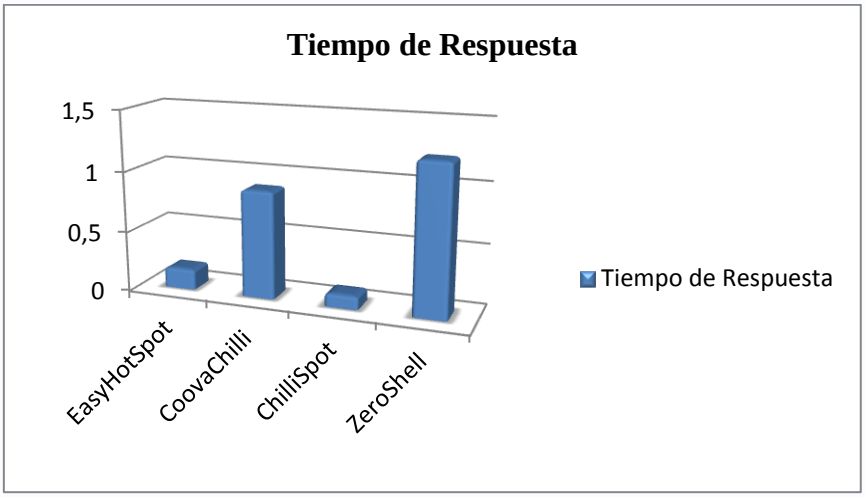


Tabla 10 Grafica de referencia Tiempo de Respuesta
Fuente: Mauricio Estrada –William Adriano

Para determinar el valor del parámetro tiempo de respuesta se tomó en cuenta el tiempo recogido con la simulación de la autenticación frente a cada portal.

Herramienta	Tiempo Respuesta	Valor
EasyHotSpot	Muy Rápida	4
CoovaChilli	Lenta	2
ChilliSpot	Muy Rápida	4
ZeroShell	Muy Lenta	1

Tabla 11 Calificación Tiempo de Respuesta
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 16 se puede observar con mayor detalle el valor de calificación del parámetro Tiempo de respuesta de cada uno de los portales cautivos sujetos a estudio

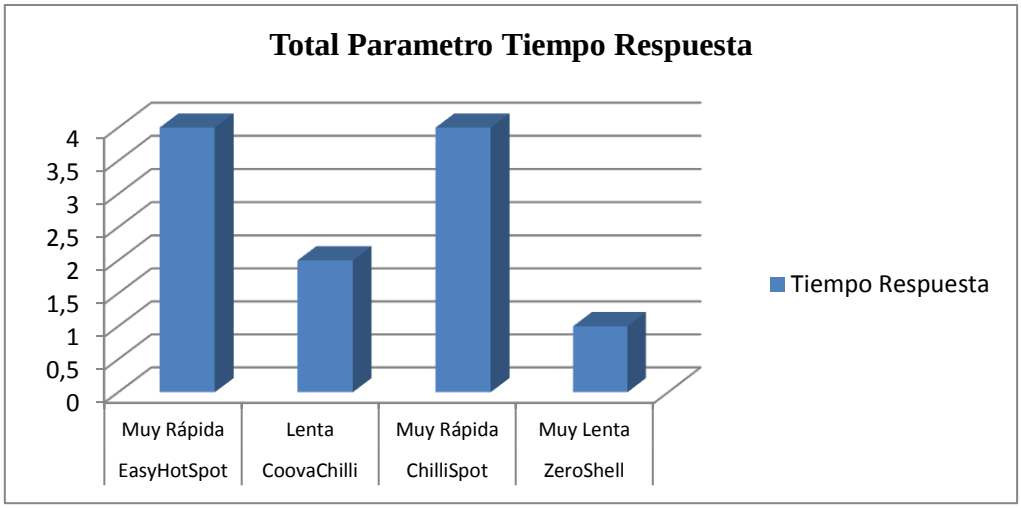


Ilustración 16 Grafica Total Tiempo de Respuesta
Fuente: Mauricio Estrada –William Adriano

4.1.4 Diseño de la Interfaz

Para determinar el valor que posee el indicador Diseño de interfaz se determinaron varias técnicas con entrevistas y encuestas a los usuarios finales, los cuales ayudaron a determinar una parte el valor final del mismo.

Para complementar este valor se realizó un análisis de la complejidad que posee cada Portal Cautivo en su página principal a la hora de ser modificable y adaptable.

La pantalla inicial de **EasyHotspot** es muy sencilla como se puede observar en la ilustración 17. Posee los campos necesarios para poder acceder al servicio.

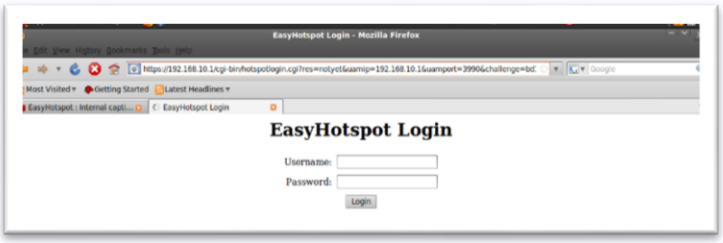


Ilustración 17 Interfaz de Login EasyHotSpot
Fuente: Mauricio Estrada – William Adriano

Para poder realizar algún cambio en la página de inicio de sesión se debe tener conocimientos en HTML y modificar directamente el archivo hotspotlogin.cgi que se encuentra en: /opt/local/web/easyhotspot/hotspot/hotspotlogin.cgi

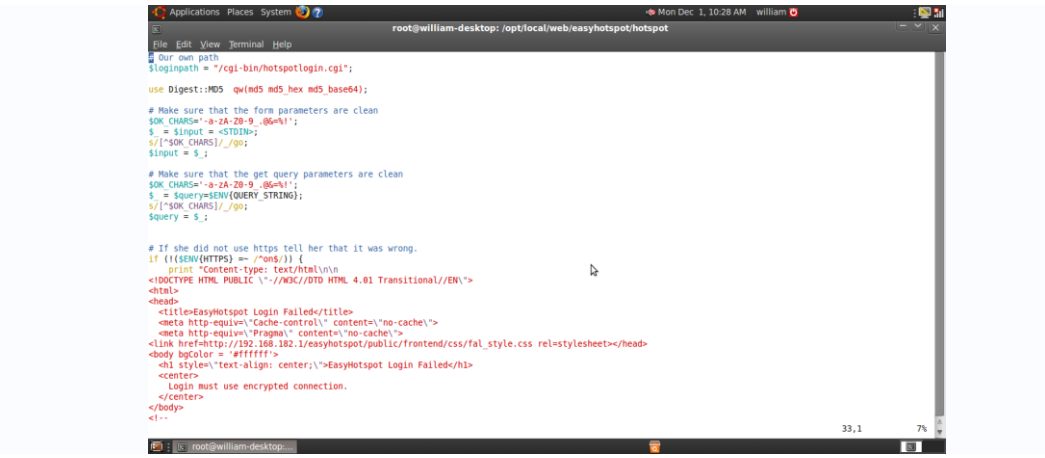


Ilustración 18 Script Edición Interfaz de Login EasyHotSpot
Fuente: Mauricio Estrada – William Adriano

CoovaChilli posee una página de inicio de sesión sencilla como se lo puede observar en la ilustración 19 y contiene los campos de usuario y contraseña.

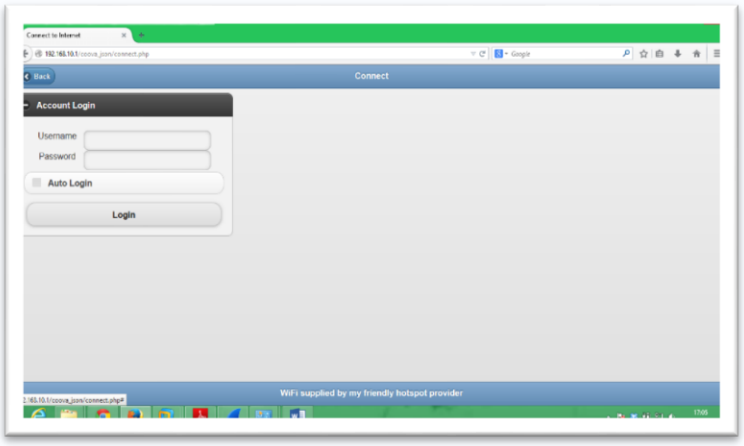


Ilustración 19 Interfaz de Login CoovaChilli
Fuente: Mauricio Estrada – William Adriano

Para poder realizar algún cambio en la página de inicio de sesión se debe tener conocimientos en programación y modificar directamente el archivo raíz **hotspotlogin.cgi** el cual se encuentra en el path o dirección raíz: /opt/local/web/chillihotspot/hotspot/hotspotlogin.cgi

ChilliSpot al igual que los otros portales cautivos su página de inicio de sesión es muy sencilla y básica, con los campos necesarios para el acceso al servicio, como se lo puede observar el la ilustración 20.

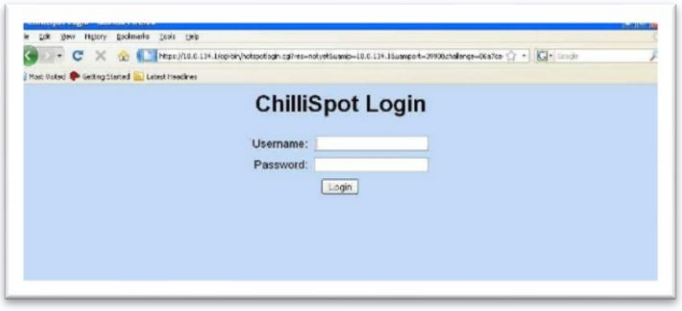


Ilustración 20 Interfaz de Login ChilliSpot
Fuente: Mauricio Estrada – William Adriano

Para poder realizar algún cambio en la página de inicio de sesión se debe tener conocimientos en HTML, PHP, JAVASCRIP, CSS entre otros ya que se lo puede modificar directamente el archivo hotspotlogin.cgi que se encuentra en: /opt/local/web/chillihotspot/hotspot/hotspotlogin.cgi. O a su vez se lo puede complementar al agregar hojas de estilos para un mejor diseño de la misma.

ZeroShell posee una interfaz de inicio de sesión no tan sencilla ya que posee un diseño como se lo puede ver en la ilustración 21. Es un diseño muy profesional a demás es más agradable que los demás portales cautivos.

Ilustración 21 Interfaz de Login ZeroShell
Fuente: Mauricio Estrada – William Adriano

Para poder realizar algún cambio en la página de inicio de sesión no se debe tener conocimientos en programación ya que no se debe modificar directamente el archivo hotspotlogin.cgi, ya que ZeroShell permite modificar la página de inicio de una forma gráfica.

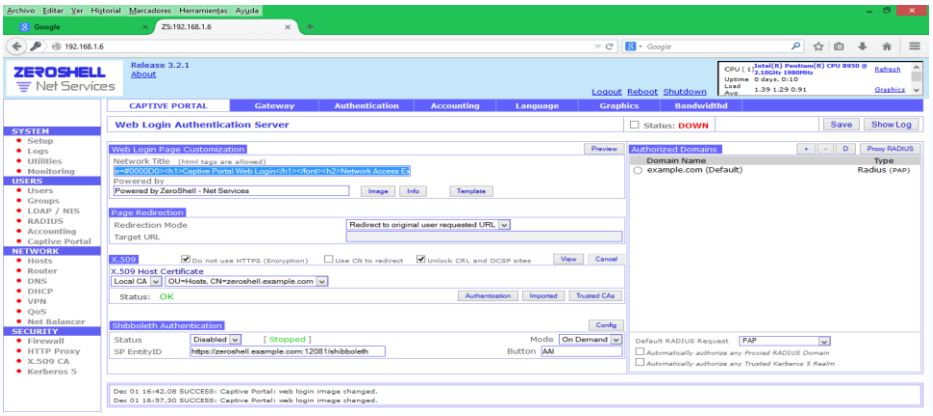


Ilustración 22 Edición de Interfaz de Login de manera grafica
Fuente: Mauricio Estrada – William Adriano

Se puede también insertar imágenes que representen nuestra organización o cualquier otra de una forma sencilla y gráficamente.

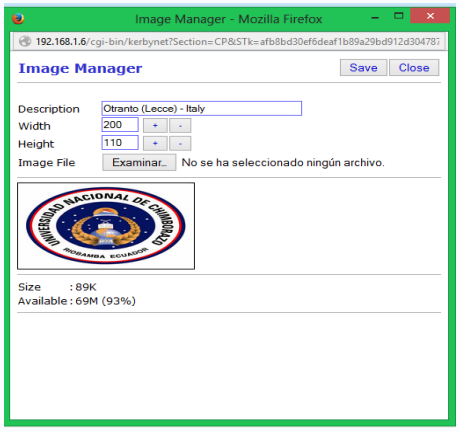


Ilustración 23 Inserción Imagen
Fuente: Mauricio Estrada – William Adriano

Para determinar el valor de interfaz de usuario se tomó en cuenta la facilidad con la que se puede editar y modificar la pantalla de inicio de sesión y las encuestas y entrevistas que se realizaron a los usuarios finales.

Herramienta	interfaz	Valor
EasyHotSpot	Poco adaptable	1
CoovaChilli	Adaptable	2
ChilliSpot	Editable	3
ZeroShell	Fácil de editar	4

Tabla 12 Calificación Interfaz de Login
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 24 se puede observar con mayor detalle el valor de calificación del parámetro Diseño de Interfaz de cada uno de los portales cautivos sujetos a estudio

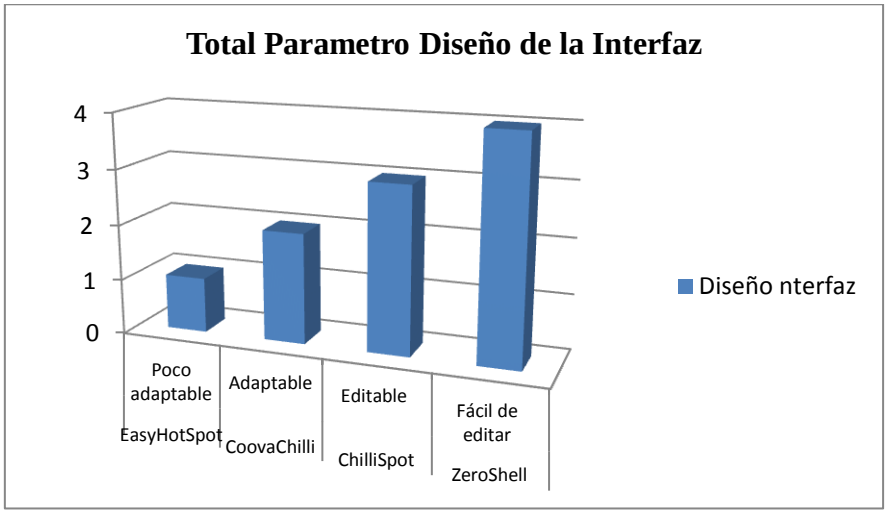


Ilustración 24 Grafica total Diseño de Interfaz
Fuente: Mauricio Estrada –William Adriano

4.1.5 Seguridad

Para medir el nivel de seguridad de cada portal se realizó dos tipos de ataques en cada uno de los servidores donde se encuentran montados cada uno de los sistemas a evaluar, los ataques realizados fueron:

- **Ataque Spoofing**

El ataque spoofing en términos de seguridad de redes hace referencia al uso de técnicas de suplantación Mac en capa 2 del modelo OSI (enlace de datos) generalmente con usos maliciosos o de investigación.

- **Inyección SQL.**

A demás se verifico el estado de trasmisión de datos de cada portal cautivo por medio de Wireshark.

4.1.5.1 Ataque Spoofing

Para realizar el ataque spoonfing se utilizó el sistema BlackTrack5 r3 el cual es un software utilizado para realizar auditorías de seguridad informática el cual se encuentra disponible en http://www.backtrack-linux.org/downloads/backtrack5r3.

Ilustración 25 Logo Sistema BackTrack 5r3
Fuente: http://www.backtrack-linux.org/downloads/backtrack5r3

Los requisitos para realizar el ataque spoofing son:

Requisitos	Descripción
Tres Computadoras	➢ Servidor (portal cautivo) ➢ Cliente (portal cautivo) ➢ Atacante (BlackTrack5r3)
Router inalámbrico	➢ Para establecer la red de los tres equipos

Tabla 13 Requisitos Ataque Spoofing
Fuente: Mauricio Estrada –William Adriano

El proceso de la realización del ataque se detallara en el anexo 3.

Luego de realizar los ataques spoofing a cada uno de los portales cautivo se determinó lo siguiente:

- EasyHotspot puede recibir ataques de spoofing o es vulnerable en ataques de suplantación Mac.
- CoovaChilli es vulnerable para ataques spoofing.
- Chillispot puede recibir ataques de suplantación Mac.
- Zeroshell puede recibir ataques de suplantación Mac y suplantación IP

Para determinar el valor de ataque spoofing se tomó en cuenta las vulnerabilidades en suplantación Mac e Ip dando la siguiente tabla:

Herramienta	Ataque Spoofing	Valor
EasyHotSpot	Escasamente Segura	1
CoovaChilli	Escasamente Segura	1
ChilliSpot	Escasamente Segura	1
ZeroShell	Escasamente Segura	1

Tabla 14 Calificación Ataque Spoofing
Fuente: Mauricio Estrada –William Adriano

4.1.5.2 Inyección SQL

Para determinar en parte el valor de la seguridad de los portales cautivos se realizó un análisis tanto como al servidor de base de datos y al servidor radius para determinar si son propensos a ser atacados con sql inyector.

Para el análisis se utilizó la herramienta SQL Power Inyector disponible en http://www.sqlpowerinjector.com/download.htm el cual permite determinar si existen fallas o vulnerabilidades que permitan estos tipos de ataques.

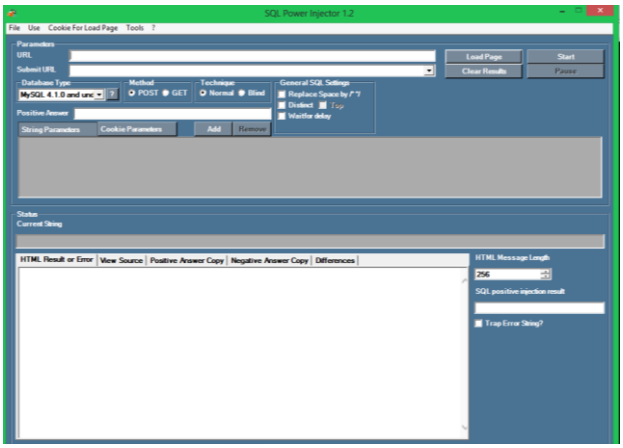


Ilustración 26 Inyección Sql
Fuente: http://www.sqlpowerinjector.com/download.htm

Con la herramienta de SQL Power Inyector se puede verificar si a través de la página de logue de los portales cautivos se puede quebrantar la seguridad y acceder al servicio.

Una vez realizado el análisis con la herramienta especificada a los distintos portales cautivos se determinó los siguientes valores:

Portal Cautivo	Inyección	Valor
EasyHotSpot	Completamente Segura	4
CoovaChilli	Completamente Segura	4
ChilliSpot	Completamente Segura	4
ZeroShell	Completamente Segura	4

Tabla 15 Calificación Inyección SQL
Fuente: Mauricio Estrada –William Adriano

Determinado así que tanto la base de datos y el servidor RADIUS no son propenso a residir este tipo de ataques.

El desarrollo del análisis se lo detalla en el anexo 2

4.1.5.3 Trasmisión de Datos

Para determinar si los datos son trasmitidos en texto plano o son cifrados con SSL o cualquier otro tipo de encriptación se realizó las pruebas de envío y recepción de datos con ayuda de Wireshark.

SSL Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones puedan transmitir información de ida y vuelta de manera segura. Las aplicaciones que utilizan el protocolo Secure Sockets Layer saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.

Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicación disponible en: https://www.wireshark.org/download.html.

Ilustración 27 Snifer WireShark
Fuente: https://www.wireshark.org/download.html.

El proceso de realización de pruebas se realizara con más detalles en el anexo4.

Luego de instalar el software en las maquinas cliente de cada una de los portales se establece que:

- EasyHotSpot trasmite con soporte SSL.
- CoovaChilli cifra el contenido de la trasmisión mediante SSL.
- Chillispot viene definido desde su instalación con SSL, al presentar su página de Login una respuesta https.
- Zeroshell soporta SSL/TLS.

Para determinar el valor del parámetro se tomó en cuenta la seguridad de trasmisión de los datos al verificar si están cifrados o son trasmitidos en texto plano

Herramienta	Transmisión	Valor
EasyHotSpot	Segura	3
CoovaChilli	Segura	3
ChilliSpot	Completamente Segura	4
ZeroShell	Segura	3

Tabla 16 Calificación Trasmisión de datos
Fuente: Mauricio Estrada –William Adriano

4.1.5.4 Resumen parámetro de Seguridad

La siguiente tabla muestra los valores a ser tomados en cuenta en el total del parámetro de seguridad.

	EasyHotspot	CoovaChilli	ChilliSpot	ZeroShell
Spoofing	1	1	1	1
Inyección SQL	4	4	4	4
Trasmisión Cifrada	3	3	4	3
TOTAL	8	8	9	8
Porcentaje	**66.66%**	**66.66%**	**75%**	**66.66%**

Tabla 17 Resumen parámetro Seguridad
Fuente: Mauricio Estrada –William Adriano

Para determinar el parámetro de seguridad se tomara en cuenta los valores obtenidos en Spoofing, inyección SQL y trasmisión de datos los cuales serán sumados y promediados.

Herramienta	Seguridad	Valor
EasyHotSpot	Medianamente Seguro	2
CoovaChilli	Medianamente Seguro	2
ChilliSpot	Seguro	3
ZeroShell	Medianamente Seguro	2

Tabla 18 Calificación parámetro Seguridad
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 28 se puede observar con mayor detalle el valor de calificación del parámetro Seguridad de cada uno de los portales cautivos sujetos a estudio

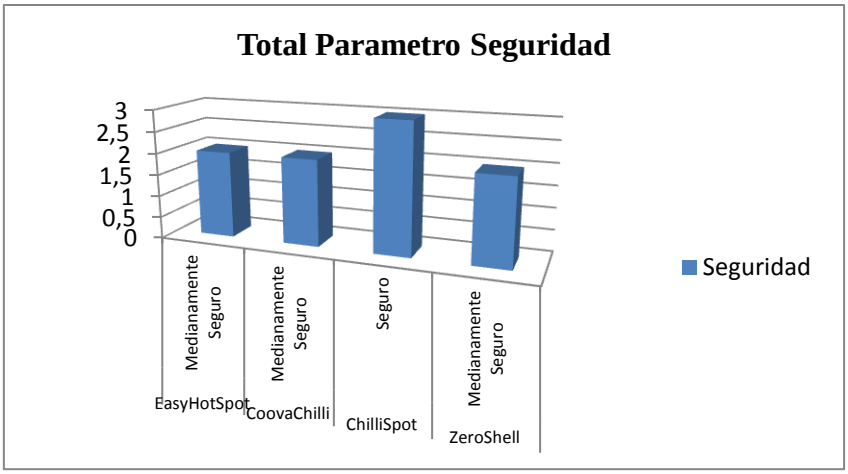


Ilustración 28 Grafica Total Seguridad
Fuente: Mauricio Estrada –William Adriano

4.1.6 Control

EasyHotSpot permite al usuario acceso a la red mediante la Autenticación por conocimientos, es decir solo si el usuario está registrado y conoce los datos de Login.

Easyhotspot posee dos tipos de administración:

- **Admin:** este usuario maneja plan de facturación, el precio y la configuración del sistema.

  También desde este tipo de administración se puede establecer la velocidad deseada para cada cuenta de pos pago, el precio por cada megabyte o cada minuto, el tiempo de inactividad cuando el usuario será desconectado, La velocidad de carga y descarga o el ancho de banda máximo permitido para una cuenta, además se puede generar un plan de facturación para usar como plantilla para la creación de vales en la página del cajero.

- **Cajero:** este usuario maneja la cuenta de usuario, generación de comprobante, factura, mira las estadísticas

  Presenta las mismas medidas de control de un administrador a excepción que en este modo se puede revisar estadísticas simples de todos los vales o comprobantes de los planes de facturación.

CoovaChilli permite al usuario acceso a la red solo si está registrado y si aún no ha terminado su plan de uso de la red, El usuario debe realizar una conexión por conocimientos.

- Cuando se autorice un cliente ChilliController actualizara periódicamente los datos de contabilidad (minutos/megabytes) mediante la emisión de estado periódico.
- CoovaChilli posee un identificador único de sesión Acct-Session-Id el cual se asegura de que varios clientes quieran conectarse con la misma cuenta de usuario y contraseña al mismo tiempo.
- Función controlador de cada usuario donde se describe el tiempo de duración de la sesión, el lapso de tiempo de des activación de cuenta, etc.
- Dificultad para integración con servicios proxy.

ChilliSpot permite al cliente acceso a la red solo si se encuentra registrado y los datos de Login no están siendo utilizados por otro usuario, la autenticación se da mediante RADIUS y Autenticación de Conocimientos.

- ChilliSpot utiliza el método WPA o UAM método de acceso universal con soporte SSL/TSL para el acceso protegido inalámbrico.
- Proporciona un scrip.cgi para solicitar al usuario su nombre de cuenta y contraseña
- ChilliSpot puede ser utilizado tanto en una red WIFi con en una red cableada
- Facilidad de creación de grupo de Usuarios privilegiados.
- Control de tiempo de sesión, numero de paquetes trasmitidos al cliente
- Limita el ancho de banda (b/s) por cliente o grupo de usuarios
- Permite establecer páginas que los usuarios pueden navegar sin la necesidad de Login.
- Monitorización por usuario con parámetros como el tiempo de sesión, download, upload, etc.
- Filtrado en la capa de enlace de datos y capa de red.
- Integración con servidor proxy, proxy-transparente, DNS.
- Archivos Log para monitorizar acciones por IP o usuario registrado.
- Página disponible para presentación de políticas de la institución o publicidad.

ZeroShell permite acceso a la red solo si el cliente se encuentra registrado.

- Servidor RADIUS para proporcionar una autenticación segura y la gestión automática de las claves de cifrado para el Wireless 802.11b, 802.11g y 802.11a redes que soportan el protocolo 802.1x en el EAP-TLS, EAP-TTLS y PEAP.
- QoS
- Soporte para redes cableadas e Inalámbricas
- Asignación del ancho de banda y priorización de la clase de tráfico.
- Integración con servidor proxy
- Balanceo de carga y tolerancia a fallos
- Integración con servidor DNS

Para determinar el valor del parámetro se tomó en cuenta el protocolo AAA Autenticación, Autorización y Contabilidad.

Herramienta	Control	Valor
EasyHotSpot	Control	3
CoovaChilli	Medianamente controlado	4
ChilliSpot	Fácil de controlar	3
ZeroShell	Control	3

Tabla 19 Calificación parámetro Control
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 29 se puede observar con mayor detalle el valor de calificación del parámetro Control de cada uno de los portales cautivos sujetos a estudio

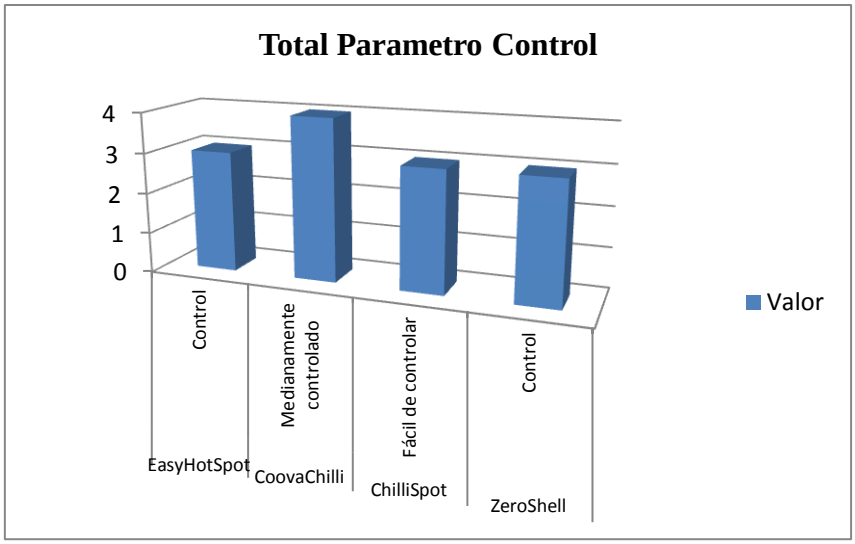


Ilustración 29 Grafica Total Control
Fuente: Mauricio Estrada –William Adriano

4.2 Resumen Comparativo

Luego de realizar un análisis de las principales características de EasyHotSpot, CoovaChilli, ChilliSpot y ZeroShell aplicaciones utilizadas para implementar portales cautivos se obtuvo la siguiente tabla resumen donde se presenta los resultados del estudio comparativo.c

	EasyHotSpot	CoovaChilli	ChilliSpot	ZeroShell
Complementos 6.5%	3	3	4	3
Tiempo de Respuesta 14.5%	4	2	4	1
Diseño de la Interfaz 5.5%	1	2	3	4
Seguridad 32.5%	2	2	3	2
Control 41%	3	4	3	3

Tabla 20 Calificación Total de todos los parámetros
Fuente: Mauricio Estrada –William Adriano

La siguiente tabla muestra la calificación total obtenida por cada uno de los portales dividido para el porcentaje de cada uno de los parámetros y la sumatoria total de la calificación obtenida.

Valor Total Por Parámetro	EasyHotSpot	CoovaChilli	ChilliSpot	ZeroShell
1,3	0,975	0,975	1,3	0,975
2,9	2,9	1,45	2,9	0,725
1,1	0,275	0,55	0,825	1,1
6,5	3,25	3,25	4,875	3,25
8,2	6,15	8,2	6,15	6,15
20	13,55	14,425	16,05	12,2
100%	67,75%	72,125%	80,25%	61%

Tabla 21 Calificación Total dividido por el porcentaje de cada Parámetro
Fuente: Mauricio Estrada –William Adriano

En la Ilustración 30 se puede observar con mayor detalle el valor de calificación total obtenida por cada uno de los portales cautivos sujetos a estudio, destacando entre los cuatro a ChilliSpot como posible ganador.

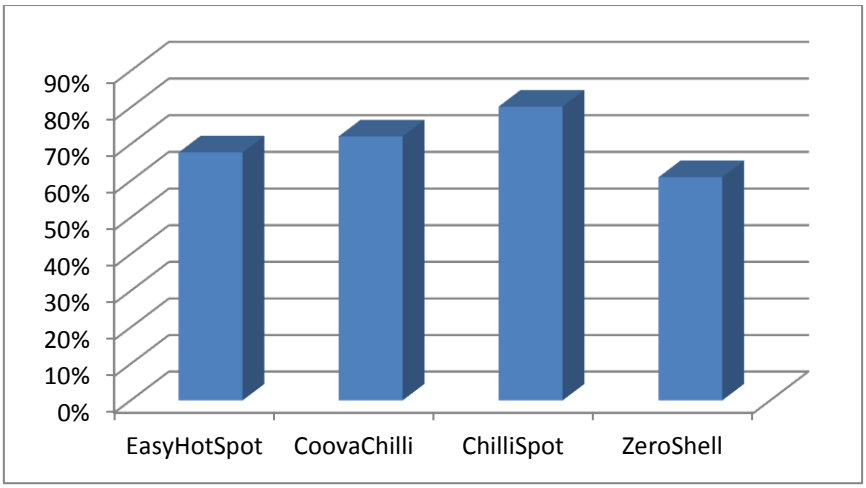


Ilustración 30 Grafica Resumen Total de Comparación
Fuente: Mauricio Estrada –William Adriano

Dado que el número de características evaluadas en el análisis comparativo de los portales cautivos, son en total 5, valoradas cada uno con un máximo de 4 puntos y con un total de 20 puntos equivalente al 100%, se puede concluir utilizando la grafica

- EasyHotSpot obtuvo un total de 13.5 puntos equivalente al 67.55%, es decir la aplicación es sencilla de implementar, sin embargo a lo que se refiere a seguridad, esta puede ser burlada con un ataque spoofing.

- CoovaChilli obtuvo un total de 14.4 puntos equivalente al 72.125%, sus puntos fuertes radican en sus medidas de control por usuario y ancho de banda, sin embargo los tiempos de respuesta de autenticación son elevados, además de que solo funciona en pc y/o servidores con arquitectura de 32 bits lo que podría dificultar su funcionamiento a largo plazo por el ya conocido error Y2K38 y su número necesario de librerías y paquetes para su implementación lo tornan dificultoso de instalar, por lo cual se necesitaría un administrador del sistema con conocimientos intermedios den Linux.

- ChilliSpot obtuvo un total de 16.05 puntos equivalente al 80.25% sus puntos débiles radican en el total de complementos necesarios para su implementación, sin embargo cada uno de ellos se encuentran disponibles en casi cualquier mirror Linux, sus puntos fuertes radican en las medidas de control y monitoreo que pueden ser activadas y/o configuradas en el portal lo que lo hace un sistema adaptable a las necesidades de cada institución, en lo que se refiere a seguridad su único defecto radica al igual que EasyHotSpot y CoovaChilli en la duplicación MAC.

- ZeroShell obtuvo un total de 12.2 puntos equivalentes a 61% sus puntos fuertes radican en los tiempos de respuesta de autenticación, además de la facilidad de editar la interfaz de Login de manera gráfica sin la necesidad de conocer lenguajes de programación, sus puntos débiles se encuentran en las medidas de control ya que para activarlas o conseguir todos los módulos del portal cautivo es necesario realizar donaciones al proyecto por medio de PayPal

4.3 Resultados de la Comparación

Después de realizar la comparación entre los diferentes sistemas de los portales cautivos, se llega a observar que:

- Los costos de implementación de cualquier portal cautivo son mínimos tanto en software y hardware.

- Los portales cautivos trasmiten su información mediante un cifrado SSL.

- Todos los portales cautivos sujetos a estudio con excepción de ZeroShell son compatibles para diferentes plataformas y navegadores web, los cuales pueden encontrarse en diferentes dispositivos como Laptops, PDAs o celulares.

- EasyHotSpot, CoovaChilli, ChilliSpot, y ZeroShell poseen soporte multilenguaje algunos más que otros, lo que permite al administrador un mejor entendimiento de la aplicación.

- ChilliSpot es una herramienta que cumple con las necesidades de la Escuela "Gabriel García Moreno" la cual permite mejorar el rendimiento de la red y la que brinda mejores beneficios para el control de usuarios.

CAPÍTULO V

5. Implementación del portal cautivo seleccionado en la Escuela Gabriel García Moreno.

5.1 Visión del Sistema

El portal cautivo que se va a implementar ofrece un servicio de autenticación centralizada para la autorización e ingreso al internet, el objetivo del sistema es mejorar el rendimiento del ancho de banda de la institución así como llevar el control de cada uno de los usuarios.

El servicio una vez montado en la red institucional permitirá que solo usuarios que pertenecen a la institución educativa puedan utilizar los recursos de internet, El sistema será gestionado por un único Administrador de la red que actuara tanto como para registro de usuarios así como para soporte del sistema.

Dentro del sistema se han diferenciado dos tipos de usuarios como son: usuarios finales y el administrador de la red.

El Administrador, tiene el derecho de supervisar el sistema, realizar reportes del sistema, gestionar cuentas de usuario (crear, modificar, eliminar asignar grupos y bloquear usuarios), Gestionar Contenido, Monitoreo, etc.

El Usuario final, que desee obtener acceso a internet por medio de puntos inalámbricos deberá poseer una cuenta registrada de usuario en el sistema para acceder a los beneficios que presenta la red.

5.2 Descripción del proceso de funcionamiento del Portal Cautivo

1. El usuario final se conecta a la red inalámbrica.
2. El usuario final ingresa a cualquier navegador web.
3. El portal cautivo se ejecuta como método de seguridad, y redirección cualquier página que el usuario solicite a una página donde debe

ingresar sus datos (nombre usuario, contraseña) los mismo que será autenticados.

4. El portal cautivo recibe los datos y los envía al servidor RADIUS para que los mismos sean verificados.
5. El servidor RADIUS verifica si las credenciales enviadas por el usuario concuerdan con la información ingresada dentro de la base de datos del servidor.
6. Si los datos enviados por el usuario concuerdan con los de la base de datos, el usuario será autenticado exitosamente y podrá acceder al servicio de internet.
7. En caso de que las credenciales no concuerden con los de la base de datos, el servidor RADIUS denegara el acceso al servicio de internet.

A continuación se muestra la topología física que tendrá el sistema en la red de la Escuela Gabriel García Moreno.

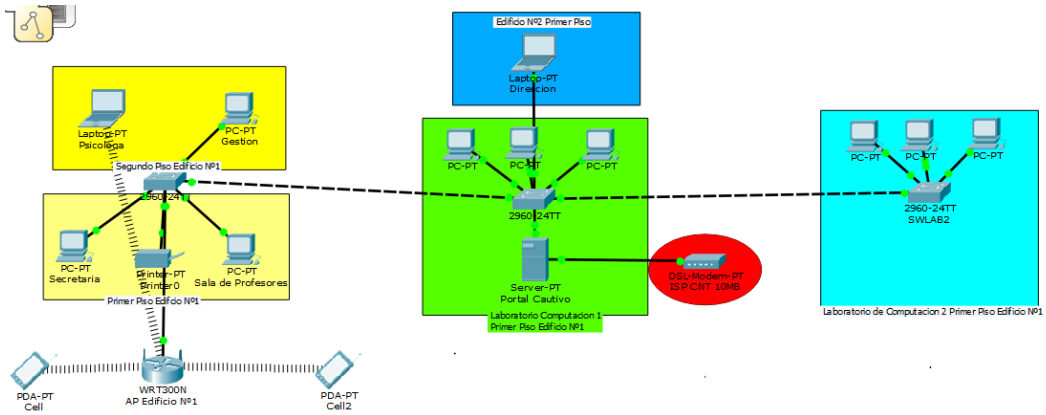


Ilustración 31 Topología Física Red Institucional
Fuente: Mauricio Estrada

5.3 Diseño e Implementación

5.3.1 Diagramas de caso de uso

El diagrama de casos de uso representa la forma en como un Cliente (Actor) opera con el sistema (aplicación) en desarrollo, además de la forma, tipo y orden en como los elementos interactúan.

En la red de la Escuela Gabriel García Moreno se diferencias dos tipos de usuarios, un administrador y un usuario final, a continuación se detalla cada uno de ellos:

a) El administrador de la red realiza la gestión de usuarios, es decir realizara acciones como: añadir, remover, editar, bloquear a los mismos, realizar actualizaciones en la interfaz, así como condicionar la navegación de usuarios o grupo de usuarios, etc.

Debe ser capaz de gestionar el contenido de la aplicación, gestionar la publicidad, monitorizar que todos los servicios se encuentren en ejecución, además de realizar informes de tráfico de red, la actividad de los usuarios.

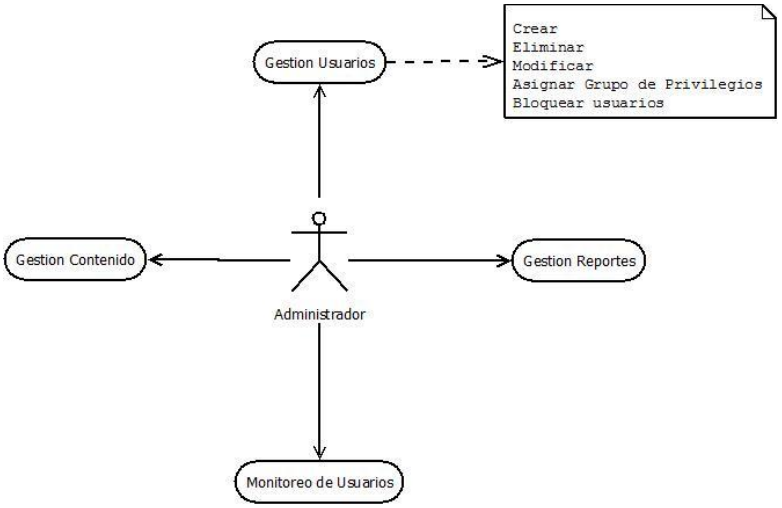


Ilustración 32 Caso de Uso Usuario Administrador
Fuente: Mauricio Estrada

El segundo tipo de actor es el usuario final, el cual puede ser solo personas que trabajan dentro de la institución educativa y busca acceso a Internet, la interacción que tendrá con el portal será básica ya que solamente deberá registrarse donde el administrador e ingresar sus datos (Login y Password) además de aceptar las condiciones de uso para poder navegar desde la institución educativa.

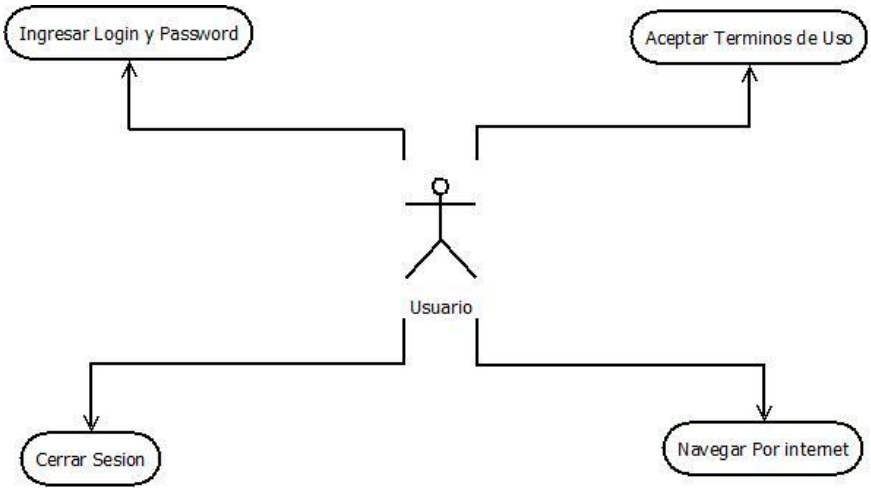


Ilustración 33 Caso de Uso Usuario Final
Fuente: Mauricio Estrada – William Adriano

5.4 Diseño del Sistema

La solución para la red de la Escuela Gabriel García Moreno está basada en la implementación del portal cautivo que permita controlar el acceso a los usuarios y mejorar el uso de la red.

El estudio centra su atención en la comparación de 4 diferentes de portales cautivos, el cual determino que el que se adapta de mejor manera a las necesidades de la institución educativa y el que brinda mejores prestaciones es ChilliSpot, al ser una herramienta open source y de necesidades mínimas respecto a hardware.

La aplicación ChilliSpot se compone de dos partes que son:

- Una aplicación denominada chilli el cual es el portal cautivo y cumple funciones, servidor DHCP, cliente RADIUS, Proxy-RADIUS.
- Un archivo cgi ubicado en el servidor web llamado hotspotlogin.cgi un script programado en lenguaje Perl el cual se encarga de la comunicación entre el cliente y el portal, Este script genera un protocolo de autenticación llamado desafío-CHAP para validar el usuario y la clave de acceso del cliente, a través del servidor web cifrado con el protocolo de seguridad HTTPS y es el enviado al chilli.

5.5 Software Utilizado

La solución para la implementación del sistema está basado en código abierto y publicado bajo licencia GPL lo que significa que la solución es libre.
Como sistema operativo se utilizó una distribución Linux Basada en RedHat y en una versión final o estable como es Centos 6.4 reléase Final.

```
[root@localhost mau]# lsb_release -idc
Distributor ID: CentOS
Description:    CentOS release 6.4 (Final)
Codename:       Final
```

Ilustración 34 Versión del S.O. Utilizado
Fuente: Mauricio Estrada – William Adriano

El software del servidor se compone de varios componentes los cuales son detallados a continuación:

- MySQL es un sistema de gestión de base de datos. Es decir, una base es una colección estructurada de datos y el usuario necesita un administrador para poder agregar, acceder o procesar esta información guardada en el ordenador, y esta es la función que realiza MySQL.

```
[root@localhost mau]# rpm -qa mysql
mysql-5.5.37-1.el6.remi.i686
```

Ilustración 35 Versión Mysql
Fuente: Mauricio Estrada – William Adriano

- El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual.

```
[root@localhost mau]# rpm -qa httpd
httpd-2.2.15-30.el6.centos.i686
```

Ilustración 36 Versión Apache
Fuente: Mauricio Estrada – William Adriano

- FreeRadius es uno de los más populares servidores RADIUS, y es totalmente software libre (licencia GPL v2).
  Usar FreeRadius permite autentificación y autorización para una red

centralizada y minimiza el trabajo de reconfiguración que se debe hacer al añadir o eliminar usuarios.

```
[root@localhost mau]# rpm -qa freeradius
freeradius-2.1.12-4.el6 3.i686
```

Ilustración 37 Versión FreeRadius
Fuente: Mauricio Estrada – William Adriano

- Los servicios de cortafuegos y NAT son proporcionados por iptables, un paquete de software que permite configurar las tablas que contienen cadenas de normas para el tratamiento de los paquetes.

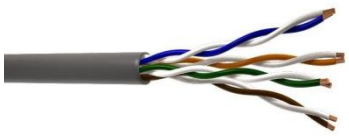
- Chillispot es una fuente de portal cautivo de código abierto o controlador de punto de acceso LAN inalámbrico. Se utiliza para la autenticación de usuarios de una LAN inalámbrica.

```
[root@localhost mau]# rpm -qa chillispot
chillispot-1.1.0-1.i386
```

Ilustración 38 Versión ChilliSpot
Fuente: Mauricio Estrada – William Adriano

- El protocolo DHCP es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente, en este caso Chillispot es aquel que brinda el servicio.

5.6 Materiales y Equipos Utilizados

Material	Cantidad	Imagen
Switch D-Link de 8 y 12 puertos	2 equipos	
Cable UTP categoría 5-e	10 metros	

Conectores RJ 45	10	
Router Inalámbrico N a 300Mbp	2 equipos	
Tarjeta de red D-link 150mbps	1 Tarjeta	

Tabla 22 Tabla de materiales Utilizados
Fuente: Mauricio Estrada –William Adriano

5.6 Herramientas Utilizadas

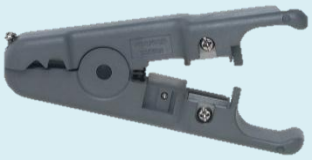
Herramienta	Cantidad	Imagen
Ponchadora	2	
Medidor de Continuidad	1	
Peladora de Cables	1	

Tabla 23 Herramientas Utilizadas
Fuente: Mauricio Estrada –William Adriano

5.7 Proceso de Instalación Infraestructura

1) Se realiza el cableado para la incorporación de los nuevos equipos como son Router Inalámbrico, Switch Laboratorio 2, PC servidor, etc.
2) Con ayuda de la peladora de cables se procede a corta 2cm de la envoltura plástica con la que se encuentra cubierta los cables UTP 5-e, para posteriormente organizar los cables según la norma indicada.

Ilustración 39 Peladora de cable UTP
Fuente: http://cocodrilosa.com/productos.php?item1=20&cat=3

3) Una vez rectos y organizados los cables se inserta los hilos en el conector RJ-45 para luego ingresarlo en el zócalo de la ponchadora

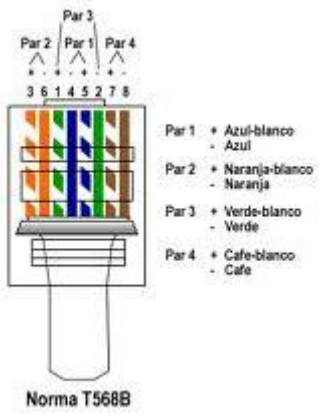


Ilustración 40 Estándar T - 568B
Fuente: http://ponchadodecablesbrissalluvia.blogspot.com/

4) Se realiza el proceso de ponchado de los cables UTP 5-e con la norma TIA/EAI 568B.
5) Se comprueba que todos los cables este correctamente instalados por medio del Medidor de Continuidad.

Ilustración 41 Medidor de Continuidad para cable UTP
Fuente: http://www.ciudadwireless.com/erize_erz-tester_tester_rj45-p-2181.html

6) Posteriormente se procede a instalar la segunda tarjeta de red en la pc servidor, en la imagen que se muestra se puede comprobar que el ordenador posee dos tarjetas de red las cuales se usaran par la red interna y para la conexión a internet

Ilustración 42 Servidor con dos interfaces de Red
Fuente: Mauricio Estrada – William Adriano

Como se puede observar en la zona inferior izquierda se encuentra la nueva tarjeta de red PCI.

7) Se realiza la ubicación del cableado del Switch y el ordenador dentro de las canaletas.
8) Se ubica el nuevo Router inalámbrico, de manera que pueda cubrir de mejor manera el edificio Nº1.

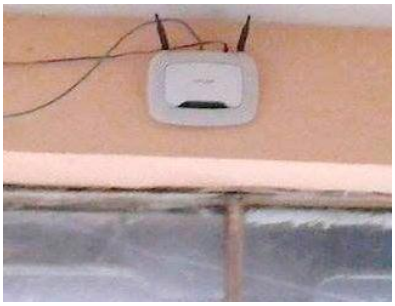


Ilustración 43 AP Edificio Central
Fuente: Mauricio Estrada –William Adriano

Como se puede observar el AP se encuentra ubicado en la parte superior de la puerta de ingreso al edificio Nº1 ya que es el lugar donde se encuentra tanto la secretaria de la institución, la sala de profesores y está frente al laboratorio de computación 2.

5.8 Implementación y Configuración del Portal Cautivo ChilliSpot

En este capítulo se detalla la instalación y configuración de todas las herramientas tanto software como hardware que trabajan en conjunto para levantar el servicio de portal cautivo.

Para realizar la implementación se iniciara por describir la instalación de cada uno de las aplicaciones necesarias para levantar el servicio y posteriormente su configuración para su correcto funcionamiento.

5.8.1 Servidor Centos 6.4

Centos tiene numerosas ventajas sobre algunos de los proyectos de otros clones que incluyen:

- La principal ventaja es que se obtiene un conjunto estable de la mayoría de paquetes que por lo general solo incluyen correcciones de errores.
- Una comunidad de usuarios activa y creciente, reconstruido rápidamente, probado.
- Una extensa red de servidores espejos, los desarrolladores que están localizables y sensible, múltiples vías de apoyo gratuitos, comoel IRC Chat en vivo **,** las listas de correo **,** Foros **,** una dinámica depreguntas frecuentes**.**
- Está dirigido a personas que buscan la estabilidad de clase empresarial del sistema operativo sin el costo de la certificación y apoyo.

Ilustración 44 Características del CPU y del S.O
Fuente: Mauricio Estrada –William Adriano

Como primer punto para la implementación del portal cautivo se realiza la instalación del sistema operativo Centos 6.6 el cual será la base en donde se implementara el portal cautivo ChilliSpot. A continuación se detallan las características del servidor de la implementación.

Características	
Procesador	Core Duo 2
MainBoard	Intel 2,53
Disco Duro	200 GB
Memoria RAM	1 GB
Interfaces de Red	Eth0 FastEthernet Eth1 FastEthernet

Tabla 24 Características Hardware Servidor
Fuente: Mauricio Estrada –William Adriano

5.8.2 Requisitos previos a la Instalación del Portal Cautivo.

Antes de iniciar la instalación del portal cautivo ChilliSpot se debe:

1. Acceder a la terminal del sistema como súper-usuario o ROOT con el fin de evitar inconvenientes de permisos durante la instalación y modificación de archivos del sistema, por medio del comando **su** donde posteriormente no pedirá la contraseña.

```
[gmoreno@localhost ~]$ su
Contraseña:
```

Ilustración 45 Inicio Súper Usuario
Fuente: Mauricio Estrada –William Adriano

2. Poseer una conexión estable de internet ya que los paquetes necesarios en la instalación se descargaran del mirror más cercano de Linux.

3. Instalar todas las actualización disponibles de los repositorios antes de empezar la configuración de los archivos del sistema, mediante el comando **yum update.**

```
[root@localhost gmoreno]# yum update
```

Ilustración 46 Actualización Sistema Operativo Centos
Fuente: Mauricio Estrada –William Adriano

4. Instalar el paquete **vim** que será utilizado para la edición de los archivos de configuración durante el proceso de instalación del portal cautivo mediante los comandos: **yum –y install vim**

5.8.3 Servidor base de Datos

El primer paquete a instalar para el funcionamiento del portal cautivo es un gestor de base de datos, en este caso se utiliza **MySQL-SERVER** para la instalación.

1. Se descarga e instala el paquete de MySQL, mediante los comandos: **yum –y install mysql mysql-server**

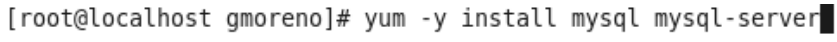


Ilustración 47 Instalación de Mysql
Fuente: Mauricio Estrada –William Adriano

2. Luego de que termine el tiempo de descarga e instalación se proecede a levantar el servicio mediante el siguiente comando: **service mysqld start**

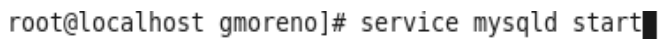


Ilustración 48 Iniciar servicio Mysql
Fuente: Mauricio Estrada –William Adriano

5.8.4 Servidor RADIUS

Para la instalación del protocolo RADIUS se utiliza FreeRadius el cual es una aplicación en código abierto.

1. Se descarga e instala el paquete **FreeRadius** con el siguiente comando: **yum –y install freeradius freeradius-mysql freeradius-utils**

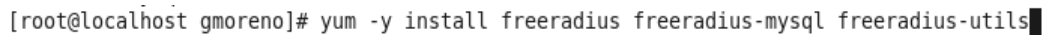


Ilustración 49 Descargar Paquete FreeRadius
Fuente: Mauricio Estrada –William Adriano

2. Se asignara una clave de acceso al usuario root de Mysql, mediante el comando: **mysqladmin –uroot password ‘ingresoroot’**

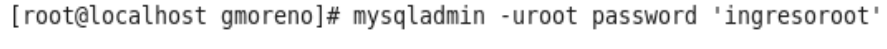


Ilustración 50 Asignación De Clave de Ingreso
Fuente: Mauricio Estrada –William Adriano

3. A continuación se creara la base de datos radius, la misma que trabajara con el servidor RADIUS con el comando: **mysqladmin -uroot –pingresoroot créate radius**

```
[root@localhost gmoreno]# mysqladmin -uroot password 'ingresoroot'
[root@localhost gmoreno]# mysqladmin -uroot -pingresoroot create radius
```

Ilustración 51 Creación de Base de Datos
Fuente: Mauricio Estrada –William Adriano

4. Despues de accederá a la consola de Mysql, como usuario root, mediante la línea de comandos: **mysql –uroot –pingresoroot**

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost gmoreno]# mysql -uroot -pingresoroot
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Ilustración 52 Consola de inicio Mysql
Fuente: Mauricio Estrada –William Adriano

5. Se designara permisos al usuario RADIUS que se creó al momento de instalar el FreeRadius y se le asignara una contraseña, mediante el siguiente comando: **GRANT all ON radius.* TO radius@localhost IDENTIFIED by “rbradius”**

- **Usuario:** radius
- **Contraseña:** rbradius

```
mysql> GRANT all ON radius.* TO radius@localhost IDENTIFIED BY 'rbradius';
```

Ilustración 53 Ingreso de permisos de base de Datos
Fuente: Mauricio Estrada –William Adriano

6. A continuación se saldrá de la consola Mysql mediante el comando: **exit.**

7. Ahora, se utilizara el usuario radius y la base de datos radius recién creadas para importar las tablas necesarias para el funcionamiento de FreeRadius.

- **uradius:** Usuario radius
- **prbradius:** Contraseña del usuario radius
- **radius:** Base de datos creada

```
[root@localhost gmoreno]# mysql -uradius -prbradius radius < /etc/raddb/sql/mysql/cui.sql
[root@localhost gmoreno]# mysql -uradius -prbradius radius < /etc/raddb/sql/mysql/ippool.sql
[root@localhost gmoreno]# mysql -uradius -prbradius radius < /etc/raddb/sql/mysql/nas.sql
[root@localhost gmoreno]# mysql -uradius -prbradius radius < /etc/raddb/sql/mysql/schema.sql
[root@localhost gmoreno]# mysql -uradius -prbradius radius < /etc/raddb/sql/mysql/wimax.sql
```

Ilustración 54 Importar tablas de Radius
Fuente: Mauricio Estrada –William Adriano

8. A continuación se editara el archivo **/etc/raddb/radiusd.conf,** mediante la línea de comando: **vim /etc/raddb/radiusd.conf**

```
[root@localhost gmoreno]# mysql -uradius -prbradius rad
[root@localhost gmoreno]# vim /etc/raddb/radiusd.conf
```

Ilustración 55 Edición del Archivo de Configuración Radius
Fuente: Mauricio Estrada –William Adriano

9. Se des comenta la línea que dice **$INCLUDE sql.conf** borrado el signo de numeral #.

```
#  Now in another file, because it is very large.
#
$INCLUDE eap.conf

#  Include another file that has the SQL-related configuration.
#  This is another file only because it tends to be big.
#
$INCLUDE sql.conf

#
#  This module is an SQL enabled version of the counter module.
#
#  Rather than maintaining seperate (GDBM) databases of
```

Ilustración 56 Configuración Radius
Fuente: Mauricio Estrada –William Adriano

10. Después, se tendrá que editar el archivo **/etc/raddb/sql.conf**, mediante la siguiente línea de comandos: **vim /etc/raddb/sql.conf**

```
[root@localhost gmoreno]# vim /etc/raddb/radiusd.cc
[root@localhost gmoreno]# vim /etc/raddb/sql.conf
```

Ilustración 57 Configuracion Freeradius
Fuente: Mauricio Estrada –William Adriano

11. Después defino los valores para la conexión a la base de datos, modificando:

#Connection info:

Server = "localhost"

#port = 3306

Login = "radius"

Password = "rbradius"

```
#  Set the database to one of:
#
#       mysql, mssql, oracle, postgresql
#
database = "mysql"

#
#  Which FreeRADIUS driver to use.
#
driver = "rlm_sql_${database}"

# Connection info:
server = "localhost"
#port = 3306
login = "radius"
password = "rbradius"

# Database table configuration for everything except Oracle
radius_db = "radius"
# If you are using Oracle then use this instead
# radius_db = "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SID=your_sid)))"
```

12. También se des comentara la línea **readclients = yes**

13. Ahora se editara el archivo **default** mediante la línea de comando: **vim /etc/raddb/sites-enabled/default**

```
[root@localhost gmoreno]# vim /etc/raddb/sites-enabled/default
```

Ilustración 58 Configuración FreeRadius
Fuente: Mauricio Estrada –William Adriano

14. En el archivo **default** se elimina el signo # en la sección **authorize** al inicio de la línea donde este **sql.**

```
#  If you don't use "radlast", you can delete this line.
unix

#
#  For Simultaneous-Use tracking.
#
#  Due to packet losses in the network, the data here
#  may be incorrect.  There is little we can do about it.
radutmp
sradutmp

#  Return an address to the IP Pool when we see a stop record.
main_pool

#
#  Log traffic to an SQL database.
#
#  See "Accounting queries" in sql.conf
sql
```

Ilustración 59 Activar comandos SQL
Fuente: Mauricio Estrada –William Adriano

15. En el mismo archivo es necesario eliminar el signo numeral al inicio de la línea donde esté ubicado **sql** para poder tener la sección **accounting** activa

```
#  Accounting.  Log the accounting data.
#
accounting {
        #
        #  Create a 'detail'ed log of the packets.
        #  Note that accounting requests which are proxied
        #  are also logged in the detail file.
        detail
#       daily

        #  See "Accounting queries" in sql.conf
        sql
```

Ilustración 60 Activar Procesos Sql
Fuente: Mauricio Estrada –William Adriano

16. Para activar la emisión de logs en el servidor radius, en el mismo archivo se elimina el signo # en la línea **sql** en la sección **posth auth,** el registro de logs generados se encuentra en /var/log/radius

5.8.5 Creación de Usuario en base de datos del Portal Cautivo

1. Se ingresa a la consola de mysql con las credenciales: **mysql –uradius –prbradius radius**

```
[root@localhost gmoreno]# mysql -uradius -prbradius radius
```

Ilustración 61 Ingresar a Mysql
Fuente: Mauricio Estrada –William Adriano

2. Después se ingresa un usuario prueba en la tabla **radcheck,** el cual no servirá para verificar el funcionamiento del servidor FreeRadius y la base de datos Mysql, mediante: **INSERT INTO radcheck (username, attribute, op, value) VALUES ('mauricio', 'Clearext-Password', ':=', '1234567890);**

```
mysql> INSERT INTO radcheck (username, attribute, op, value) VALUES ('mauricio', 'Clearext-Password', ':=', '1234567890');
Query OK, 1 row affected (0.00 sec)
```

Ilustración 62 Insertar usuario prueba
Fuente: Mauricio Estrada –William Adriano

3. Se puede salir de la consola de mysql con el comando **exit** e inicia el servicio radius con **service radiusd start** para realizar la prueba, con el comando: **radtest nombreusuario constraseñausuario localhost 1812 testing123**

```
mysql> exit
Bye
[root@localhost gmoreno]# service radiusd start
Iniciando radiusd:                                         [  OK  ]
[root@localhost gmoreno]# radtest mauricio 1234567890 localhost 1812 testing123
Sending Access-Request of id 213 to 127.0.0.1 port 1812
        User-Name = "mauricio"
        User-Password = "1234567890"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
        Message-Authenticator = 0x00000000000000000000000000000000
rad recv: Access-Reject packet from host 127.0.0.1 port 1812, id=213, length=20
```

Ilustración 63 Proceso de Respuesta Correcto FreeRadius
Fuente: Mauricio Estrada –William Adriano

El resultado deberá confirmar que radius está autentico correctamente.

5.8.6 Servidor Apache HTTP

Para que la página de Login funcione correctamente es necesario que exista un servidor web para lo cual se realiza el siguiente proceso:

1. Se descarga e instala el servicio httpd mediante: **yum install –y httpd**

```
[root@localhost gmoreno]# yum -y install httpd
```

Ilustración 64 Iniciar Servicio Apache
Fuente: Mauricio Estrada –William Adriano

2. Se inicia el servicio apache para verificar que el funcionamiento correctamente, mediante **service httpd start**

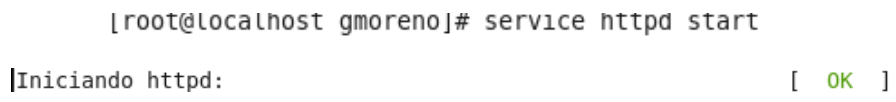


Ilustración 65 Inicio Servicio Apache
Fuente: Mauricio Estrada –William Adriano

5.8.7 Portal Cautivo ChilliSpot

Finalmente se instala el portal es si, el cual dará acceso o no al servicio de internet, en este caso ChilliSpot por sus altas medidas de seguridad sobre redes WLAN.

1. Se descarga el instalador de ChilliSpot de su página oficial mediante el comando: **wget http://www.chillispot.info/download/chillispot-1.1.0.i386**

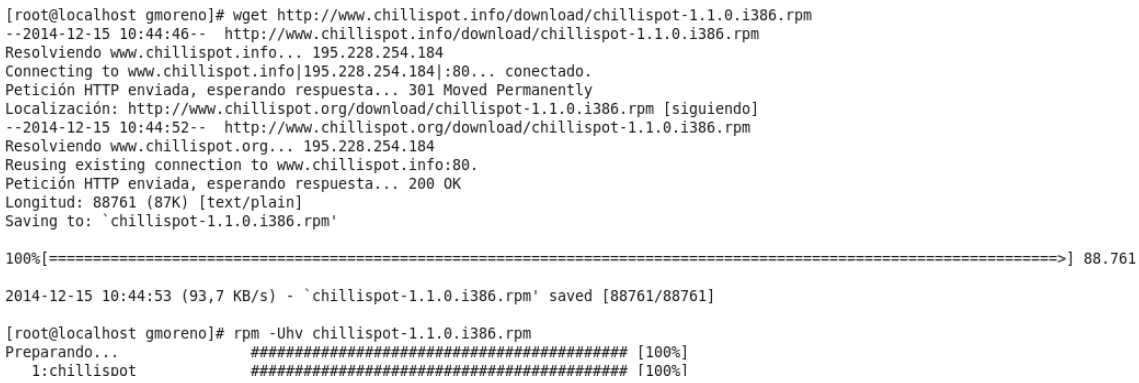


Ilustración 66 Instalación ChilliSpot
Fuente: Mauricio Estrada –William Adriano

2. Ahora se ejecuta el instalador descargado recientemente mediante: **rpm –Uhvchillispot-1.1.0.i386.rpm.**

3. A continuación se copiara la página de autenticación del ChilliSpot mediante: **cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin/**

Ilustración 67 Copia de Interfaz de Login ChilliSpot
Fuente: Mauricio Estrada –William Adriano

4. Seguido se asigna permisos de propietario APACHE para que pueda ejecutarse correctamente con el siguiente comando: **chown –R apache.apache /var/www/cgi-bin/hotspotlogin.cgi** y **chmod 777 /var/www/cgi-bin/hotspotlogin.cgi**

```
[root@localhost gmoreno]# chown apache.apache /var/www/cgi-bin/hotspotlogin.cgi
[root@localhost gmoreno]# chmod 777 /var/www/cgi-bin/hotspotlogin.cgi
```

Ilustración 68 Asignación de Permisos y Niveles de Ejecución
Fuente: Mauricio Estrada –William Adriano

5. Se define el direccionamiento lógico tanto en red interna como en red externa, las cuales deben configurarse dentro del archivo en Centos 6.4. **vim /etc/sysconfig/network-scrip/ifcg-eth…**

Eth0 Red Externa (ISP)
IP = 192.168.1.10
NETWORK = 192.168.1.0
NETMASK = 255.255.255.192

Eth1 Red Interna (LAN Institucional)
IP = 192.168.10.1
NETWORK = 192.168.10.0
NETMASK = 255.255.255.0

6. A continuación se activa NAT o ruteo para lo cual se edita el archivo con el comando: **vim /etc/sysctl.conf** y se cambia el valor de 0 por 1 en la línea **net.ip_fordward = 0**

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Ilustración 69 Activando Ruteo en Centos
Fuente: Mauricio Estrada –William Adriano

7. Seguido se reinicia el servicio de red mediante el comando: **service network restart** en caso de presentar algún error se puede ingresar el comando para detener el demonio el cual es: **service NetworkManager Stop**

```
[root@localhost mau]# service network restart
Interrupción de la interfaz eth0:                          [  OK  ]
Interrupción de la interfaz de loopback:                   [  OK  ]
Activación de la interfaz de loopback:                     [  OK  ]
Activando interfaz eth0:
Determinando la información IP para eth0...
```

Ilustración 70 Reinicio Interfaces de Red
Fuente: Mauricio Estrada –William Adriano

8. Para mejorar los niveles de seguridad por medio de los IPTABLES y dejar habilitado solo los puertos necesarios para el funcionamiento del sistema se procede editar el archivo **rc.local** mediante: **vim /etc/rc.local** y se ingresa las nuevas reglas IPTABLES.

```
IPTABLES="/sbin/iptables"
EXTIF="eth0"
INTIF="eth1"


#flush all rules
$IPTABLES -F
$IPTABLES -F -t nat
$IPTABLES -F -t mangle

#Set default behaviour
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT

#Allow related and established on all interfaces (input)
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Allow releated, established and ssh on $EXTIF. Reject everything else
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $EXTIF -j REJECT

$IPTABLES -A INPUT -i $INTIF -j DROP

$IPTABLES -A INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 443 --syn -j ACCEPT

$IPTABLES -A INPUT -p tcp -m tcp --dport 3990 --syn -j ACCEPT

$IPTABLES -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

$IPTABLES -A INPUT -i lo -j ACCEPT

$IPTABLES -A FORWARD -i $INTIF -j DROP
$IPTABLES -A FORWARD -o $INTIF -j DROP

$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
```

Ilustración 71 Reglas del Firewall y ChilliSpot
Fuente: Mauricio Estrada –William Adriano

9. Para ejecutar el archivo de las iptables se teclea **./rc.local** dentro del directorio **/etc**

10. Se cambia los runlevels o niveles de ejecución con el fin de que se ejecuten de manera automática en los niveles 3, 4, 5 al reiniciar el sistema, mediante los comandos:

```
root@localhost ~]# chkconfig --level 345 httpd on
root@localhost ~]# chkconfig --level 345 mysqld on
root@localhost ~]# chkconfig --level 345 radiusd on
root@localhost ~]# chkconfig --level 345 chilli on
```

Ilustración 72 Niveles de Ejecución en Linux
Fuente: Mauricio Estrada –William Adriano

5.8.8 Configuración del Portal Cautivo

Para La configuración del ChilliSpot, se modificara el script **chilli.conf** ubicado en el directorio **/etc/chilli.conf** mediante el comando: **vim /etc/chilli.conf.**

```
root@localhost mau]# vim /etc/chilli.conf
```

Ilustración 73 Configuración de ChilliSpot
Fuente: Mauricio Estrada –William Adriano

1. Primero se modificara el apartado TUN parameters donde se eliminara el signo # y se asignara la ip de la red con la que trabajara Chillispot en este caso: **net 192.168.10.0/24,** se realiza el mismo procedimiento de **interval 3600** y **pidfile /var/run/chilli.pid**

```
# TUN parameters

# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
net 192.168.10.0/24
```

Ilustración 74 Activación TUN (tunel) ChilliSpot
Fuente: Mauricio Estrada –William Adriano

2. A continuación en los apartados radiusserver1 y radiusserver2, se modificara con la dirección 127.0.0.1 en ambos.

Radiuslisten1 127.0.0.1

Radiuslisten2 127.0.0.1

```
# Radius parameters

# TAG: radiuslisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
radiuslisten 127.0.0.1

# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.
radiusserver1 127.0.0.1

# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 127.0.0.1
```

Ilustración 75 Activación parámetro Radius en ChilliSpot
Fuente: Mauricio Estrada –William Adriano

3. Posteriormente se activa el puerto con el que se comunicara ChilliSpot y el campo **radiussecret** con una contraseña la cual debe ser exactamente la misma con el servicio radius.

```
# TAG: radiusauthport
# Radius authentication port
# The UDP port number to use for radius authentication requests.
# The same port number is used for both radiusserver1 and radiusserver2
# Normally you do not need to uncomment this tag.
radiusauthport 1812

# TAG: radiusacctport
# Radius accounting port
# The UDP port number to use for radius accounting requests.
# The same port number is used for both radiusserver1 and radiusserver2
# Normally you do not need to uncomment this tag.
radiusacctport 1813

# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret tesis

# TAG: radiusnasid
# Radius NAS-Identifier
# Normally you do not need to uncomment this tag.
#radiusnasid nas01
```

Ilustración 76 Activación de Puertos de comunicación entre Radius y ChilliSpot
Fuente: Mauricio Estrada –William Adriano

El archivo de configuración de Radius en el cual se debe ingresar la misma contraseña se encuentra en **vim /etc/raddb/clients.conf** en la línea **secret = contraseña** de la siguiente manera:

```
#  And is at LEAST 8 characters long, preferably 16 characters in
#  length.  The secret MUST be random, and should not be words,
#  phrase, or anything else that is recognizable.
#
#  The default secret below is only for testing, and should
#  not be used in any real environment.
#
secret          = tesis
```

Ilustración 77 Contraseña entre ChilliSpot Y Radius
Fuente: Mauricio Estrada –William Adriano

4. Dentro del mismo archivo de configuración de chilli **vim /etc/chilli.conf** se busca DHCP parameters y se elimina el signo # de **dhcpif** en el cual se establece la interfaz de la red interna en este caso **eth1** o la interfaz por la cual se enviara el servicio de DHCP.

```
# DHCP Parameters

# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth1
```

Ilustración 78 Interfaz donde escucha DHCP
Fuente: Mauricio Estrada –William Adriano

5. Ahora se busca el apartado **uamserver,** el cual se editara la IP en la que se encuentra la página de Login, también se establece la contraseña **uam secret chilliweb** con la que se comunicara ChilliSpot con el servidor web

```
# Universal access method (UAM) parameters

# TAG: uamserver
# URL of web server handling authentication.
uamserver https://192.168.10.1/cgi-bin/hotspotlogin.cgi

# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
#uamhomepage http://192.168.10.1/index.html
#uamhomepage http://192.168.10.1/cgi-bin/hotspotlogin.cgi
# TAG: uamsecret
# Shared between chilli and authentication web server
uamsecret chilliweb
```

Ilustración 79 Configuración de Pagina de Login
Fuente: Mauricio Estrada –William Adriano

6. Ahora se editara el script de Login del sistema chilli con el siguiente comando: **vim /var/www/cgi-bin/hotspotlogin.cgi**

7. A continuación, se des comentará las líneas **$uamsecret**, y **$userpassword,** se elimia el numeral # al inicio de cada una de ellas, y se establecerá en **$uamsecret** el mismo password asignado en el aportado **uamsecret** del archivo de configuración **chilli.conf** y en **$userpassword** se cambia el valor de 0 por 1, de la siguiente manera:
$uamsecret = “chilliweb”; $userpassword= 1;

```
# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "chilliweb";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;
```

Ilustración 80 Contraseña ChilliSpot e Interfaz de Login
Fuente: Mauricio Estrada –William Adriano

8. Por último se inicia el servicio chilli con el comando: **service chilli start**

```
[root@localhost mau]# service chilli start
```

Ilustración 81 Inicio del Servicio ChilliSpot
Fuente: Mauricio Estrada –William Adriano

5.8.9 Gestores de Administración

Con la finalidad de facilitar la administración del portal cautivo se instalara dos gestores de interfaz gráfica, donde se podrá manejar el funcionamiento mysql y la gestión del portal cautivo.

5.8.9.1 Instalación de PhpMyAdmin

1. Primero se procede a instalar todas las dependencias necesarias para que PhpMyAdmin pueda trabajar correctamente, mediante: **yum install –y php php-mysql php-mbstring httpd mod_ssl.**

Ilustración 82 Descarga de Dependencias
Fuente: Mauricio Estrada –William Adriano

2. Después se debe habilitar el repositorio EPEL. Mediante la siguiente línea de comandos: **rpm –ivh http://ftp.jaist.ac.jp/pub/Linux/Fedora/epel/6/i386/epel-release-6-8.noarch.rpm**

Ilustración 83 Activar Repositorio Epel
Fuente: Mauricio Estrada –William Adriano

3. Posteriormente se actualiza los repositorios mediante: **yum check-update**

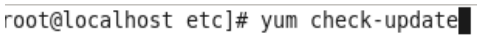


Ilustración 84 Actualización Repositorios
Fuente: Mauricio Estrada –William Adriano

4. Ahora ya se puede instalar el paquete PhpMyAdmin mediante el comando: **yum –y install PhpMyAdmin.**

5. Después se debe editar el archivo de configuración **httpd.conf** para la ejeucion de PhpMyAdmin mediante la línea de comandos: **vim /etc/httpd/conf/httpd.conf**

6. Seguidamente se ingresara las siguientes líneas de comandos para el correcto funcionamiento de PhpMyAdmin en el navegador.

```
<Directory /var/www/html/phpmyadmin>
        AllowOverride All
        Options FollowSymlinks
        Order allow,deny
        Allow from localhost
        SSLRequireSSL
        DirectoryIndex index.html index.php
</Directory>
```

```
<Directory /var/www/html/phpmyadmin>
      AllowOverride All
      Options FollowSymlinks
      Order allow,deny
      Allow from localhost
      SSLRequireSSL
      DirectoryIndex index.html index.php
 </Directory>
```

Ilustración 85 Configuración del Servicio Web de PhpMyAdmin
Fuente: Mauricio Estrada –William Adriano

7. Seguidamente se reinicia el servicio httpd mediante: **service httpd restart,** Ahora se abre el navegador web y se ingresa a **localhost/PhpMyAdmin/setup**

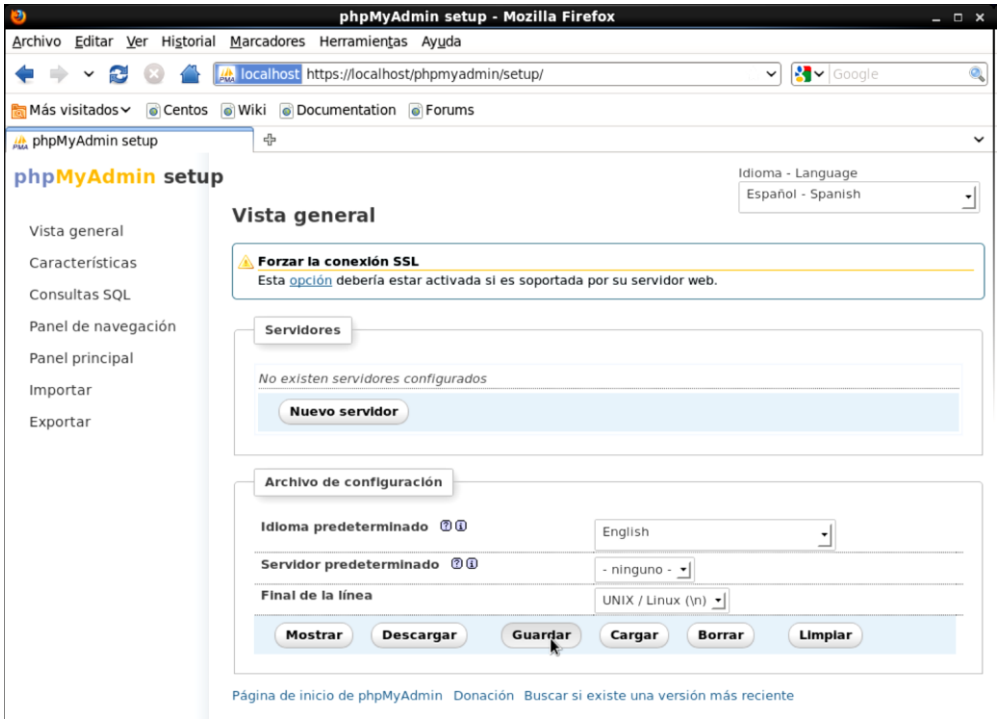


Ilustración 86 Interfaz de Configuración de PhpMyAdmin
Fuente: Mauricio Estrada –William Adriano

5.8.9.2 Instalación de DaloRadius

DaloRadius se encargara de la gestión de los usuarios en el portal cautivo ChilliSpot, además de poder generar reportes, etc.

1. Para lo cual se debe instalar todas las dependencias necesarias para lo cual se ingresa al terminal de Centos la siguiente línea de comandos: **yum -y install httpd mysql mysql-devel mysql-server php php-mysql php-gd**
php-imap php-ldap php-odbc php-pear php-xml php-xmlrpc

2. También se necesita instalar el paquete **pear** para lo cual se debe descargar mediante la línea de comandos: **wget http://download.pear.php.net/packet/DB-1.7.14RC2.tgz**

```
[root@localhost gmoreno]# wget http://download.pear.php.net/package/DB-1.7.14RC
.tgz
--2014-12-17 11:33:57--  http://download.pear.php.net/package/DB-1.7.14RC2.tgz
Resolviendo download.pear.php.net... 5.77.39.20
Connecting to download.pear.php.net|5.77.39.20|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 133426 (130K) [application/x-gzip]
Saving to: `DB-1.7.14RC2.tgz'

100%[======================================>] 133.426     48,0K/s   in 2,7s

2014-12-17 11:34:01 (48,0 KB/s) - `DB-1.7.14RC2.tgz' saved [133426/133426]
```

Ilustración 87 Paquete PHP Descarga
Fuente: Mauricio Estrada –William Adriano

3. Se procede instalar el paquete descargado mediante: **pear install db-1.7.14rc2.tgz**

```
[root@localhost gmoreno]# pear install DB-1.7.14RC2.tgz
install ok: channel://pear.php.net/DB-1.7.14RC2
```

Ilustración 88 Instalación de paquete
Fuente: Mauricio Estrada –William Adriano

4. Seguidamente se descarga el paquete DaloRadius mediante los comandos: **wget http://sourceforge.net/projects/daloradius/files/latest/download?source=files**

```
root@localhost ~]# wget http://sourceforge.net/projects/daloradius/files/latest/download?source=files
```

Ilustración 89 Descaga de Paquete Daloradius
Fuente: Mauricio Estrada –William Adriano

5. Una vez finalizado el proceso de descarga de DaloRadius, se descomprime el paquete mediante la línea de comandos: **tar –zxvf daloradius-0.9-9.tar.gz**
6. Se puede cambiar el nombre de la carpeta con el comando: **mv daloradius-0.9-9 daloradius**

7. Se copia la carpeta al directorio de apache para que pueda ejecutarse en el navegador web mediante el comando: **cp –rf daloradius /var/www/html/**

8. Seguido se asigna los permisos de propietario apache y los permisos de ejecución mediante los comandos:
c**hown –R apache.apache /var/www/html/daloradius/** también:
chmod 644 /var/www/html/daloradius/library/daloradius.conf.php

9. Luego se ingresa al directorio **/var/www/html/daloradius/contrib/db/**

10. Seguidamente, se importara las tablas de daloradius.sql a la base de datos **radius,** mediante la línea de comandos:
mysql –uroot –pingresoroot radius < mysql-daloradius.sql

11. Después, se edita el archivo **daloradius.conf.php** mediante el comando:
vim /var/www/html/daloradius/library/daloradius.conf.php

12. Se modifica los campos **DB_USER** con la base de datos radius y el campo **BD_PASS** con la contraseña que se le asignó a la base de datos radius de la siguiente manera:

```
$configValues['DALORADIUS_VERSION'] = '0.9-9';
$configValues['FREERADIUS_VERSION'] = '2';
$configValues['CONFIG_DB_ENGINE'] = 'mysql';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'rbradius';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADGROUPREPLY'] =
'radgroupreply';
$configValues['CONFIG_DB_TBL_RADGROUPCHECK'] =
'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$configValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
$configValues['CONFIG_DB_TBL_RADHG'] = 'radhuntgroup';
```

$configValues['CONFIG_DB_TBL_RADPOSTAUTH'] = 'radpostauth';
$configValues['CONFIG_DB_TBL_RADACCT'] = 'radacct';
$configValues['CONFIG_DB_TBL_RADIPPOOL'] = 'radippool';

13. A continuación, se abre el navegador web y se ingresa a daloradius mediante la siguiente línea: **http://localhost/daloradius/login.php** para ingresar a la interfaz de DaloRadius.

14. Los Datos necesarios para ingresar a DaloRadius son:

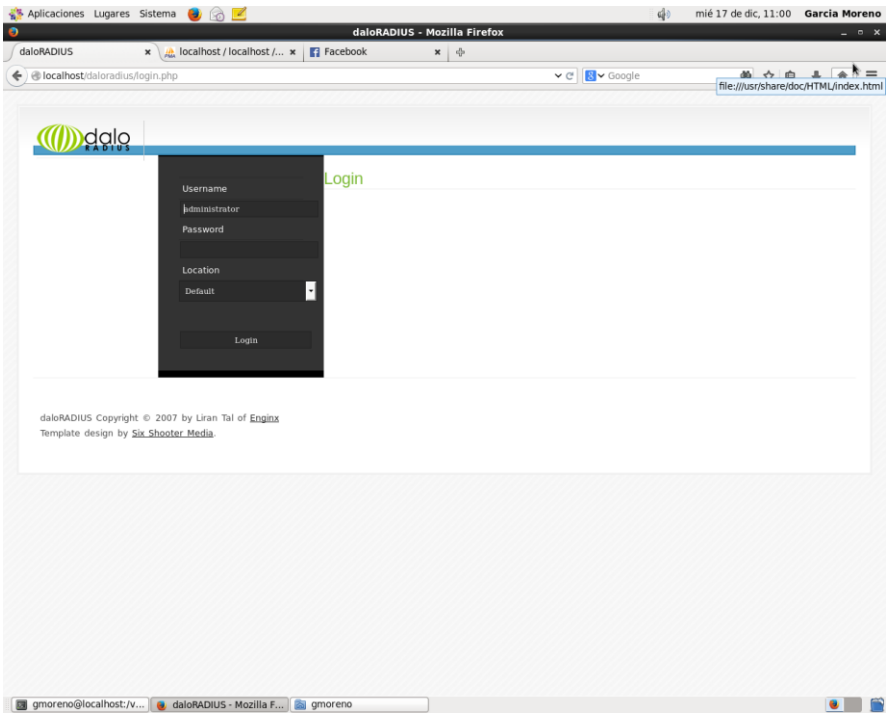


Ilustración 90 Interfaz de Login DaloRadius
Fuente: Mauricio Estrada –William Adriano

Username = administrador

Password = radius

15. Finalmente se verifica que se utilice la base de datos **radius,** se ingresa a la pestaña **config -> database Settings**

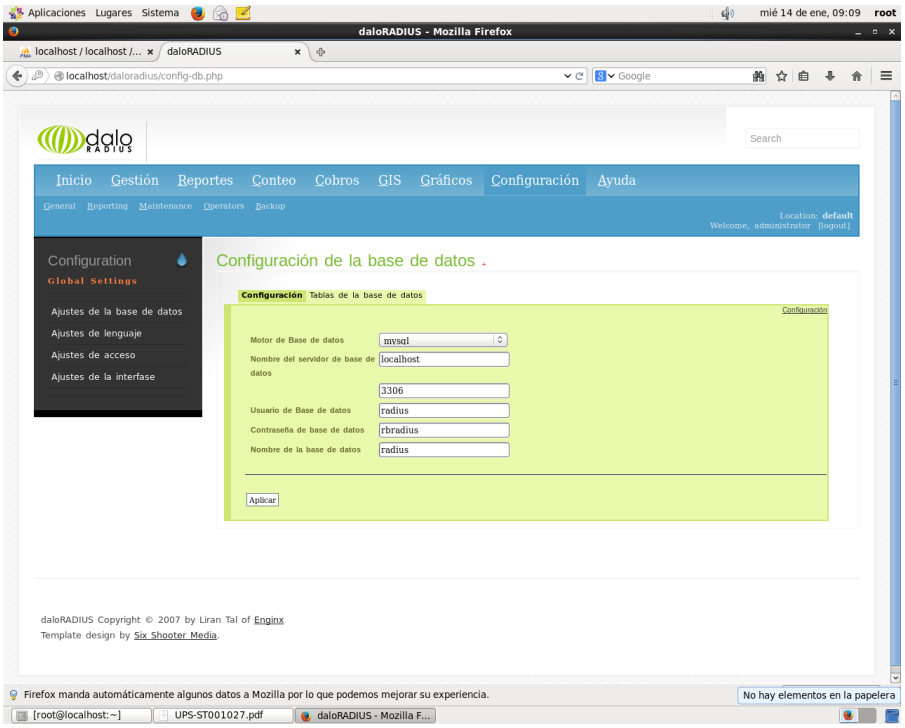


Ilustración 91 Configuración Correcta DaloRadius
Fuente: Mauricio Estrada –William Adriano

5.9 Portal Cautivo Interfaz de Login y de Políticas de uso del internet.

Una vez instalados todos los paquetes necesarios y posteriormente iniciados en el sistema operativo Centos 6.6, como son mysql, FreeRadius, httpd, ChilliSpot, Iptables y Network se puede ver ya activado el sistema del portal Cautivo, el cual se encargara de entregar al cliente una dirección IP dinámicamente por medio de la interfaz eth1 con la red 192.168.10.0, el cliente deberá acceder a un navegador web donde solicitara una página web, el sistema ChilliSpot interceptara la solicitud y presentara una página de Login para poder navegar por internet como se muestra en la ilustración 92.

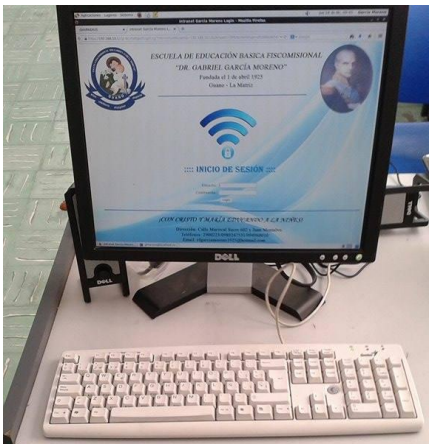


Ilustración 92 interfaz de Login ChilliSpot
Fuente: Mauricio Estrada – William Adriano

Los campos necesarios para la navegación por internet son:

Usuario: nombreUsuario@garciamoreno.edu.ec

Contraseña passwordUsuario

Los cuales deben estar registrados en la base de datos Mysql, además se utiliza DaloRadius Como Gestor de administración como se muestra en la figura 93.

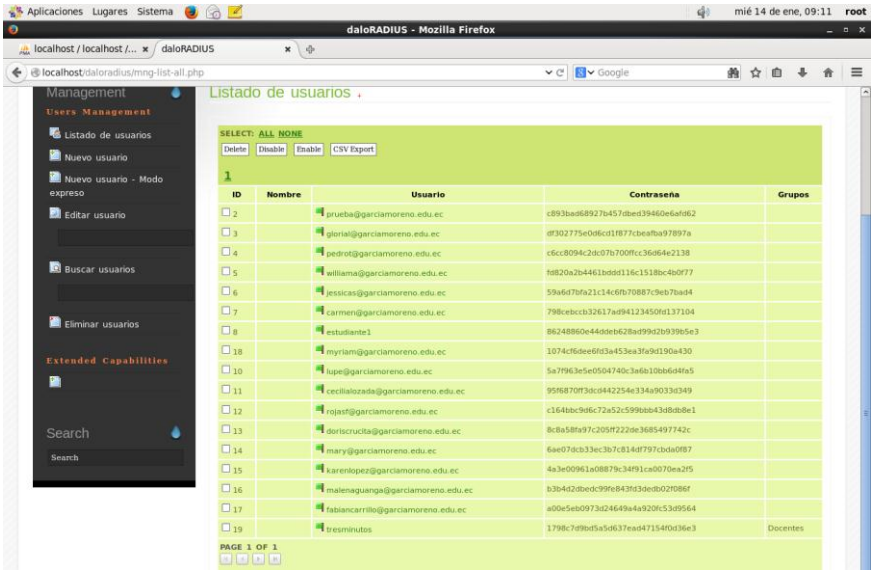


Ilustración 93 Listado de usuarios
Fuente: Mauricio Estrada – William Adriano

5.10 Seguridad firewall o Iptables

Dentro de la configuración de seguridad tanto de ip's como puertos al instalar el sistema ChilliSpot hay que detallar la necesidad de establecer las reglas necesarias para un correcto y seguro funcionamiento del servidor, el cual dará la cara a la red externa o internet, caso contrario existe la probabilidad de posibles ataques.

Al instalar ChilliSpot se puede observar que no existe ningún tipo de control tanto como para el tráfico de entrada como el de salida como se observa en la ilustración 94.

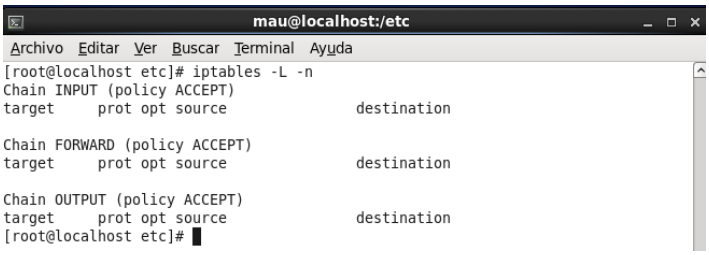


Ilustración 94 Reglas Iptables por defecto
Fuente: Mauricio Estrada – William Adriano

Para evitar este problema existen un conjunto de reglas necesarias para el firewall detalladas en el punto 5.8.7 Portal Cautivo Chillispot literal 8, las cuales se ingresaran en script de arranque rc.local en el path /etc/rc.local con el fin de que cada vez que inicie el sistema operativo detecte las reglas de seguridad como se detalla en la ilustración 95.

```
[root@localhost etc]# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTAB
LISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x
17/0x02
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-po
rt-unreachable
DROP       all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x
17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0
x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3990 flags:
0x17/0x02
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 8
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Ilustración 95 Puertos activos.
Fuente: Mauricio Estrada – William Adriano

Como se observa en la ilustración 95 los puertos activos son:

Puerto	Descripción
22	Conexión Remota segura SSH
80	Transferencia de Híper Texto http
443	Navegación Segura o https
3990	Puerto por donde escucha ChilliSpot

De esta manera se restringe los puertos que no son utilizados por el sistema y se establece las reglas tanto para el tráfico de entrada como para el tráfico de salida aumentando los niveles de seguridad.

CAPÍTULO VI

6. ANÁLISIS Y PRUEBAS DE FUNCIONALIDAD

6.1 Escenario de Pruebas

Con el fin de comprobar el desempeño del sistema del portal cautivo y detectar los posibles errores generados, para tomar medidas correctivas es necesario crear un escenario de pruebas mediante el uso del Simulador de Red Packet Tracer

6.2 Escenario de Pruebas Propuesta de Red para Escenarios de Pruebas

La red de la figura identifica el escenario en el cual se realizarán las pruebas de desempeño y funcionamiento del portal cautivo, antes de su ejecución final.

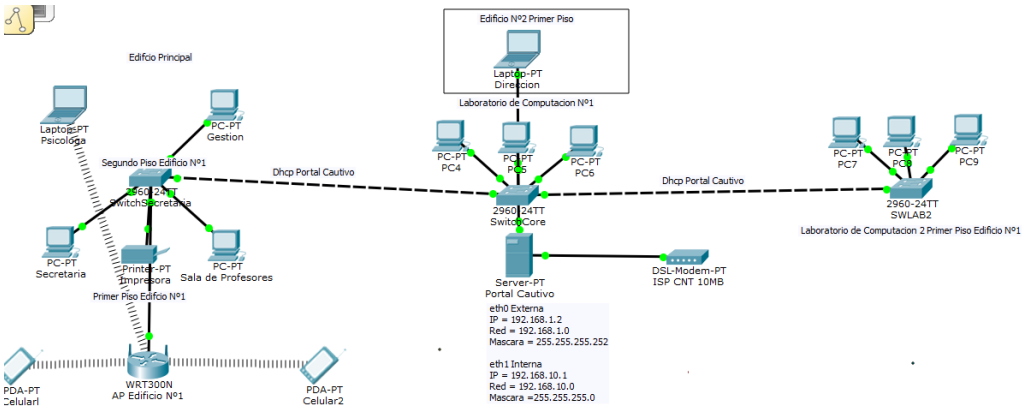


Ilustración 96 Topología Lógica Red Institucional
Fuente: Mauricio Estrada –William Adriano

En el esquema de la red de prueba se implementó un servidor principal el cual contiene el portal cautivo Chillispot, mysql, FreeRadius, Apache y adicionalmente permite dividir en dos segmentos de red:

6.2.1 Red Externa

La red externa se caracteriza por realizar la conexión por medio de un modem ADSL y una IP publica al ISP (Proveedor de Servicio de Internet), en este caso CNT como muestra la ilustración 97.

Ilustración 97 Conexión ISP
Fuente: Mauricio Estrada – William Adriano

6.2.2 Red Interna

Para la red Interna LAN se utiliza una tarjeta PCI FastEthernet el cual realiza la función DHCP y que posee una conexión directa a un Switch D-Link de 24 puertos fastEthernet el cual es el Switch principal de distribución de internet de las Institución y será llamado en el estudio Switch de Core.

Ilustración 98 Switch de Core
Fuente: Mauricio Estrada – William Adriano

El Switch de Core posee una conexión fastEthernet para un Switch de ocho puertos tp-link ubicado en secretaria, como se muestra en la ilustración 99 El cual distribuye la conexión de internet a Secretaria, AccessPoint Edificio Nº1.

Ilustración 99 Switch Secretaria
Fuente: Mauricio Estrada – William Adriano

Finalmente desde el Puerto 7 del Switch de secretaria se establece una conexión hacia el Access Point del Edificio Central En cuál será el encargado de proporcionar internet Inalámbrica como muestra la figura 100.

Ilustración 100 AP Edificio Nº1
Fuente: Mauricio Estrada – William Adriano

6.3 Pruebas en el Escenario Planteado

6.3.1 Prueba 1: Computador de Escritorio

Para esta prueba se utilizó una Computadora de Escritorio conectada a la red institucional mediante el Access Point Inalámbrico con un cable UTP categoría 5e, La PC solicito una página de internet, al instante se le presento la interfaz de Login del Portal Cautivo ChilliSpot con el diseño de la Escuela García Moreno, El Usuario utilizado para el Login se llamó prueba@garciamoreno.edu.ec el cual estuvo Registrado en la base de datos como muestra la ilustración 101.

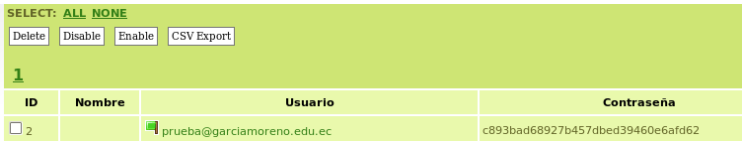


Ilustración 101 Usuario de Prueba
Fuente: Mauricio Estrada – William Adriano

Posteriormente de Login el sistema redirecciónó correctamente a la página solicitada por el cliente y presento una ventana donde muestra la acción de salir de la cuenta y el tiempo de uso del internet como muestra la figura 102.

Ilustración 102 PC Prueba 1
Fuente: Mauricio Estrada – William Adriano

6.3.2 Prueba 2: Teléfono Inteligente

En esta prueba se utiliza un celular Samsung S3 con una conexión inalámbrica hacia el AP del Edificio Nº1 en el cual el portal cautivo envió una IP dinámica y posteriormente se solicita la página www.google.com, como se puede observar en la ilustración 103, ChilliSpot intercepto correctamente la solicitud y presento la interfaz de Login de la Institución

Ilustración 103 Prueba 2 Samsung S3
. Fuente: Mauricio Estrada – William Adriano

De la misma manera se utilizó el usuario prueba@garciamoreno.edu.ec para ingresar a internet, el cual se autentico correctamente y presento la página solicitada como se puede observar en la ilustración 104.

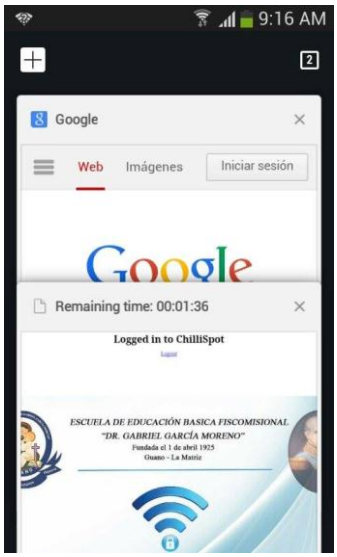


Ilustración 104 Autenticación Correcta Samsung S3
Fuente: Mauricio Estrada – William Adriano

6.3.3 Pruebas 3: Seguridad

Las redes inalámbricas siempre han sido vulnerables a ciertas amenazas y/o ataques en busca de obtener conexión a internet de manera gratuita, existen herramientas que permiten descifrar claves WEP, WPA o WPA-PSK, y algunas para realizar auditorías informáticas como Wireshark el cual será el software que tratara de obtener información de ingreso a la red por medio del análisis de protocolos.

El análisis se realizó con el siguiente ambiente de prueba:

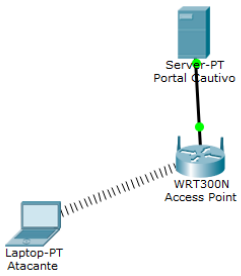


Ilustración 105 Ambiente de prueba de Seguridad
Fuente: Mauricio Estrada – William Adriano

Por medio del Wireshark se intercepto los paquetes enviados y recibidos por el portal cautivo y se obtuvo como resultado el uso de algunos protocolos como son:

- **TCP:** Permite enviar el flujo de datos entre el cliente y servidor y viceversa.
- **ARP:** Realiza consultas MAC por medio de la IP
- **UDP:** Envió de datagramas en la red.
- **TLS:** Protocolo criptográfico que permite comunicación segura en la red.
- **DNS:** Asignación de Nombres de dominio en la red.
- **HTTPS**: Transferencia de datos de forma segura.

Gracias a Wireshark se pudo reconocer los distintos protocolos que utiliza el portal cautivo, así como observar que la información transferida entre cliente y servidor en correctamente criptografía mediante TLS. Por lo cual se concluye que la red Institucional de la Escuela Gabriel García Moreno Posee un alto grado de seguridad contra usuarios ajenos a la red, También se pudo observar que las contraseñas trasmitidas entre cliente servidor no se trasmiten en texto plano como muestra la Ilustración 106.

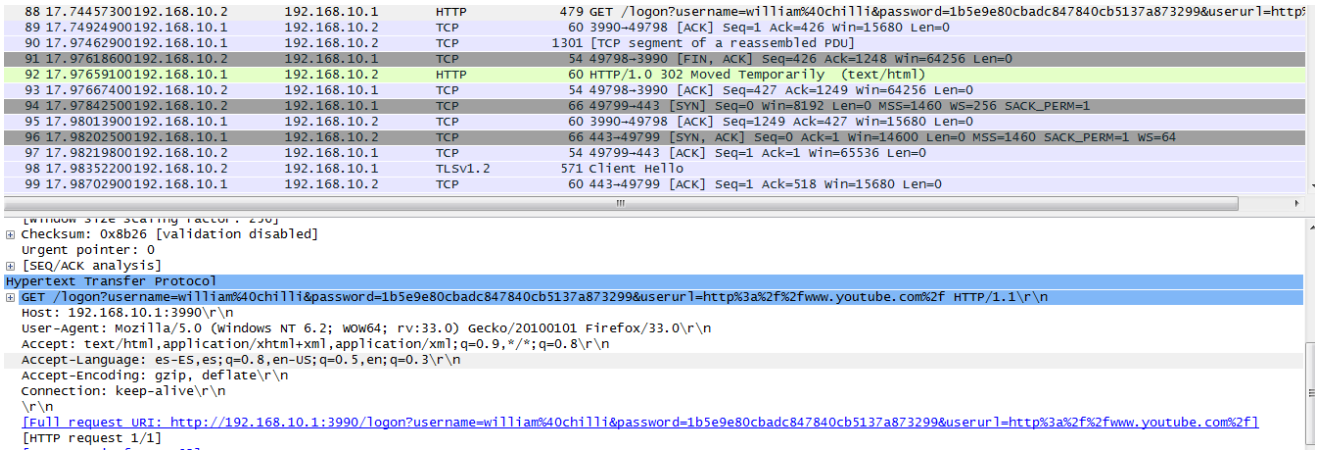


Ilustración 106 Trasmisión Cifrada Password
Fuente: Mauricio Estrada – William Adriano

CAPÍTULO VII

7. DEMOSTRACIÓN DE LA HIPÓTESIS

7.1 Hipótesis a demostrar

La implementación del portal cautivo permitirá obtener un mejor control de las redes inalámbricas.

7.1.1 Muestra de la Población

La demostración de la hipótesis está basada en las encuestas que se realizaron al personal docente de la escuela "Gabriel García Moreno" ver Anexo 4, Anexo 5 una vez recolectada la información necesaria se aplicara el método T Student para la comprobación de la hipótesis.

Se realizaron las encuestas respectivas a los usuarios, que determinaran un antes y un después el uso y control de la red inalámbrica de la institución.

Para la determinación de la población se optó por la siguiente manera:

- A los usuarios finales se determinó que existen 18 docentes y 3 administradores de la red inalámbrica de la institución con un total de 21 usuarios finales.

Para calcular el tamaño de la muestra se aplica la siguiente fórmula:

$$n = \frac{Z^2 pqN}{Ne^2 + Z^2 pq}$$

Dónde:

n = Tamaño de la muestra.

N = Tamaño de la población =21

p = variabilidad positiva.

q = variabilidad negativa

Z = Nivel de confianza

e = Limite de error = 0,05

$$n = \frac{(0{,}95)^2(0{,}5)(0{,}5)21}{21(0{,}05)^2 + (0{,}95)^2(0{,}5)(0{,}5)}$$

$$n = \frac{4{,}74}{0.2781}$$

n = 17,04 encuestas realizadas

7.2 Resultados de las Encuestas

7.2.1 Resultados de las encuestas realizadas sobre el acceso de internet inalámbrico antes de implementar un portal cautivo.

|PREGUNTAS	RESPUESTAS					
¿Conoce si la escuela Gabriel García Moreno brinda el algún servicio de internet para los estudiantes y profesores?	No					Si
	0					17
¿Está de acuerdo con que la escuela Gabriel García Moreno brinde un servicio de Internet Gratuito a los maestros y estudiantes?	No					Si
	0					17
¿Utiliza actualmente el servicio de internet inalámbrico?	No					Si
	4					13
¿Ha utilizado anteriormente el servicio de internet inalámbrico?	No					Si
	6					11
¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico?	Muy malo	Malo	Regular	Bueno	Muy Bueno	Excelente
	0	0	3	7	7	0
¿Ha tenido usted problemas para conectarse a la Red inalámbrica de la escuela?	No					Si
	9					8
¿Cómo fue la velocidad de navegación del Internet inalámbrico de la escuela?	Muy Lenta	Lenta	Aceptable	Buena	Muy Rápida	Excelente
	0	4	5	8	0	0

¿Qué uso le da usted al Internet inalámbrico?	Educativos	Entretenimientos	Descargas	Otros		
	17	0	0	0		
¿Qué rango de tiempo usa usted el Internet inalámbrico de la escuela?	1 - 15min	16–30min	31-45min	+ de 45 min		
	11	4	1	1		
¿Qué tipo de dispositivo usa usted para conectarse a la red inalámbrica?	Laptop	Celular	Tablet	Otros		
	7	10	0	0		
TOTAL	54	18	9	16	7	66
PORCENTAJE	32%	11%	5%	9%	4%	39%

Tabla 25 Total de Encuetas 1
Fuente: Mauricio Estrada –William Adriano

7.2.2 Resultados de las encuestas realizadas sobre el acceso de internet inalámbrico después de implementar un portal cautivo.

PREGUNTAS	RESPUESTAS				
¿Conoce que es un Portal Cautivo?	Si				No
	0				17
¿Con que frecuencia se conecta a las redes inalámbricas de la escuela?	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca
	4	10	3	0	0
¿Se le hace sencilla la conexión a las redes inalámbricas de la escuela?	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca
	10	7	0	0	0
¿Se siente seguro de ataques informáticos, virus y otro tipo de amenazas en las redes inalámbricas de la escuela?	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca
	17	0	0	0	0
¿La conexión a la red inalámbrica de la escuela está disponible?	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca
	17	0	0	0	0
¿La velocidad de conexión en la red inalámbrica de la	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca

escuela es la adecuada?	15	2	0	0	0
¿La conexión en la red inalámbrica de la escuela falla?	Siempre	Casi Siempre	Ocasionalmente	Casi Nunca	Nunca
	0	0	2	5	10
¿Desde qué parte dela escuela se conecta a las redes inalámbricas?	Biblioteca	Aulas	Pasillos		
	2	7	8		
Según el portal cautivo cuál cree usted que tiene una página de inicio adecuada.	EasyHotspot	Coovachilli	Zeroshell	ChilliSpot	
	1	2	8	6	
TOTAL	66	28	21	11	27
PORCENTAJE	43%	18,5%	14%	7%	17,5%

Tabla 26 Total Encuesta 2
Fuente: Mauricio Estrada –William Adriano

7.2.3 Resultados de las encuestas realizadas sobre complementos, tiempo de respuesta y seguridad que debería tener un portal cautivo.

PREGUNTAS	RESPUESTAS			
¿Conoce los complementos que hay detrás de un Portal Cautivo?	Si			No
	0			17
¿Conoce o ha escuchado alguno de estos términos?	Base de datos	servidor RADIUS	Protocolo de autenticación	servidor web
	10		2	5
¿Es importante para usted el tiempo en el que se demora tener acceso al internet?	Si			No
	17			0
¿Qué tipo de información maneja a través de la red inalámbrica de la institución?	Personal	Académica	Otra	
	4	14	0	
¿Es importante para usted la información que maneja a través de la red de la institución?	Si			No
	17			0

¿Cree usted que en el estado en el que se encuentra la red inalámbrica de la institución existe seguridad de los datos académicos?	Si			No
	17			0
¿Cómo calificaría la seguridad de la red institucional en el estado que se encuentra actualmente?	Muy seguro	Medio seguro	Seguro	Critico
	10	1	6	0
TOTAL	75	15	8	22
PORCENTAJE	62,5%	12,5%	7%	18%

Tabla 27 Total Encuesta 3
Fuente: Mauricio Estrada –William Adriano

7.3 Resultados totales:

- Una vez obtenidos y analizados los datos de las encuestas realizadas sobre el acceso de internet inalámbrico antes de implementar un portal cautivo se determinó, que la red inalámbrica de la escuela Gabriel García Moreno no posee ninguna aplicación o herramienta que le otorgue una administración o control de la misma y que lo usuarios se conectan fácilmente a la red sin ninguna restricción, puede poner en riesgo los datos académicos de la institución.

- Por otro lado los resultados conseguidos en las encuetas realizadas sobre el acceso de internet inalámbrico después de implementar un portal cautivo dio como resultados que los usuarios están un 65,5% satisfechos después de implementar un portal cautivo ya que se sienten que sus datos académicos están seguros, el acceso a la red no es nada complicado a la hora de conectarse, fácil de utilizar adaptables a cualquier tipo de dispositivo móvil, los administradores tiene control de la misma y se consigue así monitorear la red y los usuarios quienes acceden al servicio a través de interfaces adaptables y fácil de utilizar.

7.4 Demostración de hipótesis

Para la demostración de la hipótesis se realizaron una serie de encuestas dirigidas a los 3 administradores de la red con una serie de preguntas que determinara un antes y un después de implementar un portal cautivo.

A los datos obtenidos se les ha dado un valor de significancia de acuerdo a las respuestas de las encuestas:

Cuantitativa	6	5	4	3	2	1
Cualitativa	No					Si
	Nunca	Casi nunca	Ocasionalmente		Casi Siempre	Siempre
	Muy Lenta	Lenta	Aceptable	Buena	Muy Rápida	Excelente

Tabla 28 Calificación de la Hipótesis
Fuente: Mauricio Estrada –William Adriano

ENCUESTADOS	PREGUNTAS																																							
	#1		#2		#3		#4		#5		#6		#7		#8		#9		#10		#11		#12		#13		#14		#15		#16		#17		#18		#19		#20		TOTAL	
	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D	A	D
1	1	1	1	1	2	1	1	1	4	2	2	5	5	2	6	1	1	1	2	1	5	1	2	1	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	65	31
2	1	1	1	1	1	1	2	1	5	2	2	6	5	2	6	1	2	1	1	1	5	1	2	1	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	66	32
3	1	1	1	1	4	1	1	1	3	1	2	6	6	1	6	1	1	1	2	2	6	1	2	2	6	2	2	6	6	1	6	1	1	1	1	1	6	1	6	1	69	33
4	1	1	1	1	1	1	4	1	6	1	2	6	6	2	6	1	1	1	2	1	6	1	2	1	5	1	1	6	6	1	1	1	1	1	1	1	6	1	6	1	65	31
5	1	1	1	1	1	1	1	2	6	2	2	6	6	2	6	1	1	1	2	1	6	1	2	1	5	1	2	5	6	1	6	1	1	1	1	1	6	1	6	1	68	32
6	1	1	1	1	2	1	5	1	5	3	4	5	5	2	6	1	2	2	1	1	6	1	2	1	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	73	33
7	1	1	1	1	1	1	1	1	5	1	4	5	6	2	6	1	1	1	1	2	6	1	4	1	4	2	2	6	6	1	1	1	1	1	1	1	6	1	6	1	64	32
8	1	1	1	1	5	1	1	1	5	1	2	4	6	3	6	1	2	1	2	1	5	1	2	2	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	71	31
9	1	1	1	1	1	1	1	2	5	2	2	5	5	2	6	1	2	1	2	1	6	1	2	1	5	1	1	6	6	1	6	1	1	1	1	1	6	1	6	1	66	32
10	1	1	1	1	2	1	2	1	4	2	2	5	5	2	6	1	1	1	1	2	6	1	4	1	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	68	32
11	1	1	1	1	1	1	1	1	4	2	2	6	6	1	6	1	1	2	1	1	5	1	2	1	5	1	2	6	6	1	1	1	1	1	1	1	6	1	6	1	59	32
12	1	1	1	1	4	1	1	1	5	2	2	6	5	2	6	1	1	1	2	1	6	1	2	1	5	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	69	32
13	1	1	1	1	1	1	5	1	5	2	4	6	6	3	6	1	1	1	2	1	6	1	2	2	5	2	2	5	6	1	6	1	1	1	1	1	6	1	6	1	73	34
14	1	1	1	1	5	1	1	1	6	3	2	5	6	1	6	1	1	1	2	1	6	1	1	1	6	1	2	6	6	1	6	1	1	1	1	1	6	1	6	1	72	31
15	1	1	1	1	2	1	1	1	4	1	2	6	5	2	6	1	2	1	2	1	5	1	2	1	5	1	1	6	6	1	1	1	1	1	1	1	6	1	6	1	60	31
16	1	1	1	1	1	1	4	2	5	3	4	5	5	2	6	1	1	1	1	1	6	1	2	1	5	2	2	6	6	1	6	1	1	1	1	1	6	1	6	1	70	34
17	1	1	1	1	5	1	1	1	5	1	2	5	5	2	6	1	1	1	1	1	5	1	2	1	5	1	2	5	6	1	6	1	1	1	1	1	6	1	6	1	68	29

Tabla 29 Resultado total Antes y Despues

Fuente: Mauricio Estrada – William Adriano

Una vez obtenidos los resultados totales de las encuestas realizadas se procede a demostrar la hipótesis:

- La implementación del portal cautivo permitirá obtener un mejor control de las redes inalámbricas

Con la ayuda de métodos estadísticos, en este caso el método T-Student, debido a que la población es específica, con dos tipos de muestras una antes de la implementación de un portal cautivo y otra después en donde:

Hipótesis alternativa (Ha.) = El control de la red inalámbrica ha mejorado con la implementación de un portal cautivo.

Hipótesis Nula (Ho.) = El control de la red inalámbrica es igual o menor que la que otorga la administración de un portal cautivo.

Nivel de significación:

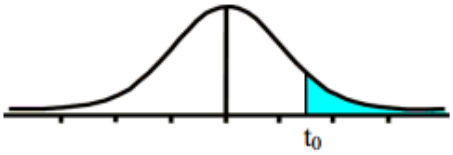
Por todo valor de probabilidad igual o menor que 0,05 se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis Nula (Ho)

Zona de Rechazo:

Por todo valor de probabilidad mayor que 0,05 se acepta la hipótesis Nula (Ho) y se rechaza la hipótesis alternativa (Ha)

Con ayuda de la tabla T-Student se estableciera nuestro grado de libertad que tendrá nuestra investigación, en nuestro caso para 0,05 con una muestra de 17 usuarios -1 el grado de libertad seria: 1.7459

Tabla t-Student



Grados de libertad	0.25	0.1	0.05	0.025	0.01	0.005
1	1.0000	3.0777	6.3137	12.7062	31.8210	63.6559
2	0.8165	1.8856	2.9200	4.3027	6.9645	9.9250
3	0.7649	1.6377	2.3534	3.1824	4.5407	5.8408
4	0.7407	1.5332	2.1318	2.7765	3.7469	4.6041
5	0.7267	1.4759	2.0150	2.5706	3.3649	4.0321
6	0.7176	1.4398	1.9432	2.4469	3.1427	3.7074
7	0.7111	1.4149	1.8946	2.3646	2.9979	3.4995
8	0.7064	1.3968	1.8595	2.3060	2.8965	3.3554
9	0.7027	1.3830	1.8331	2.2622	2.8214	3.2498
10	0.6998	1.3722	1.8125	2.2281	2.7638	3.1693
11	0.6974	1.3634	1.7959	2.2010	2.7181	3.1058
12	0.6955	1.3562	1.7823	2.1788	2.6810	3.0545
13	0.6938	1.3502	1.7709	2.1604	2.6503	3.0123
14	0.6924	1.3450	1.7613	2.1448	2.6245	2.9768
15	0.6912	1.3406	1.7531	2.1315	2.6025	2.9467
16	0.6901	1.3368	1.7459	2.1199	2.5835	2.9208
17	0.6892	1.3334	1.7396	2.1098	2.5669	2.8982
18	0.6884	1.3304	1.7341	2.1009	2.5524	2.8784
19	0.6876	1.3277	1.7291	2.0930	2.5395	2.8609
20	0.6870	1.3253	1.7247	2.0860	2.5280	2.8453

Tabla 30 T-Student
Fuente: Mauricio Estrada –William Adriano

Una vez determinados nuestra probabilidad de 0.05 con un grado de libertad de 1.7459 se procede a determinar las medias. Desviación estándar y la t calculada de la siguiente manera.

Usuarios	Encuesta antes	Encuesta después	$(x1 - \bar{x}1)^2$	$(x2 - \bar{x}2)^2$
1	65	31	5.80	0.77
2	66	32	1.98	0.014
3	69	33	2.52	1.25
4	65	31	5.80	0.77
5	68	32	0.34	0.014
6	73	33	31.24	1.25
7	64	32	11.62	0.014
8	71	31	12.88	0.77

9	66	32	1.98	0.014
10	68	32	0.34	0.014
11	59	32	70.7	0.014
12	69	32	2.52	0.014
13	73	34	31.24	4.49
14	72	31	21.06	0.77
15	60	31	54.90	0.77
16	70	34	6.70	4.49
17	68	29	0.34	8.29
Sumatoria	$\sum x1 = 1146$	$\sum x2 = 542$	$\sum (x1 - \overline{x}1)^2 = 261.96$	$\sum (x2 - \overline{x}2)^2 = 23.71$

Tabla 31 Desviación Estándar
Fuente: Mauricio Estrada – William Adriano

En donde:

t= valor estadístico del procedimiento

X

$\overline{x}$ = Media aritmética de las diferencias entre los tiempos antes y después.

S = Desviación estándar de las diferencias entre los tiempos antes y después.

s^2= Varianza

Calculo de la Media aritmética:

$$\overline{x}1 = \frac{\sum x1}{N} \qquad \overline{x}2 = \frac{\sum x2}{N}$$

$$\overline{x}1 = \frac{1146}{17} \qquad \overline{x}2 = \frac{542}{17}$$

$$\overline{x}1 = 67.41 \qquad \overline{x}1 = 31.88$$

Para calcular la desviación estándar se aplica la siguiente formula:

$$s = \sqrt{\frac{\sum(x1-\overline{x}1)^2}{N-1}} \qquad s = \sqrt{\frac{\sum(x2-\overline{x}2)^2}{N-1}}$$

$$s = \sqrt{\frac{261.96}{16}} \qquad s = \sqrt{\frac{23.71}{16}}$$

$$s = 4.04 \qquad s = 1.21$$

Para calcular la varianza se realiza los siguientes cálculos:

$$s^2 1 = (s1)^2 \qquad s^2 2 = (s2)^2$$

$$s^2 1 = (4.04)^2 \qquad s^2 1 = (1.21)^2$$

$$s^2 1 = 16.32 \qquad s^2 1 = 1.46$$

Con los datos obtenidos tanto la media aritmética, Varianza, y la desviación estándar se precede a calcular el valor estadístico del procedimiento con el uso de la siguiente formula:

$$t = \frac{\overline{x1} - \overline{x2}}{Sx1x2}$$

$$t = \frac{67.41 - 31.88}{1.043}$$

$$t = 34{,}06$$

$$Sx1x2 = \sqrt{\frac{N1 * S1^2 + N2 * S2^2}{N1 + N2 - 2}} * \sqrt{\left(\frac{1}{N1} + \frac{1}{N2}\right)}$$

$$Sx1x2 = \sqrt{\frac{17 * 16.32 + 17 * 1.46}{17 + 17 - 2}} * \sqrt{\left(\frac{1}{17} + \frac{1}{17}\right)}$$

$$Sx1x2 = \sqrt{\frac{277.44 + 24.82}{32}} * \sqrt{\frac{2}{17}}$$

$Sx1x2 =$1.043

$t = 34{,}06$

Una vez obtenido el valor t calculado en nuestro caso se tiene 34.06 se compara con la tabla y se observa que nuestro grado de libertad es de 1.7459 corresponde a una probabilidad de 0.05, por lo cual el valor estadístico 34.06 tiene una probabilidad menor que 0.05

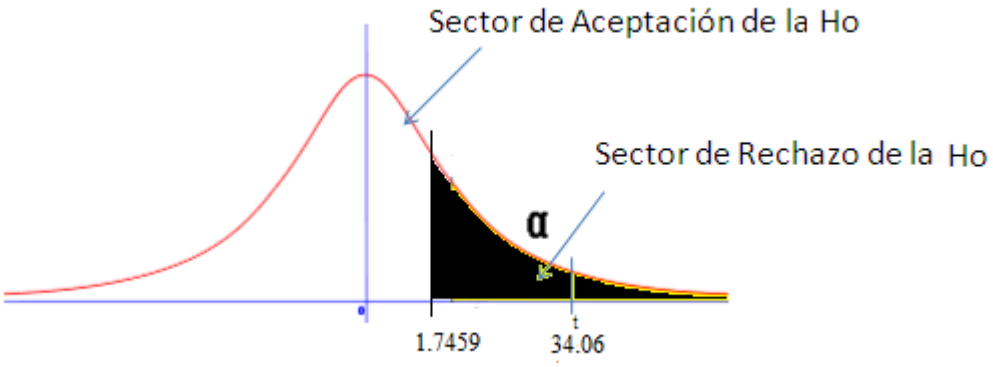


Tabla 32 Grafica de Decisión de Hipótesis
Fuente: Mauricio Estrada – William Adriano

Decisión:

Como se puede observar el valor de t que se calculo tiene una probabilidad menor que la t de origen lo cual nos indica que se rechaza la Ho y se acepta la Ha

Interpretación:

El control de la red inalámbrica y acceso de los usuarios de la escuela "Gabriel García Moreno" después de haber sido implementado un portal cautivo ha mejorado notablemente ya que se ha observado cambios positivos en el servicio y sus usuarios se sienten satisfechos con mismo.

CONCLUSIONES

- La investigación de los cuatro portales cautivos determino las principales ventajas y desventajas que poseen cada uno, además de las características únicas para adaptarse a las necesidades de una institución.

- Los parámetros de comparación para el estudio permitieron un enfoque equitativo de comparación para los cuatro portales cautivos sujetos a estudio, considerando que el parámetro de comparación con mayor ponderación fue el de Control con un 41% y el de menor ponderación fue el de Diseño de Interfaz con 5,5%

- La red institucional de la escuela Gabriel García Moreno se encuentra apta para la trasmisión de los servicios web montados en el servidor de la institución, ya que posee una red FastEthernet y las características tanto de los Switch y del servidor permiten un funcionamiento apto para el número de usuarios de la Institución Educativa.

- El portal cautivo implementado en red institucional de la escuela Gabriel García Moreno es ChilliSpot ya que obtuvo en promedio de parámetros de comparación un 80.25% obteniendo un puntaje mayor en los parámetros Seguridad 4.87 sobre 6.5 y Control 6.15 sobre 8.2, mientras que en el parámetro de comparación donde obtuvo un menor puntaje fue, diseño de Interfaz al necesitar conocimientos de programación .cgi para la edición de la interfaz

- El portal cautivo ChilliSpot brinda todas las facilidades de administración de red, gracias a su facilidad de control, pues en comparación con los otros tres portales cautivos obtuvo una calificación de 4.8/6.5 teniendo una diferencia de 3.25/6.5 con sus inmediatos seguidores.

- DaloRadius permite monitorear los intentos de conexión gracias a la tabla radpostauth de la base de datos radius, además del 100% de los usuarios conectados y usuarios a los que se les denegó el servicio por el mal uso de credenciales, lo cual facilita la elaboración de reportes de administración.

- Luego de la implementación del portal cautivo ChilliSpot se determinó que la seguridad de los datos académicos está protegidos de cualquier amenaza de hacking o pérdida de información pues se realizaron tres tipos de ataques con el fin de encontrar vulnerabilidades, como son Inyección Sql con una calificación de 4/4, intercepción de paquetes con un Sniffer valorado en 4/4 mientras que el ataque con menor calificación es spoofing calificada con 1/4 el cual es el talón de Aquiles de todos los portales sujetos al estudio.

RECOMENDACIONES

- Para una buena administración de una red empresarial o institucional es aconsejable optar por medidas de seguridad y control para evitar así posibles ataques internos y externos, una de las medidas más optimas es implementar un portal cautivo que posee una buena administración y control de la misma.

- Las políticas de la institución educativa deben ser acopladas al sistema de administración de la red, recomendadas en la implementación de algún tipo de sistema de administración de red como un portal cautivo.

- Para determinar los parámetros de comparación entre portales cautivos se debe elegir solo los indispensables mediante un análisis, de técnicas de e instrumentos faciliten la recolección de datos que puedan ser evaluados y que ayuden a la demostración de la hipótesis.

- Con el fin de evitar fugas de los parámetros de seguridad de los sistemas de administración de la red se debe nombrar un solo administrador que gestiones y de solución a cualquier problema que se presente.

- Para garantizar la sostenibilidad del proyecto es recomendable realizar capacitaciones al administrador del sistema con el fin de mantener y corregir problemas presentados, además para extender e integrar nuevos servicios al sistema del portal cautivo ya implantado.

- Adicionalmente al alcance de esta investigación e implementación real, se sugiere implementar portales cultivos con filtrado web restringiendo acceso a páginas no autorizadas por la institución para mejorar la seguridad y rendimiento del servicio.

BIBLIOGRAFÍA

1. Platea.pntic. (06 de 09 de 2010). Recuperado el 18 de 10 de 2014, de www.platea.pntic.mec.ec: http://platea.pntic.mec.es/~lmarti2/optral/cap2/fibra-5.htm

2. Angelfire. (21 de 07 de 2011). Recuperado el 10 de 09 de 2014, de Componentes de una Red: http://www.angelfire.com/mi2/Redes/componentes.html

3. Fojenet. (13 de 01 de 2011). Recuperado el 29 de 08 de 2014, de Cables de Red: http://www.fojenet.com/cableado-de-red/tipos-categorias-cable-red/

4. Technology-training. (30 de 09 de 2012). Recuperado el 01 de 012 de 2014, de www.technology-training.co.uk: http://www.technology-training.co.uk/8029.php

5. Uazuay. (11 de 03 de 2012). Recuperado el 19 de 08 de 2014, de www.uazuay.edu.ec: http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/optica.htm

6. Axis Comunication. (19 de 05 de 2013). Recuperado el 10 de 01 de 2015, de axis.com: http://www.axis.com/es/products/video/about_networkvideo/security.htm

7. Perlesystems. (15 de 05 de 2013). Recuperado el 20 de 07 de 2014, de www.perlesystems.es: http://www.perlesystems.es/products/Ethernet-to-Fiber-Media-Converter.shtml

8. Fierro, M. M. (2011). Estudio comparativo de aplicaciones para la implementacion de portales cautivos enmpleando conectividad entre los locales de bonny restaurant. Riobamba: ESPOCH.

9. Flores, D. M. (2013). Analisis, diseño y Propuesta de implementacion de un portal cautivo para la red inalambrica de la Universidad Politecnica Salesiana sede Quito Campus Sur. Quito: Salesiana.

10. Haros, B. (8 de 11 de 2012). Blogspot.com. Recuperado el 5 de 01 de 2015, de http://ponchadodecablesbrissalluvia.blogspot.com/

11. Rodrigez, V. (2 de 12 de 2008). scribd.com. Recuperado el 01 de 27 de 2015, de https://es.scribd.com/doc/8609173/6/Portal-cautivo-para-redes-inalambricas-publicas-con-Chillispot

12. Zuñiga, V. (5 de 11 de 2005). UAEH. Recuperado el 2 de 01 de 2015, de http://www.uaeh.edu.mx: http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/redes%20de%20transmision%20de%20datos.pdf

13. Boquera, M. C. (2003). Sericios avanzadosde telecomunicación. Madrid, España: Ediciones Díaz de Santos, S.A.

14. Cesar Augusto, N. J. (2012). repositorio.utp.edu.com. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/2734/1/0058R173.pdf

15. Dhawan, S. (2007). Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX. Obtenido de http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4299663&queryText%3Dwireless+technologies

16. Flickenger, R. (2006). Redes Inalámbricas en los Países en Desarrollo. Londres: Limehouse Book Sprint Team.

17. Izaskum Pellejero, F. A. (2006). Fundamentos y Aplicaciones de seguridad en redes wlan. Barcelona, España: MARCOMBO S.A.

18. Larouche, F. (2006). SQL Power Injector. Obtenido de http://www.sqlpowerinjector.com/

19. PascuaL, A. E. (2007). Obtenido de Estándares en Tecnologías Inalámbricas: http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

20. Royer, J.-M. (2004). Seguridad en la informátia de la empresa. ediciones ENI.

21. Spaulding, J. (18 de Octubre de 2012). Obtenido de Exploring an open WiFi detection vulnerability : http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6461013

23. Zeroshell. (19 de 01 de 2005). Recuperado el 2 de 11 de 2014, de zeroshell.net: http://www.zeroshell.net/es/captiveportaldetails/

24. Chillispot. (21 de 03 de 2008). Recuperado el 8 de 08 de 2014, de chillispot.org: http://www.chillispot.org/features.html

25. Easyhotspot. (21 de 06 de 2010). Recuperado el 22 de 09 de 2014, de easyhotspot.inov: http://easyhotspot.inov.asia/

26. CoovaChilli. (29 de 07 de 2012). Recuperado el 12 de 07 de 2014, de www.coovachilli.org: http://coova.org/CoovaChilli

GLOSARIO

Access Point (AP): el objetivo de este dispositivo es determinar en base a su configuración, que dispositivos están autorizados a acceder a la red y cuáles no, así mismo permite interconectar redes.

DHCP: Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo pueda obtenga su configuración de red en forma *dinámica*.

HTTP: Protocolo de transferencia de hipertexto, es el método más común de intercambio de información en la (world wide web), el método mediante el cual se transfieren las páginas web desde el servidor a un ordenado.

LAN: Una LAN es una red que conecta los ordenadores en un área relativamente pequeña.

MAN: Red de Área Metropolitana, es una red que ofrece cobertura en un área extensamente geográfica perteneciente a una misma institución.

IP: Protocolo de internet se trata de un estándar que se emplea en él envió y recepción de información mediante una red tanto no guiada como guiada.

MAC: la dirección MAC *(Media Access Control address*) es un identificador o código único de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red.

PDA: conocidos también como asistentes personales, básicamente son pequeñas computadoras.

SSID: es una clave secreta que es fijado por el administrador de la red.

WLAN: es un sistema de comunicación de datos inalámbrico en un área relativamente pequeña.

WEP: es un sistema de cifrado o encriptación para el estándar 802.11 como protocolo para redes Wi-Fi.

WIFI: Es una metodología de conexión que permite interconectar dispositivos y acceder a Internet sin usar cables ni configuraciones complicadas, también conocido como medio de trasmisión no guiado, lo que permite una gran simpleza de uso y movilidad.

ANEXOS

Anexo 1 RadLogin

Para la simulación de la muestra de la población del portal cautivo en este caso de 20 peticiones se utilizó el software RadLogin el cual fue instalado en cada uno de los servidores virtuales donde fueron montados los portales cautivos EasyHotSpot, ChilliSpot, ZeroShell y CoovaChilli.

Con ayuda de un navegador de internet se lo invoco de manera local con el siguiente path: http://127.0.0.1:8082/radlogin.

Se selecciona la pestaña de RadLogin donde muestra el tipo de test que se desea realizar al servidor RADIUS.

En este caso se quiere simular 20 logeos con el servidor RADIUS por lo cual se se seleccionó:

RADIUS Server: El servidor al que se va a realizar la prueba

Profile: El método que se va a simular en este caso Autenticación

Iterations: El número de la muestra o el número de peticiones.

Login: El nombre del usuario de la prueba

Password: la contraseña del usuario.

Se realizó las mismas configuraciones en cada uno de los servidores dando los siguientes resultados:

Simulación de tiempo de respuesta de autenticación del servidor RADIUS frente al portal cautivo EasyHotSpot.

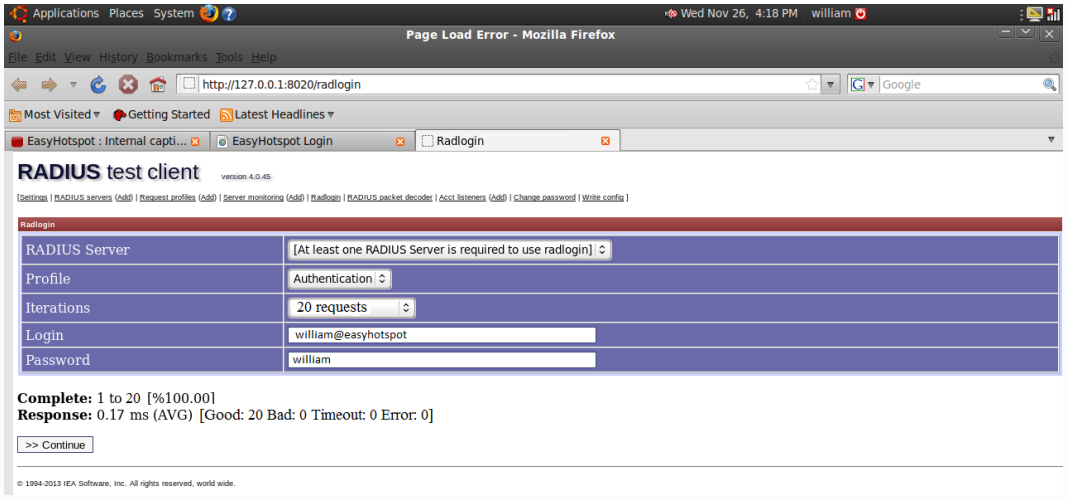


Ilustración 107 RadLogin Frente a EasyHotSpot
Fuente: Mauricio Estrada –William Adriano

El tiempo de respuesta del servidor RADIUS en el portal cautivo EasyHotSpot es de 0.17 (ms) milésimas de segundo.

Simulación de tiempo de respuesta de autenticación del servidor RADIUS frente al portal cautivo CoovaChilli.

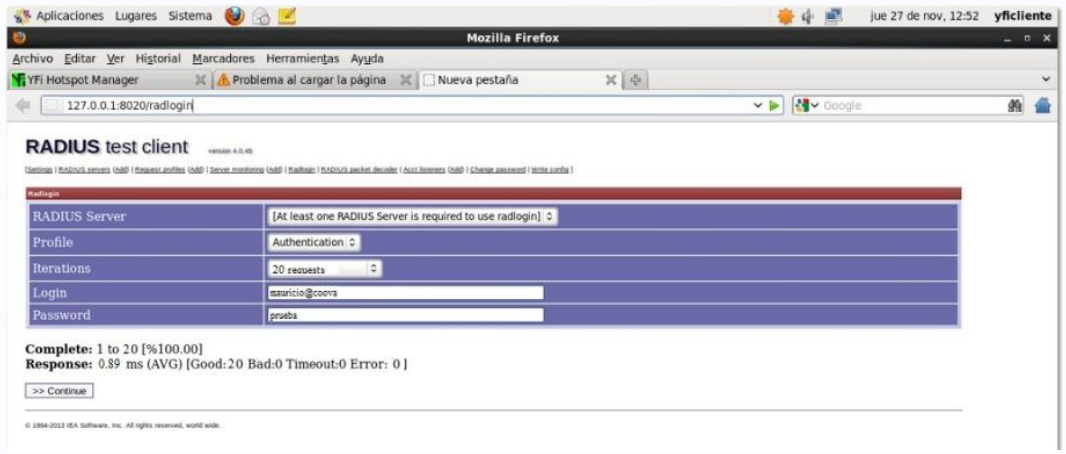


Ilustración 108 RadLogin Frente a CoovaChilli
Fuente: Mauricio Estrada –William Adriano

El tiempo de respuesta del servidor RADIUS en el portal cautivo CoovaChilli es de 0.89 (ms) milésimas de segundo

Simulación de tiempo de respuesta de autenticación del servidor RADIUS frente al portal cautivo ChilliSpot.

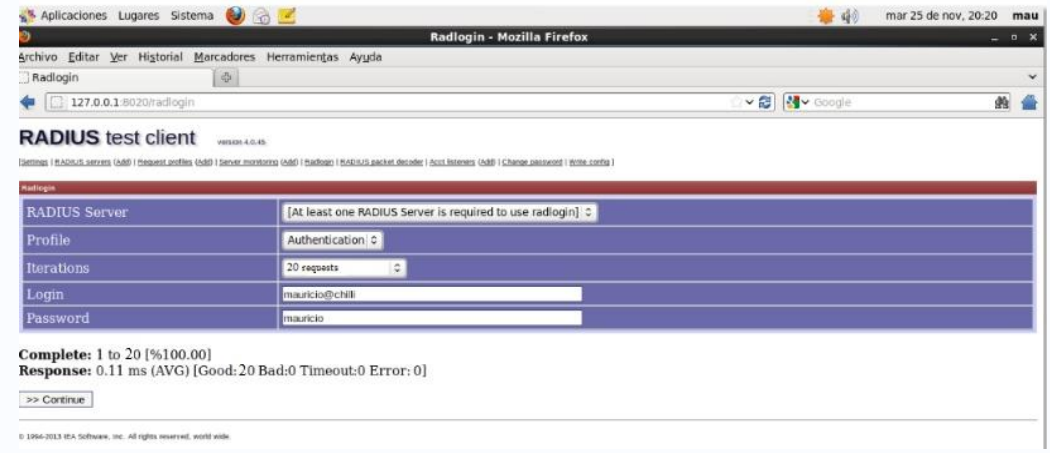


Ilustración 109 RadLogin frente a ChilliSpot
Fuente: Mauricio Estrada –William Adriano

El tiempo de respuesta del servidor RADIUS en el portal cautivo ChilliSpot es de 0.11 (ms) milésimas de segundo

Simulación del tiempo de respuesta de autenticación del servidor RADIUS frente al portal cautivo ZeroShell.

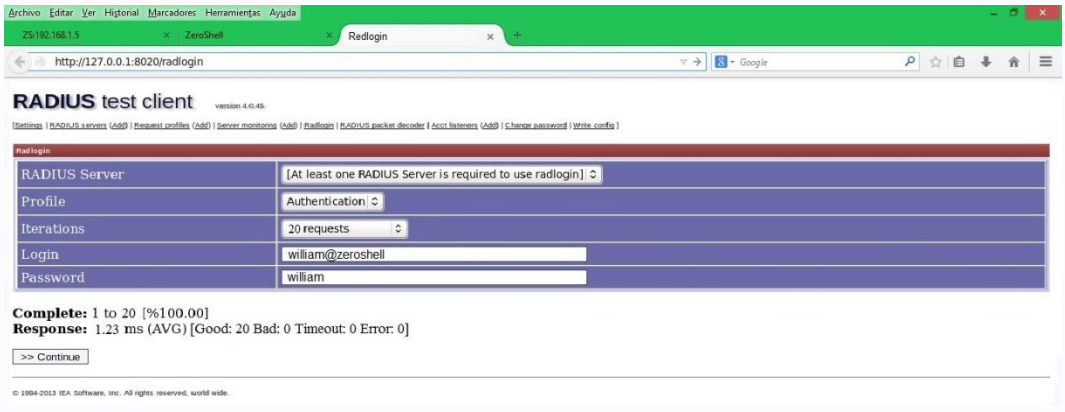


Ilustración 110 RadLogin frente a ZeroShell
Fuente: Mauricio Estrada –William Adriano

El tiempo de respuesta del servidor RADIUS en el portal cautivo EasyHotSpot es de 1.23 (ms) milésimas de segundo.

Anexo 2 Inyección SQL

La herramienta SQL Power Inyector se lo instala en las maquinas clientes de los portales cautivos para poder de esa forma determinar un análisis hacia el servidor Radius y de base de datos.

SQL Power Inyector nos determina si existen fallas o vulnerabilidades que se puedan utilizar para este tipo de ataques y nos muestra en la parte de abajo si existe o no fallas algunas y la parte en donde posiblemente está el error, caso contrario se mostrara un mensaje especificándonos que no existe ninguna falla

Se lo coloca el URL de la página de logue de cada portal Cautivo y se escoge la base de datos con la que trabaja se puede escoger entre sql server, Mysql entre otras.

Al principio se observara la página de logue gráficamente, para empezar el análisis damos clic en el botón **start** para iniciar el análisis hacia las páginas de Login de los portales.

Una vez terminado el análisis nos muestra un mensaje especifico, si existe o no falla alguna de existir algún error nos muestra la parte específica en donde se encuentra el error.

Zeroshell analizado con SQL Power Inyector, como se puede observar que no posee ningún tipo de vulnerabilidades de sql inyector que pueda ser utilizado

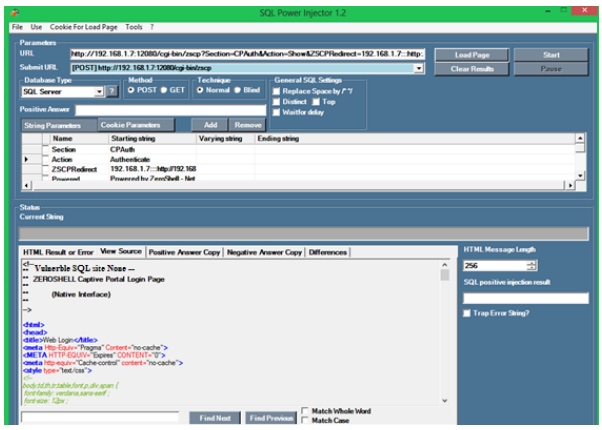


Ilustración 111 Inyector Frente a ZeroShell
Fuente: Mauricio Estrada –William Adriano

EasyHotspot analizado con SQL Power Inyector, como se puede observar el portal cautivo no posee ningún tipo de vulnerabilidades de sql inyector.

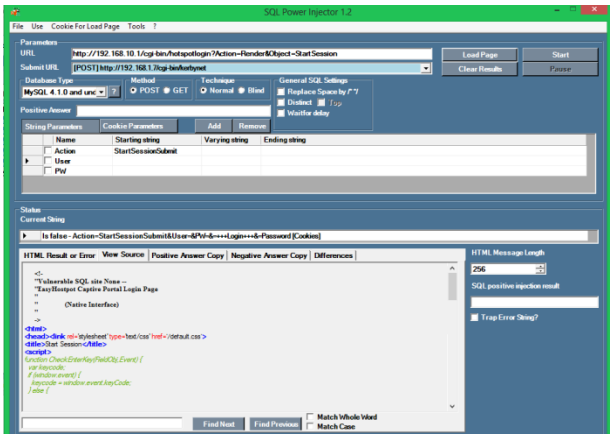


Ilustración 112 Inyector frente a EasyHotSpot
Fuente: Mauricio Estrada –William Adriano

Chillispot analizado con SQL Power Inyector, como se puede observar el portal cautivo no posee ningún tipo de vulnerabilidades de sql inyector.

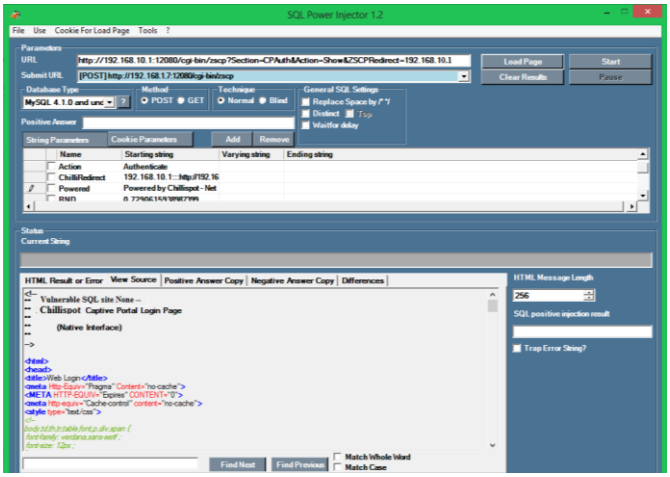


Ilustración 113 Inyector frente a ChilliSpot
Fuente: Mauricio Estrada –William Adriano

Coovachilli analizado con SQL Power Inyector, como se puede observar el portal cautivo no posee ningún tipo de vulnerabilidades de sql inyector.

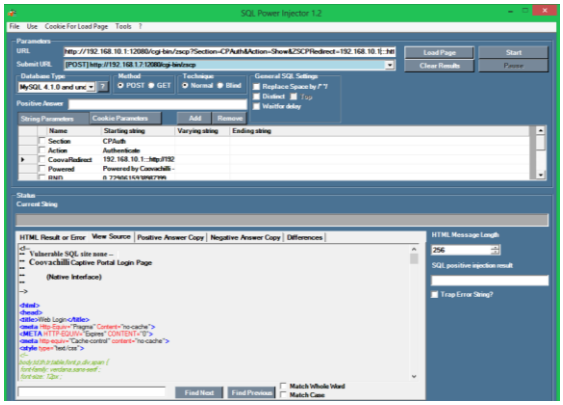


Ilustración 114 Inyector Frente a CoovaChilli
Fuente: Mauricio Estrada –William Adriano

Anexo 3 Man in the Middle

Para realizar la prueba de Spoofing se necesita instalar en una máquina virtual BackTrack 5 r3 que es un sistema auditor de seguridad basado en Ubuntu el cual posee las herramientas necesarias para realizar este tipo de pruebas a una red inalámbrica. También se puede utilizar el sistema como LiveCd.

Lo primero que se debe realizar posteriormente a iniciar BackTrack es revisar la Ip con la que se inició el sistema, ya que uno de los requisitos para realizar pruebas de seguridad con el sistema auditor es ubicarse en la misma red a la cual se vaya a auditar en este caso el sistema del portal cautivo brindara la Ip dinámicamente al sistema BackTrack 5 r3, en este caso se obtuvo la Ip 192.168.10.2 como se muestra en la Ilustración 101.

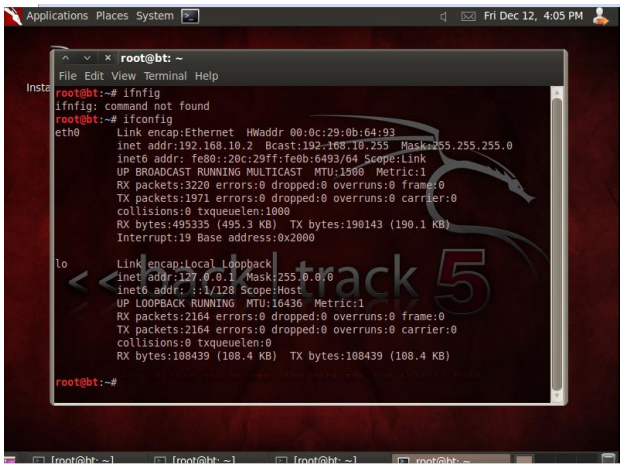


Ilustración 115 Unir PC atacante a red
Fuente: Mauricio Estrada –William Adriano

El segundo paso es Ingresar a un nuevo terminal de BackTrack e interceptar el tráfico entre el cliente y el servidor mediante el siguiente comando **arpspoof –t ipcliente ipservidor & > /dev/null.**

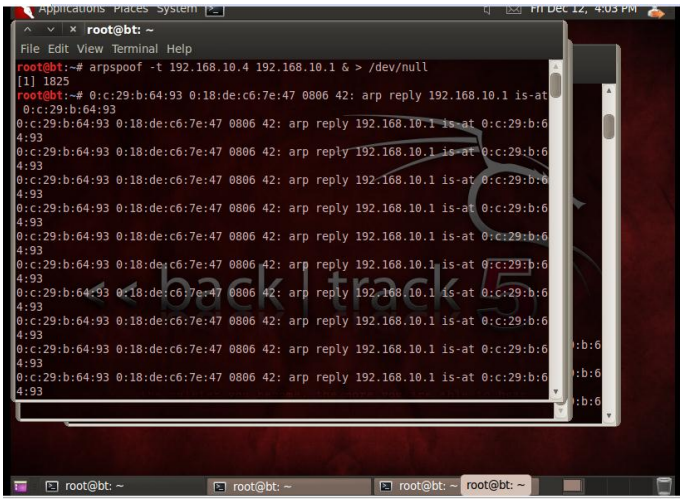


Ilustración 116 Intercepción de paquetes de ida desde el cliente
Fuente: Mauricio Estrada –William Adriano

Del mismo modo se intercepta el tráfico de vuelta desde el servidor hacia el cliente con el comando: **arpspoof –t ipservidor ipcliente > /dev/null** como se muestra en la ilustración 103.

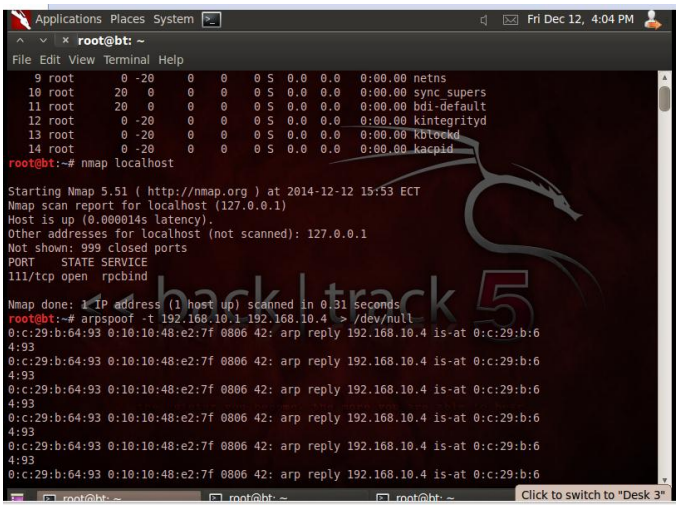


Ilustración 117 Intercepción de paquetes de Vuelta desde el servidor al cliente
Fuente: Mauricio Estrada –William Adriano

Como se puede observar en la ilustración 104, el cliente empieza a tener problemas de comunicación con el servidor que en este caso es: 192.168.10.1.

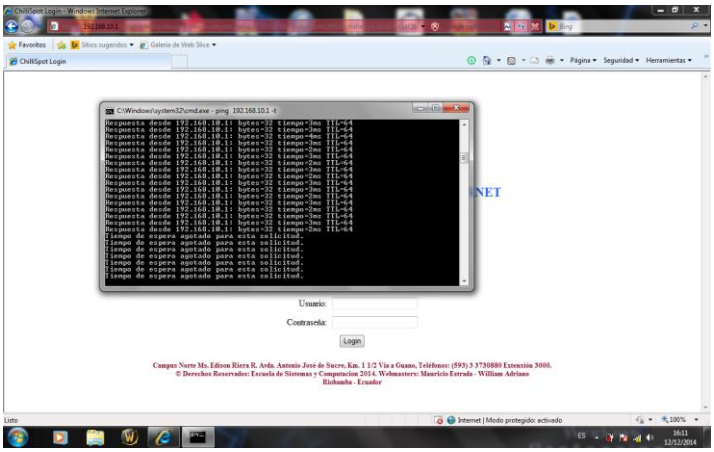


Ilustración 118 Interrupción de la comunicación entre cliente servidor por arpspoof
Fuente: Mauricio Estrada –William Adriano

Para que no suceda este problema se realiza otro proceso paralelo a los procesos que ya ejecutados, se abre un nuevo terminal, y se coloca el comando: **echo 1 > /proc/sys/net/ipv4/ip_forward.** Como se muestra en la Ilustración 119.

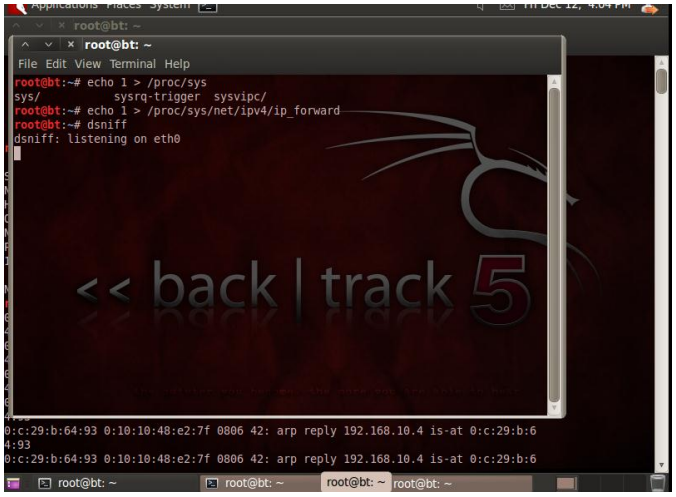


Ilustración 119 Reenvió de Paquetes interceptados
Fuente: Mauricio Estrada –William Adriano

Finalmente para mostrar la información escuchada se ingresa el comando: **dsniff** el cual se mantendrá en estado: **stand by** hasta que se dé por terminada la conversación entre cliente-servidor o hasta cuando se termine la sesión del usuario, lo que nos mostrara la siguiente información.

Ilustración 120 Resultado de conversación Escuchada
Fuente: Mauricio Estrada –William Adriano

Anexo 4 Encuestas

Encuesta sobre acceso y uso del internet inalámbrico de la escuela Gabriel García Moreno <u>Antes de la Implementación,</u> Dirigida a los usuarios de la red de la escuela Dr. Gabriel García Moreno

INSTRUCCIONES:

El cuestionario consta de una serie de preguntas sobre el acceso y uso de internet que se ofrece en la escuela Gabriel García Moreno. Responda con sinceridad y responsabilidad en cada una de las preguntas.

Conteste marcando con una **X** aquélla o aquéllas que considere correcta:

1. **¿Conoce si la escuela Gabriel García Moreno brinda el algún servicio de internet para los estudiantes y profesores?**

   Si [ ] No [ ]

2. **¿Está de acuerdo con que la escuela Gabriel García Moreno brinde un servicio de Internet Gratuito a los maestros y estudiantes?**

   Si [ ] No [ ]

3. **¿Utiliza actualmente el servicio de internet inalámbrico?**

   Si [ ] No [ ]

4. **¿Ha utilizado anteriormente el servicio de internet inalámbrico?**

   Si [ ] No [ ]

5. **¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico**?

   Muy malo [ ] Malo [ ] Regular [ ] Bueno [ ] Muy Bueno [ ] Excelente [ ]

6. **¿Ha tenido usted problemas para conectarse a la Red inalámbrica de la escuela?**

   Si [ ] No [ ]

7. **¿Cómo fue la velocidad de navegación del Internet inalámbrico de la escuela?**

   Muy Lenta [ ]Lenta [ ] Aceptable [ ] Buena [ ] Rápida [ ]

8. **¿Qué uso le da usted al Internet inalámbrico?**

   Educativos [ ] Entretenimientos [ ] Descargas [ ] Otros [ ]

9. **¿Qué rango de tiempo usa usted el Internet inalámbrico de la escuela?**

   1 - 15min [ ] 16 – 30min [ ] 31 – 45min [ ] Más de 45 minutos [ ]

10. **¿Qué tipo de dispositivo usa usted para conectarse a la red inalámbrica?**

    Laptop [ ] Celular [ ] Tablet [ ] Otros [ ]

Encuesta sobre acceso y uso del internet inalámbrico de la escuela Gabriel García moreno Despues de la Implementación, Dirigida a los usuarios de la red de la escuela Dr. Gabriel García Moreno

INSTRUCCIONES:

El cuestionario consta de una serie de preguntas sobre el acceso y uso de internet que se ofrece en la escuela Gabriel García Moreno después de haber implementado un Portal Cautivo en la red institucional. Responda con sinceridad y responsabilidad en cada una de las preguntas.

Conteste marcando con una **X** aquélla o aquéllas que considere correcta:

1. **¿Conoce que es un Portal Cautivo?**
   Si [ ] No [ ]
2. **¿Con que frecuencia se conecta a las redes inalámbricas de la escuela?**
   Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]
3. **¿Se le hace sencilla la conexión a las redes inalámbricas de la escuela?**
   Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]
4. **¿Se siente seguro de ataques informáticos, virus y otro tipo de amenazas en las redes inalámbricas de la escuela?**
   Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]
5. **¿La conexión a la red inalámbrica de la escuela está disponible?**
   Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]
6. **¿La velocidad de conexión en la red inalámbrica de la escuela es la adecuada?**

Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]

7. **¿La conexión en la red inalámbrica de la escuela falla?**

   Siempre [ ] Casi Siempre [ ] Ocasionalmente [ ] Casi Nunca [ ] Nunca [ ]

8. **¿Desde qué parte dela escuela se conecta a las redes inalámbricas?**

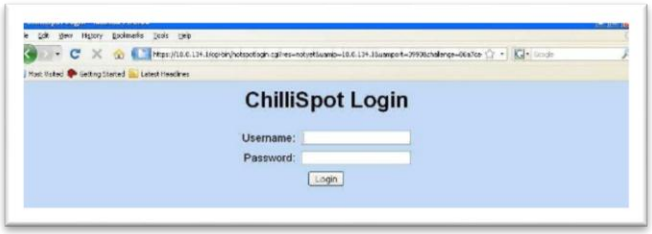
   Biblioteca [ ] Aulas [ ] Pasillos [ ]

9. **Según el portal cautivo cuál cree usted que tiene una página de inicio adecuada.**

a) EasyHotspot [ ]

c) Coovachilli [ ]

d) Zeroshell [ ]



e) ChilliSpot [ ]

ENCUESTA 3 APLICADA A LOS INGENIEROS ENCARGADOS DE LA ADMINISTRACIÓN DE LA RED INSTITUCIONAL DE LA UNACH

INSTRUCCIONES:

El cuestionario consta de una serie de preguntas que justificaran la ponderación de los parámetros de comparación determinados en la investigación de "ESTUDIO COMPARATIVO DE PORTALES CAUTIVOS BASADOS EN SOFTWARE LIBRE PARA AUTENTIFICAR Y CONTROLAR UNA RED INALÁMBRICA"

Conteste marcando con una **X** aquélla que considere correcta:

1. **En porcentaje del 1 al 100.- ¿Qué importancia daría usted como profesional en el área a los complementos que hay detrás de un portal cautivo tales como base de datos, servidor radius, servidor web, entre otros?**

   10 [ ] 20 [ ] 30 [ ] 50 [ ] otro

2. **En porcentaje del 1 al 100.- ¿Qué importancia daría usted como profesional en el área al tiempo de respuesta en que se demoraría en conectarse a una red inalámbrica?**

   10 [ ] 20 [ ] 30 [ ] 50 [ ] otro

3. **En porcentaje del 1 al 100.- ¿Qué importancia daría usted como profesional en el área a la interfaz de acceso a la red inalámbrica a través de un portal cautivo?**

   10 [ ] 20 [ ] 30 [ ] 50 [ ] otro

4. **En porcentaje del 1 al 100.- ¿Qué importancia daría usted como profesional en el área a la seguridad que debería tener una red inalámbrica institucional?**

   10 [ ] 20 [ ] 30 [ ] 50 [ ] otro

5. **¿Cómo calificaría usted como profesional en el área a la seguridad de una red inalámbrica con la implementación de un portal cautivo?**

   Critico [ ] Medio seguro [ ] Seguro [ ]

   Muy seguro [ ] otro _____

6. **En porcentaje del 1 al 100.- ¿Qué importancia daría usted como profesional en el área al control que debería tener una red inalámbrica con respecto a usuarios, ancho de banda entre otros?**

   10 [ ] 20 [ ] 30 [ ] 50 [ ] otro

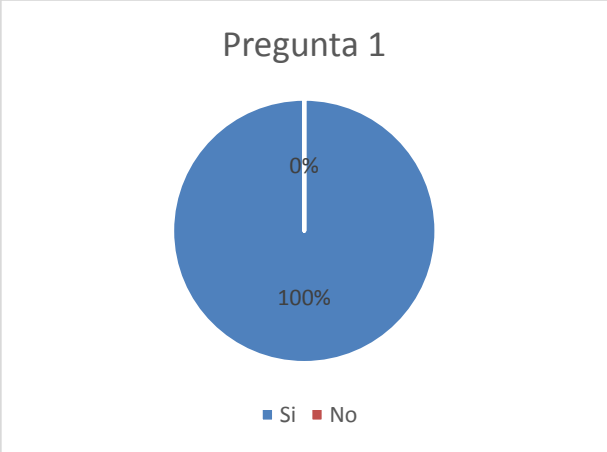
Anexo 5 Tabulación por Pregunta
Encuesta 1 Escenario Antes de la Implementación

Resultados de las encuestas realizadas sobre el acceso de internet inalámbrico antes de implementar un portal cautivo, dirigido a los usuarios de la red.

PREGUNTA N° 1

¿Conoce si la escuela Gabriel García Moreno brinda el algún servicio de internet para los estudiantes y profesores?

Si	**17**	**100%**
No	0	0%
Total	17	100%



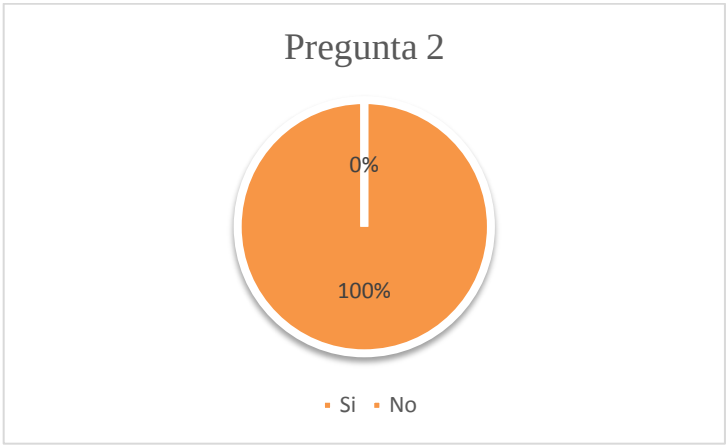
ANÁLISIS

Luego de analizar los resultados obtenidos en las encuestas se concluye que el 100% de encuestados que representa a 17 personas sabían que la escuela Gabriel García Moreno brinda un servicio de internet para los estudiantes y profesores

PREGUNTA N° 2

¿Está de acuerdo con que la escuela Gabriel García Moreno brinde un servicio de Internet Gratuito a los maestros y estudiantes?

Si	**17**	**100%**
No	0	0%
Total	17	100%



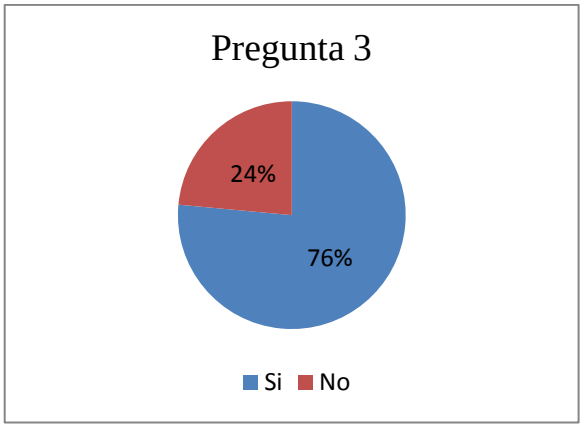
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 100% de encuestados que representa a 17 personas están de con que la escuela Gabriel García Moreno brinde un servicio de Internet Gratuito a los maestros y estudiantes

PREGUNTA N° 3

¿Utiliza actualmente el servicio de internet inalámbrico?

Si	**13**	**76%**
No	4	24%
Total	17	100%



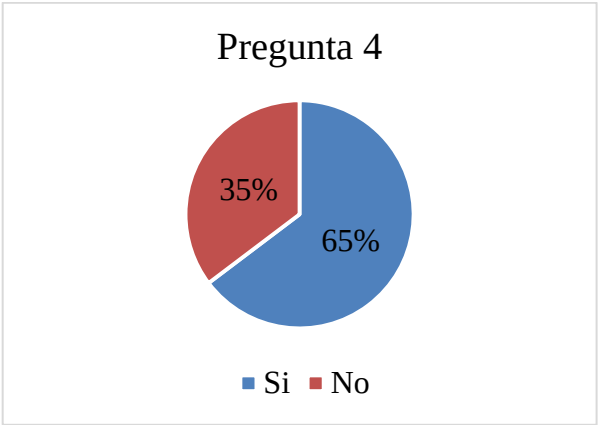
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 76% de encuestados que representa a 13 personas utilizan actualmente el servicio de internet, mientras que el 24% que representa a 4 personas no utilizan el servicio de internet institucional.

PREGUNTA N° 4

¿Ha utilizado anteriormente el servicio de internet inalámbrico?

Si	**11**	**65%**
No	6	35%
Total	17	100%



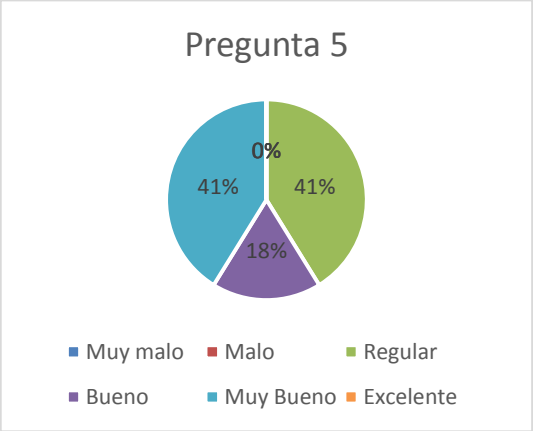
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 65% de encuestados que representa a 11 personas dicen que si han utilizado el servicio de internet anteriormente, mientras que el 34% que representa a 6 personas indican que no han utilizado anteriormente el servicio de internet institucional.

PREGUNTA N° 5

¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico?

Muy malo	**0**	**0%**
Malo	0	0%
Regular	7	41%
Bueno	3	18%
Muy Bueno	7	41%
Excelente	0	0%
Total	17	100%



ANÁLISIS

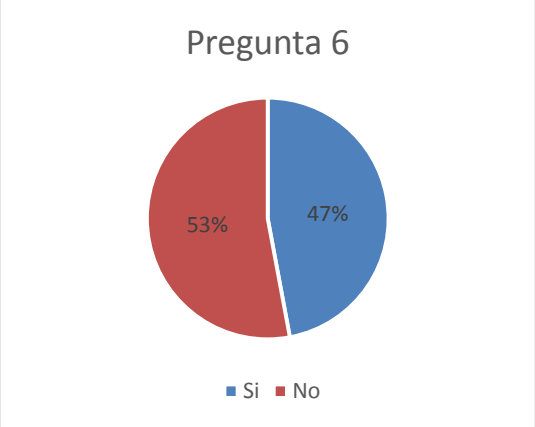
Luego de analizar los resultados obtenidos se concluye que el 41% de encuestados que representa a 7 personas dicen que el grado de satisfacción que le

daría al servicio de internet inalámbrico es regular, el 3% que representa a 3 personas indican que grado de satisfacción que le daría al servicio de internet inalámbrico es bueno y el otro 41% que representa a 7 personas indican que le grado de satisfacción que le daría al servicio de internet inalámbrico es muy bueno.

PREGUNTA N° 6

¿Ha tenido usted problemas para conectarse a la Red inalámbrica de la escuela?

Si	**8**	**47%**
No	9	53%
Total	17	100%



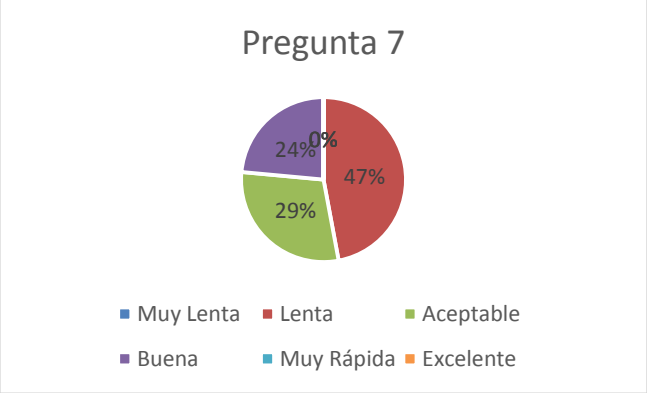
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 47% de encuestados que representa a 8 personas dicen que si tienen problemas para conectarse a la Red inalámbrica de la escuela, mientras que el 53% que representa a 9 personas indican que no tienen problemas para conectarse a la Red inalámbrica de la escuela

PREGUNTA N° 7

¿Cómo fue la velocidad de navegación del Internet inalámbrico de la escuela?

Muy Lenta	**0**	**0%**
Lenta	8	47%
Aceptable	5	29%
Buena	4	24%
Muy Rápida	0	0%
Excelente	0	0%
Total	17	100%



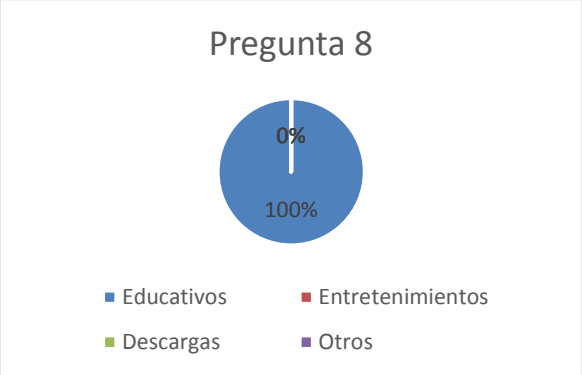
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 47% de encuestados que representa a 8 personas dicen que la velocidad de navegación del Internet es lenta, el 29% que representa a 5 personas indican la velocidad de navegación del internet es aceptable y el otro 24% que representa a 4 personas indican que la velocidad de navegación del internet es buena.

PREGUNTA N° 8

¿Qué uso le da usted al Internet inalámbrico?

Educativos	**17**	**100%**
Entretenimientos	0	0%
Descargas	0	0%
Otros	0	0%
Total	100	100%



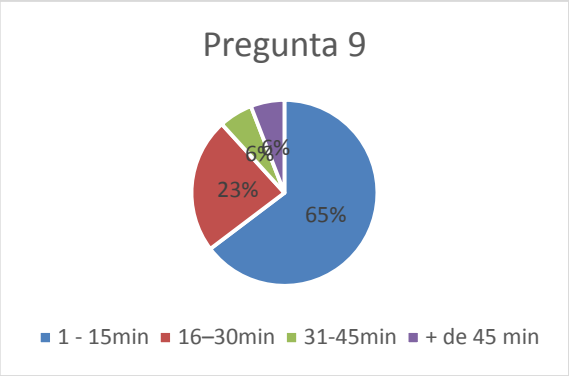
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 100% de encuestados que representa a 17 personas dicen que el uso que le dan al internet de la institución es de carácter educativos.

PREGUNTA N° 9

¿Qué rango de tiempo usa usted el Internet inalámbrico de la escuela?

1 - 15min	**11**	**65%**
16–30min	4	23%
31-45min	1	6%
+ de 45 min	1	6%
Total	17	100%



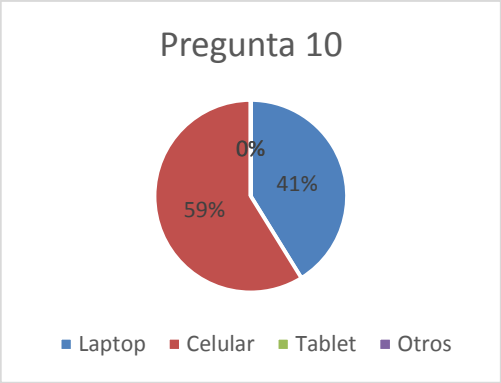
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 65% de encuestados que representa a 11 personas dicen que el tiempo que usan el internet institucional es de 1 a 15 min, el 23% que representa a 4 personas indican que el tiempo que usan el internet institucional es de 16 a 30 min, un 6% que representa a 1 personas indican que el tiempo que usan el internet institucional es de 31 a 45 min y el otro 6% que representa a 1 persona india que el tiempo que usan el internet institucional es de más de 45 min.

PREGUNTA N° 10

¿Qué tipo de dispositivo usa usted para conectarse a la red inalámbrica?

Laptop	**7**	**41%**
Celular	10	59%
Tablet	0	0%
Otros	0	0%
Total	17	100%



ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 41% de encuestados que representa a 7 personas dicen que el dispositivo que usan para conectarse a la red institucional es una laptop, el 59% que representa a 10 personas indican que el dispositivo que usan para conectarse a la red institucional es un celular.

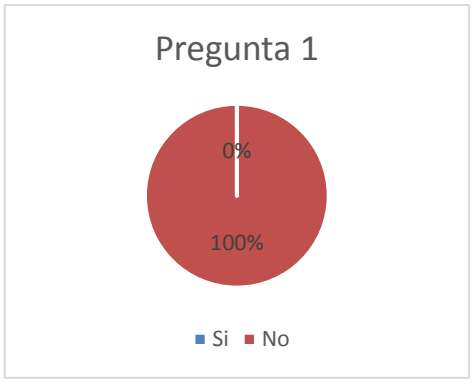
Encuesta 2 Escenario Después de la Implementación

Resultados de las encuestas realizadas sobre el acceso de internet inalámbrico después de implementar un portal cautivo, dirigido a los usuarios de la red.

PREGUNTA N° 1

¿Conoce que es un Portal Cautivo?

Si	**0**	**0%**
No	17	100%
Total	17	100%



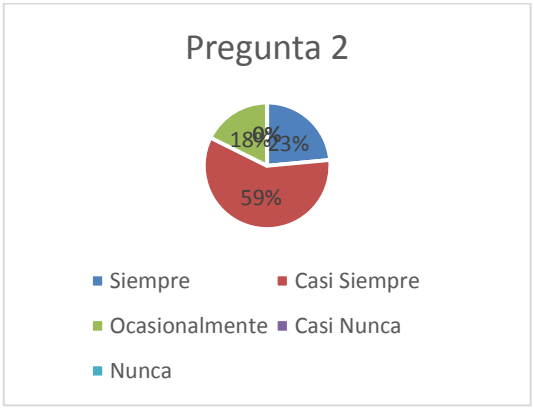
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 100% de encuestados que representa a 17 personas dicen no conocer lo que es un portal cautivo.

PREGUNTA N° 2

¿Con que frecuencia se conecta a las redes inalámbricas de la escuela?

Siempre	**4**	**24%**
Casi Siempre	10	59%
Ocasionalmente	3	18%
Casi Nunca	0	0%
Nunca	0	0%
Total	17	100%



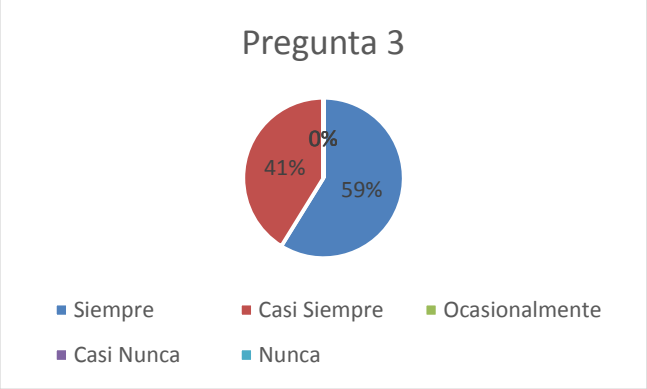
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 24% de encuestados que representa a 4 personas dicen que la frecuencia con que se conectan a la red institucional es siempre, el 59% que representa a 10 personas indican que la frecuencia con que se conectan a la red institucional es casi siempre, un 18% que representa a 3 personas indican que la frecuencia con que se conectan a la red institucional es ocasionalmente.

PREGUNTA N° 3

¿Se le hace sencilla la conexión a las redes inalámbricas de la escuela?

Siempre	**10**	**59%**
Casi Siempre	7	41%
Ocasionalmente	0	0%
Casi Nunca	0	0%
Nunca	0	0%
Total	17	100%



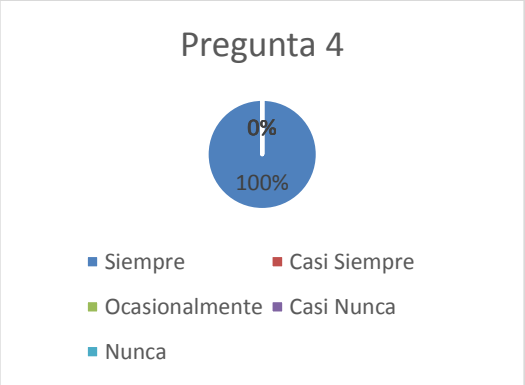
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 59% de encuestados que representa a 10 personas dicen la conexión a las redes inalámbricas de la escuela es siempre sencilla, el 41% que representa a 7 personas indican que la conexión a las red inalámbrica de la escuela es casi siempre sencilla.

PREGUNTA N° 4

¿Se siente seguro de ataques informáticos, virus y otro tipo de amenazas en las redes inalámbricas de la escuela?

Siempre	17	100%
Casi Siempre	0	0%
Ocasionalmente	0	0%
Casi Nunca	0	0%
Nunca	0	0%
Total	17	100%



ANÁLISIS

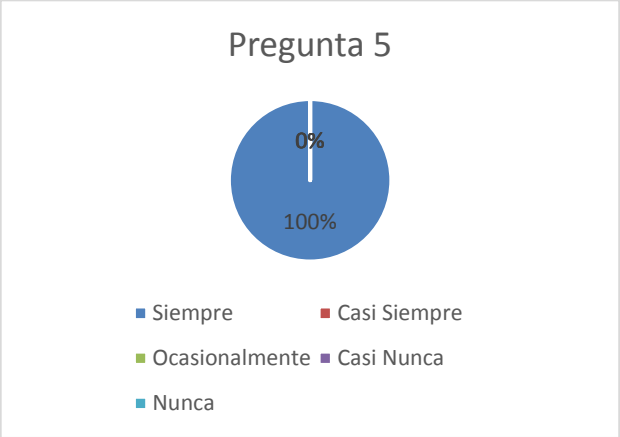
Luego de analizar los resultados obtenidos se concluye que el 100% de encuestados que representa a 17 personas indican que se sienten seguro de ataques informáticos, virus y otro tipo de amenazas en las redes inalámbricas de la escuela.

PREGUNTA N° 5

¿La conexión a la red inalámbrica de la escuela está disponible?

Siempre	17	100%
Casi Siempre	0	0%

Ocasionalmente	0	0%
Casi Nunca	0	0%
Nunca	0	0%
Total	17	100%



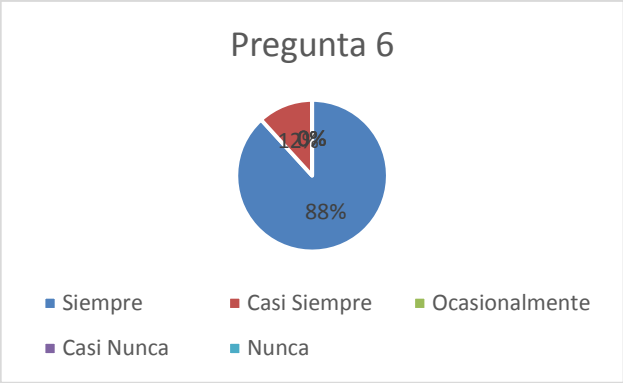
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 100% de encuestados que representa a 17 personas indican que la conexión a la red inalámbrica de la escuela está siempre disponible

PREGUNTA N° 6

¿La velocidad de conexión en la red inalámbrica de la escuela es la adecuada?

Siempre	**15**	**88%**
Casi Siempre	2	12%
Ocasionalmente	0	0%
Casi Nunca	0	0%
Nunca	0	0%
Total	17	100%



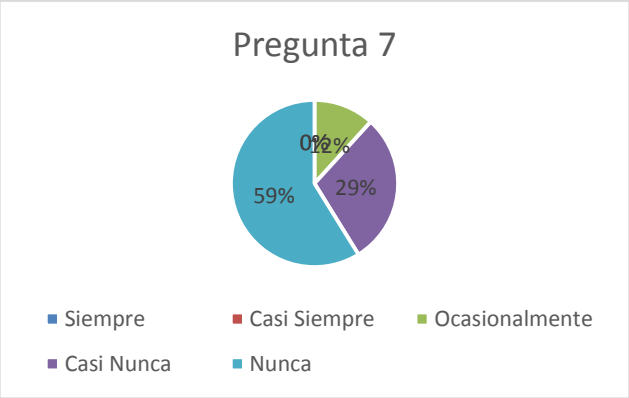
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 88% de encuestados que representa a 15 personas indican que la velocidad de conexión en la red inalámbrica de la escuela es siempre la adecuada, el 12% que representa a 2 personas indican que la velocidad de conexión en la red inalámbrica de la escuela es casi siempre la adecuada.

PREGUNTA N° 7

¿La conexión en la red inalámbrica de la escuela falla?

Siempre	**0**	**0%**
Casi Siempre	0	0%
Ocasionalmente	2	12%
Casi Nunca	5	29%
Nunca	10	59%
Total	17	100%



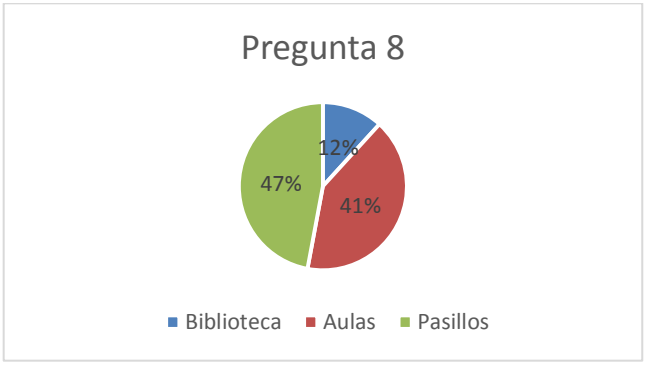
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 29% de encuestados que representa a 5 personas indican que la conexión en la red inalámbrica casi nunca falla, el 59% que representa a 10 personas indican que la conexión en la red inalámbrica nunca falla.

PREGUNTA N° 8

¿Desde qué parte de la escuela se conecta a las redes inalámbricas?

Biblioteca	**2**	**12%**
Aulas	7	41%
Pasillos	8	47%
Total	17	100%



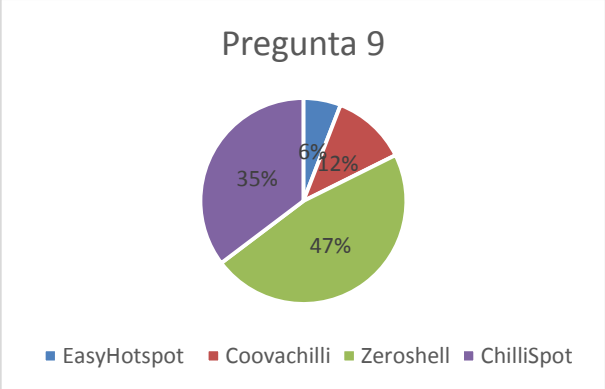
ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 12% de encuestados que representa a 2 personas indican los sectores de donde más se conectan es desde la biblioteca, el 41% que representa a 7 personas indican que los sectores de donde más se conectan es desde las aulas, el 47% que representa a 8 personas indican que los sectores de donde más se conectan es desde los pasillos.

PREGUNTA N° 9

Según el portal cautivo cuál cree usted que tiene una página de inicio adecuada.

EasyHotspot	**1**	**6%**
Coovachilli	2	12%
Zeroshell	8	47%
ChilliSpot	6	35%
Total	17	100%



ANÁLISIS

Luego de analizar los resultados obtenidos se concluye que el 6% de encuestados que representa a 1 personas indican que según la página de inicio la más adecuada para ellos es la del EasyHotspot, el 12% que representa a 2 personas indican que según la página de inicio la más adecuada para ellos es la del Coovachilli, el 47% que representa a 8 personas indican que según la página de inicio la más adecuada

para ellos es la del Zeroshell, el 35% que representa a 6 personas indican que según la página de inicio la más adecuada para ellos es la del ChilliSpot.

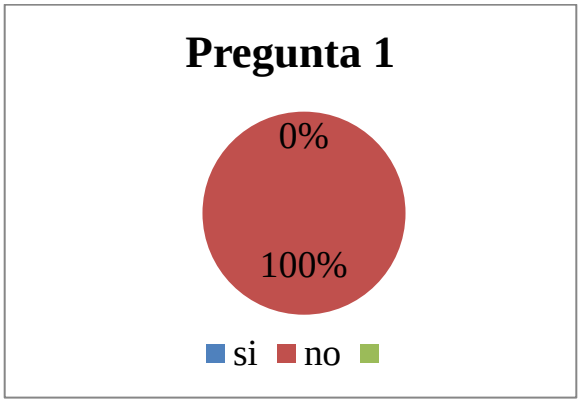
Encuesta 3 Porcentajes Correspondientes a los Parámetros de Comparación dirigida a los usuarios de la red Dr. Gabriel García Moreno

Resultados de las encuestas realizadas sobre complementos, tiempo de respuesta y seguridad que debería tener un portal cautivo.

PREGUNTA N° 1

¿Conoce los complementos que hay detrás de un Portal Cautivo?

Si	**0**	**0%**
No	17	100%
Total	17	100%



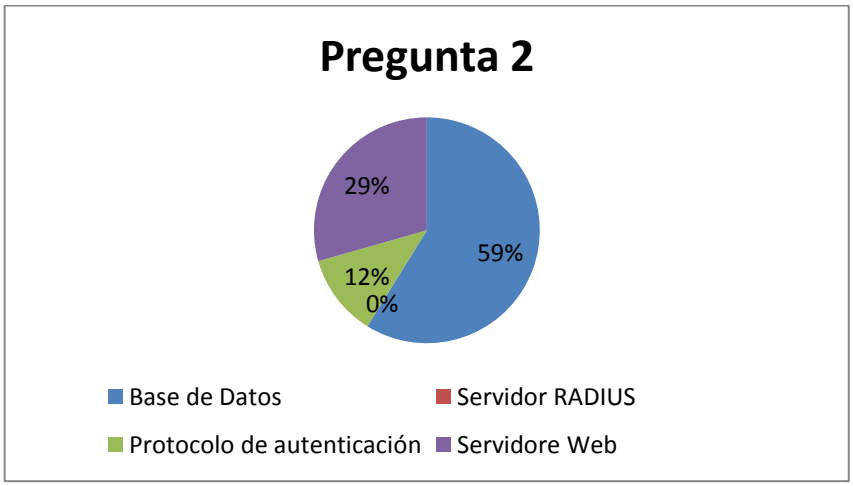
ANÁLISIS

En nuestro estudio se considero importante saber si los encuestados conocen los complementos que hay detrás de un portal cautivo, determinando así que 17 personas que corresponden el 100% no conocen acerca de los complementos que están detrás de un portal cautivo.

PREGUNTA N° 2

¿Conoce o ha escuchado alguno de estos términos?

Base de Datos	10	59%
Servidor RADIUS	0	0%
Protocolo de autenticación	2	12%
Servidor Web	5	29%
Total	17	100%



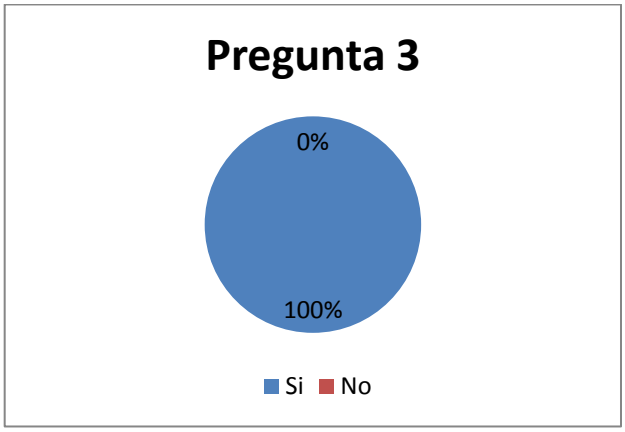
ANÁLISIS

Se consideró importante saber si los encuestados han escuchado alguno de estos términos, determinando así que 10 personas que son el 59% han escuchado el término base de datos, 2 personas que son el 12% han escuchado el término protocolo de autenticación, 5 personas que son el 20% han escuchado el término servidor web.

PREGUNTA N° 3

¿Es importante para usted el tiempo en el que se demora tener acceso al internet?

Si	**17**	**100%**
No	0	0%
Total	17	100%



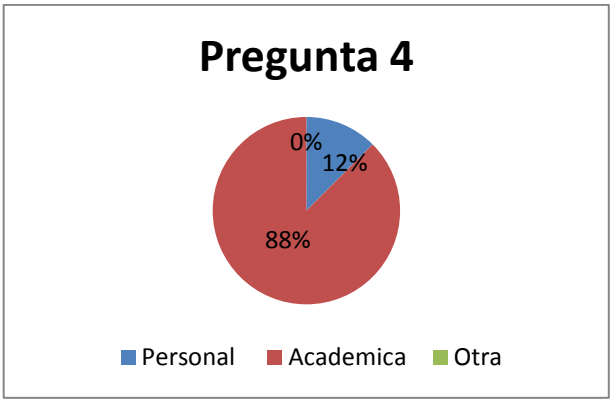
ANÁLISIS

En nuestro estudio se consideró importante saber si para los encuestados es importante el tiempo en el que se demora tener acceso al internet, determinando así que 17 personas que corresponden el 100% dicen que si es importante para ellos el tiempo en el que se demora tener acceso al internet.

PREGUNTA N° 4

¿Qué tipo de información maneja a través de la red inalámbrica de la institución?

Personal	**3**	**12%**
Académica	14	88%
Otra	0	0%
Total	17	100%



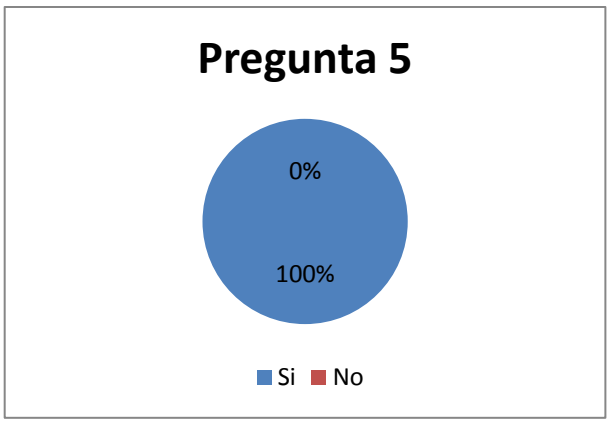
ANÁLISIS

Se consideró importante saber qué tipo de información manejan a través de la red institucional, determinando así que 3 personas que son el 12% manejan información personal, 14 personas que son el 88% manejan información académica.

PREGUNTA N° 5

¿Es importante para usted la información que maneja a través de la red de la institución?

Si	**17**	**100%**
No	0	0%
Total	17	100%



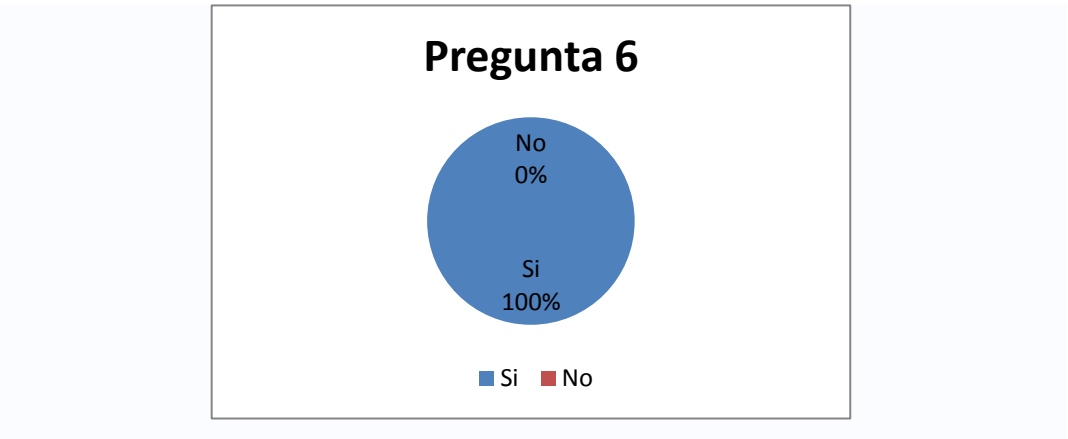
ANÁLISIS

En nuestro estudio se consideró importante saber si para los encuestados es importante la información a través de la red institucional, determinando así que 17 personas que corresponden el 100% dicen que si es importante la información que manejan a través de la red de la institución.

PREGUNTA N° 6

¿Cree usted que en el estado en el que se encuentra la red inalámbrica de la institución existe seguridad de los datos académicos?

Si	**17**	**100%**
No	0	0%
Total	17	100%



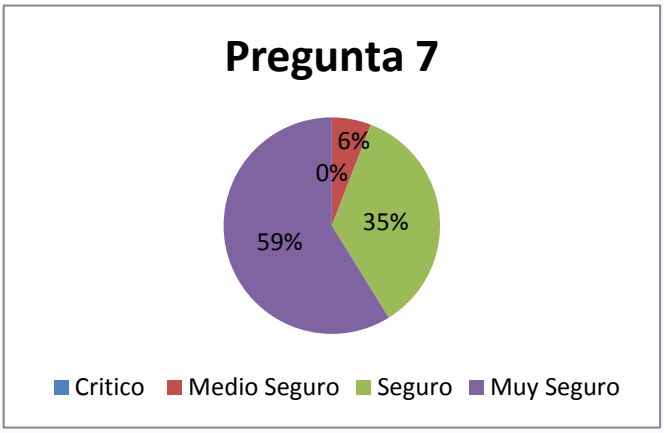
ANÁLISIS

En nuestro estudio se consideró importante saber si para los encuestados es importante saber si existe seguridad de los datos académicos, determinando así que 17 personas que corresponden el 100% dicen que si es importante saber que existe seguridad de los datos académicos.

PREGUNTA N° 7

¿Cómo calificaría la seguridad de la red institucional en el estado que se encuentra actualmente?

Critico	**0**	**0%**
Medio Seguro	1	6%
Seguro	6	35%
Muy Seguro	10	59%
Total	17	100%



ANÁLISIS

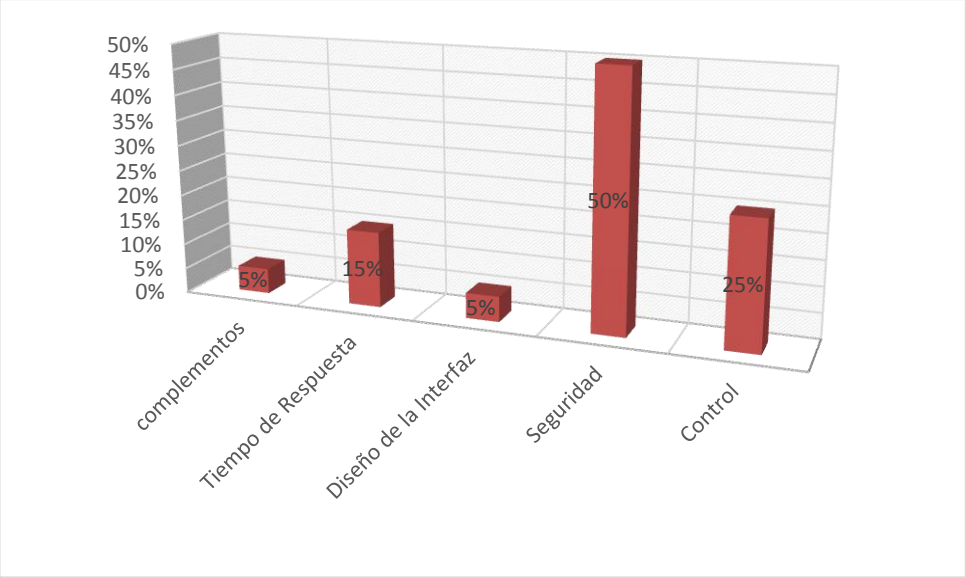
Se consideró importante saber cómo los encuestados calificaría la seguridad de la red institucional en el estado que se encuentra actualmente, determinando así que 1 personas que es el 6% califica a la seguridad como medio seguro, 6 personas que son el 35% califican a la seguridad como seguro, 10 personas que son el 59% califican a la seguridad como muy seguro.

Resultados de las encuestas realizadas para establecer la ponderación del porcentaje de cada uno de los parámetros de comparación

Ponderación de los resultados de las encuestas dirigidas a los Profesionales en redes o administración de las mismas.

Complementos	**5%**
Tiempo de Respuesta	15%
Diseño de la Interfaz	5%
Seguridad	50%
Control	25%
Total	100%

La grafica a continuación detalla cuales son los parámetros más importantes para los profesionales de la red.

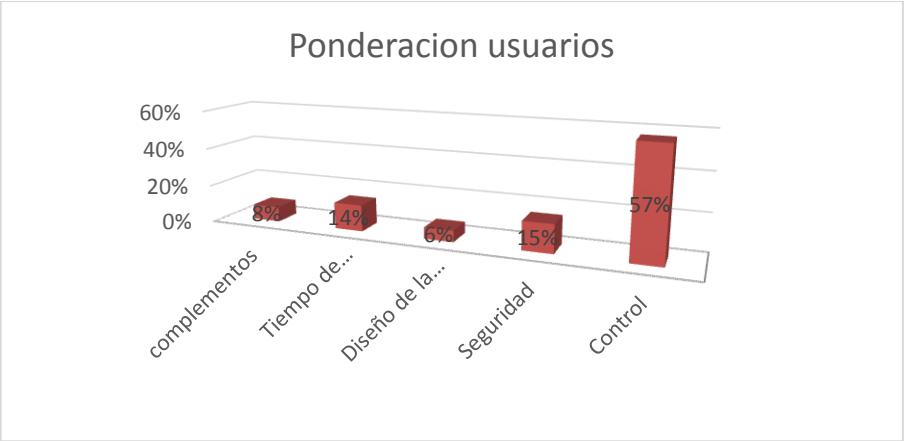


Ponderación de os resultados de las encuestas dirigidos a usuarios de una red.

Complementos	**8%**
Tiempo de	14%

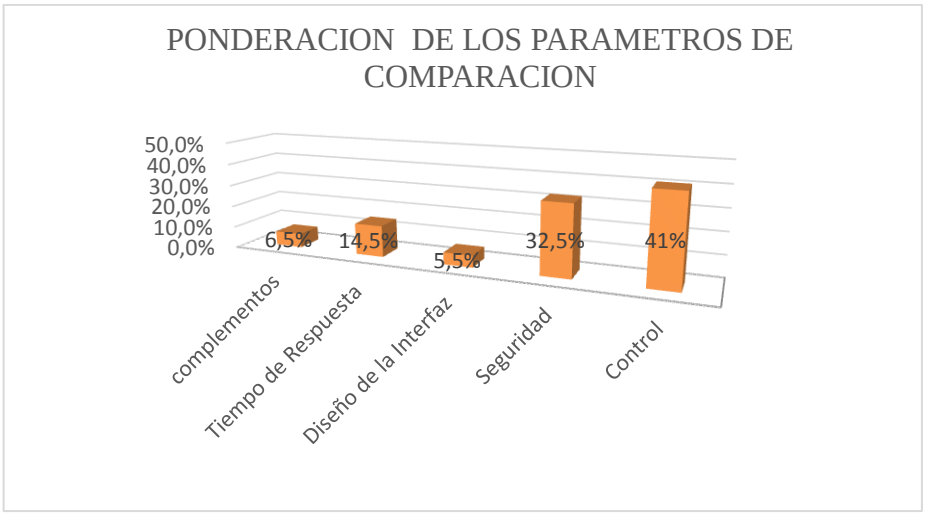
Respuesta	
Diseño de la Interfaz	6%
Seguridad	15%
Control	57%
Total	100%

La grafica a continuación detalla cuales son los parámetros más importantes para los usuarios de la red de la escuela Gabriel García Moreno.



Total de la ponderación obtenida entre la ponderación profesionales y de los usuarios

	Profesionales	Usuarios	TOTAL
Complementos	5%	8%	6,5%
Tiempo de Respuesta	15%	14%	14,5%
Diseño de la Interfaz	5%	6%	5,5%
Seguridad	50%	15%	33,5%
Control	25%	57%	41%
Total	100%	100%	100%


PONDERACION DE LOS PARAMETROS DE COMPARACION
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
6,5%
14,5%
5,5%
32,5%
41%
complementos
Tiempo de Respuesta
Diseño de la Interfaz
Seguridad
Control