



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

**“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE
SEGURIDAD PARA EL ACCESO DE LA RED
INALÁMBRICA DEL COLEGIO OTTO AROSEMENA
GÓMEZ”**

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

INGENIERO EN TELEMÁTICA

LUIGGY ALBERTO ALLAUCA GUSQUI

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Mis más sinceros agradecimientos a mi familia que siempre está presente y me han ayudado durante todo este proceso de preparación que forjando mis proyectos a largo plazo y que con sacrificio los estoy logrando; de manera especial agradezco a Dios que es el pilar fundamental en mi vida y bajo su intercesión he podido alcanzar mis metas.

Además mi infinito agradecimiento al profesor de la Materia Integradora y tutor que gracias a sus conocimientos transmitidos he podido realizar con éxito la culminación del proyecto de Investigación.

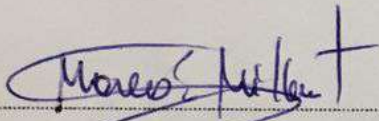
DEDICATORIA

El presente proyecto lo dedico a Dios y a la Virgen, por regalarme con mucho amor el don de la vida y permitirme haber llegado hasta este momento tan importante en mi formación profesional.

A mis padres que me han impulsado a seguir adelante con sus sabios consejos y ejemplos de lucha que han logrado motivar cada esfuerzo que he realizado en mi proceso de formación. A mis hermanos que han estado prestos a ayudarme dándome su apoyo incondicional.

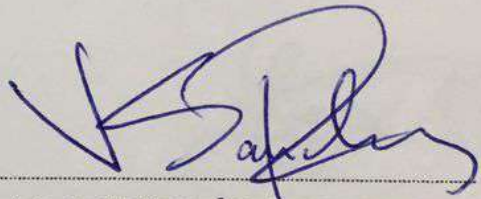
Y a mis profesores que hicieron posible realizar mis pasantías y que siempre estuvieron pendientes de mi desempeño estudiantil.

TRIBUNAL DE EVALUACIÓN



MS. MARCOS MILLAN TRAVERSO

PROFESOR EVALUADOR

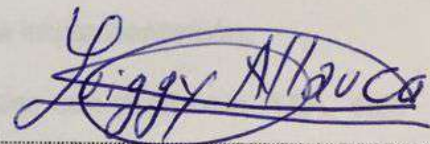


ING. VLADIMIR SÁNCHEZ PADILLA

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Luiggy Allauca

RESUMEN

El presente proyecto integrador brinda una solución oportuna y eficaz para la seguridad de los datos enviados por el usuario final dentro de una red WI-FI, para la comunicación entre los diferentes dispositivos informáticos que se tengan en el laboratorio de computación del colegio Otto Arosemena Gómez.

Se desarrolla un sistema de seguridad con autenticación de usuarios mediante el uso de una plataforma administradora que permita tener control de todos los usuarios finales que se conecten a la red inalámbrica. Para una mejor solución del problema de seguridad en la red, se plantea usar software libre para el desarrollo total del sistema, esto permitirá una mejor retroalimentación de algún problema que surja en la implementación.

El proceso de autenticación se lo realiza mediante un servidor con protocolo AAA, esto significa que el cliente posee privilegios de estar asignado en la red para gozar de autenticación, autorización y acceso a toda la información que posea la red inalámbrica de la institución educativa. Se usa el método de autenticación WPA en el punto de acceso de la red WI-FI, además se habilita el direccionamiento dinámico DHCP para que el usuario pueda tener direcciones IP dinámicas.

En el capítulo uno se especifica en detalle las causas y efectos que producen la inseguridad de la red inalámbrica del colegio, así como el alcance y limitación del sistema. El capítulo dos se implementa el desarrollo de la tecnología que se usó en el proyecto, las configuraciones de cada uno de los servicios informáticos que se establecen en el servidor de autenticación que se manejan de manera conjunta para su correcto funcionamiento.

El tercer capítulo se muestra la funcionalidad del proyecto integrador, las pruebas que se tomaron fueron en base a la información proporcionada por el colegio, puesto que se implementó según la necesidad que requerían en la institución.

ÍNDICE GENERAL

AGRADECIMIENTOS.....	ii
DEDICATORIA	iii
TRIBUNAL DE EVALUACIÓN.....	iv
DECLARACIÓN EXPRESA	v
RESUMEN	vi
CAPÍTULO 1	1
1. PROBLEMÁTICA.....	1
1.1 Planteamiento del Problema.....	1
1.1.1 Causa y Efecto	2
1.2. Justificación.....	4
1.3. Objetivo General.....	4
1.4. Objetivos Específicos.....	4
1.5. Alcances y limitaciones.....	5
CAPÍTULO 2	6
2. IMPLEMENTACIÓN.....	6
2.1 Diseño de la solución.....	6
2.2 Instalación del software	7
2.2.1 Instalación del sistema operativo Linux	7
2.2.2 Instalación del servidor web Apache.....	14
2.2.3 Instalación de la base de datos MySQL	15
2.2.4 Instalación de PHP	16
2.2.5 Instalación de FreeRadius	17
2.2.6 Instalación de DaloRadius	24
2.3 Instalación del hardware.....	26
2.3.1 Configuración del router inalámbrico.....	26

CAPÍTULO 3	29
3. PRUEBAS Y RESULTADOS.....	29
3.1 Primera prueba	29
3.2 Segunda prueba	31
CONCLUSIONES Y RECOMENDACIONES.....	41
BIBLIOGRAFÍA.....	43

CAPÍTULO 1

1. PROBLEMÁTICA

1.1 Planteamiento del Problema

Los avances tecnológicos actualmente han evolucionado a gran escala por la alta disponibilidad de internet que existe en el mundo, esto se debe a la comunicación instantánea entre las redes que alberga el internet; dicha comunicación permite tener acceso a recursos informáticos de hardware o software. Si se desea gozar de este tipo de acceso sin duda se deberá contar con una red informática segura que permita una mejor disponibilidad de los recursos [1]. Con esto se manifiesta que la tecnología y la comunicación van de la mano para brindar soluciones a necesidades que tenga la humanidad; los campos donde la tecnología informática ha marcado innovación han sido muchos pero destacamos el empresarial, educativo, científico, gubernamental, etc.

El tener acceso a una red de área local, es una forma de comunicación para facilitar los recursos al usuario de la red LAN; pero contar con acceso a información, es también estar tentado a que se filtren intrusos que hagan mal uso de la información impartida, para esto se debe de contar con el uso de esquemas de seguridad que garanticen la confidencialidad de la información solicitada [2]. Ante esta necesidad surgen los protocolos de seguridad, los cuales facilitan la comunicación entre una entidad emisora y receptora, en muchas ocasiones estas entidades poseen usuarios con diferentes sistemas operativos, esta mezcla de sistemas permiten que los protocolos se creen para satisfacer la comunicación entre ambas entidades.

Uno de los protocolos de seguridad más usados en los software libres es Radius[3], este protocolo brinda servicios de autenticación, autorización y acceso de la información que solicite; dicho protocolo ayuda a crear una red segura donde los usuarios beneficiados por la red LAN deben ser claramente identificados para que puedan tener acceso a la red y de esta manera gozar de todos los privilegios de la información que solicite dicho usuario [4].

La problemática encontrada mediante varias visitas realizadas al Colegio Fiscal Otto Arosemena Gómez ubicado en la ciudad de Guayaquil muestra que la institución no posee una red inalámbrica segura que ayude en el control de la banda ancha del internet en los laboratorios informáticos del colegio, esto dificulta que los estudiantes y profesores exploten al máximo los beneficios que podrían obtener de los laboratorios; actualmente la institución cuenta con un irregular acceso a internet, debido que no existe un control de los usuarios que ingresan a la red Wi-Fi [5]. Cabe acotar que el colegio posee dos laboratorios de computación con pc de escritorio que poseen tarjetas de red inalámbrica en un laboratorio y en el otro con cableado a la red; nuestro proyecto se centrará en el laboratorio que posee conexión inalámbrica y de los usuarios que deseen conectarse mediante cualquier otro dispositivo que no sea del laboratorio.

El presente proyecto plantea una solución práctica y verificable para suplir las necesidades de inseguridad en la red, en nuestro caso el desarrollo de un sistema de seguridad en la red inalámbrica del colegio; con esto se controlará el acceso de todos los usuarios que deseen conectarse a la red inalámbrica mediante una forma segura, en la cual garantice al usuario el ingreso a la red de una manera confiable; para controlar dicho acceso se implementará un servidor Radius que disponga de sus servicios para el control de los usuarios que se autentifiquen. El desarrollo de dicho sistema permitirá colaborar en el proceso de aprendizaje del estudiante, además de crear un ambiente de fácil acceso a la red inalámbrica con el respaldo de internet seguro y eficiente. De esta manera se obtendrá la interacción de los alumnos, profesores y demás autoridades del colegio de manera que gocen de todos los privilegios que posee el internet a nivel mundial, sobre todo en el campo educativo [6].

1.1.1 Causa y Efecto

Habiendo evidenciado la carencia de recursos informáticos en los laboratorios de computación del colegio, el problema que se plantea en el proyecto es la inseguridad de la red inalámbrica del Colegio Fiscal Otto Arosemena Gómez. Para esto se establece un análisis de causas y efectos del problema detectado.

Los efectos producidos del problema planteado, son los siguientes:

- Mala calidad de la señal Wi-Fi
- Limitación del banda ancha del internet
- Alta conectividad insegura
- Altos gastos de mantenimiento
- Baja productividad de los usuarios
- Mal uso del internet
- Alta autenticación de usuarios intrusos

Las causas que producen el problema planteado, son los siguientes:

- Inadecuada disposición del laboratorio
- No hay control en la red Wi-Fi
- No hay registros de usuarios
- Mal manejo de usuarios y contraseñas
- No hay certificaciones de seguridad
- Escasos recursos informáticos de seguridad

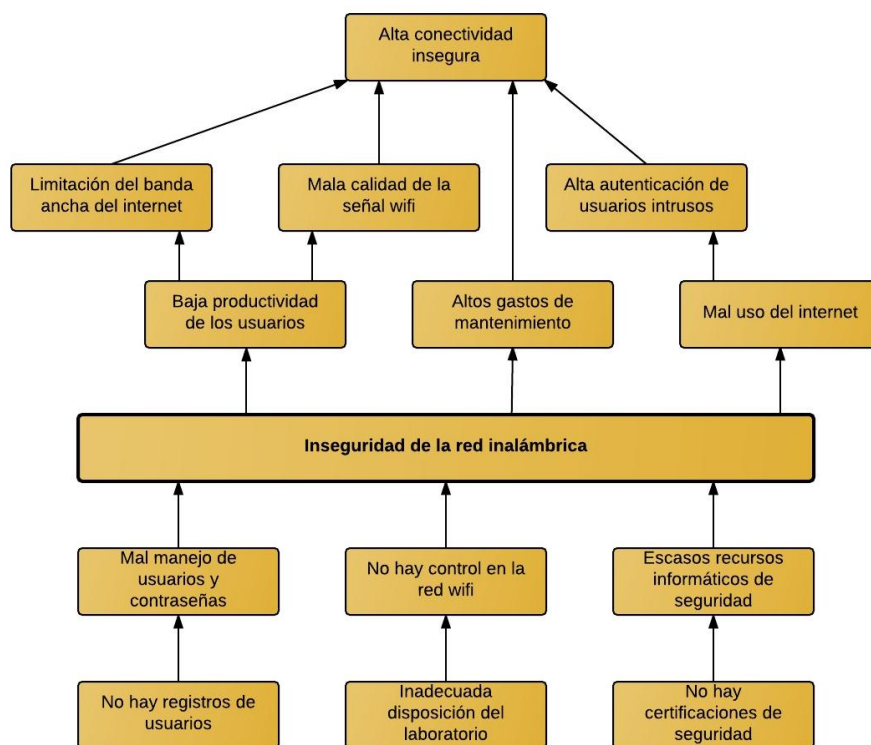


Figura 1.1: Diagrama de Causa y Efecto.

1.2. Justificación

Actualmente la mayoría de las instituciones educativas del Ecuador poseen laboratorios de computación equipados con internet para los usuarios de las entidades educativas; esto requiere de la construcción de sistemas de seguridad sofisticados que faciliten a la persona una experiencia de navegación segura en internet, sin preocupación de intrusos en la red. Tanto el docente como el estudiante tendrán la facilidad de contar con un nuevo espacio de aprendizaje continuo proporcionado por la red inalámbrica con abastecimiento de internet, donde se pueda tener total libertad de navegación en la web, siempre que sea con fines educativos e investigativos para el sano esparcimiento del usuario final.

Precisamente el presente proyecto se centra en la necesidad de implementar técnicas que ayuden en la construcción de un sistema de seguridad interactivo, el cual garantice al usuario final una navegación segura en internet por la previa autenticación del usuario mediante un portal cautivo; con esto se tendrá un control de quienes se conecten a la red, además esto ayudará en el desenvolvimiento académico que tenga el estudiante en el colegio, dado que su ingreso quedará registrado para el control de un aplicativo administrador de usuarios y contraseñas.

1.3. Objetivo General

Construir un sistema de seguridad que permita el mejoramiento de la red inalámbrica en el consumo de la banda ancha de internet en el Colegio Fiscal Otto Arosemena Gómez.

1.4. Objetivos Específicos

- Crear un sistema de seguridad interactivo que facilite la comunicación entre el cliente y servidor.
- Mejorar el proceso de autenticación de usuarios en la red inalámbrica mediante la creación del sistema de seguridad.
- Permitir el fácil acceso a la red inalámbrica con internet seguro y eficiente.

1.5. Alcances y limitaciones

El Colegio Fiscal Otto Arosemena Gómez es una institución educativa respalda por el gobierno y que beneficia a jóvenes del suburbio de Guayaquil. Cuenta con diversos laboratorios técnicos, cursos, biblioteca, auditorio, espacios recreacionales y departamentos para la atención de estudiantes o padres de familias.

En los últimos años el colegio ha tenido valiosa ayuda de parte del gobierno, pero aun así, hacen falta los recursos que permitan al estudiante lograr el crecimiento académico que necesitan. El proyecto será diseñado para cubrir las necesidades tanto del estudiante como del profesor. El número estimado de personas que se abarcará en el proyecto será para estudiantes del laboratorio de computación que poseen entrada inalámbrica al colegio, ya que son las más idóneas para el sistema; los profesores ayudarán a impartir la funcionalidad del sistema y la aplicación que se posea en el colegio.

El proyecto contará con restricciones para los estudiantes y profesores, esto debido a que son usuarios con distintos roles dentro del sistema de seguridad; por lo tanto se debe contar con confiabilidad y seguridad total dentro de la plataforma, para el bienestar de cada uno de los usuarios que se verán involucrados. Cabe destacar que el proyecto contará con pruebas piloto tanto para el profesor como para el estudiante; previamente se harán capacitaciones a los distintos usuarios que se vean involucrados en el sistema.

CAPÍTULO 2

2. IMPLEMENTACIÓN

En este capítulo, se mostrará toda la configuración e implementación del servidor Radius y del aplicativo administrador. Se plantea la metodología con un diseño de la solución a desarrollarse, además se detalla la instalación de todas las herramientas de hardware y software que funcionan de manera simultánea para la aplicabilidad en la seguridad de la red inalámbrica de la institución educativa.

Para el sistema de seguridad, se configurará un LAMP, que es una arquitectura de código abierto que proporcionará la funcionalidad de integrar varios elementos como un método de desarrollo en conjunto; el LAMP está compuesto por Linux, Apache, Mysql y Php [7]. En el proyecto se detallará cada uno de los pasos de instalación para conformar esta eficiente herramienta que ayudará en la implementación del sistema de seguridad.

2.1 Diseño de la solución

El diseño que se plantea para la implementación de la solución, proporciona una topología extendida que facilitará la conexión a la red WI-FI mediante cualquier dispositivo que tenga accesibilidad con internet. La red inalámbrica con direccionamiento IP clase C 192.168.10.0 y con máscara de red 255.255.255.0, está configurada para una conectividad que no sobre pase los 254 elementos conectados a la red wifi de la institución educativa.

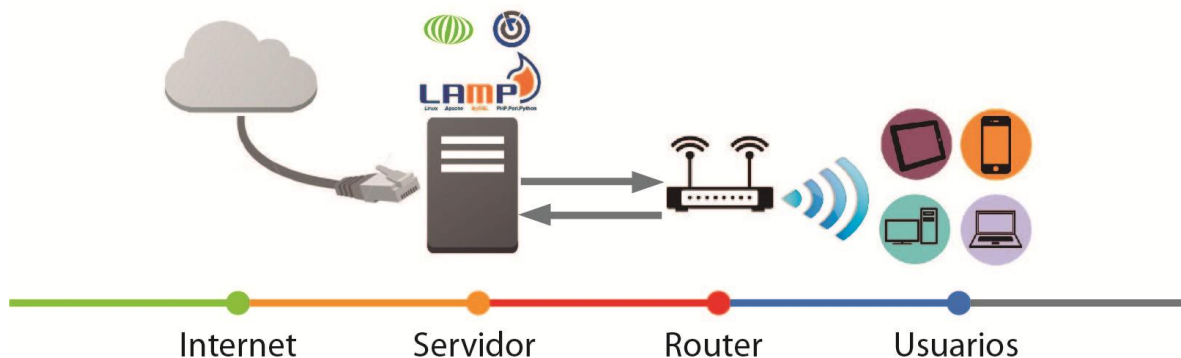


Figura 2.2: Topología de conexión y comunicación de la red inalámbrica.

La topología mostrada en la figura 2.2; presenta una arquitectura cliente-servidor, donde se involucran tres elementos en la autenticación de los usuarios finales hacia un servidor radius, donde son los siguientes:

1. Servidor radius: sistema que permite la autenticación de los usuarios, dependiendo de la información que proporcione el usuario se verifica en la base de datos que se maneja en el servidor. Si la información proporcionada se encuentra en la base se permite la autenticación, caso contrario se deniega su ingreso a la red.
2. Cliente radius (router): es el punto de acceso que proporciona comunicación entre equipos de comunicación inalámbrica; este dispositivo de red se conecta al servidor radius, preguntando si la información proporcionada por el usuario final son válidos para el proceso de autenticación.
3. Usuarios: son dispositivos de comunicación inalámbrica que envían peticiones de conexión al cliente radius.

Los tres elementos de autenticación deben emplear una conectividad a internet hacia el servidor radius de acceso a la red (NAS), esto permitirá que los servicios y configuraciones que solicitan los usuarios tengan accesibilidad a internet. El router inalámbrico permitirá el acceso a la red inalámbrica del colegio, será el canal por el cual se filtrarán todos los datos del usuario.

2.2 Instalación del software

2.2.1 Instalación del sistema operativo Linux

Para el proyecto se escogió al sistema operativo Linux por la flexibilidad, seguridad y estabilidad que ofrece para un servidor. La distribución que se escogió para instalar Linux fue Debian 8 con entorno virtual mate; existen una gran variedad de distros para Linux, se escogió entre una gama extensa de distribuciones las cuales se hace una tabla comparativa para ver cuál distribución es la más óptima para el proyecto. Ejemplo: ver Tabla 1.

Distribución	Tipo	Usos	Distribución Base
CentOS	Gratuita	Servidores Est. trabajo Producción	Red Hat Linux
Red Hat Linux	Comercial	Servidores Est. trabajo Producción	Ninguna
SUSE	Comercial	Servidores Est. trabajo Producción	Ninguna
Ubuntu	Gratuita Comercial	Servidores Escritorios Est. trabajo Producción	Debian
Debian	Gratuita	Multiusos Producción	Ninguna
Fedora	Gratuita	Multiusos Vanguardia	Red Hat Linux

Tabla 1: Distribuciones linux

La distribución que nos permite tener un servidor con una plataforma segura y estable, es Debian por poseer requisitos muy adaptables a un servidor. Ejemplo: ver Tabla 2.

Distribución	CPU	RAM	Disco Duro
CentOS	1GHz	128Mb - 512 Mb	1.2Gb - 2Gb
Red Hat Linux	2.4GHz	2Gb – 8Gb	5Gb
SUSE	500MHz - 2.4 GHz	512Mb - 1Gb	3Gb - 5Gb
Ubuntu	1GHz	512 Mb	5Gb
Debian	1GHz	256Mb – 512 Mb	1Gb – 5Gb
Fedora	400MHz	768Mb - 1Gb	10Gb

Tabla 2: Requisitos del Sistema operativo linux

Para proceder con cada uno de los pasos de instalación del sistema operativo, se debe considerar lo siguiente:

- Se debe descargar la imagen de debían 8, esto se lo puede descargar desde <http://cdimage.debian.org/debian-cd/8.6.0/i386/iso-cd/>
- Para instalar nuestro sistema operativo se boteo un pendrive, usando el programa unetbootin-windows-625.
- El pendrive debe estar formateado para que sea booteable y para de esta manera instalar el sistema operativo.
- Antes de instalar Linux Debian, se debe descargar el firmware para Debian 8, esto servirá para activar el servidor desde el encendido y preparar al sistema operativo en la memoria RAM. Los archivos que se descargan del firmware se copiarán directamente en la carpeta del mismo nombre dentro del pendrive booteado.

Con las consideraciones mencionadas se procede con los pasos para la instalación del sistema operativo Linux Debian 8:

1. El primer paso es bootear el pendrive con el programa unetbootin-windows-625, se seleccionará la imagen ISO de Debian 8 y se escogerá la unidad USB que ha sido asignado a su pendrive, en nuestro caso G:\. Luego dar clic en aceptar, posteriormente quedará booteado nuestro pendrive. Como ejemplo observar la figura 2.3.

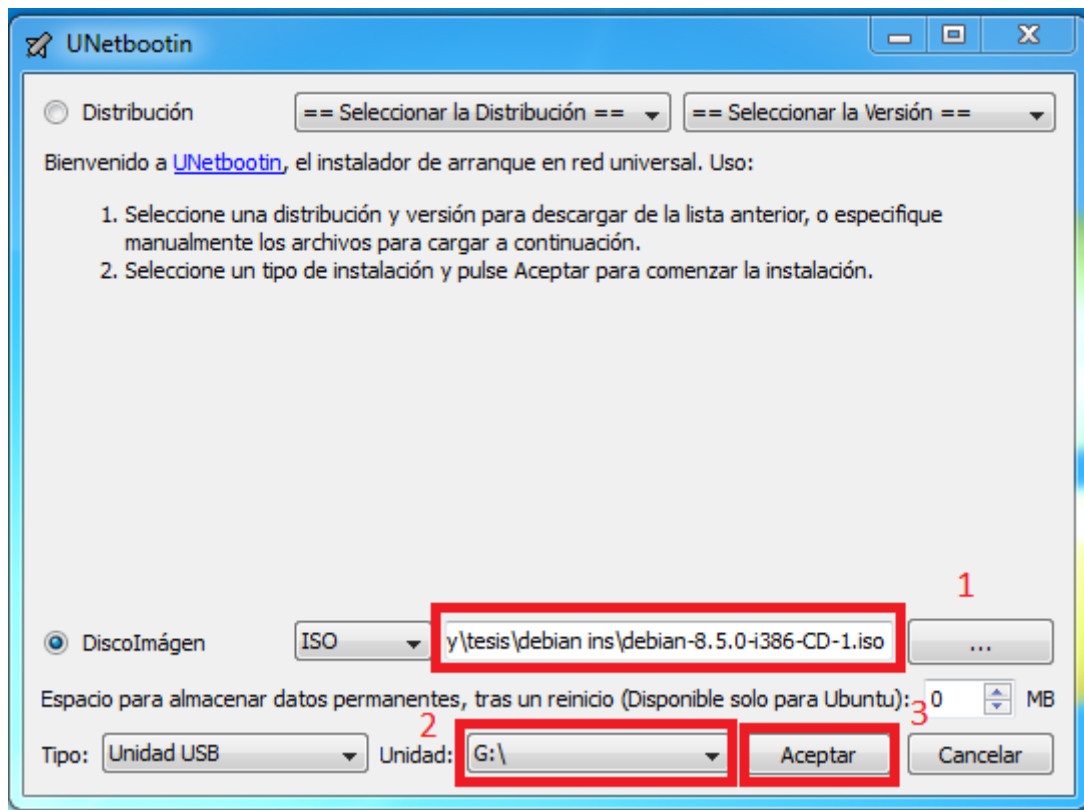


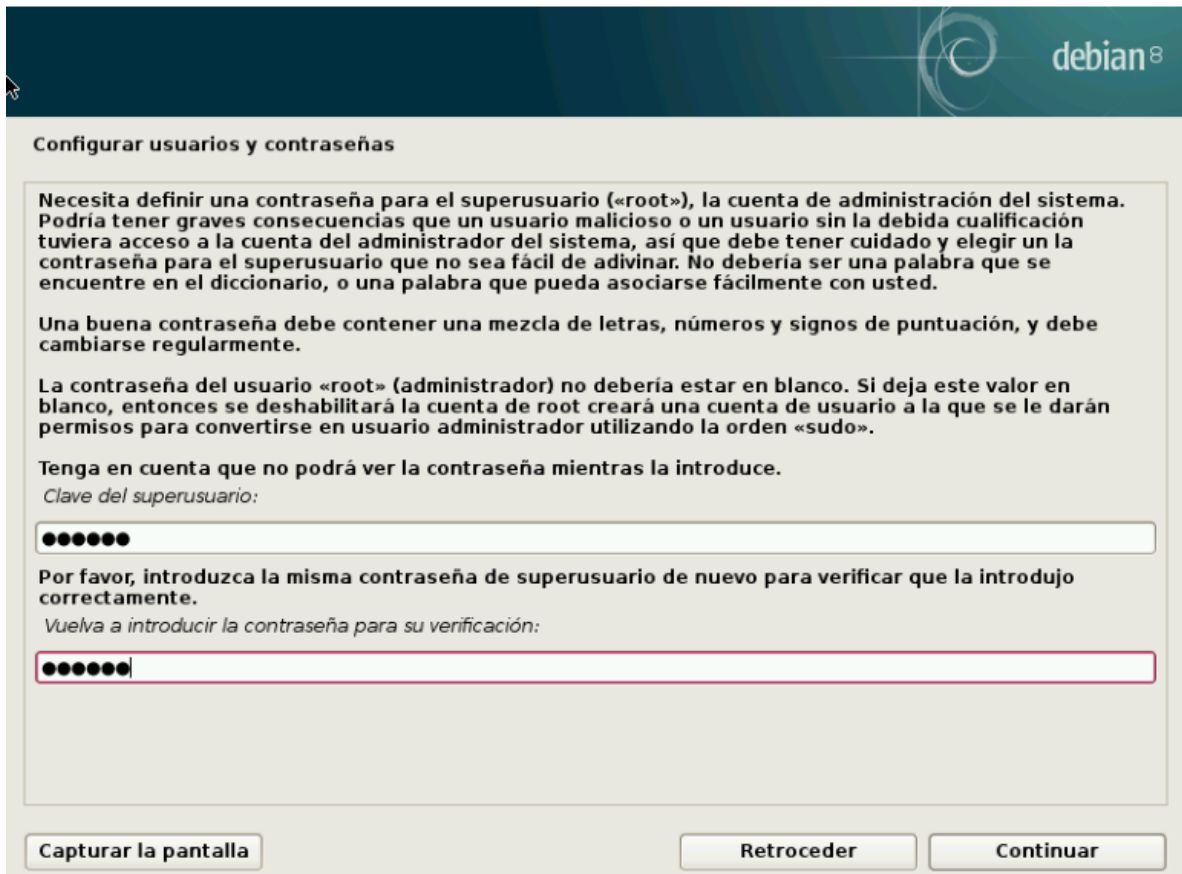
Figura 2.3: Booteo del Pendrive

2. Se inserta el pendrive y al encender la máquina servidora, se presionará la tecla F10 de manera inmediata cuando se ejecute la BIOS; de esta forma se accederá al pendrive booteable. Luego nos mostrará una pantalla para elegir la forma de instalar Debian 8; damos enter en la opción Graphical Install. Como ejemplo observar la figura 2.4.



Figura 2.4: Menú para Instalación de Debian

3. Para proceder con la instalación de Debian 8 se deberá ingresar información básica de idioma, ubicación, uso horario, mapa de teclado y nombre de la máquina.
4. De manera automática o manual se configura la red, cabe destacar que debe haber conexión a internet para que la instalación se ejecute de manera exitosa.
5. Se crea automáticamente la cuenta de superusuario "root", para el administrador de la máquina servidora; luego se pedirá una contraseña para el superusuario, el cual se configura con un estricto nivel de seguridad para que no exista algún usuario no autorizado en la administración de los servicios del sistema operativo. Como ejemplo observar la figura 2.5.



Configurar usuarios y contraseñas

Necesita definir una contraseña para el superusuario («root»), la cuenta de administración del sistema. Podría tener graves consecuencias que un usuario malicioso o un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del sistema, así que debe tener cuidado y elegir un la contraseña para el superusuario que no sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o una palabra que pueda asociarse fácilmente con usted.

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

La contraseña del usuario «root» (administrador) no debería estar en blanco. Si deja este valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario a la que se le darán permisos para convertirse en usuario administrador utilizando la orden «sudo».

Tenga en cuenta que no podrá ver la contraseña mientras la introduce.

Clave del superusuario:

●●●●●●

Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

●●●●●●

Capturar la pantalla Retroceder Continuar

Figura 2.5: Creación de la Contraseña Root.

6. Se crea una cuenta de usuario estándar, para que se pueda acceder al sistema operativo; este usuario no será privilegiado para administrar en su totalidad el sistema, si se desea la administración total del sistema operativo se deberá ingresar como usuario root desde la terminal.
7. Se define la partición del disco duro con método de particionado manual, para poder instalar el sistema operativo. Se establece una partición swap con área de intercambio de manera lógica, donde su espacio será el doble de la memoria RAM del servidor; en el espacio que queda libre se escoge todo para realizar la instalación del sistema operativo.

8. Se instala todos los paquetes y programas necesarios para la instalación del sistema base de Debian 8; el proceso de instalación incluye las herramientas dpkg y apt para la administración de los paquetes de Debian. En los programas a instalar se escoge el entorno gráfico mate. Como ejemplo observar la figura 2.6 [8].

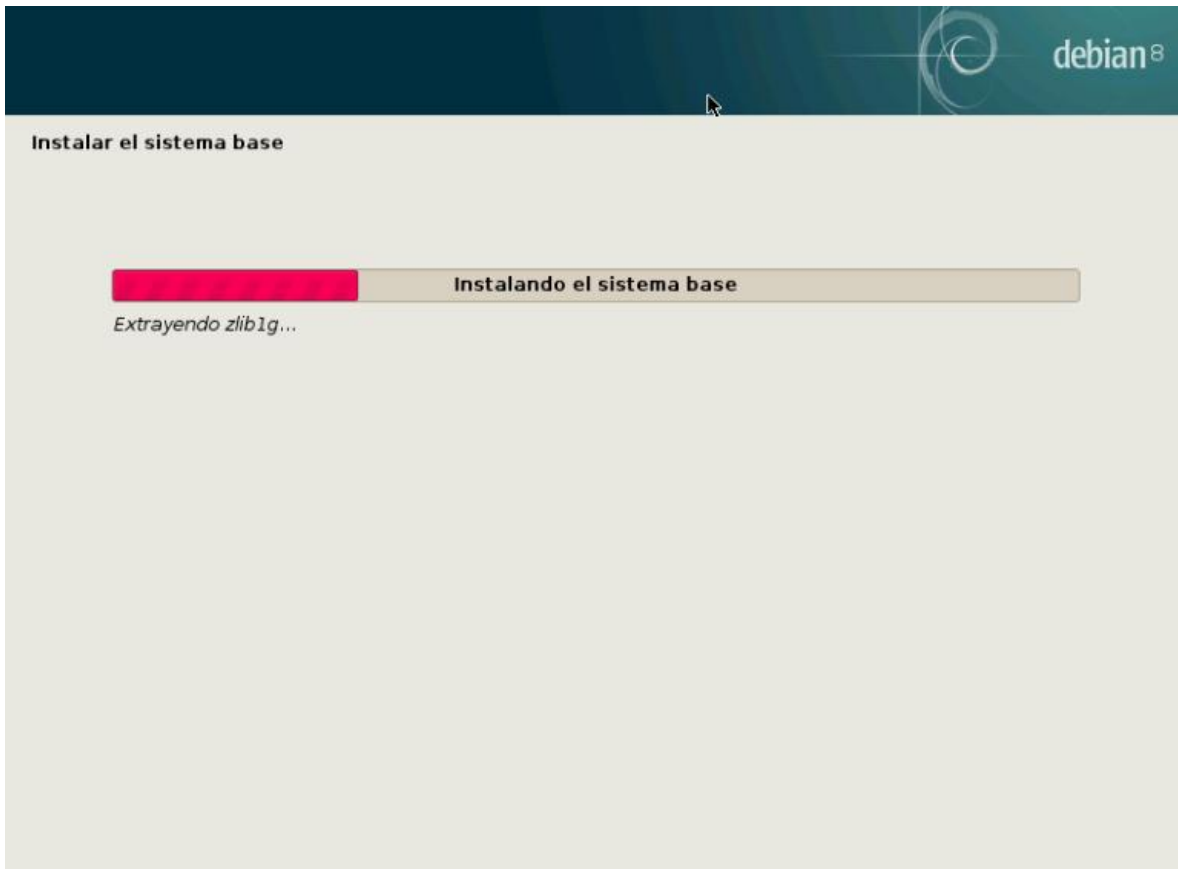


Figura 2.6: Instalación del Sistema Base Debian.

9. Al finalizar el proceso de instalación se procederá a quitar el pendrive del servidor para dar paso al inicio de sección, con el entorno gráfico del sistema operativo Debian 8.

Instalado el sistema operativo y ejecutándose correctamente, se debe considerar los siguientes puntos antes de instalar el resto de programas y servicios que se configurarán para el sistema de seguridad:

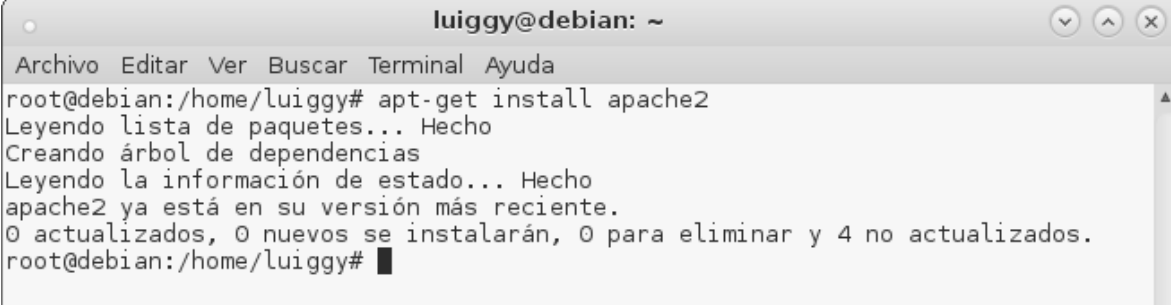
- Para realizar cambios o instalaciones en el sistema operativo se deberá ingresar como superusuario “root” desde la terminal de Debian, mediante líneas de comandos.
- Para descargar o actualizar, se deberá gozar de acceso a internet de forma permanente e ininterrumpida.

Con las consideraciones mencionadas anteriormente; se abre una ventana de la terminal y se ingresa como usuario “root”, para administrar el sistema. Para instalar los programas que se nos pide en el sistema de seguridad primeramente se actualiza los paquetes del repositorio con el comando:

```
#apt-get update
```

2.2.2 Instalación del servidor web Apache

El servidor web se instaló de manera conjunta con Debian, se procede a verificar la correcta instalación desde la terminal; como se puede apreciar en la figura 2.7, no se instala el servidor apache puesto que se encuentra instalado.



```
luiggy@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/luiggy# apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
root@debian:/home/luiggy# █
```

Figura 2.7: Instalación del Servidor Web Apache.

Para comprobar la funcionalidad que cumple el servidor web, se ingresa al browser insertando la ruta localhost; habiendo ingresado a la ruta local del servidor web se puede demostrar que apache está trabajando correctamente dentro del servidor. Como ejemplo se puede observar la figura 2.8

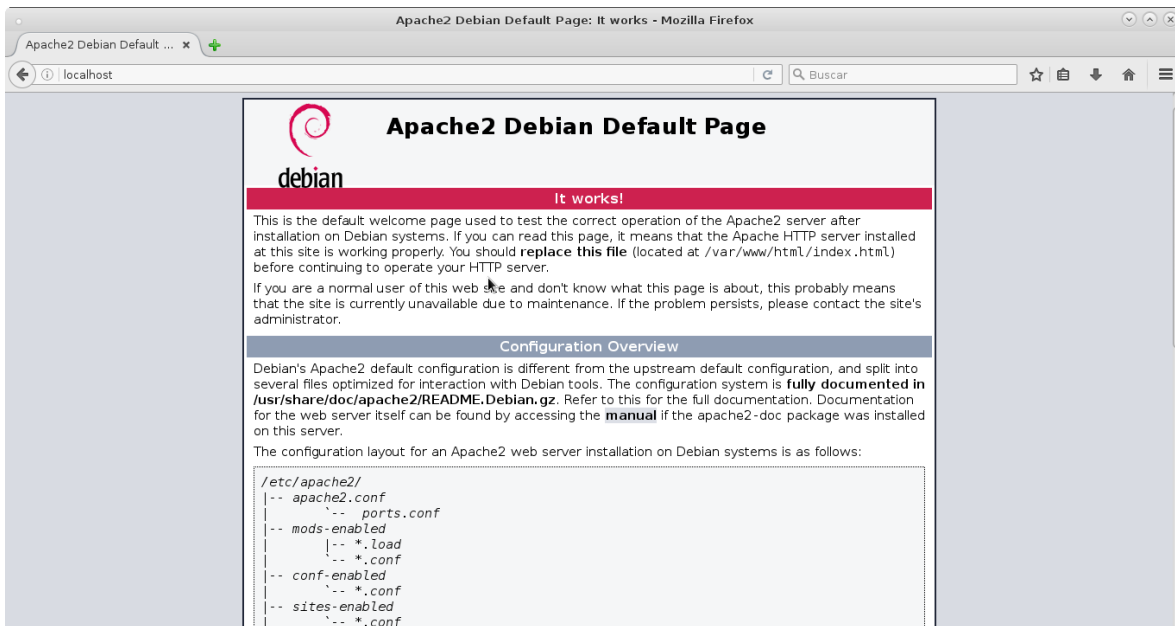


Figura 2.8: Servidor Web Apache Funcionando.

2.2.3 Instalación de la base de datos MySQL

Teniendo el servidor web ya instalado, se procede con la instalación del gestor de base de datos; para instalar MySQL se ingresa por la terminal la siguiente línea de comando:

```
#apt-get install mysql-server
```

En el proceso de instalación nos mostrará una ventana de configuración de mysql-server, el cual pedirá una contraseña para el usuario root de MySQL; ingresar una nueva contraseña es opcional pero en nuestro proyecto se cambió de contraseña por seguridad de la base. Como ejemplo se puede ver la figura 2.9.

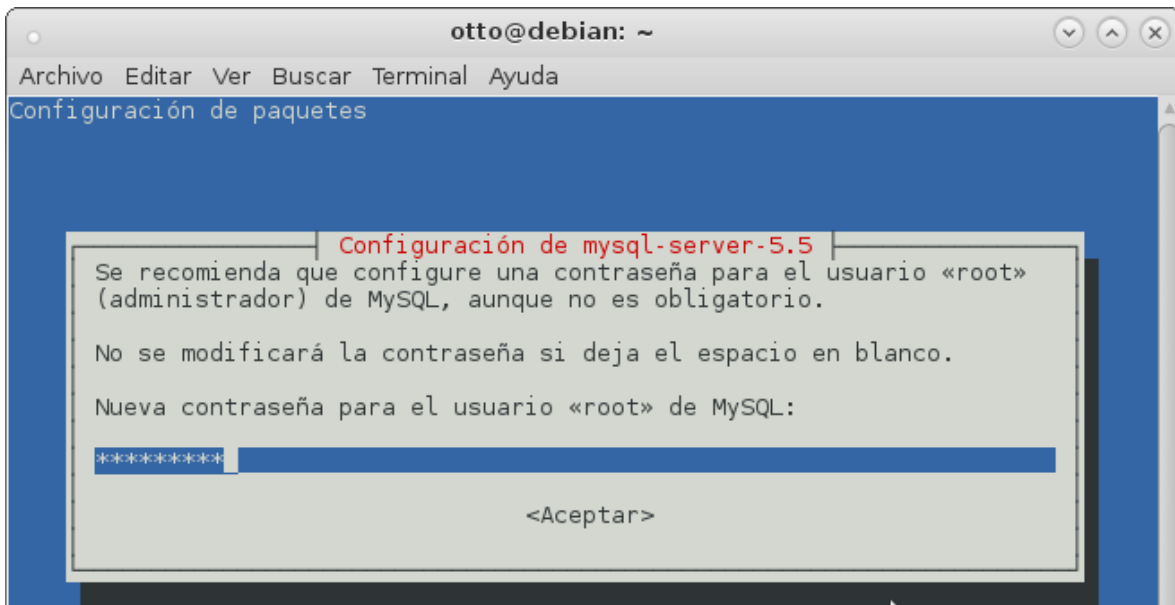


Figura 2.9: Configuración de la Contraseña del Usuario Root.

2.2.4 Instalación de PHP

Para completar la instalación del último elemento que compone nuestro LAMP se procede a instalar el lenguaje de programación que interpretará los códigos de programación que se encuentran en nuestro aplicativo administrador dadoradius y en el servidor de base de datos.

En el proyecto se instaló php5 con otros paquetes adicionales para el buen funcionamiento del aplicativo dadoradius. Como ejemplo se observa la figura 2.10.


```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/otto/Descargas# apt-get install php5 php5-mysql php-pear php5-
gd php-DB
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
php5 ya está en su versión más reciente.
Paquetes sugeridos:
  php5-dev
Se instalarán los siguientes paquetes NUEVOS:
  php-db php-pear php5-gd php5-mysql
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 439 kB de archivos.
Se utilizarán 3.040 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://ftp.us.debian.org/debian/ jessie/main php-pear all 5.6.24+dfsg-0+de
b8u1 [268 kB]
Des:2 http://ftp.us.debian.org/debian/ jessie/main php-db all 1.7.14-3 [73,0 kB]
Des:3 http://ftp.us.debian.org/debian/ jessie/main php5-gd i386 5.6.24+dfsg-0+de
b8u1 [29,6 kB]
Des:4 http://ftp.us.debian.org/debian/ jessie/main php5-mysql i386 5.6.24+dfsg-0
+deb8u1 [68,1 kB]
Descargados 439 kB en 1s (391 kB/s)
Seleccionando el paquete php-pear previamente no seleccionado.
(Leyendo la base de datos ... 135161 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar .../php-pear_5.6.24+dfsg-0+deb8u1_all.deb ...
Desempaquetando php-pear (5.6.24+dfsg-0+deb8u1) ...
Seleccionando el paquete php-db previamente no seleccionado.
Preparando para desempaquetar .../php-db_1.7.14-3_all.deb ...
Desempaquetando php-db (1.7.14-3) ...
Seleccionando el paquete php5-gd previamente no seleccionado.
Preparando para desempaquetar .../php5-gd_5.6.24+dfsg-0+deb8u1_i386.deb ...

```

Figura 2.10: Instalación de PHP5.

2.2.5 Instalación de FreeRadius

Luego de haber instalado la base de datos con su respectivo lenguaje procedemos a instalar FreeRadius, para lo cual colocamos la siguiente línea de comandos en la terminal:

```
#apt-get install freeradius freeradius-mysql
```

El inicio de la instalación de freeradius se puede observar en la figura 2.11.

```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/otto# apt-get install freeradius freeradius-mysql
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  freeradius-common freeradius-utils libfreeradius2
Paquetes sugeridos:
  freeradius-ldap freeradius-postgresql freeradius-krb5
Se instalarán los siguientes paquetes NUEVOS:
  freeradius freeradius-common freeradius-mysql freeradius-utils
  libfreeradius2
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.040 kB de archivos.
Se utilizarán 3.544 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://ftp.us.debian.org/debian/ jessie/main libfreeradius2 i386 2.2.5+dfsg-0.2 [112 kB]
Des:2 http://ftp.us.debian.org/debian/ jessie/main freeradius-common all 2.2.5+dfsg-0.2 [227 kB]
Des:3 http://ftp.us.debian.org/debian/ jessie/main freeradius i386 2.2.5+dfsg-0.2 [582 kB]
Des:4 http://ftp.us.debian.org/debian/ jessie/main freeradius-mysql i386 2.2.5+dfsg-0.2 [36,7 kB]
Des:5 http://ftp.us.debian.org/debian/ jessie/main freeradius-utils i386 2.2.5+dfsg-0.2 [82,0 kB]
Descargados 1.040 kB en 1s (775 kB/s)
Seleccionando el paquete libfreeradius2 previamente no seleccionado.
(Leyendo la base de datos ... 134585 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libfreeradius2_2.2.5+dfsg-0.2_i386.deb ...
Desempaquetando libfreeradius2 (2.2.5+dfsg-0.2) ...
Seleccionando el paquete freeradius-common previamente no seleccionado.

```

Figura 2.11: Instalación de Freeradius.

Concluida la instalación de FreeRadius se procede a autenticar los usuarios contenidos en una base de datos, en este caso MySQL, que fue la que se instaló con anterioridad. Para esto se procede a editar el fichero `radiusd.conf` accediendo a la siguiente ruta: `#/etc/freeradius/radiusd.conf`.

Para editar el fichero mencionado utilizamos el comando:

```
#nano radiusd.conf
```

En este fichero se elimina el comentario a la línea `$INCLUDE sql.conf`. El fichero `radiusd.conf` se puede apreciar en la figura 2.12.

```

otto@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
#
# As of 2.0.5, most of the module configurations are in a
# sub-directory.  Files matching the regex /[a-zA-Z0-9_]+/
# are loaded.  The modules are initialized ONLY if they are
# referenced in a processing section, such as authorize,
# authenticate, accounting, pre/post-proxy, etc.
#
$INCLUDE ${confdir}/modules/

# Extensible Authentication Protocol
#
# For all EAP related authentications.
# 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 separate (GDBM) databases of
# accounting info for each counter, this module uses the data
# stored in the raddacct table by the sql modules.  This
# module NEVER does any database INSERTs or UPDATEs.  It is
# totally dependent on the SQL module to process Accounting
# packets.
#

```

Figura 2.12: Configuración del archivo radiusd. cont

Ahora ingresamos en MySQL con el usuario root que se creó en la instalación, por medio de la siguiente línea de comandos:

```
#mysql -u root -p
```

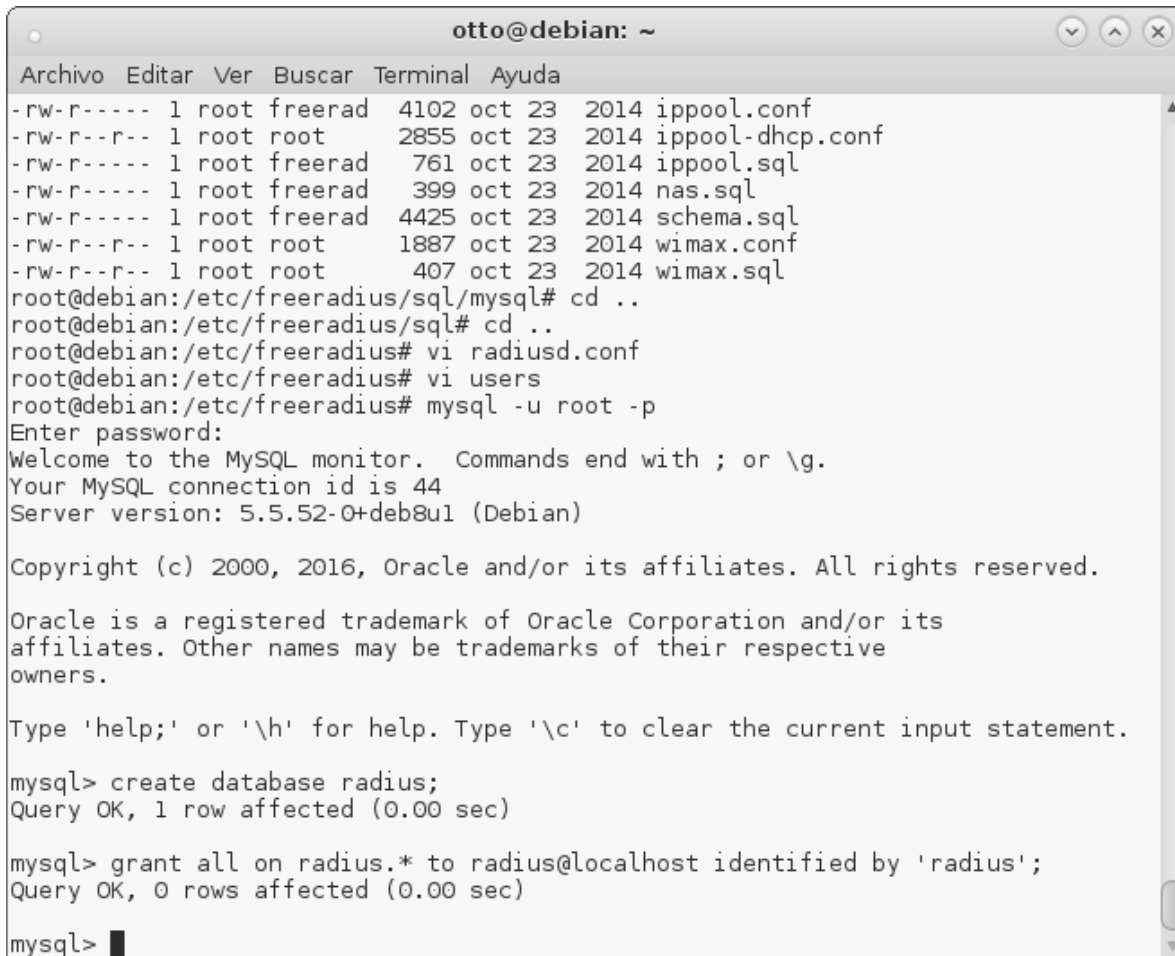
Dentro de MySQL se procede a crear la base de datos con el nombre radius y el usuario radius con la siguiente línea de comandos:

```
mysql> create databases radius;
```

Con el comando grant all se otorgan todos los permisos a dicha base de datos:

```
mysql> grant all on radius.* to radius@localhost identified by 'radius';
```

Se puede apreciar los comandos mencionados para crear la base de datos con su respectivo nombre, usuario y otorgando todos los permisos en la figura 2.13.



```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
-rw-r----- 1 root freerad 4102 oct 23 2014 ippool.conf
-rw-r--r-- 1 root root 2855 oct 23 2014 ippool-dhcp.conf
-rw-r----- 1 root freerad 761 oct 23 2014 ippool.sql
-rw-r----- 1 root freerad 399 oct 23 2014 nas.sql
-rw-r----- 1 root freerad 4425 oct 23 2014 schema.sql
-rw-r--r-- 1 root root 1887 oct 23 2014 wimax.conf
-rw-r--r-- 1 root root 407 oct 23 2014 wimax.sql
root@debian:/etc/freeradius/sql/mysql# cd ..
root@debian:/etc/freeradius/sql# cd ..
root@debian:/etc/freeradius# vi radiusd.conf
root@debian:/etc/freeradius# vi users
root@debian:/etc/freeradius# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 5.5.52-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, 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> create database radius;
Query OK, 1 row affected (0.00 sec)

mysql> grant all on radius.* to radius@localhost identified by 'radius';
Query OK, 0 rows affected (0.00 sec)

mysql> █

```

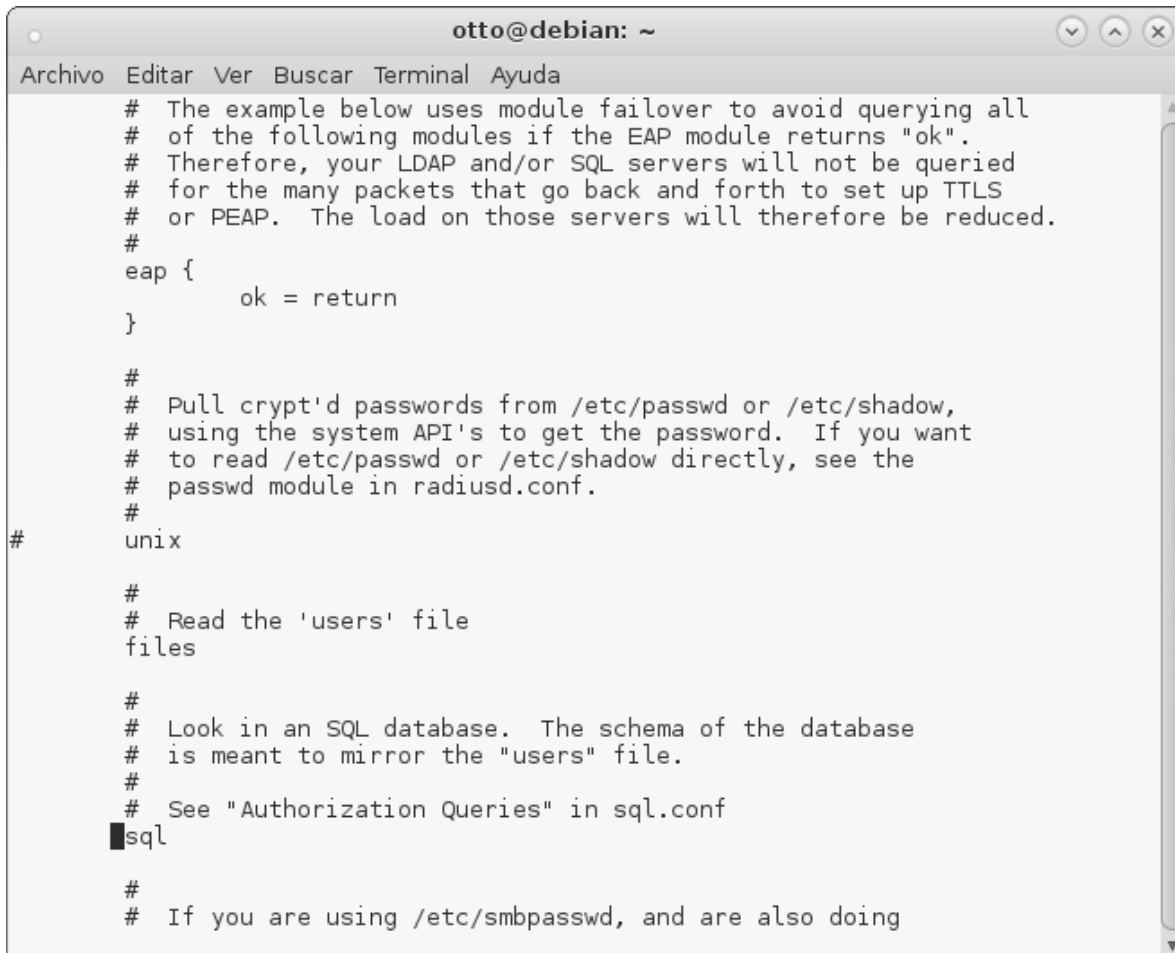
Figura 2.13: Creación de la base de datos radius.

Habiendo llegado a esta instancia, se sale de MySQL y se ubica nuevamente al directorio `/etc/freeradius` para editar el fichero `sites-available/default`. Para esto utilizamos los siguientes comandos:

```
#cd /etc/freeradius
```

```
#nano sites-available/default
```

Buscamos las secciones authorize y accounting para quitar comentarios donde aparezca la palabra sql, como se indica en la figura 2.14 y figura 2.15 respectivamente.

A screenshot of a terminal window titled "otto@debian: ~". The window contains configuration text for a default file. The text includes comments and code blocks for EAP, password retrieval, and SQL database lookups. A cursor is visible at the end of the "sql" line.

```
otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
# The example below uses module failover to avoid querying all
# of the following modules if the EAP module returns "ok".
# Therefore, your LDAP and/or SQL servers will not be queried
# for the many packets that go back and forth to set up TTLS
# or PEAP. The load on those servers will therefore be reduced.
#
eap {
    ok = return
}

#
# Pull crypt'd passwords from /etc/passwd or /etc/shadow,
# using the system API's to get the password. If you want
# to read /etc/passwd or /etc/shadow directly, see the
# passwd module in radiusd.conf.
#
#
# unix

#
# Read the 'users' file
files

#
# Look in an SQL database. The schema of the database
# is meant to mirror the "users" file.
#
# See "Authorization Queries" in sql.conf
# sql

#
# If you are using /etc/smbpasswd, and are also doing
```

Figura 2.14: Configuración del archivo default.

```

otto@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
# Note that accounting requests which are proxied
# are also logged in the detail file.
detail
#
daily

# Update the wtmp file
#
# 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

#
# If you receive stop packets with zero session length,
# they will NOT be logged in the database. The SQL module
# will print a message (only in debugging mode), and will

```

Figura 2.15: Configuración del archivo default.

Se ingresa a la base de datos radius de MySql por medio de la siguiente línea de comandos:

```
#mysql -u root -p radius;
```

Utilizando el comando describe para que muestre los campos que contiene la tabla radcheck:

```
mysql> describe radcheck
```

Se muestra la forma en la que se ingresaron las líneas de comando mencionadas, a continuación en la figura 2.16.

```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/freeradius# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 46
Server version: 5.5.52-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, 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> use radius
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> describe radcheck;
+-----+-----+-----+-----+-----+-----+
| Field      | Type                | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id         | int(11) unsigned   | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)        | NO   | MUL |         |                |
| attribute  | varchar(64)        | NO   |     |         |                |
| op        | char(2)            | NO   |     | ==      |                |
| value     | varchar(253)       | NO   |     |         |                |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql> █

```

Figura 2.16: Descripción de la tabla radcheck.

Se edita el archivo `sql.conf` y quitar comentarios en `readclients=yes`. Luego de haber editado el archivo `sql.conf` nos dirigimos al directorio `/etc/freeradius/sql/mysql` para verificar dos ficheros y accediendo a la base de datos radius por medio de `#mysql -u root -p radius`, ejecutamos los scripts que se encuentran en el directorio `mysql` que son `ippool.sql` y `nas.sql` mediante los siguientes comandos:

```
mysql> source ippool.sql;
```

```
mysql> source nas.sql;
```

Con las líneas ejecutadas anteriormente se generaron una serie de tablas, en la que está la tabla nas, en la cual se ingresarán los clientes remotos. Los campos que se ingresarán son:

- nasname: Dirección ip del cliente remoto
- shortname: Nombre con el que se identificara al cliente remoto.
- type: Se recomienda utilizar other.
- secret: Clave secreta que compartirán servidor y cliente. Este es el password que se configuro para el usuario radius de la base de datos radius y en el fichero sql.conf.

2.2.6 Instalación de DaloRadius

DaloRadius posee una interface de administración GUI, la cual podemos descargar la versión más reciente colocando la siguiente línea de comando:

```
#wget  
http://softlayer.dl.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-8/daloradius-0.9-8.tar.gz
```

Luego de haber descargado el archivo procedemos a descomprimirlo utilizando el comando tar xvzf de la siguiente manera:

```
#tar xvz daloradius-0.9-8.tar.gz
```

El archivo que ha sido descomprimido debe ser copiado al directorio de publicación del servidor web. El directorio por defecto es: /var/www/. Por lo tanto escribimos la siguiente línea de comandos:

```
#cp -R daloradius-0.9-8 /var/www/daloradius
```

Para el buen funcionamiento de la aplicación es necesario instalar algunas librerías, como se describe en la siguiente línea de comandos:

```
#apt-get install php5 php5-mysql php-pear php5-gd php-DB
```


Ahora se procede a cambiar los permisos y propiedades del directorio daloradius y los permisos del archivo, como se indica respectivamente en las siguientes líneas de comando:

```
#chown www-data:www-data /var/www/daloradius/ -R
```

```
#chmod 644 /var/www/daloradius/library/daloradius.conf.php
```

Se debe editar el archivo daloradius.conf.php para poner los valores de la conexión al servidor de la base de datos:

Se reinicia el servidor apache, por medio de la siguiente línea de comandos:

```
# /etc/init.d/apache2 restart
```

Luego de haber reiniciado el servidor apache, se accede a la GUI colocando el siguiente enlace en el navegador: <https://localhost/daloradius/login.php>. En la figura 2.17 se puede observar la pantalla de login de daloradius.

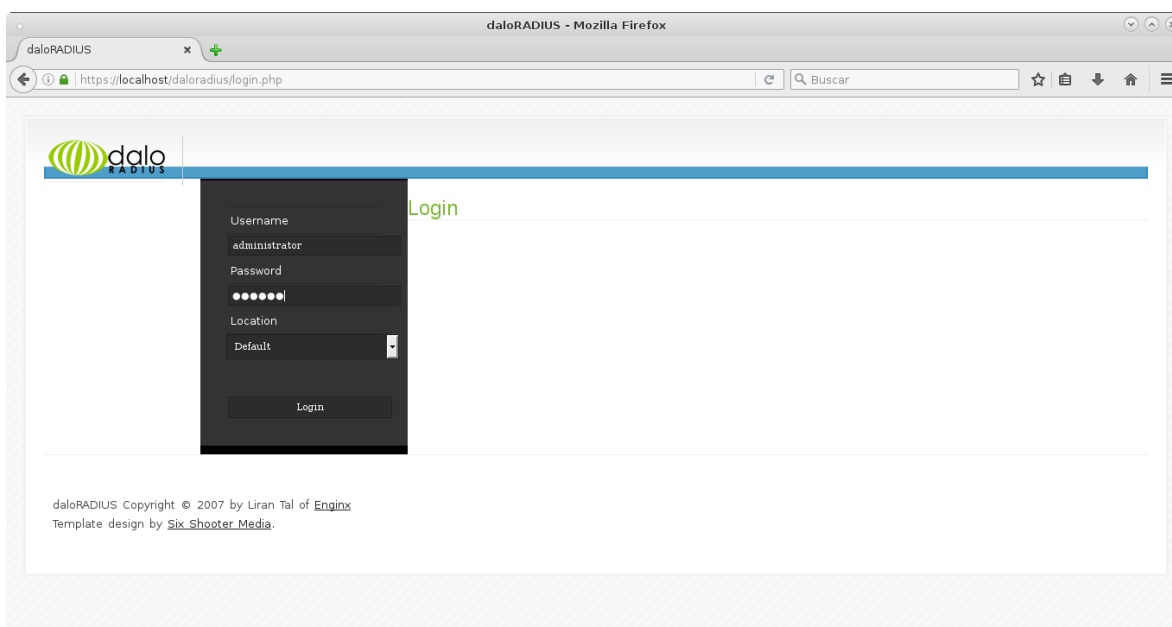


Figura 2.17: Login del aplicativo administrador.

Aquí se muestra la pantalla inicial de la aplicación, luego de haber ingresado con el respectivo username y password creado, como se muestra en la figura 2.18.

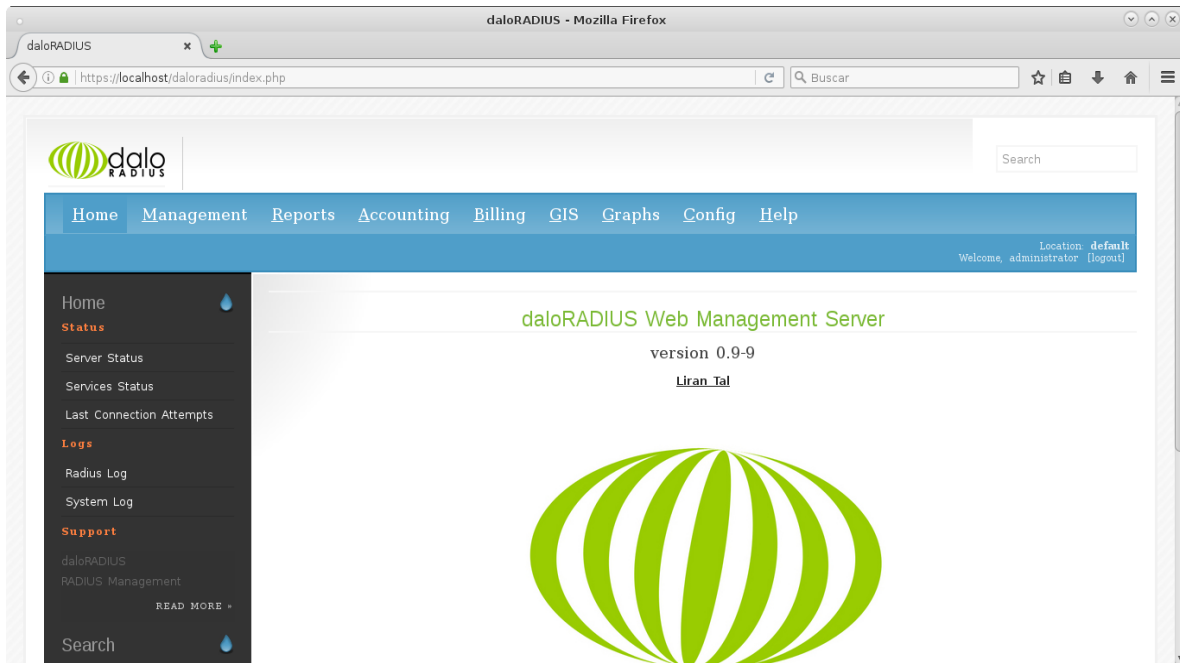


Figura 2.18: Home del aplicativo administrador.

2.3 Instalación del hardware

2.3.1 Configuración del router inalámbrico

Dentro de lo que es el acceso de forma inalámbrica para el servidor se configuraron los parámetros como el SSID que es el nombre de la red inalámbrica, la región y selección de canal de forma automática, lo cual es muy ventajoso utilizarlo en el caso de que el canal predeterminado se encuentre ocupado y pueda seleccionar uno que esté libre. Como se puede apreciar en la figura 2.19.

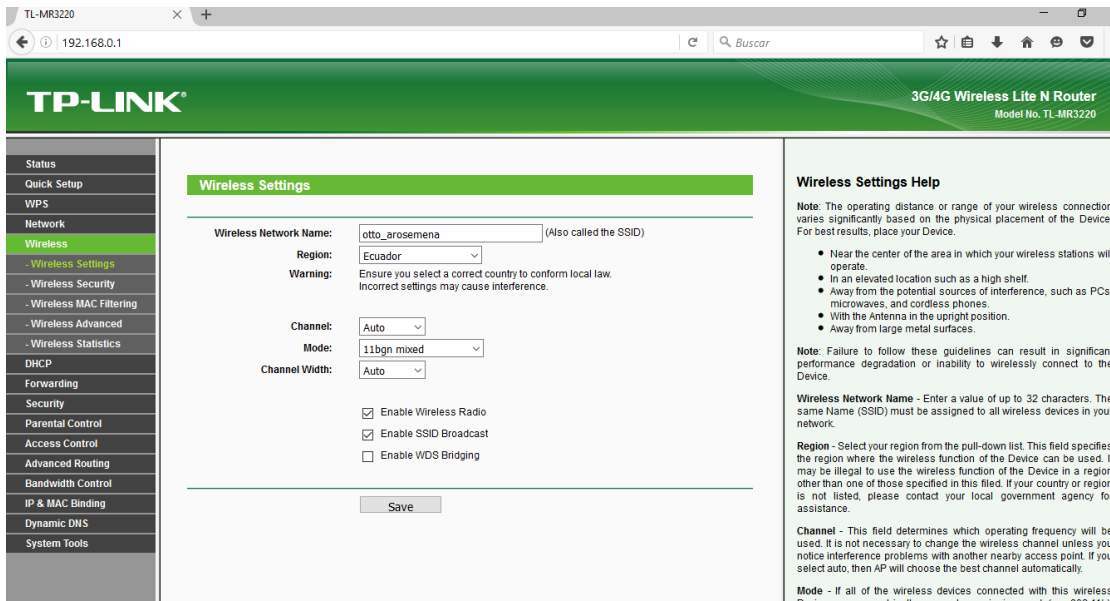


Figura 2.19: Configuración del router inalámbrico.

Con respecto a la seguridad inalámbrica trabajamos con WPA2 que es un protocolo más robusto que otros como por ejemplo WEP. La ventaja que tiene este protocolo es que soporta hasta 63 caracteres alfanuméricos, con lo cual podremos lograr una clave más segura y además el sistema va generando nuevas claves que transmite al resto de equipos lo cual dificulta la acción de descifrado por medio de alguna herramienta como un sniffer.

Se asignó una dirección IP para el servidor, el puerto con el que trabaja Radius que es 1812 para establecer conectividad con el servidor FreeRadius y la respectiva contraseña para la red la cual se recomienda alternar números y letras para que así la misma sea robusta. Los parámetros que se ajustaron se muestran en la figura 2.20.

The screenshot shows the configuration interface for a TP-LINK 3G/4G Wireless Life N Router (Model No. TL-MR3220). The page is titled "TP-LINK 3G/4G Wireless Life N Router Model No. TL-MR3220". The left sidebar contains a navigation menu with options: Status, Quick Setup, WPS, Network, Wireless (highlighted), Wireless Settings, Wireless Security (highlighted), Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, and System Tools.

The main content area is divided into three sections:

- WPA/WPA2 - Personal(Recommended)**: This section is currently unselected. It includes fields for Version (Automatic(Recommended)), Encryption (Automatic(Recommended)), Password, and Group Key Update Period (0 seconds).
- WPA/WPA2 - Enterprise**: This section is selected and highlighted with a red border. It includes fields for Version (Automatic), Encryption (Automatic), Radius Server IP (192.168.10.1), Radius Port (1812), Radius Password (aro123otto), and Group Key Update Period (30 seconds).
- WEP**: This section is unselected. It includes fields for Type (Automatic), WEP Key Format (Hexadecimal), and a table for WEP keys:

Key Selected	WEP Key (Password)	Key Type
Key 1: <input type="radio"/>	<input type="text"/>	Disabled
Key 2: <input type="radio"/>	<input type="text"/>	Disabled

On the right side, there is a "Wireless Security Help" section with the following content:

Wireless Security Help
You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA/WPA2 - Personal** - Select WPA based on pre-shared passphrase.
- **WPA/WPA2 - Enterprise** - Select WPA based on Radius Server.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described follows.

WPA/WPA2 - Personal
Version - You can select one of following versions,

- **Automatic** - Select WPA-Personal or WPA2-Personal automatically based on the wireless station's capability and request.
- **WPA-Personal** - Pre-shared key of WPA.
- **WPA2-Personal** - Pre-shared key of WPA2.

Encryption - You can select either **Automatic**, or **TKIP** or **AES**.

Password - You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Figura 2.20: Configuración del router inalámbrico.

CAPÍTULO 3

3. PRUEBAS Y RESULTADOS

Finalizada la implementación del servidor, con cada uno de los servicios configurados; ahora hacemos las pruebas necesarias para el correcto funcionamiento del sistema de seguridad en la red inalámbrica. Para probar la autenticación de usuarios con acceso a la red inalámbrica, se procederá a realizar dos pruebas prácticas

3.1 Primera prueba

En esta primera prueba se verifica la comunicación que existe entre el servidor radius y el servidor de base de datos MySQL; en primera instancia se inserta un usuario en la base de datos radius, para ello se ingresa en la base mediante la terminal, la tabla donde se ingresa al usuario es en “radcheck”, los campos que se afectan con la inserción del usuario son los siguientes:

- **username:** luiggy
- **attribute:** password
- **op:** ==
- **value:** luiggy123

Ingresar al gestor de base de datos mediante el siguiente comando:

```
#mysql -u root -p radius
```

Ingresar la contraseña root que se configuró en la instalación de MySQL.

Insertar el usuario en la tabla radcheck mediante el siguiente comando:

- `mysql> INSERT INTO radcheck(username, attribute, op, value)`
- `VALUES('luiggy', 'password', '==', 'luiggy123');`
- Salir de la base con el comando exit. Como ejemplo se observa en la figura 3.21.

```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> describe radcheck;
+-----+-----+-----+-----+-----+-----+
| Field      | Type                | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id         | int(11) unsigned    | NO   | PRI | NULL     | auto_increment |
| username   | varchar(64)         | NO   | MUL |          |                |
| attribute  | varchar(64)         | NO   |     |          |                |
| op         | char(2)             | NO   |     | ==       |                |
| value      | varchar(253)        | NO   |     |          |                |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql> INSERT INTO radcheck(username,attribute,op,value)
-> VALUES('luiggy','password','==','luiggy123');
Query OK, 1 row affected (0.04 sec)

mysql> exit
Bye

```

Figura 3.21: Registro del usuario.

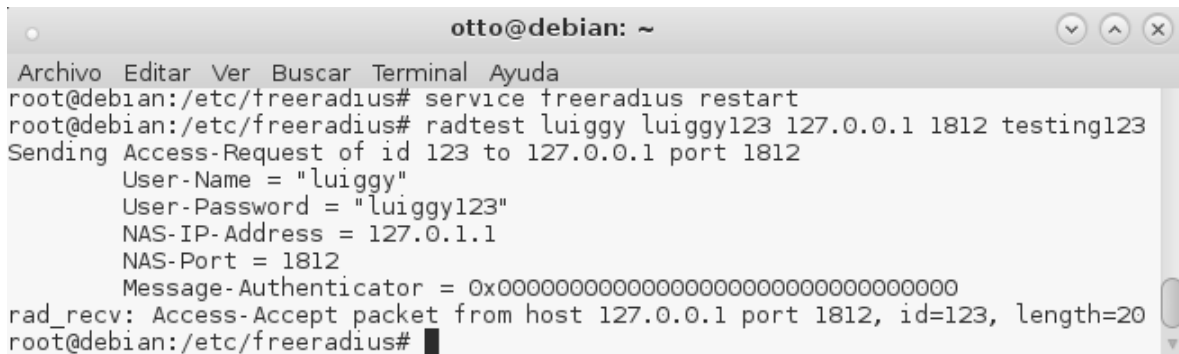
Antes de hacer la prueba de autenticación del usuario, se reinicia los servicios del freeradius con el siguiente comando:

```
#service freeradius restart
```

Para comprobar que el usuario creado en el apartado anterior está funcionando correctamente, se inserta la siguiente línea de comando como verificación:

```
#radtest luiggy luiggy123 127.0.0.1 1812 testing123
```

Con esto se verifica que el usuario ingresado en la base de datos fue autenticado correctamente por el servidor radius y además se comprueba que existe conexión entre la base de datos y el servidor freeradius. Como ejemplo se observa la figura 3.22.



```

otto@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/freeradius# service freeradius restart
root@debian:/etc/freeradius# radtest luiggy luiggy123 127.0.0.1 1812 testing123
Sending Access-Request of id 123 to 127.0.0.1 port 1812
  User-Name = "luiggy"
  User-Password = "luiggy123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=123, length=20
root@debian:/etc/freeradius#

```

Figura 3.22: Autenticación exitosa del usuario.

3.2 Segunda prueba

En esta segunda prueba se pone en consideración al aplicativo daloradius, que para el proyecto servirá como ingreso de los usuarios a la base de datos del servidor; además se considera al router TP-LINK TL-MR3220 como nexo de comunicación entre el usuario y el servidor radius.

Para la prueba se toma en cuenta al laboratorio de computación donde sus máquinas poseen tarjetas de red inalámbrica, dado que estas máquinas son las que tendrán prioridad por el momento. A su vez se configura la red inalámbrica que se presentará en las redes disponibles, para esto nos ubicamos en la señal inalámbrica de la máquina, dar clic derecho y Abrir el Centro de redes y recursos compartidos. Ver el ejemplo de la figura 3.23.

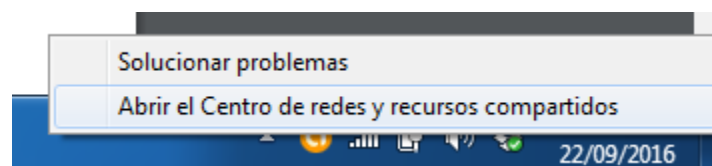


Figura 3.23: Configuración de la red inalámbrica.

Se escoge la opción Administrar redes inalámbricas, ver figura 3.24.

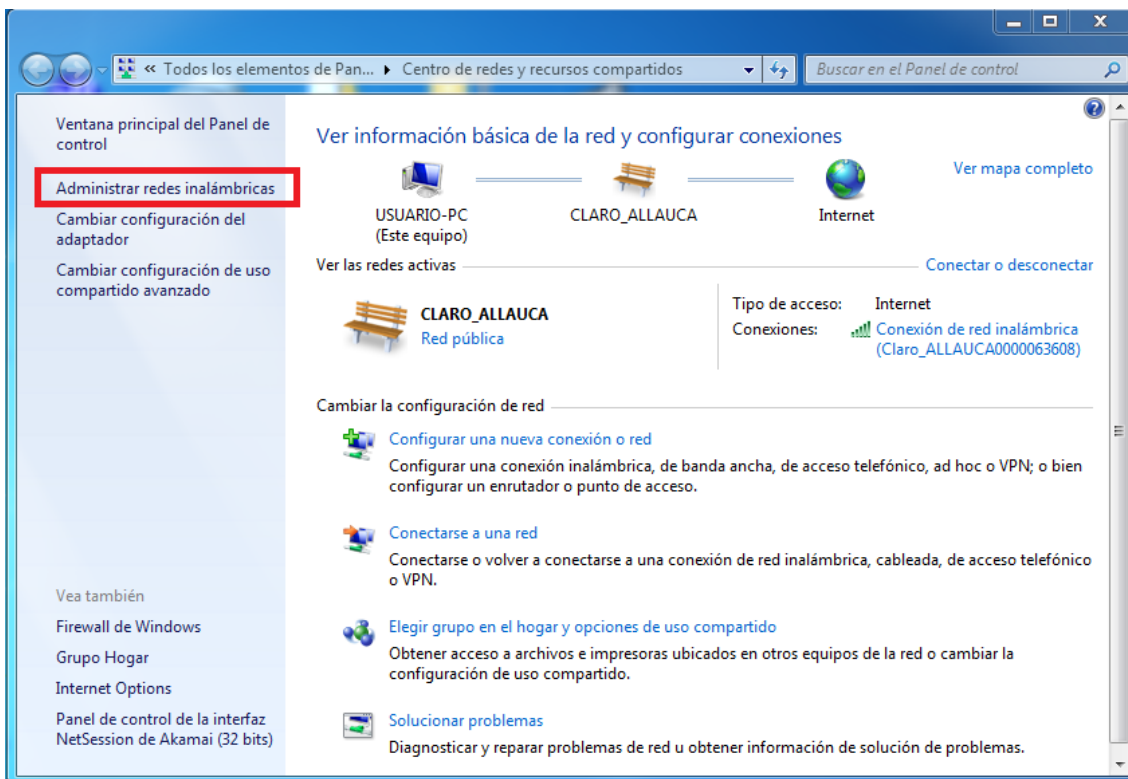


Figura 3.24: Configuración de la red inalámbrica.

Se procederá agregar un nuevo perfil de usuario para la red inalámbrica que se desea ingresar, se da clic en Agregar. Ver figura 3.25.

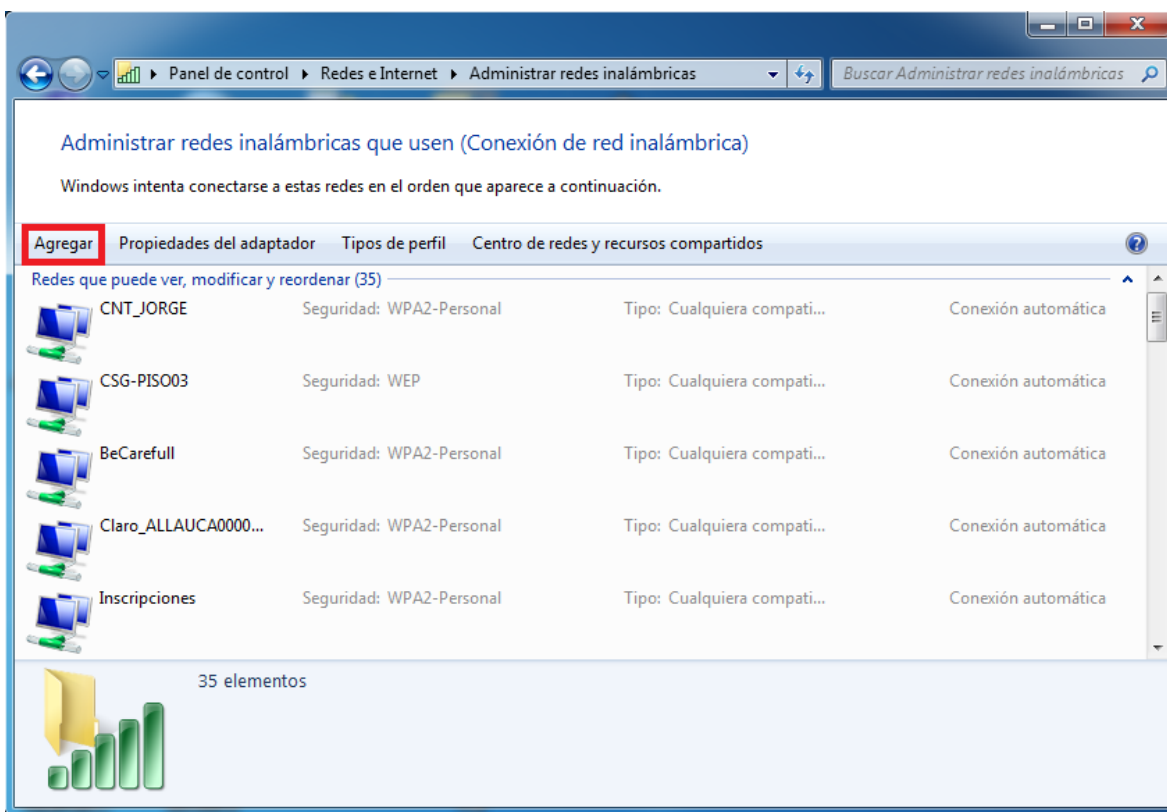


Figura 3.25: Ingreso de la red inalámbrica.

Luego de esto se ingresará a Crear un perfil de red manualmente. Se ingresa información de la red inalámbrica que se desea agregar manualmente; como ejemplo se observa la figura 3.26, establecemos lo siguiente:

- **Nombre de la red:** otto_rosemena
- **Tipo de seguridad:** WPA-Enterprise
- **Tipo de cifrado:** TKIP

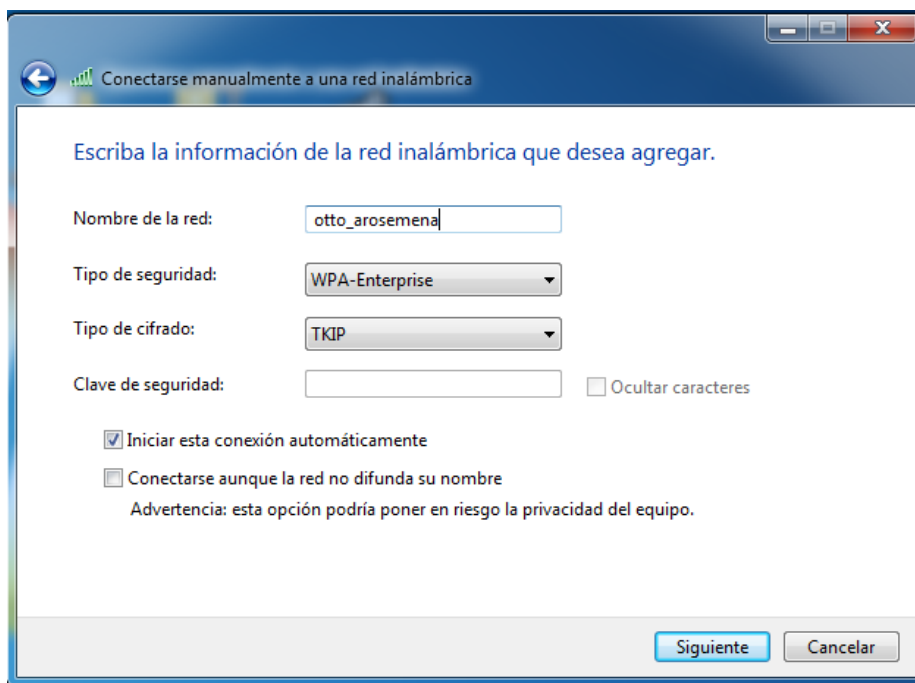


Figura 3.26: Información de la red inalámbrica.

Dar clic derecho en la red creada manualmente y ubicarse en propiedades, luego de esto se da clic en seguridad y es aquí donde se ingresa a Configuración avanzada. Ver figura 3.27.

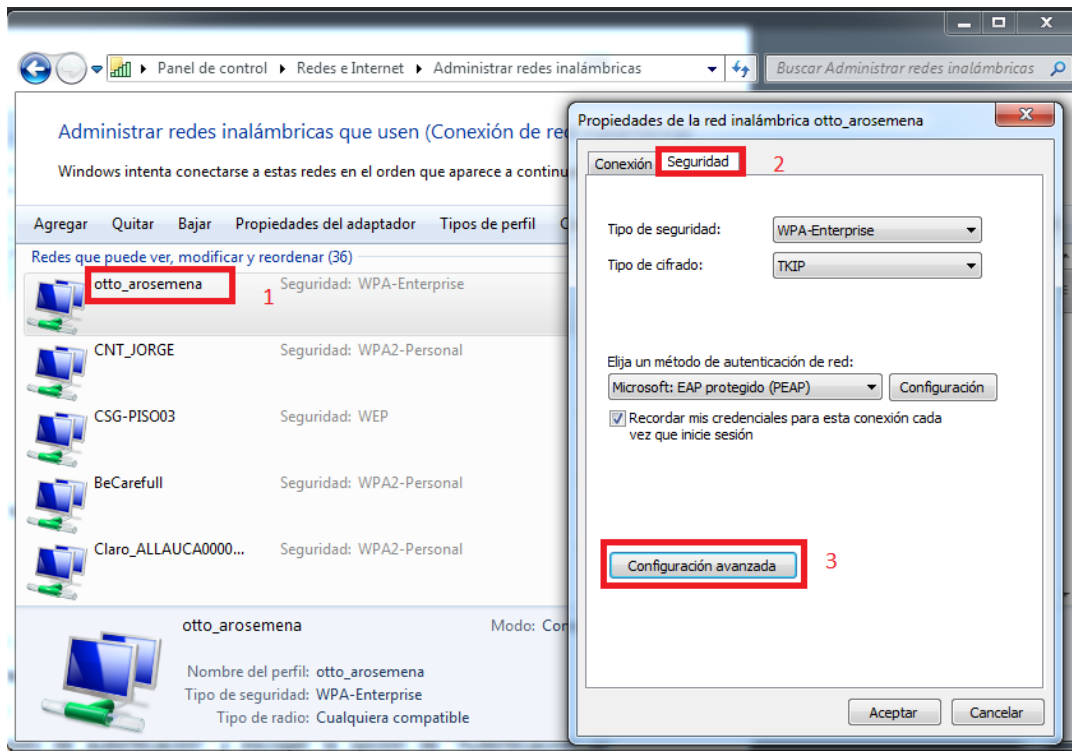


Figura 3.27: Configuración de la seguridad en la red.

Dentro de configuración avanzada se especifica el modo de autenticación, en este caso será Autenticación de usuarios y luego dar clic en aceptar, ver figura 3.28. Con la configuración que se tiene se obliga al usuario a ingresar su user y password de la cual fue asignado mediante el aplicativo daloradius.

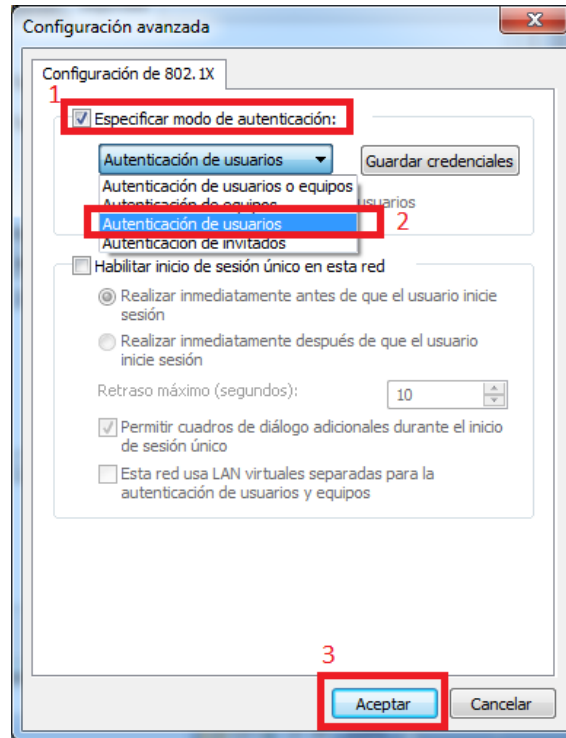


Figura 3.28: Especificación del modo de autenticación.

Habiendo terminado el modo de autenticación de usuarios se procede a aceptar todos los cambios efectuados en la configuración, ahora verificamos que nuestra red inalámbrica se esté habilitada y conectada con nuestro router TP-LINK TL-MR3220. Ver figura 3.29.

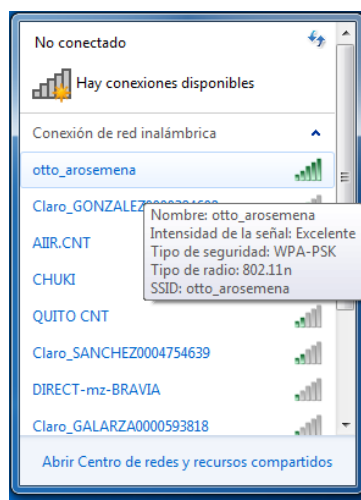


Figura 3.29: Habilitación de la red inalámbrica otto_rosemena.

Con nuestra red inalámbrica habilitada para acceder a internet, ingresamos al aplicativo administrador daloRADIUS; aquí ingresaremos nuestros usuarios para que tengan acceso a la red inalámbrica del colegio, nos dirigimos a nuestro navegador web ingresando la dirección localhost/daloradius, nos mostrará el login con el cual ingresaremos el user y password.

Luego se ingresa el nombre del usuario en la opción Management y clic en New User – Quick Add, se mostrará el ingreso de información del usuario y para finalizar se da clic en Apply. Ver el ejemplo de la figura 3.30.

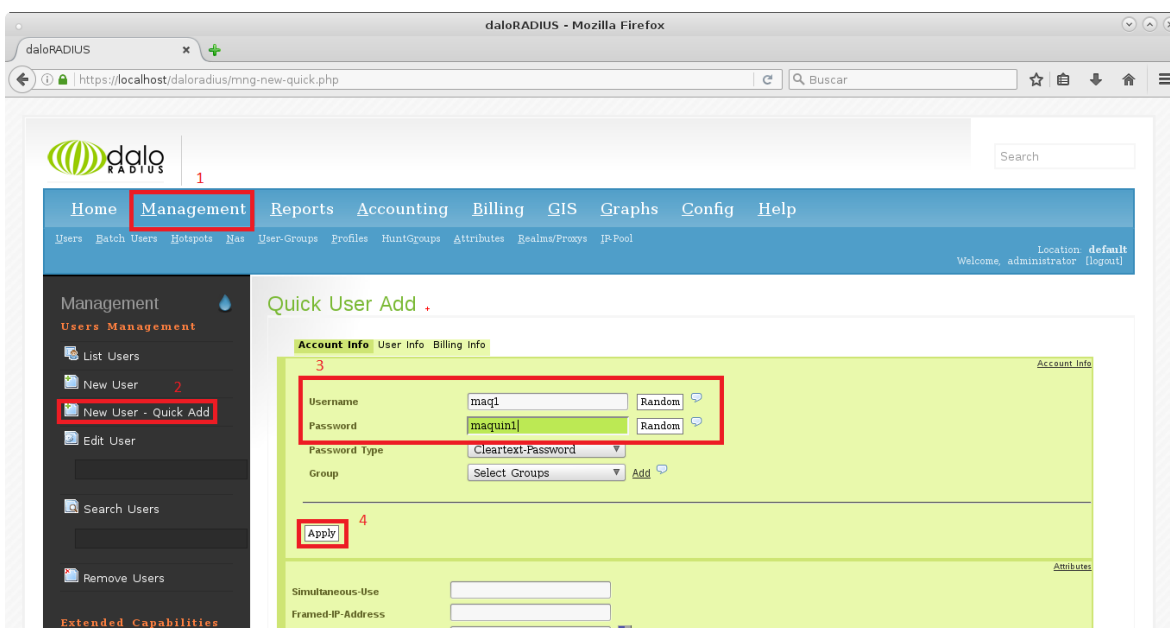
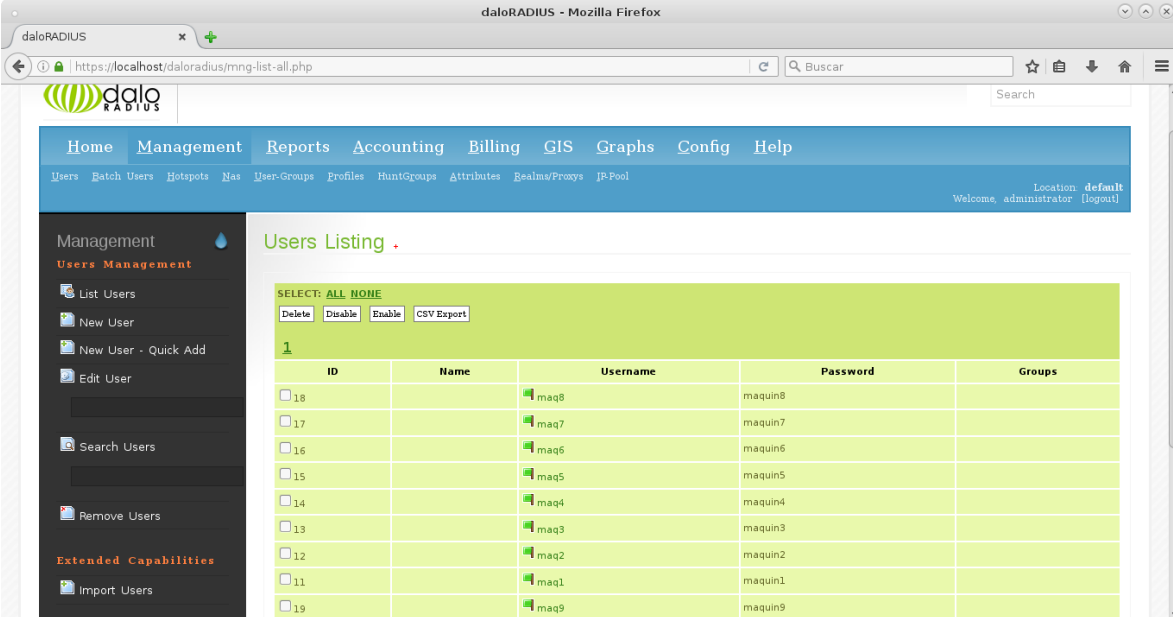


Figura 3.30: Registro del usuario.

Se ingresa la información de todos los usuarios que se autentican en la red inalámbrica del colegio; todos estos usuarios estarán permitidos de acceder la red wifi con acceso a internet. Como ejemplo se observa la figura 3.31.



The screenshot shows the daloRADIUS web interface in a Mozilla Firefox browser. The page title is "daloRADIUS" and the URL is "https://localhost/daloradius/mng-list-all.php". The interface features a navigation menu with options like Home, Management, Reports, Accounting, Billing, GIS, Graphs, Config, and Help. A search bar is located in the top right corner. The main content area is titled "Users Listing" and displays a table of users. The table has columns for ID, Name, Username, Password, and Groups. The users listed are maq8 through maq9, with IDs 18 through 19. The interface also includes a sidebar with "Management" and "Users Management" options, and a top right corner with "Location default" and "Welcome, administrator (Logout)".

ID	Name	Username	Password	Groups
<input type="checkbox"/> 18		maq8	maquin8	
<input type="checkbox"/> 17		maq7	maquin7	
<input type="checkbox"/> 16		maq6	maquin6	
<input type="checkbox"/> 15		maq5	maquin5	
<input type="checkbox"/> 14		maq4	maquin4	
<input type="checkbox"/> 13		maq3	maquin3	
<input type="checkbox"/> 12		maq2	maquin2	
<input type="checkbox"/> 11		maq1	maquin1	
<input type="checkbox"/> 19		maq9	maquin9	

Figura 3.31: Listado de los usuarios habilitados.

Esta aplicación permite al administrador hacer un chequeo de la conectividad del usuario, tal como se muestra en la figura 3.32.

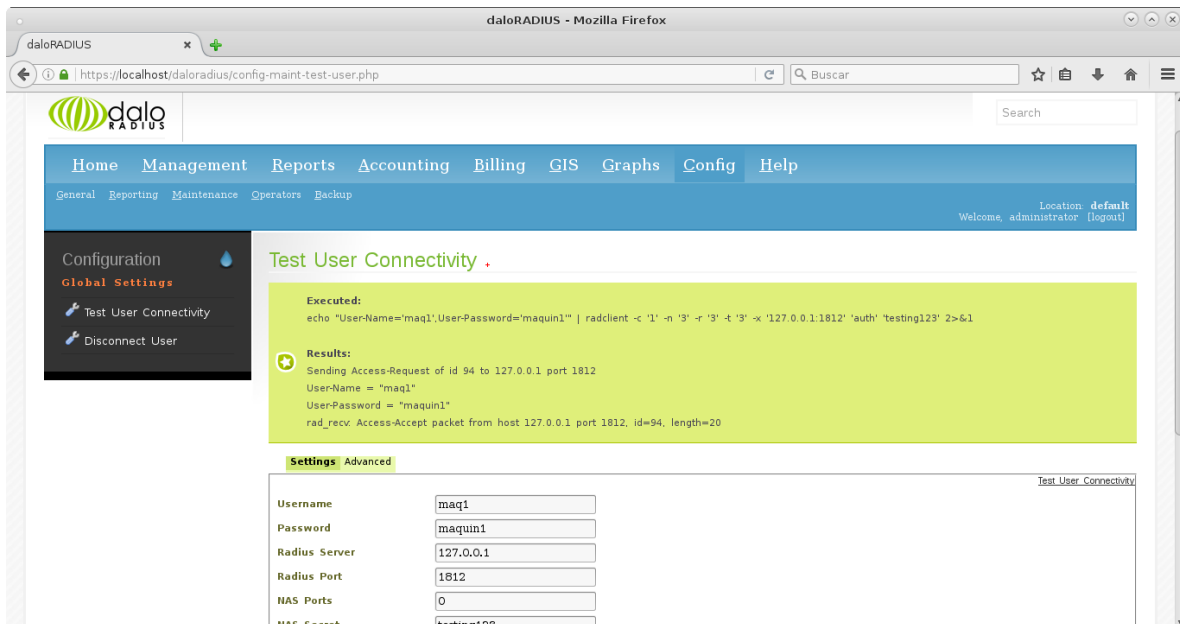


Figura 3.32: Testeo de conectividad del usuario.

Con los usuarios ingresados en el servidor, se procede a comprobar que los usuarios registrados en el aplicativo administrador se autenticuen en la red WI-FI otto_rosemena; para esto se selecciona la red WI-FI, luego de esto nos pedirá el ingreso del usuario y contraseña. Ver como ejemplo la figura 3.33.

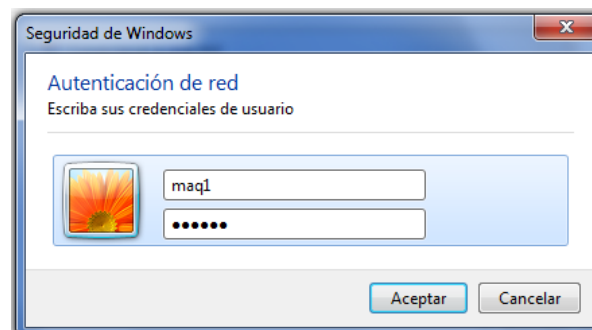


Figura 3.33: Autenticación del usuario.

La información enviada del usuario es captada por el servidor radius, realiza las validaciones del usuario que se autentica haciendo una petición en el servidor de la base de datos, ver el ejemplo de la figura 3.34. Si el usuario está dentro de la base enviará al servidor radius una respuesta de Access-Accept caso contrario si el usuario no ha sido ingresado por el aplicativo administrador no permitirá el acceso a la red.

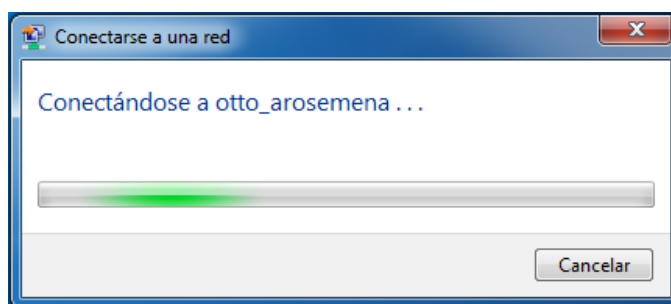


Figura 3.34: Conexión a la red inalámbrica otto_rosemena.

CONCLUSIONES Y RECOMENDACIONES

Se implementó un sistema de seguridad bajo el esquema de un LAMP, que permite la comunicación entre cada uno de los elementos del servidor radius. Este sistema permitió que el consumo de la banda ancha de internet mejore en un 80% de su capacidad; con esta mejora en el consumo de internet, se cuenta con un ambiente de conexión segura y eficiente para el acceso de cada uno de los usuarios dentro de la red inalámbrica del colegio Otto Arosemena Gómez.

Se desarrolló un sistema de seguridad interactivo donde el cliente debe ser ingresado mediante el aplicativo administrador daloradius para tener acceso a la red WI-FI del colegio; luego de ser registrado, el usuario podrá contar con total acceso a la red inalámbrica y gozar de comunicación con el servidor de autenticación.

Se mejoró el proceso de autenticación de usuarios en la red WI-FI en un 95%, puesto que el colegio no contaba con ninguna restricción y seguridad para los usuarios que accedían a la red.

Se ejecutó el aplicativo administrador daloradius para tener un control total de los usuarios que acceden a la red mediante la autenticación, se pudo restringir el tiempo de conectividad del usuario visitante y se permitió total acceso a los estudiantes y docentes del colegio mediante cada una de las máquinas con tarjeta de red inalámbrica que posee el colegio en su laboratorio de computación.

Se instaló y configuró todos los servicios en un mismo servidor físico, cada uno de los servicios se ejecuta de forma conjunta y son mutuamente dependientes. Además se cuenta con comunicación entre software y hardware de manera en que el servidor se ejecute de manera eficiente y segura.

Se recomienda incluir un portal cautivo donde se ingresen los datos del usuario mediante una autenticación web, con esto se evitaría la configuración de la red inalámbrica de forma manual y se daría paso a la restricción del usuario sin privilegios. Existen algunos portales cautivos que facilitarían el acceso al usuario para una futura actualización del sistema de seguridad, un claro ejemplo de portales cautivos son chillispot y coovachilli.

El laboratorio de computación debe tener una apropiada climatización del lugar con aires acondicionados acordes con el laboratorio, puesto que se cuenta con un total de 35 máquinas que al prenderse generan un ambiente muy caluroso y poco amigable para el laboratorio. Además se recomienda una mejor iluminación del laboratorio con luces fluorescentes que permitan la visibilidad de la pizarra o de la proyección de alguna presentación.

Un servidor de seguridad debe estar debidamente protegido en un lugar donde solo pueda acceder el administrador de la red inalámbrica, para esto se sugiere instalarse en un lugar apartado de los laboratorios de computación, se recomienda instalar un rack o datacenter donde el servidor pueda contar con mayor seguridad.

Se sugiere la creación de contraseñas seguras para cada uno de los servicios que se establecen en el servidor, con caracteres alfanuméricos, mayúsculas y minúsculas. Esto servirá para una mejor seguridad al acceso del sistema; también se recomienda que solo el administrador de la red tenga el archivo con todas las claves generadas por los servicios levantados en el servidor.

BIBLIOGRAFÍA

- [1] J. M. Duart, "Internet y Aprendizaje: una estrecha relación," RUSC, vol. 3, no. 02, Octubre, 2006.
- [2] S. Barajas, "Protocolos de Seguridad en redes inalámbricas," Univ. Carlos III, Madrid, España, 2013.
- [3] A. Mendoza, A. Barraza, F. Estrada, C. Esquivel, D. Calderón, "Análisis del desempeño del protocolo RADIUS en redes inalámbricas," Culcyt, Juárez, México, Rep. 51, 2013.
- [4] D. Pontón, "Investigación del servidor Radius para la seguridad en redes LAN Inalámbricas" Tesis de Grado, Facd. Esc. Ing. Sist. Comp, Univ. Nacional de Chimborazo, Riobamba, Ecuador, 2011.
- [5] J. Prats. (2002). Internet en las aulas de educación secundaria [Online]. Disponible en: http://www.quadernsdigitals.net/datos/hemeroteca/r_1/nr_490/a_6671/6671.pdf.
- [6] J. Pilla, "Implementación de seguridad en la red interna de datos para el manejo adecuado de usuarios y acceso remoto en el Instituto tecnológico Pelileo" Tesis de Grado, Facd. Ing. Electr. Indust, Univ. Técnica de Ambato, Ambato, Ecuador, 2013.
- [7] E. Rosebrock y E. Filson, "Setting Up LAMP: Getting Linux, Apache, MySQL, and PHP Working Together," SYBEX, San Francisco, London, 2004.
- [8] R. Hertzog y R. Mas, "Debian Wheezy from Discovery to Mastery," en The Debian Administrator's Handbook, 1er ed., Ed. Eyrolles, 2015.