# UNIVERSIDAD TÉCNICA DE COTOPAXI

## FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

### CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

**"DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA"**

Proyecto de Titulación presentado previo a la obtención del Título de Ingeniero en Informática y Sistemas Computacionales


**AUTOR:**

Espinel Pilicita Jorge Santiago

**TUTOR:**

Ing. MSc. Jorge Bladimir Rubio Peñaherrera


**Latacunga – Ecuador**

**Julio - 2019**

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

## DECLARACIÓN DE AUTORÍA

Yo, **ESPINEL PILICITA JOGE SANTIAGO** declaro ser autor del presente proyecto de investigación: **"DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DE MEJÍA"**, siendo el Ing. MSc. Jorge Rubio tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

**Espinel Pilicita Jorge Santiago**

**C.I.:172317756-2**

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

## AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:

**"DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DE MEJÍA"**, de **ESPINEL PILICITA JORGE SANTIAGO**, de la **CARRERA INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES**, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Julio, 2019

El Tutor
Ing. Jorge Bladimir Rubio
C.I: 050222229-2

Universidad Técnica de Cotopaxi

Ingeniería Informatica Y Sistemas Computacionales

## APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**; por cuanto, el postulante: **ESPINEL PILICITA JORGE SANTIAGO** con el título de Proyecto de titulación: **"DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DE MEJÍA"** ha considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

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

Latacunga, 22 de julio del 2019

Para constancia firman:

**Lector 1 (Presidente)**
**Ing. Villa Quishpe Manuel William**
**CC: 180338695-0**

**Lector 2**
**Ing. Murillo Calderón Félix Mauricio**
**CC: 180299840-9**

**Lector 3**
**Phd. Rodriguez Barcenas Gustavo**
**CC: 175700135-7**

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN MEJÍA
DIRECCIÓN ADMINISTRATIVA

# CERTIFICADO

Yo, **NARANJO QUINALUISA OSCAR PAUL** con cedula de identidad **171256066-1**, en calidad de Coordinador de Tics del GAD Municipal del cantón Mejía, certifico que el Sr. **ESPINEL PILICITA JORGE SANTIAGO**, con cedula de identidad **172317756-2**, egresado de la Universidad Técnica de Cotopaxi, de la Carrera de Ingeniería en Informática y Sistemas Computacionales, ha concluido satisfactoriamente el **DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA.** Dicho trabajo ha sido entregado y aprobado, sujeto a los parámetros establecidos al principio del mismo.

Es todo cuanto puedo certificar, autorizo al interesado hacer uso lícito del presente documento como lo estime conveniente.

Machachi, julio 2019

G.A.D. MUNICIPAL DEL CANTÓN MEJÍA
JEFATURA DE T.I.C.S.

ING. NARANJO QUINALUISA OSCAR PAUL
171256066-1
Coordinador de TICS

## AGRADECIMIENTO

Agradezco a Dios por bendecirme con vida y fortaleza para concluir con éxito mi formación académica.

A mi amada Madre por el apoyo infinito que me brinda, por confiar y nunca perder la fe en mí, por impulsarme a cada día ser mejor, por sus consejos, valores y principios inculcados.

A mis Hermanas Yolanda, Jaqueline, Aracelly les agradezco infinitamente por su apoyo incondicional, por estar en los momentos más duros de mi vida, quienes siempre me alentaron gritándome no te rindas falta poco.

De la misma manera mis agradecimiento a la Universidad Técnica de Cotopaxi, a toda la Facultad de Ciencias de la Ingeniería y Aplicadas, a mis docentes por trasmitir sus valiosos conocimientos, gracias a cada uno de ustedes por su dedicación, paciencia y amistad. De manera especial a mi tutor Ing. MSc Jorge Rubio, por haberme guiado y brindado su apoyo para desarrollarme profesionalmente.

**Santiago**

## DEDICATORIA

El presente trabajo de investigación lo dedico principalmente a Dios y la Virgen de Guadalupe, por bendecirme todas las mañanas, ser los guías de mi vida.

A mi Madre, por trazar una cruz en el aire con su mano siempre que salía con mi mochila llena de sueños, por su amor y sacrificio de todos estos años el cual floreció y dio fruto alcanzando el sueño de los dos. Es un orgullo tenerte como madre y un privilegio ser tu hijo, eres la mejor.

A mi Esposa e hija quienes llegaron a reforzar el apoyo. Adriana, por ayudarme a crecer por amarme ser mi confidente, cómplice, amiga, pero por sobre todo gracias por caminar a mi lado y confiar en mí. Najhary, el ser de luz que hace que mis días sean maravillosos con su sonrisa, con esos ojos de gato y sus palabritas de aliento fortalecen mi corazón.

A mis Hermanas, por estar presente siempre en mi vida, por el apoyo total que me brindan a lo largo de esta y todas las etapas de mi vida. Por sus consejos y palabras de aliento, por corregirme o apoyarme en mis decisiones algunas buenas, algunas malas y otras locas, son parte de este sueño cumplido son las hermanas perfectas.

**Santiago**

# ÍNDICE DE CONTENIDO

## ÍNDICE DE TABLAS



## ÍNDICE DE FIGURAS

# UNIVERSIDAD TECNICA DE COTOPAXI

**FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS**

**TITULO:** "Implementación de Seguridad A.A.A (Authentication authorization and accounting) en las redes Wi-Fi del GAD municipal del Cantón Mejía"

**Autor:** Espinel Pilicita Jorge Santiago

**RESUMEN**

Este proyecto fue propuesto para dar una solución de seguridad para el control de acceso con base a la infraestructura del GAD municipal del Cantón Mejía mediante la identidad basada en servicios de red la cual está basada en un servidor AAA (Authentication Authorization And Accounting / Autenticación Autorización y Contabilidad) utilizando el protocolo de libre uso RADIUS, este se encargara la autenticación, autorización y contabilidad o auditoria de las redes inalámbricas, debido a la filtración de contraseñas que se evidencio, cualquier persona podía tener acceso y las redes quedaban expuestas y vulnerables. Para lo cual aplicamos el método teórico practico para la abstracción y deducción de soluciones para realizar un análisis de las cualidades necesarias con las que debía contar el servidor AAA y ponerlas en práctica con un modelo experimental en el cual tenemos control de acceso de las redes inalámbricas lo que nos brinda seguridad en la red, ya que como es posible controlar el acceso a estas, fue posible resguarda y evitar el uso inadecuado de la información, ya implantado para los funcionarios de la institución el acceso es mediante credenciales de usuarios y filtros por MAC address del equipo, una vez ingresados tienen roles y perfiles para el desarrollo de su actividad laboral. Formándose el concepto de servidor AAA, ya que este modelo ofrece alternativas de protección en el acceso de una red, a pesar de la existencia de muchas alternativas que cumplen esta función, un servidor AAA cuenta con las condiciones necesarias para cumplir este objetivo, el fin era implementar un servidor con estas características utilizando software libre para el servidor fue un sistema operativo centOS 7 y FreeRadius para los servicios RADIUS con un panel de control web y un equipo wireless lan controller, todo esto nos brindó nuevas alternativas de acceso a la red inalámbrica, beneficiando no solo a los funcionarios sino a la comunidad en general, ofreciendo un ambiente más confiable en el GAD municipal del Cantón Mejía, El cual era el principal objetivo de este proyecto. El servidor Radius ofrece un control, monitoreo, y administración. Esto garantizo la seguridad en el acceso a las redes inalámbricas del GAD municipal del Cantón Mejía, mediante una interfaz gráfica que permite al administrador monitorear la red.

**Palabras claves:** servidor AAA, MAC address, RADIUS.

# TECHNICAL UNIVERSITY OF COTOPAXI

## FACULTY OF ENGINEERING AND APPLIED SCIENCES

**THEME:** "Implementation of Security A.A.A (Authentication authorization and accounting) in the Wi-Fi networks of the Decentralized Autonomous Government of "Mejía" Canton"

**Author:** Espinel Pilicita Jorge Santiago

## ABSTRACT

This project was proposed to give a security solution for access control with base to the infrastructure Decentralized Autonomous Government of the "Mejía" Canton by means of the identity based on network services which is based on an AAA (Authentication Authorization and Accounting) server. Using the RADIUS free use protocol will be responsible for the authentication, authorization and accounting of wireless networks, due to the filtering of passwords that was evidenced anybody could have access as well as the networks were exposed and vulnerable. To which we apply the practical theoretical method for the abstraction and deduction of solutions and execute an analysis of the necessary qualities that the AAA server should count and put them in practice with an experimental model in which we have access control of wireless networks that gives us security in the network, since as it is possible to control the access to these, it was possible to safeguard and prevent the inappropriate use of the information, already implemented for the institution's employees access is through user's credentials and filters by MAC address of the equipment, once the session is initiated roles and profiles for their work development. In this way the AAA server concept is formed, since this model offers alternative of protection in the network access, despite the existence of many alternatives that fulfill this function, an AAA server has the necessary conditions to fulfill this objective, the purpose was to implement a server with these features using free software for the server was an operating system centOS 7 and FreeRadius for RADIUS services with a web control panel and a wireless lan controller, all this gave us new alternatives to access the wireless network , benefiting not only the functionary but also the community in general, offering a more reliable environment in the DAG of the "Mejía" Canton, which was the main objective of this project. The Radius server offers control, monitoring, and administration. This assure the security of access to the wireless networks of the DAG of "Mejía" Canton, through a graphical interface that allows to the administrator monitors the network.

**Keywords:** AAA server, MAC address, RADIUS.

Universidad Técnica de Cotopaxi

CENTRO DE IDIOMAS

# *AVAL DE TRADUCCIÓN*

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen del proyecto de investigación al Idioma Inglés presentado por el señor Egresado de la Carrera de **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES** de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS, ESPINEL PILICITA JORGE SANTIAGO**, cuyo título versa **"IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimare conveniente.

Latacunga, Julio del 2019

Atentamente,

**LIC. MARÍA FERNANDA AGUAIZA**
**DOCENTE CENTRO DE IDIOMAS**
**C.C. 050345849-9**

CENTRO DE IDIOMAS

## 1. INFORMACIÓN GENERAL

**Título del proyecto:**

"Diseño e Implementación de Seguridad A.A.A (Authentication Authorization and Accounting) en las redes Wi-Fi del GAD municipal del Cantón Mejía"

**Fecha de inicio:** abril 2019

**Fecha de finalización:** agosto 2019

**Lugar de ejecución:**

Machachi – Cantón Mejía - Pichincha - Zona 2 - GAD municipal del Cantón Mejía

**Facultad que auspicia**

Facultad de Ciencias de la Ingeniería y Aplicas

**Carrera que auspicia:**

Carrera de Ingeniería en Informática y Sistemas Computaciones

**Equipo de Trabajo:**

Tutor de titulación

Ing. MSc. Jorge Bladimir Rubio

Coordinador del proyecto

Jorge Santiago Espinel Pilicita

**Área de Conocimiento:**

Seguridad Informática

**Línea de investigación:**

Tecnologías de la información y comunicación

**Sub líneas de investigación de la Carrera:**

Diseño, implementación, configuración de redes y seguridad computacional aplicando normas y estándares Internacionales

- Seguridad informática

## 2. RESUMEN DEL PROYECTO

Este proyecto propone dar una solución de seguridad para el control de acceso con base a la infraestructura del GAD municipal del Cantón Mejía mediante la identidad fundamentada en servicios de red la cual está basada en un servidor AAA (Authentication Authorization And Accounting / Autenticación Autorización y Contabilidad) utilizando el Protocolo AAA utilizado por RADIUS, este se encargará de la autenticación, autorización y auditoria de las redes inalámbricas, debido a las conexiones no autorizadas en la red. Para lo cual se aplicará el método teórico práctico para la abstracción y deducción de soluciones para realizar un análisis de las cualidades necesarias con las que debe contar el servidor AAA y ponerlas en práctica con un modelo experimental con el cual tengamos control de acceso de las redes inalámbricas lo que nos brinda seguridad en la red, lo cual hace posible resguardar y evitar el uso inadecuado de la información, a los funcionarios de la institución el acceso será mediante credenciales de usuarios, una vez ingresados tendrán perfiles para el desarrollo de su actividad laboral. Formándose el concepto de servidor AAA, ya que este modelo ofrece alternativas de protección en el acceso de una red, a pesar de la existencia de muchas alternativas que cumplen esta función, un servidor AAA cuenta con las condiciones necesarias para cumplir este objetivo, el fin es implementar un servidor AAA con sistema operativo CentOS7 y el software FreeRaius para los servicios RADIUS con un panel de control web, lo cual brindara una capa de seguridad de acceso a la red inalámbrica. El servidor Radius ofrece un control, monitoreo, y administración solicitando el uso de credenciales únicas para el acceso a las redes inalámbricas y creación de perfiles para el uso adecuado de los recursos de la red.

## 3. JUSTIFICACIÓN DEL PROYECTO

Es importante investigar y dar solución a este problema porque ha existido filtración de las contraseñas de las redes Wi-Fi los funcionarios sin autorizaciones y el público tienen acceso a las mismas de forma fácil por lo que las redes quedan expuestas y vulnerables, esto trae preocupación a la institución, porque puede darse la fuga o manipulación de información de cuentas de usuarios institucionales.

Para la realización de este proyecto es necesaria una investigación acerca de los servidores RADIUS utilizando el protocolo AAA y los mecanismos para la integración del mismo con la base de datos del sistema administrativo para su correcta implementación.

Los principales beneficios que se obtiene al implementar un servidor RADIUS utilizando el protocolo AAA son: el uso exclusivo de las redes para los funcionarios del GAD municipal del Cantón Mejía, contar con perfiles de acuerdo al cargo que desempeñan, la confianza de los usuarios al brindar su información.

Un servidor RADIUS utilizando el protocolo AAA como alternativa que nos facilita la tecnología para salvaguardar la información, este elemento juega un papel muy importante y además es una de las alternativas más usadas en el mundo de las redes de comunicaciones. Los servidores de autenticación, debido a que permiten acceso a la información y a los equipos de una empresa solo a personal autorizado, evitando de esta manera la manipulación y la malversación de cada una de los elementos de esta institución.

El servidor RADIUS utilizando el protocolo AAA se encarga de la autenticación, autorización y auditoria de las rede inalámbricas a los funcionarios de la institución, el acceso será mediante credenciales de usuarios o filtros MAC address del equipo, una vez autenticado se concederá autorización mediante perfiles para el desarrollo de su actividad laboral, las cuales pueden ser auditadas de forma remota por el administrador del servidor.

## 4. BENEFICIARIOS DEL PROYECTO

**Beneficiarios directos:**

- Los beneficiarios directos del presente proyecto son, el Jefe de Departamento de Redes y Telecomunicaciones y 579 funcionarios del GAD municipal del Cantón Mejía.

**Beneficiarios indirectos:**

- Ciudadanía del Cantón Mejía, Dirección Administrativa, Área TIC´S.

## 5. EL PROBLEMA DE INVESTIGACIÓN

En la actualidad el internet es una herramienta muy importante en el mundo de la comunicación, comercial y aprendizaje ya que a través del mismo se ha podido tener acceso a los recursos de forma remota.

A nivel mundial existen ciberataques y brechas de seguridad diarias, esto nos lleva a tomar más importancia a la protección del acceso a los computadores sea de empresas, instituciones y hogares. Como de forma física en los hogares existen sistemas de alarmas de protección de intrusos, todos debemos tener el mismo sistema de seguridad para prevenir ataques virtuales e intrusiones de usuarios maliciosos. El WPA2 es el sistema de cifrado que se usa para proteger las redes inalámbricas desde hace más de una década. Por años había sido considerado uno de los protocolos más seguros que se habían creado pero, tal y como se ha comprobado, tenía una falla en su seguridad que ha sido descubierta y que está, por lo menos potencialmente, a la mano de usuarios maliciosos, según la fuente (Hidalgo, 2017). Por estos motivos fueron creados los servicios de seguridad informática que se encargan de encontrar y controlar los accesos de intrusos y funcionamiento de la seguridad, como también se encarga de dar soluciones a las fallas encontradas.

Según este reporte, cualquier red abierta deja vulnerables a las computadoras portátiles y teléfonos de ser interceptados, pero quienes usan Wi-Fi en las cafeterías tienen un riesgo mayor, pues la ciberseguridad es muy baja, según la fuente (Comercio, s.f.). En el Ecuador todos estamos afectados por las vulnerabilidades de las redes inalámbricas, estudiantes, trabajadores involucrados

con la tecnología, funcionarios públicos, banqueros entre otros que se ven influidos directamente por mantenerse en conexión constante a las redes Wi-Fi por el simple hecho de tener q utilizarlo para comunicación, juegos, deberes, trabajo es por eso que hoy en día existen varios ataques de seguridad e intrusiones a redes inalámbricas comprometiendo la información.

El GAD Municipal del Cantón Mejía está ubicado en la ciudad de Machachi ha venido teniendo problemas de control de acceso de sus redes Wi-Fi mientras dan el servicio a sus usuarios. A lo largo de este tiempo la institución ha ido detectando que se encuentra expuestas sus redes, su cobertura por la filtración de claves de seguridad de las mismas por parte de los usuarios, es por ello que necesita que sus procesos se realicen de la forma más personalizada posible al contar con unas credenciales de acceso únicas para la autenticación y autorización para el consumo de servicio de internet y perfiles determinados los usuarios tendrán mayor eficiencia en sus funciones que cumple en la institución.

## 6. OBJETIVOS

### 6.1.General

Implementar una alternativa de seguridad en el acceso de las redes WI-FI por medio de un servidor AAA utilizando el protocolo de libre uso RADIUS, en el GAD Municipal del Cantón Mejía.

### 6.2.Específicos

- Analizar la arquitectura y los componentes de un servidor AAA utilizando el protocolo de libre uso RADIUS.
- Controlar el acceso a las redes WI-FI institucional y asignar perfiles a los usuarios del GAD municipal del Cantón Mejía.
- Presentar un servidor AAA beta funcional, seguro y confiable para garantizar la seguridad en el acceso a las redes inalámbricas del GAD municipal del Cantón Mejía.

## 7. ACTIVIDADES Y SISTEMA DE TAREAS EN RELACIÓN A LOS OBJETIVOS PLANEADOS

La tabla 1 que se presenta a continuación describe la correlación directa entre cada uno de los objetivos del proyecto, las actividades que los mismos involucran, los resultados de dichas

actividades y sus medios de verificación con el fin de obtener una secuencia lógica en el desarrollo del presente proyecto de investigación.

**Tabla 1.** Sistema de tares en relación a los objetivos planteados

| Objetivo | Actividad (tareas) | Resultado de la actividad | Descripción de la actividad (técnicas e instrumentos) |
|---|---|---|---|
| Analizar la arquitectura y los componentes de un Servidor AAA utilizando el protocolo de libre uso RADIUS. | Recopilación de información bibliográfica de:<br><br>Libros, artículos científicos, tesis, páginas web.<br><br>Lectura crítica de la información recogida.<br><br>Escritura de la fundamentación teórica del proyecto de investigación | Fundamentación teórica del proyecto de investigación. | • Libros<br>• Investigación Documental |
| Controlar el acceso a la red institucional y asignar perfiles a los usuarios del GAD municipal. | Probar el Control de las autenticaciones y autorizaciones de Usuarios | Configuración de WLC y NAS, usuarios en los administradores web correspondientes.<br><br>Envió de credenciales desde | • Interfaz de administración<br>• Interfaz Gráfica de usuario |

Siguiente

| | | | |
|---|---|---|---|
| | | una interfaz amigable. | |
| Presentar un servidor AAA beta funcional, seguro y confiable para garantizar la seguridad en el acceso a las Red institucional. | Implementar | Levantamiento de servicio en un centro de datos definido por software. | • Servidor<br>• Investigación Documental |

**Fuente:** El investigador

## 8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

### 8.1.Antecedentes

Desde que en 1979 los ingenieros de IBM en Suiza realizaron los primeros experimentos de WLAN usando rayos infrarrojos para conectar un par de ordenadores, la tecnología ha progresado considerablemente. Pero el mayor auge en el mundo de las conexiones entre computadores se ha producido en los últimos años gracias a la aparición del internet. Actualmente este auge aumento más si cabe debido a la existencia de protocolos de comunicación estándar que definen la conexión vía radio entre los distintos nodos de una red WLAN. Estos estándares han permitido la disponibilidad en el mercado de Tarjetas Interfaz de Red (NIC) inalámbricas de muy bajo precio y fácilmente implementables en todo tipo de dispositivos (PC, portátil, AP), así como de "chipsets" embebidos en portátiles con lo que la seguridad en el mundo de las conexiones inalámbricas paso de no tener ninguna importancia a ser de gran relevancia en muy poco tiempo (Dafonte & Pallardo, 2012).

Para responder a este problema surgieron varias soluciones, una de ellas servicios AAA basadas en protocolo RADIUS. Fue especificado originalmente en una RFI por Merit Network en 1991 para hacer un control de acceso por dial para NSFnet. A continuación, Livingston Enterprises respondió al RFI con una descripción del servidor RADIUS. Merit Network gano el contrato para Livingston Enterprises para que el pusiese RADIUS a la serie PortMaster de sus Servidores de Acceso a la red (NAS). Más tarde, en 1997, se publicó como RFC 2058 y RFC 2059(aunque las

versiones actuales de estos RFC con la 2865 y la 2866). Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto (Dafonte & Pallardo, 2012).

RADIUS se creó siguiendo un modelo cliente/servidor que pretendía ofrecer seguridad en las redes. Para ello se incorporaron muchos mecanismos de autenticación flexible. Además de esto se pretendía que este protocolo fuera extensible para que se pudieran añadir más atributos para dar información sin que esto corrompiera el funcionamiento del mismo (Dafonte & Pallardo, 2012).

### 8.2.Servicios AAA

AAA es una arquitectura de sistema, la cual sirve para la configuración de tres funciones de seguridad (Authentication, Authorization and Accounting, por sus siglas en ingles) de una forma coherente. AAA ofrece una forma modular de proveer los siguientes servicios

Autenticación: proporciona el método de identificación de usuarios, incluye nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería, y según el protocolo de seguridad que seleccione, puede ofrecer cifrado. La autenticación es la forma en que un usuario se identifica antes de poder acceder a la red y los servicios que esta ofrece. Configurando la autenticación AAA mediante la definición de una lista llamada métodos de autenticación, y luego aplicado esa lista a varias interfaces. En la lista de métodos se defines los tipos de autenticación a realizar y la secuencia en la que se llevara a cabo, esto debe ser aplicado a una interfaz específica antes de que cualquiera de los métodos de autenticación definidos se utilice. La única excepción es la lista de método por defecto (que se denomina “default”). La lista método por defecto se aplica automáticamente a todas las interfaces sin ninguna lista de otro método está definida. Una lista de método definida reemplaza automáticamente la lista de método por defecto. Todos los métodos de autenticación, excepto local, línea de contraseña y habilitación de la autenticación, debe ser definidas a través de AAA (Catalogo No OL-28850-04, 2018).

Autorización: Provee el método de control de acceso remoto, incluyendo autorización total o autorización para cada servicio, lista de cuentas y perfil por usuario, soporte para grupos de usuarios, y soporte para IP, IPX, ARA y Telnet. AAA Autorización trabaja agrupando atributos que se describen lo que el usuario está habilitado a usar o acceder. Estos atributos son comparados con la información contenida en una base de datos de un usuario determinado y el resultado se

devuelve a AAA para determinar las capacidades reales de los usuarios y las restricciones. La base de datos se puede localizar de forma local en el servidor de acceso o router también puede ser alojado de forma remota en un servidor de seguridad RADIUS o TACACS+, los servidores remotos de seguridad, utilizan a los usuarios de los derechos específicos mediante la asociación de atributos de valor (AV) pares, que los derechos con el usuario apropiado. Todos los métodos de autorización deben ser definidos a través de AAA. Así como en la autenticación, configurar AAA Autorización es definida por una lista llamada métodos de autorización, y luego aplicando esa lista a varias interfaces (Catalogo No OL-28850-04, 2018).

Contabilización: posee un método de recolección y un envió de información al servidor de seguridad, el cual es usado para facultar, auditoria y reportar: nombre de usuario, tipo de inicio y final, comando ejecutados (como PPP), cantidad de paquetes enviados, y numero de bytes. Contabilidad permiten realizar el seguimiento de los usuarios que tienen acceso a los servicios, así como la cantidad de recurso de red que están consumiendo. Cuando AAA contabilidad se activa, el acceso a la red del servidor informa la actividad del usuario al servidor de seguridad de RADIUS o TACACS+. Cada registro contable se compone de la contabilidad de pares AV y se almacena en el servidor de control de acceso. Estos datos pueden ser utilizados para la gestión de red, la facturación del cliente y auditoria. Todos los métodos de contabilidad deben ser definidos a través de AA. Al igual que con la autenticación y autorización, se configura la contabilidad AAA mediante la definición de una lista llamada métodos de contabilidad, y luego la aplicación esta lista a varias interfaces. AAA provee los siguientes beneficios:

- Incrementación de flexibilidad y control de configuración de acceso
- Estabilidad
- Métodos de autorización estandarizados, como RADIUS, TACACS+ o Kerberos
- Múltiples sistemas de backup

AAA está diseñado para q el administrador de la red pueda configurar dinámicamente el tipo de autenticación y autorización que se quiere, puede ser por línea (por usuario) o por servicio (por ejemplo, IP, IPX, VPDN) base. Para definir el tipo de autenticación y autorización que se desee, se hace mediante la creación de listas de métodos, a continuación, la aplicación d esas listas de método para determinados servicios o interfaces. Una lista de métodos es una lista de secuencias

que define los métodos de autenticación usados para autenticar usuarios. Las listas de método le permiten asignar uno o varios protocolos de seguridad que utilizaran para autenticación, lo que garantiza un sistema de copia de seguridad para la autenticación en caso de que el método inicial falle. El software utiliza el primer método de la lista para autenticar a los usuarios, y si ese método no responde, el software selecciona el método de autenticación siguiente de la lista de métodos. Este proceso continuo hasta que haya una comunicación exitosa con un método de autenticación de la lista o la lista de método de autenticación se ha agotado, es los que la autenticación caso de falla (Catalogo No OL-28850-04, 2018).

### 8.3.Comunicación

Comunicar es llegar a compartir algo de nosotros mismos. Es una cualidad racional y emocional específica del hombre que surge de la necesidad de ponerse en contacto con los demás, intercambiando ideas que adquieren sentido o significación de acuerdo con experiencias previas comunes (Fonseca, 2010).

### 8.4.RFC (Request for coments)

Son un conjunto de documentos que sirven de referencia para la comunidad de internet, que describen, especifican, asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con internet y las redes en general (Villagomez, 2018).

**Tabla 2.** Las RFC, protocolos o servicios más comunes.

| Especificación | RFC |
|---|---|
| Protocolo UDP (Protocolo de datagrama de usuario) | RFC768 |
| Protocolo IP | RFC791 |
| Protocolo ICMP (Protocolo de mensajes de control de Internet) | RFC792 |
| Protocolo TCP (Protocolo de control de transmisión) | RFC793 |
| Protocolo FTP (Protocolo de transferencia de archivos) | RFC959 |
| Correo electrónico | RFC822 |
| Protocolo Telnet | RFC854 |
| Protocolo NNTP (Protocolo de transferencia de noticias a través de la red) | RFC977 |
| Netbios | RFC1001 |
| Protocolo SLIP (Protocolo de línea serial de Internet) | RFC1055 |
| MIB | RFC1156 |
| TCP/IP | RFC1180 |

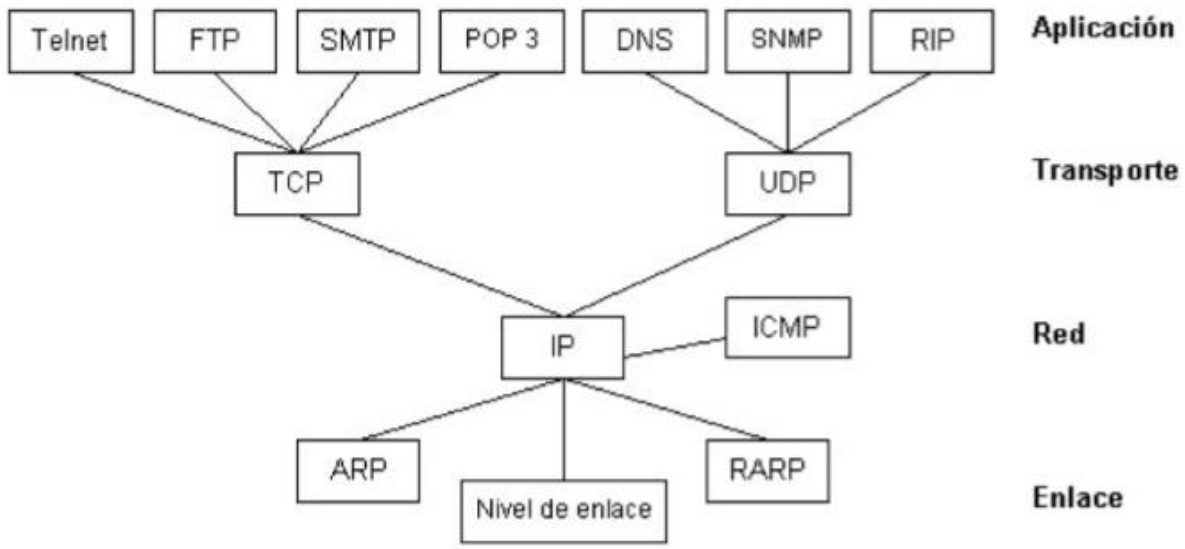
| | |
|---|---|
| Preguntas frecuentes para principiantes | RFC1206 |
| Preguntas frecuentes para usuarios experimentados | RFC1207 |
| Glosario de la red | RFC1208 |
| RFC (petición de comentarios) | RFC1325 |
| MIME (*Extensiones multipropósito de correo Internet*) | RFC2045, RFC2046 y RFC2047 |
| Asignación de direcciones IP para Intranet | RFC1597 |
| Protocolo PPP (Protocolo punto a punto) | RFC1661 |
| Números de puerto | RFC3232 |
| Protocolo HTTP | RFC2068 |
| Protocolo LDAPv3 | RFC2251 |
| Protocolo SMTP (Protocolo simple de transferencia de correo) | RFC2821 |

**Fuente:** (Villagomez, 2018)**.**

### 8.5.Protocolos de transporte en TCP/IP

Los protocolos de transporte de la arquitectura TCP/IP son el TCP (Transmission Control Protocol: protocolo de control de la trasmisión) y UDP (User Datagram Protocol: protocolo de datagrama de usuarios). Es decir, TCP/IP ofrece dos opciones de protocolo de transporte al nivel superior, el de aplicación. Ambos protocolos trabajan de forma muy diferente, y están orientados a distintos usos. No hay que pensar que TCP es mejor que UDP en general o viceversa. Así, existen aplicaciones que utilizan TCP y otras que usan UDP, véase la arquitectura en las figura 1, (Candelas & Baeza, 2009).

**Figura 1.** Conjunto de protocolos en la arquitectura de red TCP/IP.




**Fuente:** (Candelas & Baeza, 2009).

Como características principales, TCP es un protocolo orientado a conexión que ofrece un servicio muy fiable, aunque implica bastante tráfico adicional en la red. En cambio, UDP no está orientado a conexión y ofrece un servicio poco fiable, aunque rápido y con poca carga adicional en la red (Candelas & Baeza, 2009).

### 8.5.1. TCP (Transmission control protocol)

Las características principales de este protocolo son:

- **Trabaja con un flujo de bytes.** El nivel de aplicación entrega o recibe desde el de transporte bytes individuales. El protocolo TCP del emisor agrupa esos bytes en paquetes de tamaño adecuado para mejorar el rendimiento y evitar a la ve la fragmentación a nivel IP.
- **Transmisión orientada a conexión.** Se requiere una secuencia de conexión previa al envió – recepción de datos entre cliente y servidor, y una desconexión final. La conexión implica que solo hay dos equipos involucrados en el intercambio de datos (un cliente y un servidor).
- **Fiable.** Emplea control de flujo mediante ventana deslizante de envió continuo y asentimientos positivos (ACKs o Acknowledgements) para confirmar las tramas validas recibidas. La ventana deslizante se aplica a los bytes: se mueran y confirman bytes y no paquetes.
- **Flujo de bytes ordenado.** Aunque IP trabaja con datagrama, el proceso de TCP en el receptor ordena los paquetes que recibe para entregar los bytes al nivel superior en orden (Candelas & Baeza, 2009).

### 8.5.2. UDP (User datagrama protocol)

Un protocolo sin conexión que, como TCP, Funciona en redes IP.

UDP/IP proporciónala muy pocos servicios de recuperación de errores, ofreciendo en su lugar una manera directa de enviar y recibir datagramas atreves de una red IP se utiliza sobre todo cuando la velocidad es un factor importante en la trasmisión de la información (Atom, 2015).

Las características principales de este protocolo son:

- **Sin conexión.** No emplea ninguna sincronización entre origen y destino.
- **Trabaja con paquetes o datagramas enteros**, no con bytes individuales como TCP. Una aplicación que emplea protocolos UDP intercambia información en forma de bloques de bytes, de forma que, por cada bloque de bytes enviado de la capa de aplicación a la capa de transporte, se envía un paquete UDP.
- **No es fiable.** No emplea control de flujo ni ordena los paquetes
- **Una gran ventaja es** que provoca poca carga adicional en la red, ya que es sencillo y emplea cabeceras muy simples.
- **Un paquete UDP** puede ser fragmentado por el protocolo IP para ser enviado fragmentado en varios paquetes IP si resulta necesario.
- **Puesto que no hay conexión,** un paquete UDP admite utilizar como dirección IP de destino la dirección de broadcast o de multicast de IP. Esto permite enviar un mismo paquete a varios destinos de forma simultánea (Candelas & Baeza, 2009).

Algunas aplicaciones de UDP pueden ser:

- Transmisión de datos LANs fiable, como el protocolo TFTP (Tivial file transfer protocol), que es una variable del protocolo FTP que emplea como protocolo de transporte UDP.
- Operaciones de sondeo. Transmisión de paquetes de datos pequeños o esporádicos para informar el estado de los equipos de la red, o para intercambiar información de encaminamiento, como es el caso de los protocolos DNS (Domain name system), RIP (Routing information protocol) o SNMP (simple network management protocol).
- Transmisión multicast de video o audio. UDP es usado por aplicaciones VoIP (Vice over IP), difusión del video y multiconferencias en la trasmisión de señales digitales suele ser más importante una respuesta rápida de los protocolos que un envió complementario viable. No importa que se pierdan algunos datos: lo importa es que se mantenga un flujo constante de información. Además, con UDP es posible que una misma fuente envíe la señal a múltiples destinos, si repetir paquetes de datos en la red
- Otra aplicación es el envió de transacciones rápidas a BB.DD a través de las redes LAN fiables. En este caso también premia la rapidez de respuesta, y dado que la red ofrece una alta calidad, no es necesario el complejo control de flujo de TCP (Candelas & Baeza, 2009).

### 8.6.NAS (Network Access Server)

El servidor de acceso a la red actúa como la puerta de enlace entre el usuario y la red más amplia. Cuando un usuario intenta obtener acceso a la red, el NAS pasa información de autenticación (por ejemplo, nombre de usuario y contraseña) entre el usuario y el servidor RADIUS. Este proceso se denomina una sesión de autenticación. Tenga en cuenta que el inicio de sesión del usuario inicia esta conversación de sesión de autenticación. Este es un concepto clave (DeKok, 2018).

Al final de la sesión de autenticación, el servidor le indica al NAS que rechace al usuario y le niegue el acceso a la red o que acepte al usuario y le brinde acceso a la red. Una vez que el usuario ha accedido a la red, el NAS aplica las restricciones de seguridad (definidas por el servidor RADIUS), que actúa como el enrutador de la puerta de enlace y el firewall para ese usuario (DeKok, 2018).

### 8.7.Wi-Fi

Básicamente se trata de un sistema que permite que diferentes dispositivos electrónicos se conecten a las redes de comunicación atreves de un punto de acceso de red inalámbrica. Dicho punto de acceso tiene un alcance limitado, siendo mayor al aire libre que en interiores. La popularidad de estas redes se deba a que están asociadas a una supuesta transmisión de datos gratuita, lo que solo es cierto en ocasiones (Roca, 2014).

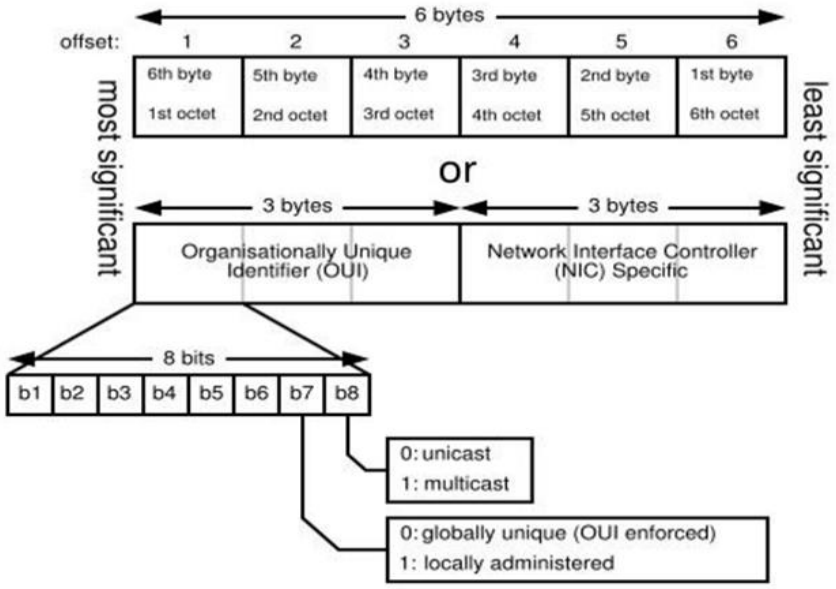
De forma simple, una red Wi-FI es el nexo de unión entre una red de datos fija y una serie de dispositivos que funcionan de modo inalámbrico. Si esos dispositivos quieren conectarse con cualquier usuario, portal u ordenador que esté cerca o en el otro lado del planeta, y no quiere usar las redes de los operadores móviles tradicionales, una de las opciones más utilizadas es la red WiFi. Esta rede dispone de uno o varios puntos de acceso, que captan la señal de los dispositivos y la canalizan a la red fija, o a la inversa. Puede agregarse puntos de acceso para generar redes de cobertura más amplia, conectar antenas Wi-Fi más grandes q amplifiquen la señal o usar repetidores Wi-Fi inalámbricos para extender la cobertura de una red que tiene la señal más débil. En caso de redes de dimensiones más reducidas el elemento clave es el router Wi-Fi, que hace las veces de punto de acceso El proveedor de la rede de banda ancha fija es el que normalmente suele

proporcionar ese router Wi-Fi que puede tener la doble opción de enviar la señal por cable o de forma inalámbrica dentro de esa casa o local (Roca, 2014).

### 8.8.MAC address

La dirección MAC (siglas en ingles de Media Access Control / Control de acceso al medio) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una ethernet de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. Composición del MAC address (Gorgona, 2017).

**Figura 2.** Identificador MAC.




**Fuente:** (Gorgona, 2017).

### 8.9.Red informática

Una red informática es un sistema conformado por dos o más computadores interconectados entres si cuya conexión permite compartir y transportar datos en tiempo real a través de los equipos y programas habilitados para ello. Estas redes pueden estar conectadas de forma física o inalámbrica (Torres, 2018).

La red informática tiene como principal objetivo la difusión de la información de manera instantánea y eficaz entre varios usuarios en línea. En consecuencia, las redes informáticas están diseñadas con un protocolo de comunicaciones que requiera de un ente emisor, un medio a través del cual se trasmite un mensaje y un receptor de la información (Torres, 2018).

### 8.10. PPP (Point to Point Protocol)

El protocolo PPP (Point to Point Protocol / Protocolo punto a punto), es un protocolo de nivel de enlace especificado para el implementar protocolos de red sobre enlaces entre pares de estaciones que esta normalizado en el documento RFC 1661 (Candelas & Baeza, 2009).

PPP proporciona sobre una línea punto a punto detección de errores, verificación de autenticación en el enlace, reconocimiento de varios protocolos de nivel de red (IP, IPX, OSI, CLNP, etc.) y negociaciones de direcciones de red IP, lo que le convierte en el protocolo de nivel de enlace muy utilizado (Candelas & Baeza, 2009).

El protocolo PPP emplea para delimitar cada trama la secuencia de bits “011111110” al principio y al final de la misma. Los campos dirección y control están a un valor fijo y sirve para mantener la compatibilidad con otros protocolos de nivel de enlace existentes (por ejemplo, HDLC). Hay que tener en cuenta que en un enlace punto a punto entre un par de estaciones no resulta necesario usar direcciones de enlace o MAC, ya que solo hay dos equipos, y lo que uno envía llena directamente al otro. Así mismo, tampoco se requiere usar ARP para resolver las direcciones de enlace. En el campo protocolo se especifica el tipo de paquete que hay en el cuerpo de datos del paquete PPP: un paquete IP, IPX, etc. Después de los datos aparece una secuencia de verificación de la trama (Frame Control Secuence) que es un código de 16 o 32 (Candelas & Baeza, 2009).

De esta forma, cada paquete PPP incorpora una cantidad total de 10 bytes redundantes en la cabecera y la cola (Candelas & Baeza, 2009).

### 8.11. PAP (Password authentication protocol)

PAP fue uno de los primeros protocolos de Usuario que facilitaba el suministro de un username y password cuando se hace conexiones punto a punto. Con PAP la NAS toma el PAP ID y password y los envía en un paquete Access – Request como el user-name y user-pasword. PAP es simple

comparado con CHAP y MS- CHAP por que el NAS simplemente entrega al servidor RADIUS un username y password, las cuales son verificadas. Este username and password viene directamente del usuario atreves del NAS a el servidor en una sola acción (Der, 2011).

Aunque PAP trasmite password en texto claro, usándolo no siempre debería ser mal visto. Este password está en texto claro entre el usuario y el NAS. El password de usuario será encriptado cuando el NAS reenvié la petición a le servidor RADIUS (Der, 2011).

Si PAP es usado dentro de un túnel seguro esto es tan seguro como el túnel. Esto es similar a cuando los detalles de tu tarjeta de crédito están tuneados dentro de una conexión HTTPS y entregado a un servidor web seguro (Der, 2011).

### 8.12. CHAP (Challenge-Handshake Authentication Protocol)

CHAP representa Challenge-Handshake Authentication Protocol y fue diseñado como una mejora a PAP. Esto impide trasmitir un password de texto claro (Der, 2011).

CHAP fue creado en el día cuando los modems de acceso telefónico eran populares y la precaución sobre PAP password de texto claro era alta (Der, 2011).

Después un enlace es establecido a la NAS, la NAS genera un desafío aleatorio y lo envía al usuario. El usuario después responde a este desafío por retornar un hash unidireccional calculado en un identificador, el desafío y el password de usuario, la respuesta del usuario es después usado por el NAS para crear un paquete Access-Request, el cual es enviado a el servidor RADIUS. Dependiendo en la respuesta del servidor RADIUS, el NAS regresara CHAP Success o CHAP Failure al usuario (Der, 2011).

El NAS puede además pedir aleatorios intervalos de que el proceso de autenticación se repita enviando un nuevo desafío al usuario. Esta es otra razón por que es considerado más seguro que PAP (Der, 2011).

### 8.13. Protocolos AAA

La familia de protocolos AAA, acrónimo de Authentication Authorization y Accounting (Autenticación, Autorización y Contabilización) fueron diseñados como mecanismos de control de

acceso remoto y provisión de servicios de red originalmente a través de modem y línea telefónica (dial- in), pero se siguen implementando actualmente en múltiples arquitecturas (Lopez, 2015).

Entre los protocolos que consideran relacionados directamente con un sistema AAA encontramos a RADIUS, Diameter, TACACS+ y COPS, los cuales serán descritos en los siguientes puntos.

Por lo general, la conexión entre los elementos que conforman un sistema AAA es punto a punto la cual requiere de seguridad para poder trasmitir información. Para esto existe ciertos protocolos que permiten implementar y también puede ser considerados, entre estos se tiene a PAP (Password Authentication Protocol / Protocolo de autenticación por Contraseña), CHAP (Challenge Handshake Authentication Protocol / Protocolo de Autenticación por Desafío Mutuo) o EAP (Extensible Authentication Protocol / Protocolo de Autenticación Extensible) (Rensing, Karsten, & Stiller, 2002).

### 8.13.1. RADIUS (Remote Access Dial In User Service)

RADIUS es un acrónimo de Remote Access Dial In User Service. RADIUS fue parte de un AAA solución entregada por Livingston Enterprises a Merit Network en 1991. Merit Network es un proveedor de Internet sin fines de lucro, que requería una forma creativa de administrar el acceso telefónico a varios puntos de presencia (POP) en su red (Der, 2011).

Es un protocolo que destaca sobre todo por ofrecer un mecanismo de seguridad, flexible, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red (Crespo, 2017).

La solución suministrada por Livingston Enterprises tenía una tienda de usuario central utilizada para autorizar esto podría ser utilizado por numerosos servidores RAS (acceso telefónico). Autorización y conteo también se podría hacer mediante la cual se saltó la AAA. Otro aspecto clave de la solución de Livingston incluía proxying para permitir el escalado (Der, 2011).

El protocolo se utiliza en esquema cliente servidor. Es decir, un usuario con unas credenciales de acceso al recurso se conecta contra un servidor que será el que se encarga de verificar la autenticidad de la información y ser el encargado de determinar si el usuario accede o no al recurso compartido. Ya hemos mencionado que se utiliza sobre todo por los operadores de red, pero es

cierto que en las redes Wi-Fi de hoteles u otros establecimientos también es habitual encontrarse con esto (Crespo, 2017).

El protocolo RADIUS se publicó posteriormente en 1997 como RFC, algunos cambios aplicados, y hoy tenemos RFC2865, que cubre el protocolo RADIUS, y RFC2866, que cubre la rendición de cuentas de RADIUS. También hay RFC adicionales que cubren mejoras en ciertos aspectos del RADIUS. Tener RFCs para trabajar permite a cualquier persona o proveedor implementar el protocolo RADIUS en su equipo o software. Esto dio lugar a una amplia adopción del protocolo RADIUS para manejar AAA en redes TCP / IP. Usted va a la palabra RADIUS se usa de forma general para significar el protocolo RADIUS o el cliente RADIUS / sistema servidor. El significado debe quedar claro en el contexto en el que se utiliza (Der, 2011).

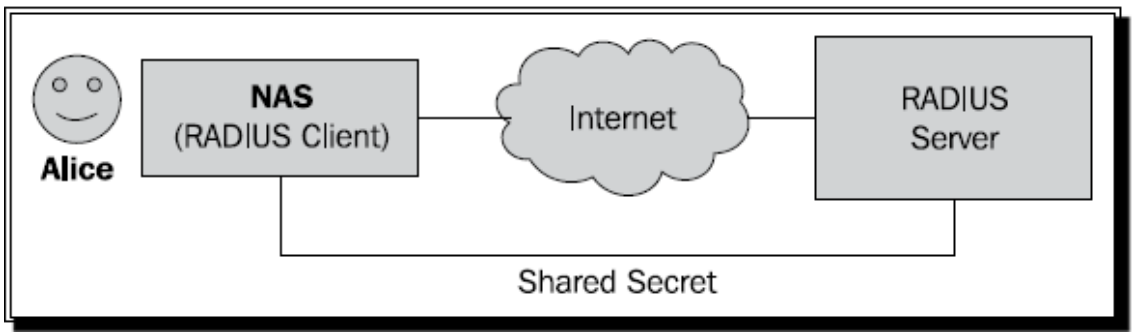
#### 8.13.1.1. RADIUS protocol (RFC2865)

Esta sección explora el protocolo RADIUS a nivel técnico como se publicó en RFC2865. Se excluye el Accounting RADIUS. Esto se publica como RFC2866 y se explora en su propia sección (Der, 2011).

El protocolo RADIUS es un protocolo cliente / servidor, que hace uso de UDP para comunicarse. El uso de UDP en lugar de TCP indica que la comunicación no es estricta en el estado. Un bajo típico de datos entre el cliente y el servidor consiste en una única solicitud del cliente seguida de una sola respuesta del servidor. Esto hace que RADIUS sea un protocolo muy ligero y ayuda con su eficiencia a través de enlaces de red lentos (Der, 2011).

Antes de poder establecer una comunicación exitosa entre el cliente y el servidor, cada uno tiene para definir un secreto compartido. Esto se utiliza para autenticar clientes (Der, 2011).

**Figura 3.** Comunicación Radius cliente-servidor.



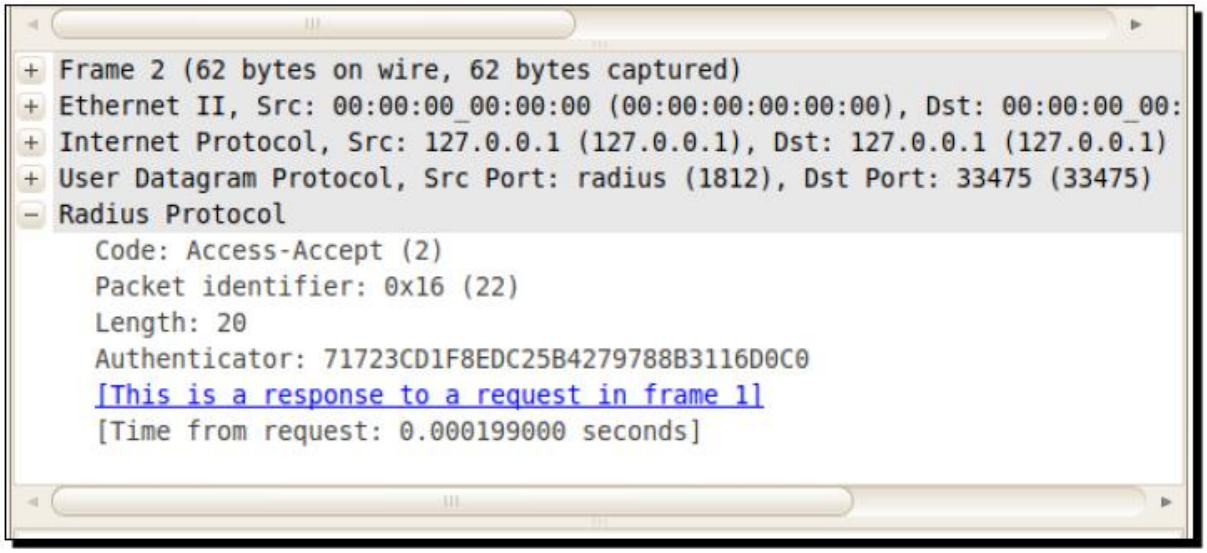

**Fuente:** (Der, 2011).

## Los paquetes de datos

Conocer el formato de un paquete RADIUS ayudará en gran medida a entender el RADIUS protocolo. Veamos más de cerca el paquete RADIUS. Veremos una simple solicitud de autorización. Un cliente envía un paquete de solicitud de acceso al servidor. El servidor responde con un paquete de aceptación de acceso para indicar el éxito (Der, 2011).

Los paquetes RADIUS que se muestran aquí son solo la carga útil de un paquete UDP.

**Figura 4.** Paquete de aceptación de acceso.




**Fuente:** (Der, 2011).

- **Código**

Cada paquete es identificado por un código. Este campo es de un octeto de tamaño. El valor de este código determina ciertas características y requisitos del paquete. La siguiente tabla puede ser utilizará como referencia para enumerar algunos de los códigos definidos actualmente para paquetes RADIUS: (Der, 2011).

**Figura 5.** Códigos de características y requisitos de los paquetes.

| RADIUS code (decimal) | Packet type | Sent by |
|---|---|---|
| 1 | Access-Request | NAS |
| 2 | Access-Accept | RADIUS server |
| 3 | Access-Reject | RADIUS server |
| 4 | Accounting-Request | NAS |
| 5 | Accounting-Response | RADIUS server |
| 11 | Access-Challenge | RADIUS server |
| 12 | Status-Server (Experimental) | |
| 13 | Status-Client (Experimental) | |
| 255 | Reserved | |

**Fuente:** (Der, 2011).

- **RADIUS server**

  El protocolo RADIUS está basado en cliente / servidor. El servidor RADIUS escuchará en el puerto UDP 1812 y 1813. El puerto 1812 se utiliza para la autenticación. Esto implicará Solicitud de Access-Request, Access-Accept, Access-Reject, y Access-Challenge. El puerto 1813 se utiliza para rendir cuentas. Esta implicará paquetes de Solicitud de Cuenta y Respuesta de Cuenta de Respuesta (Der, 2011).

  Un cliente y el servidor requieren un secreto compartido para cifrar y descifrar ciertos campos en el paquete de RADIUS (Der, 2011).

- **RADIUS client**

  Los clientes RADIUS suelen ser equipos que proporcionan acceso a una red de datos TCP / IP. El cliente actúa como un intermediario entre el servidor RADIUS y un usuario o dispositivo que desea obtener acceso a la red (Der, 2011).

  La funcionalidad de proxy de RADIUS también permite que un servidor RADIUS sea el cliente de otro servidor RADIUS, que eventualmente puede formar una cadena (Der, 2011).

  Los comentarios del servidor RADIUS no solo determinan si un usuario está permitido en la red (autenticación), pero también puede dirigir al cliente a imponer ciertas restricciones en el usuario (autorización) (Der, 2011).

La responsabilidad de imponer los ajustes recomendados a la sesión del usuario recae en aunque el cliente Debido a la naturaleza sin estado del protocolo RADIUS no hay manera de el servidor RADIUS sabrá si el cliente está imponiendo las restricciones recomendadas. En orden para que el cliente se comunique con éxito con el servidor RADIUS debe haber un compartido secreto entre los dos. Esto se utiliza para cifrar ciertos atributos (Der, 2011).

#### 8.13.1.2. RADIUS accounting (RFC2866)

Esta sección explora la funcionalidad conteo del protocolo RADIUS. Conteo es un medios de seguimiento del uso de los recursos y normalmente utilizados para la facturación (Der, 2011).

- **Operación**

  El servidor de cuentas RADIUS se ejecuta en el puerto 1813. Cuando la sesión de un usuario comienza el NAS envía un paquete de solicitud de cuenta al servidor RADIUS. Este paquete debe contener cierta

  AVPs. Es el primer paquete enviado con éxito en la autenticación. El servidor confirmará recepción enviando un paquete de respuesta-cuenta correspondiente.

  A lo largo de la sesión, el NAS puede enviar informes de actualización opcionales sobre la imagen y los datos uso de un usuario particular. Cuando finaliza la sesión del usuario, el NAS informa al servidor al respecto. Esto pone un cierre a los detalles contables registrados durante la sesión del usuario.

  La funcionalidad del cliente RADIUS proporciona provisiones para instancias cuando el servidor está inactivo. El NAS luego, dependiendo de su configuración, volverá a intentarlo o se pondrá en contacto con otro servidor RADIUS.

  Cuando un servidor RADIUS funciona como un proxy de reenvío a otro servidor RADIUS, servir de relevo para los datos contables. También puede registrar los datos contables localmente antes reenviarlo (Der, 2011).

**Formato de paquete**

La cuenta implica el código RADIUS 4 (solicitud de la cuenta) y el código 5 (respuesta de la cuenta) los paquetes Los paquetes de cuentas como los paquetes de autenticación utilizan el mismo protocolo RADIUS.

Una característica única de los paquetes de cuentas es que el atributo de contraseña de usuario no se envía en la solicitud (Der, 2011).

**RADIUS extensions**

Después de que los RFC iniciales definan RADIUS en general y RADIUS, varias extensiones se propuso ampliar el uso de RADIUS o mejorar algunas debilidades.

También hay un protocolo RADIUS mejorado llamado Diámetro (juego de palabras, el doble de bueno que RADIUS). Sin embargo, la captación de Diámetro ha sido muy lenta, y el umbral de RADIUS sigue siendo el estándar de facto para el futuro previsible. Una razón importante para esto es probablemente el hecho que las muchas mejoras que se suponía que Diameter debía traer ya están cubiertas por las diversas extensiones de RADIUS. Existe, por ejemplo, el protocolo RadSec que transporta (Der, 2011).

### 8.13.2. TACACS+ (Terminal Access Control Access Control System)

TACACS acrónimo de Terminal Access Controller Access Control System, es un protocolo estándar de la industria especificado para reenviar la información de nombre y contraseña de un usuario a un servidor centralizado. El protocolo TACACS+ es la nueva versión del protocolo TACACS referenciado en FRC1942 y desarrollado por la compañía BBN para la MILNET, existe hoy en día una implementación de seguro de tipo propietario de la compañía Cisco, la cual, ha sido ampliada y modificada varias veces mediante extensiones. TACACS+ ha sido mejorada de TACACS y XTACACS, ahora son dos protocolos totalmente diferentes al TACACS+ actual. TACACS+ es un protocolo cliente servidor al igual que RDS en donde un cliente NAS envía una petición que es respondida por un servidor AAA, el componente fundamental de TACACS+ es la separación de los procesos de authentication, authorization y accounting; con lo que permite que en la implementaciones no sea obligatorio el empleo de los tres (Forero, 2009).

#### 8.13.2.1. Operación de TACACS+

Cuando la conexión se establece el NAS contacta al demonio de TACACS+ para obtener una pantalla de acceso al sistema. El usuario indica su nombre de usuario y el NAS se comunica con el

demonio TACACS+ para obtener una pantalla de contraseña luego de indicar la contraseña la información es enviada de nuevo al demonio para que la procese (Forero, 2009).

El NAS recibe una de las siguientes posibilidades de respuesta:

Accept: El usuario es autenticado y el servicio puede iniciar.

Reject: Ha fallado la autenticación del usuario. El usuario puede ser rechazado o invitado a reintentar la conexión.

Error: Un error sucede durante la autenticación. Responde un mensaje de error y el servidor NAS intenta un método alternativo de autenticación.

Continue: El usuario es invitado a suministrar información adicional para proceder con la autenticación (Forero, 2009).

### 8.13.3. Diameter

Diameter es un protocolo de la industria de próxima generación utilizado para intercambiar de información Authentication, Authorization, Accounting (AAA) en LTE (Long-Term Evolution) evolución a largo plazo y IMS (IP Multimedia Systems) sistemas multimedia IP de redes. Se derivó y mejoro ampliamente de los protocolos RADIUS y LDAP (Lightweight Directory Access Protocol / Protocolo de Acceso de Directorio ligero), Proporcionando más fiabilidad, seguridad y mecanismos de transporte flexible para las redes de datos móviles. Una variedad de LTE y IMS conecta una red de computadoras las funciones hacen uso de Diameter (Ribbon Communications, 2019).

### 8.13.4. COPS (Common Open Policy Service)

Actualmente existen dos arquitecturas dominantes para QoS: Servicios integrados y Servicios Diferidos (Grupo de teleinformatica y automatizacion, 2017).

Varios refinanciamientos y extensiones para ambas arquitecturas han sido presentados y ampliamente desarrollados. Una importante extensión para este protocolo es la posibilidad de

controlar quien puede acceder cierto nivel de servicio (Grupo de teleinformatica y automatizacion, 2017).

Si este control, cualquier persona puede elegir el mejor servicio, la reducción de la aplicación de la calidad controlar el mayor esfuerzo del envío. Con el fin de proporcionar este control, un punto de decisión (PDP) se introduce dentro de cada área. Este PDP puede ser un sistema autónomo (AS), un router o un dominio de red (Grupo de teleinformatica y automatizacion, 2017).

En la arquitectura diferenciada Servicios el usuario se dirige a la PDP y pregunta acerca de un servicio específico, por ejemplo, finalizar una conexión virtual a fin con una banda de anchura definida. Si el servicio se permite al usuario, el PDP se pone en contacto con los routers implicados en esa zona y otras unidades que controlan el trafico IP (PEP) y las configura para guiar la solicitud de solicitud (Grupo de teleinformatica y automatizacion, 2017).

En la arquitectura de servicios integrados, el usuario accede al PEP, por ejemplo, un router, que hace contacto con el PDP. Con el fin de hacer posible el uso de PEP y PDP de diferentes fabricantes en una misma red, existe un protocolo que estandariza el intercambio de información. Este es el COPS (Common Open Policy Service), el cual es un protocolo básico que se puede extender con funcionalidades específicas para ciertas arquitecturas. Uso COPS para la Directiva de aprovisionamiento, COPS uso para RSVP son algunos ejemplos de extensiones (Grupo de teleinformatica y automatizacion, 2017).

El propósito del protocolo COPS es intercambiar información entre el PDP y sus clientes, llamados PEP. Se determina la asignación de recursos de tráfico de red de acuerdo con las prioridades deseadas de servicio. Para realizar un alto nivel de seguridad. Los mensajes se pueden escribir con una clave y una función de encriptación utilizando el algoritmo HMAC (Grupo de teleinformatica y automatizacion, 2017).

## 9. HIPÓTESIS

Con la implementación de un servidor AAA para el control de acceso de las Redes WI-FI institucional del GAD municipal del cantón Mejía, se podrá verificar el acceso a la red y la reducción de riesgo de intrusiones y vulnerabilidades.

# 10. METODOLOGÍAS Y DISEÑO EXPERIMENTAL

## 10.1. Método teórico practico

Para la investigación propuesta utilizaremos el método teórico practico, sabiendo que este método permite realizar una investigación a fondo en el conocimiento de las regularidades y cualidades principales de los fenómenos, así podemos realizar una investigación minuciosa con la cual pondremos en producción un servidor AAA para el control de acceso de las redes Wi-Fi del GAD municipal de Mejía. Por ello se apoya fundamentalmente en los procesos de abstracción, deducción, síntesis y análisis.

## 10.2. Diseño Experimental

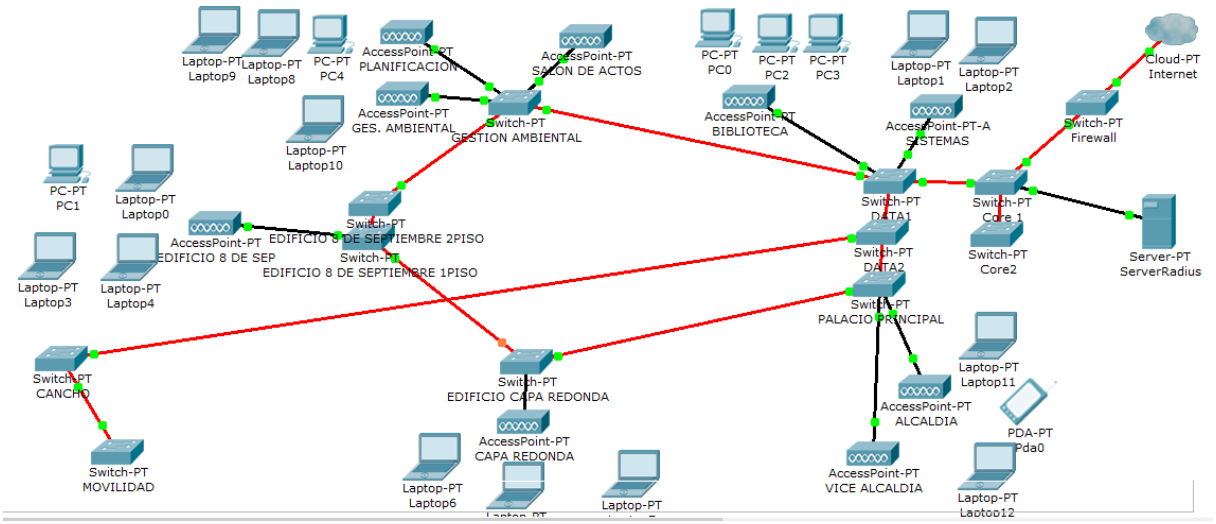
En el diseño experimental, para poder realizar el proyecto de investigación de servicios A.A.A en las redes Wi-Fi del GAD Municipal del Cantón Mejía. Se investigó topologías, servicios, protocolos, puertos, estándares, sistemas operativos, aplicaciones GUI sobre la implementación de servicios A.A.A basados en la utilizando el protocolo de libre uso RADIUS.

### 10.2.1. Diseño de la infraestructura de RADIUS

Para la realización de este proyecto se planea realiza el diseño físico o lógico de la red para el acceso a la WLAN basada en el estándar 802.1X, comprendido en la configuración del servidor RADIUS, dispositivos electrónicos, conexiones inalámbricas, equipos clientes, decisiones y opciones seleccionadas para la solución.

La topología usada en el GAD municipal del cantón Mejía es una topología mixta la cual es una de las más frecuentes y se crea de la unión de los diferentes tipos de topologías, en este caso es una topología estrella-anillo dado que los equipos están conectados a un switch HP s200cs con topología estrella. Sin embargo, estos switch están conectados con una topología en anillo, con el propósito de la redundancia en la red en caso de fallos de enlace para garantizar la comunicación de datos en un 99.9%.

**Figura 6**. Diseño de la infraestructura de Radius.




**Fuente:** El investigador.

Por los recursos y usuarios definidos administrativamente conectados a la red, estos están configurados mediante Vlan las cuales están organizas por departamentos porque nos brinda varias ventajas como la simplificación de la administración de la red, flexibilidad, seguridad.

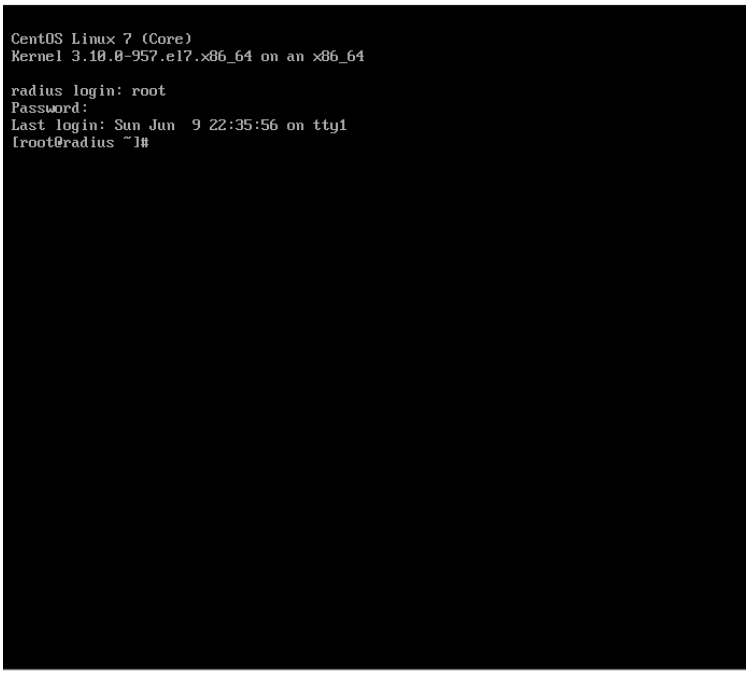
Las vlans están configurado para los distintos departamentos pero se cuenta también con vlans para teléfonos, cámaras y equipos biométricos 37vlans en total de clase C y con mascara 255.255.255.0.

### 10.2.2. Servidor CentOS 7

Para la implementación de este proyecto servidor AAA utilizando el protocolo de libre uso RADIUS se decidió hacer uso del software de licencia libre FreeRadius sobre un ambiente Linux, CentOS 7 como servidor RADIUS el cual se conectara a un Wireless Lan Controller que administra todos los puntos de acceso de la red y los configura para que sean clientes del servidor.

Para la investigación el GAD Municipal concedió el acceso a un servidor CentOS 7 mediante su infraestructura definida por software, así mismo como su dirección IP, User name y password, Véase en la figura 7.

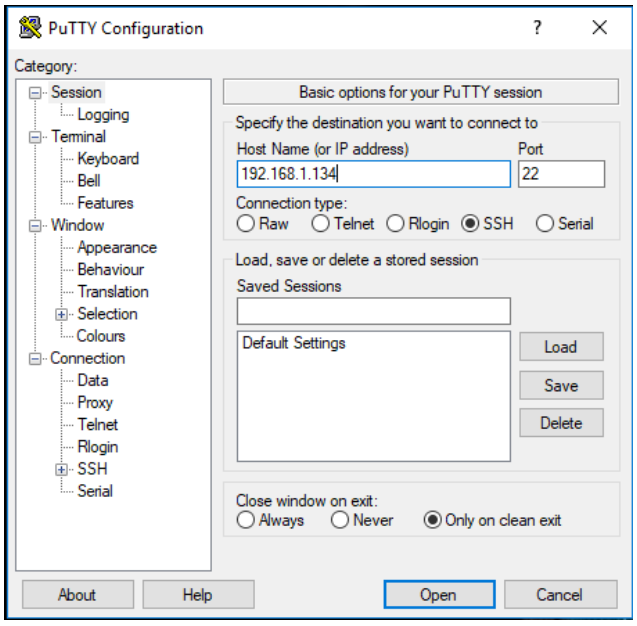
**Figura 7.** Servidor CentOS 7.




**Fuente:** El investigador.

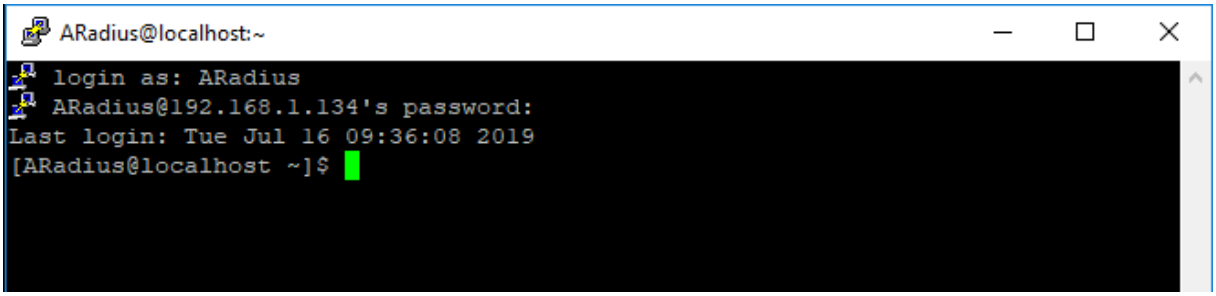
La comunicación con el servidor será mediante la utilización de PuTTY herramienta de conexión de línea de comando, utilizada para sesiones SSH y proporciona control al usuario sobre el terminal, entrando a la consola tal como se muestra en la figura 8 y 9, para con esto poder realizar la configuración del servidor.

**Figura 8**. Interfaz gráfica de PuTTY.




**Fuente:** El investigador.

**Figura 9.** Conexión de línea de comandos.



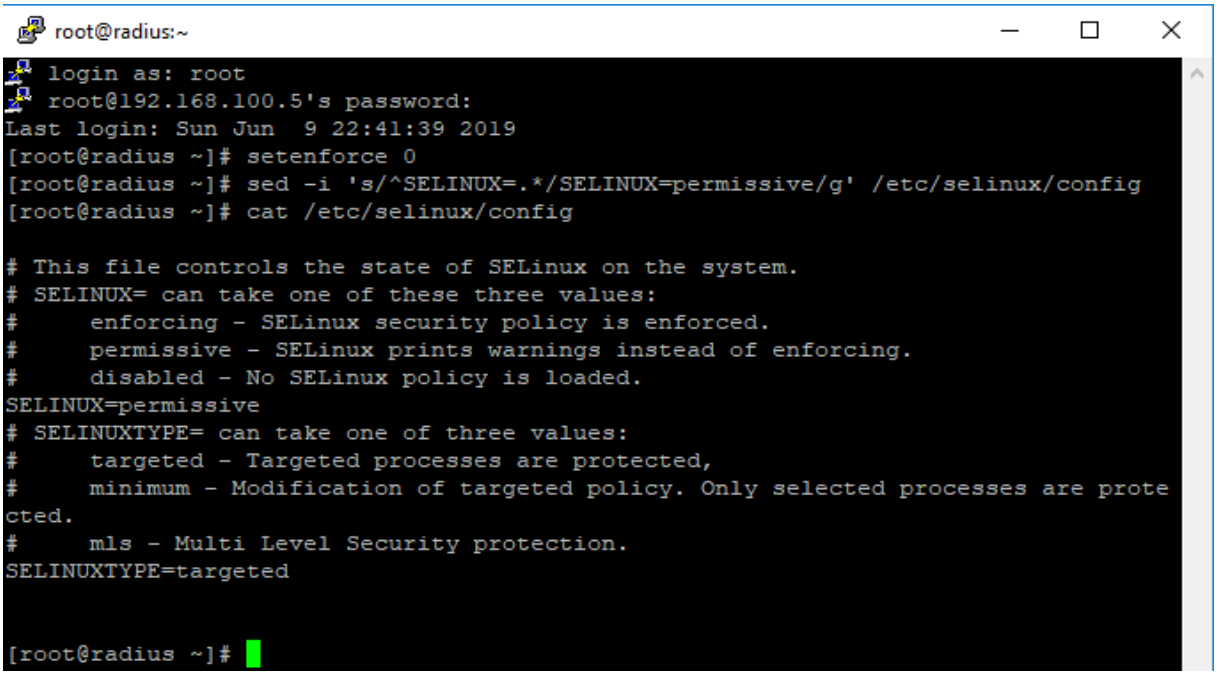

**Fuente:** El investigador.

### 10.2.3. Preparación para la instalación FreeRadius server.

Para comenzar la configuración del servidor RADIUS, debemos realizar la instalación del software freeRadius el cual es de código abierto, como mencionamos anterior mente la instalación será mediante la conexión de line de comandos.

Para comenzar la instalación se recomiendo desactivar SELinux o configurarlo en modo permisivo como se muestra en la figura 10.

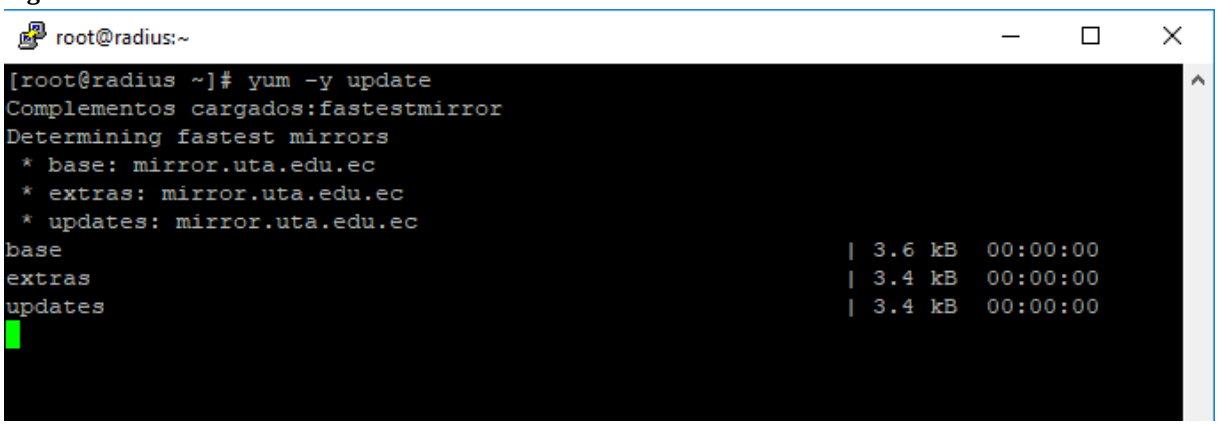
**Figura 10.** Recomendación antes de la instalación.




**Fuente:** El investigador

Otra recomendación esencial es actualizar el servidor centOS 7 para trabajar con los paquetes más actuales para evitar que el servidor tenga fallas de seguridad conocidas para lo cual lo realizamos como se muestra en la figura 11.

**Figura 11.** Actualización CentOS 7

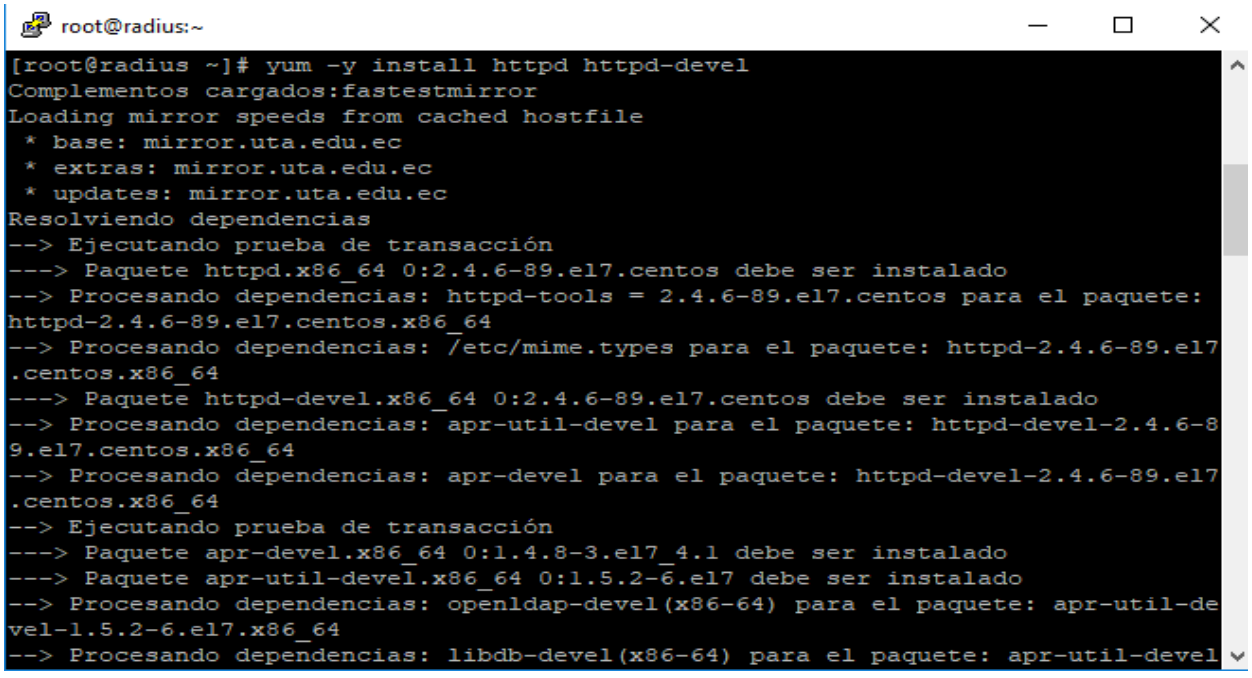



**Fuente:** El investigador.

### 10.2.4. Instalación del servicio httpd

Es necesario contar con servicios previamente instalados para la instalación de FreeRadius como es el servicio de HTTPD, véase en la figura 12.

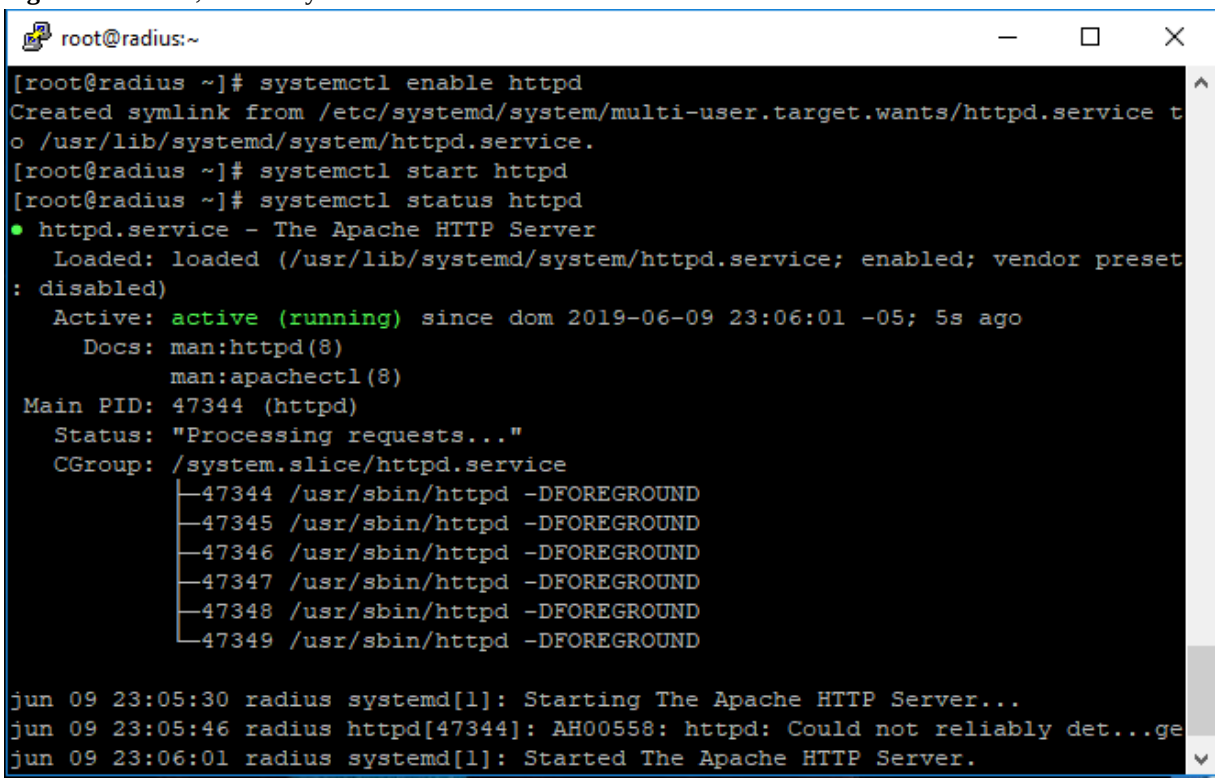
**Figura 12**. Instalación servicio httpd.




**Fuente:** El investigador.

Cuando la instalación haya finalizado, puede habilitar e iniciar su servicio HTTPD de la misma forma también puede verificar el estado de ejecución del servicio HTTPD usando los siguientes comandos. Como se ve en la figura 13.

**Figura 13.** Iniciar, habilitar y verificar el estado del servicio.




**Fuente:** El investigador.

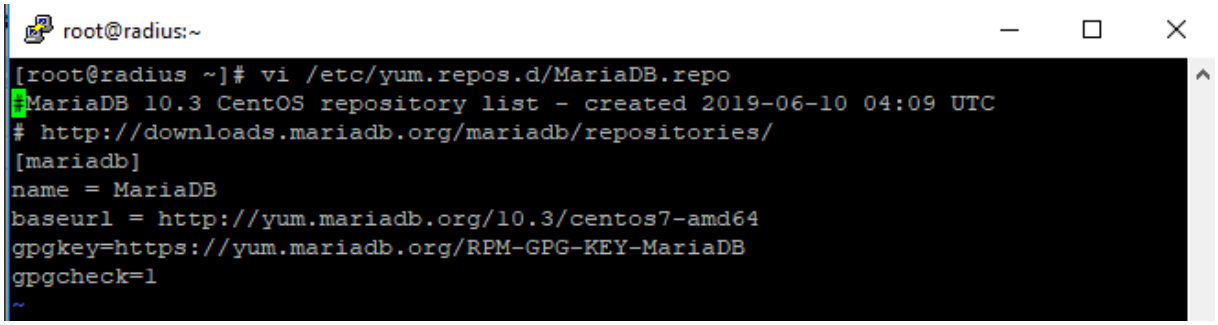
### 10.2.5. Instalación y configuración de MariaDB

A continuación vamos a instalar y configurar MariaDB 10.3 en nuestro caso la última versión, para lo cual es recomendable seguir los pasos que presentamos continuación:

#### 10.2.5.1. Agregar contenido de repositorio oficial de MariaDB al sistema CentOS 7

En la figura 14, Añadimos el contenido a continuación en el archivo MariaDB.repo luego guardamos el archivo.

**Figura 14.** Agregar repositorio de MariaDB.

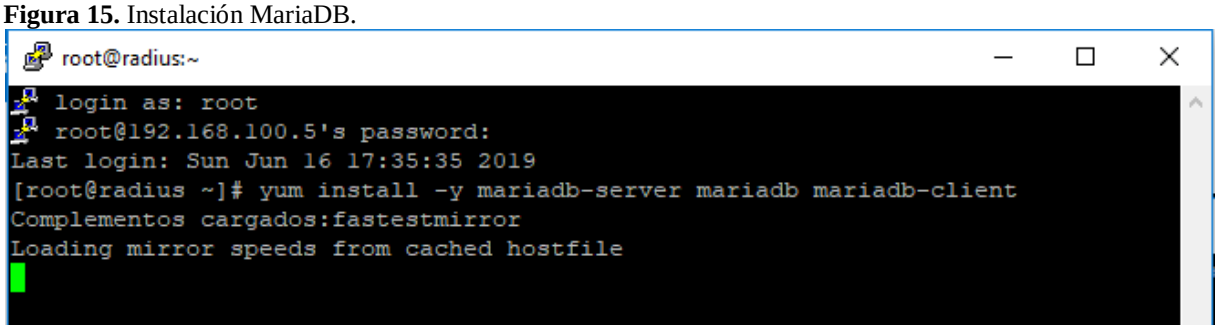



**Fuente:** El investigador.

### 10.2.5.2. Actualizar el sistema e instalar MariaDB

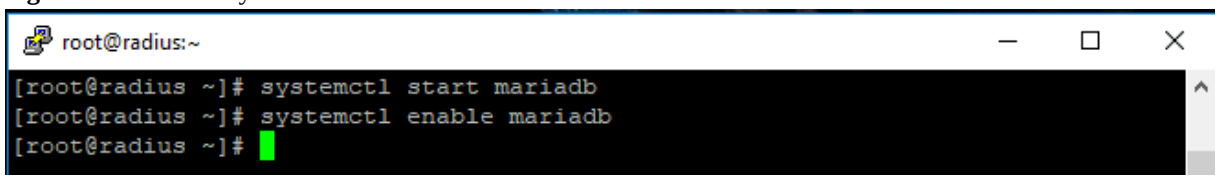
La actualización es necesaria para que el repositorio de MariaDB que acabamos de crear pueda ejecutarse en modo comando, seguido instalamos MariaDB servidor y cliente, véase en la figura 15.

**Figura 15.** Instalación MariaDB.




**Fuente:** El investigador.

**Figura 16.** Iniciamos y habilitamos MariaDB.

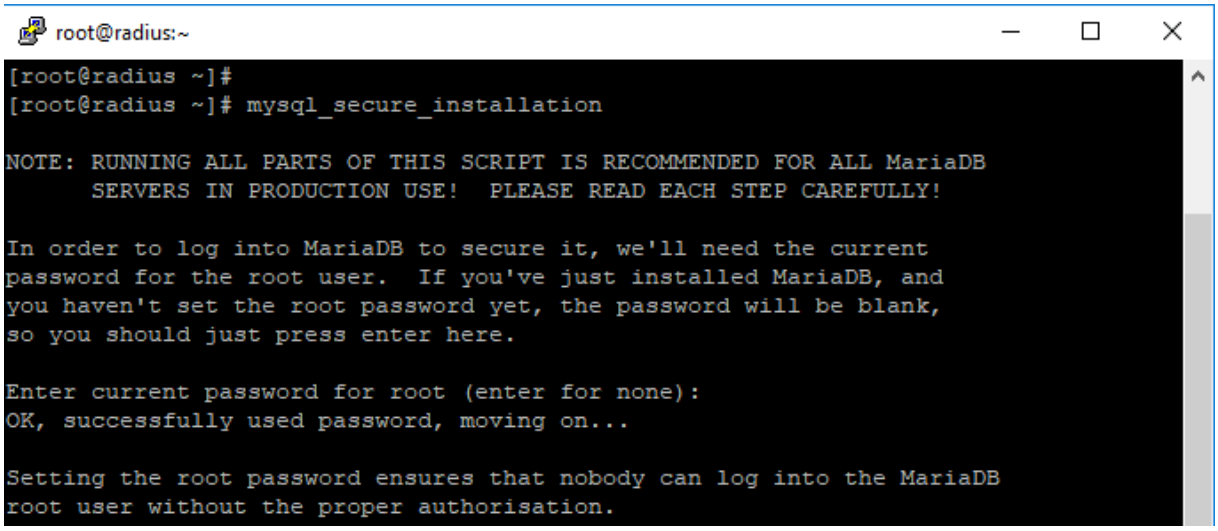



**Fuente:** El investigador.

### 10.2.5.3. Configuración de los ajustes iniciales de MariaDB.

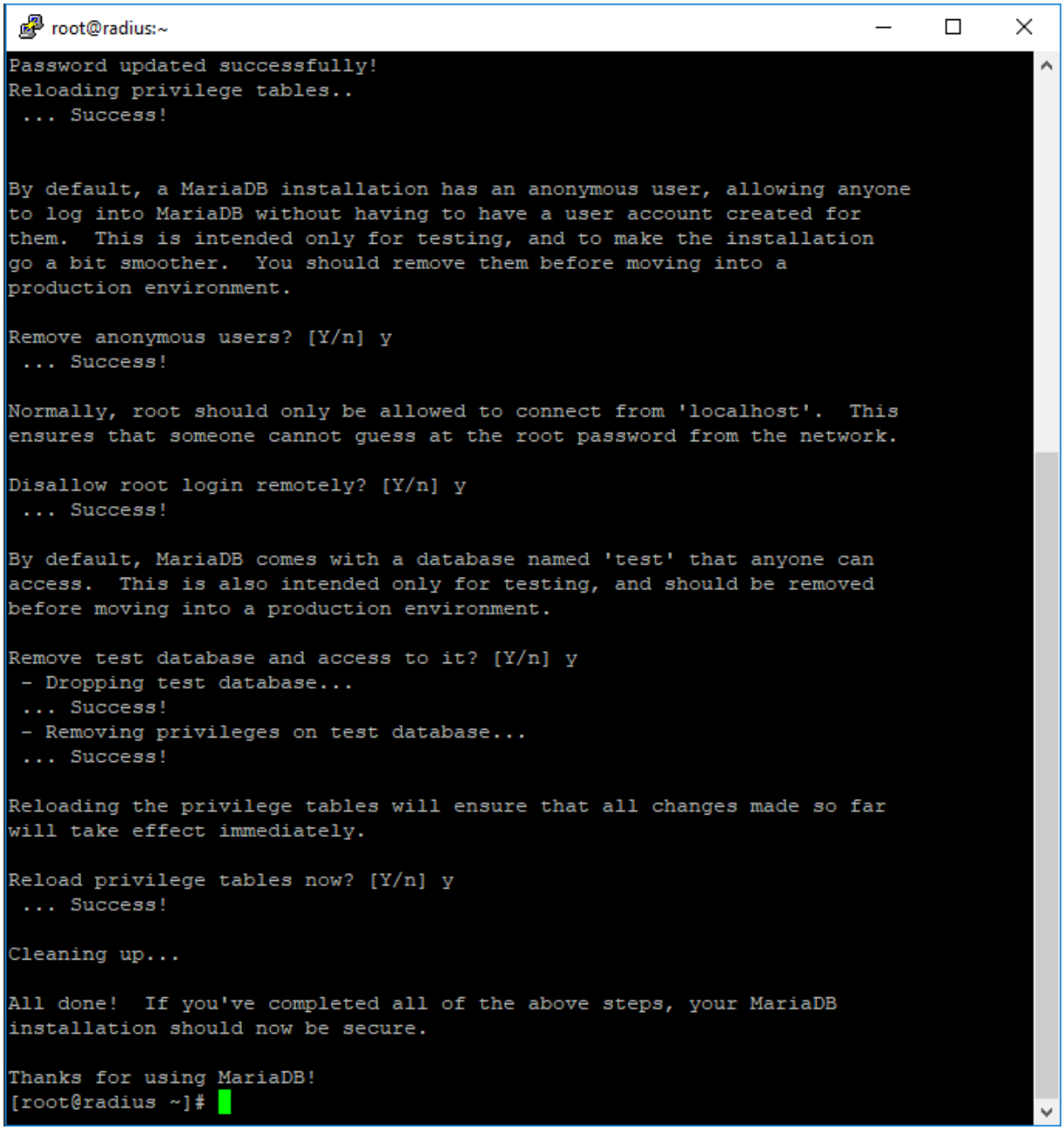
En este paso vamos a establecer la contraseña de root. Hay que tomar en cuenta que por motivos de seguridad, debemos considera eliminar usuarios anónimos y también deshabilitar el inicio de sesión remoto como un mecanismo de seguridad. Para todas estas configuraciones solo debemos escribir Y para la configuración recomendada. Véase en las figuras 17 y 18.

**Figura 17.** Configuración MariaDB.




**Fuente:** El investigador.

**Figura 18.** Configuración MariaDB.

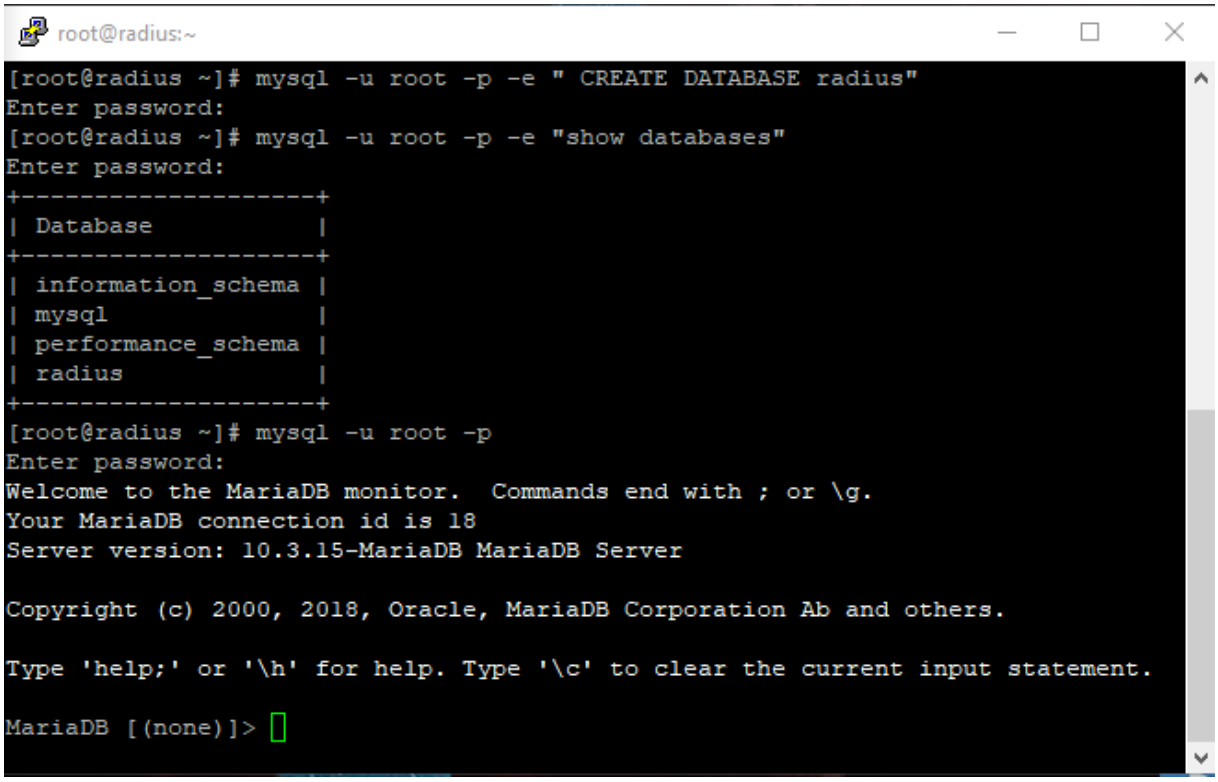



**Fuente:** El investigador.

## Configuración la base de datos para freeradius

Para la conexión y ejecución de FreeRadius debemos crear la base de datos llamada en este caso "radius" al mismo tiempo configuramos el identificador para la conexión la cual es "radiuswfpassword" como se muestra en la figura 19.

**Figura 19.** Creación de BDD para FreeRadius.



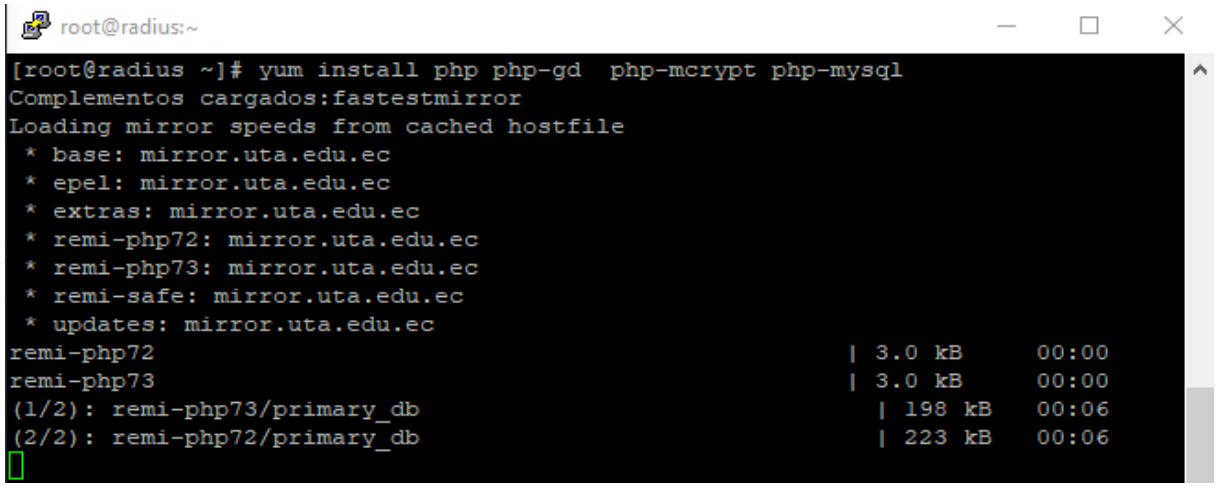

**Fuente:** El investigador.

### 10.2.6. Instalación de php 7

PHP 7 es un requisito para facilitar el manejo de los servicios.

La instalación de este paquete se desarrolla tal cual se muestra en la figura 20.

**Figura 20.** Instalación php 7.

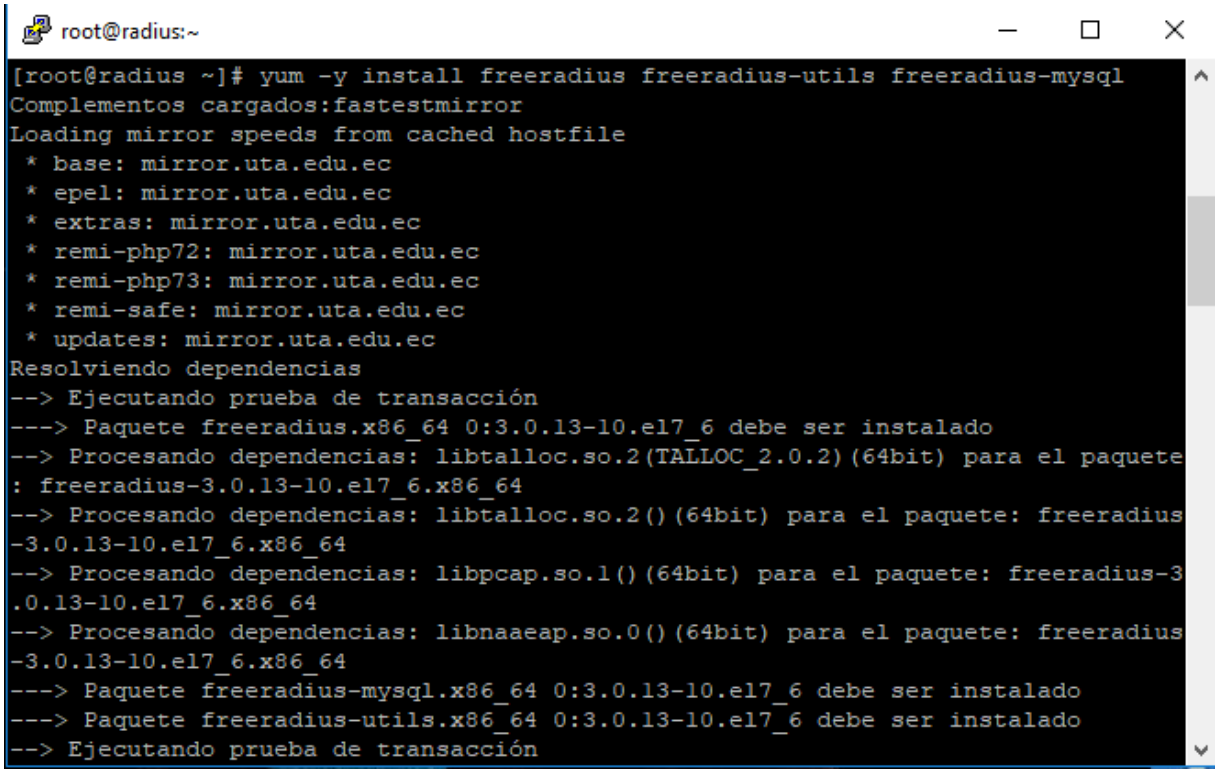



**Fuente:** El investigador.

### 10.2.7. Instalación de FreeRadius

Una vez que tenemos instalado todos los requerimientos para el funcionamiento correcto de FreeRadius vamos a continuación instalarlo con la siguiente línea de comando se instalara freeradius, friradius-utils y freeradius-mysql como se ve en la figura 21.

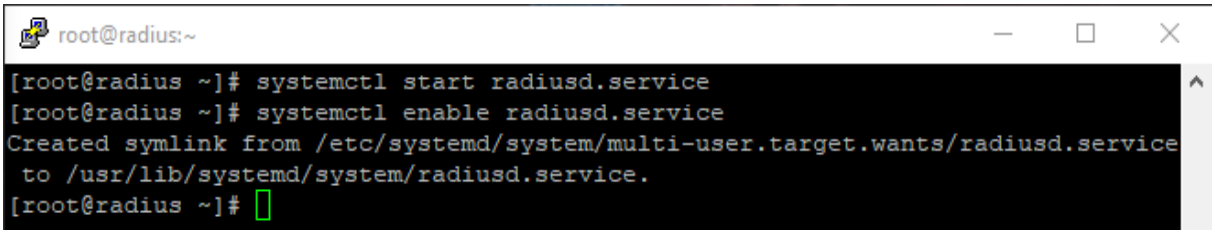
**Figura 21.** Instalación de FreeRadius.




**Fuente:** El investigador.

Debemos iniciar y habilitar freeradius una vez la instalación sea exitosa con los siguientes comandos que se puede visualizar en la figura 22.

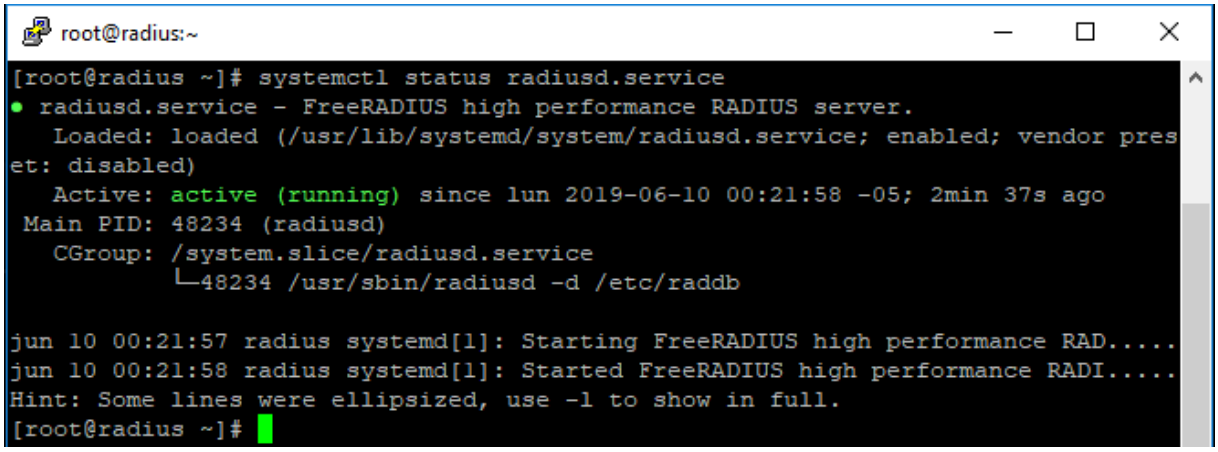
**Figura 22.** Habilitar el servicio radiusd.




**Fuente:** El investigador.

En la figura 23, consultaremos el estado para asegurarnos que esté funcionando correctamente el servicio radiusd.

**Figura 23**. Verificamos el estado de servicio radiusd.

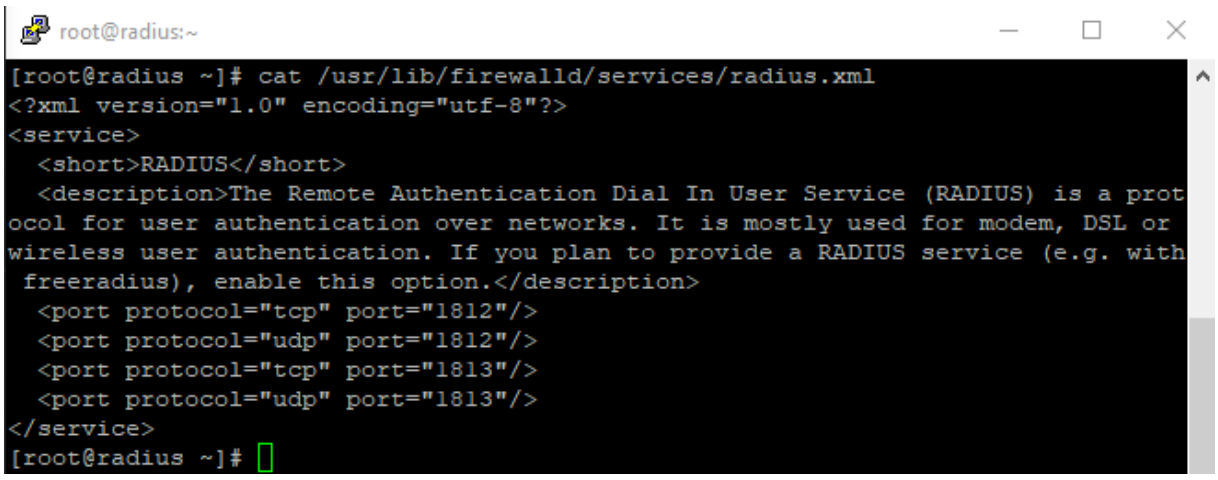



**Fuente:** El investigador.

Con el servidor Radius listo para su uso tenemos que configurar firewalld para permitir la entrada y salida de los paquetes de radius y httpd.

Como lo mencionamos anteriormente en la fundamentación científico técnica los servidores Radius usan los puertos udp 1812 y 1813. Para lo cual podemos constatarlo al ver el contenido del archivo radius.xml en la siguiente dirección /usr/lib/firewalld/services/radius.xml. Usted puede mostrar como salida este archivo y ver, véase en la figura 24.

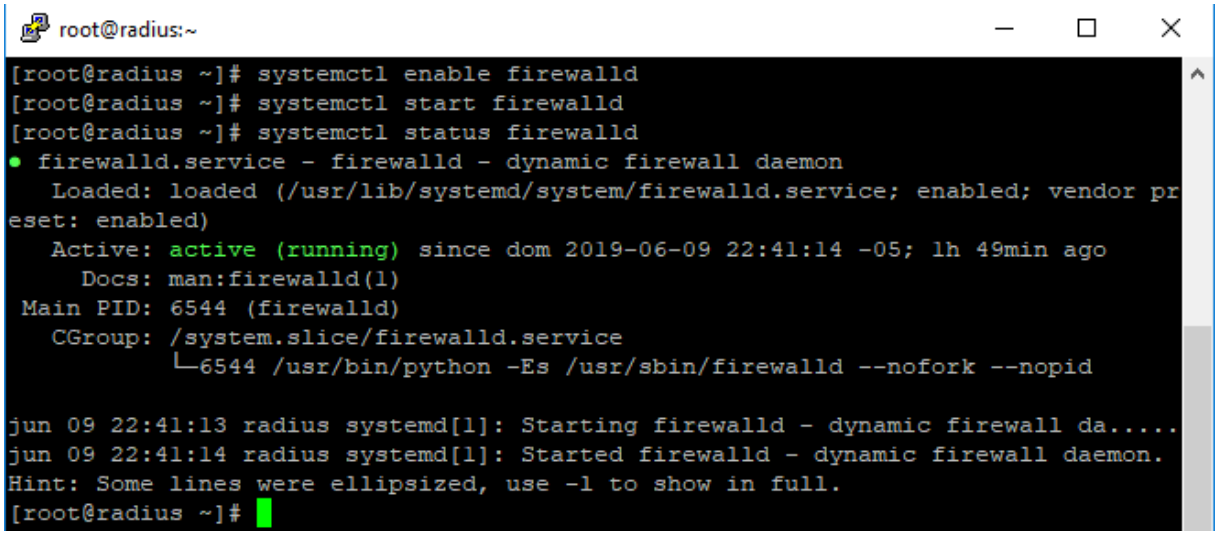
**Figura 24.** Verificación de puertos.




**Fuente:** El investigador.

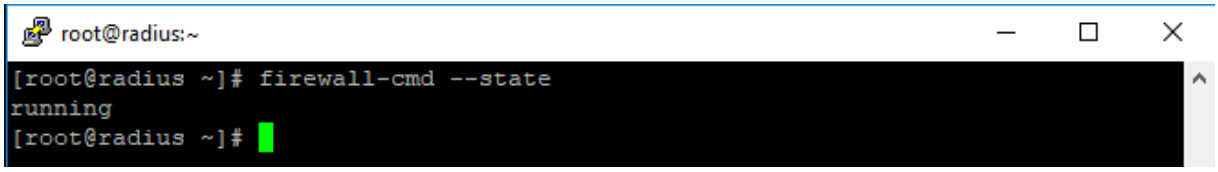
Verificado los puertos, a continuación iniciamos, habilitamos y verificamos el estado de firewalld para seguridad, véase en la figura 25.

**Figura 25.** Iniciar, habilitar, verificar estado de servicio firewalld.




**Fuente:** El investigador.

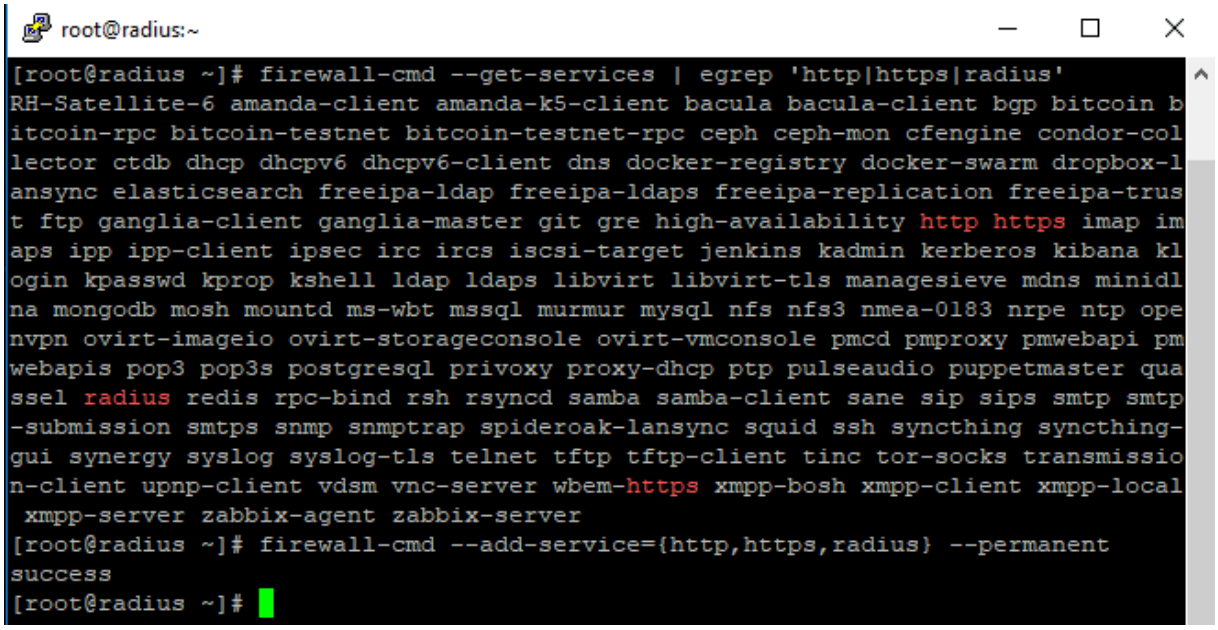
**Figura 26.** Confirma que firewalld está funcionando correctamente.




**Fuente:** El investigador.

En este paso agregamos reglas que deben ser permanentes a la zona predeterminada para permitir los servicios de http, https y radius como podemos ver en la figura 27.

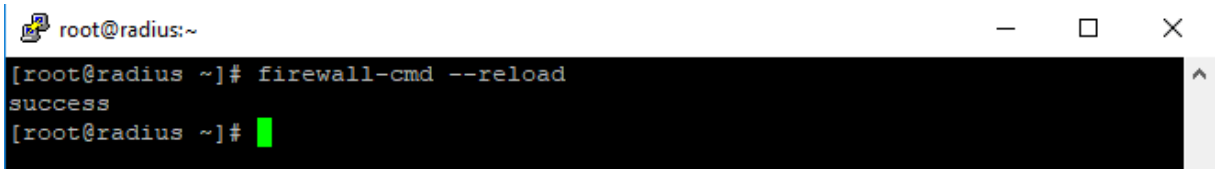
**Figura 27.** Reglas para http, https, radius.




**Fuente:** El investigador.

Seguido recargue firewalld para que los cambios hagan efecto, véase en la figura 28.

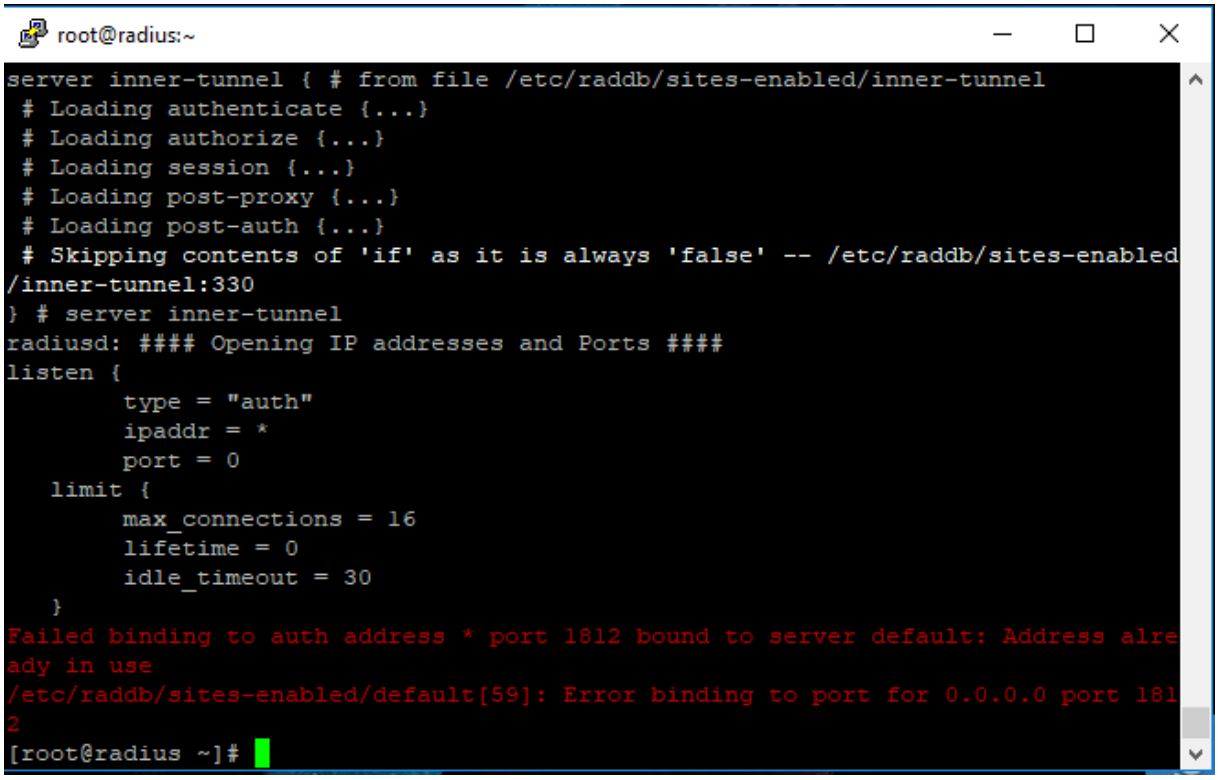
**Figura 28.** Recargar firewall.




**Fuente:** El investigador.

Si deseamos ejecutar el servidor de radius en modo de depuración. Puede ejecutar este comando **radiusd -X** en caso de que el modo de depuración no se puede enlazar a los puertos, puede ser que primero deba matar a el proceso del servidor de radio. Por lo cual obtendremos este tipo de masaje porque su servidor radius no puede enlazar el puerto como lo vemos en la figura 29.

**Figura 29.** Ejecutar servidor radius en modo depuración.



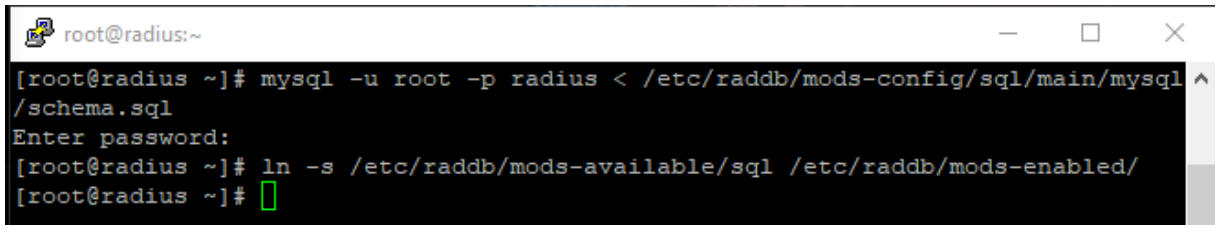

**Fuente:** El investigador.

### 10.2.8. Configuración FreeRadius

La configuración de FreeRarius para usar MariaDB, puede seguir una secuencia que la exponemos a continuación.

Tenemos que importar el esquema de base de datos de Radius para poder completar la base de datos de radius. En primer lugar, tenemos que crear un enlace flexible para SQL en **/ etc / raddb / mods-enabled**, como se muestra en la figura 30.

**Figura 30.** Crear un enlace flexible para SQL.




**Fuente:** El investigador.

En seguida configuraremos el servidor freeRadius para usar el servidor de base de datos. Esto lo podemos hacer abriendo el archivo de le configuración **/ raddb / mods-available / sql** usando el editor de texto vi.

Los pasos a seguir son:

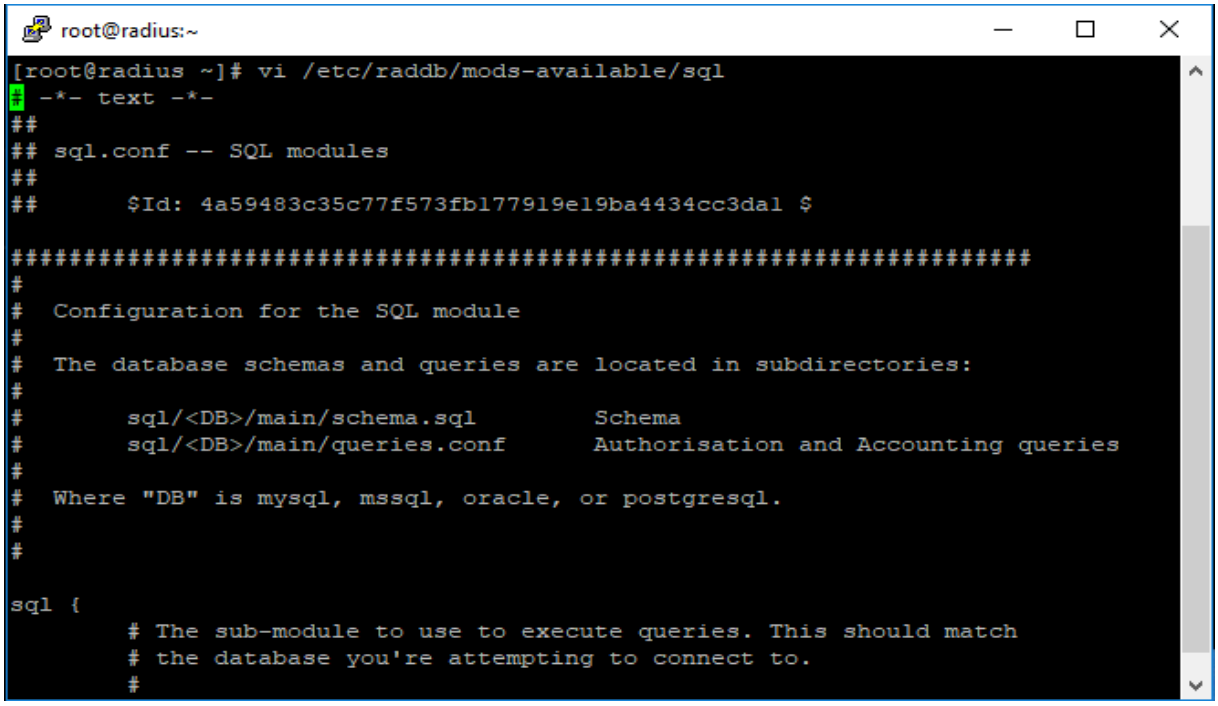
- Cambiar **driver = "rlm_sql_null"** por **driver = "rlm_sql_mysql"**
- Cambiar **dialect = "sqlite"** por **dialect = "mysql"**
- Descómete **server, port, login y password** eliminando **#** del principio de la línea, así como cambiando **password = "radpass"** a **password = "radiuspassword"**.
- Descómete la línea **read_clients = yes**, eliminando # del principio de la línea.

Las otras líneas ya las encontramos configuradas de acuerdo con nuestras necesidades, con lo que podemos guardar y cerrar el archivo cuando hayamos terminado. Sin embargo, puede verificar que todo esté en orden. El archivo sql debería tener un aspecto similar al siguiente, aunque lo podremos ver que en el documento es más largo debido a las instrucciones y otras líneas que están comentadas.

```
sql {
        driver = "rlm_sql_mysql"
        dialect = "mysql"

        # Connection info:

        server = "localhost"
        port = 3306
        login = "radius"
        password = "radiuspassword"

        # Database table configuration for everything except Oracle

        radius_db = "radius"
}
        # Set to ‘yes’ to read radius clients from the database (‘nas’ table)
        # Clients will ONLY be read on server startup.
        read_clients = yes

        # Table to keep radius client info
        client_table = “nas”
```

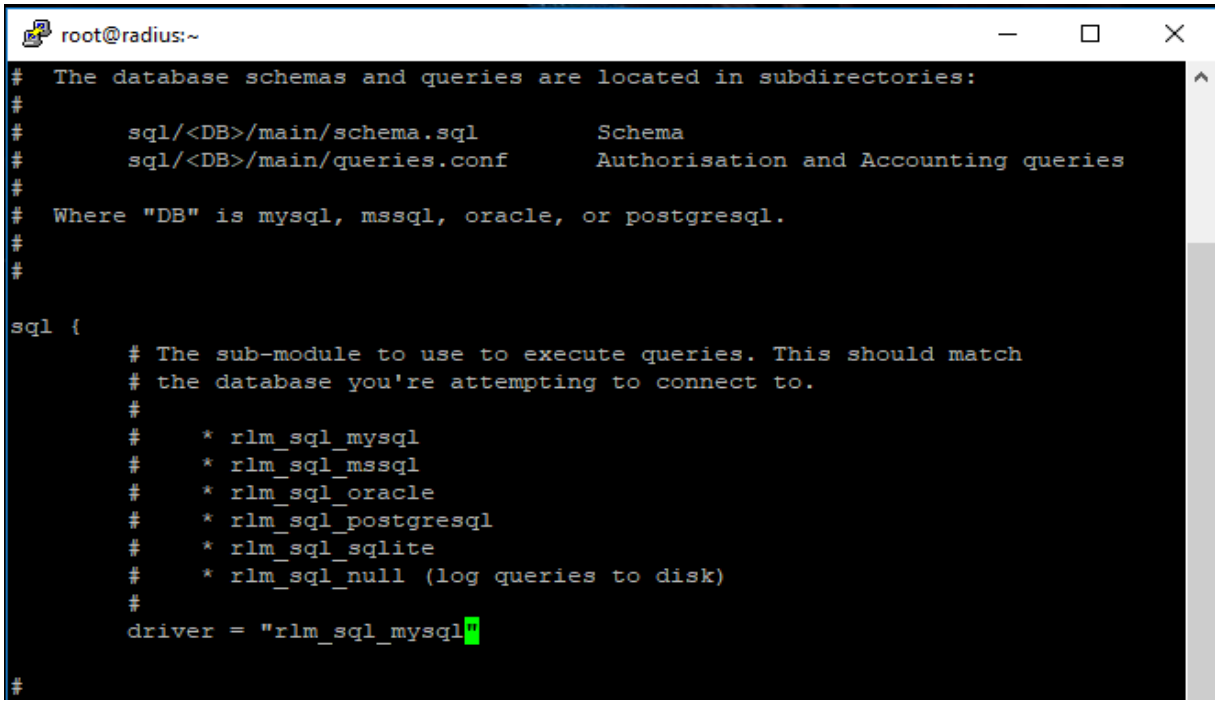
En las figuras 31, 32, 33 y 34 es posible apreciar la configuración del archivo sql.

**Figura 31.** Configuración de FreeRADIUS para usar MariaDB.



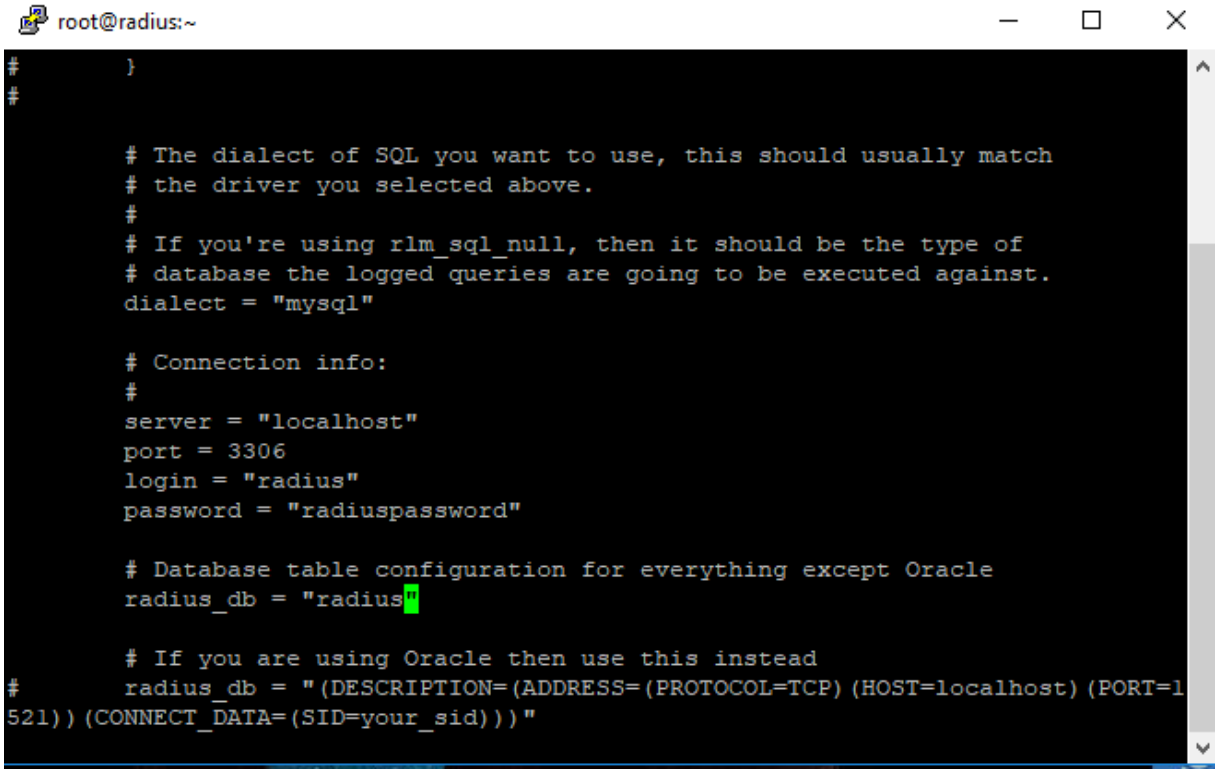

**Fuente:** El investigador.

**Figura 32.** Configuración de driver.



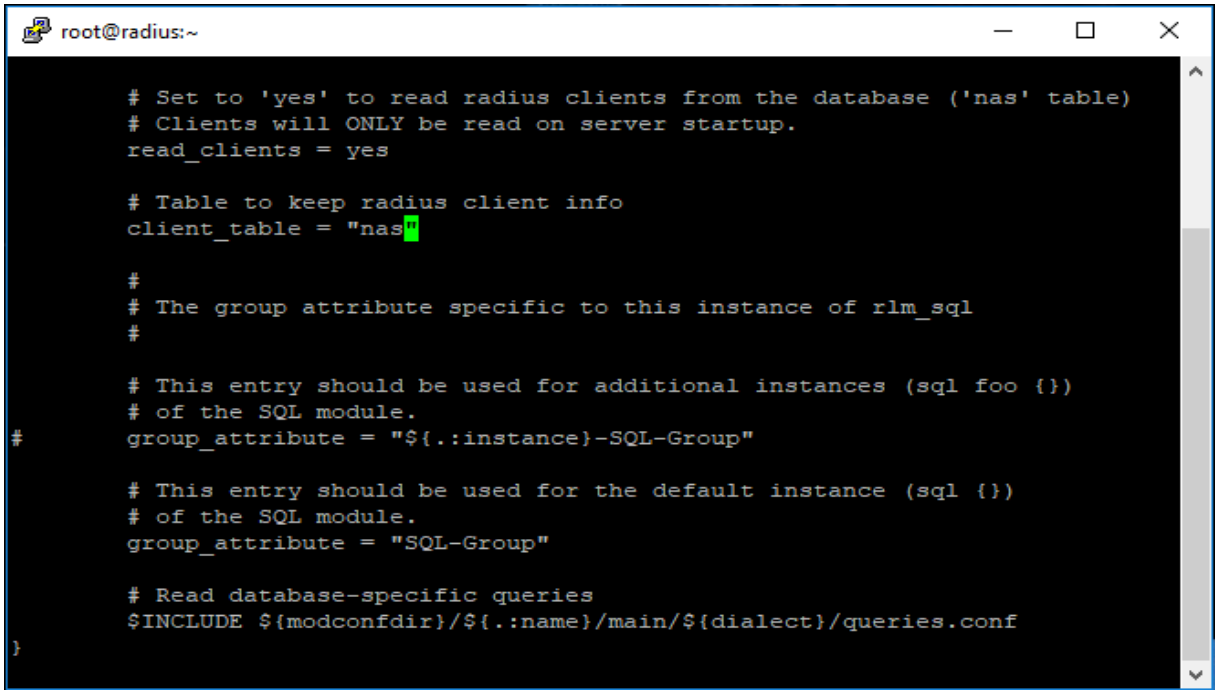

**Fuente:** El investigador.

**Figura 33.** Configuración de conexión con MariaDB.




**Fuente:** El investigador.

**Figura 34.** Ajuste de lectura de clientes radius.




**Fuente:** El investigador.

En la figura 35, Luego de la configuración finalmente, cambiamos los derechos de grupo de **/ etc / raddb / mods-enabled / sql** a radiusd.

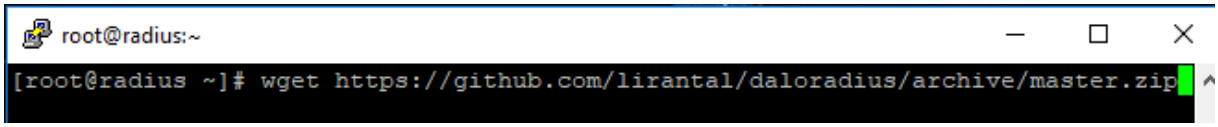
**Figura 35.** Cambiar grupo de usuario.


**Fuente:** El investigador.

### 10.2.9. Instancian y Configuración Daloradius

Podemos utilizar el administrador web Daloradius para comunicarnos con nuestro servidor radius, la cual nos permite configurar y administrar de una manera más practica el servidor radius es totalmente opcional y no se debe realizar antes de instalar FreeRadius. Descargaremos daloradius de los repositorios de github como se ve en la figura 36.

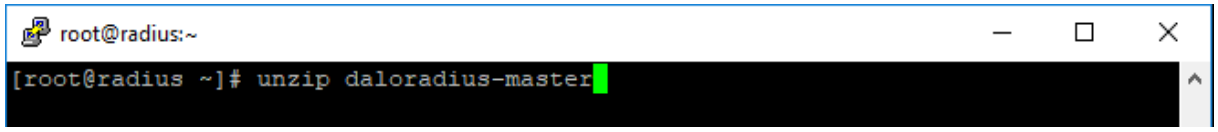
**Figura 36.** Repositorio de Daloradius.




**Fuente:** El investigador.

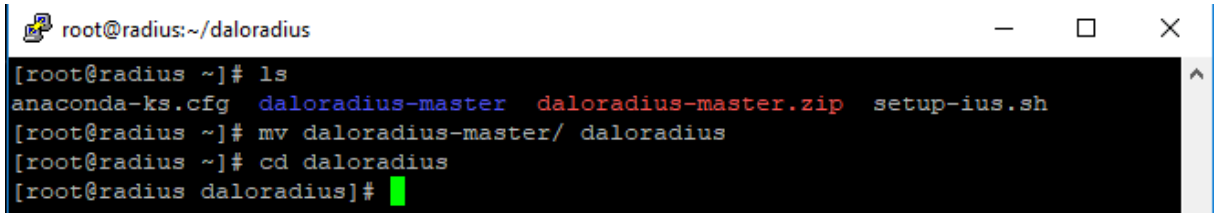
En las figura 37, 38, Descomprimimos la descarga y nombramos Daloradius, en el terminal se realiza una copia de este programa, se cambia su propietario y los permisos haciendo uso de los siguientes comandos.

**Figura 37.** Descomprimir daloradius.




**Fuente:** El investigador.

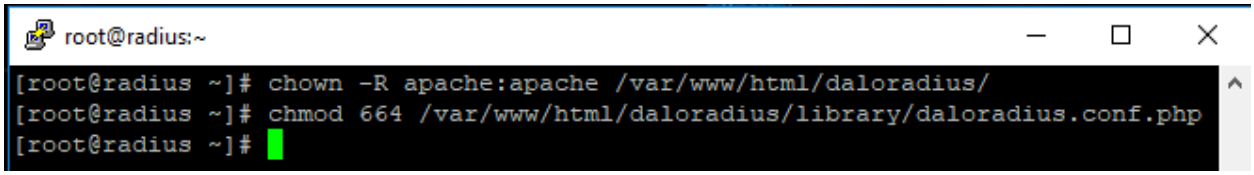
**Figura 38.** Movemos a la carpeta daloradius.




**Fuente:** El investigador.

Es necesario cambiar los permisos para la carpeta http y establecer los permisos correctos para el archivo de configuración de daloradius, véase en la figura 39.

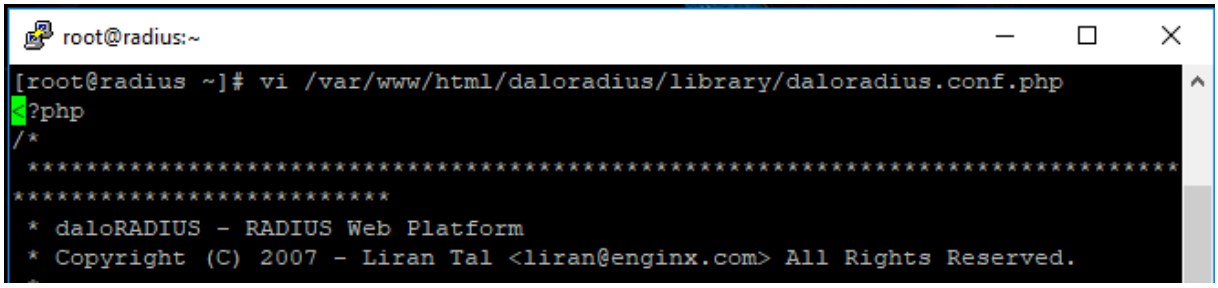
**Figura 39.** Cambiamos el propietario para la configuración de daloradius.




**Fuente:** El investigador.

Casi para terminar tenemos que modificar el archivo daloradius.conf.php para realizar ajustes en la información de la base de datos MariaDB. Así que abramos el archivo daloradius.conf.php y agreguemos el nombre de usuario, la contraseña y el nombre de la base de datos como se presenta en la figura 40.

**Figura 40.** Ajustes de información de la base de datos.



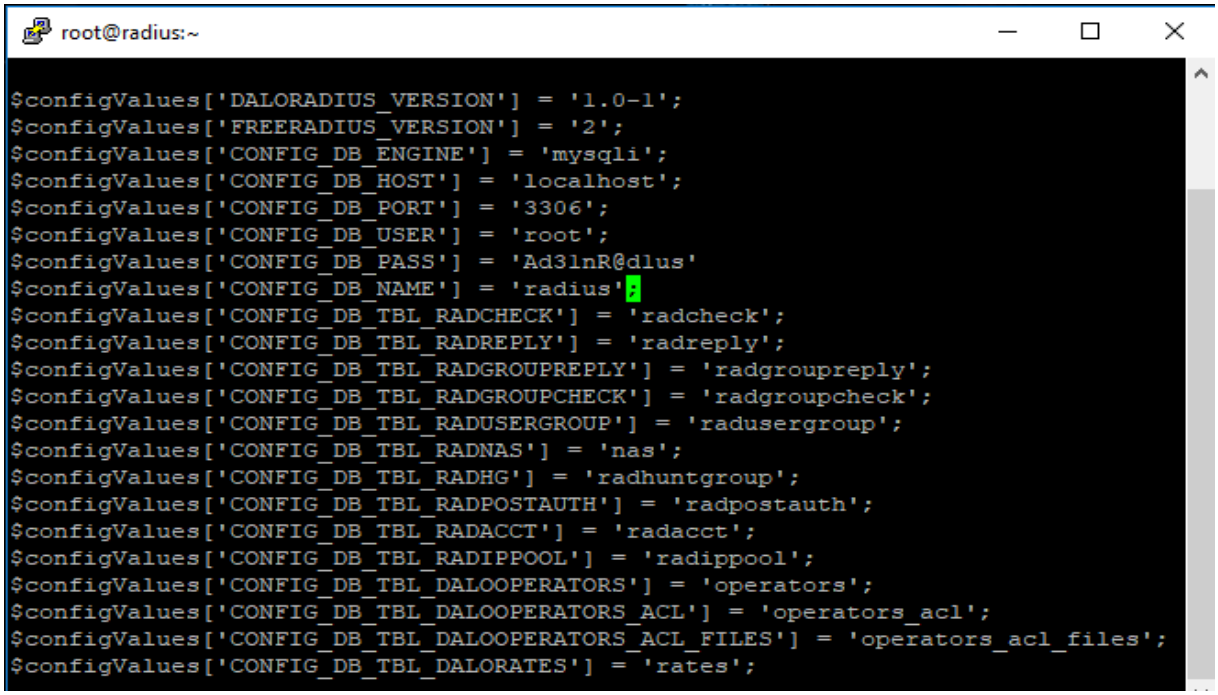

**Fuente:** El investigador.

La configuración que más debemos tomar en cuenta relevantes para configurar son 3:

CONFIG_DB_USER = ‘ ’;
CONFIG_DB_PASS = ‘ ’;
CONFIG_DB_NAME = ‘ ‘;

La configuración completa podemos plasmarla en la figura 41.

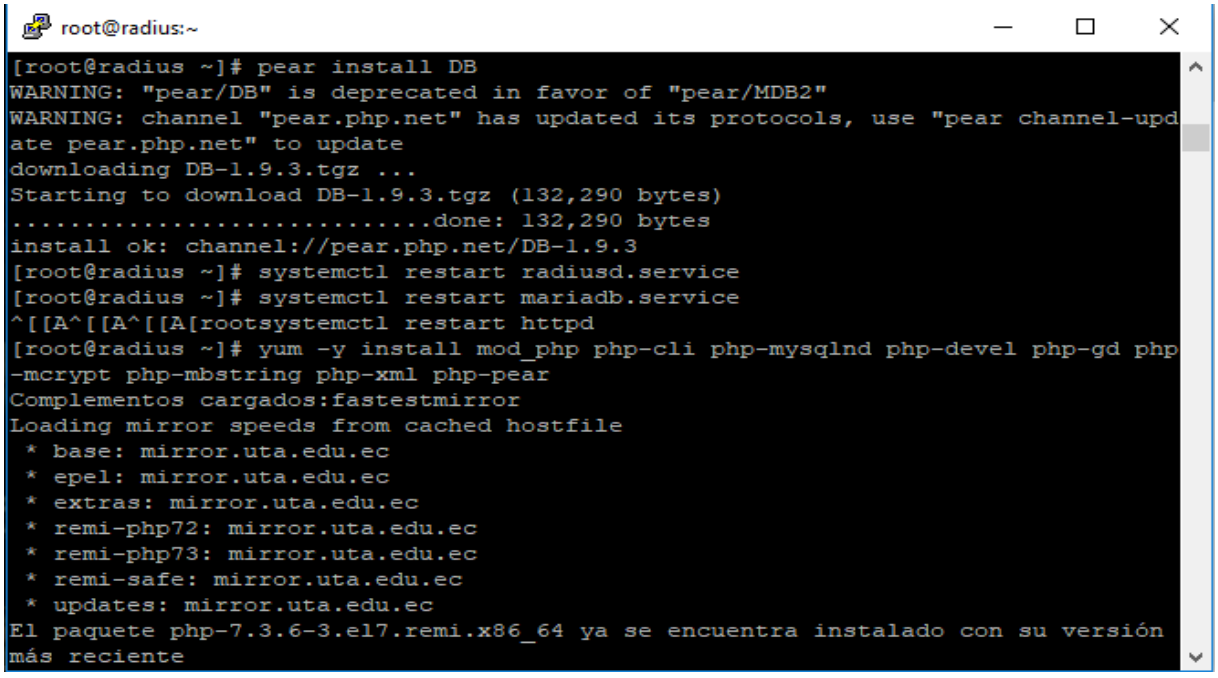
**Figura 41.** Configuración de conexión con la base de datos.




**Fuente:** El investigador.

Una particularidad es que si tenemos instalado php 7, puede ignorar la instalación de php-pear. Y solo tienes que ejecutar pear install DB como se muestra en la figura 42.

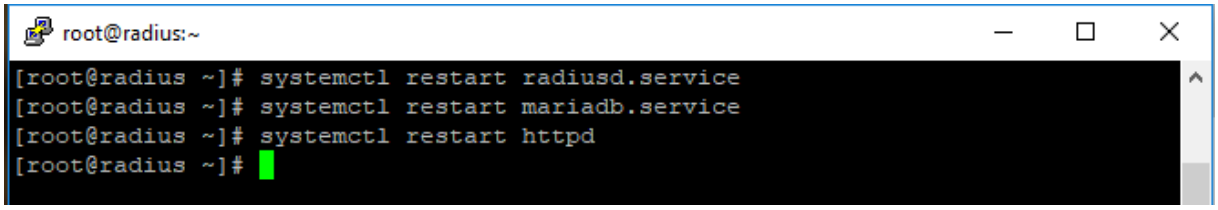
**Figura 42.** Instalación de php-pear.




**Fuente:** El investigador.

Hemos terminado la instalación y configuración de Freeradius, finalmente nos aseguramos que todos los servicios funcionen correctamente para lo cual reiniciamos radiusd, httpd y mysql como lo evidenciamos en la figura 43. Como todos los reinicios fueron exitosos tenemos listo un servidor AAA con el protocolo de libre uso RADIUS para poner en producción con el Wireless Lan Controller y sincronizar con los Access point del GAD municipal de Mejía.

**Figura 43.** Reiniciar los servicios radiusd, mariadb, httpd.




**Fuente:** El investigador.

### 10.2.10. Administrador web

Una vez completado la instalación y configuración de daloradius y freeradius. Podemos ya ha administrar nuestro servidor radius mediante una interfaz gráfica, para acceder a daloradius, debemos abrir navegador web y digitar su dirección IP, al instante obtendremos el panel de control del radius, como lo muestra la figura 44.

Por defecto las credenciales de acceso son:

Username: **administrator**

Password: **radius**

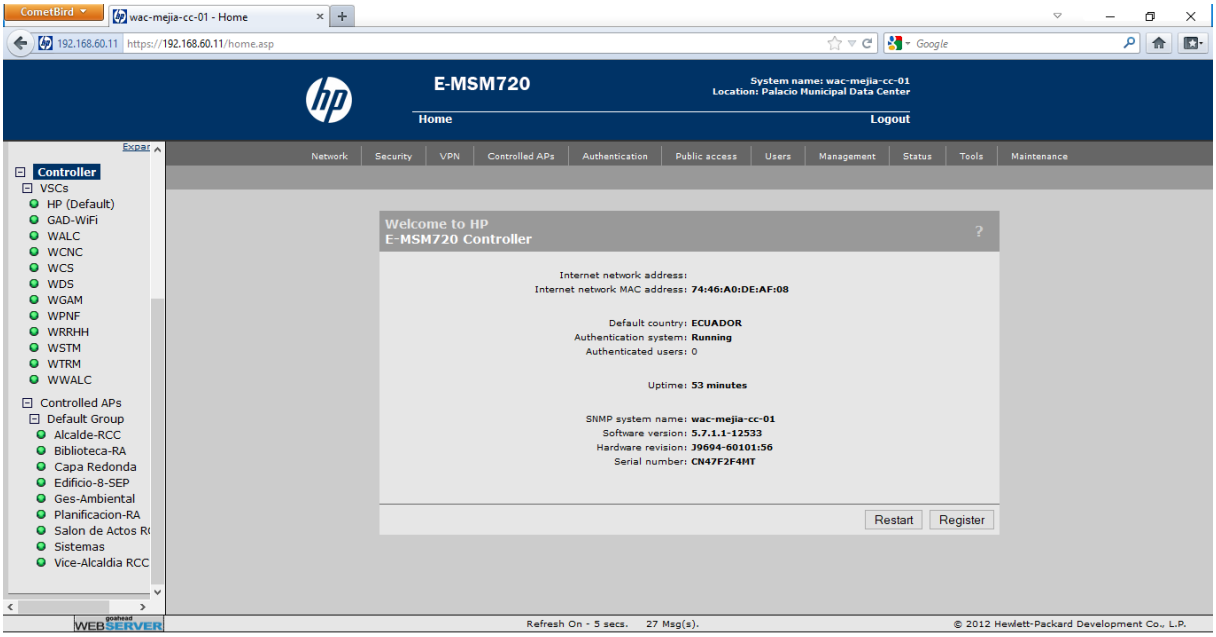
**Figura 44.** Administrador web.


**Fuente:** El investigador.

## Configuración de Wireless Lan Controller

Un controlador de Lan inalámbrico es utilizado con ayuda del protocolo de punto de acceso ligero para administrar puntos de acceso livianos en grandes cantidades, este controlador maneja automáticamente la configuración de los puntos de acceso inalámbricos directamente por el administrador de la red, véase en la figura 45.

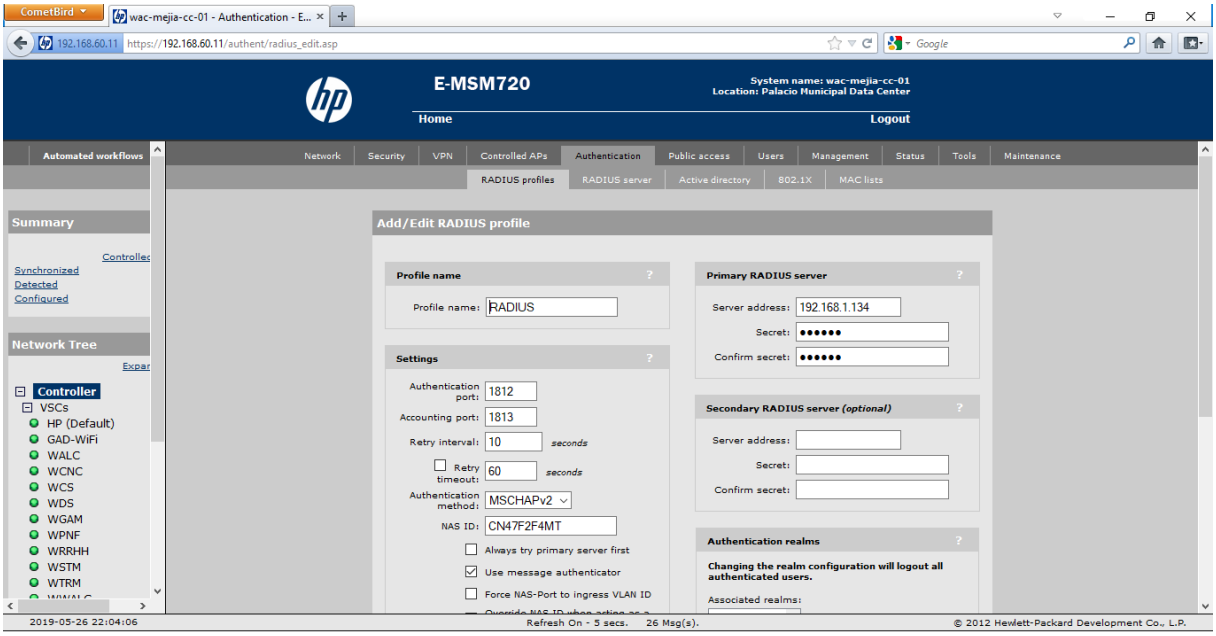
**Figura 45.** Wireless Lan Controller.




**Fuente:** El investigador.

En la figura 46, una vez que ingresamos al controlador como podemos ver que tenemos varios APs reconocidos. Para la conexión en la pestaña **Authentication** debemos crear un perfil con el nombre RADIUS colocamos la dirección IP de nuestro servidor y colocamos la clave que configuramos cuando creamos el cliente también demos asegurarnos que la configuración se encuentre **puerto: 1812** método de **autenticación: MSCHAPv2** y solamente marcado en la casilla de **user message authentication**.

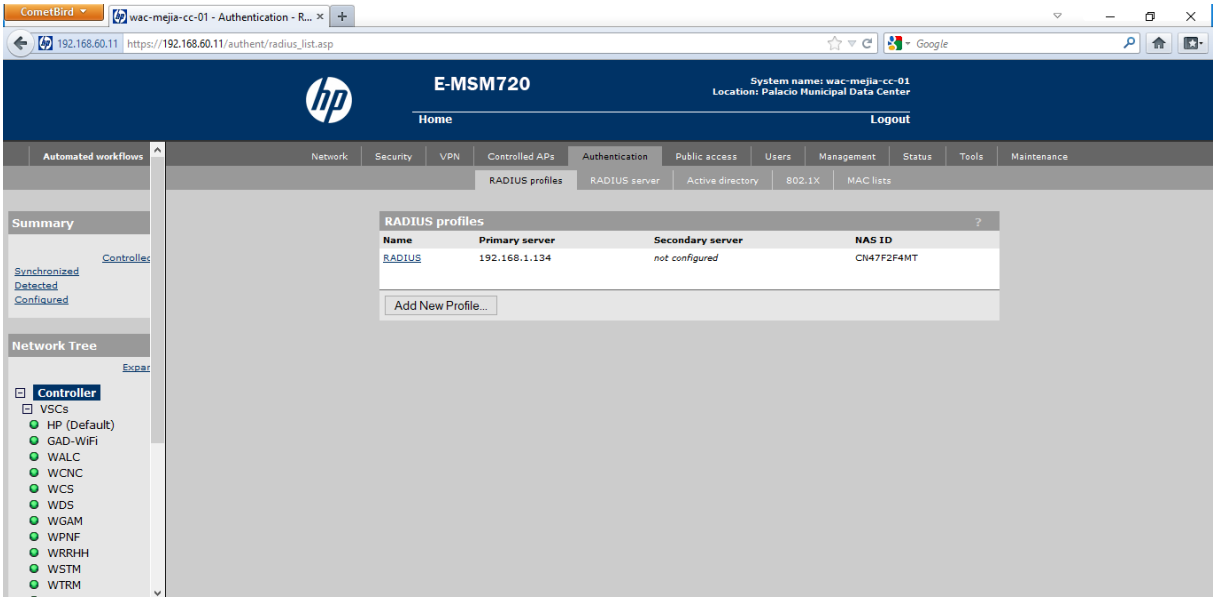
**Figura 46.** Crear perfil para la conexión con el servidor Radius.




**Fuente:** El investigador.

Una vez creado el perfil, nos ubicamos en LAN en la opción **key source** por defecto se encuentra en **Preshared Key** nosotros elijaremos **Dynamic** en Authentication marcamos remote y Radius elegimos el perfil que hemos creado anteriormente con esto estamos conectando al Radius server como podemos ver en la figura 47.

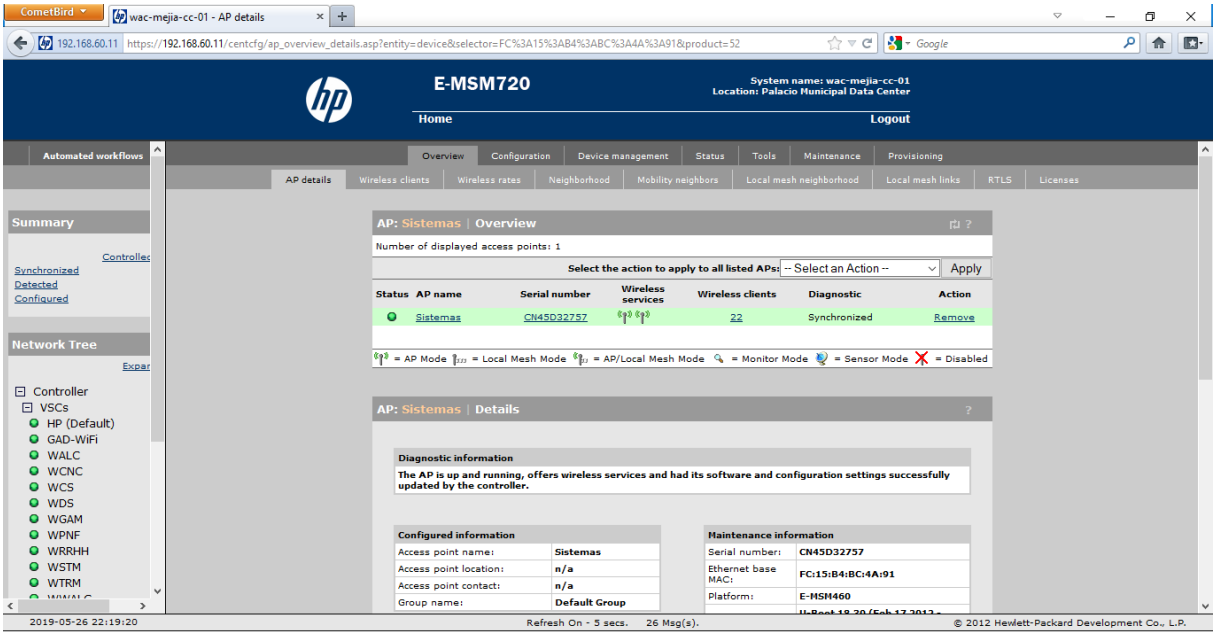
**Figura 47.** Perfil configurado.




**Fuente:** El investigador

Luego sincronizamos nuestros APs para que obtenga las configuraciones del controlador, véase en la figura 48.

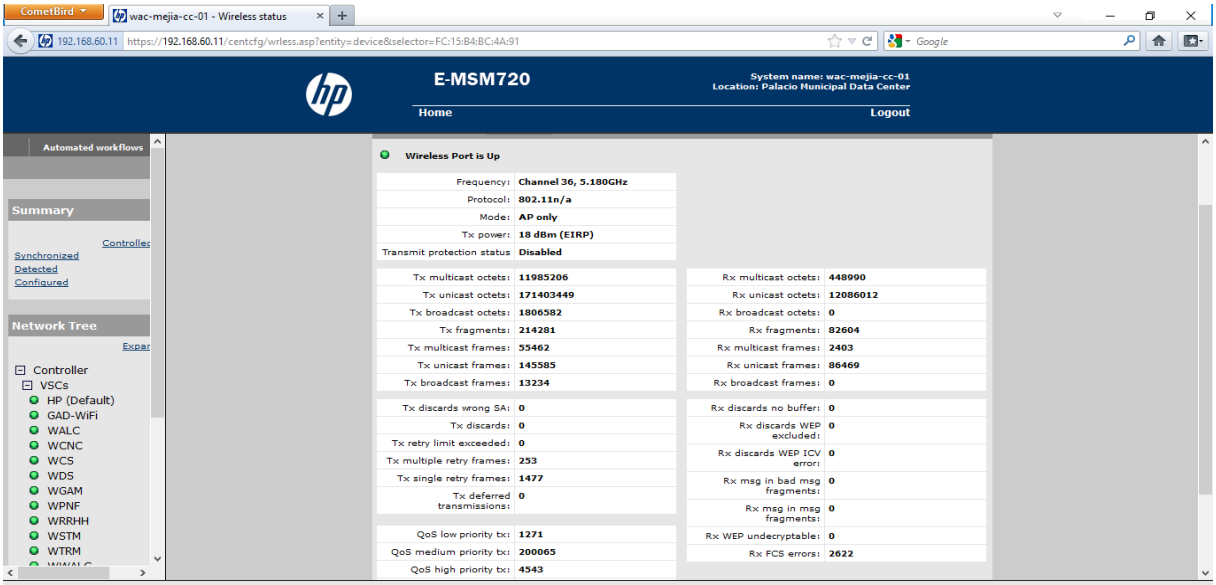
**Figura 48.** Sincronización de los Access point.




**Fuente:** El investigador.

Por ultimo podemos constatar que la sincronización fue efectiva ya que están nos muestra un mensaje del puerto inalámbrico está listo, véase en la figura 49.

**Figura 49.** Verificación de la sincronización.

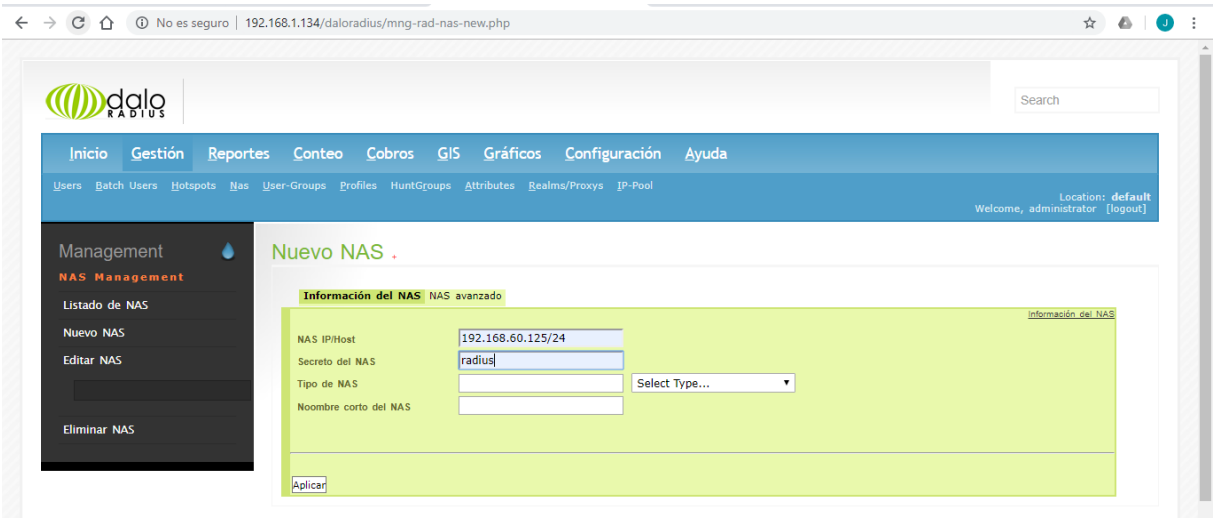



**Fuente:** El investigador.

### 10.2.11. Administración por DaloRadius

En la figura 50, mediante nuestro administrador web vamos añadir nuestro AP al servidor Radius ingresamos a Gestión y a NAS creamos un nuevo NAS con la IP de nuestro access point con el slach de la máscara que está utilizando, también pondremos la clave secreta de comunicación entre el AP y el Radius.

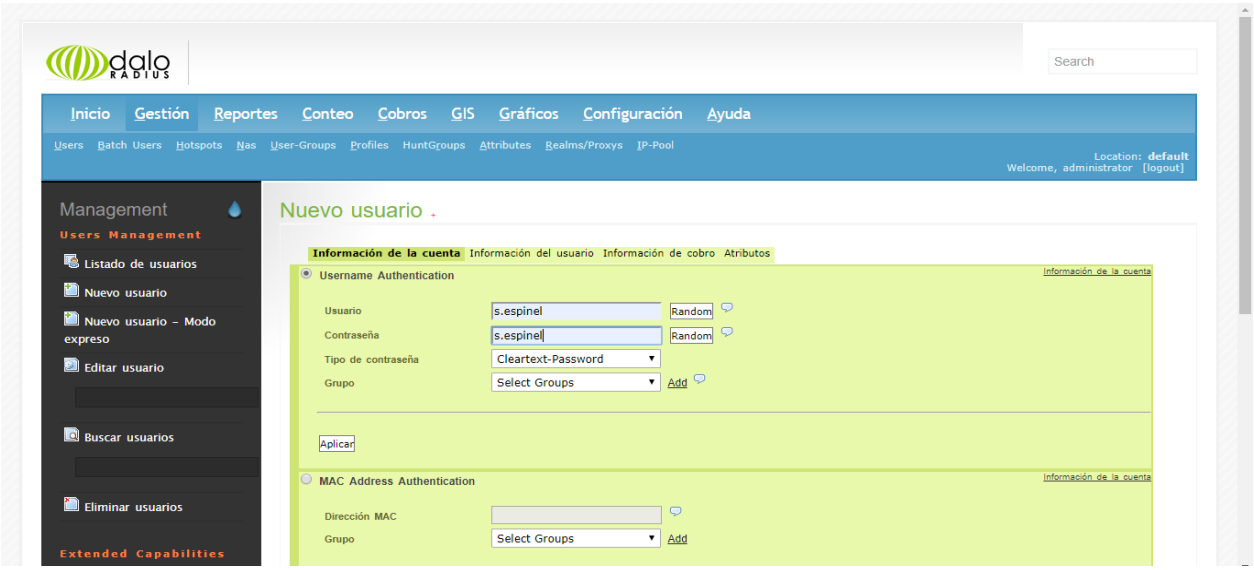
**Figura 50.** Creación de NAS.




**Fuente:** El investigador.

Luego crearemos nuestros usuarios en User, Nuevo usuario como vemos en la figura 51.

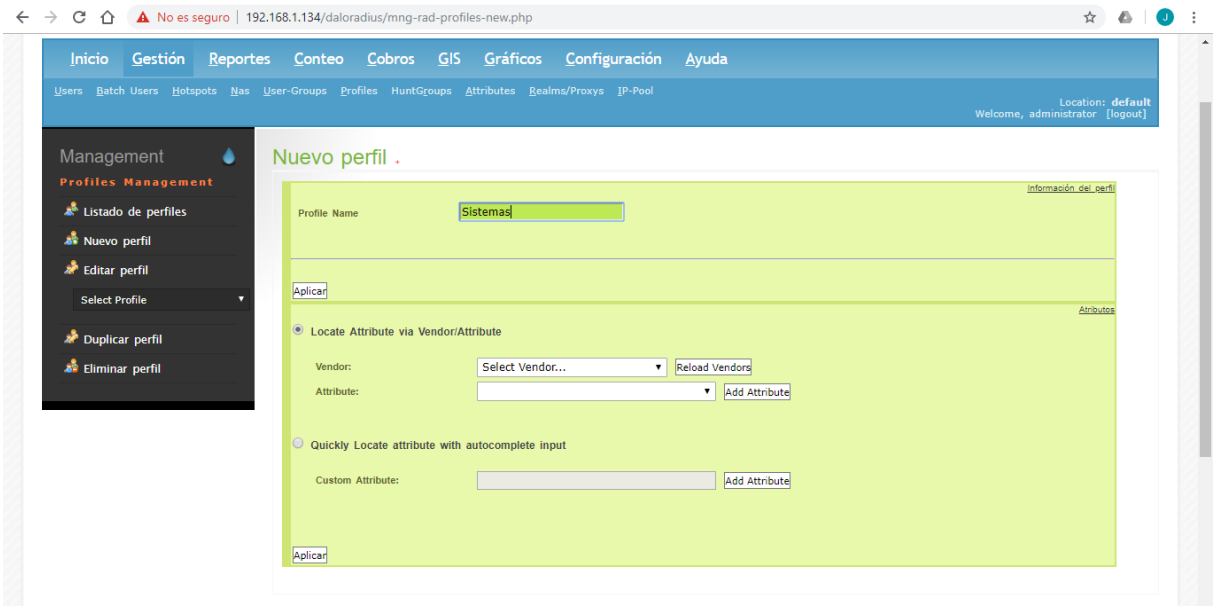
**Figura 51.** Creación de usuarios.




**Fuente:** El investigador.

También crearemos perfiles para nuestros usuarios en perfiles, nuevo perfil como podemos constatar en la figura 52.

**Figura 52.** Creación de Perfiles.




**Fuente:** El investigador.

## 11. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

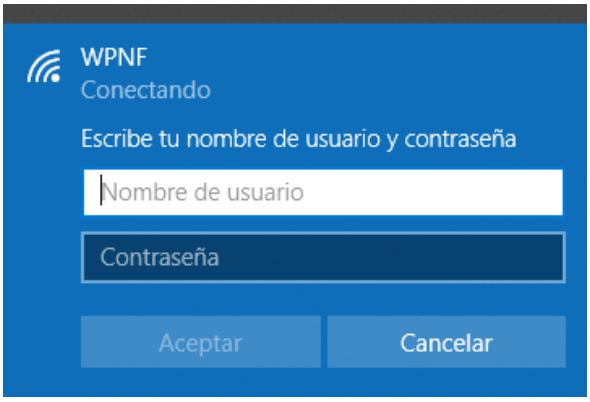
### 11.1. Análisis técnico operativo

#### 11.1.1. Prueba de acceso

Se verifica la que al momento de conectar al punto de acceso se despliega la interfaz gráfica solicitando credenciales usuario y contraseña para la autenticación, esta prueba se realizó posterior a la creación de usuarios en daloRadius

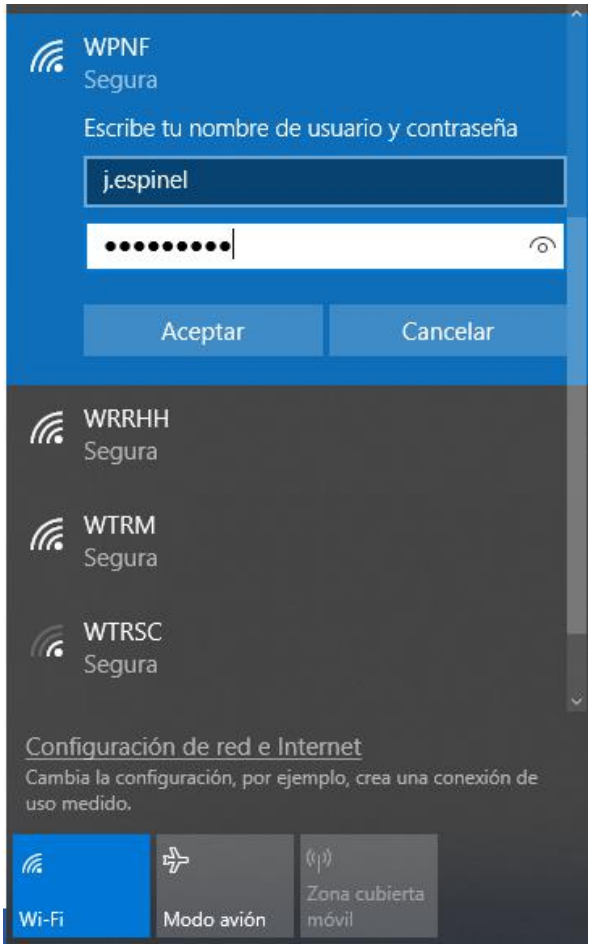
**Prueba 1:** Verificación de solicitud de credenciales con el usuario **j.espinel**, véase en la figura 53, 54 y la conexión exitosa véase en la figura 55.

**Figura 53.** Prueba de verificación.



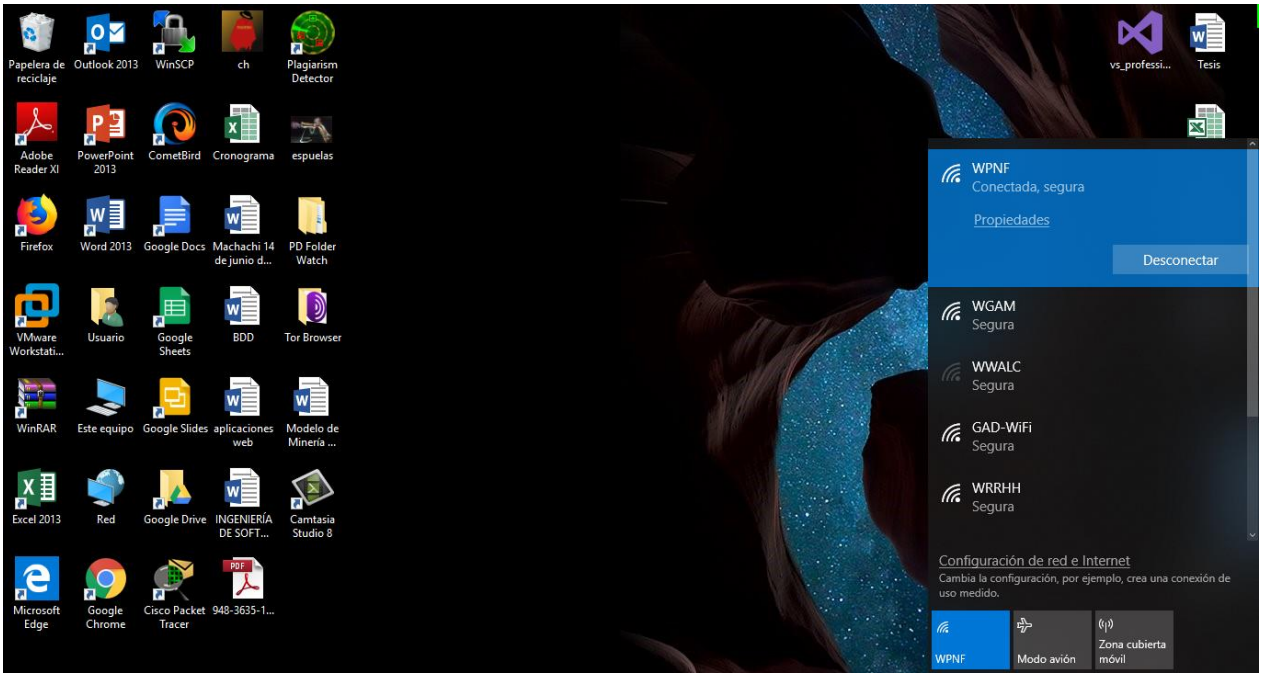

**Fuente:** El investigador

**Figura 54.** Ingreso de credenciales.




**Fuente:** El investigador

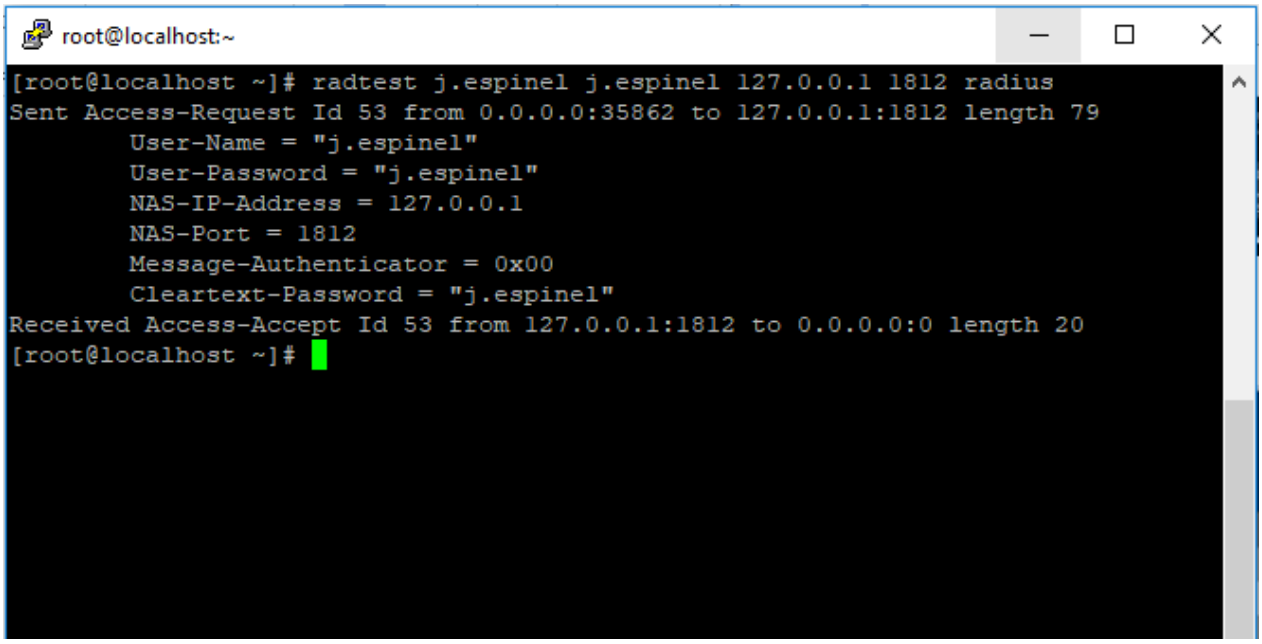
**Figura 55.** Conexión exitosa mediante el protocolo Radius.




**Fuente:** El investigador.

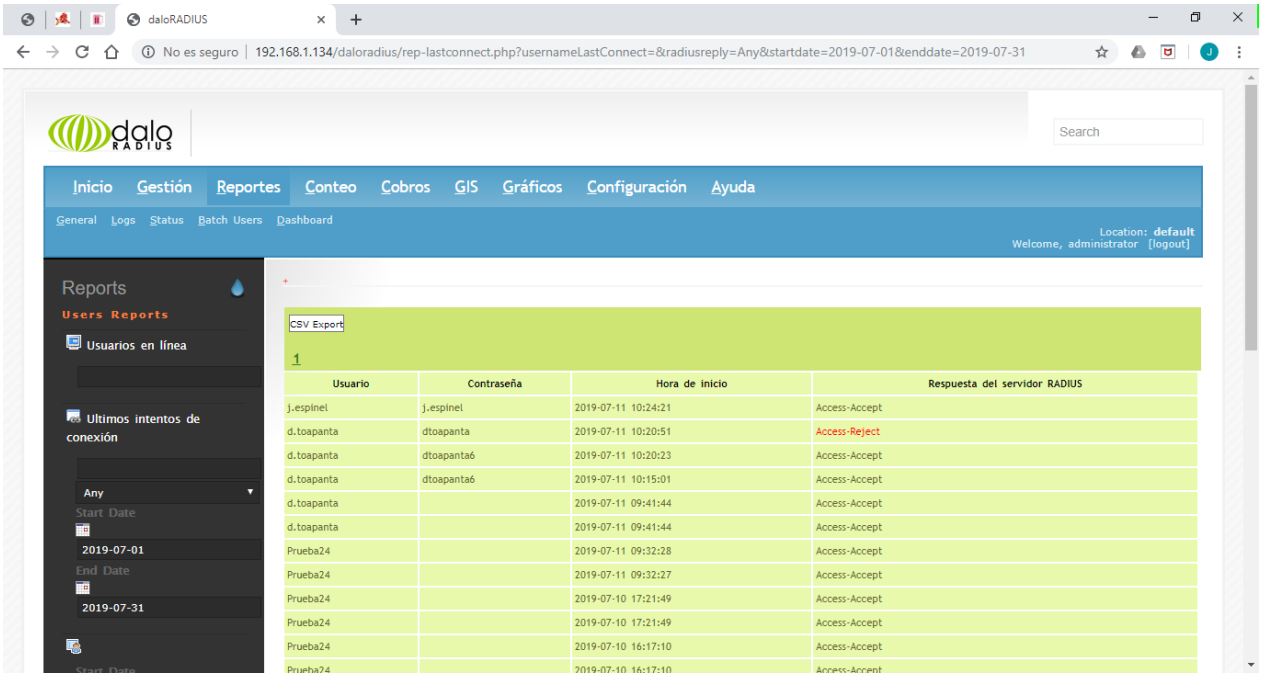
**Prueba 2:** verificación de solicitud de credenciales con el usuario j.espinel mediante línea de comando en el servidor Radius. Véase los resultados en las figuras 56 y 57.

**Figura 56.** Paquete de datos Access-Accept.




**Fuente:** El investigador.

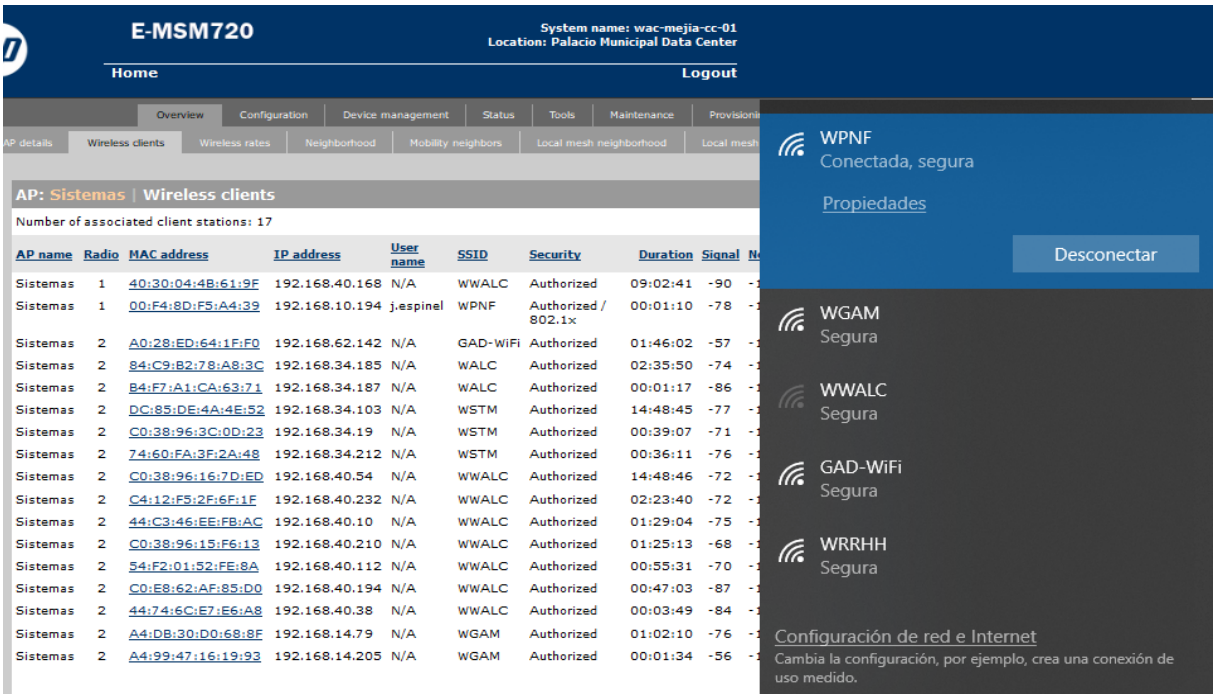
**Figura 57**. Reporte de solicitud de conexión aceptada.




**Fuente:** El investigador.

Figura 58. Se verifica el usuario que al momento está conectado en la red inalámbrica WPNF, las credenciales de usuario fueron la llave para la autenticación exitosa.

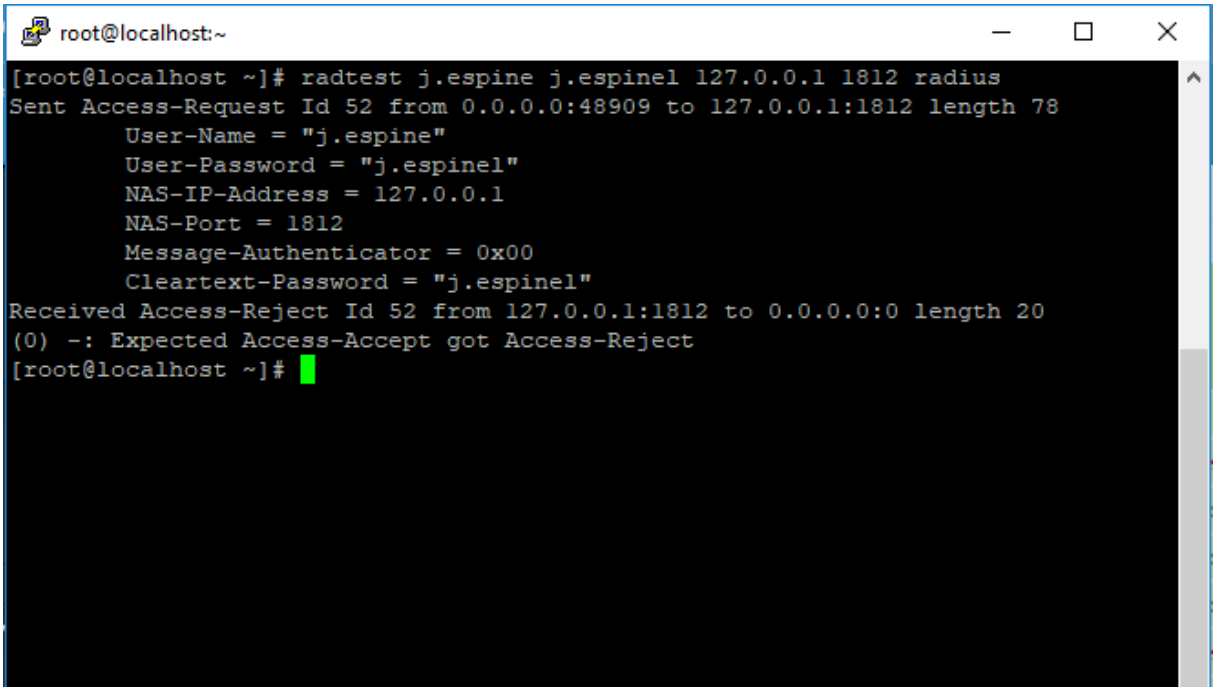
**Figura 58.** Verificación de uso de  protocolo Radius.




**Fuente:** El investigador.

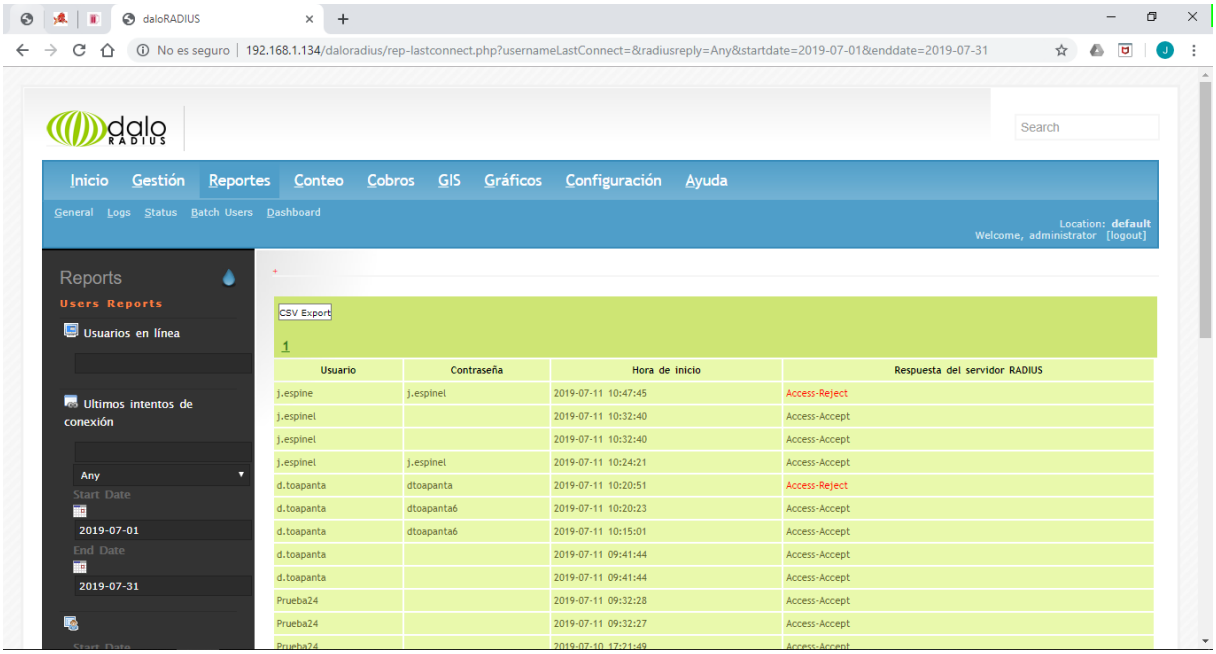
**Prueba 3:** verificación de solicitud de credenciales con el usuario j.espinel mediante línea de comando en el servidor radius pero con la variación que el usuario ingresado es incorrecto por lo cual nos notificara con una solicitud rechazada. Véase los resultados en las figuras 59 y 60.

**Figura 59.** Paquete de datos Access-Reject.




**Fuente:** El investigador.

**Figura 60.** Reporte de solicitud de conexión Rechazada.




**Fuente:** El investigador.

## 12. IMPACTOS (TÉCNICOS, SOCIALES, O ECONÓMICOS)

### 12.1. Impacto técnico

Se alcanzó la autenticación de usuarios mediante credenciales únicas de acceso y con esto seguridad y disminución de tráfico en las rede Wi-Fi, los cambios pueden notarse en el tráfico de Vlans en las áreas del GAD Municipal de Mejía. Lo cual genera gran confianza para el administrador por tener ya el control en tiempo real de los usuarios anclados a los access point.

### 12.2. Impacto social

Muchas empresas están consideran la seguridad informática como un factor de riesgo en la seguridad de la información, este problema puede verse en la forma en cómo los departamentos de Tics de las entidades públicas y particulares se acogen la herramientas que facilita y aseguran el control de acceso que se realizan en sus respectivos equipos y área de trabajo.

### 12.3. Impacto económico

Debido a que es una tecnología robusta de software libre que podemos implantar en sistemas operativos open source desde su creación su distribución fue libre causando una aceptación grande en las entidades públicas y privadas, los requisitos de bajo presupuesto son los cuales nos brinda un impacto positivo ya que muchas veces de este depende el desarrollo de los proyectos de seguridad.

## 13. PRESUPUESTO PARA LA PROPUESTA DEL PROYECTO

**Tabla 3.** Detalla la mano de obra, equipos y recursos empleados.

| **Recursos** | **Cantidad** | **Unidad** | **V. Unitario ($)** | **Valor Total** |
|---|---|---|---|---|
| Equipos | 1 | Laptop | 618,00 | 618,00 |
| Materiales y suministros | 1 | Resmas de papel boom y materia estudiantil | 35,00 | 35,00 |
| Recursos básicos | 1 | Energía eléctrica, internet, alimentación, agua. | 126,00 | 126,00 |
| Entregables | 4 | Anillados | 4,00 | 16,00 |
| SUB TOTAL | | | | 795,00 |
| IVA 12% | | | | 95,40 |
| **TOTAL 2** | | | | **890,40** |

**Fuente:** El investigador.

Ya en la tabla 4, esta detallado los materiales empleados para el desarrollo del proyecto.

**Tabla 4.** Material utilizado por el investigador para el desarrollo del proyecto.

| **Ítem** | **Descripción** | **Cantidad** | **P. Unitario $** | **P. Total $** |
|---|---|---|---|---|
| 1 | Servidor SuperMicro Rack Server SKL3104-SR3GM Intel Xeon Bronze 3104 8GB DDR4-2666 ECC RDIMM | 1 | 1.142,39 | 1.142,39 |
| 2 | Access Point Hewlett-Packard-E-MSM460 (J9590A) Radio Dual 802. 11n AP (AM) | 9 | 209,43 | 1884,87 |
| 3 | HP E-MSM720 Wireless Lan Controllers | 1 | 881,95 | 881,95 |

| | | | | |
|---|---|---|---|---|
| 4 | Access Point Inalámbrico de Doble Banda N300 Linksys Wap300n | 1 | 130,00 | 130,00 |
| SUB TOTAL | | | | 4.039,21 |
| IVA 12% | | | | 484,70 |
| **TOTAL 1** | | | | **4523,91** |

**Fuente:** El investigador.

Con todos los gastos mencionados anteriormente en las tablas 1 y 2, se tiene una inversión total del proyecto de 5.414,31 USD.

## 14. CONCLUSIONES Y RECOMENDACIONES

### 14.1. Conclusiones

- La búsqueda de información sistematizada en revistas científicas sobre la seguridad del acceso a una red y los componentes de un servidor AAA muestra la existencia de una gran variedad de opciones para brindar este servicio, por medio de la realización del presente proyecto es posible determinar que la opción más viable la implementación de un servidor AAA Radius el cual tiene las características de seguridad y confiabilidad, acorde a las necesidades de GAD Municipal de Mejía.
- Se controla el acceso a las redes WI-FI, mediante la creación de credenciales de acceso y relacionándolos con un perfil de usuario, esto brinda un gran apoyo a la institución por su flexibilidad al momento de implementar y manejar, evitando que personas sin autorización tengan acceso a la información de la red solamente los usuarios del GAD municipal del Cantón Mejía.

- El servidor Radius ofrece un control, monitoreo y administración. Finalizamos realizando la implementación de un servidor AAA con FreeRadius que puede gestionar la información de los usuarios mediante el uso de base de datos, en este caso mariadb y un panel de control web, una interfaz gráfica que permite administrar el servidor AAA Radius, brindando un servicio integro para garantizar la seguridad en el acceso a las redes inalámbricas del GAD municipal del Cantón Mejía.

### 14.2. Recomendaciones

- Establecer políticas de seguridad para la creación de usuarios y la asignación de credenciales para los usuarios así también como para los equipos.
- Realizar frecuentemente un respaldo del servidor como precaución para mantener un backup en caso de que el servidor pueda corromperse.
- Designar y capacitar una persona del área de sistemas para que administre el servidor radius mediante el panel de control daloRadius.

## 15. BIBLIOGRAFÍA


Atom, A. (30 de Jinio de 2015). *UDP Protocolo de datagramas de usuario*. Obtenido de https://cutt.ly/OQy8HF

Candelas, F., & Baeza, J. (2009). *Protocolos de Transporte TCP y UDP*. España: Tech.

Catalogo 9SIAD6H8HC6719. (2019). Hewlett-Packard-E-MSM460 (J9590A) Radio Dual 802. 11n AP (AM) . Quito: ecuador.

Catalogo No OL-28850-04. (isco ME 2600X Series Ethernet Access Switch). Cisco.

Comercio, E. (s.f.). *Por qué pensar dos veces antes de volver a usar el Wi-Fi de las cafeterías*. Obtenido de https://cutt.ly/FQqYmL

Crespo, A. (2 de Junio de 2017). *Que es un servidor RADIUS y cómo funciona*. Obtenido de https://www.redeszone.net/2017/06/02/servidor-radius-funciona/

Dafonte, P., & Pallardo, C. (2012). Seguridad en Sistemas de Información. Coruña.

DeKok, A. (3 de Enero de 2018). *FreeRadius Documentacion*. Obtenido de https://networkradius.com/doc/3.0.10/concepts/introduction/network_access_server.html

Der, D. (2011). *Manage your networrk resources with FreeRADIUS.* Birmingham: Packt Publishing Ltd.

Fonseca, S. (2010). Comunicación Oral Fundamentos y Practica Estratégica. México: Pearson Educación.

Forero, N. (2009). Taxonomia de los Servidores AAA: Radius, Diameter y TACACS+. *INGENIO Libre*, 97 – 101.

Gorgona, L. (2017). *Redes de Computadoras*. Obtenido de https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf

Grupo de teleinformatica y automatizacion. (2017). *Protocolo COPS ( Common Open Policy Service )*. Obtenido de https://www.gta.ufrj.br/grad/01_2/arquivos/COPShtml.htm

Hidalgo, S. (16 de Octubre de 2017). *Todas las redes Wi-Fi del mundo están en peligro por un nuevo hackeo*. Obtenido de https://codigoespagueti.com/noticias/internet/alerta-todas-las-redes-wifi-del-mundo-estan-en-peligro/

Lopez, A. (05 de 02 de 2015). *Protocolos AAA y control de acceso a red*. Obtenido de https://www.incibe-cert.es/blog/protocolos-aaa-radius

Rensing, C., Karsten, M., & Stiller, B. (2002). *AAA: a survey and a policy-based architecture and framework* (Vol. 16). in IEEE Network.

Ribbon Communications. (2019). *What is Diameter Protocol?* Obtenido de https://ribboncommunications.com/company/get-help/glossary/diameter-protocol

Roca, J. (14 de Febrero de 2014). *¿Qué es WiFi?* Obtenido de http://www.informeticplus.com/que-es-wifi

Torres, J. (2018). *Red Informática: Componentes y Tipos*. Obtenido de https://www.lifeder.com/red-informatica/

Villagomez, C. (10 de Enero de 2018). *RFC Petición de comentarios*. Obtenido de https://es.ccm.net/contents/276-rfc-peticion-de-comentarios

# ANEXOS

**Anexo1: Hoja de vida del grupo de trabajo**

**Datos personales del tutor:**

**Nombres:** Jorge Bladimir

**Apellidos:** Rubio Peñaherrera

**C.I.:** 050222229-2

**Fecha de nacimiento:** 16 de mayo de 1976

**Ciudad de Domicilio:** Latacunga

**Teléfonos:** 0995220308

**E-mail:** jorge.rubio@utc.edu.ec

**Estudios:** Universidad Técnica de Cotopaxi

Pontificia Universidad Católica del Ecuador sede Ambato.

**Títulos obtenidos:** Ingeniero en Informática y Sistemas Computacionales

Diploma Superior en Gerencia Informática

Magister en Gerencia Informática mención Desarrollo de Software y Redes

**Jorge Bladimir Rubio**

**C.I.:** 050222229-2

**Datos Personales del Autor:**

**Nombres:** Jorge Santiago

**Apellidos:** Espinel Pilicita

**C.I:** 172317756-2

**Fecha de nacimiento:** 18 de julio de 1990

**Edad:** 29 años

**Estado civil:** Soltero

**Teléfono:** 0998202178

**Correo electrónico:** jorge.espinel2@utc.edu.ec

**Estudios:** Universidad Técnica de Cotopaxi (UTC)

**Jorge Santiago Espinel Pilicita**

**C.I.:** 172317756-2

**Anexo 2.** Glosario de términos

| Termino | Descripción |
|---|---|
| **AAA** | Autorización de autenticación y contabilidad / Authentication authorization and accounting |
| **RADIUS** | Servicio de usuario de acceso telefónico de autenticación remota / Remote access dial in user service |
| **MAC** | Control de acceso al medio / Media Access Control |
| **WPA** | Acceso Wi-Fi protegido / Wi-Fi Protected Access |
| **NIC** | Tarjetas Interfaz de Red / network interface card |
| **RFI** | Solicitud de información / Request for Information |
| **NAS** | Servidor de acceso a la red / Network access server |
| **RFC** | Solicitud de comentarios / Request for coments |
| **TACACS+** | Sistema de control de acceso mediante control del acceso desde terminales / Terminal access control access control system |
| **TCP** | Protocolo de control de la trasmisión / Transmision Control Protocol |
| **UDP** | Protocolo de datagrama de usuarios / User Datagram Protocol |
| **TFTP** | Protocolo de transferencia de archivos de Tivial / Tivial file transfer protocol |
| **DNS** | Sistema de nombres de dominio / Domain name system |
| **RIP** | Protocolo de información de enrutamiento / Routing information protocol |
| **SNMP** | Protocolo Simple de Manejo de Red / Simple network management protocol |
| **PPP** | Protocolo punto a punto / Point to Point Protocol |
| **PAP** | Protocolo de autenticación de contraseña / Password authentication protocol |
| **CHAP** | Desafío protocolo de autenticación de apretón de manos / Challenge-handshake authentication protocol |
| **COPS** | Servicio de política abierta común / Common open policy service |
| **SSH** | Cubierta segura / Secure shell |