
# REPÚBLICA DEL ECUADOR

# UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

**TRABAJO DE GRADO**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**

**INGENIERO EN SISTEMAS COMPUTACIONALES CON MENCIÓN EN REDES Y COMUNICACIÓN**

## TEMA:

# DISEÑO DE UN SISTEMA DE AUTENTICACIÓN Y CONTROL DE ACCESO BASADO EN LA ARQUITECTURA AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) PARA LA RED INALÁMBRICA DE UNA PYMEs (PEQUEÑAS Y MEDIANAS EMPRESAS) EN GUAYAQUIL

## AUTOR:

**JACOBO STANLEY SARMIENTO FRANCO**

**OCTUBRE – 2016**

**GUAYAQUIL – ECUADOR**

# DECLARACIÓN DE RESPONSABILIDAD

Yo, Jacobo Sarmiento Franco

DECLARO QUE:

El Trabajo de Titulación DISEÑO DE UN SISTEMA DE AUTENTICACIÓN Y CONTROL DE ACCESO BASADO EN LA ARQUITECTURA AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) PARA LA RED INALÁMBRICA DE UNA PYMEs (PEQUEÑAS Y MEDIANAS EMPRESAS) de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas Computacionales Mención en Redes y Comunicación, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los (días) del mes de Octubre del año 2016

El Autor

_____

Jacobo Sarmiento Franco

# AGRADECIMIENTO

A Dios, quien me ha dado salud, sabiduría y fuerza para continuar cada día, a mis padres, que estuvieron conmigo apoyándome en el transcurso del desarrollo de este trabajo de grado, gracias a sus consejos, enseñanzas y ejemplo que se ven reflejados en cada línea de este texto.

# DEDICATORIA

A Dios, quien siempre está a mi lado y siempre me protege.

A mi papá quien con su ejemplo y dedicación, me demostró que todo es posible con trabajo y amor.

A mi mamá, que con cada palabra me incentiva a seguir adelante, a no desmayar, y culminar cada trabajo que se ha empezado con empeño y dedicación.

A mis familiares quienes me dieron su respaldo en cada momento en el desarrollo de este trabajo de grado.

# RESUMEN

El proyecto de tesis descrito a continuación, está basado en el diseño y posterior aplicación de la arquitectura AAA (Autenticación, Autorización y registro), mediante un servidor RADIUS y la vinculación de los protocolos 802.1x y EAP. El enfoque que se le da está basado en el control de acceso y gestión de la red inalámbrica de una PYMEs, el fin es evitar el acceso a la información y el uso de recursos no autorizados, así como impedir el uso injustificado del servicio de internet por dispositivos ajenos a la empresa.

La implementación de la propuesta permite un control adecuado y gestionado a la red de datos inalámbrica que acceden los usuarios así como los recursos que utilizan. Lo cual otorga al administrador de la red tener un mejor panorama de la actividad de cada usuario que ingresa a la red WLAN; haciendo que la administración de la red sea eficiente y esté disponible. Mediante un análisis y diseño de la topología de la red se puede implementar mecanismos de seguridad que se ajusten a la infraestructura de la empresa.

Previo una investigación se pudo evidenciar que existen empresas que no poseen mecanismo de seguridad adecuados implementados en sus redes inalámbricas, por lo cual se ofrece la implementación del diseño AAA. El software a utilizar para la implementación es propietario, se utilizan roles así como servicios del sistema operativo para servidores, además certificados digitales y el directorio activo. Finalmente se obtiene como resultado una solución robusta para un acceso efectivo, controlado y gestionable de acceso a los usuarios.

**Palabras Claves:** AAA, RADIUS, Protocolos de seguridad, Seguridad Inalámbrica.

# ABSTRACT

The thesis project described below is based on the design and subsequent implementation of the AAA (Authentication, Authorization and registration) architecture, using a RADIUS server and linking 802.1x and EAP protocols. The approach given is based on access control and management of the wireless network of SMEs, the aim is to prevent access to information and the use of unauthorized resources and prevent unjustified use of the internet service by devices outside the company.

The implementation of the proposal allows adequate control and managed to wireless data network that user's access and the resources they use. Allowing the network administrator to have a better picture of the activity of each user accessing the WLAN; making the network management is efficient and available. Through analysis and design of the network topology can be deployed security mechanisms that conform to the infrastructure of the company.

Prior research it was evident that there are companies that have not implemented adequate security mechanism in their wireless networks, thus implementing AAA design is offered. The software to be used for implementation is proprietary, handle roles as operating system services for servers and digital certificates and Active Directory are used. Finally, it is resulting in a robust solution for effective, controlled and manageable access to the users.

**Keywords:** AAA, RADIUS, Security Protocols, Wireless Security.

# INDICE DE CONTENIDO

# INDICE DE TABLAS

# INDICE DE FIGURAS

# INTRODUCCIÓN

Las empresas en la actualidad hacen uso cada vez más de las redes de datos corporativa, el acceso por lo general es de forma alámbrica o inalámbrica. Sin embargo las redes inalámbricas tienen mayor acogida dentro de los usuarios ya que les permite tener movilidad, flexibilidad y por ende mayor productividad, otra de las bondades por la que más empresas la utilizan, son los bajos costos de implementación lo que permite que sean escalables.

La seguridad que pueda otorgarse a los dispositivos de acceso inalámbrico, está basada en mecanismos que controlan los accesos de los usuarios. Pero no siempre son robustos y eficientes, quedando las empresas expuestas a pérdidas, sustracción o divulgación de información. De allí que deben existir mecanismos de control adecuados que permita dar un acceso fiable y controlado a los distintos recursos y plataformas tecnológicas que brinda la red de datos, mediante la verificación de la identidad del usuario, así como también el registro de accesos, todos estos componentes permiten un correcto control de accesos mediante la definición de políticas de seguridad.

Este trabajo de grado se enfoca en la arquitectura AAA (siglas en ingles de autenticación, autorización y registro), la cual fusiona una serie de procesos y procedimientos que se aplican en entornos de seguridad informática. Permitiendo una adecuada administración y control de los puntos de accesos inalámbricos a los administradores de la red, así como la selección idónea de los protocolos de seguridad y algoritmos de cifrado con el fin de poder indicar los beneficios que obtendrá la implementación del protocolo RADIUS.

La investigación también tendrá en cuenta el costo-beneficio de la implementación proporcionando una opción de dispositivos de comunicación, servidores, así como el costo de licenciamiento del sistema operativo del servidor.

# CAPÍTULO 1.

## 1. Planteamiento de la situación problemática.

### 1.1 Antecedentes

A finales del siglo 20 empezó a desarrollarse el estándar IEEE 802.11 y con ello la aparición de dispositivos que se conectan de forma inalámbrica a las diferentes redes de datos, Según el libro Wireless Network in Developing World (2013, p.130) "Los estándares son la base de muchos productos inalámbricos, lo que asegura su interoperabilidad y su uso por parte de los que desarrollan, instalan y gestionan redes inalámbricas". De tal manera que el desarrollo de redes inalámbricas seguirá avanzando e implementándose de manera continua.

Las velocidades de transmisión de datos han tenido su evolución en redes inalámbricas así lo indica Diab, A. (2016, p.162) "Wi-Fi o WLAN ofrece muy alta velocidad de datos (de 1 a 55 Mbps) dentro de su área de distribución limitada. La cual se basa en la norma IEEE 802.11. Las redes WLAN se popularizaron en el año 2004 para proporcionar Internet a redes privadas y corporativas". Tal como se indica el auge de las redes inalámbricas empezaron con fuerza en la década pasada expandiéndose de gran forma.

La evolución de la familia del standard IEEE 802.11 se la aprecia en la siguiente tabla.

**Tabla 1 Evolución del standard IEEE 802.11**

| Estándar | Año de lanzamiento | Ancho de banda | Velocidad (Mbps) |
|---|---|---|---|
| IEEE 802.11 | 1997 | 2.4 GHz | 2 Mbps |
| IEEE 802.11 a | 1999 | 5 GHz | 11 Mbps |
| IEEE 802.11 b | 1999 | 2.4 GHz | 54 Mbps |
| IEEE 802.11 g | 2003 | 2.4 GHz | 54 Mbps |
| IEEE 802.11 n | 2009 | 2.4 GHz -5 GHz | 600 Mbps |
| IEEE 802.11 ac | 2013 | 5 GHz | 6.93 Gbps |

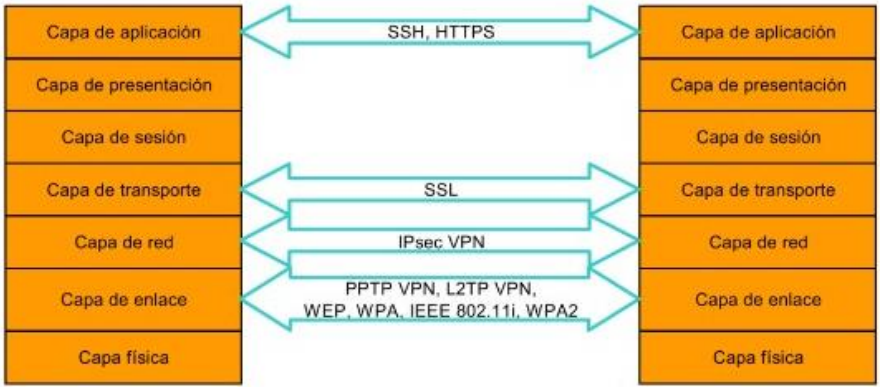
**Elaborado por: Jacobo Sarmiento**

Este crecimiento en el desarrollo de tecnologías inalámbricas, hace que las empresas e instituciones empiecen a implementar puntos de accesos inalámbricos que puedan otorgar mayor movilidad, productividad y eficiencia dejando de lado el uso de los cables de red.

Sin embargo en las implementaciones se llega a omitir los niveles de seguridad que se les debe otorgar a los puntos de acceso inalámbrico siendo estos objeto de incursiones no autorizados y en ocasiones indetectables, logrando acceder al recurso más valioso de la empresa, como lo es la información.

Para Pellejero I, Andreu F, Lesta A, (2006, p. 97) “son diversos los mecanismos de seguridad que se pueden aplicar en redes WLAN y estos actúan en diferentes capas del modelo OSI”. La representación gráfica de los niveles de seguridad se los puede apreciar en la figura 1.

**Figura 1.- Niveles de seguridad en el modelo OSI**




***Fuente: Mecanismos de seguridad existentes en las distintas capas de OSI (Pellejero I, Andreu F, Lesta A. 2006, p. 97).***

El acceso por autenticación se convierte en una necesidad en redes inalámbricas mientras que en las redes alámbricas el acceso es a través de un cable de red, obteniéndose un mayor control debido a que para acceder a la red de datos y por ende a la infraestructura tecnológica es necesario estar dentro de la organización.

En las redes inalámbricas el medio físico es el espectro electromagnético por el cual viajan distintas frecuencias, que transportan la información, las mismas que son vulnerables, de allí que nace la necesidad de establecer mecanismos

de seguridad que permitan acceder de una forma fiable a la información, para evitar que existan fisuras en la red inalámbrica.

Con lo anteriormente expuesto, el mecanismo de seguridad que será objeto de estudio estará enfocado en la capa de enlace del modelo OSI para el standard IEEE 802.11.

## 1.2 Planteamiento del Problema

Las redes inalámbricas en su mayoría tienen establecida seguridades a nivel de la capa de enlace, con los protocolos WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) o WPA-2(Wi Fi Protected Access 2), los mismos que se vuelven no fiables cuando se conoce la clave de autenticación, por lo tanto sus mecanismos no son seguros en ambientes empresariales.

Uno de los principales problemas que se dan en la red inalámbrica de una empresa sin la seguridad eficiente, es el acceso no autorizado así como el consumo descontrolado del ancho de banda que repercute en los servicios online o las aplicaciones de trabajo.

La problemática es evidente cuando llegan visitantes a una locación de una empresa con cobertura inalámbrica, usualmente solicitan la clave de acceso a la conexión Wi-Fi (Wireless Fidelity), al ser proporcionada deja de ser secreta, por ende no solamente se les brinda el servicio de internet sino también a la red de datos, y en muchos casos al no estar segmentada dicha red, estos usuarios pueden ingresar sin ningún tipo de control a los recursos compartidos de la red.

Otra situación que se da es que los usuarios que laboran en la compañía, pueden utilizar las claves de acceso a la red inalámbrica para conectar sus dispositivos móviles los cuales consumen de forma indiscriminada el ancho de banda del servicio de internet.

En virtud de esta problemática se plantea el siguiente cuestionamiento:

¿Cómo se puede controlar los accesos a la red de datos mediante un sistema de autenticación y gestión de políticas de seguridad en una red inalámbrica empresarial?

Partiendo de este cuestionamiento surge la oportunidad de implementar una solución integral y escalable, que evitaría accesos no autorizados, así como proporcionar una herramienta de gestión de políticas de seguridad informática y autenticación para una empresa.

### 1.3 Objetivo General

Diseñar un sistema de autenticación y control basada en la arquitectura AAA (Authorization, Authentication and Accounting) para la red de datos inalámbrica de una empresa.

### 1.4 Objetivos Específicos

- Identificar los estándares y protocolos usados en un servidor RADIUS
- Proporcionar una red de datos inalámbrica segura a través de mecanismos de autenticación y cifrado de datos
- Diseñar y configurar puntos de acceso inalámbrico seguros

### 1.5 Alcance

Este proyecto tiene como finalidad el diseño de un sistema de autenticación y control de seguridad para una empresa.

Con el propósito de lograr los objetivos se debe configurar todos los equipos Inalámbricos de la red bajo los protocolos de acceso seguro haciendo uso del estándar IEEE 802.1X, y el protocolo RADIUS, vinculado al Directorio Activo de Windows Server el mismo que debe ser configurado por especialistas en el área de TI.

## 1.6 Justificación

El diseño de una arquitectura AAA, involucra un servidor el cual centralizará los dispositivos de comunicación inalámbricos, este servidor permitirá que los usuarios que se encuentren registrados puedan acceder a la red, por lo que no se necesitará una clave específica para ingresar a la red de datos inalámbrica y por ende a los recursos.

Con la implementación de un eficiente mecanismo de seguridad aplicada a la capa de enlace del modelo OSI, se evitara el acceso no autorizado a la red de datos y recursos informáticos.

Es importante indicar, que con el uso del esquema AAA, el administrador de la red gestionará de mejor forma los dispositivos de comunicación, controlará el acceso a los usuarios de la red inalámbrica y aplicará políticas de seguridad a los diferentes recursos informáticos.

La utilización de este esquema, mediante el diseño de la arquitectura de seguridad AAA, involucra varios procesos de hardware y software, siendo considerado como una buena práctica para el área de TI.

## 1.7 Delimitación

La investigación será orientada a la seguridad en accesos que se le otorgue a una WLAN (Wireless Local Area Network), mediante un servidor RADIUS (Servidor Remoto de Autenticación de Usuarios) que estará vinculado al directorio activo de Windows Server configurado por personal del departamento de TI.

## 1.8 Hipótesis

Con la implementación de mecanismos de seguridad vinculados al servidor RADIUS (Servidor Remoto de Autenticación de Usuarios), se controlara el acceso de los usuarios así como también gestionará de forma más óptima los recursos y servicios de la red de datos inalámbrica.

## 1.9 Operatividad de las Variables

## 1.10 Variable Dependiente

**Tabla 2 Variable Dependiente**

| Variable | Operacionalidad | Dimensión | Indicadores |
|---|---|---|---|
| Protocolo RADIUS como parte de la Arquitectura AAA aplicada a una empresa PYMEs (Pequeñas y Medianas Empresas). | Configuración del servidor RADIUS, utilizando el servicio NPS de Windows Server 2012 | • Administración y Gestión de la red de datos<br>• Aplicación de políticas bajo entornos de seguridad informática | • % de administradores de la red de datos encuestados<br>• Confiabilidad de la red inalámbrica<br>• Seguridad de la red inalámbrica<br>• Gestión de la red inalámbrica |

**Elaborado por: Jacobo Sarmiento**

## 1.11 Variable Independiente

**Tabla 3 Operacionalidad Variable Independiente**

| Variable | Operacionalidad | Dimensión | Indicadores |
|---|---|---|---|
| Seguridad en los puntos de accesos inalámbricos | El standard IEEE 802.1X, proporciona una red segura y con mayor control en los accesos de los usuarios. | • Dispositivos de accesos inalámbricos con mecanismos de seguridad empresarial<br>• Mejora en el rendimiento de los servicios en la red de datos. | • Identificación de usuarios en la red<br>• Tiempo de permanencia<br>• % de usuarios que se autentican en la red inalámbrica. |

**Elaborado por: Jacobo Sarmiento**

# CAPITULO 2

# 2. Marco Teórico

## 2.1 Seguridad informática

Según Pellejero I, Andreu F, Lesta A (2006, p. 1) “Las redes inalámbricas se diferencian de las redes cableadas, en la naturaleza que emplean para transmitir sus datos. Las redes WLAN, también conocidas como WI-FI utilizan como medio el aire” mediante este concepto se puede intuir que las redes inalámbricas subsisten en el medio ambiente haciendo que estas estén expuestas a un libre acceso si no se aplican mecanismos adecuados de seguridad.

Arana, J. R., Villa, L. A., & Polanco, O. (2013) indica que “las compañías están cada vez más basando sus modelos de negocios en proveer acceso a recursos. Estos recursos pueden ser páginas Web, acceso a Internet, cuentas de correo electrónico, o cualquier activo de información que necesite estar protegido o controlado” se observa que las empresas están moviéndose de forma dinámica ya no solo utilizan servicios externos de Internet, sino que publican servicios y recursos de la red de datos la misma que debe estar blindada y protegida contra intrusos.

Siguiendo el enfoque de la seguridad de la información Nogales, J. L. M., Beltrán, S. V., & Bonilla, J. L. L. (2006, p.199) indica que “para garantizar la seguridad en las redes inalámbricas, el Instituto de Ingenieros Eléctricos y Electrónicos define mecanismos de encriptación y autenticación dentro de su estándar 802.11” el objetivo que se persigue es impedir el acceso a usuarios no autorizados y por ende que ningún intruso pueda descifrar una señal de datos para cometer actos indebidos o apropiación ilícita de la información.

Continuando con este punto de vista se puede mencionar que existen dos categorías de seguridad en redes inalámbricas: La seguridad al autenticar los usuarios e identificar sus permisos y la seguridad al momento de transmitir los

datos entre dispositivos inalámbricos usando ondas de radio. (Nogales, J. L. M., Beltrán, S. V., & Bonilla, J. L. L., 2006).

La seguridad de la información ha tenido varios cambios en las últimas dos décadas las mismas que se conseguían por medios físicos y administrativos. (Stallings, W., 2011). Al hablar de estas dos formas de seguridad nos enfocamos a cajas fuertes, cerraduras, barreras de seguridad incluso guardias de seguridad. Los mismos que están para prevenir el acceso a personas no autorizadas a una instalación; y al hablar de medios administrativos se menciona el sigilo profesional que no es otra cosa que la obligación de un colaborador a no divulgar información confidencial de una empresa u organización.

Sin embargo el avance de la tecnología y la introducción de los computadores hicieron que toda la información que se tenía de forma física sea almacenada ahora en ficheros y más adelante en bases de datos. Por ende fue cada vez más necesaria la creación de herramientas automáticas para la protección de los mismos. (Stallings, W., 2011).

Según Stallings, W. (2011) El segundo cambio más relevante, que ha afectado a la seguridad, es la introducción de sistemas distribuidos y la utilización de redes y facilidades de comunicación para transportar datos entre terminales de usuario y computadores, y de computador a computador. Las medidas de seguridad en red son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos. Las redes han sido de gran aporte en el desarrollo de las comunicaciones, sin embargo la información que transita debe ser resguardada con los instrumentos adecuados de seguridad tanto de hardware como de software.

Dentro del compendio de seguridad Informática se deben tener políticas de seguridad que definan responsabilidades y reglas a seguir para evitar amenazas o minimizar sus efectos en caso de que llegasen a presentarse. (Santos, J. C., 2000). Tal como se indica deben existir regulaciones en los recursos y accesos que están disponibles en la red de datos.

## 2.2 Amenazas en la seguridad de redes

De acuerdo con Stallings, W. (2011). Si se quiere entender los tipos de amenazas a la seguridad en computadoras y redes se debe tener en cuenta los siguientes requisitos:

**Secreto:** la información debe ser accesible por los usuarios autorizados solo para lectura. Los tipos de salida son impresos o por pantallas u otra forma de evidenciar un objeto

**Integridad:** la información debe ser modificada por los usuarios autorizados. Esto es cambiar, escribir, eliminar, crear o cambiar un estado

**Disponibilidad:** Los recursos de una computadora deben estar disponible ante los usuarios autorizados.

Existen dos categorías de amenazas a la seguridad de una red de datos: **amenazas pasivas** que suponen un intento de ataque por parte de un sujeto; y **amenazas activas** que pueden ser la modificación de un dato que es transmitido o la creación de una falsa transmisión. (Stallings, W., 2011).

Según el periódico Expansión, refiere los siguientes:

> “No mezclar el uso profesional con el personal: para no comprometer datos corporativos, es aconsejable no utilizar los mismos dispositivos para entretenimiento y trabajo. También hay que controlar las páginas que se visitan, especialmente las de descargas ilegales”. (Enrique Ordiales., 4 de Octubre de 2016)

Se evidencia que en la mayoría de ocasiones no se acoge esta indicación, debido a que hay dispositivos móviles de la compañía y propios de los usuarios que acceden a la red de datos empresarial inalámbrica, por lo que se recomienda no dar accesos a dispositivos ajenos a la organización.

## 2.3 Arquitectura AAA (Authentication, Authorization and Accounting - Autenticación, Autorización y Registro)

Para Nakhjiri, M., & Nakhjiri, M. (2005, p.1) "La autenticación, autorización y registro son tres importantes bloques utilizados en la construcción de una arquitectura de red que ayuda a proteger al operador de red y sus clientes contra el fraude, ataques, la gestión inadecuada de recursos, y la pérdida de ingresos". La Arquitectura AAA está conformado por varios actores que componen un solo cuerpo encargado de blindar la red contra intrusos que puedan acceder a la red.

J. Zhang, Y. Guo, Y. Chen, & J. Ma. (2015, p.219) "AAA es un marco de gestión que proporciona funciones de autenticación, autorización y contabilidad. En lo practican se da cuenta de AAA mediante el uso de protocolo RADIUS normalmente".

En relación a lo mencionado se puede decir que la arquitectura AAA, ofrece ventajas en gestión de la red, administración de los puntos de acceso, integridad de datos, escalabilidad y estandarización de métodos de cifrado de datos.

## 2.4 Funcionamiento de la Arquitectura AAA

La arquitectura la conforman los siguientes elementos:

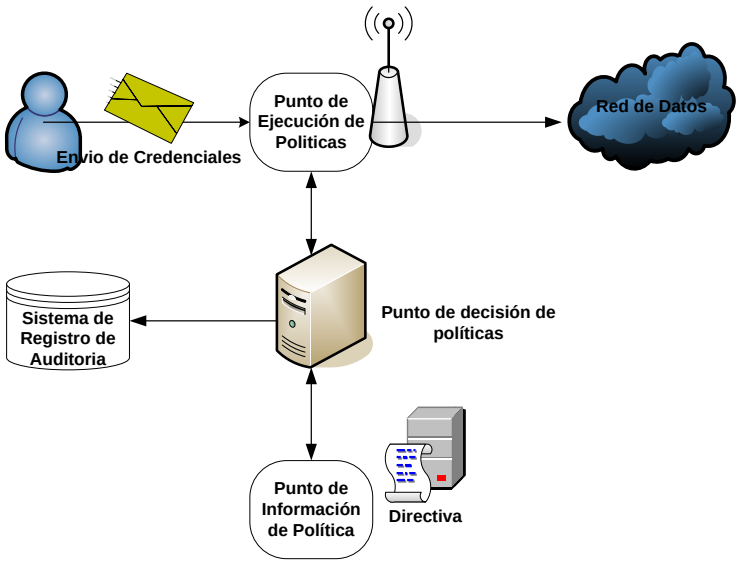
1. El usuario desea acceder a la red a través de cualquier dispositivo móvil o PC.
2. El punto de ejecución de políticas es el que aplica los términos de acceso a la red de datos en este caso en dispositivos de comunicación inalámbricos, aunque puede ser un conmutador, cortafuegos o un dispositivo que realice esta función en la red.
3. El punto de información de políticas, es el repositorio de información que puede ser usado para la evaluación de la solicitud de acceso a la red, en este caso sería el Directorio Activo.
4. El punto de decisión de políticas, quien se encarga de la toma de decisiones dentro de la arquitectura, toma la información del punto de ejecución de políticas y el punto de información de políticas, este decide

si permite o rechaza el acceso a la red o recursos en este caso sería el servidor RADIUS.

5. El sistema de registro y auditoria almacena la información de cada actividad de los usuarios así como el tiempo de permanencia.

En la figura 2, se puede apreciar la arquitectura AAA.

**Figura 2.- Arquitectura AAA**




***Elaborado por: Jacobo Sarmiento***

## 2.5 Autenticación (Authentication)

Autenticación consta de dos actos: en primer lugar se tiene el acto de proporcionar una prueba de la autenticidad de la información que se está entregando o es almacenada, y en segundo lugar, el acto de verificación de la prueba de la autenticidad de la información que se está recibiendo o se está recuperando. (Nakhjiri, M., & Nakhjiri, M., 2005).

Entonces la autenticación no es otra cosa que un mecanismo de verificación de la identidad visto de otra forma la identificación es solicitar una identificación mientras que la autenticación es demostrarla.

En el mundo real la autenticación se da cuando se muestra la cedula de identidad, pasaporte o el carné de conducción, para posteriormente realizar una comprobación del documento que se presenta.

## 2.6 Autenticación de un solo factor

Según Dulaney, E., & Easttom, C. (2014, p.132) “la forma más básica de la autenticación se conoce como la autenticación de un solo factor (Single Factor Authentication), porque se comprueba sólo un tipo de autenticación. Con mayor frecuencia implementado como el nombre de usuario tradicional / combinación de contraseña. El nombre de usuario y la contraseña son identificadores únicos para un proceso de inicio de sesión”.

***Figura 3.- Autenticación de un solo Factor***

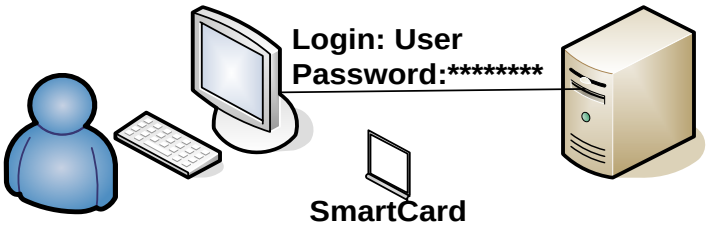

***Elaborado por: Jacobo Sarmiento***

## 2.7 Autenticación Multifactor

Este tipo de autenticación tiene más acogida en sitios web los cuales están presente a menudo en plataformas electrónicas bancarias donde se solicita un token (dispositivo electrónico de seguridad). De esta forma se evidencia la doble autenticación.

Cuando dos o más métodos de acceso se incluyen como parte del proceso de autenticación, se esta la implementando un sistema de autenticación de múltiples factores. Un sistema que utiliza tarjetas inteligentes y contraseñas es conocido como un sistema de autenticación de dos factores. Un sistema de múltiples factores puede consistir en un sistema de dos factores, de tres factores, y así sucesivamente. En tanto exista más de un factor involucrado en el proceso de autenticación, se considera un sistema multifactorial (Dulaney, E., & Easttom, C, 2014).

**Figura 4.- Autenticación Multifactorial**




**Elaborado por: Jacobo Sarmiento**

Siguiendo con lo indicado por Dulaney, E., & Easttom, C. (2014) menciona que los sistemas de autenticación o métodos en la actualidad están basados en uno o cinco factores:

- Algo que la persona conoce: una clave o pin.
- Algo que la persona tiene: una tarjeta inteligente token o un dispositivo de identificación.
- Algo que es parte de la persona: huella digital o patrón de retina (usualmente llamados biométricos).
- Algo que hace a la persona: una acción o comportamiento como objeto de autenticación.
- Algún lugar donde se encuentre la persona: ubicación geo-referencial. (Dulaney, E., & Easttom, C., 2014)

## 2.9 Autorización (Authorization)

Es un proceso donde la información que se proporciona a una repuesta es evaluada. Esta información que proporciona el usuario se contrasta con los datos obtenidos de un archivo, base de datos o directorio activo. La autorización se da después de la autenticación y no concierne el chequeo de la clave. Se puede usar varias comparaciones lógicas para determinar si un usuario está autorizado para conectarse a la red (Van der Walt, D., 2011).

## 2.10 Registro (Accounting)

Para Nakhjiri, M., & Nakhjiri, M. (2005) registro se refiere a la recopilación de información y el consumo de los recursos toda la red o en un sector específico

de esta. Esta información se denomina generalmente como registro de datos o métricas de registro. Típicamente, el dispositivo de comunicación de la red que proporciona servicios a un usuario recoge la información sobre el consumo de recursos de usuario.

En un entorno AAA se efectúa el método de recopilación y envió de información a un servidor de seguridad que es usado para auditoria y reporte de datos tales como: nombres de usuario, tiempo de inicio, fin, cantidad de paquetes enviados, números de bytes.

Dicho de otra forma es el acto de obtener registros de los usuarios que utilizan un recurso. Mediante la implementación de una base de datos para emitir reportes el cual puede mantener información concerniente al usuario que inicio sesión en el servidor, la hora, la dirección IP, recursos a los cuales acceso, los accesos otorgados o denegados. Sin embargo el protocolo RADIUS no ofrece esta característica propia pero puede ser adaptada mediante una base de datos.

## 2.11 Protocolo RADIUS

RADIUS, Remote Authentication Dial-In User Server/Servicio de Autenticación Remota para Usuario de Acceso Telefónico, fue desarrollado por Steve Willens de la empresa Livingston para la serie Postmaster de servidores de accesos de red. (C. Rigney, et al., 2000).

Para J. Zhang, Y. Guo, Y. Chen, & J. Ma. (2015) RADIUS es usado para identificar usuarios por nombre y contraseña, si los usuarios son autenticados exitosamente se les deberá autorizar los recursos. Se puede apreciar que existen siempre la autenticación y autorización. El registro se lo hace con la finalidad de obtener un pago por los recursos que se consuma, pero por lo general se aplica para tener registro de lo que realiza un usuario en la red de datos.

En seguridad de redes se puede decir que las transacciones entre el cliente y el servidor RADIUS son autenticados a través del uso de un secreto compartido, el cual no es enviado a la red. Además, todas las contraseñas de usuarios se

envían de forma cifrada entre el cliente y el servidor RADIUS. (C. Rigney, et al., 2000).

Actualmente, el funcionamiento del protocolo para los procesos de autenticación y autorización se describe en el RFC 2865, y los procesos para registro o auditoría se encuentran descritos en el RFC 2866. (López D., Suasnavas, C., Andrea, E., & Calderón A., 2012).

Según lo descrito en el RFC 2865 de C. Rigney, et al. (2000). RADIUS utiliza sus propios puerto UDP (User Datagram Protocol) 1812 siendo este el oficial. Previamente uso el 1645, sin embargo existía conflictos con el servicio de datametrics.

De aquí salta la inquietud de saber porque el protocolo UDP, el mismo que tiene una razón técnica, por lo que continuando con el RFC 2865 C. Rigney, et al. (2000). Indicando que si por alguna razón la petición que se realiza a un servidor primario falla, un servidor secundario debe ser consultado. Por lo que la solicitud debe quedarse en la capa de transporte para ser retransmitido.

Existiendo un temporizador el cual se maneja diferente para TCP, entonces se tiene que del lado del servidor no se necesita una detección de la perdida de datos, pero del lado del cliente existe un tiempo de espera que no puede maximizarse haciendo que TCP no sea un protocolo eficiente aplicado en RADIUS.

Siguiendo con lo indicado por el RFC 2865 descrito por C. Rigney, et al. (2000) al usar UDP hay que pagar un precio como desventaja del protocolo TCP y es que se debe gestionar artificialmente temporizadores de retransmisión para un mismo servidor, si se utiliza TCP muy probablemente se tendría una cola de espera por la cantidad de solicitudes sin respuestas las cuales no serían procesadas ante eventuales fallos.

RADIUS utiliza un esquema cliente/servidor el mismo que interactúa recibiendo la información del usuario a autenticar, realiza una comprobación de la información verificando que sea correcta mediante esquemas de autenticación como: PAP CHAP, MS-CHAP, MS-CHAP V2 o EAP. Del Rio, A. M. (2006), el

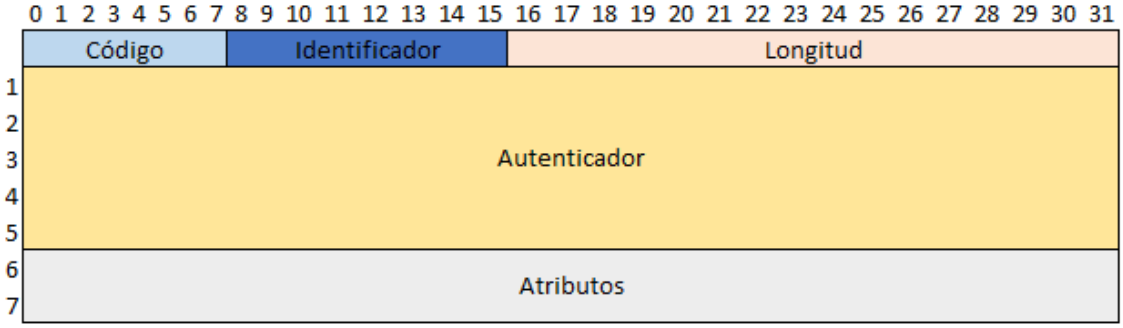
mismo que al ser aceptado, el servidor autoriza la asignación de la configuración necesaria para que este pueda acceder a la red de datos, caso contrario lo negara impidiéndole acceder.

En la actualidad RADIUS es multiplataforma siendo implementado en redes con un alto nivel de seguridad, es muy flexible se ajusta a la red de datos, pudiendo ampliarse a mejoras de seguridad acoplándose a nuevas tecnologías, a esto sumando que la información que se registra puede ser usada en auditoria por temas de seguridad así como también en ambientes de facturación siendo un ejemplo las redes móviles.

## 2.12 Paquete RADIUS

El paquete RADIUS es de longitud variable consta de los siguiente elementos que se aprecia en la figura 4

**Figura 5.- Formato del paquete RADIUS**




**Elaborado por:** Jacobo Sarmiento

Son 5 elementos que conforman el paquete y se detallan a continuación

**Código:** Octeto que identifica el tipo de paquete RADIUS que está siendo transmitido

**Identificador:** Octeto que numera el paquete RADIUS con la finalidad de ayudar al servidor RADIUS a emparejar las peticiones con respuestas

**Longitud:** Identifican el tamaño del paquete incluye el campo atributos con una longitud mínima de 20 octetos y una máxima de 4096 octetos.

**Autenticador:** conformado por 16 octetos contiene información que el cliente y el servidor RADIUS necesitan para autenticarse recíprocamente.

**Atributos**: su longitud es variable y contiene información necesaria para autenticar y autorizar detalles de la configuración. (López D., Suasnavas, C., Andrea, E., & Calderón A., 2012).

## 2.13 Funcionamiento del Servidor RADIUS

El RFC 2865 descrito por C. Rigney, et al. (2000) describe la operacionalidad del protocolo RADIUS en 4 pasos:

1. Cuando un cliente está configurado para utilizar RADIUS, cualquier usuario del cliente presenta la información de autenticación al cliente. Esto podría ser un inicio de sesión personalizable, donde se espera que el usuario introduzca su nombre de usuario y contraseña. Alternativamente, el usuario podría utilizar un protocolo de enlace de encuadre como él (PPP) punto a punto Protocolo, que tiene los paquetes de autenticación que llevan esta información.

2. Una vez que el cliente ha obtenido dicha información, se puede optar por autenticar mediante RADIUS. Para ello, el cliente crea un "Una solicitud de accesos" que contiene atributos tales como el nombre del usuario, el usuario de contraseña, el ID del cliente y la ID de puerto que el usuario con los cuales accede. Cuando una contraseña está presente, se oculta utilizando un método basado en el RSA Message Digest MD5 Algoritmo.

3. La solicitud de acceso se envía al servidor RADIUS a través de la red. Si no existe ninguna respuesta dentro de un período de tiempo, la solicitud es re-enviado un número de veces. El cliente también puede enviar a la solicitud a un servidor alternativo o servidores, en caso de que el servidor primario es inactivo o inaccesible. Un servidor alternativo se puede utilizar ya sea después de una serie de intentos cuando el servidor principal falla, o en modo round-robin.

4. Una vez que el servidor RADIUS recibe la solicitud, valida la solicitud del cliente. La solicitud del cliente hacia el servidor RADIUS sin secreto compartido deberá ser desechada en silencio. Si el cliente es válida, el servidor RADIUS consulta a una base de datos de los usuarios para encontrar al usuario cuyo nombre coincide con el pedido. La entrada del usuario en la base de datos contiene una lista de los requisitos que se deben cumplir para permitir el acceso del usuario. Esto siempre incluye la verificación de la contraseña, pero puede también especificar el cliente (s) o el puerto (s) a la que el usuario está autorizado acceso. (C. Rigney, et al. 2000).

Durante todo el proceso de autenticación el usuario puede recibir las siguientes respuestas por parte del servidor cabe indicar que los mensajes son adecuados de acuerdo al servidor RADIUS implementado. Ver figura 6.

**Figura 6.- Diferentes respuestas que proporciona RADIUS**

| | |
|---|---|
| ACCEPT | Se autentica el usuario |
| REJECT | El usuario no se autentica realizando una nueva solicitud para ingresar la información, de no acatar la solicitud esta es rechazada |
| CHALLENGE | Es emitido por el servidor RADIUS el mismo que colecciona datos adicionales del usuario |
| CHANGE PASSWORD | Es emitido por el servidor RADIUS con la finalidad que cambie la clave |
| ACCEPT o REJECT | RADIUS solicita autenticarse antes que proceder a autorizar accesos |

**Elaborado por: Jacobo Sarmiento**

## 2.14 Tipos de Seguridad en WLAN

Según Santos, J. C. (2000) las redes inalámbricas son flexibles y ofrecen muchos beneficios pero a su vez existen limitaciones dado por el rango del espectro de radiofrecuencia que por ser sin costo de licenciamiento sufre

interferencias o saturación en el canal de transmisión. Cabe mencionar que la seguridad es una problemática ya que cualquier equipo con una tarjeta de red inalámbrica puede interceptar la señal. La seguridad en redes inalámbricas es muy sensible por lo cual se implementan mecanismos que protejan la transmisión tales como la encriptación o la autenticación.

Según lo indica WIFI-Alliance (2008) se realizó un trabajo en conjunto entre WIFI-Alliance y la IEEE (Institute Electrical and Electronics Engineers) con el objetivo de proporcionar seguridad a la norma IEEE 802.11 de red inalámbrica con la finalidad que sean implementado en todos los dispositivos inalámbricos.

## 2.15 WPA2 (WI-FI Protected Access version 2)

Para Wi-FI, A. (2012) “WPA2 es la generación actual de seguridad Wi-Fi desde el lanzamiento actual cuyo fin fue mejorar las brechas de seguridad que tiene WEP de autenticación y cifrado”.

Se basa en dos principales protocolos de seguridad:

- AES (Advanced Encription Standard) usado por gobiernos y empresas asegurando la confidencialidad de la información.
- IEEE 802.1x un estándar que se utiliza en redes corporativas proporcionando autenticación robusta y funciones de red sofisticada. (WIFI-Alliance, 2012).

Continuando con Wi-FI, A. (2012) WPA2 se basa en el estándar 802.1i y proporcionando cifrado de datos en AES de 128 bits. También proporciona autenticación mutua con Pre-Shared Key (en el modo personal) y con 802.1 x/EAP (en el modo empresa). En la actualidad en la mayoría de dispositivos de conexión inalámbrica se puede apreciar este tipo de seguridad, además están aplicados desde un teléfono móvil hasta un computador, se evidencia que no solamente WPA2 está orientado a las empresas, también está orientado a los dispositivos de la línea hogar o personal.

La certificación WI-FI se encuentra en la mayoría de dispositivos inalámbricos de esta forma se está evitando incompatibilidades tanto en el emisor como el

receptor de la señal y por ende se asegura la transmisión de la información mediante el cifrado de datos.

En el siguiente cuadro se puede apreciar alguna de las características de WPA-2, ver la figura 7.

**Figura 7.- Características WPA-2**


**Elaborado por: Jacobo Sarmiento**

## 2.16 WPA2 – Enterprise (WI-FI Protected Access - Enterprise)

Según Wi-FI, A. (2012) “WPA2-Enterprise cifra los datos con AES y verifica la identidad de los usuarios de la red mediante el protocolo de autenticación extensible, o EAP. El programa WPA2-Enterprise incluye pruebas para cinco tipos de EAP ampliamente implementado para atender a una variedad de escenarios de uso y tipos de dispositivos”.

El diseño de WPA2-Enterprise le permite soportar redes grandes empresariales, pero este necesita un servidor que es el responsable de crear las

claves de cifrado bajo pedido del cliente, en este caso el usuario que intenta acceder y lo solicita.

A continuación se muestra las características en la figura 8.

**Figura 8.- Características WPA2- Enterprise**


**Elaborado por: Jacobo Sarmiento**

## 2.17 Protocolos de seguridad Punto a Punto para Autenticación

Existen varios protocolos punto a punto de autenticación cuyo fin es autenticar las conexiones establecidas de tal forma que estas sean segura. Se debe mencionar que la interacción de estos protocolos se produce en la capa 2 del modelo OSI (capa de enlace).

## 2.18 Protocolo 802.1X

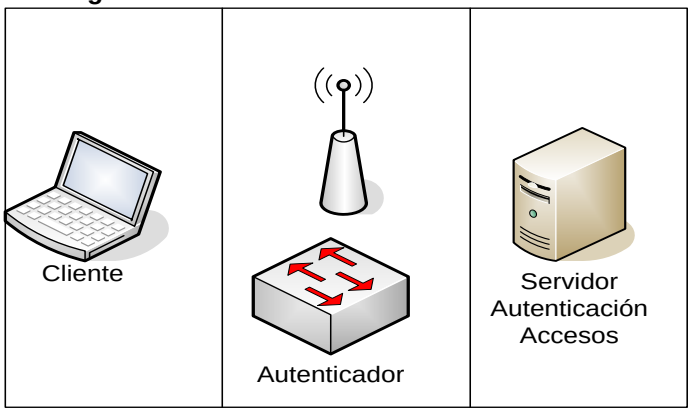
Según J. Zhang, Y. Guo, Y. Chen, & J. Ma, (2015, p. 618). ”802.1X se define como un protocolo el cual se lo denomina puerto basado en control de acceso a la red. El puerto puede ser físico o también puede ser lógico. El protocolo provee un esquema de autenticación de usuarios”. También se hace énfasis en el uso de EAP para la autenticación el cual actúa en una arquitectura basada en tipos de autenticación actuando de intermedio entre el solicitante (cliente) y el motor

de validación (servidor de autenticación) permitiendo la comunicación entre ambos.

802.1X transporta las credenciales desde el usuario suplicante (dispositivo móvil) al servidor de Autenticación, Para lo cual utiliza el protocolo EAP (Extensible Authentication Protocol).

Asegurando que las redes inalámbricas estén protegidas de robos de identidades. Al combinar 802.1X con el protocolo EAP también denominado EAPOL (EAP OVER LAN) se asegura de forma transparente la encapsulación y transporte de credenciales desde el suplicante (dispositivo móvil) al servidor de autenticación (servidor RADIUS). Ver figura 6.

**Figura 9.- Entidades en la interacción 802.1X**

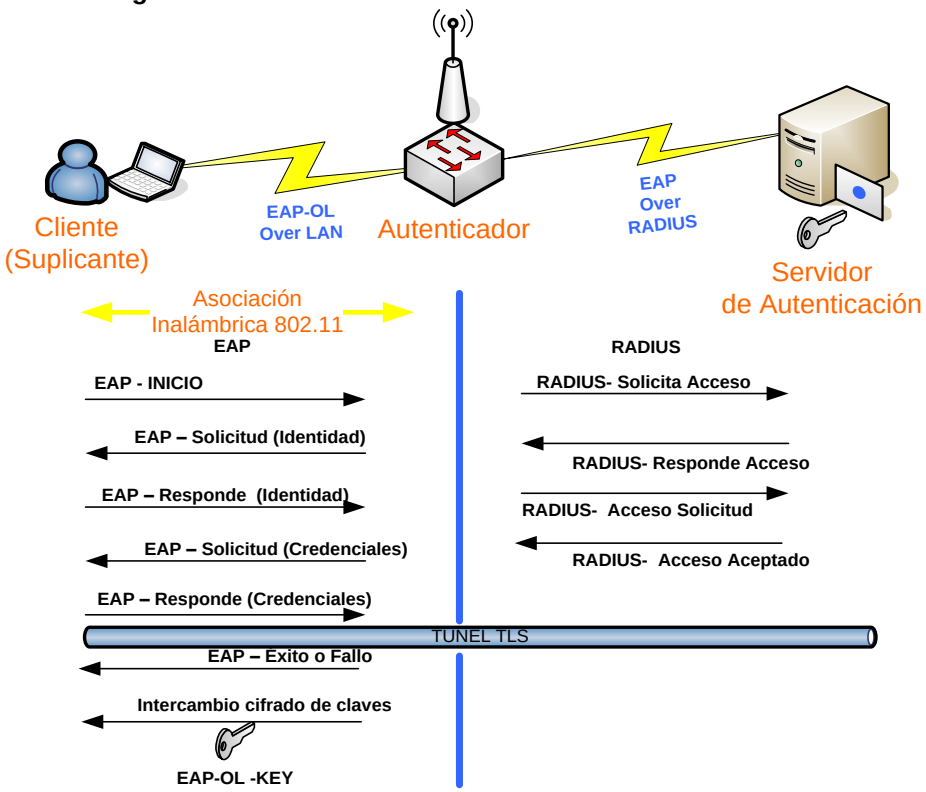



**Elaborado por: Jacobo Sarmiento**

## 2.19 Funcionamiento de Autenticación 802.1X

Siguiendo con lo expuesto por J. Zhang, Y. Guo, Y. Chen, & J. Ma, (2015, p. 618) “El objetivo de la autenticación 802.1X, es garantizar que el puerto sea utilizable, es decir, que para que un puerto se abra este debe ser autenticado correctamente permitiendo el pase de los mensajes, si no es aceptado, este se cerrara y permitiendo solo EAPOL” el proceso de autenticación tiene un flujo que va desde el suplicante hasta el servidor de autenticación, en la siguiente gráfica se puede apreciar como esta dada la asociación inalámbrica la cual siempre es desde el suplicante hasta el dispositivo Autenticador, ver figura 10.

**Figura 10.- Proceso autenticación 802.1x EAP - RADIUS**




**Elaborado por Jacobo Sarmiento**

## 2.20 EAP (Extensible Authentication Protocol)

Para J. Zhang, Y. Guo, Y. Chen, & J. Ma. (2015, p. 618) "Extensible Authentication Protocol es el método más usado entre el cliente y el switch. Este modo de autenticación alivia la carga del switch hasta cierto punto, porque el desafío y los procesos de computación son llevados a cabo por el servidor"

Según lo indicado por Dulaney, E., & Easttom, C., (2014, p.181) " Los estándares WPA y WPA2, han adoptado cinco esquemas EAP los cuales son: EAP-TLS (Extensible Authentication Protocol – Transport Layer Security), EAP-PSK (Extensible Authentication Protocol - Pre-Shared Security), EAP-MD5 (Extensible Authentication Protocol - Message Digest Algorithm-5), PEAP (Protected Extensible Authentication Protocol) siendo este último el más utilizado por la mayoría de sistemas operativos".

Pellejero I, Andreu F, Lesta A (2006, p.76) indica que "En función del método EAP seleccionado será posible emplear diferentes tipos de servidores RADIUS".

Implica que no todas los métodos EAP son compatibles en las diferentes plataformas RADIUS.

Continuando con Pellejero I, Andreu F, Lesta A (2006) las soluciones basadas en Microsoft soportan PEAP y TLS lo cual implica instalar un certificado en cada terminal de usuario. Sin embargo EAP-PEAP se basa en identificar el usuario y contraseña haciendo fácil su implementación. Es importante conocer esta característica para poder realizar una correcta implementación en plataformas Microsoft.

### 2.21 PEAP (Protected Extensible Authentication Protocol)

Para (Dulaney, E., & Easttom, C, 2014, p.182) “Es un protocolo creado por Cisco, RSA y Microsoft. Este protocolo apareció con Windows XP siendo incluido hasta la actualidad en las últimas versiones de los sistemas operativos de Windows. Se lo considera seguro porque establece un canal cifrado entre el suplicante (dispositivo móvil) y el servidor de autenticación (servidor RADIUS)”.

### 2.22 CHAP (Challenge Handshake Authentication Protocol)

(Dulaney, E., & Easttom, C, 2014, p.139) indica que CHAP “Es un protocolo de autenticación el cual no hace uso de claves compartidas. Durante la autenticación inicial se solicita al suplicante (dispositivo móvil) generar un numero aleatorio (por lo general es un algoritmo hash en MD5) para que este sea enviado al servidor periódicamente para lo cual el servidor de autenticación (servidor RADIUS) solicitara al suplicante ver ese número cada cierto tiempo para garantizar su autenticidad”2.23 MS-CHAP V2 (Microsoft - Challenge Handshake Authentication Protocol)

Es un protocolo de Microsoft el cual se efectúa mediante una autenticación de dos vías verifica la identidad de ambos lados de la conexión. El cliente de acceso remoto se autentica en el servidor de acceso remoto y el servidor de acceso remoto se autentica en el cliente de acceso remoto (Technet, M. 2010). ¿Que se obtiene con este protocolo? Se asegura que el cliente de acceso remoto que este

accediendo a un servidor de acceso remoto solicite la contraseña del usuario que requiere ingresar a la red de datos.

## 2.24 Algoritmos de Cifrado de datos

Los algoritmos de cifrado de datos se implementaron en los computadores partiendo del uso de métodos de encriptación que se utilizaban en tiempos remotos para ocultar información confidencial.

Estos algoritmos se han implementado a través de métodos matemáticos cuya finalidad es proteger la información desde que se emite hasta que se recibe.

## 2.25 AES

Según Boxcriptor (s.f) “Advanced Encription Standard (AES) El estándar de cifrado (encriptación) avanzado AES, Advanced Encryption Standard (AES), es uno de los algoritmos más seguros y más utilizados hoy en día - disponible para uso público. Está clasificado por la Agencia de Seguridad Nacional, National Security Agency (NSA), de los Estados Unidos para la seguridad más alta de información secreta”. Es básicamente un algoritmo de encriptación utilizado por varias entidades gubernamentales así como ambientes empresariales proporcionando un alto nivel de seguridad en cuanto al cifrado de información.

Asi mismo Boxcriptor (s.f) indica que “el algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de datos de 16 bytes - por lo que se le llama blockcipher “. En la actualidad existen AES-128, 192 y 256 bits.

## 2.26 Autoridad de Certificación

Como lo indica Dulaney, E., & Easttom, C. (2014) “Una autoridad de certificación es una organización que se encarga de la emisión, revocación y distribución de certificados. Un certificado es nada más que un mecanismo que asocia la clave pública con un individuo. Contiene una gran cantidad de información sobre el usuario”.

# CAPITULO 3

## 3. Metodología de la investigación

### 3.1 Enfoque y Tipo de Investigación

Se puede indicar que existen dos enfoques aplicados en la investigación las cuales se mencionan en este proyecto.

Para Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014, p.4) el enfoque cuantitativo “es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos brincar o eludir pasos. Parte de una idea que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación”.

Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014, p.7) menciona que el enfoque cualitativo “en lugar de que la claridad de las preguntas de investigación e hipótesis proceda de la recolección y el análisis de datos, los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y análisis de datos.

En el diseño del marco metodológico según Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014, p.90) indica que la investigación cuantitativa tiene 4 alcances que se detallan a continuación.

Estudio exploratorio “se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes” (Sampieri, R. H., Collado, C. F., & Lucio, P. B., 2014, p.91).

Estudio descriptivo “busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis” (Sampieri, R. H., Collado, C. F., & Lucio, P. B., 2014, p.92).

Estudio correlacional “tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una

muestra o contexto en particular" (Sampieri, R. H., Collado, C. F., & Lucio, P. B., 2014, p.93).

Estudio explicativo "van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas los eventos y fenómenos físicos o sociales" (Sampieri, R. H., Collado, C. F., & Lucio, P. B., 2014, p.95).

El tipo de investigación que se ha utilizado es de tipo Explorativa, esto debido al desconocimiento al momento de implementar mecanismos de seguridad para un control eficiente de los accesos a la red inalámbrica. Así como también se identifican los elementos que se necesitan para una posterior implementación de la solución propuesta.

La investigación de campo que se realiza se orienta a las PYMEs (Pequeñas Y Medianas Empresas). Enfocándose a la seguridad en la red inalámbrica de datos. Y como dar la solución a un problema de accesos sin control.

### 3.2 Método de Investigación

Según lo indica Bernal, C. (2006, p.55) "el método científico se entiende como el conjunto de postulados, reglas y normas para el estudio y la solución de los problemas de investigación, que son institucionalizados por la denominada comunidad científica reconocida".

Método deductivo "Es un método de razonamiento que consiste en tomar conclusiones generales para explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes, principios, etcétera, de aplicación universal y de comprobada validez, para aplicarlos a soluciones o hechos particulares" (Bernal, C., 2006, p.56).

Método inductivo-deductivo "Este es un método de inferencia basado en la lógica y relacionando con el estudio de hechos particulares, aunque es deductivo en un sentido (parte de lo general a lo particular) e inductivo en sentido contrario (va de lo general a lo particular)" (Bernal, C., 2006, p.56).

Método hipotético-deductivo "El método consiste en un procedimiento que parte de unas aseveraciones en calidad de hipótesis y busca refutar o falsear tales hipótesis, deduciendo de ellas conclusiones que deben confrontarse con los hechos" (Bernal, C., 2006, p.56).

Una vez que se han evaluado los métodos anteriormente expuestos, el método de investigación a utilizar es inductivo-deductivo debido a que parte de una problemática general y se puede llegar a un objetivo específico.

De allí se determina que deben existir criterios que validen la implementación de la arquitectura AAA. La cual puede ser adoptada en pequeñas y medianas empresas. Estos criterios se los expone a continuación:

1. Las pequeñas y medianas empresas implementan cada vez más redes inalámbricas de tal manera que son de uso cotidiano por ser de gran utilidad en el desempeño de sus colaboradores.
2. Esta expansión de redes inalámbricas en las empresas no siempre posee mecanismos de seguridad efectivos aplicados a los puntos de acceso inalámbricos.
3. Con el crecimiento y expansión de la red inalámbrica los administradores de redes en ocasiones se descuidan de quienes acceden y los permisos que deben ser concedidos a los usuarios o grupos de usuarios.

De estos criterios se pretende demostrar que al utilizar una arquitectura AAA existirá un mejor control de acceso y utilización de mecanismos de seguridad en una red inalámbrica. De tal forma que implementando este esquema se dará solución a los problemas encontrados, siendo esta una solución factible que puede ser implementada por los administradores de redes.

### 3.3 Población

Para Tamayo, M. (2004, p180)."Población es la totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis o entidades de población que integra dicho fenómeno y que debe cuantificarse para un determinado estudio integrando un conjunto N de entidades".

La población en la que se realiza esta investigación, esta encaminada a las empresas pequeñas y medianas, las mismas que poseen una infraestructura de red propia administrada por su departamento de TI.

Según el INEC en su última estadística realizada en el año 2014, considera que una empresa es pequeña o mediana por medio de dos criterios, el rango de ventas comprendido entre $1'000.000 a $5'000.000 y el rango de empleados de 10 a 49 personas o de 50 a 199 personas. (INEC, E., 2014).

Así mismo indica que existen 78652 PYMEs (Pequeñas Y Medianas Empresas) a nivel nacional de las cuales el sector comercial es la actividad económica que ocupa el segundo lugar.

### 3.4 Muestra

Según Tamayo, M. (2004, p180)." Para determinar el tamaño de la muestra debe tenerse en cuenta los parámetros de la población que se desea investigar; el rango de invalidez o infidedignidad permisible en las estimaciones y una estimación aproximada de la distribución de la característica de la investigada en la población".

Para la muestra se toma como fuente los índices estadísticos que según el último censo del INEC realizado en el año 2014 indican que aproximadamente el 21% equivalente a 16355 se encuentran en la ciudad de Guayaquil donde se sitúan las sedes de las empresas que cuentan con mayor infraestructura tecnológica.

Sin embargo hay que indicar que la solución propuesta se aprovecha con mayor eficiencia en empresas cuyo número de usuarios está entre 50 y 200 personas ya que allí es donde se presentan más problemas en el control de usuarios y en este rango aún se consideran una empresa como PYMEs (Pequeñas Y Medianas Empresas).

Partiendo de estos dos criterios se obtiene el total de 3234 empresas domiciliadas en la ciudad de Guayaquil.

**Figura 11.- Encuesta del INEC**

**Número de empresaspara PYMES, nivel nacional y cantón Guayaquil, año 2014.**

| Tamaño | Nacional | Guayaquil |
|---|---|---|
| Pequeña empresa | 65,135 | 13,121 |
| Mediana empresa "A" | 7,929 | 1,869 |
| Mediana empresa "B" | 5,588 | 1,365 |

***Fuente: Instituto Ecuatoriano de Estadísticas y Censos***

Para esta investigación se va a seleccionar como población en la encuesta a 12 empresas, que son consideradas como PYMEs (Pequeñas Y Medianas Empresas), se selecciona esta población porque cuentan con la infraestructura tecnológica, números de usuarios, ancho de banda y cantidad de dispositivos móviles adecuados.

Se tomara un nivel de confianza de 85% con un margen de error del 15% utilizando la siguiente fórmula para determinar la muestra:

$$\mathrm{n}= \frac{k^2 * p * q * N}{\left(e^2 * (N-1)\right) + k^2 * p * q}$$

**Donde:**

**N**:Tamaño de la población
**K**: constante depende del nivel de confianza que se asigna
**e**: Error de la muestra
**p**: población con característica de estudio
**q**: población sin características de estudio
**n**: Tamaño de la muestra

Reemplazando los valores escogidos se obtiene una muestra de **n= 8**

$$n = \frac{1.44^2 * 0.5 * 0.5 * 12}{\left(0.15^2 * (12-1)\right) + 1.44^2 * 0.5 * 0.5}$$

$$n = \frac{2.0736 * 0.5 * 0.5 * 12}{(0.0225 * 11) + 2.0736 * 0.5 * 0.5}$$

$$n = \frac{6.2208}{0.2475 + 0.5184}$$

$$n = \frac{6.2208}{0.7659}$$

$$n = 8$$

### 3.5 Técnicas y herramientas de colección de información

Según Ross, S. M. (2007, p.3) “En ocasiones un análisis estadístico comienza con un conjunto de datos: por ejemplo, el gobierno habitualmente reúne datos sobre la tasa de desempleo y sobre el producto interior bruto. La estadística se utiliza después para describir, clasificar y analizar esos datos”.

Una vez que se obtuvo la muestra se procede a planificar citas con las empresas y sus representantes en el área de TI, quienes son los indicados a colaborar en el proceso de levantamiento de información. Para lo cual se procede al uso de las herramientas de recolección de datos como son las entrevistas y encuestas.

Ambas herramientas serán aplicadas tanto al administrador de red o encargado del área de TI, con la intención de obtener su percepción sobre el control que se está ejerciendo en su red de datos inalámbrica y el tipo de mecanismos de seguridad que se ha implementado.

Se prevé obtener una percepción del impacto que tienen las herramientas que utilizan en su infraestructura tecnológica como también de que manera influyen en el usuario final. Finalizada dichas entrevistas y encuestas se obtienen datos estadísticos que son procesados y analizados.

Para Tamayo, M. (2004, p.312).”Instrumento de observación formado por una serie de preguntas formuladas y cuyas respuestas son anotadas por el empadronador”. Se puede decir que las encuestas son el tipo de técnicas de recolección de información más utilizada, debido a que es fácil de estructurar y permitir una recopilación masiva de la información.

Dependiendo de la forma como se contacta al encuestado se determina como se administran los datos que pueden ser:

- Encuesta por e-mail
- Encuesta por videoconferencia
- Encuesta telefónica
- Encuesta por plataformas en Internet
- Encuestas presenciales (Bernal. 2006)

Para el levantamiento de la información se realizan encuestas por videoconferencia y telefónica las cuales fueron planificadas para no interrumpir las labores del encuestado.

Según Llauradó, O. (2014). Indica que la escala Likert "Resulta especialmente útil emplearla en situaciones en las que queremos que la persona matice su opinión. En este sentido, las categorías de respuesta nos servirán para capturar la intensidad de los sentimientos del encuestado hacia dicha afirmación". En el caso particular del diseño de esta encuesta se tomó como referencia la aplicación de la escala de Likert, con un número de 5 respuestas las cuales ayudaran a determinar el grado de rechazo o satisfacción del encuestado, es bastante visual y amigable ante el encuestado.

También se pretende a través de este tipo de encuesta descubrir el nivel de acuerdo con una afirmación o rechazo con una respuesta negativa, la frecuencia con que realiza una determinada actividad, el grado de importancia que le da, la valoración y la probabilidad que pueda realizar una determinada acción.

La tabulación de las encuestas será mucho más rápida de tal forma que al momento de analizar los datos y colocar su respectiva ponderación no se encuentren valoraciones intermedias.

El tipo de encuesta aplicada es exploratorio que permita elaborar un análisis basado en la hipótesis del tema que se investiga. De esta forma se determinará la valides del estudio y se verificará las variables orientadas a dar una solución al problema de seguridad que puedan presentarse en una corporación.

Según Bernal. (2006, p.184) indica que la entrevista “es la relación directa establecida entre el investigador y su objeto de estudio a través de individuos o grupos con el fin de obtener testimonios orales”.

Se debe tener en claro que al momento de realizar la entrevista, el entrevistador debe conocer el tema de tal manera que pueda llevar el hilo de la entrevista sin que esta sufra un desorden o se esquiva del tema al cual se hace referencia. La misma que puede ser orientada hacia un problema específico generando en el entrevistado una actitud de auto-observación y auto-exploración.

Dentro de los consejos que se puede dar para un mejor desenvolvimiento del entrevistado están:

- Se le permita usar una forma narrativa.
- Cuando se le interrumpe menos.
- Cuando se le anima a seguir un orden cronológico.
- Cuando las preguntas se utilizan únicamente para suscitar narraciones. Bernal. (2006, p.185)

En el transcurso de la investigación se solicitó por parte de los encuestados, que la información que se ha compartido sea de carácter confidencial. Los encargados del área de TI solicitaron no mencionar sus nombres y menos el de las compañías para las cuales prestan sus servicios profesionales.

# CAPITULO 4

# 4. Análisis y discusión de los resultados

## 4.1 Análisis y procesamiento de datos

La investigación de campo se la realizó a los encargados del área de TI o administradores de redes que conocen la infraestructura tecnológica (servidores, dispositivos de comunicación y topología de la red) de la empresa para la cual prestan servicio. La encuesta fue realizada a 8 empresas PYMEs (Pequeñas Y Medianas Empresas) de diferentes sectores económicos de la ciudad de Guayaquil.

Para este proceso se optó por la utilización de la herramienta de Microsoft office Excel. Que permite realizar la tabulación de datos, así como también la generación de gráficos estadísticos.

Definida la herramienta de procesamiento de datos se procede a realizar las encuestas de forma digital para poder enviarla a cada una de las personas que son participes del levantamiento de información y así facilitar la recopilación de datos.

Las preguntas contienen como respuesta 5 categorías las cuales son: Excelente, Muy Buena, Buena, Regular, Deficiente. La tabulación que se realice será sencilla y eficaz.

Según el valor que se haya obtenido por cada categoría en cada pregunta se calculará el porcentaje de participación. De esta forma se podrá construir los gráficos estadísticos a partir de los datos procesados

El gráfico que se ha elegido es el de tipo pastel siendo el gráfico ideal cuando las categorías a representar no superan las 5 categorías. Con esta información se procede a realizar el debido análisis e interpretación de datos.

Con la información proporcionada mediante encuestas y entrevistas se podrá validar las variables que permitan demostrar la factibilidad de la implementación del proyecto que se ha propuesto.

## 4.2 Resultados de las encuestas

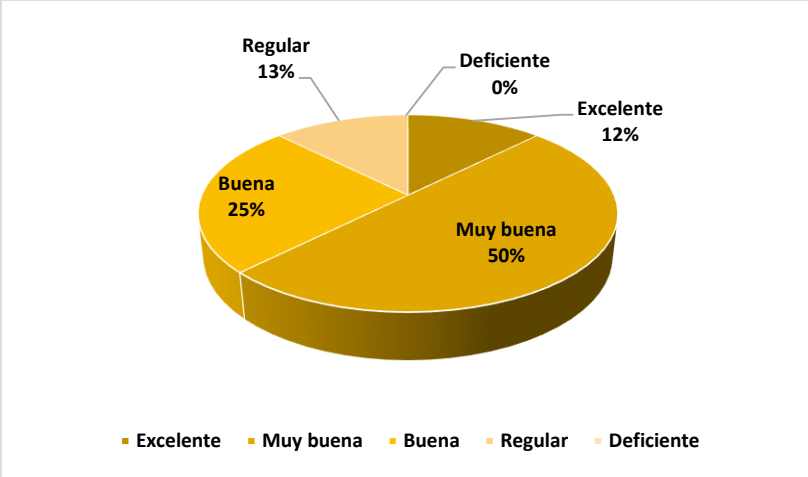
1. Los dispositivos de comunicación alámbricos e inalámbricos que forma parte de la infraestructura de red de su empresa, ¿cómo los considera?

**Tabla 4 Resultado de la pregunta 1 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 1 | 4 | 2 | 1 | 0 | 8 |
| 12.50% | 50.00% | 25.00% | 12.50% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 12.- Pregunta 1**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 1:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 12.50% de encuestados indican que la infraestructura de su red es excelente, para el 50% es muy buena, para el 25% es buena, para el 12.50% es regular y el 00.00% la considera de deficiente. Los dispositivos inalámbricos son de tipo Enterprise y en algunos casos tipo Home, esto no es impedimento ya que se puede actualizar el firmware con software propio de la marca del dispositivo o software libre.

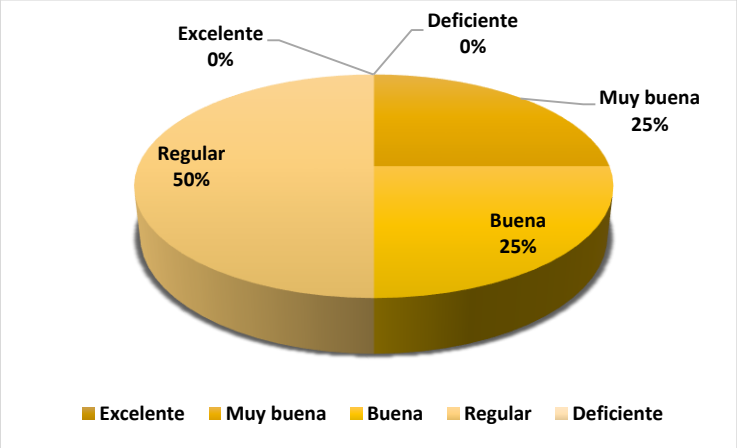
2. El control de accesos a los usuarios que ingresan a su red de datos corporativa por dispositivos inalámbricos es:

**Tabla 5 Resultado de la pregunta 2 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 0 | 2 | 2 | 4 | 0 | 8 |
| 0.00% | 25.00% | 25.00% | 50.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 13.- Pregunta 2**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 2:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 00.00% de encuestados califica de excelente el control de accesos a los usuarios que ingresan red de datos corporativa por dispositivos inalámbricos, el 25% de los encuestados considera de muy buena, el otro 25% la considera de buena el 50 % indica que es regular y finalmente el 00.00% la considera deficiente. Se puede apreciar que no se ejerce un control riguroso a los usuarios que acceden a la red de datos corporativa a través de los dispositivos de comunicación inalámbricos.

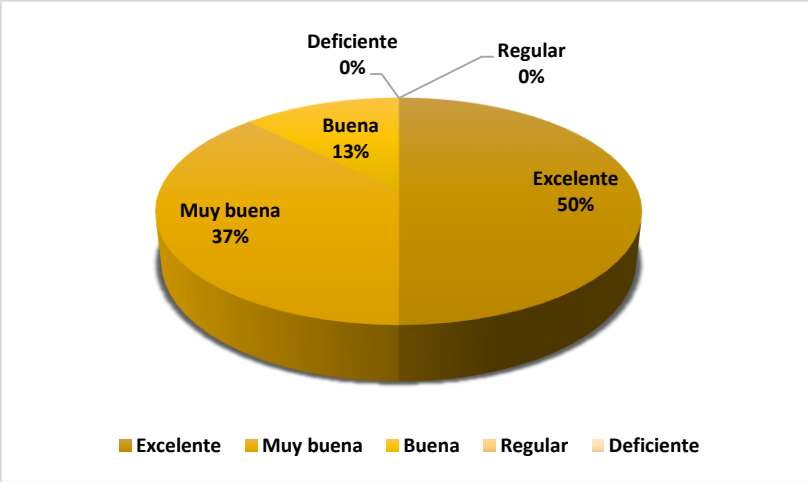
3. El esquema de administración que les proporciona el directorio activo de Windows (Unidades Organizativas Usuarios Equipos Directivas de Grupo entre otros) ¿cómo la calificaría?

**Tabla 6 Resultado de la pregunta 3 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 4 | 3 | 1 | 0 | 0 | 8 |
| 50.00% | 37.00% | 13.00% | 00.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 14.- Pregunta 3**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 3:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 50.00% de encuestados califica de excelente el esquema de administración que les proporciona el directorio activo, para el otro 37.00% de los encuestados es muy buena, el 13.00 % indica que es buena y finalmente para el 00.00% la considera regular y deficiente. Se puede denotar que el directorio activo de Windows es una de las herramientas más usada por parte de los administradores de red para gestión y administración de usuarios.

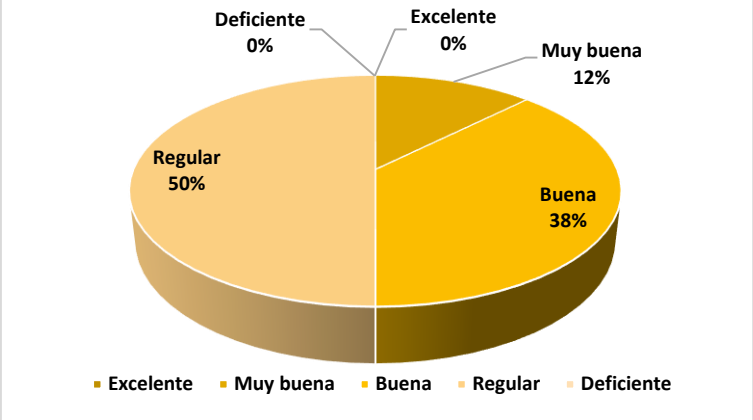
4. La identificación de los dispositivos móviles o usuarios que acceden por los dispositivos de comunicación a la red de datos corporativa es:

**Tabla 7 Resultado de la pregunta 4 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 0 | 1 | 3 | 4 | 0 | 8 |
| 00.00% | 12.00% | 38.00% | 50.00% | 0.00% | 100.00% |

**Elaborado por: Jacobo Sarmiento**
**Fuente: Encuesta**

**Figura 15.- Pregunta 4**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 4:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 00.00% de encuestados califica de excelente la identificación de los dispositivos móviles o usuarios que acceden a la red corporativa a través de los dispositivos inalámbricos, el 12.00% de encuestados la califica de muy buena, el 38.00% de los encuestados indican que es buena mientras que el 50.00 % indica que es regular y finalmente el 00.00% la califica defectuosa. No existe una identificación adecuada y precisa de los dispositivos móviles o usuarios que acceden a la red inalámbrica por lo tanto no se puede determinar si son externos o internos.

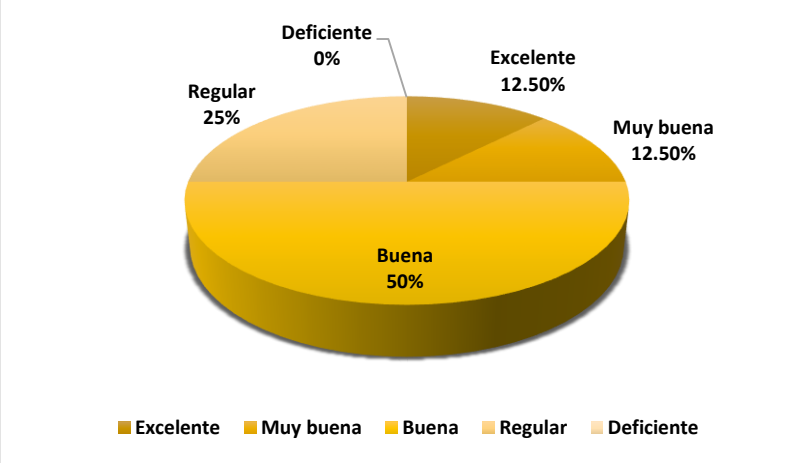
5. Los usuarios que acceden a la red mediante los dispositivos de comunicación inalámbrica mencionan que el servicio de conexión y disponibilidad que se ofrece es:

**Tabla 8 Resultado de la pregunta 5 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 1 | 1 | 4 | 2 | 0 | 8 |
| 12.50% | 12.50% | 50.00% | 25.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 16.- Pregunta 5**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 5:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 12.50% de encuestados califica de excelente el servicio de conectividad y disponibilidad que se ofrece mediante los dispositivos de comunicación inalámbricos, el 12.50% de encuestados la califica de muy buena, el 50.00% de los encuestados indican que es buena, el 25.00 % indica que es regular y finalmente el 00.00% la califica defectuosa. La percepción que se obtiene es que los usuarios que utilizan las redes inalámbricas no gozan de un buen servicio de conectividad en la mayoría de las empresas encuestadas.

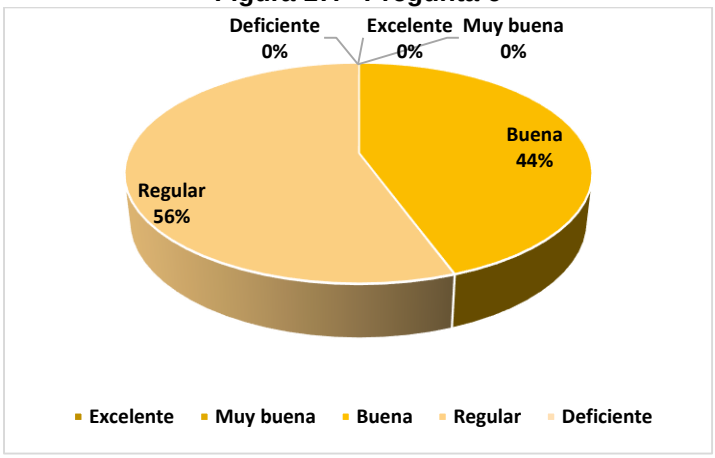
6. ¿Cómo calificaría la administración de las claves de acceso e identificadores de red de los dispositivos inalámbricos en su empresa?

**Tabla 9 Resultado de la pregunta 6 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 0 | 1 | 3 | 4 | 0 | 8 |
| 00.00% | 12.00% | 38.00% | 50.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 17.- Pregunta 6**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 6:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 00.00% de encuestados califica de excelente la administración de las claves de acceso e identificadores de red de los dispositivos inalámbricos, el 00.00% de encuestados la califica de muy buena, el 44.00% de los encuestados indican que es buena mientras que el 56.00 % indica que es regular y finalmente el 00.00% la califica defectuosa. En la mayoría de las empresas se puede apreciar que no poseen un control continuo para el cambio o actualización de claves de acceso que en ocasiones no se actualizan para evitar cargas operativas al departamento de TI.

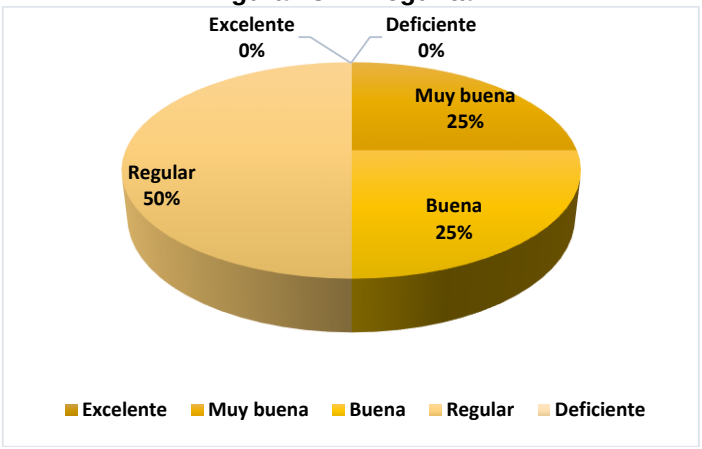
7. Considera que las herramientas de administración para gestión de la red implementadas en su empresa de datos son:

**Tabla 10 Resultado de la pregunta 7 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 0 | 2 | 2 | 4 | 0 | 8 |
| 00.00% | 25.00% | 25.00% | 50.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 18.- Pregunta 7**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 8:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 00.00% de encuestados califica de excelente las herramientas de administración y gestión de la red implementadas en su empresa, el 25.00% de encuestados la califica de muy buena, para el 25.00% de los encuestados es buena mientras que el 50.00 % la califica de regular y finalmente el 00.00% la valora defectuosa. En la mayoría de las empresas se puede apreciar que las herramientas de administración para gestión de la red son positivas para departamento de IT, siempre y cuando sean bien aplicadas y aprovechadas.

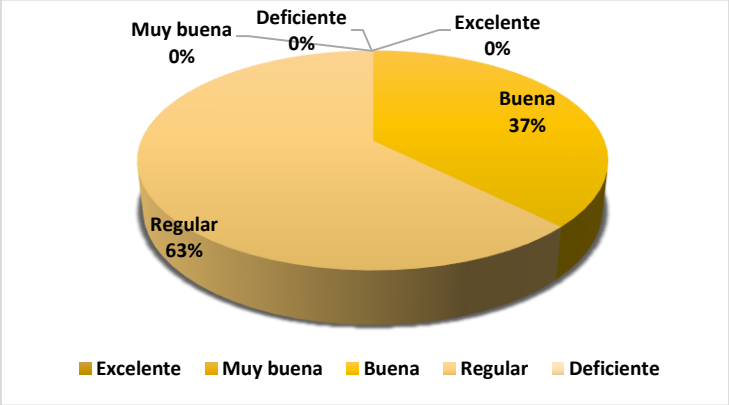
8. Los mecanismos de seguridad aplicados a los dispositivos de comunicación en su empresa son:

**Tabla 11 Resultado de la pregunta 8 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 2 | 2 | 4 | 0 | 0 | 8 |
| 50.00% | 25.00% | 25.00% | 00.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 19.- Pregunta 8**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 8:** Se encuesto a 8 administradores de red o encargados del área de TI, donde se observa que el 00.00% de encuestados Los mecanismos de seguridad aplicados la red que se implementan en su empresa, el 00.00% de encuestados la califica de muy buena, para el 37.00% de los encuestados es buena mientras que el 63.00 % considera de regular y finalmente el 00.00% la valora de defectuosa. En la mayoría de las empresas se puede apreciar que los mecanismos de seguridad aplicados no satisfacen las áreas de IT los factores pueden ser básicamente por presupuesto.

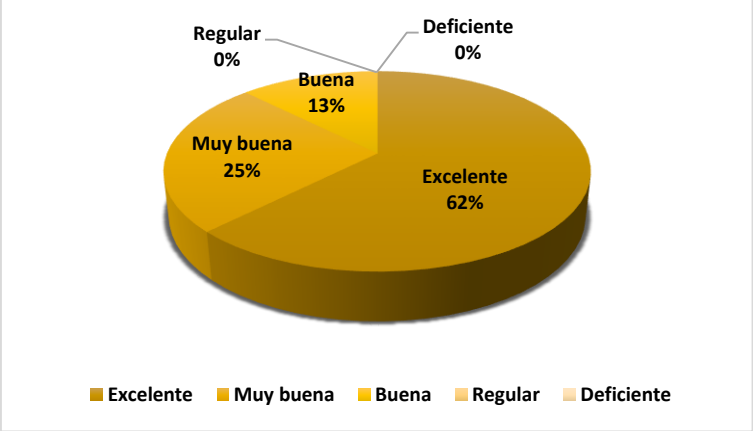
9. De introducir la arquitectura de autenticación, autorización y registro (AAA), a su red inalámbrica ¿Cómo calificaría el aporte de esta tecnología?

**Tabla 12 Resultado de la pregunta 9 (Administrador de Red o encargado área TI)**

| Excelente | Muy buena | Buena | Regular | Deficiente | Total |
|---|---|---|---|---|---|
| 5 | 2 | 1 | 0 | 0 | 8 |
| 63.00% | 25.00% | 13.00% | 00.00% | 0.00% | 100.00% |

***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Figura 20.- Pregunta 9**




***Elaborado por: Jacobo Sarmiento***
***Fuente: Encuesta***

**Análisis de datos pregunta 9:** Se encuesto a 8 administradores de red o encargados del área de IT, donde se observa que el 63.00% de encuestados les gustaría contar con la arquitectura de autenticación, autorización y registro (AAA), en su empresa, el 25.00% de encuestados la califica de muy buena, para el 13.00% de los encuestados es buena mientras que el 00.00 % la considera de regular y el 00.00% restante la considera defectuosa. Después de explicar los beneficios de la implementación de la arquitectura AAA se pudo tener una buena aceptación por parte de los implementadores de la red ya que sería de vital importancia en la administración y gestión de la red con un robusto esquema de seguridad.

# CAPITULO 5

## 5. La Propuesta

### 5.1 Resumen Ejecutivo

El presente trabajo de grado consiste en el diseño de un sistema de autenticación y gestión para una red inalámbrica, fundamentado en la arquitectura AAA.

La intención es evitar el acceso de terceros a la red de datos y proporcionar un sistema de seguridad más robusta a los dispositivos de comunicación inalámbrica en una PYMEs (Pequeña y Mediana Empresa), otorgándole una herramienta de gestión al administrador de la red. El desarrollo de este trabajo de grado está definido en cinco capítulos que van desde la problemática hasta una solución propuesta.

En el primer capítulo, se observan los factores que afectan a las redes inalámbricas y dan origen a un problema de seguridad, se definen los objetivos así como el alcance de la solución.

En el segundo capítulo, se habla de la Arquitectura AAA y los componentes que la conforman, así como de los protocolos de seguridad que se implementaran en el servidor RADIUS.

El tercer capítulo, explica el tipo de investigación realizada así como la aplicación de instrumentos estadísticos, y herramientas de investigación, aplicada a los administradores de la red de datos

El cuarto capítulo, es el análisis y procesamiento de los datos para poder obtener conclusiones de la información obtenida.

En el quinto capítulo, se presenta un análisis FODA y las estrategias que conforman la solución así como el porqué de la solución elegida. Finalmente se exponen las conclusiones y recomendaciones que se derivan de esta investigación.

## 5.2 Análisis situacional del entorno

Para lograr llegar al diseño que se plantea se debió realizar un análisis FODA para determinar las fortalezas, oportunidades, debilidades y amenazas que se pueden presentar durante el desarrollo de la implementación

Según Barrios, A. Z. (2011, p.85) “Combinando los factores externos (amenazas y oportunidades) y los factores internos (debilidades y fortalezas). Identificados estos elementos externos e internos, luego de un análisis de confiabilidad, se puede establecer unas líneas gruesas de carácter estratégico para la institución”. Tal como se indica se debe identificar los factores y los entornos internos y externos para trazar las estrategias a utilizar en el desarrollo de un proyecto.

Partiendo de esta perspectiva se procede a realizar el respectivo análisis FODA.

### 5.2.1 Fortalezas

Al hablar de fortalezas que se aplican en el desarrollo de este proyecto se menciona como beneficio el sistema operativo Microsoft Windows Server 2012 ya que aunque tiene un costo por la licencia, incluye la administración del directorio activo y las directivas de grupo el cual no tiene una versión igual o superior en software gratuito y además porque trae sus propios servicios de red y diferentes roles de administración como virtualización los cuales son de gran ayuda al momento de obtener los mejores resultados en la implementación de la arquitectura AAA.

Los sistemas operativos que se encuentran en los computadores de las empresas, que utilizan los usuarios permiten métodos y mecanismos de seguridad para el intercambio del login y contraseña.

La disponibilidad, escalabilidad, administración, seguridad y sobre todo la utilización de normas fortalece la utilización del servidor RADIUS desde la perspectiva de la arquitectura AAA.

### 5.2.2 Oportunidades

En la actualidad las empresas están fijando su mirada cada vez más en la seguridad que se le pueda dar a la información. Por lo que cada día crece la necesidad de implementar mecanismos de seguridad que no solamente van aplicados al software sino al hardware

Sin embargo existe varias plataformas de acceso pagado y libre los cuales son aplicables en los diferentes entornos ya sea de hogar como empresarial.

La arquitectura AAA evoluciona con el pasar del tiempo haciendo que a corto plazo llegue a convertirse en una política de seguridad que deba instaurarse en los departamentos de TI de las empresas.

Se plantea instaurar la arquitectura AAA en un futuro, aplicando la misma lógica de seguridad al momento de iniciar una sesión, para acceder a la configuración de un dispositivo de comunicación, pudiendo ser estos un: Router, Firewall, Switch, Access Point, entre otros.

### 5.2.3 Debilidades

Las debilidades en la implementación de la arquitectura AAA se enfocan en los siguientes puntos:

- Infraestructura de hardware o software obsoleto o desactualizada, no permitirá la implementación de la arquitectura AAA.
- Adquisición de nuevos dispositivos de acceso inalámbrico.
- Desaprobación o rechazo por parte de los usuarios al momento de realizar la implementación.
- La no implementación de políticas y mecanismos de seguridad que resguarden la información de la empresa.

Se prevé disminuir o evitar esta debilidad con un previo levantamiento de información así como la demostración de un piloto de prueba en el sitio donde se vaya a introducir la implementación

### 5.2.4 Amenazas

Dentro de las amenazas que se podrían presentar para no implementar la arquitectura AAA, se encuentran las siguientes:

- Dificultad en la adquisición de los equipos por temas externos como la importación de los mismos al no encontrarse en el país.
- Si algún método o estándar llegase a ser quebrantado puede quedar desprotegida la red de datos inalámbrica.
- Si algún dispositivo no es compatible con la arquitectura AAA, ya sea en hardware o software
- La falta de soporte o actualización del protocolo RADIUS o la creación de un nuevo protocolo para la Arquitectura AAA, la cual imposibilite seguir con el desarrollo e implementación de este tipo de seguridad.

## 5.3 Planteamiento Estratégico

La seguridad aplicada a la red inalámbrica se basa en la arquitectura AAA, por lo tanto el proceso se inicia cuando se realiza la entrega de credenciales por parte del usuario para que este pueda acceder a la red de datos utilizando su dispositivo móvil. Sin embargo este proceso debe ser soportado sobre la infraestructura de Hardware que incluye al servidor de dominio y los roles que soportan el protocolo RADIUS el cual es parte de la arquitectura AAA, así como los dispositivos de comunicación de la red de datos.

La estrategia planteada se basa en proporcionar servicios y métodos de seguridad para protección ante posibles intrusos el cual involucra procesos internos del departamento de TI.

Se deben valorar los siguientes ítems al momento de implementar la arquitectura AAA.

- Cantidad de usuarios que usan la red inalámbrica.
- Cantidad de dispositivos inalámbricos y móviles.

- Recursos a los cuales acceden (unidades de red, impresoras, servidores)
- El tráfico de datos de la red inalámbrica tanto del ancho de banda del internet como el que se genera por el uso de los servidores de datos.

Identificado estos ítems se puede proceder a realizar una evaluación y análisis de tres pilares que soportaran la arquitectura AAA:

- Infraestructura de servidores involucrando el tipo de hardware y software.
- Topología de la red inalámbrica corporativa.
- La seguridad aplicada en las distintas capas del modelo OSI.

Finalmente se debe adaptar o diseñar el escenario donde se implementará la arquitectura AAA para la red inalámbrica. Esto implica lo siguiente:

- El Hardware debe poseer las características mínimas para un piloto de prueba y posterior puesta en producción. Otro de los escenarios para optimizar el hardware podría ser la virtualización.
- El Software del servidor debe tener tecnología Microsoft ya que se utilizará características de conectividad e integración con el directorio activo.
- Las características AAA basadas en la autenticación y autorización estarán aplicadas mediante políticas a todos los usuarios que se encuentren en el directorio activo de Microsoft.

La preparación del administrador de la red es importante, ya que es quien gestiona y administra la red. El mismo que identifica una brecha de seguridad en el acceso a través de los dispositivos inalámbricos. Posibilitando a los usuarios propios o ajenos a la empresa la libre navegación en la red corporativa.

El administrador de la red deberá ser instruido en las herramientas que proporciona Microsoft para la implementación del protocolo RADIUS

Los dispositivos de comunicación pueden tener dentro de su propio firmware el mecanismo de seguridad que se adapta al protocolo RADIUS. De no poseer

el mecanismo de seguridad apropiado, se realizará una actualización con un firmware libre.

La creación de políticas de seguridad para los usuarios o los grupos de usuarios mediante las directivas de grupo que se configuren en el directorio activo de Microsoft. Cuyo fin es asignar y limitar el acceso a los recursos de la red que se asigne a cada empleado de la compañía. La flexibilidad y movilidad que los dispositivos otorguen a los usuarios aumentando el nivel de seguridad cuando los usuarios se trasladen a lo largo de las zonas donde existan mayor cobertura.

La distribución de los puntos de acceso inalámbricos permitirá la conexión de dispositivos móviles facilitando el acceso de los usuarios a la red inalámbrica corporativa para lo cual se debe tener en cuenta las siguientes características:

- El tipo de seguridad proporcionado por el dispositivo de comunicación.
- La velocidad de transmisión de datos.
- La cobertura de los dispositivos inalámbricos.
- Facilidad en la administración y agrupamiento de dispositivos.

La planeación del piloto de prueba se realizará con un grupo reducido de usuarios y eligiendo las zonas de menos concurrencia para evitar un posible rechazo u oposición al cambio si existiese un problema. Los usuarios que se conecten a la red lo harán de forma automática sin que soliciten una clave.

La puesta en marcha de la arquitectura AAA se cumplirá con la configuración de los puntos de acceso inalámbricos, el servicio NPS para el protocolo RADIUS y la aplicación de las políticas a los usuarios. Es fundamental el soporte al usuario el cual garantizará el correcto funcionamiento de la solución como así evitara posibles rechazos por parte de los usuarios.

### 5.4 Planteamiento Operativo

Evaluar los recursos con los que cuenta la empresa es importante al momento de realizar la adquisición o implementación de tecnología e incluso para el presupuesto en el área de TI.

Sin embargo se debe considerar el recurso humano y financiero que tenga asignado el área de TI. La empresa debe contar con el personal adecuado que pueda ejecutar el proyecto de preferencia debe estar coordinado por el administrador de redes y soportado por los técnicos del área de TI.

La función principal del administrador de redes será el análisis y evaluación de la infraestructura de red y la de los técnicos configurar los dispositivos de acceso y brindar el respectivo soporte a los usuarios.

El diseño de la red es fundamental al momento de implementar la arquitectura AAA. Las configuraciones de los dispositivos de comunicación y los servidores de aplicación son de vital importancia ya que estos también definen el rendimiento de la red.

Los recursos tecnológicos de hardware y software deben ser analizados y evaluados por el responsable del proyecto con las siguientes características:

**Tabla 13 Características Software, Hardware, Dispositivo de Comunicación**

| Software | Hardware | Dispositivo de Comunicación |
|---|---|---|
| • Licencia Microsoft Windows server 2012 R2 Standard | • Procesador Intel Xeon o Core i7<br>• Memoria 4 Gb<br>• Disco Duro 500 TB<br>• Tarjeta de Red 10/100/1000 | • Access point de la línea empresarial |

**Elaborado por: Jacobo Sarmiento**

De no contar con el recurso tecnológico, se realizó una investigación con valores aproximados para la inversión en la infraestructura tecnológica:

**Tabla 14 Valores Aproximados Software, Hardware y Dispositivos de Comunicación**

| | | |
|---|---|---|
| **Software (Servidor)** | • Licencia Microsoft Windows server 2012 R2 Standard | $800 |
| **Hardware (Servidor)** | • Procesador Intel Xeon o Core i7<br>• Memoria 4 Gb<br>• Disco Duro 500 TB<br>• Tarjeta de Red 10/100/1000 | $1100 |
| **Dispositivo de Comunicación** | • Access Point de preferencia la línea empresarial | $260 |

**Elaborado por: Jacobo Sarmiento**

En el mercado existen alternativas para el hardware del servidor y los dispositivos de comunicación.

### 5.5 Evaluación de la propuesta

Los proyectos informáticos tienen como objetivo dar una solución a un problema, el impacto que genere sobre la empresa así como el valor agregado serán visibles luego de la implementación, los resultados se darán en un espacio corto de tiempo. Por lo que la propuesta será evaluada basado en los siguientes ítems:

Seguridad: solo los usuarios autorizados podrán acceder a la red, evitando el robo de información mediante la captura de las ondas de transmisión realizada por terceros, a esto se le suma que la información llegara cifrada.

Consumo de ancho de banda: al existir restricciones el consumo de ancho de banda por terceros será tangible al momento de navegar por internet.

Mejora en la presentación de reportes a gerencia: esto se realiza basado en los usuarios que acceden a la red y el consumo de recursos.

Aplicación de restricciones: sea esta por usuarios o grupos de usuarios, si un usuario se desvincula de la empresa, no es necesario el cambio de claves a los dispositivos de red donde tenía acceso.

# CONCLUSIONES

El diseñar e Implementar una arquitectura AAA basada en seguridad de la red, en cualquier tipo de organización o empresa, involucra tomar muchas consideraciones que parten del diseño de la arquitectura.

Para lo cual se utiliza el servicio NPS de Microsoft Windows Server 2012 en conjunto con dispositivos de red, que posean el método WPA2-Enterprise asociado al Directorio Activo de Windows, el cual permite el control de acceso a la red mediante un único perfil de acceso, todo esto gracias a la correcta implementación del servidor RADIUS con los protocolos 802.1x y EAP-TLS.

Los dispositivos como se mencionó, deben soportar 802.1x que básicamente va ligado al método WPA2-enterprise, e incluso la mayoría de empresas han adquirido dispositivos de comunicación inalámbricos con estas características.

Sin embargo también se debe tener en claro el entorno tecnológico y los servicios que la red de datos ofrece, partiendo desde el hardware, software, topología de la red, dispositivos de red, las políticas de TI que se aplican en la gestión y control de la red, así como los mecanismos de seguridad utilizados por ejemplo el bloqueo de acceso por la dirección MAC de los dispositivos y sobre todo el presupuesto asignado al área de TI.

El escenario que se eligió para esta propuesta no fue realizada en software libre debido a que las empresas que se encuesto tienen software propietario en este caso Microsoft. Esto no quiere decir que aplicar RADIUS en software libre sea inequívoco sin embargo se trata de aprovechar al máximo los recursos que ya están puestos en marcha en la empresa. A esto se suma que la vinculación del directorio activo al servidor RADIUS no involucra muchos costos operativos o quita disponibilidad a la red de datos inalámbrica que ya está operativa.

El resultado que se obtiene es un sistema AAA de seguridad en dispositivos de comunicación, protección de la información, control de accesos a usuarios y sobre todo la gestión de recursos.

# RECOMENDACIONES

Se recomienda implementar un piloto para las pruebas, eligiendo un punto de acceso configurado con el servidor RADIUS, en lo posible permitir la navegación de usuarios de la red a este dispositivo.

Capacitar al administrador de la red, en el uso de las herramientas y en la mecánica del proceso de autenticación, la idea es mantener un solo perfil de conexión a la red.

Muy importante el mantenimiento habitual al servidor de dominio y RADIUS, se debe tener en cuenta que si no se realiza el respectivo mantenimiento pueden existir usuarios desligados de la empresa que podrían accesar a la red.

El secreto compartido del servidor RADIUS y los dispositivos inalámbricos debe contener números, caracteres, mayúsculas y minúsculas. Como medida de seguridad adecuada.

Complementar la seguridad con firewall físicos y lógicos así como la segmentación de la red de datos, esto puede ser mediante la implementación de Vlan en los Switch como la implementación de DMZ para aislar los servidores críticos.

La capacitación a los usuarios es fundamental muchas veces de esto depende del uso o no de un producto o servicio tecnológico, se deben indicar los beneficios que se obtendrá así como la forma de conectarse a la red.

Se recomienda utilizar dispositivos de la línea empresarial, de no ser así en algunos casos y dependiendo el modelo se puede actualizar el firmware con open source.

El certificado de autoridad, tiene una caducidad es importante saber cuándo se hace efectiva para evitar que quede obsoleto y por ende los usuarios no puedan acceder.

# BIBLIOGRAFÍA


1. Arana, J. R., Villa, L. A., & Polanco, O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. Ingeniería y Competitividad, 15(1), 127-137.
2. B. Potter. (2003). Wireless security's future. IEEE Security & Privacy, 1(4), 68-72. doi:10.1109/MSECP.2003.1219074
3. Barrios, A. Z. (2011). Planificación estratégica, presupuesto y control de la gestión pública Universidad Católica Andres.
4. Bernal, C. (2006). Metodología de la investigación.
5. Bhaiji, Y. (2008). Network security technologies and solutions (CCIE professional development series) Pearson Education.
6. Bonnet, N. (2014). Windows server 2012 R2: Las bases imprescindibles para administrar y configurar su servidor Ediciones ENI.
7. Boxcriptor, B.Cifrado AES y RSA. Recuperado de https://www.boxcryptor.com/es/cifrado
8. C. Rigney, et. al. (2004). "Remote authentication dial in user service (RADIUS)," network working group. Recuperado de http://www.ietf.org/rfc/rfc2865.txt?number=2865
9. Del Rio, A. M. (2006). Implementacion del protocolo CHAP en un sistema de seguridad para redes WLAN.
10. Diab, A. (2016). Self-organized mobile communication technologies and techniques for network 6th edition
11. Dulaney, E., & Easttom, C. (2014). CompTIA security+ study guide 6th edition John Wiley & Sons.
12. Expansión, R. (2016). Evite que su empresa sufra ataques informáticos. Recuperado de http://www.expansion.com/pymes/2016/09/20/57dc3248e5fdea3f018b45da.html
13. Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 256, 57-73.
14. INEC, E. (2014). principales_resultados_diee_2014. Recuperado de http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Empresas_2014/Principales_Resultados_DIEE_2014.pdf
15. J. Zhang, Y. Guo, Y. Chen, & J. Ma. (2015). Research of AAA messages based on 802.1x authentication. 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 618-621. doi:10.1109/IAEAC.2015.7428627
16. Llauradó, O. (2014). La escala de likert: Qué es y cómo utilizarla. Recuperado de http://www.netquest.com/blog/es/la-escala-de-likert-que-es-y-como-utilizarla/
17. López Ramírez, M. D., Suasnavas, C., Andrea, E., & Calderón Hinojosa, X. A. (2012). Diseño e implementación de un prototipo de meta distribución del sistema operativo linux bajo licencia GPL orientada al servicio AAA (Radius) integrando un módulo de administración web.

18. Lv, Y., & Du, B. (2013). Application of AAA security management in classified network. Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on, 660-663.
19. Nakhjiri, M., & Nakhjiri, M. (2005). AAA and network security for mobile access: Radius, diameter, EAP, PKI and IP mobility John Wiley & Sons.
20. Nogales, J. L. M., Beltrán, S. V., & Bonilla, J. L. L. (2006). Sistema de acceso seguro a recursos de información para redes inalámbricas 802.11. Científica, 10(4), 199-205.
21. Pellejero, I., Andreu, F., & Lesta, A. (2006). Fundamentos y aplicaciones de seguridad en redes WLAN: De la teoría a la práctica Marcombo.
22. Ross, S. M. (2007). Introducción a la estadística Reverté.
23. Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014). Metodología de la investigación 6ta edición. Edición McGraw-Hill,
24. Santos, J. C. (2000). Seguridad y alta disponibilidad RA-MA Editorial.
25. Stallings, W. (2011). Comunicaciones y redes de Computadores.
26. Tamayo, M. (2004). El proceso de la investigación científica Editorial Limusa.
27. Technet, M. (2010). MS-CHAP v2 - TechNet - Microsoft. Recuperado de https://technet.microsoft.com/en-us/library/cc957983.aspx
28. Van der Walt, D. (2011). FreeRADIUS beginne's guide
29. Wi-FI, A. (2006). WPA2™ security now mandatory for wi-fi CERTIFIED™. Recuperado de http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products
30. Wi-FI, A. (2008). Wi-fi protected access. Recuperado de http://web.archive.org/web/20081006071203/http://wi-fi.org/white_papers/whitepaper-042903-wpa
31. Wi-FI, A. (2012). The state of wi-fi® security: Wi-fi CERTIFIED™ WPA2™ delivers advanced security to homes, enterprises and mobile devices. Recuperado de http://www.wi-fi.org/downloads-registered-guest/20120229_State_of_Wi-Fi_Security_09May2012_updated_cert.pdf/7600.

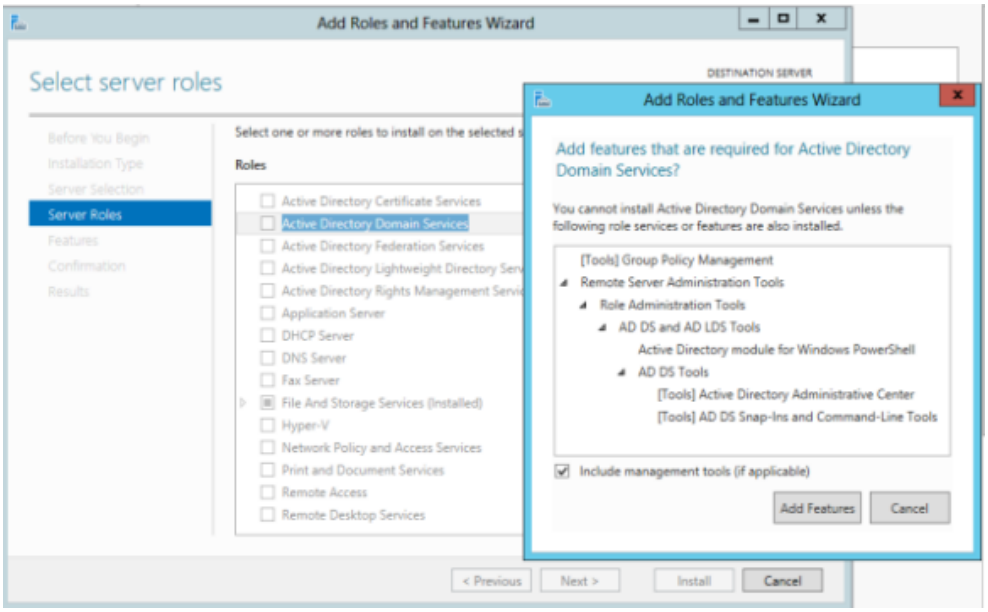
## ANEXO 1

**Modelo de Encuesta Likert:** A continuación encontrará las siguientes preguntas cuya finalidad es medir la perspectiva que se tiene sobre la seguridad en las redes inalámbricas. Para lo cual se ha creado una encuesta donde el 5 es Excelente, 4 Muy buena, 3 Buena, 2 Regular, 1 Deficiente,

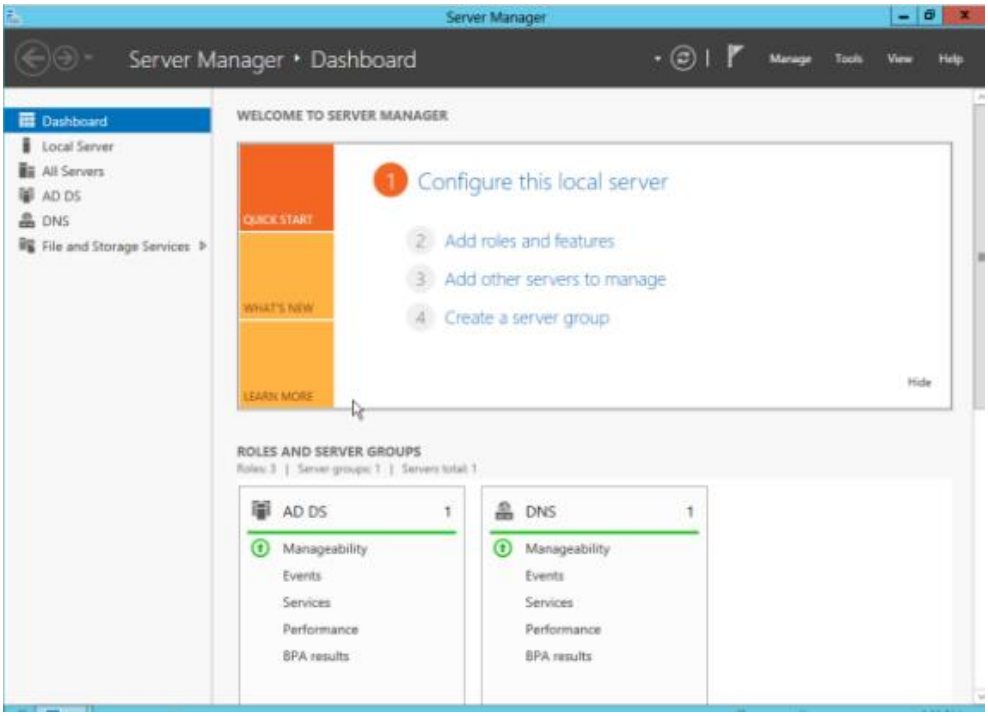
| **Encuesta** | **Excelente** | Muy buena | **Buena** | Regular | **Deficiente** |
|---|---|---|---|---|---|
| **1.) Los dispositivos de comunicación alámbricos e inalámbricos que forma parte de la infraestructura de red de su empresa, ¿cómo los considera?** | | | | | |
| **2.) El control de accesos a los usuarios que ingresan a su red de datos corporativa por dispositivos inalámbricos es:** | | | | | |
| **3.) El esquema que le proporciona el directorio activo (Unidades Organizativas Usuarios Equipos Directivas de Grupo entre otros) ¿cómo la calificaría?** | | | | | |
| **4.) La identificación de los dispositivos móviles o usuarios que acceden por los dispositivos de comunicación a la red de datos corporativa es** | | | | | |
| **5.)Los usuarios que acceden a la red mediante los dispositivos de comunicación inalámbrica, le mencionan que el servicio de conexión y disponibilidad que se ofrece es** | | | | | |
| **6.) Como calificaría la administración de las claves de acceso e identificadores de red de los dispositivos inalámbricos en su empresa** | | | | | |
| **7.) Considera que las herramientas de administración y gestión de la red implementadas en su red de datos son:** | | | | | |
| **8.) Los mecanismos de seguridad aplicados a los dispositivos de comunicación de su empresa son:** | | | | | |
| **9.) De introducir un servicio de autenticación, autorización y registro (AAA) a su red inalámbrica ¿Cómo calificaría el aporte de esta tecnología?** | | | | | |

## ANEXO 2 Configuración del Servidor RADIUS en Windows Server 2012

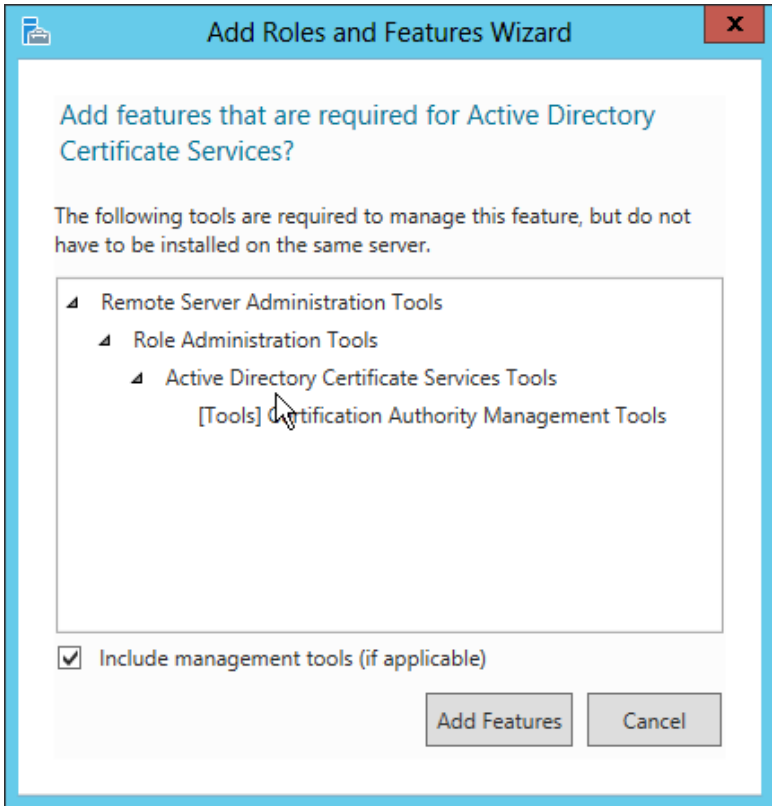
Pasos previos se debe tener configurado un entorno Microsoft Windows Server 2012. El mismo que debe tener los roles del Directorio Activo y el DNS



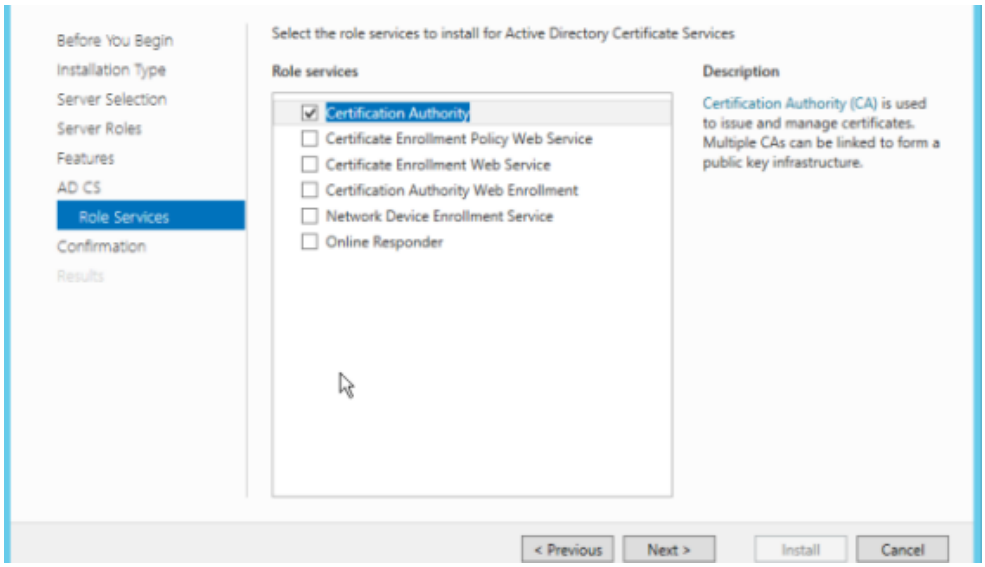

Roles del Active Directory y DNS creados previamente



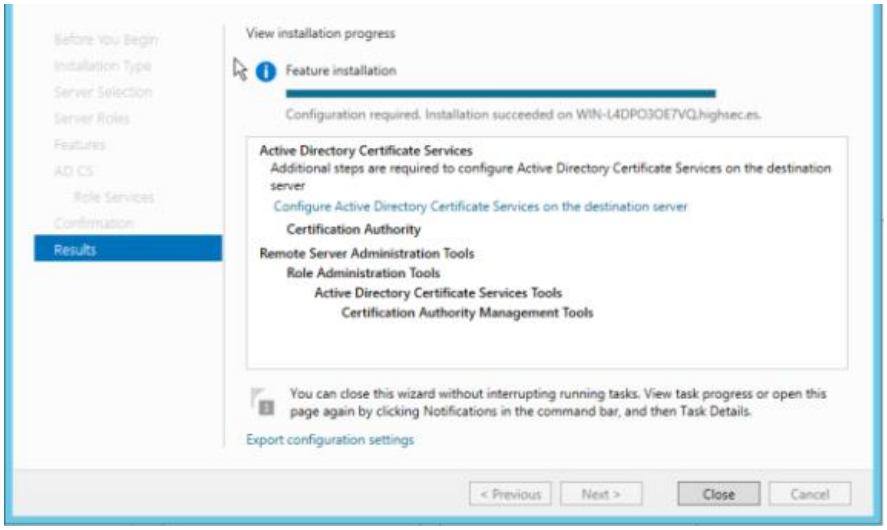
Instalar los roles y características que son necesario para la configuración del servidor RADIUS, este es el Certificado de Autoridad del Active Directory



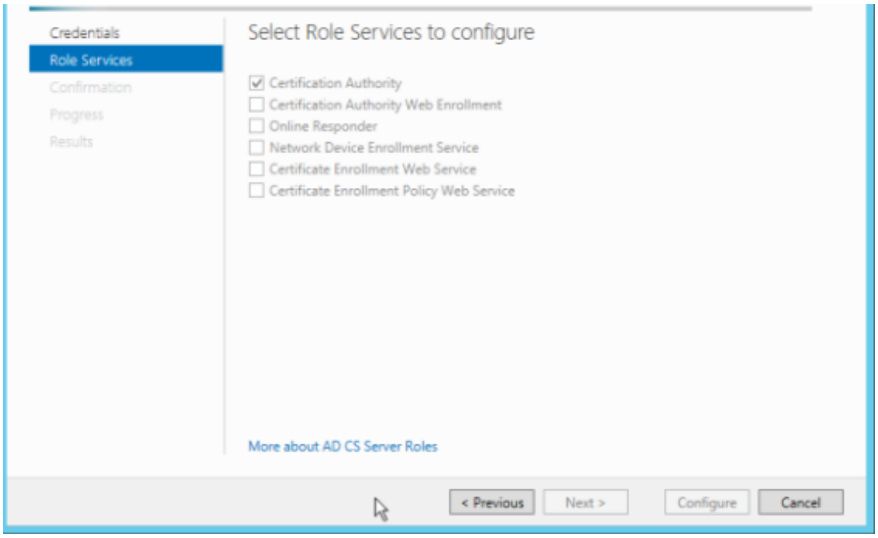

Seleccionar el certificado de Autoridad, y damos clic en siguiente:



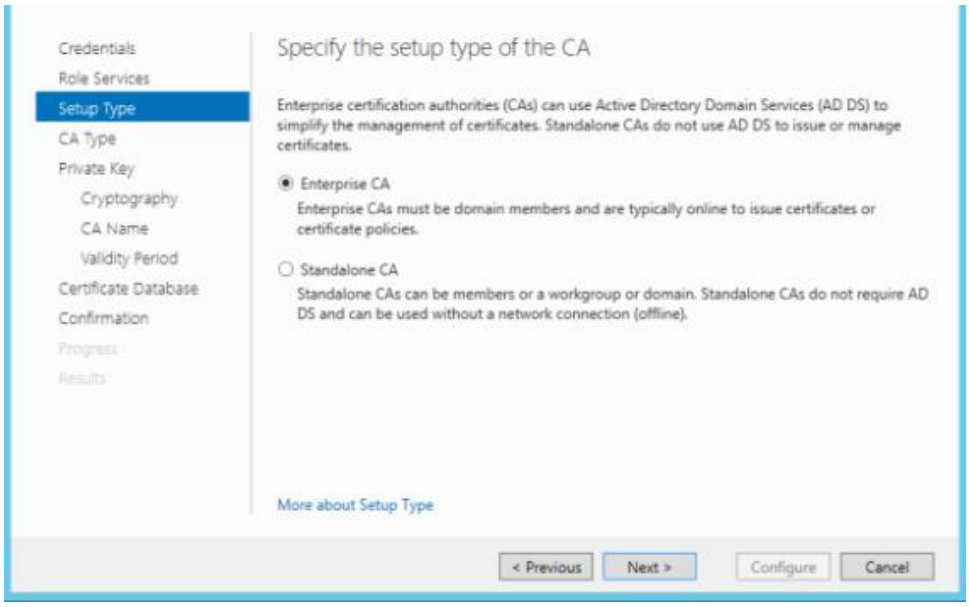
Instalar el rol de certificado de seguridad se mostrará el siguiente mensaje



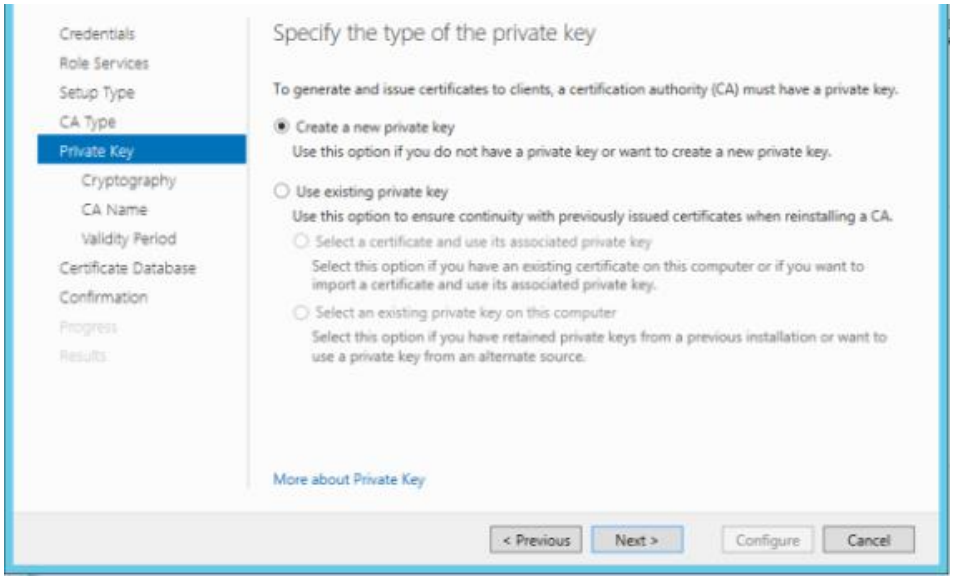

Seleccionar el rol de Autoridad de Certificación



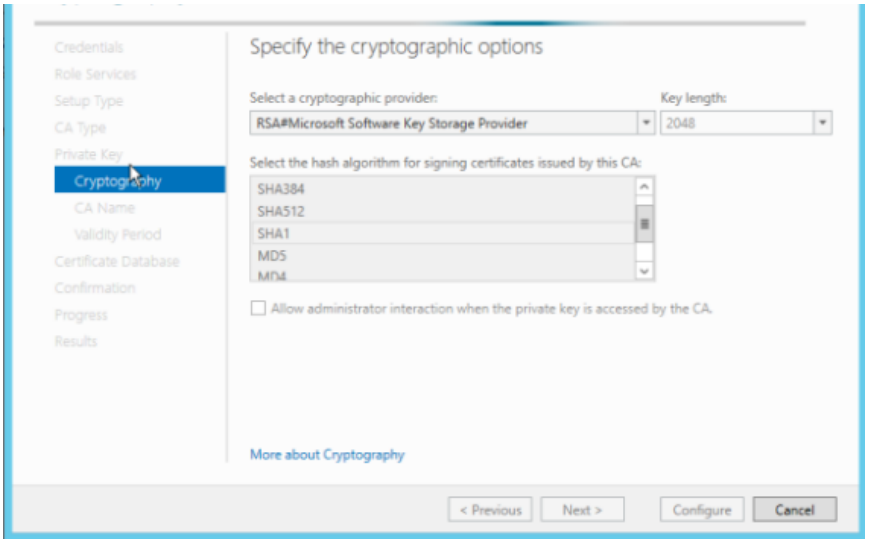
Seleccionar el tipo de certificado Enterprise CA



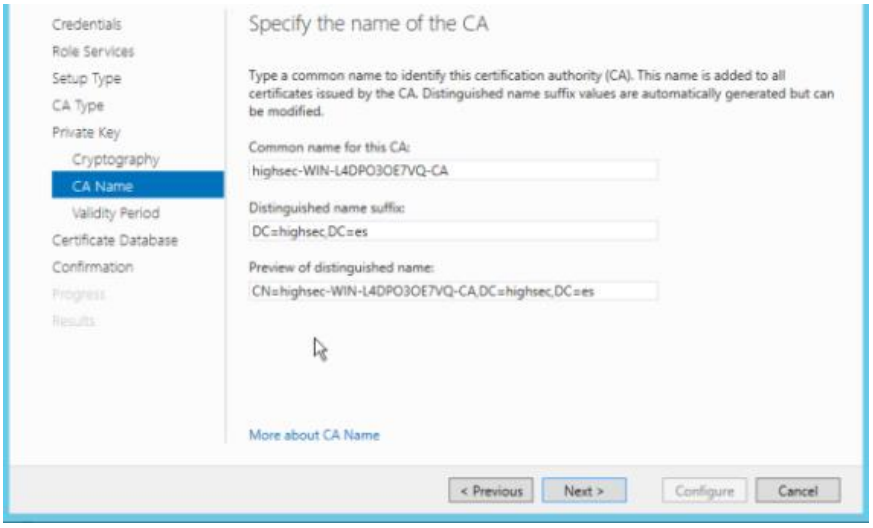

Crear la nueva Llave Privada



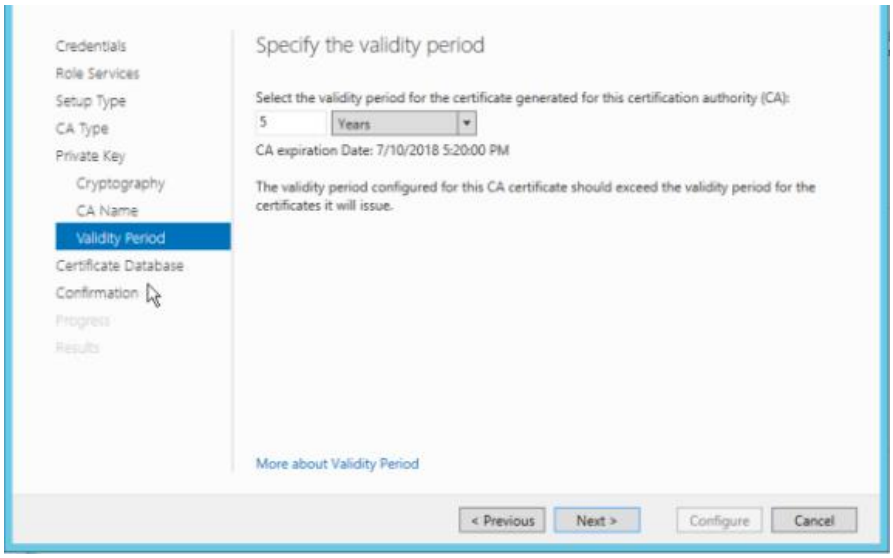
Seleccionar la opción de criptografía para el Certificado de Autoridad.



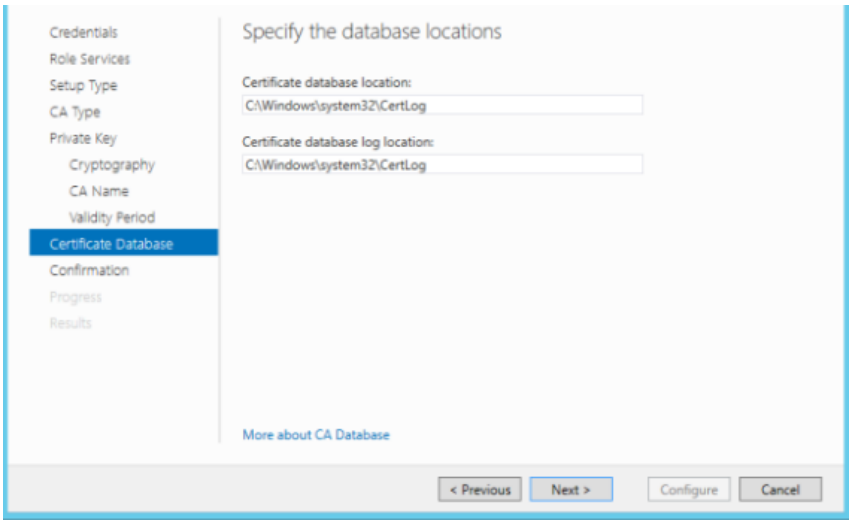

Especificar el nombre del Certificado de Autoridad



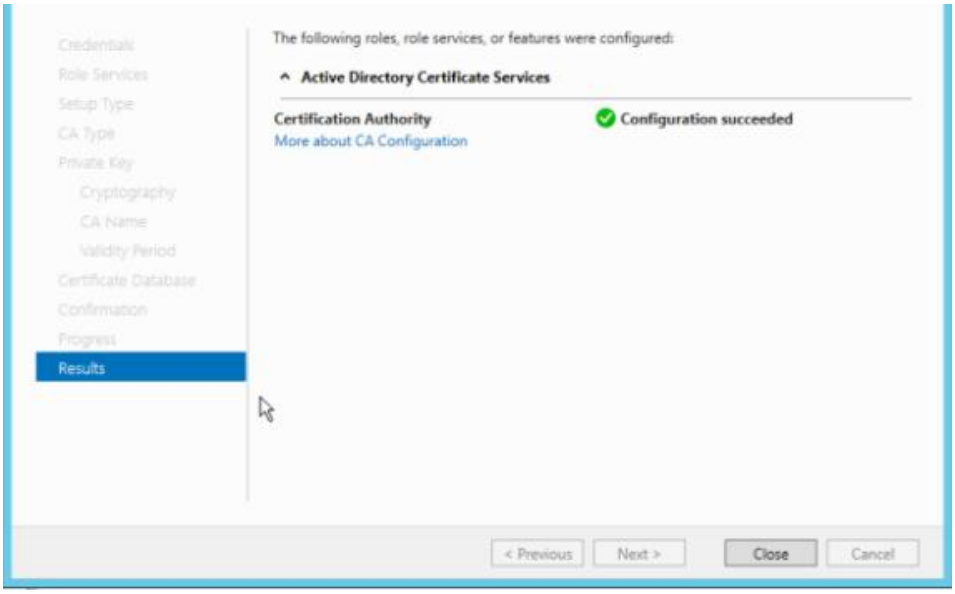
Especificar el periodo de validez del Certificado de Autoridad



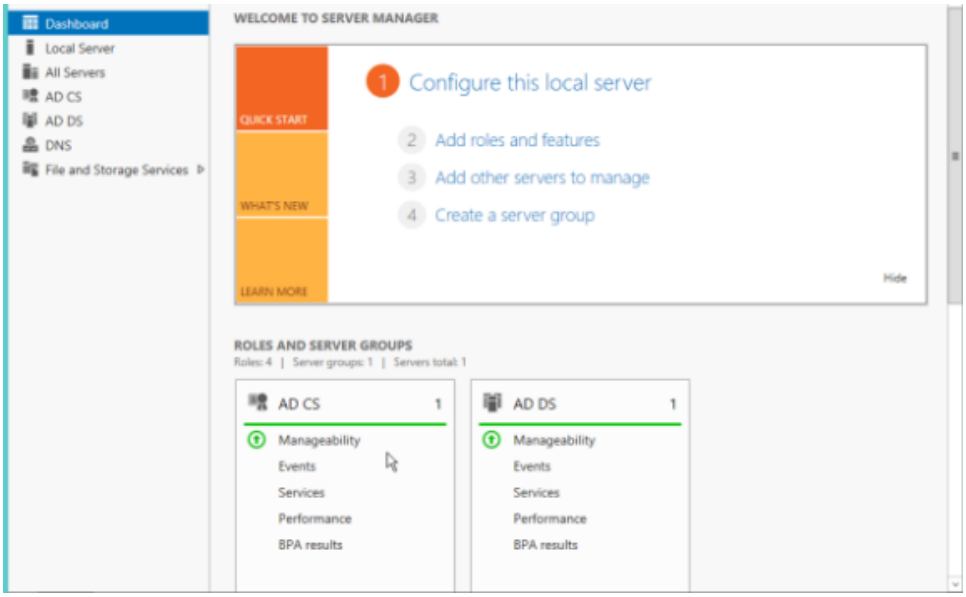

Elegir la localización del certificado de autoridad



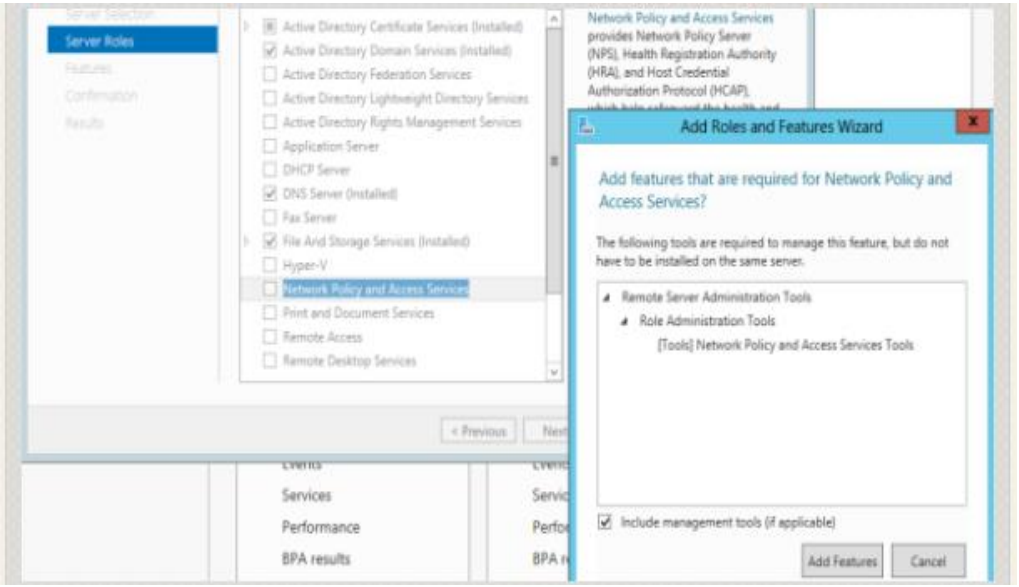
Culminar la instalación del certificado de autoridad



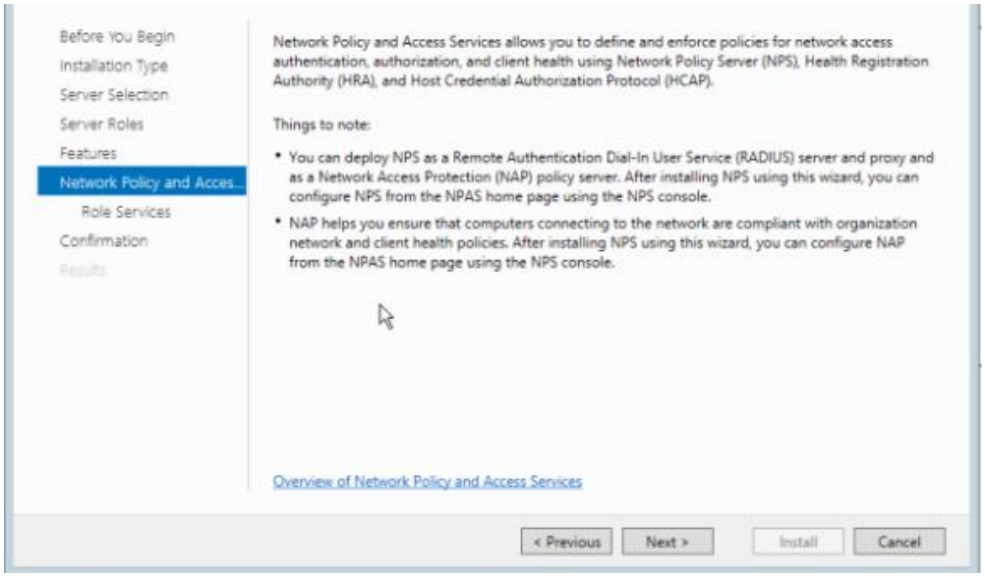

Se mostrará el rol y el certificado tal como se aprecia en la siguiente imagen



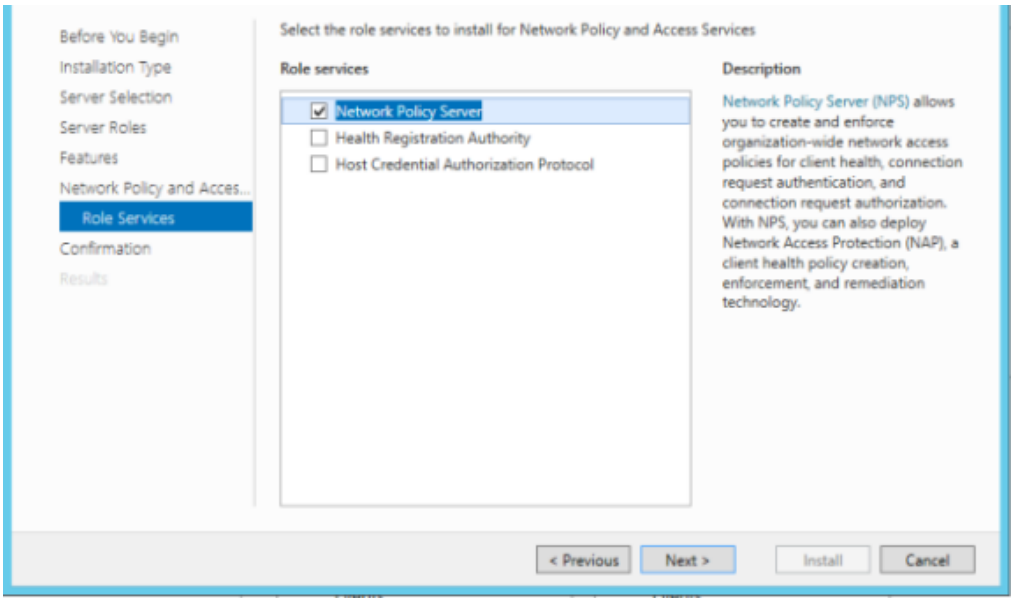
Instalar las políticas de red y servicio de accesos (NPS)



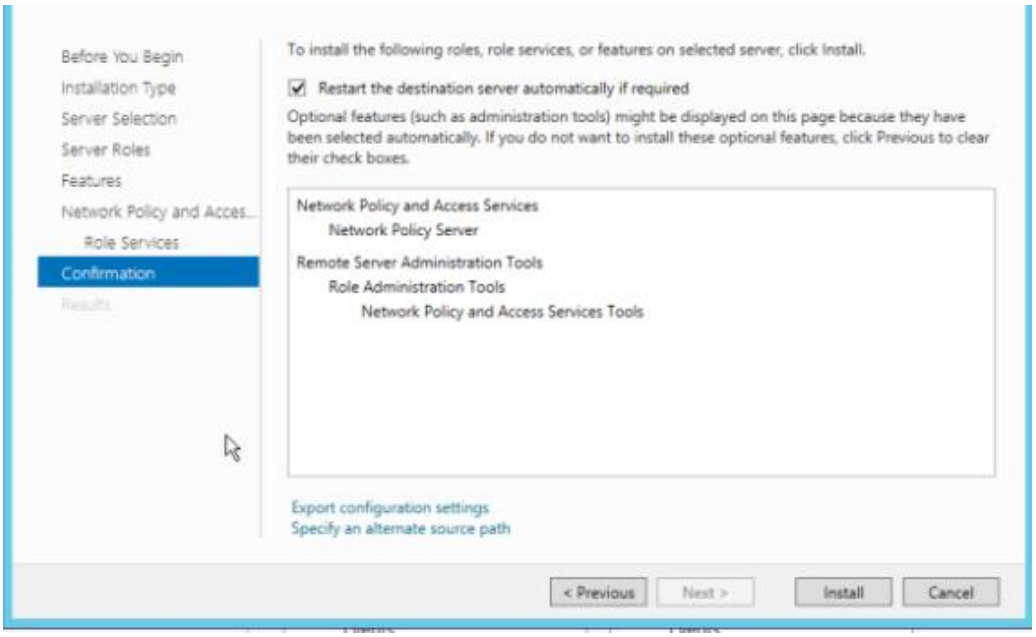

Seleccionar el rol y empezar con el proceso de instalación



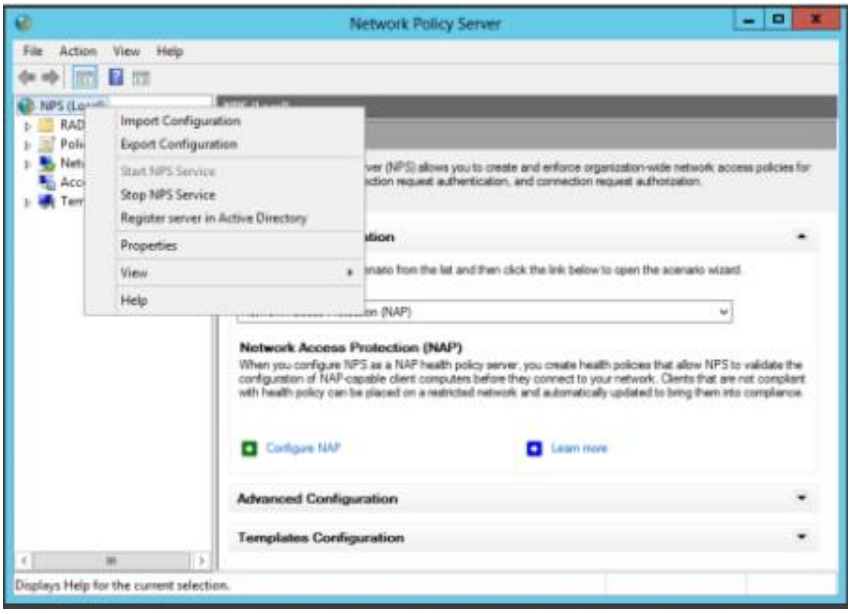
Seleccionar el Role Service (Network Policy Server)



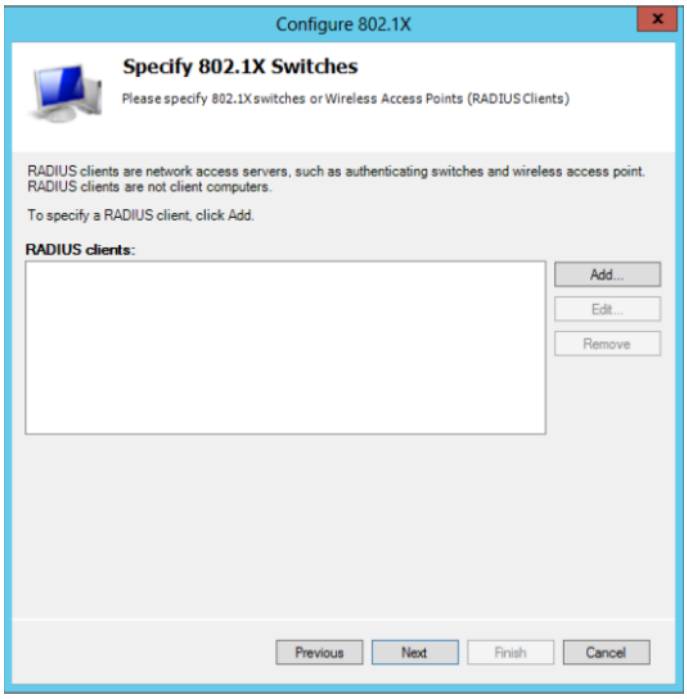

Confirmar la instalación del Rol



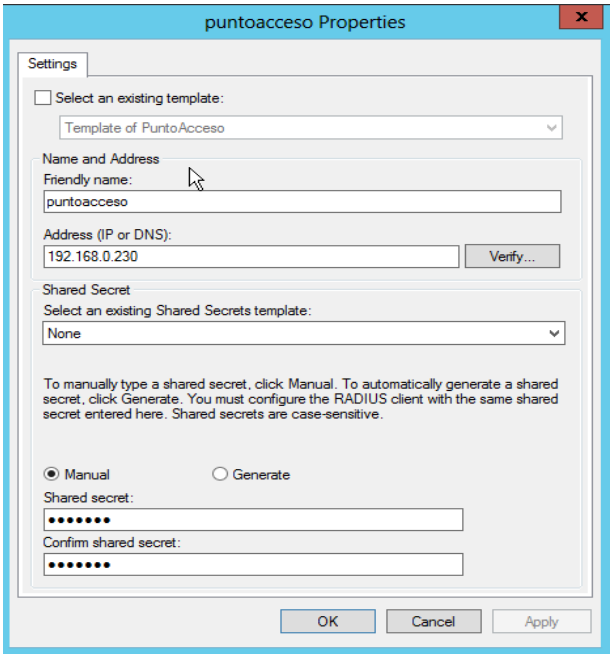
Abrir la consola de Network Policy Service



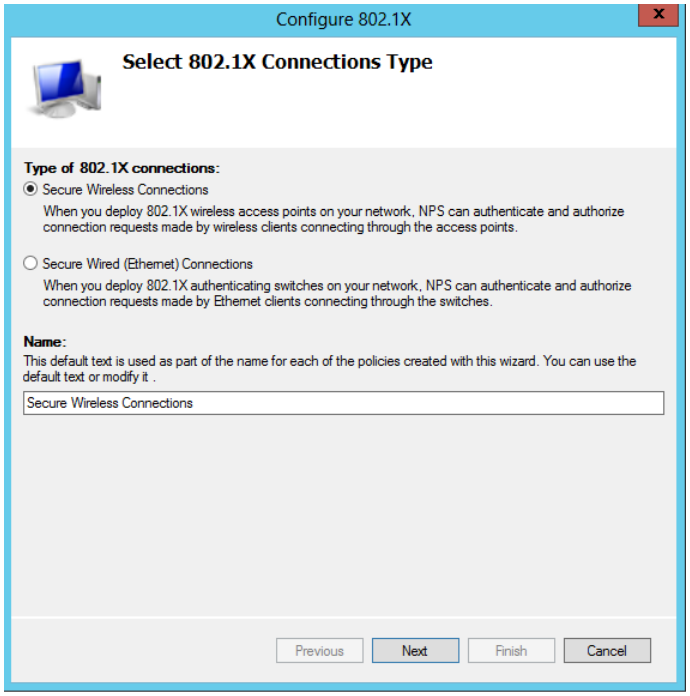

Configurar 802.1X



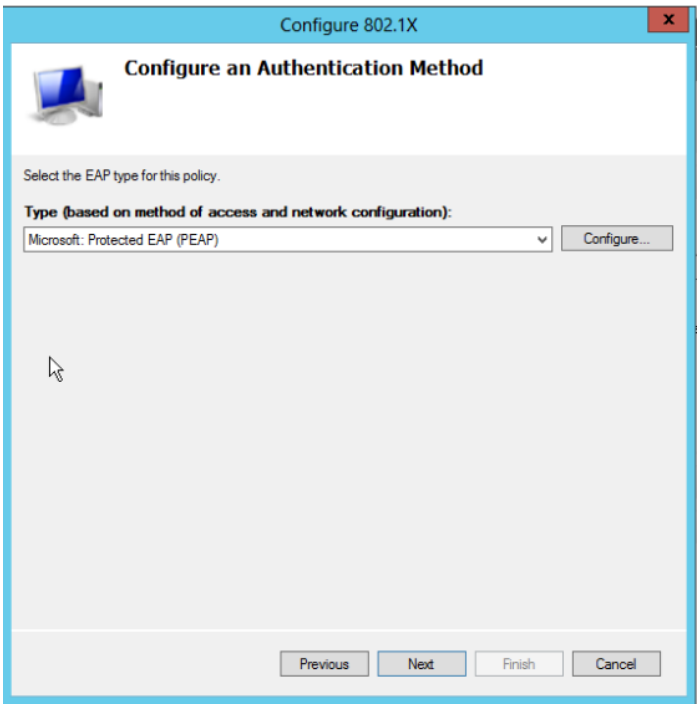
Seleccionar siguiente, y colocar los datos de los puntos de accesos, como son nombres, IP y el secreto compartido



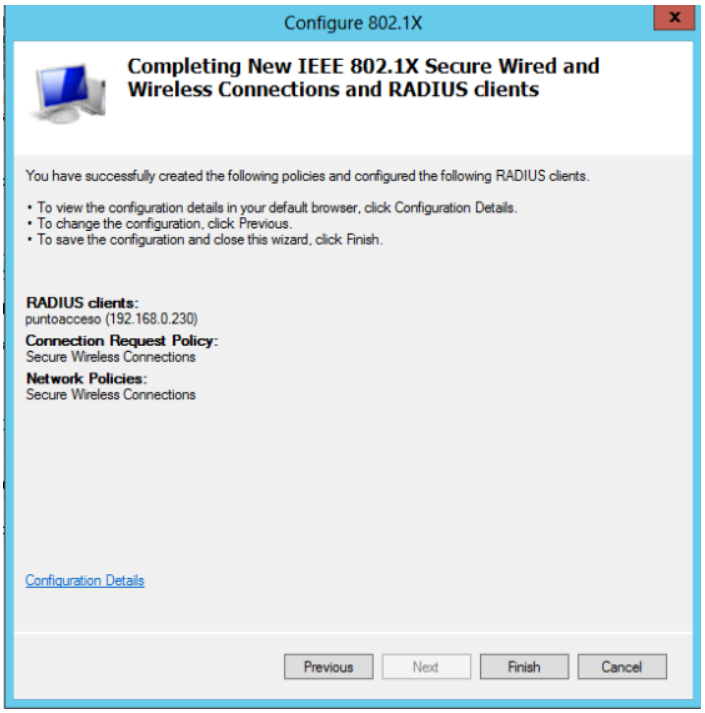

Seleccionar el tipo de conexión 802.1x en este caso inalámbrico



Seleccionar el tipo de EAP en este caso será EAP-PEAP

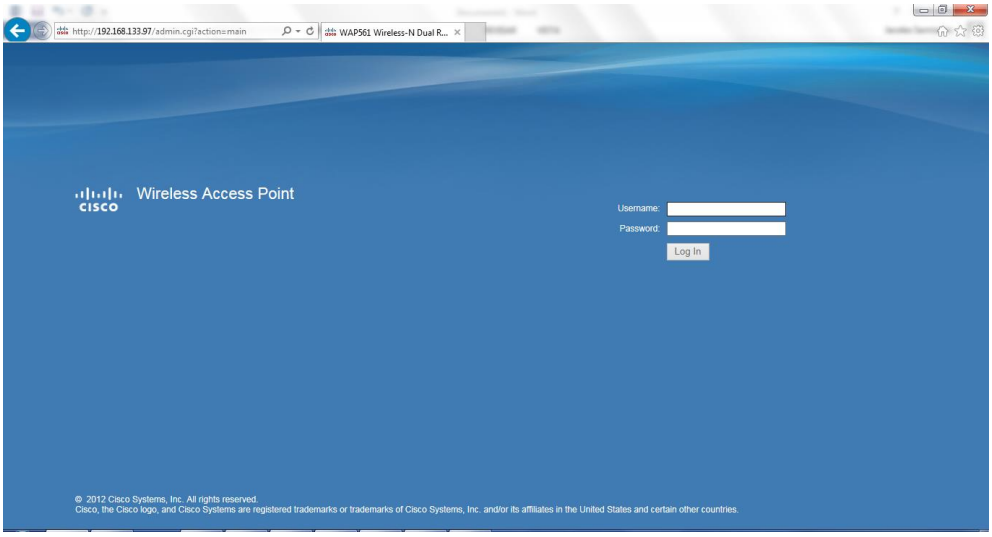



Finalizar la instalación, para la red inalámbrica con 802.1x y los clientes RADIUS

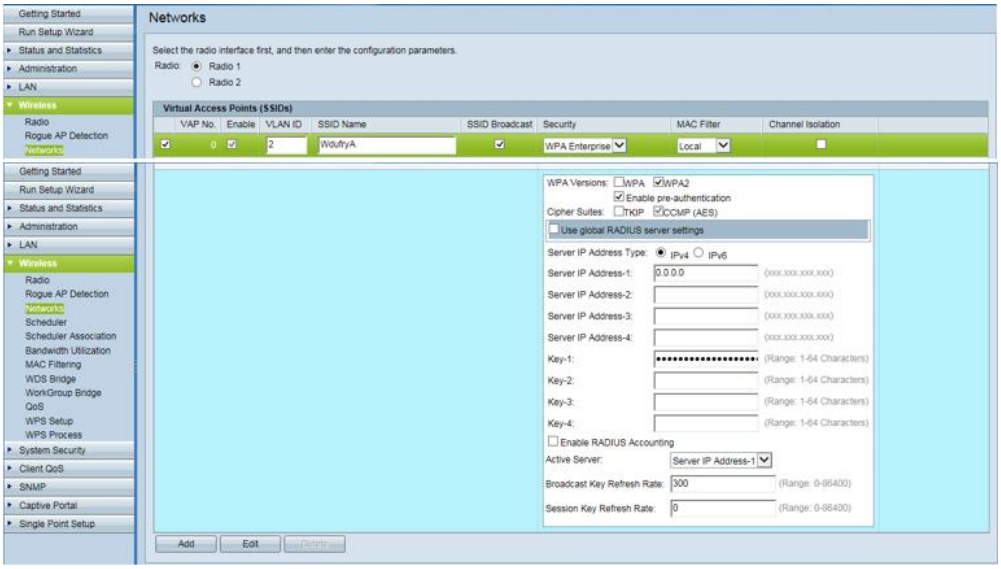


## ANEXO 3 Configuración de Access Point con software propietario para RADIUS

Acceder al dispositivo de comunicación inalámbrico mediante un web-browser, en este caso se ha seleccionado un Access Point de la marca Cisco con software propietario

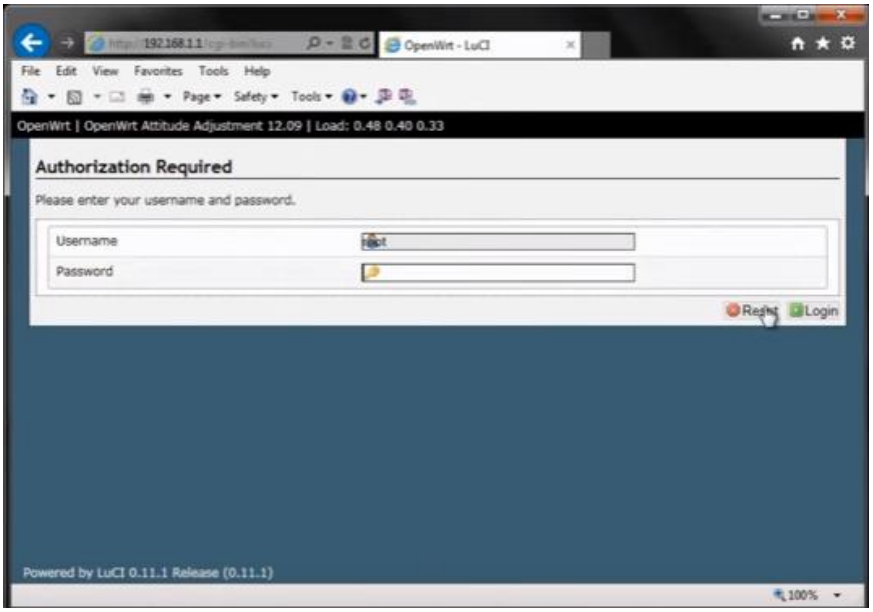



Seleccionar en la opción Wireless, Networks, Security, seleccionar WPA-2 Enterprise, se deberá colocar la IP del servidor RADIUS, el tipo de cifrado del dispositivo y digitar el secreto compartido y clic en ADD.

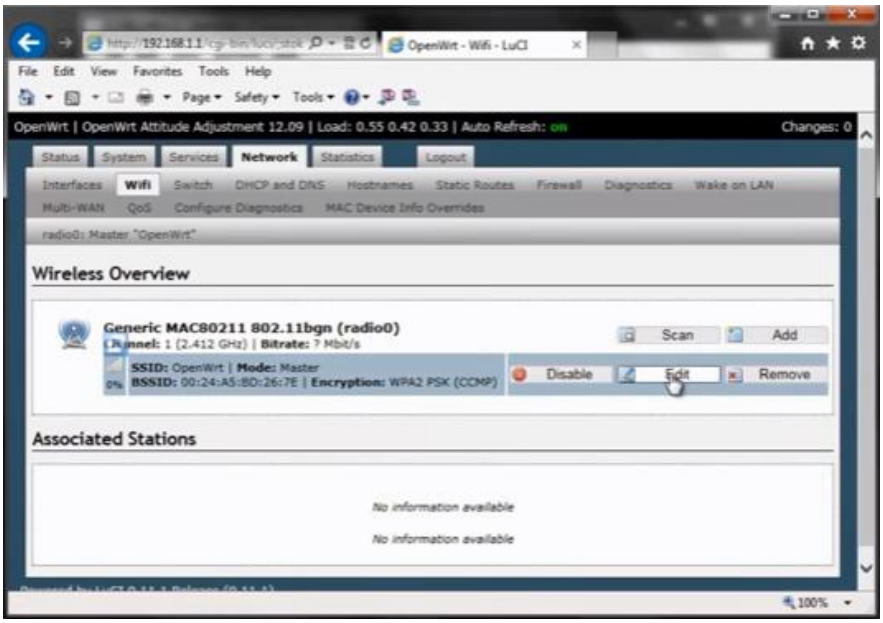


## ANEXO 4 Configuración de Access Point con software propietario para RADIUS

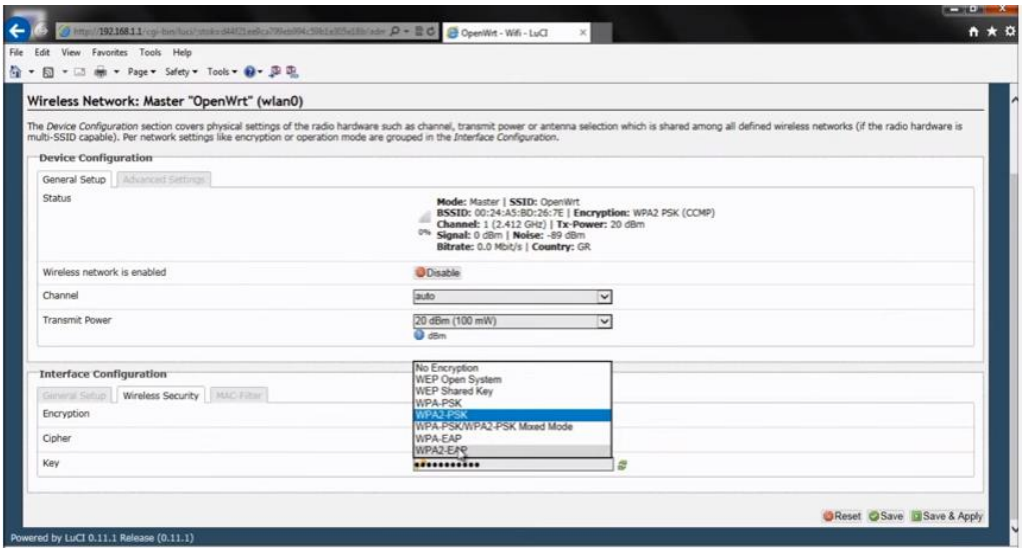
Acceder al dispositivo de comunicación inalámbrico mediante un web-browser, en este caso se ha seleccionado un Access Point de la marca Cisco con software Open Source (OpenWrt)




Seleccionar la opción WIFI y posteriormente dar clic al boton Edit



En la opción Interface Configuration seleccionar el cifrado WPA2-EAP




Digitar los siguientes datos:

- Radius-Authentication Server: IP del servidor Radius
- Radius Authentication-Port: 1812,
- Radius Authentication Secret: secreto compartido

Clik en Save&Apply