UNIVERSIDAD NACIONAL

"SANTIAGO ANTÚNEZ DE MAYOLO"

FACULTAD DE CIENCIAS

ESCUELA ACADÉMICO-PROFESIONAL

INGENIERÍA DE SISTEMAS E INFORMÁTICA

"DISEÑO DEL SISTEMA DE SEGURIDAD DE REDES BASADO EN EL PROTOCOLO RADIUS PARA MEJORAR LA ADMINISTRACIÓN DE ACCESO A LA RED DE LA MUNICIPALIDAD PROVINCIAL DE CARHUAZ, 2019"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR

Bach. ROJAS MÉNDEZ JIMMY WILFREDO

ASESOR:

Ingº ROMERO AGUILAR DANTE ENRIQUE

HUARAZ - PERU

2022

Nº Registro: T1

ACTA DE SUSTENTACIÓN DE TESIS

Siendo las 11:45 horas del día miércoles 07 de diciembre del año 2022, los miembros del Jurado de Sustentación de Tesis que suscriben, designados según Resolución Decanatural N° 208-2022-UNASAM-FC de fecha 02 de diciembre del 2022; se reunieron en Acto Público, de manera semipresencial en el Auditorio de la Facultad de Ciencias de la Universidad Nacional "Santiago Antúnez de Mayolo" y plataforma institucional MS-Teams, para evaluar la defensa de la tesis presentada por el Bachiller Jimmy Wilfredo Rojas Méndez, de la Escuela Profesional de Ingeniería de Sistemas e Informática, Título de la tesis "Diseño del Sistema de Seguridad de Redes Basado en el Protocolo Radius para Mejorar la Administración de Acceso a la Red de la Municipalidad Provincial de Carhuaz, 2019".

Después de haber escuchado la sustentación, demostración y respuestas a las preguntas formuladas, el jurado, **DECLARA POR UNANIMIDAD**, al Bachiller **Jimmy Wilfredo Rojas Méndez, APTO** para optar el título profesional de Ingeniero de Sistemas e Informática, con el calificativo de **APROBADO**, con la nota de **CATORCE (14.00).**

En consecuencia, el sustentante queda en condición de recibir el Título de Ingeniero, Conferido por el Consejo Universitario de la UNASAM, de conformidad con las normas estatutarias y la Ley Universitaria vigente.

Huaraz, 07 de diciembre de 2022.

Ingº Elizabeth Gladys Arias Lazarte
PRESIDENTE
CIP Nº 43138

Ingº Alberto Martin Medina Villacorta
SECRETARIO
CIP Nº 143211

Ingº Dante Enrique Romero Aguilar
VOCAL
CIP Nº 90440

NOMBRE DEL TRABAJO

tesis final jimmy rojas.pdf

AUTOR

JIMMY WILFREDO ROJAS MÉNDEZ

RECUENTO DE PALABRAS

26247 Words

RECUENTO DE CARACTERES

145998 Characters

RECUENTO DE PÁGINAS

153 Pages

TAMAÑO DEL ARCHIVO

6.0MB

FECHA DE ENTREGA

May 4, 2023 5:52 PM GMT-5

FECHA DEL INFORME

May 4, 2023 5:54 PM GMT-5

24% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base c

- 23% Base de datos de Internet
- 5% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 15% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 8 palabras)

DEDICATORIA

Dedico esta tesis a mi madre, por brindarme su apoyo en cada uno de mis pasos e inculcarme buenos valores, a la vez, por ser un ejemplo de perseverancia, esfuerzo y valentía, también me motivo constantemente para ser la persona quien soy hoy en día.

Finalmente quiero dedicárselo a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de mis anhelos más deseados

AGRADECIMIENTO

Mi profundo agradecimiento a todas las autoridades y personal de la Municipalidad Provincial de Carhuaz, por abrirme las puertas y permitirme desarrollar todo el proceso de investigación dentro de la institución, sin estos no hubiese podido alcanzar los resultados obtenidos.

A mi asesor el Ingeniero Romero Aguilar Dante Enrique, el cual con su apoyo y aportes profesionales me guio en cada uno de las etapas en esta importante investigación.

Por ultimo a mi madre y hermano quienes siempre fueron el motor que impulsa mis sueños y esperanzas, quienes estuvieron siempre a mi lado para darme apoyo en los momentos más difíciles de mi investigación. Siempre han sido mis mejores guías de vida.

RESUMEN

La tesis tuvo el objetivo general de desarrollar el sistema de seguridad para la administración de accesos a la red usando el protocolo RADIUS en la Municipalidad Provincial de Carhuaz; la metodología comprende una investigación cuantitativa, nivel explicativo, diseño cuasi experimental de corte longitudinal, cuya población fue conformada por los 53 trabajadores y la muestra fue censal, la técnica empleada fue la encuesta, el instrumento fue el cuestionario. Los resultados indican que el 64,1% no se encuentran conformes con la anterior administración de acceso a la red, se recolectaron requerimientos para el nuevo sistema de seguridad de redes basado en RADIUS, que fue implementado en un servidor Windows Server 2008 mejorando la administración de acceso con un 73,6% como regular. Se concluye que el sistema de seguridad implementado mejora la administración de acceso a la red comprobado mediante la prueba de Wilcoxon con un Z=6,276 y un p-valor de 0,000.

Palabras clave: Diseño de red, protocolo Radius, administración de acceso a la red.

ABSTRACT

The thesis had the general objective of developing the security system for the administration of access to the network using the RADIUS protocol in the Provincial Municipality of Carhuaz; The methodology includes a quantitative investigation, explanatory level, quasi-experimental design of longitudinal cut, whose population was made up of 53 workers and the sample was census, the technique used was the survey, the instrument was the questionnaire. The results indicate that 64.1% are not satisfied with the previous administration of access to the network, requirements were collected for the new network security system based on RADIUS, which was implemented on a Windows Server 2008 server, improving administration. access with 73.6% as regular. It is concluded that the implemented security system improves the administration of access to the network, verified by the Wilcoxon test with a Z=6.276 and a p-value of 0.000.

Keywords: Network design, Radius protocol, network access management.

ÍNDICE

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

I. INTRODUCCIÓN

1.1. Antecedentes de la investigación

1.1.1. Antecedentes internacionales

En la investigación de Tobar y Mora (2016) titulada "Implementación de un servidor RADIUS en Windows Server para Centralizar la administración de nuevos Access Point en las oficinas remotas de Galpones y Huertos del Gobiernos Autónomo Descentralizado de Guayas", presentada a la Universidad Salesiana , se tuvo como objetivo Implementar una asignación dinámica de VLANs en la red inalámbrica mediante la instalación de un servidor RADIUS, usando un Servidor Windows, una WLC y un active directory , con respecto a su metodología la tesis fue de tipo cualitativa y de diseño descriptivo teniéndose como población a la dirección del Gobierno Provincial de Guayas ubicados en galpones y huertos, y a los cuatro trabajadores a cargo del departamento de redes tratándose de una muestra censal , en cuanto a sus conclusiones los autores afirman que la implementación de un servidor RADIUS incidió positivamente en la asignación dinámica de VLAN's a través de la red inalámbrica. La construcción del diseño propuesto fue acorde a las necesidades de brindar cobertura a los sitios remotos garantizando autentificación y control en el acceso inalámbrico a los recursos de red. A su vez el proyecto de implementación resultó más económico para el Gobierno Provincial de Guayas que cubrió con los gatos de implementación. Los resultados a los que se arribaron fueron que se pudo evaluar los objetivos y expectativas del proyecto de implementación del servidor RADIUS en las oficinas administrativas, la conexión entre los dispositivos se realizó con éxito logrando un acceso con autenticación de usuarios; así mismo el uso de la controladora WLC permitió optimizar el tiempo de configuración de los Access

point, debido al estar conectados al WLC son configurados automáticamente con el Cisco Discovery Protocol.

En la tesis de Pazmiño y Pinargote (2016) denominada “Servidor para autenticación en la red de comunicación de datos del GAD municipal del Cantón Bolívar” presentada en la Escuela Superior Politécnica Agropecuaria De Manabí Manuel Félix López, se obtuvo como objetivo Implementar un servidor con autenticación en la red de comunicación de datos del GAD Municipal del Cantón Bolívar para mejorar el rendimiento de seguridad en la entidad, con respecto a su metodología la tesis fue de tipo mixta y de diseño descriptivo teniéndose como población y muestra a la red de comunicación de datos de la entidad, la cual comprendió la documentación respecto a ella así como su infraestructura, en cuanto a sus conclusiones los autores afirman que el método de autenticación, y acceso del servidor RADIUS ayudó generar perfiles de navegación y por ende a mejorar la seguridad de la institución, permitiendo el ingreso a la red privada al usuario correcto. En los resultados los autores indican que la GAD municipal cuenta con 50 terminales, que emplean una IP estática de clase C los cuales se encuentra conectados mediante 2 switches, 10 Access point y 4AP de acceso público, así mismo se halló que la red no presenta errores de transmisión de datos pero que no son segmentadas adecuadamente.

En el trabajo de investigación de Murillo (2015), denominada “Diseño e implantación de una red inalámbrica unificada en el Colegio Nuestra Señora de Fátima de Valencia”, presentada a la Universidad Politécnica de Valencia, se tuvo como objetivo mostrar cómo se ha diseñado, implantado y configurado una red de comunicaciones inalámbrica unificada en el colegio Nuestra Señora de Fátima de Valencia, con respecto a su metodología la tesis fue de tipo cualitativo y de diseño descriptivo que tuvo como unidad de estudio a la red inalámbrica instalada en la

institución en estudio, en cuanto a sus conclusiones el autor afirma que se garantiza una conexión de calidad con una alta seguridad y fiabilidad de la red a su vez ayudara a gestionar de forma centralizada todos los puntos de acceso ahorrando considerable el tiempo a las personas encargadas de la tareas de administrar de la red. En los resultados se detalla el proceso de diagnóstico, diseño, implementación y configuración de la red propuesta conformada por 12 AP, un controlador DWC, un servidor Radius y un router.

1.1.2. Antecedentes nacionales

En la tesis de Espinoza (2018), denominada "Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS", presentado a la Universidad Mayor de San Marcos, tuvo como objetivo desarrollar e implementar los efectos que produce un sistema de seguridad de acceso con RADIUS en el grado de autentificación y autorización del control de tráfico inalámbrico de información, con respecto a su metodología la tesis fue de tipo cuantitativa y de diseño correlacional, la población estuvo conformada por 40 científicos investigadores quienes son candidatos al uso del servicio eduroam quienes conformaron parte de la muestra, en cuanto a sus conclusiones el autor afirman que el protocolo RADIUS ha mostrado ser un mecanismo de protección y salvaguardo de información, empleando los estándares de seguridad, y juntamente a Eduroam brinda un valor agregado a la institución catalogándola como una institución de confianza a nivel internacional y a su vez los usuarios dispondrán de acceso a este servicio desde cualquier parte de la institución. En los resultados se halló mediante un coeficiente de correlación de Pearson de valor de 0,911 y una significación asintótica bilateral de 0,003 que un sistema de seguridad de control de acceso con RADIUS es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico.

En la tesis de Albujar (2017), denominada "Diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux para fortalecer el acceso de la red de la clínica Millenium Chiclayo 2016", Presentado a la Universidad Nacional Pedro Ruiz Gallo, tuvo como objetivo diseñar un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux para fortalecer el acceso de la red de la clínica Millenium Chiclayo, con respecto a su metodología la tesis fue de tipo cualitativo y de diseño descriptivo, en cuanto a sus conclusiones el autor afirma que la autentificación es importante para proteger el accesos a la información para lo cual es necesario uso de herramientas que cumplan esa labor enfocada a usuarios de un red, con el uso de estas se disminuiría considerablemente las vulnerabilidades que presenta. En lo concerniente a los resultados el autor indica que la red propuesta optimizó la red de la clínica la cual se encontraba fortaleciendo la seguridad, integrando la configuración de VLAN y reduciendo las vulnerabilidades existentes debido a la falta de optimización de los servicios de banda ancha y acceso a la red interna.

En el trabajo de investigación de Bardales (2015) titulada “Sistema de gestión de acceso a una Red Wi-Fi utilizando Software Libre para mejorar el nivel de seguridad del acceso a la Información”, presentado a la Universidad César Vallejo, tuvo como objetivo mejorar el nivel de seguridad del acceso a la información de la Municipalidad Distrital de Esperanza, a través de un Sistema de Gestión de Acceso a una Red Wi-Fi utilizando Software Libre, con respecto a su metodología la tesis fue de tipo cualitativo y de diseño correlacional, en cuanto a sus conclusiones el autor afirma que al implementar sistema de seguridad mejora el nivel de seguridad del acceso a la información así mismo aumento el nivel de satisfacción de los trabajadores de la Municipalidad de la Esperanza debido a que se redujo el tiempo

de búsqueda de la información en un 29.56%. Con respecto a los resultados el nivel de satisfacción de los trabajadores en el pre test se tiene un promedio de 12,67 mientras que en el post test se tiene 25,75, hallándose un coeficiente de T de Student de t=-13,74 con lo cual se logró determinar que el nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el sistema actual es mayor o igual que el Nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el sistema propuesto.

1.1.3. Antecedentes locales

En la investigación de Ortega (2017) titulada "Diseño de un cableado estructurado bajo la metodología Top Down Network Design aplicando políticas de seguridad para el Colegio El Pinar de la ciudad de Huaraz 2017" presentado a la Universidad Católica Los Ángeles Chimbote, tuvo como objetivo diseñar un cableado estructurado aplicando políticas de seguridad bajo la metodología TOP DOWN NETWORK DESIGN, para mejorar la gestión en las oficinas del Colegio El Pinar de la ciudad de Huaraz 2017, con respecto a su metodología la tesis fue de tipo mixta y de diseño descriptivo, en cuanto a sus conclusiones el autor afirma que con el desarrollo del diseño de la estructura de tecnología de red y las políticas de seguridad ha mejorado positivamente en los procesos de atención a los usuarios. En cuanto a los resultados se halló que el 67.50 % hacia arriba manifiesta incomodidades e insatisfacciones con la red actual que vienen trabajando pues éstos se sienten que la red es vulnerable, poco disponible, con errores en la transmisión y con accesos asequibles del personal de diferentes áreas, por lo cual la propuesta planteada representa una mejora a futuro.

En el trabajo de investigación de Chavéz (2016) titulada "Diseño de un cableado estructurado para mejorar la comunicación de datos de la Municipalidad Provincial

de Carhuaz, departamento de Ancash 2016" presentado a la Universidad Católica Los Ángeles Chimbote tuvo como objetivo diseñar un cableado estructurado que mejore la comunicación de datos de la Municipalidad Provincial de Carhuaz, Departamento de Ancash 2016, con respecto a su metodología la tesis fue de tipo cualitativo y de diseño descriptivo, en cuanto a sus conclusiones el autor afirma que si la municipalidad implementa mecanismos de seguridad a través de un servicio de servidores sería fundamental para asegurar la información y que no exista pérdida o robo de la misma a su vez asegura que se agiliza la transmisión de datos y que los trabajadores realicen su labor más rápido debido a que se disminuye el tiempo de respuesta del acceso a la información de la red. Los resultados obtenidos en referencia a los objetivos dan respuesta que el tiempo que se tiene en la transmisión de datos es demasiado largo y entorpece la labor cotidiana, la seguridad de la información esta vulnerable a ataques ya que no cuenta con ningún medio para respaldarlos y la satisfacción de los usuarios en la velocidad de transmisión de información, muestran datos altos de insatisfacción.

1.2. Bases teóricas

1.2.1. Redes informáticas

En concordancia con Dordoigne (2015) las redes informáticas son un grupo de equipos que se encuentran en constante comunicación usando un mismo lenguaje para lo cual usan un mismo protocolo y así puedan compartir información y servicios dentro de un determinado grupo.

A. Clasificación de las redes

En cuanto a la clasificación de las redes, Pérez y Facchini (2017) sostienen que son las siguientes:

- Red de Área Personal (PAN): Mendoza y Andrade (2016) mencionan que es una red de computadoras de corto alcance usada para la comunicación entre los equipos informáticos que se encuentren a escasos metros del usuario.
- Res de Área Local (LAN): En concordancia con Ruiz (2014) las redes LAN son redes privadas con un propio sistema de comunicación, se encuentran restringidos a un determinado espacio que, por lo general se localiza dentro de un edificio, aunque estas puedan extenderse a varios edificios como un campus, para lo cual se usará distintos mecanismos y medios de interconexión.

  A si mismo Pérez y Facchini (2017) señalan que las redes LAN comúnmente son utilizados dentro de organizaciones, empresa o personas, para así poder interconectar sus equipos ya sea de forma alámbrica o inalámbrica estas conexiones pueden alcanzar velocidades desde 54 Mbps hasta los 10 Gbps.
- Red de Área Metropolitana (MAN): Es una red que se extiende dentro de una ciudad o una zona suburbana, a menudo dentro de esta se pueden encontrar interconectadas dos o más Redes LAN, y para lograr esto se utiliza un proveedor de servicio utilizando líneas de comunicación privadas (Cobos y Gutiérres, 2016).
- Red de Área Amplia (WAN): Las redes WAN son redes de gran extension geometrica las cuales como medios de interconexion usan los satelites, cables interoceanicos, fibra optica, etc. (Mendoza y Andrade, 2016)

B. Topología de las redes

De acuerdo con Mendoza y Andrade (2016) cuando se habla de topología de redes se refieren a la forma en la que están distribuidas las estaciones de trabajo y los cables que lo conectan, cuyo objetivo es hacer más económica, eficaz y fiable la conexión de la red, Las topologías de red son las siguientes:

- En bus: Permite conectar a todas las computadoras de la red en una sola línea compartiendo el mismo canal de datos en el cual cuando se envía una información cada computadora revisa el mensaje recibido y la compara con la dirección de la terminal de recepción, cuando es la misma la recibe caso contrario la rechaza. (Cobos y Gutiérres, 2016).
- En estrella: En concordancia con Cobos y Gutiérres (2016) que mencionan que en esta topología se cuenta con un computadora central o servidor el cual se encarga de administrar la información de la red. La información que maneja contiene datos almacenados, manipulación de archivos, mensaje entre los usuarios, etc.
- En anillo: Esta topología tiene la forma de un bucle cerrado o un anillo, que incluye conexiones de punto a punto entre los dispositivos. La información enviada transita por cada computadora que se comporta como un repetidor (Dordoigne, 2015).

1.2.2. Sistemas de seguridad

En concordancia con Soriano (2014) estas son herramientas y procedimientos que deben de utilizar los empleados y la alta dirección de una organización, para

garantizar la protección de los datos confidenciales para esta, así como de los sistemas informáticos durante su transmisión a través de una red de telecomunicación.

La revista Seguridad en América (2017) menciona que los sistemas de seguridad se deben de adaptarse a los constantes avances tecnología para así ser más eficientes en la seguridad, consideran como una de sus principales herramientas a los controles de acceso ya que resultan ser más eficientes en las instituciones y ofrecen mayores beneficios a bajo costo como lo es el protocolo de seguridad RADIUS.

- **RADIUS:** Es un protocolo de red cliente/servidor que fue desarrollada por Livingston Enterprises, Inc. en 1991, este se encuentra en la capa de aplicación y cumple la función de autenticación, autorización y contabilidad (AAA), el cual se encarga de gestiona a todos los usuarios que acedan a una red (Espinoza Arana, 2018)

De acuerdo a Microsoft (2017) las dimensiones de la variable diseños de sistemas de seguridad basado en el protocolo RADIUS son las siguientes, pues se encuentran en concordancia con su estructura:

A. Utilización del servicio de autentificación para la administración de acceso a la red

Consiste en la implementación de un servidor y proxi, el cual pueda cumplir la función de autentificación autorización y contabilidad (AAA) en la infraestructura de acceso a la rede, como lo son los puntos de acceso inalámbrico y los conmutadores Ethernet; también es necesario la utilización de una base de datos centralizada como lo es el Active Directory para así centralizar las directivas de acceso a la red en los

servidores, lo cual reduciría en gran medida los costos y los riesgos de seguridad (Microsoft, 2017).

Así mismo, Dordoigne (2015) indica que se le debe de considerar como un servicio muy importante para que solo acceda el personal autorizado, para lo cual cuando un dispositivo se conecta a una red se hará el reconocimiento y la comprobación de la identidad de esta; este servicio de debe de considerar en primera instancia y después se deberá validaría el acceso a la información.

A esto se suma lo dicho por CISCO (2014) el cual menciona que para la autentificación de usuarios es necesario ingresar un nombre de usuario y contraseña validos antes de completar la conexión, estos se almacenan en los dispositivos de terminación VPN, el cual suministra autentificación a muchas otras bases de datos como lo son Windows, Novell, etc.; este proceso verifica quien es el que ingreso, que puede hacer y que hace realmente; así mismo menciona que es utilizado para un acceso más seguro.

B. Identificación de los requisitos previos de la solución

Para Microsoft (2017) antes de empezar a hacer el diseño de la solución es necesario hacer un análisis para conocer las condiciones actuales en su entorno, que principalmente se tiene que hacer a la infraestructura informática, a los Servidores de Dominio que se están utilizando, el Active Directory.

- Servicio de dominio: Es usado por los usuarios de una red para poder identificar a cada ordenador que internamente es traducido por la dirección IP con la que corresponde, de esta tarea se encarga los

servidores DNS, los cuales mediante sistemas de bases de datos distribuidas traduce los nombres de dominios a direcciones IP (Microsoft, 2017).

- Infraestructura informática: Para definir a esta ISO (Organisno Internacional de Normalización, 2018) hace referencia a la norma ITIL/ISO 2000 la cual indica que la infraestructura tiene que cumplir los requisitos económicos y proporcionar las herramientas para mejorar la eficiencia de esta, así mismo se definen mecanismos para establecer la administración de servicios, también se tiene que tener en cuenta la mejora continua de la infraestructura.
- Activity Directory: El Active Directory guarda información la cual debe de ser fácil de encontrar y usar por los administradores y usuarios, este utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de la información del directorio, este almacén de datos usa un directorio con una estructura jerárquica el cual almacena información sobre objetos en la red los cuales por lo general pueden ser recursos compartidos como servidores, impresoras, las cuentas de usuario y computadora de la red (Microsoft, 2017).

C. Diseño de la infraestructura RADIUS

De acuerdo con Microsoft (2017) cuando se usa un sistema de autentificación como lo es RADIUS para el acceso a la red, antes de elegir el diseño será necesario determinar las funciones que va ejercer esta en el entorno, las funciones serian:

- Servidor RADIUS: En concordancia con Gómez (2014) quien señala que es un protocolo de autentificación cliente/servidor muy importante, el cual se basa en un servidor centralizado encargado de autentificar las credenciales directamente con el Active Directory de las conexiones remotas a la red de manera segura, para los cual efectúa las tareas de Autentificación, Autorización y Contabilidad (AAA), estos se encuentran especificados en el RFC 2865 y el RFC 2866.
- Proxy RADIUS: Para Microsoft (2017) es útil para la implementación de arquitecturas AAA de red cliente/servidor a gran escala, el cual agrega reglas para mejorar cualquier atributo del servidor RADIUS mediante solicitudes las cuales se hacen a través del enrutamiento.

D. Plan de administración

Microsoft (2017) señala que los servidores RADIUS basado en el Servicio de Autenticación de Internet (IAS) requieren de poco mantenimiento para que se garantice la disponibilidad continua del servicio y la seguridad de la red, no obstante, es necesario determinar estrategias para la administración de IAS, por lo que es necesario capacitar y equipar al personal para que administre la infraestructura de RADIUS, por ende, se ha de tener en cuenta los permisos, la configuración y cambios, la recuperación de servicios y por último la supervisión y auditoria de seguridad.

1.2.3. Administración de accesos a la red

De acuerdo con la norma ISO 27001 la cual indica que la administración de accesos a la red es la encargada del control de accesos para prevenir y no dejar entrar a las personas no autorizadas a través de controles los cuales podrán registra y revocar permisos a los usuarios; también se implementan medidas para evitar amenazas, manteniendo la seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella; es necesario emplear técnicas para tener una evaluación permanente de red y de los usuarios que están dentro de esta (ISO, 2018).

A esto se suma lo dicho por CISCO (2018) esta tiene como objetivo controlar el acceso a los recursos de la red, solo a los usuarios autorizados en las directivas del Active Directory, para que la red no pueda ser saboteada intencionalmente o voluntariamente; es necesario la implantación de políticas para el acceso a la red, por ende, es necesario crear un estándar o protocolo dentro de la red que sigan las mejores prácticas de seguridad y funcionamiento.

De acuerdo a ISO (2018) las dimensiones de la variable administración de accesos a la red son las siguientes, pues se encuentran en concordancia con sus controles:

A. Requisitos de negocio para el control de accesos

Es necesario controlar los accesos a la información y los procesos de negocio de una organización en base a las necesidades de seguridad de esta; las regulaciones para el control de acceso deben de ser considerados en las políticas de distribución de información y de autorizaciones, por ende, será necesario implementar normas para el control de acceso las cuales todo el personal deberá de cumplirlas y ser responsable ante la alta dirección de la información que manejan (ISO, 2018).

- Control de Accesos: Es un factor muy importante de la arquitectura de un sistema de seguridad, así mismo no se la debe de confundir con la autentificación, ya que el control de accesos es posterior a la autentificación y regula a los usuarios para que solo puedan acceder a los recursos e información sobre los cuales tengan derecho y a ningún otro más, con el fin de prevenir cualquier acceso no autorizado a la red y a la información de la organización; por eso es necesario la implementación de políticas de seguridad para definir adecuadamente quienes pueden acceder a la red (ISO, 2018).

B. Gestión de Accesos de usuarios

Consiste en la administración de los usuarios de la red donde a través de controles se realiza un procedimiento, los cuales deben de estar correctamente formalizados dentro de la institución, para poder hacer el registro y revocación de permisos a los usuarios, es decir se gestionan los privilegios que tienen cada uno de los usuarios (ISO, 2018).

C. Responsabilidades del usuario

En concordancia con ISO (2018) donde se indica que todos los usuarios dentro de una red sin importar su jerarquía, han de tener documentada sus obligaciones dentro de la seguridad de la información de una institución, sin embargo, existen diversos grados de responsabilidades y obligaciones, algunas responsabilidades que se tienen que aplicar son el correcto uso de las contraseñas, ser consiente de los equipos que se manejan y su correcto cuidado, qué acciones tomar cuando un equipos se encuentran desatendido y la protección de la información, por ende es

necesario que todos los empleados estén comprometidos con la institución para realizar correctamente sus responsabilidades.

- Nivel de compromiso: De acuerdo con la ISO (2018) está relacionado con el liderazgo de la alta dirección los cuales, mediante políticas de seguridad (la cual todo el personal de la empresa debe de conocer) y asignación de roles a los empleados se busca involucrarlos en el sistema para que estos tengan participación en la implantación de las normas.

D. Control de accesos y aplicaciones

Se encuentra dirigida a prevenir el acceso no autorizado a la información guardada en las aplicaciones de una institución, por ende, es necesario que dentro de las políticas de seguridad se detallen los controles de acceso a las aplicaciones y al aislamiento de los sistemas más importantes de la institución, para así tener a buen resguardo la información crítica de negocios de la organización, por lo tanto, si se tiene alguna aplicación e información que sea considerada importante para la organización, debe ser evaluada la necesidad de mantenerla o no en red con el resto de la infraestructura (ISO, 2018)

1.2.4. Comparación entre protocolos de seguridad

A. RADIUS versus TACACS+:

Con respecto al sistema de seguridad CISCO (2006), señala que es un protocolo cliente/servidor, el cual proporciona seguridad centralizada a los usuarios que deseen acceder a la administración de dispositivos de la red y proporciona el servicio de Autentificación, Autorización y Administración (AAA).

Cuadro 1: Comparación entre RADIUS y TACAS+

RADIUS	TACAS+
Protocolo de estándar abierto.	Protocolo de propiedad de Cisco.
Utilizado para la administración de accesos a la red.	Utilizado solo para la administración de accesos a los dispositivos.
Tiene un soporte contable extenso.	Tiene poco soporte contable.
Los procesos de AAA se combinan.	Los procesos de AAA se separan.
Es ligera y consume menos recursos.	Es pesado y consume más recursos.
Su implementación es económica.	Su implementación es costosa.

Fuente: CISCO (2006)

B. RADIUS versus DIAMETER

Está basado en el protocolo RADIUS, y se encarga de la autentificación de los usuarios que se conectan remotamente a Internet mediante líneas conmutadas, además cuentan con el servicio de servicio de Autentificación, Autorización y Contabilidad (AAA), este puede ser usado para trabajar de manera local (Vinay, 2015).

Cuadro 2: Comparación entre RADIUS y DIAMETER

RADIUS	DIAMETER
Protocolo de estándar abierto.	Protocolo privado.
Solicitud/respuesta del cliente al servidor.	Solicitud/respuesta de una parte a otra.
No usa comandos.	Usa comandos complejos.

Su mantenimiento no es costoso.	EL mantenimiento es costoso.
Es fácil de utilizar y administrar.	Necesita de comandos para administrar.
Su implementación es económica.	Su implementación es costosa.

Fuente: CISCO (2006) y Vinay (2015)

1.3. Justificación de la investigación

1.3.1. Justificación teórica

La presente investigación se realiza mediante la recolección de las teorías existentes sobre los sistemas de seguridad basada en el protocolo RADIUS y la administración de accesos a la red, para después contrastar con los resultados que serán obtenidos, por lo que se verificarán dichos conocimientos, generando nuevos saberes que podrán ser usados en futuras investigaciones a manera de antecedentes.

Es en tal sentido que la justificación teórica se sostiene en la teoría que proporcionará la presente tesis en base a una recopilación y análisis de datos provenientes de fuentes documentales y su prueba en el campo real; es de esta manera que futuros investigadores podrán emplearla como fuente teórica para el desarrollo de sus investigaciones contando con una validación científica.

1.3.2. Justificación metodológica

Esta justificación se sostiene en que, al ser una investigación que se apoya en la metodología científica, empleó los enfoques, diseños y niveles del método científico, que permitió conseguir el propósito que tiene este estudio. Asimismo, esta justificación se sustenta debido a la aplicación de técnicas de recolección de información como lo son las encuestas y los cuestionarios, para que mediante su

respectivo procesamiento se pueda obtener datos sobre los sistemas de seguridad y la administración de accesos en la Municipalidad de Carhuaz, pudiendo ser utilizados en otros trabajos de investigación.

Así mismo la investigación científica se justifica metodológicamente siendo modelo para el desarrollo e implementación de sistemas de seguridad u otros de características similares en el campo de la Ingeniería de Sistemas e Informática.

1.3.3. Justificación práctica

Con esta investigación se busca proponer una solución a la problemática existente dentro de la Municipalidad Provincial de Carhuaz, con respecto a los sistemas de seguridad de red para la administración de accesos, por ende, se hará uso del protocolo de seguridad RADIUS con el fin de que solo se permitir el acceso a la red al personal autorizado y sea solo a cierta parte de la información, mediante el cual se garantice tener un sistema confiable; pues este protocolo apoyara para tener a salvo la información importante para la municipalidad.

La justificación práctica también se sostiene en el aporte que realizan los profesionales de la carrera profesional de ingeniería de sistemas en la sociedad mediante la aplicación de los conocimientos adquiridos durante su formación profesional. La presente investigación representa la puesta en práctica de los aprendido y lo investigado con respecto a la seguridad y la administración de redes lo cual puede ser adaptado a entornos de situaciones de condiciones similares como una solución práctica.

1.3.4. Justificación social

Debido a que la Municipalidad Provincial de Carhuaz al igual que todas aquellas entidades tanto públicas como privadas se encuentran compuestas por personas, que

en su mayoría están constantemente trabajando con información de éstas y de personas que pertenecen a estos entornos, la solución ofrecida beneficiaría a la población, ya que se garantizaría la protección de información sensible la cual pueden ser utilizada con maleficencia.

La justificación social radica en la contribución que se realiza en una entidad pública la cual presta sus servicios a la población en general, en tanto el beneficio aportado sobre los procesos internos de la municipalidad permitirán agilizar los trámites u obtener otros beneficios traducidos de manera indirecta para los usuarios municipales.

1.3.5. Justificación tecnológica

La presente investigación sustenta su aporte tecnológico en la aplicación de nuevas tecnologías para la resolución de un problema real con respecto a la administración de accesos de la Municipalidad Provincial de Carhuaz, es decir que la justificación tecnológica es el uso de nuevas tecnologías para lograr la eficiencia y eficacia en el manejo de recursos de la oficina de tecnologías de información

La tesis a su vez denota la innovación en cuanto al diseño de redes en contraste al proceso de autentificación tradicional WPA2, en el que un solo una clave cualquier usuario puede acceder a la red con todos los permisos administrativos; en tal la investigación busca propiciar en otros investigadores y organizaciones la búsqueda de nuevas soluciones a los problemas aparentemente insolubles o con una solución parcial.

1.3.6. Justificación legal

Esta investigación se justifica de manera legal, debido a que se sustenta en la normativa peruana existente en relación a la protección de datos personales como lo

estipula la Ley N° 29733, la misma que es de cumplimiento obligatorio en las organizaciones públicas y privadas para garantizar dado derecho fundamental para los colaboradores siendo que estos no vean vulnerados sus datos personales debido a un hackeo o robo de información en la entidad donde laboran.

Así mismo la investigación se sostiene en el Decreto Supremo Nº 029-2021-PCM en el que se establecen las disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, siendo que el personal durante las horas de trabajo debe desarrollar actividades únicamente relacionadas a su campo laboral y no acceder a contenido ajeno a los fines organizacionales. En tal sentido la implementación del sistema de seguridad planteado permitirá a la oficina encargada el restringir el acceso a sitios que no guardan relación a las actividades laborales en tanto se mejorará la productividad de los colaboradores del municipio.

1.4. Planteamiento del problema

Con el cambio constante de las tecnologías y el mayor uso de estas para el manejo de la información dentro de las organizaciones, la seguridad de las redes ha adquirido un rol muy importante, ya que se han desarrollado amenazas que la vulneran e involucran el robo de información crítica de negocio (como los secretos que las hacen sobresalir ante las demás entidades del mismo rubro), y datos de personas que pertenecen a estos entornos. Es por ello que, a nivel mundial más del 40% de las organizaciones tanto públicas como privadas, están invirtiendo cada vez más en seguridad para garantizar un mejor salvaguardo de la información que les compete, hecho que además los dota de cierta competitividad, puesto que están entregando un valor agregado a sus usuarios (Diario Gestión, 2016).

Dicha preocupación por la seguridad se origina por la ocurrencia de casos tan sonados que ha afectado a grandes organizaciones y países, como lo es el caso reportado por la British Broadcasting Corporation (McGuinness, 2017), el cual menciona que Rusia, tuvo un ataque masivo donde sus organizaciones gubernamentales fueron las más afectadas, y colapsaron al punto de quedar inoperativas y sin poder ofrecer ningún servicio al público en general.

Paralelamente, en la investigación de Fortinet, empresa multinacional de desarrollo de software y servicios de ciberseguridad, se revela que en los últimos años hubo más de 150 millones de ataques de seguridad informática solo en Latinoamérica; en este mismo sentido, la investigación de Shutterstock, menciona que el cibercrimen ha aumentado un 10 000 % a nivel mundial entre el 2011 y el 2017, cifra que continúa creciendo (RPP Noticias, 2018).

De igual modo, el una publicación realizada en el diario por Riofrío (2018) mencionó el caso de Chile, el cual sufrió una serie de ataques a sus redes, especialmente al sector financiero donde se logró robar más de 10 millones de dólares y se revelo los datos de más de 67 mil tarjetas de credito a manos del grupo Hacktivista conocido también como Shadow Brokers, los cuales mediante el uso de herramientas buscaron las vulnerabilidades de los sistemas y de la administración de sus accesos, para robar información, tomar control de sus sistemas y detener su funcionamiento por completo. Por otra parte, según los reportes de Fortnet, Perú se halla como el quinto puesto de los países más atacados, pese a esto la inversión en sistemas de seguridad apenas creció un 10% en promedio, llegándose a encontrar que las empresas peruanas invierten como máximo un 20% de su presupuesto en sistemas de seguridad.

Siguiendo la tendencia señalada anteriormente, en el departamento de Ancash, específicamente en la Municipalidad Provincial de Carhuaz, el principal problema encontrado está relacionado con los sistemas de seguridad, puesto que no se cuenta con un adecuado sistema para la administración de accesos a la red, por ende las personas no autorizada desde cualquier dispositivo pueden acceder a esta y a sus recursos, donde se guarda información importante para la institución; actualmente los empleados pueden acceder a la red desde cualquier equipo sin hacerse la correcta verificación de las credenciales de estos, los cuales en la mayoría de los casos no poseen, y no se da de baja las credenciales de los empleados que han dejado de trabajar en la Municipalidad ; a su vez, no se cuenta con una adecuada restricción del tipo de contenido o información al que pueden acceder dentro de la municipalidad, lo cual debería estar limitado por el área donde se encuentre el empleado y el cargo que tenga en este; por ultimo no se cuenta con un compromiso de parte de los empleados de la municipalidad para cumplir las políticas de seguridad (las cuales no están bien detalladas actualmente), por lo cual estas normas se rompen al punto de que la seguridad puede quedar expuesta, ya que, en algunos casos los empleados revelan las claves o contraseñas de seguridad a personas ajenas a la municipalidad.

En vista de lo mencionado, Gómez (2014) sustenta que al no contar con un adecuado sistema de seguridad se vería afectada económicamente la organización, debido a que se perdería información relevante para esta, lo que afectaría su funcionamiento, incluso se podría ver afectado la información de terceros como sus datos personales, lo cual infringe la ley de protección de datos personales (según la Ley N° 29733) del consumidor de los servicios que presta la organización.

De este modo, como medida de seguridad informática Fortinet (2019) indica que para cualquier dispositivo que se conecte a la red de una organización es necesario contar

con un sistema de seguridad el cual permita la visualización de todos los usuarios que se conectados, para así poder tener un control de estos, y así se podrá limitar o bloquear sus acciones dentro de la red, a su vez esta tiene que ser dinámica y automatizada constantemente. A esto se suma lo dicho por CISCO (2006) que propone un sistema Cliente/Servidor para la autentificación de usuarios que accedan a la red haciendo uso de su respectivas credenciales, así mismo se tendrá que restringir a estos al tipo de contenido y acciones que pueden realizar dentro de la organización, para lo cual recomienda al protocolo de seguridad RADIUS (Remote Authentication Dial-In User Server) el cual mediante el proceso de autentificación y autorización, verifica que los usuarios que deseen entrar a la red se encuentren registrados en el activity directory para que puedan acceder a ésta.

Finalmente, en base a todo lo expuesto con anterioridad, se formula el siguiente enunciado del problema, frente al cual surge la presente investigación, la misma que encaminará al desarrollo de esta.

1.4.1. Formulación del problema

A. Problema general

¿Cómo un sistema de seguridad de redes mejorará de la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019?

B. Problemas específicos

Problema específico 1: ¿Cómo se encuentra valorada la administración de acceso en la Municipalidad Provincial de Carhuaz?

Problema específico 2: ¿Cuáles son las características del sistema de seguridad de redes que mejorará el control de acceso?

Problema específico 3: ¿Cómo se realiza la implementación del sistema de seguridad de redes que mejorará la gestión de acceso de usuarios?

Problema específico 4: ¿En qué medida el sistema de seguridad de redes basado en el protocolo RADIUS mejorará el control de acceso a sistemas y aplicaciones?

1.5. Objetivo

A. Objetivo general

Diseñar el sistema de seguridad de redes basado en el protocolo RADIUS para mejorar la administración de accesos a la red en la Municipalidad Provincial de Carhuaz, 2019.

B. Objetivos específicos

Oe1: Evaluar la administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz.

Oe2: Desarrollar el sistema de seguridad de redes basado en el protocolo RADIUS para mejorar del control de accesos.

Oe3: Implementar el sistema de seguridad de redes basado en el protocolo RADIUS para mejorar la gestión de acceso de usuarios**.**

Oe4: Evaluar la influencia del sistema de seguridad de redes basado en el protocolo RADIUS para mejorar el control de acceso a sistemas y aplicaciones.

1.6. Hipótesis significativa

A. Hipótesis general

H_1: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

B. Hipótesis específicas

H_1e1: Existe una deficiente administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz.

H_1e2: Se realizó el desarrollo del sistema de seguridad de redes basado en el protocolo RADIUS para la mejora del control de accesos.

H_1e3: Se implementó el sistema de seguridad de redes basado en el protocolo RADIUS para la mejora de la gestión de acceso de usuarios**.**

H_1e4: El sistema de seguridad de redes basado en el protocolo RADIUS influye positiva y significativamente sobre la mejora del control de acceso a sistemas y aplicaciones.

1.7. Hipótesis nula

A. Hipótesis general

H_0: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS no mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

B. Hipótesis específicas

H_0e1: Existe una eficiente administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz.

H_0e2: No se realizó el desarrollo del sistema de seguridad de redes basado en el protocolo RADIUS para la mejora del control de accesos.

H_0e3: No se implementó el sistema de seguridad de redes basado en el protocolo RADIUS para la mejora de la gestión de acceso de usuarios**.**

H_0e4: El sistema de seguridad de redes basado en el protocolo RADIUS no influye positiva y significativamente sobre la mejora del control de acceso a sistemas y aplicaciones.

II. MATERIALES Y MÉTODOS

2.1. Variables

2.1.1. Variable independiente

Diseño del sistema de seguridad basado en el protocolo RADIUS

2.1.2. Variable dependiente

Administración de acceso a la Red

2.2. Operacionalización de variables

Cuadro 3: Matriz de operacionalización de variables

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems
Diseño del sistema de seguridad basado en el protocolo RADIUS	En concordancia con Soriano (2014) estas son herramientas y procedimientos que deben de utilizar los empleados y la alta dirección de una organización, para garantizar la protección de los datos confidenciales para esta, así como de los sistemas informáticos durante su transmisión a través de una red de telecomunicación.	Para el diseño de la red de una infraestructura de Radius para la seguridad de redes LAN se han determinado las etapas de Utilización de IAS para la administración de acceso a la red, identificación de los requisitos previos de la solución, diseño de la infraestructura de RADIUS, y la creación de un plan de administración (Microsoft, 2018).	Utilización del servicio de autentificación para la administración de acceso a la red	Acceso inalámbrico	Se verá en los resultados como el proceso de diseño de red
				Acceso por cable	
				Acceso VPN	
				Acceso internet	
				Acceso intranet	
			Identificación de los requisitos previos de la solución	Características de dominio	
				Infraestructura preexistente	
				Requerimientos finales	
			Diseño de la infraestructura RADIUS	Diseño de servidor RADIUS	
				Proxy de RADIUS	
				Organización de infraestructura	
				Protocolos de autentificación	
			Plan de administración	Administración de configuración y cambios	
				Planeamiento de la recuperación de servicios	

				Planeamiento de permisos administrativos	
				Supervisión y auditoría de seguridad	
Administración de acceso a la Red	En la norma ISO 27001 indica que es la encargada del control de accesos para prevenir y no dejar entrar a las personas no autorizadas a través de controles los cuales podrán registra y revocar permisos a los usuarios (ISO, 2018).	De acuerdo a la ISO 27001 el objetivo de la administración del acceso es limitarla a aquellos agentes ajenos a la organización, así mismo dar a los usuarios el acceso necesario únicamente para sus funciones. Para ello se establecen dentro de sus objetivos determinar los requisitos de negocio para el control de acceso y la gestión de acceso de usuario con sus respectivos controladores, responsabilidades del usuario, y el control de acceso a	Requisitos de negocio para el control de accesos	Política de control de accesos	La municipalidad Provincial de Carhuaz difunde las políticas relacionadas al acceso a la red.
					Los trabajadores de la municipalidad cumplen con las políticas relacionadas al acceso a la red.
				Control de acceso a las redes y servicios asociados	Durante la incorporación de nuevos equipos, estos son formateados y revisados adecuadamente.
					El área de informática monitorea constantemente el funcionamiento de los equipos conectados a la red
			Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios	Existe una lista o registro de los usuarios activos de la red de la municipalidad
					El personal de área de informática registra los equipos de los nuevos usuarios
				Gestión de los derechos de acceso asignados a usuarios	Cada usuario de la red municipal tiene acceso solo a ciertos recursos de la red
					Los recursos de red con los que dispone son los pertinentes con respecto a sus labores

		sistemas y aplicaciones (ISO, 2018).		Gestión de los derechos de acceso con privilegios especiales	Los usuarios externos o invitados son registrados por el área de informática
					Existe una adecuada administración de permisos de los usuarios externos o invitados
				Gestión de información confidencial de autenticación de usuarios	Existen políticas o normas que regulan la confidencialidad de los datos personales de los usuarios de la red.
					Los trabajadores son responsables en cuanto al acceso a sus equipos y cuentas
				Revisión de los derechos de acceso de los usuarios	Los trabajadores conocen sus derechos y responsabilidades en cuanto al uso de sus equipos y recursos de red.
					El MOF y el ROF comprenden las funciones de los trabajadores y los recursos empleados para cumplirlos.
			Responsabilidades del usuario	Uso de información confidencial para la autenticación	Los trabajadores usan sus credenciales de acceso a recursos de red de manera personal
					Los trabajadores conocen los riesgos de compartir sus credenciales de acceso con los demás
				Protección de información confidencial	Los trabajadores utilizan claves personales para acceder a sus equipos y a sus cuentas.

					Existen políticas que permiten asegurar la seguridad de datos confidenciales en la municipalidad.
				Empleo de indicaciones realizada	Los trabajadores dan cumplimiento a las normas y políticas establecidas sobre el uso de los equipos y recursos de red
					El alcalde, los gerentes y regidores comprenden la necesidad de cumplir con las normas y políticas sobre el uso de equipos y recursos de red.
			Control de acceso a sistemas y aplicaciones	Restricción del acceso a la información	El área de informática restringe el acceso a información confidencial de la municipalidad.
					Los usuarios externos o invitados requieren del permiso del área de informática.
				Procedimientos seguros de inicio de sesión	Se cuenta con manuales e instructivos para el uso de equipos y acceso a los recursos de red.
					El personal conoce las pautas para crear y recordarse de sus credenciales de usuario.
				Gestión de contraseñas de usuario	Sus contraseñas son impuestas por el área de informática o por los recursos a los cuales desea acceder.
					Cuenta con las opciones para modificar las contraseñas sin depender del área de informática.

					Cuenta con una opción para recuperar sus contraseñas de manera segura.
				Uso de herramientas de administración de sistemas	Se cuenta con un soporte técnico para solucionar problemas de acceso a la red.
					Existen políticas y herramientas para la gestión de riesgos (en caso de pérdida de datos, vulnerabilidad, intrusiones o algún otro riesgo)
					Se cuentan con herramientas y software de ayuda para resolver los inconvenientes en el uso de plataformas virtuales.

Fuente: Elaboración propia.

2.3. Definición conceptual

Diseño del sistema de seguridad basado en el protocolo RADIUS: En concordancia con Soriano (2014) estas son herramientas y procedimientos que deben de utilizar los empleados y la alta dirección de una organización, para garantizar la protección de los datos confidenciales para esta, así como de los sistemas informáticos durante su transmisión a través de una red de telecomunicación.

Administración de acceso a la Red: En la norma ISO 27001 indica que es la encargada del control de accesos para prevenir y no dejar entrar a las personas no autorizadas a través de controles los cuales podrán registra y revocar permisos a los usuarios (ISO, 2018).

2.4. Definición operacional

Diseño del sistema de seguridad basado en el protocolo RADIUS: Para el diseño de la red de una infraestructura de Radius para la seguridad de redes LAN se han determinado las etapas de Utilización de IAS para la administración de acceso a la red, identificación de los requisitos previos de la solución, diseño de la infraestructura de RADIUS, y la creación de un plan de administración (Microsoft, 2018).

Administración de acceso a la Red: De acuerdo a la ISO 27001 el objetivo de la administración del acceso es limitarla a aquellos agentes ajenos a la organización, así mismo dar a los usuarios el acceso necesario únicamente para sus funciones. Para ello se establecen dentro de sus objetivos determinar los requisitos de negocio para el control de acceso y la gestión de acceso de usuario con sus respectivos controladores, responsabilidades del usuario, y el control de acceso a sistemas y aplicaciones (ISO, 2018).

III. METODOLOGÍA

3.1. Tipo de estudio

3.1.1. De acuerdo a la orientación

El presente proyecto se enmarca dentro de los proyectos de investigación y desarrollo del tipo aplicada, porque se busca lograr un nuevo conocimiento para el mejoramiento de la seguridad de acceso a la red e información para la administración de accesos mediante el protocolo RADIUS de la municipalidad.

3.1.2. De acuerdo a la técnica de contrastación

La investigación es de tipo cuasi experimental, puesto que se hará un estudio de la influencia de la implementación del sistema de seguridad de redes basado en el protocolo RADIUS causando una alteración sobre la variable independiente con el fin de evaluar los cambios sobre la variable dependiente.

3.2. El diseño de investigación

3.2.1. Según su enfoque

En la investigación según su enfoque es considerada de tipo mixta debido a que en el desarrollo se aplicaron los enfoques cualitativo y cuantitativo; de acuerdo con Hernández y otros (2014) el enfoque cuantitativo desarrolla el análisis de la realidad objetiva (es decir los datos se recolectan tal como se muestra en la realidad) mediante una serie de mediciones numéricas y el análisis estadístico para determinar patrones de comportamiento de la variable dependiente; en la presente investigación se aplicó este enfoque en la recolección de datos de la administración de accesos a la Red en dos momentos, en el pre test y post test.

Con respecto al enfoque cualitativo Hernández y otros (2014) manifiestan que bajo este se realiza el análisis de la realidad subjetiva (es decir de acuerdo a la percepción del investigador) en un ámbito natural de acuerdo a la experiencia de los participantes, y el procesamiento de datos se hace mediante organizadores visuales u otros instrumentos, siendo que en la presente investigación se realizó el procesamiento de datos en base a la percepción y conocimientos ingenieriles del investigador.

3.2.2. Según su diseño

A. Según la manipulación de las variables

La presente investigación se desarrolló bajo el enfoque cuasi experimental, según Hernández y otros (2014) es el estudio donde se manipula de manera intencional a la variable independiente para ver su efecto sobre la variable dependiente, por ende, se buscó determinar la influencia del sistema de seguridad de redes basado en el protocolo RADIUS sobre la administración de acceso a la red en la Municipalidad Provincial de Carhuaz.

B. Según la recolección de datos

En este caso la investigación es de tipo longitudinal que, de acuerdo a Hernández y otros (2014) tienen como propósito describir variables y analizar su incidencia en varios momentos, es decir la recolección de datos se produjo en dos momentos siendo uno el pre test y el otro el post test, por lo cual los instrumentos de recolección de datos fueron aplicados en dos momentos a la misma muestra.

3.2.3. Según su nivel

La investigación es de tipo explicativa la cual es definida por Hernández y otros (2014) como aquellos estudios que buscan especificar o determinar las propiedades e influencia de la variable dependiente sobre la variable independiente de acuerdo a

las condiciones establecidas por el investigador, para mostrar con precisión un fenómeno o suceso dentro del estudio, por ende, este fue aplicado para determinar y describir las propiedades de cada una de las actividades del proceso de diseño del sistema de seguridad de redes basado en el protocolo RADIUS sobre la mejora de la administración de acceso a la red.

3.3. Población y muestra

3.3.1. Población

En cuanto a la definición, se dice que "La población es la totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis que integran dicho fenómeno y que debe cuantificarse para un determinado estudio integrando un conjunto N de entidades que participan de una determinada característica" (Tamayo, 2012, p. 23).

Según información brindada por la Municipalidad Distrital de Carhuaz, esta cuenta con 53 personas que tienen acceso a la red e información, de los cuales solo 37 son nombrados y 16 son contratados, ambos grupos tienen acceso a la red e información desde las computadoras de la municipalidad, a continuación, se muestra un cuadro con la cantidad de computadoras por área.

Cuadro 4: Usuarios de la municipalidad con acceso a la red

Área	cantidad de usuarios
Segundo piso	
Alcaldía	1
Secretaria General	4
Sala de regidores	1
imagen institucional	2
Gerencia Municipal	3
Informática	3
División de acondicionamiento territorial	4
División de estudios y obras	4

Gerencia de agricultura turismo y medio ambiente	5
Primer piso	
Tesorería	3
Administración y finanzas	2
Rentas	5
caja	1
Gerencia de planificación y presupuestos	3
Turismo	1
RR. HH.	2
Coactivo	2
Sótano	
Logística	4
Agua potable	1
Transito	2
Total	53

Fuente: Elaboración propia

3.3.2. Muestra

En el trabajo de investigación se aplicó una muestra censal, según Ramírez (2009) se define como muestra censal a aquellas muestras donde todas las unidades de investigación son parte de la muestra; por ende, se tomaron a toda la población que son 53 personas, como parte de la muestra debido a que no se cuenta con muchas unidades de muestra.

3.4. Técnicas e instrumentos de recolección de datos

3.4.1. Técnicas

En la investigación empleó la técnica de la entrevista que según Hernández y otros (2014) se trata de una reunión para conversar e intercambiar información sobre el tema de estudio, entre el entrevistador y los entrevistados, este técnica fue aplicada para determinar los requerimientos de la red; a su vez, fue necesario la aplicación de encuestas el cual define Hernández y otros (2014) como una técnica usada para

analizar y evaluar la problemática planteada, será aplicado para evaluar el estado de la red actual.

3.4.2. Instrumentos

Con respecto a la entrevista se utilizó la guía de entrevista la cual Hernández y otros (2014) define como un documento que contiene los temas, preguntas sugeridas y aspectos a analizar en una entrevista, cuya finalidad es obtener información necesaria para responder el planteamiento del problema, por ende, es utilizado para tener documentada a la entrevista.

Como instrumento de recolección de datos en el trabajo de investigación se empleó al cuestionario que según Hernández y otros (2014) son utilizados en las encuestas como instrumentos de recolección de datos el cual consiste en un conjunto de preguntas respecto a las variables a medir, los cuales deben de ser congruentes con el planteamiento del problema y la hipótesis, por lo cual se aplicaron para elaborar preguntas estructuradas de nivel.

Cuadro 5: Técnicas e instrumentos aplicados

Técnica	Instrumento
Entrevista	Guía de entrevista
Encuesta	Cuestionario

Fuente: Elaboración propia

3.5. Técnicas de análisis y prueba de hipótesis

Fase 1: Diagnostico de la situación actual de la administración de accesos a la Red en la Municipalidad provincial de Carhuaz

Esta se realizó mediante la aplicación de la encuesta a los 53 empleados de la municipalidad quienes tuvieron acceso a la Red, los cuales son parte de la muestra,

la cual permitió determinar las necesidades insatisfechas con respecto a la administración de acceso.

Fase 2: Determinación de los requerimientos de la red

Esta se realizó mediante la aplicación de la entrevista a los empleados de la municipalidad sobre los sistemas de seguridad con el fin de poder determinar los requerimientos de la red.

Fase 3: Implementación del sistema de seguridad

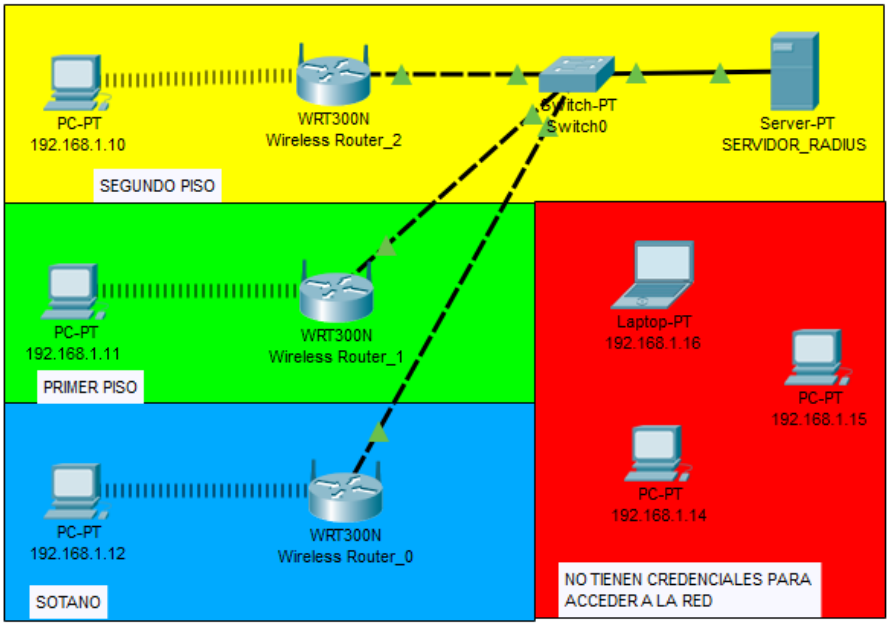
Se implementó el sistema de seguridad para la administración de acceso a la Red usando el protocolo RADIUS, el cual permite evitar que las personas no autorizadas accedan a esta y consecuentemente a la información de la Municipalidad, con el fin de proteger los datos personales de la población y que no pueden ser expuestos ante los usuarios no autorizados.

Asimismo, dicha solución fue simulada por medio de un prototipo sobre máquinas virtuales utilizando el software VMware y emulando las características de los equipos del caso de estudio; esto se debe a que la aplicación de la propuesta de la nueva estructura de red no pudo ser realizada directamente en el caso de estudio por motivos de que esta es una institución pública y por ende se rige bajo las prácticas burocráticas impuestas por el estado.

Fase 4: Simulación de la estructura de la Red mediante el Software Cisco Packet Tracer versión 7.2

Se realizó la simulación mediante el Software Cisco Packet Tracer, el cual permitió elaborar el modelo de comprobación acerca del funcionamiento del sistema de autentificación de accesos llamado RADIUS, el cual quedo de la siguiente manera:

Figura 1: Simulación de la red



Fuente: Elaboración propia

Fase 5: Evaluación de la implementación de la red

Se aplicó una encuesta final a los empleados de la municipalidad, sobre la eficiencia del sistema de seguridad usando el protocolo RADIUS, para saber su perspectiva y si cumple con sus expectativas.

Fase 6: Redacción de informe final de tesis

Al obtener los resultados de la encuesta y cuestionarios se procedió a elaborar el presente informe final.

IV. RESULTADOS DE LA INVESTIGACIÓN

4.1. Descripción del trabajo de campo

4.1.1. Objetivo específico 1: Evaluación de la administración de accesos

En lo que respecta al diagnóstico preliminar sobre el desempeño de la red que viene funcionando en la Municipalidad Provincial de Carhuaz se realizó la aplicación del cuestionario sobre la administración de accesos de red a todo el personal que labora en el municipio en estudio. Para la clasificación de los datos obtenidos se aplicó las siguientes tablas de baremación:

Cuadro 6: Baremación de la variable y sus dimensiones

Dimensiones y variable	Rangos de los niveles		
	Bueno	**Regular**	**Malo**
Dimensión 1: Requisitos de negocio para el control de accesos	15 - 20	10 - 14	4 - 9
Dimensión 2: Gestión de acceso de usuario	37 – 50	24 – 36	10 - 23
Dimensión 3: Responsabilidades del usuario	23 – 30	14 – 22	6 – 13
Dimensión 4: Control de acceso a sistemas y aplicaciones	37 – 50	24 – 36	10 - 23
Variable: Administración de acceso a la red	111 – 150	70 – 110	30 – 69

Fuente: Elaboración propia

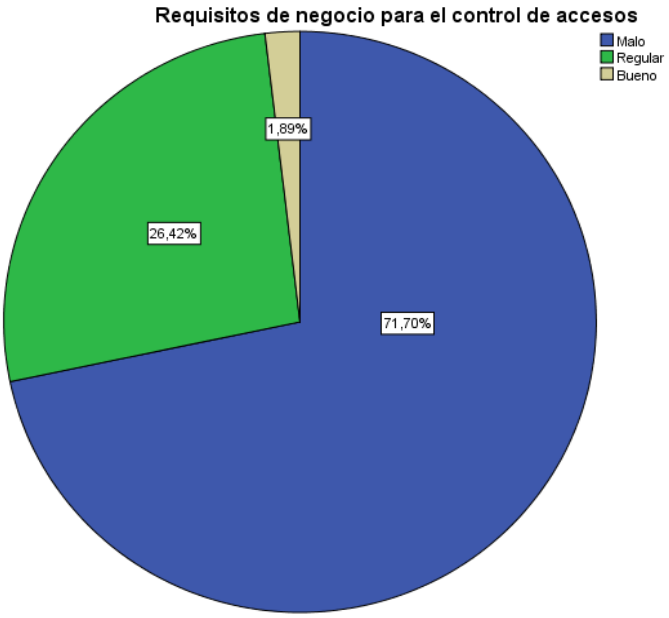
En lo que respecta a la dimensión requisitos de negocio para el control de acceso se hallaron los siguientes resultados:

Cuadro 7: Calificación de los requisitos de negocio para el control de acceso

	Frecuencia	**Porcentaje**
Bueno	1	1,9
Regular	15	26,4%
Malo	37	71,1%

Fuente: Elaboración propia

Figura 2: Calificación de la dimensión requisitos de negocio para el control de accesos



Fuente: Elaboración propia

En el cuadro 7 y figura 2 se observa que la mayoría de encuestados, representados por el 71,1% del total califican a los requisitos de negocio para el control de accesos de la administración de acceso a la red como malo, seguidamente un 26,4% la califican como regular y finalmente un 1,9% lo califican como bueno.

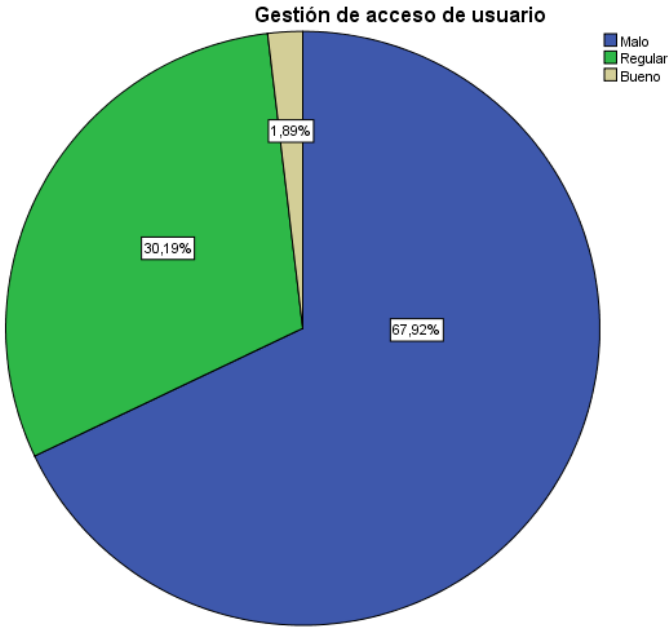
En lo que respecta a la dimensión gestión de acceso de usuario se hallaron los siguientes resultados:

Cuadro 8: Calificación de la gestión de acceso de usuario

	Frecuencia	**Porcentaje**
Bueno	1	1,9%
Regular	16	30,2%
Malo	36	67,9%

Fuente: Elaboración propia

Figura 3: Calificación de la dimensión gestión de acceso de usuario



Fuente: Elaboración propia

En el cuadro 8 y figura 3 se observa que la mayoría de encuestados, representados por el 67,9% del total califican a la gestión de acceso de usuario de la administración de acceso a la red como mala, seguidamente un 30,2% la califican como regular y finalmente un 1,9% lo califican como buena.

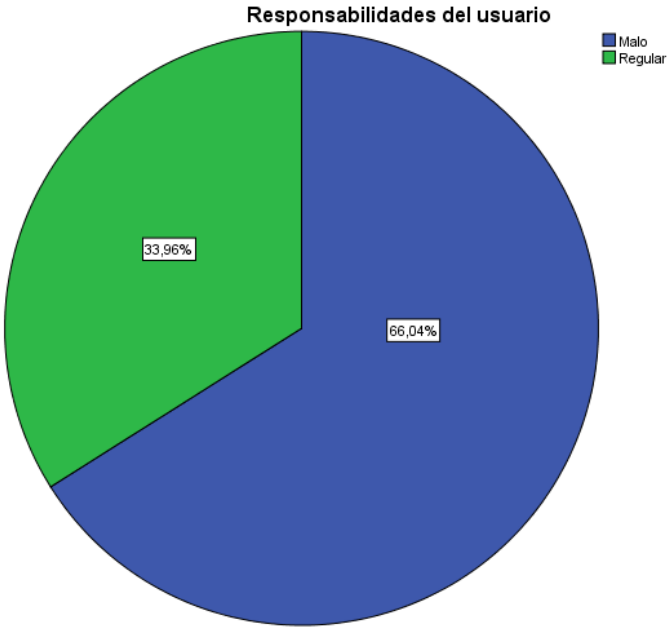
En lo que respecta a la dimensión responsabilidades del usuario se hallaron los siguientes resultados:

Cuadro 9: Calificación de las responsabilidades del usuario

	Frecuencia	**Porcentaje**
Regular	18	34%
Malo	35	66%

Fuente: Elaboración propia

Figura 4: Calificación de la dimensión responsabilidades del usuario



Fuente: Elaboración propia

En el cuadro 9 y figura 4 se observa que la mayoría de encuestados, representados por el 66% del total califican a las responsabilidades del usuario en la administración del acceso a la red como malas, y finalmente un 34% lo califican como regulares.

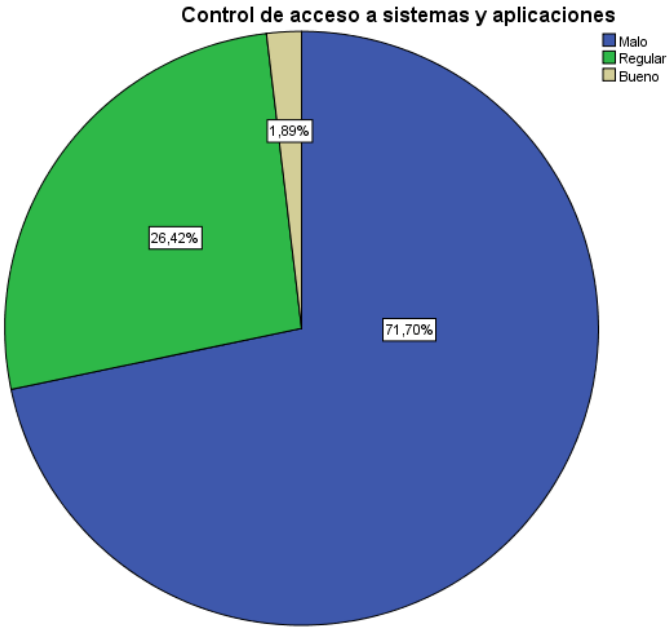
En lo que respecta a la dimensión control de acceso a sistemas y aplicaciones se hallaron los siguientes resultados:

Cuadro 10: Calificación del control de acceso a sistemas y aplicaciones

	Frecuencia	**Porcentaje**
Bueno	1	1,9%
Regular	14	26,4%
Malo	38	71,7%

Fuente: Elaboración propia

Figura 5: Calificación de la dimensión control de acceso a sistemas y aplicaciones



Fuente: Elaboración propia

En el cuadro 10 y figura 5 se observa que la mayoría de encuestados, representados por el 71,7% del total califican al control de acceso a sistemas y aplicaciones en la administración del acceso a la red como malo, seguidamente el 26,4% la califican como regular y finalmente un 1,9% lo califican como bueno.

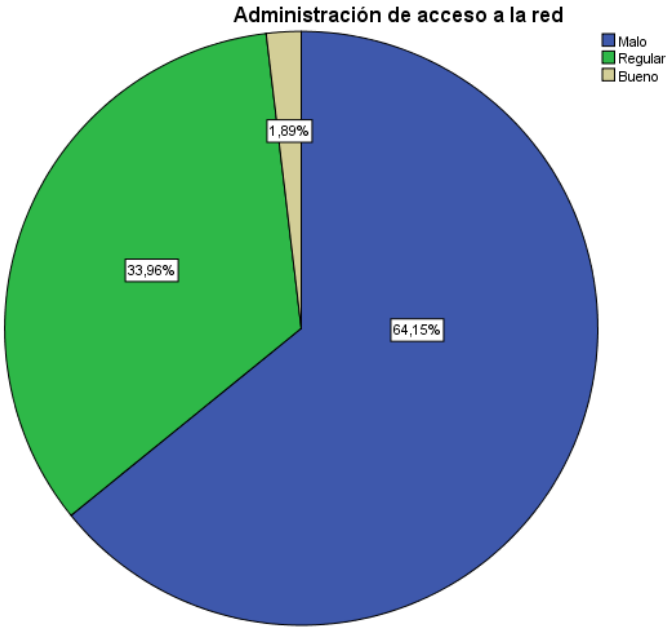
En cuanto al estudio de la variable administración de acceso a la red se hallaron los siguientes resultados:

Cuadro 11: Calificación de la administración de acceso a la red

	Frecuencia	**Porcentaje**
Bueno	1	1,9%
Regular	18	34,0%
Malo	34	64,1%

Fuente: Elaboración propia

Figura 6: Calificación de la variable administración de acceso a la red



Fuente: Elaboración propia

En el cuadro 11 y figura 6 se observa que la mayoría de encuestados, representados por el 64,1% del total califican a la administración del acceso a la red como mala, seguidamente el 34% la califican como regular y finalmente un 1,9% lo califican como buena.

4.1.2. Objetivo específico 2: Desarrollo del sistema de seguridad de redes

A. Diagnóstico

La municipalidad provincial de Carhuaz es una entidad autónoma en lo que respecta a política, economía y administración, la cual tiene bajo su jurisdicción el territorio de la provincia de Carhuaz del departamento de Ancash y cuya sede se encuentra en el distrito de Carhuaz, siendo la capital de la mencionada provincia.

La Municipalidad Provincial de Carhuaz tiene dentro de sus órganos de asesoramiento a la Gerencia de Planeamiento y Presupuesto, la cual tiene a su cargo a la Oficina de Estadística, Tecnología y Redes informática encargada de conducir los procesos de producción y gestión de datos e información relacionada con el

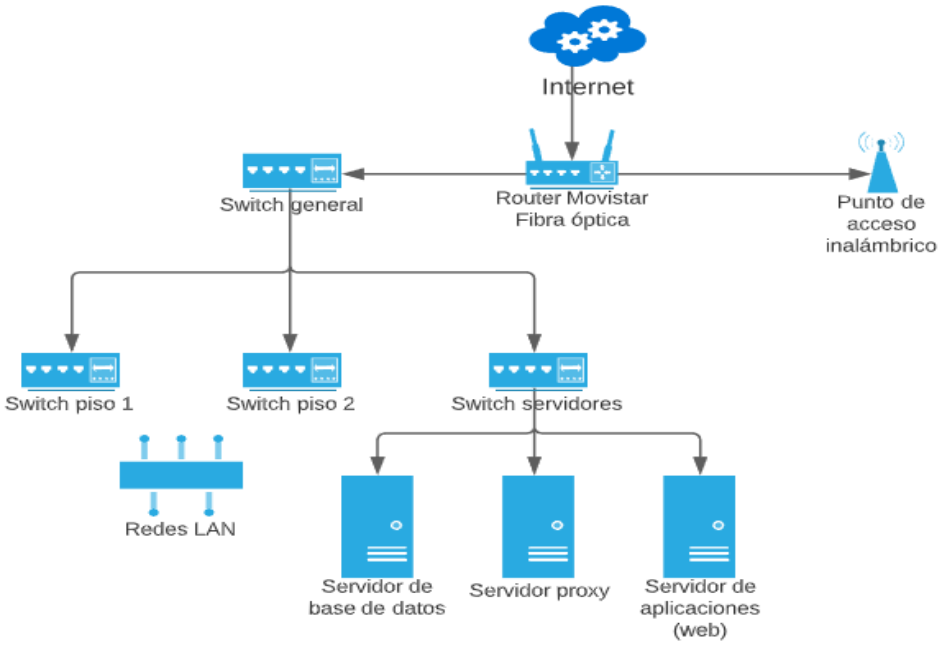
Sistema de Estadísticas; así mismo esta oficina se encarga de gestionar los procesos de actualización tecnológica mediante la incorporación de equipos, redes y software de última generación con fines de sistematización de procesos y simplificación administrativa.

De acuerdo a información proveniente de la oficina en estudio la Municipalidad provincial de Carhuaz posee una infraestructura de red IP operativa, la cual permite que los usuarios puedan compartir recursos y servicios mediante una red de área local, así como permitir el acceso al servicio de internet, sin embargo, se logró identificar la ausencia de políticas de seguridad que controlen el tráfico de paquetes que circulan entre las redes (Anexo 5).

El diseño actual de red garantiza la conectividad de los dispositivos pertinentes más no garantiza el nivel de seguridad apropiado para una entidad pública de nivel, ello es ocasionado por la ausencia de mecanismos que administren el acceso a los recursos de red, siendo ello el motivo por el que la información de carácter privado puede ser accesible mediante un ataque desde la intranet, pudiendo ocasionar sustracciones o modificaciones lo cual traería consigo graves consecuencias en el municipio.

La topología lógica de la red de datos de la Municipalidad Provincial de Carhuaz es la siguiente:

Figura 7: Topología lógica de la red de datos



Fuente: Elaboración propia en base a la infraestructura actual de la Red de la Municipalidad Provincial de Carhuaz.

La infraestructura actual de la Municipalidad Provincial de Carhuaz no posee un diseño jerárquico de red, como se puede observar en la Figura 2 es una LAN plana de libre acceso que no cuenta con un sistema de seguridad para su control, resultando vital para la institución administrar la red y proteger la información, recurso de mucho valor que de ser manipulada de manera inadecuada generaría pérdidas irreparables a la institución.

La interconexión con redes externas se lo realiza a través de la Red de Movistar, único proveedor del servicio de internet del municipio. Para la comunicación se ha asignado la red LAN, con un pool de direcciones IP públicas en el rango 192.168.1.1/30.

Para la conexión de los dispositivos de usuario final con la red local se utilizan los switch de 24 puertos de marca Satra de la serie SA-S0124, los conmutadores son completamente administrables y gestionables mediante web pero actualmente no poseen ninguna configuración.

No existe un firewall que proteja y controle el tráfico de paquetes que circulan entre las redes LAN e Internet, la navegación de páginas web no es restringida mediante un Proxy que corre sobre la plataforma Linux (CentOS 5.5) implementado en la computadora de escritorio que funciona como servidor, siendo esta de Marca HP de modelo SLIM DESKTOP 290-P003LA.

La infraestructura tecnológica de la Municipalidad Provincial de Carhuaz contiene la información necesaria para su funcionamiento, conteniéndose datos sobre los procesos internos, personal, catastro, impuestos, etc. Los cuales son necesarios para la prestación de servicios.

La página web Institucional se encuentra alojada en un servidor externo, por tal razón dentro de la red LAN no se cuenta con los privilegios necesarios para establecer reglas y políticas que controlen los accesos no autorizados, sino que ello responde a las cuentas de acceso a este servicio.

Dentro de los requerimientos técnicos para la implementación del estándar 802.1x se tienen a tres elementos básicos para su operación, un servidor de autenticación, el equipo autenticador (punto de acceso inalámbrico o switch) con soporte 802.1x y el suplicante instalado en todos los dispositivos de usuario final.

El equipamiento actual con el que cuenta la infraestructura de la red de la Municipalidad Provincial de Carhuaz:

Cuadro 12: Equipos de red de la Municipalidad Provincial de Carhuaz

Cantidad	Equipo	Marca	Modelo
1	Router inalámbrico	MITRASTAR	GPT – 2741GNAC
1	Servidor	DELL	PowerEdge T40 8/1
1	PC - Servidor	HP	SLIM DESKTOP 290-P003LA
1	Servidor	DELL	PowerEdge T40 16/2

4	Switch	SATRA	SA-S0124
2	Acces Point	SATRA	SA-AP300AG

Fuente: Elaboración propia

Hardware

La Municipalidad Provincial de Carhuaz se encuentra equipado con 2 servidores Dell PowerEdge T40 16/2, los cuales ideales para ambientes de todo tipo y tamaño, eficientes para aplicaciones de virtualización, servidor de aplicaciones web, correo electrónico, base de datos, etc. Las especificaciones de estos servidores son las siguientes:

Cuadro 13: Especificaciones de servidor PowerEdge T40 8/1

Recurso	Descripción
Número de Procesadores	2
Núcleo de Procesador	4
Velocidad del Procesador	3.5GHZ
Tipo de Memoria	DDR4 2666
RAM	8 GB
Tipo de Procesador	Intel Xeon E-2224G
Procesadores Compatibles	Intel Xeon E Series
Almacenamiento	1 TB
Interfaz de Red	Two BCM5709C with dual-port Gigabit
Virtualización	Sí

Fuente: Elaboración propia

Cuadro 14: Especificaciones de servidor PowerEdge T40 16/2

Recurso	Descripción
Número de Procesadores	2
Núcleo de Procesador	4
Velocidad del Procesador	3.4GHZ
Tipo de Memoria	DDR4 2666
RAM	16 GB

Tipo de Procesador	Intel Xeon E-2224G
Procesadores Compatibles	Intel Xeon E Series
Almacenamiento	2 TB
Interfaz de Red	Broadcom 5720 Dual Port 1GBE
Virtualización	Sí

Fuente: Elaboración propia

Cuadro 15: Especificaciones de la PC – Servidor SLIM DESKTOP 290-P003LA

Recurso	Descripción
Número de Procesadores	2
Núcleo de Procesador	4
Velocidad del Procesador	3,6 GHz
Tipo de Memoria	DDR4-2400
RAM	4 GB
Tipo de Procesador	Intel Core i3
Procesadores Compatibles	Procesador Intel® Core™ i3
Almacenamiento	1 TB
Interfaz de Red	LAN Ethernet Gigabit 10/100/1000 integrada
Virtualización	Sí

Fuente: Elaboración propia

Los equipos usados son los Switch Marca SATRA del modelo SA-S0124, los cuales ofrece funciones básicas de administración, seguridad y calidad de servicio (QoS), la administración y configuración se la realiza mediante una interfaz de usuario web. En el cuadro 10 se detallan las especificaciones del switch SATRA:

Cuadro 16: Especificaciones del Switch modelo SA-S0124

Recurso	Descripción
Capacidad y velocidad de envío	100 Mbps
Estándar	IEEE 802.3/u/x (No se asocia a la autenticación radius)
Interface	24 x 10/100 Mbps con autonegociación (auto MD/MDIX)

Medio de transmisión	100 BASE – TX: UTP Categoría 5, 5e o superior
Métodos de transmisión	Almacenamiento y reenvío con aprendizaje automático de direcciones MAC
Capacidad de conmutación	4.8 Gbps

Fuente: Elaboración propia

En la actualidad, la implementación de redes inalámbricas se considera como una solución de movilidad, flexibilidad y productividad, lo que ha permitido que esta tecnología crezca y esté presente en casi todos los lugares donde exista una red cableada.

Sin embargo, todas las ventajas que ofrece una red inalámbrica traen consigo muchos riesgos de seguridad que se deben contrarrestar, principalmente los fallos asociados a la falta de mecanismos de seguridad robustos que protejan los recursos de red frente a los accesos no autorizados.

Para brindar el servicio Wi-Fi, la municipalidad utiliza puntos de acceso inalámbricos marca SATRA, las especificaciones técnicas de los equipos se pueden ver en el cuadro 11.

Cuadro 17: Especificaciones del Access Point SA-AP300AG

Recurso	**Descripción**
Velocidad de transmisión inalámbrica	300 Mbps
Estándar	IEEE 802.11n (No se asocia a la autenticación radius)
Frecuencias	2.4GHz
Antenas	2 antenas fijas omnidireccional de 5dBi
Firewall	Integrado
Seguridad inalámbrica	64/128-bits WEP, WPA/WPA2

Fuente: Elaboración propia

En lo que respecta al router inalámbrico empleado en la red de la Municipalidad Provincial de Carhuaz se tienen las siguientes características:

Cuadro 18: Especificaciones del Router Mitrastar – 2741GNAC

Recurso	Descripción
Velocidad de transmisión alámbrica	1000Mbps Gigabit Ethernet
Velocidad de transmisión inalámbrica	
Ancho de banda máximo en el upstream	1Gbps
Ancho de banda máximo en el downstream	1Gbps
Estándar	802.11
Frecuencias	20/40/80MHz
Antenas	2 antenas internas 3dBi /
Firewall	Sí
Proxy	Sí
Seguridad inalámbrica	Canales soportados: del 1 al 13. Acceso sin encriptación, WEP (64 / 128bit), WPA2 con PSK, WPA + WPA2 modo mixto. Posibilidad de restringir acceso por dirección MAC

Fuente: Elaboración propia

Software

La identificación de los sistemas operativos instalados en cada uno de los equipos que se conectan a la red de datos de la Municipalidad Provincial de Carhuaz, es de suma importancia a la hora de elegir el método de autenticación del sistema AAA.

La infraestructura actual de red consta de un servidor proxy y un servidor de aplicaciones para base de datos. En la siguiente se detallan los sistemas operativos instalados en cada uno de los equipos del municipio:

Cuadro 19: Servidores de la Municipalidad Provincial de Carhuaz

Servidor	Sistema operativo	Aplicación
PowerEdge T40 8/1	CentOS 6.3	Apache server, JSP
Slim Desktop 290-p003la	CentOS 6.3	Proxy Transparente
PowerEdge T40 16/2	Windows Server 2008	SQL Server y Mysql server

Fuente: Elaboración propia

En lo que respecta a la conexión del sistema operativo de las estaciones de trabajo se tiene que el estándar 802.1X del router controla el acceso de los usuarios a la red mediante el proceso de autenticación, fue estandarizado para implementaciones únicamente en la red inalámbrica. Uno de los tres elementos del estándar 802.1x son los suplicantes, por tal razón, es de suma importancia identificar las plataformas instaladas en los equipos de los usuarios, que permita determinar si el sistema operativo soporta el método de autenticación que se utilizará o si por el contrario se requiera de algún software adicional.

B. Determinación de los requerimientos

El diseño de una red funcional que cumpla con todos los requerimientos para un correcto funcionamiento implica mucho más que solo hecho de interconectar computadoras, siendo que debe de satisfacer todas las necesidades por las cuales ha sido concebida, orientada para que logre un alto rendimiento, mediante lo cual los usuarios que van hacer uso de la red puedan cumplir todas las actividades que les demanda su trabajo, con una conectividad a las diferentes aplicaciones con un tiempo de respuesta razonable. También tiene que cumplir características como escalabilidad y adaptabilidad; lo cual implica que tenga la capacidad de un continuo crecimiento y adaptación para poder incorporar nuevas tecnologías que van apareciendo y uno de los factores más críticos para el éxito de una red es la capacidad para que pueda ser

administrable es decir monitorear y controlar las incidencias que puedan ocurrir en la red.

El diseño de una red inalámbrica planteada en la presente investigación comprende al conjunto de protocolos de comunicación 802.11n/ac y con el protocolo de autenticación, autorización y contabilización Radius, la cual está enfocada en suplir las necesidades actuales de la Municipalidad Provincial de Carhuaz. Para elaborar se tiene en consideración las limitaciones y deficiencias encontradas actualmente en la red. Las principales características para desarrollar esta metodología son:

- Integrar a los equipos conectados a la red.
- Establecer las herramientas para la elaboración de la topología física y lógica de la red.
- Determinar los equipos que cumplan con los estándares requeridos.
- Determinar y detallar el tipo seguridad, monitoreo y mantenimiento de la red

La actual red institucional no cumple con ningún estándar de cableado estructurado, llegando al punto de considerarla una red subestándar con serias deficiencias desde todos los puntos de vista del cual se quiera analizar, para determinar las principales deficiencias de esta red se recurrió diferentes técnicas, así como la opinión de los usuarios y sobre todo las practicas realizada en la institución para poder identificar estas necesidades que precisan ser subsanadas y las cuales son la seguridad, la velocidad, la escalabilidad, el control de usuarios y la movilidad.

Los problemas mencionados se encuentran asociados con los problemas de la institución ya que la falta de espacio físico, el hacinamiento y alto índice de rotación del personal repercuten directamente en la red para este tipo de problema la solución más idónea que se propone es una red inalámbrica ya que este tipo de red va

solucionar parte la problemática principal de la red institucional y para poder solucionar las demás problemáticas se tiene que recurrir a diferentes tipos de tecnologías que integradas a la red inalámbrica va representar la solución a todos los problemas que aquejan a la red.

Una vez conocido las necesidades de la red se realizó un análisis comparativo de las diferentes tecnologías que integradas a la red inalámbrica subsanas todas esas deficiencias teniendo en cuenta para la solución se debe contemplar visión de futuro, compatibilidad entra las distintas soluciones y sobre todo el uso de los recursos de la municipalidad.

Cuadro 20: Comparación de los recursos disponibles

	Req.	Seguridad	Velocidad		Escalabilidad	Control de usuarios	Movilidad	Compatibilidad	
	Protocolo		Mínima	Máxima				Equipos	Protocolos
Recursos existentes	802.11g	WEP	10 Mbit/s	54 Mbit/s	---	Independiente	Diferentes SSID	Sí	No
	802.11. n	WPA	54 Mbit/s	600 Mbit/s	---	Independiente	Diferentes SSID	Sí	Sí
	Kerberos	Cliente – Servidor	---	---	Dominio	Directorio activo	Windows server	Sí	Sí
Recursos por adquirir	Radius	802.1X	---	---	Dominio	Directorio activo	Windows server	Sí	Sí
	802.11 ac	WPA2	150 Mbit/s	54 Gbit/s	---	Independiente	Diferentes SSID	Sí	Sí
	Diameter	802.1X	---	---	Dominio	Directorio activo	Windows server	No	No

Fuente: Elaboración propia

La solución más conveniente para subsanar las deficiencias es el uso de los protocolos de comunicación 802.11n/ac, a su vez se requieren modernizar algunos equipos debido a que estos no poseen conectividad para ambos protocolos y el protocolo Radius, el cual cumple con las características de autenticación, autorización y contabilización, el cual puede ser habilitados con los recursos que existen en la institución específicamente en el servidor Windows Server 2008 R2, la mezcla de estos protocolos dan solución a las necesidades que afronta la red actual, como también una solución para escenarios futuros.

En lo que respecta a los requerimientos para la red a diseñarse se tiene:

Cuadro 21: Requerimientos de la red a diseñarse

Requerimiento	Normativa	Módulo
Gestión del acceso de usuarios	Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.	Registro de usuarios
		Gestión de privilegios
		Gestión de contraseñas de usuario
		Revisión de los derechos de acceso de los usuarios
Responsabilidades del usuario	Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que la cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.	Uso de contraseña
		Equipo informático de usuario desatendido
Control de acceso a la red	Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que el acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan: • Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones. • Que se aplican los mecanismos de autenticación adecuados a los usuarios y equipos.	Política de uso de los servicios de red
		Autenticación de usuario para conexiones externas
		Autenticación de nodos de red
		Segregación de las redes
		Control de conexiones a las redes

	• El cumplimiento del control de los accesos de los usuarios a los servicios de información.	Control de encaminamiento de la red
Integración de ordenadores portátiles	Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que la protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo. En el uso de la informática móvil deberían considerarse los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente.	Informática Móvil

Fuente: Elaboración propia

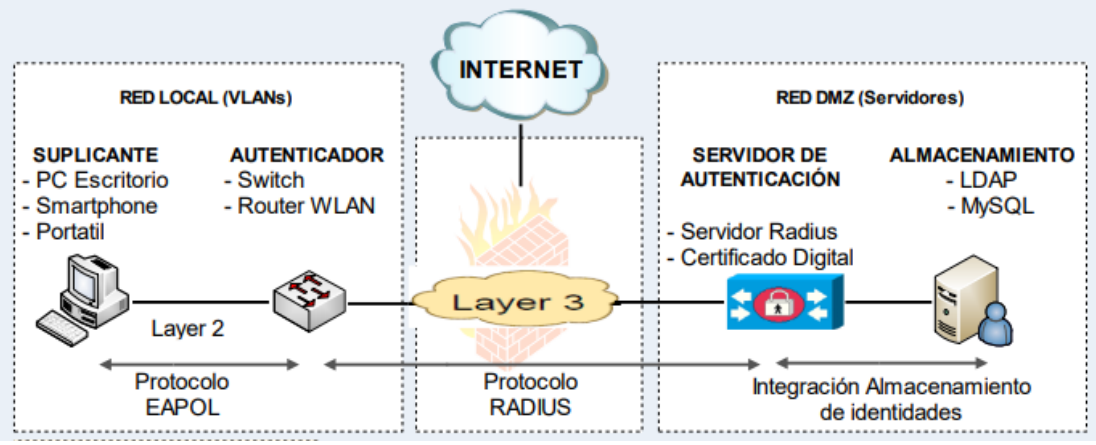
C. Diseño de la infraestructura de red

En lo que respecta al diseño físico de la red se tiene al tipo de infraestructura del lugar donde se desea montar la red, debido a que puede ocasionar que no se reciba la señal de los puntos de acceso hacia las tarjetas inalámbricas por atenuaciones de señal, los diferentes tipos de material de acuerdo a su composición representa un obstáculo muy importante para la propagación de las ondas de radio. No todos están estructurados de la misma manera esa va varias dependiendo el lugar y los factores climáticos. Por esto hay que inspeccionar el lugar previamente. El entorno físico va ser un factor clave ya que las áreas despejadas o abiertas proporcionan un mejor alcance de la señal de los Access Point que las áreas cerradas o congestionadas; todos estos aspectos son relevantes al momento de la distribución adecuada de los Access Point.

Así mismo es necesario resaltar que el diseño de la red de datos de la Municipalidad Provincial de Carhuaz se encuentra realizado en base al estándar IEEE 802.1x para el control de acceso a la red, el modelo usado en la implementación se muestra en el esquema de la Figura 8. Todas las consideraciones de diseño que se describen a

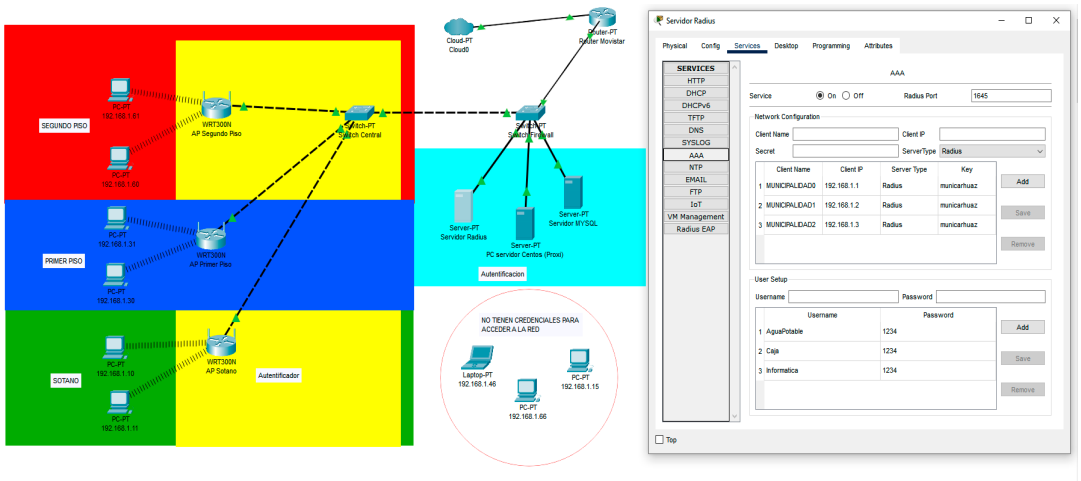
continuación, se basan en los requerimientos del estándar 802.1x usando como método de autenticación EAP-TTLS.

Figura 8: Modelo de implementación del control de acceso



Fuente: Adaptación de Deploying Wired 802.1x de CISCO.

Figura 9: Diseño de la red y configuración usada



Fuente: Elaboración propia.

Los componentes básicos para un sistema 802.1x son: suplicante, autenticador y el servidor de autenticación, sin embargo, la solución planteada en la red de datos del Municipio requiere cuatro componentes adicionales, una autoridad certificadora, un firewall, un directorio LDAP y una base de datos MySQL.

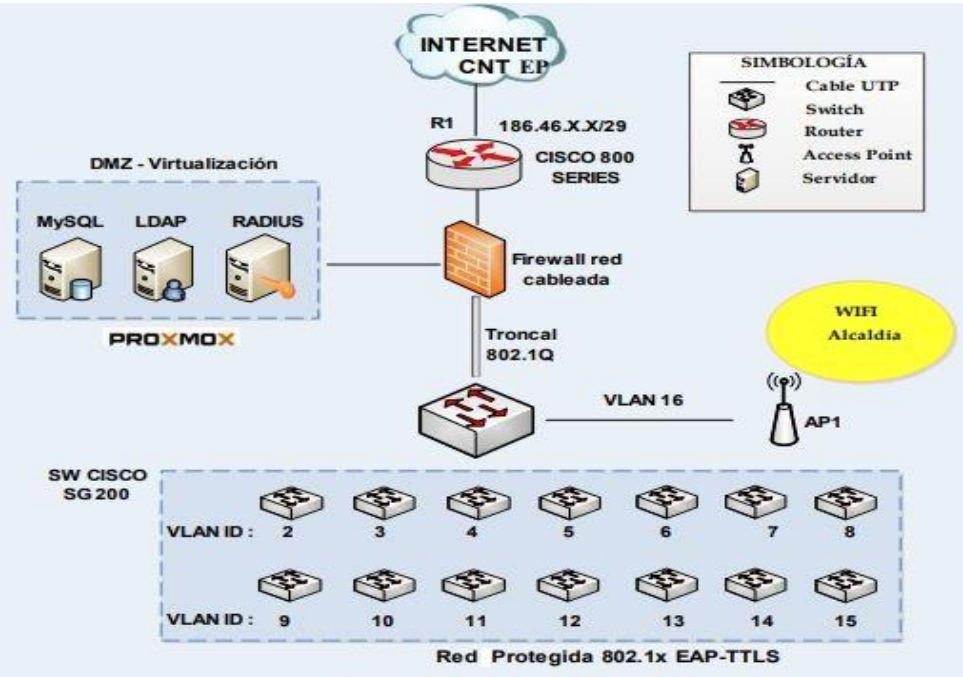
El primer elemento de la arquitectura es un cliente inalámbrico que se conecta al punto de acceso a través de una tarjeta de red inalámbrica, el segundo elemento es un

punto de acceso que sirve como medio para que el cliente inalámbrico se conecte con el servidor de seguridad y la red ethernet, y el tercer elemento es el servidor de seguridad que contiene los servicios de DHCP para que los clientes obtengan una dirección IP, webRADIUS para administrar la autenticación de los clientes y un firewall para autorizar o denegar el acceso a la red ethernet o al Internet.

D. Integración del servicio AAA a la red

El servidor Radius será instalado en el servidor proxy, en el cual se encuentra instalado el Sistema Operativo Windows Server 2008 R2, el cual interactuará con el servidor de base de datos para validar las credenciales de usuario y permitir el acceso a los dispositivos acorde a las políticas del municipio. La integración de la red se realizará de la siguiente manera:

Figura 10: Integración del control de acceso a la red actual



Fuente: Elaboración propia en base a la infraestructura actual de la red de la Municipalidad Provincial de Carhuaz

El software propuesto para la administración de la Red Radius será empleada a Activación del Active Directory Domain Services para minimizar los costos de

licencia, en este sentido es necesario mencionar que los software especializados para la gestión de una Red Radius poseen un elevado coste. En lo que respecta al hardware a emplearse se requerirán de nuevos dispositivos electrónicos debido a que los switchs y Access point con los que cuenta la Municipalidad Provincial de Carhuaz no soportan el protocolo 802.1X; los recursos hardware a emplearse son:

Acces point: Los Access Point (AP) son equipos que brinda a los dispositivos que desean conectarse a la red de forma inalámbrica puedan hacerlo mediante Wi-Fi, o protocolos relacionados. Por lo general se conecta a un Router como un dispositivo independiente o también puede conectarse a un switch para formar parte de la red y de esa manera tener una red hibrida.

Cisco WAP371 Wireless-AC: Es un dispositivo que entregar alta velocidad de conectividad inalámbrica a los usuarios además brinda acceso más seguro y fiable. El Cisco WAP371 Wireless Access Point tiene doble banda 2.4/5 GHz, posee una instalación sencilla pero potente de un alto rendimiento. Ofrece funciones de clase empresarial, tales como la conectividad Gigabit Ethernet, un portal cautivo personalizable para el acceso a invitados y una seguridad robusta.

Figura 11: Equipo Cisco WAP371 Wireless-AC

Fuente: Catálogo CISCO

Hawking HW7ACB Wireless-AC: El HW7ACB ofrece el estándar inalámbrico más rápido y lo combina con potentes antenas de alta ganancia para mejorar su red inalámbrica en fiabilidad, alcance y cobertura. Fácil de instalar procedimientos permiten que cualquier usuario de la computadora pueda configurar. Con capacidades integradas de Wireless-AC, este access point es compatible con el estándar IEEE 802.11 y sus protocolos 802.11 n/ac, así como con dispositivos inalámbricos compatibles a 5.0GHz para ofrecer una transferencia de hasta 750Mbps.

Figura 12: Equipo Hawking HW7ACB Wireless-AC

Fuente: Catálogo CISCO

Wireless LAN Controller: Es un dispositivo controlador de LAN inalámbricas que se utiliza en combinación con el Protocolo de Acceso Ligero Point (LWAPP) para administrar puntos de acceso en grandes cantidades de operaciones de red. El controlador de LAN inalámbrica es parte del plano de datos en el modelo inalámbrico de Cisco. El controlador WLAN se encarga de automatizar la configuración de los puntos de acceso inalámbricos.

CISCO 2500 AIR-CT2504-15-K9: Esta serie de equipos están hechos para administrar las funciones inalámbricas. Ayuda a los puntos de acceso Cisco Aironet a comunicarse en tiempo real para simplificar el despliegue y operación de redes inalámbricas. El Wireless Controller trabaja con los protocolos 802.11n/ac los cuales proveen fiabilidad y da la flexibilidad para escalar a medida que crecen sus necesidades de la red.

Figura 13: Equipo CISCO 2500 AIR-CT2504-15-K9

Fuente: Catálogo CISCO

ZyXEL NXC2500 Wireless Controller: El ZyXEL NXC2500 está diseñado para proporcionar a las empresas una solución que funciona como una respuesta a la planificación implementación, mantenimiento, monitoreo y al tiempo que ofrece la gestión de autenticación además el acceso para invitados. El dispositivo apoya el manejo inicial de 8 puntos de acceso y proporciona escalabilidad, con un total máximo soportado hasta 64 puntos de acceso, además ofrece tranquilidad y el futuro de las redes LAN inalámbricas centralizadas de las pequeñas y medianas-empresas.

Figura 14: Equipo ZyXEL NXC2500 Wireless Controller

Fuente: Catálogo ZyXEL

Tarjetas de red inalámbrica: Una tarjeta de red inalámbrica (WNIC) es un controlador de interfaz de red que se conecta a una red de ordenadores basada en ondas de radio, al igual que otras tarjetas de red, funciona en la Capa 1 y Capa 2 del modelo OSI. Una WNIC es un componente esencial para que una PC de escritorio pueda integrase a la red inalámbrica.

Satechi® Wireless Mini Dual Band Wi-Fi USB Mini Adapter: El Satechi Wireless Mini Adaptador USB Wifi es un adaptador para actualizar la velocidad de la red inalámbrica de una computadora. Alcanza una velocidad de hasta 433Mbps, incluso en equipos antiguos para que se unan a una red inalámbrica. Con el adaptador Wifi Satechi, todo lo que necesita para la configuración es instalar los controladores y conecte a un puerto USB.

Figura 15: Equipo Wireless Mini Dual Band Wi-Fi USB Mini Adapter

Fuente: Catálogo Satechi

Sabrent Hi-Gain AC600 Dual Band Wi-Fi USB Mini Adapter: El Sabrent Hi-Gain AC600 Dual Band Wi-Fi USB Mini Adapter es un adaptador para actualizar la velocidad de la red inalámbrica de una computadora. Alcanza una velocidad de hasta 433Mbps, incluso en equipos antiguos para que se unan a una red inalámbrica. Con el adaptador Wifi Satechi, todo lo que necesita para la configuración es para instalar los controladores y conecte a un puerto USB.

Figura 16: Hi-Gain AC600 Dual Band Wi-Fi USB

Fuente: Catálogo Sabrent

E. Distribución de los dispositivos

Se distribuirán los access point de manera se cubra la mayor parte de las instalaciones de la Municipalidad Provincial de Carhuaz teniendo en cuenta el menor uso de access point para este fin, brindando la posibilidad de establecer los obstáculos que se van a presentar ya sea el tipo de material con que fue construido el edificio para tener en cuenta la perdida de señal de los Access Point. Las siguientes figuras son la representación de los diferentes ambientes del edificio, mostrando la distribución, cobertura e intensidad de señal inalámbrica de los equipos para cada ambiente. En el

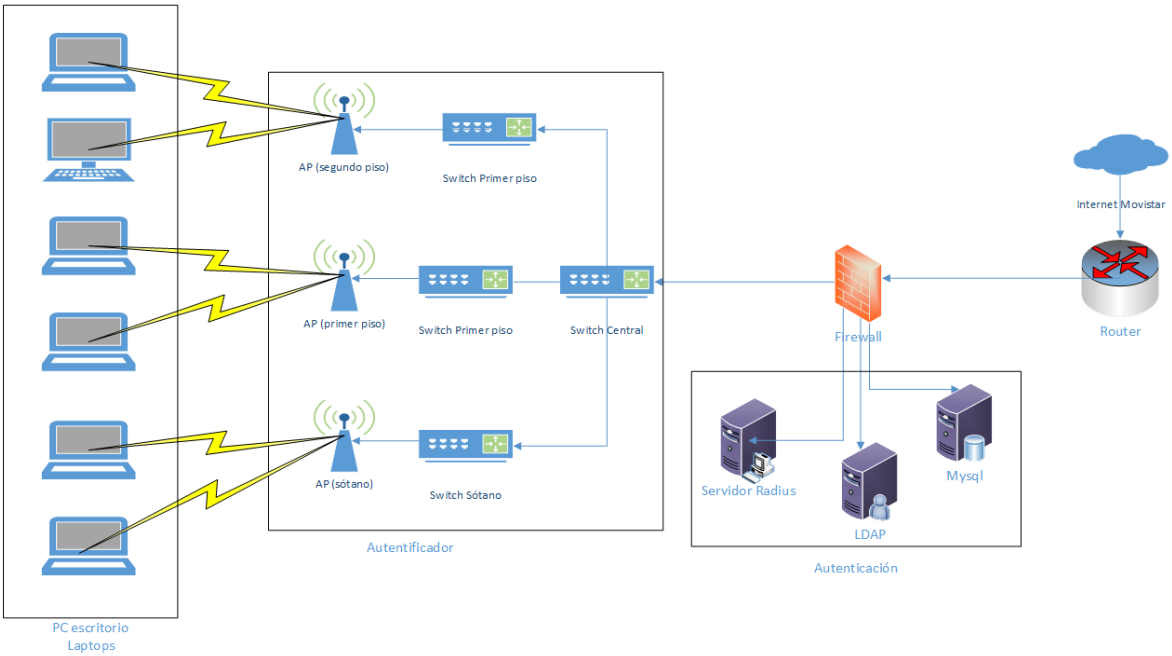
Anexo 4 se muestra el plano de la infraestructura del primer piso de la zona A con la distribución de los Access Point, indicando la intensidad de señal y cobertura.

F. Arquitectura de la red

El tipo de arquitectura que se va emplear es a una red tipo campus, ya que posee múltiples capas antes que se conecte con el dispositivo final de red. Esto brinda la oportunidad de poder usar diferentes tipos de tecnologías en función al nivel al cual se desea configurar, contando con switches de alto rendimiento en la capa central, lo cual brindara a la capa de acceso una gran facilidad a la hora de utilizarlos switches con menor nivel de complejidad, como también el uso de un Wireless LAN Controller con el cual se va gestionar todos los access point de manera centralizada aplicando todas las configuraciones requeridas en este y no de manera individual.

Para este caso en particular la arquitectura que se va emplear va una donde los dispositivos finales se van a comunicar a través de los access point y solo los equipos que no puedan contar con una tarjeta inalámbrica se van a comunicarse de manera directa con los switches, los cuales van a conectarse a los switches centrales de la oficina de tecnologías de información.

Figura 17: Diseño de la arquitectura de la red



Fuente: Elaboración propia

G. Análisis de costos

La cantidad de equipos que se emplearan para la realización de este proyecto son los siguientes:

Cuadro 22: Equipos requeridos en el diseño de red

Dispositivos	Cantidad
Access Point	24
Wireless LAN Controler	1
Tarjetas inalámbricas	28

Fuente: Elaboración propia

Cuadro 23: Costo de los equipos requeridos en el diseño de red

Dispositivo	Valor unitario	Valor total
Access Point	S/. 226,78	S/. 5.442,72
Wireless LAN Controler	S/. 1.009,52	S/. 1.009,52
Tarjetas inalámbricas	S/. 62,18	S/. 1.741,04
Total		S/. 8.193,28

Fuente: Elaboración propia

El presupuesto anual que el estado le asigna a la institución para el mantenimiento de LAN es de S/ 1.500,00; de los cuales se emplea para las diferentes áreas para la resolución de inconvenientes, atención de necesidades y problemas de conexión.

En el flujo de caja se va considerar principalmente el ahorro que se va tener por el costo de mantenimiento, como uno de los ingresos de valores para la implementación de este proyecto

Para el coste de mantenimiento de la nueva estructura de red WLAN se ha tomado en consideración posibles averías que pueden presentar los diferentes equipos de la red WLAN. La municipalidad cuenta con área especializada, los cuales se tendrán que encargar de controlar el buen estado de la señal inalámbrica en los diferentes ambientes de la Municipalidad Provincial de Carhuaz, así como también del mantenimiento y el posible cambio de equipos. Este beneficio va significar un ahorro sustancial a la institución respecto al costo de mano de obra elevado que se podría generar en un agente externo.

Cuadro 24: Análisis de costo beneficio

Flujo de caja	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**
Detalle de ingresos					
Capital	8.500,00				
Presupuesto de Mantenimiento		1.500,00	1.500,00	1.500,00	1.500,00
Total de Ingresos	8.200,00	1.500,00	1.500,00	1.500,00	1.500,00
Costo de Implementación	8.200,00				
Costo de Mantenimiento		250,00	250,00	500,00	250,00
Total de Egresos	8.200,00	250,00	250,00	500,00	250,00
Saldo Neto	300,00	1.250,00	1.250,00	1.000,00	1.250,00
Saldo Acumulado	300,00	1.550,00	2.800,00	3.800,00	5.050,00

Fuente: Elaboración propia

En el análisis costo beneficio se indican los beneficios que la institución puede obtener con la implementación de este proyecto, ya sea en el aspecto económico como también a nivel laboral.

En el aspecto económico el ahorro que se va experimentar por concepto de mantenimiento de la red es sustancial, pudiendo llegar a un ahorro aproximado del 600 %, teniendo como referencia que existen periodos que en los cuales el costo por concepto de mantenimiento de la red la sobrepasado el valor del presupuesto anual.

Cuadro 25: Análisis económico de la inversión

Periodo	Costo Estimado Mantenimiento Red WLAN	Costo Presupuestado Mantenimiento Red LAN
Año 1	250,00	1500,00
Año 2	250,00	1500,00
Año 3	500,00	1500,00
Año 4	250,00	1500,00

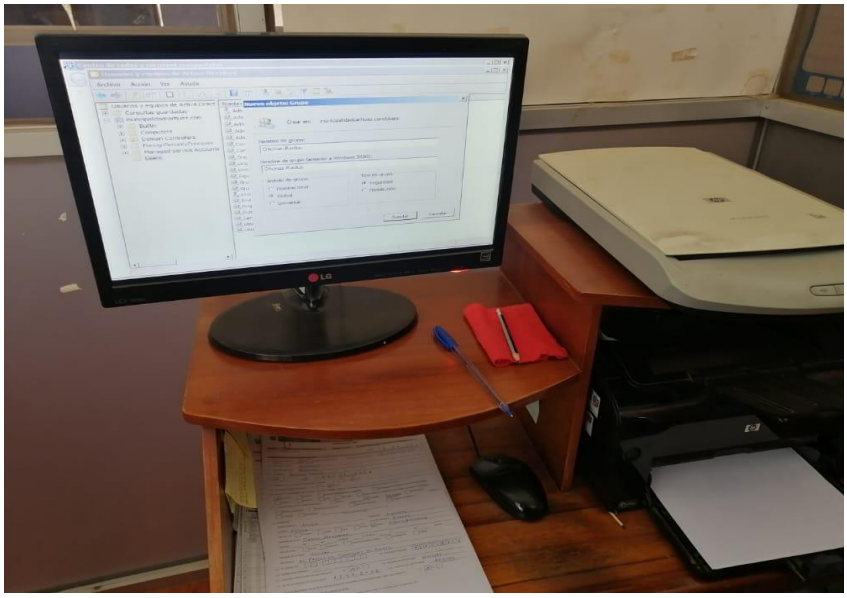
Fuente: Elaboración propia

Respecto a la parte laboral los trabajadores administrativos van a poder acceder a la red desde cualquier ubicación que se encuentren, sin tener la imperiosa necesidad de conectarse mediante un cable de red, entre otros múltiples beneficios. Esto tendrá como mayor ventaja el poder acceder a la información en tiempo real.

4.1.3. Objetivo específico 3: Implementación del sistema de seguridad de redes

La implementación del sistema de seguridad de redes basado en el protocolo RADIUS inició en el mes de agosto del 2021 mediante la autorización de las autoridades pertinentes, a medianos del mes de agosto se realizó el acercamiento a las instalaciones de acuerdo a lo constatado en el Anexo 8.

Figura 18: Inicio de la instalación del Servidor RADIUS

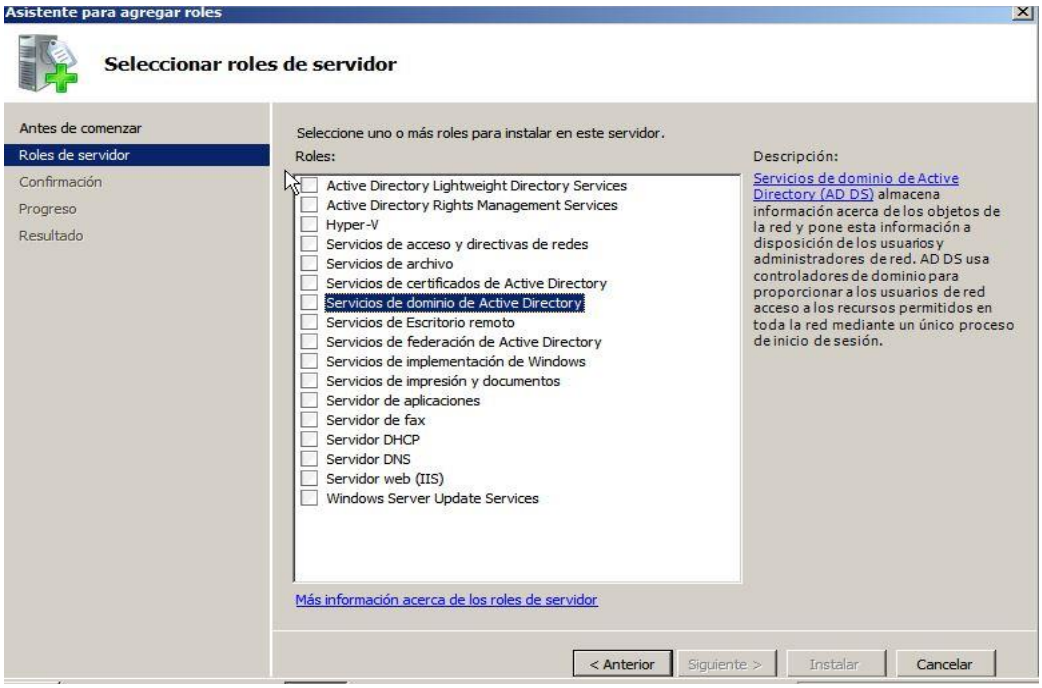


Fuente: Elaboración propia

Se procedió a configurar los siguientes puntos y se podrá visualizar en las figuras, que rol o que la actividad se realizó, el servidor en el que se implementó fue el servidor principal cuyo sistema operativo es Windows Server 2008.

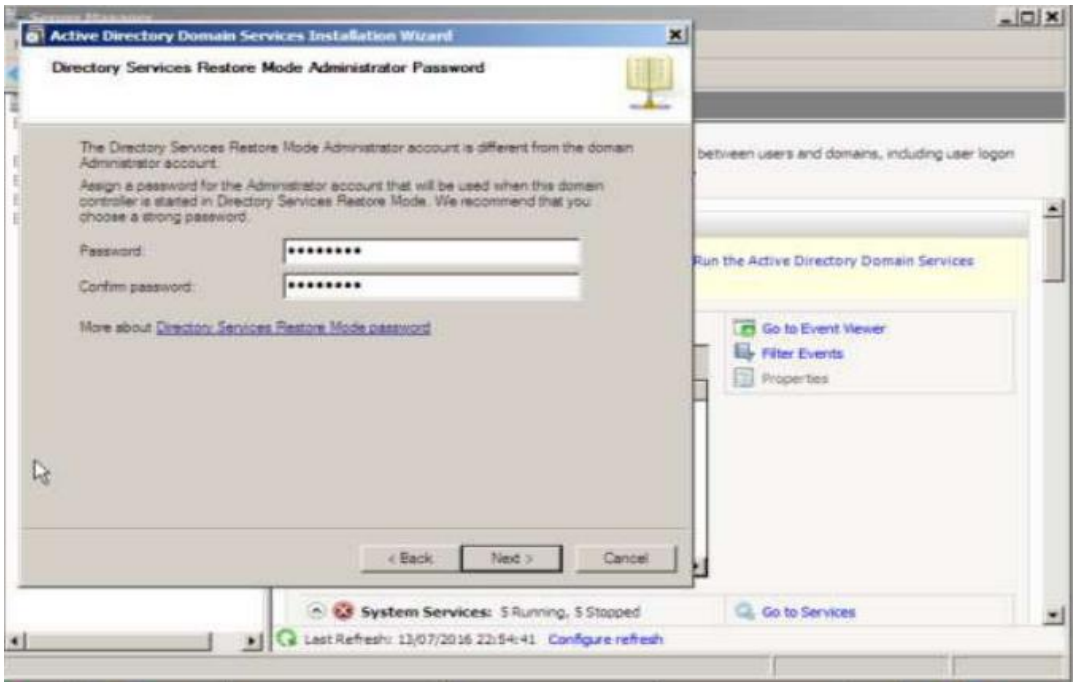
Dentro del Sistema Operativo Windows Server 2008 R2 primero se configuró el controlador del servidor de dominio, agregando el rol de Active Directory Domain Services, para lo cual se procedió con la instalación del Active Directory Domain Services Installation Wizard, se creó un nuevo dominio para el árbol y se asignó una contraseña de administrador.

Figura 19: Configuración del Servidor Radius



Fuente: Elaboración propia

Figura 20: Creación de usuario administrador en el Servidor Radius

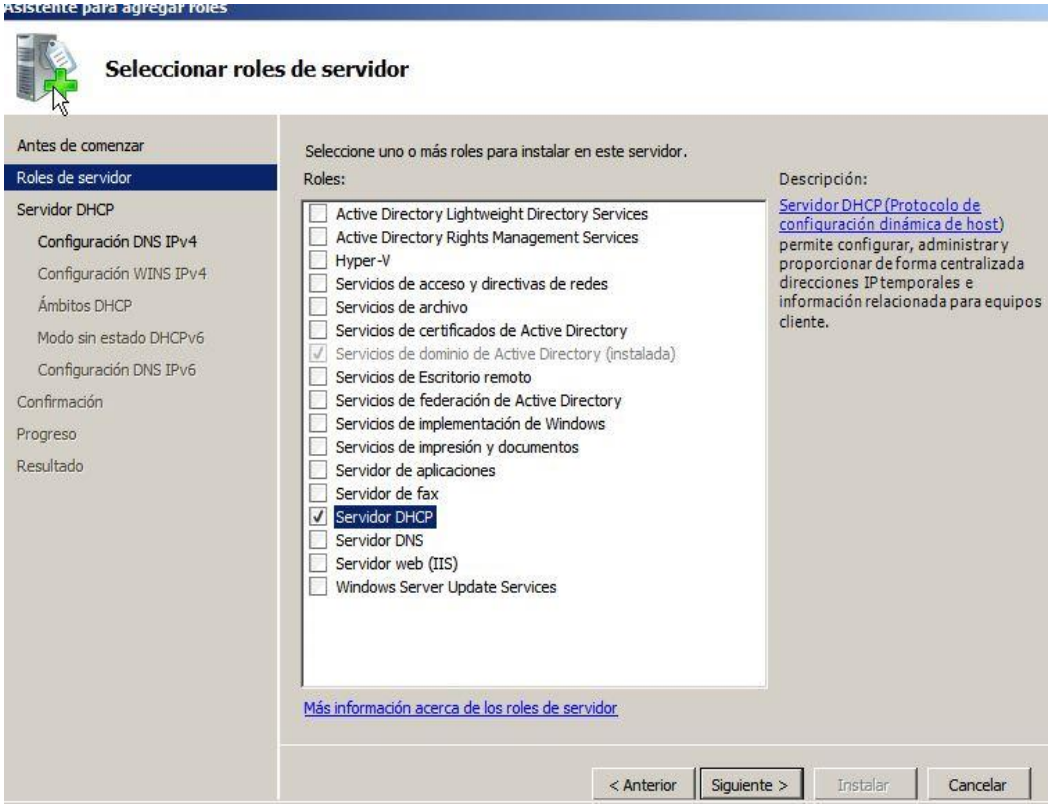


Fuente: Elaboración propia

Posteriormente e instaló y configuraron los servicios DHCP, añadiendo el rol DHCP Server, luego la respectiva configuración del servidor DHCP que establecieron direcciones IP al cliente, se indicó que no se necesita el Windows Internet Naming

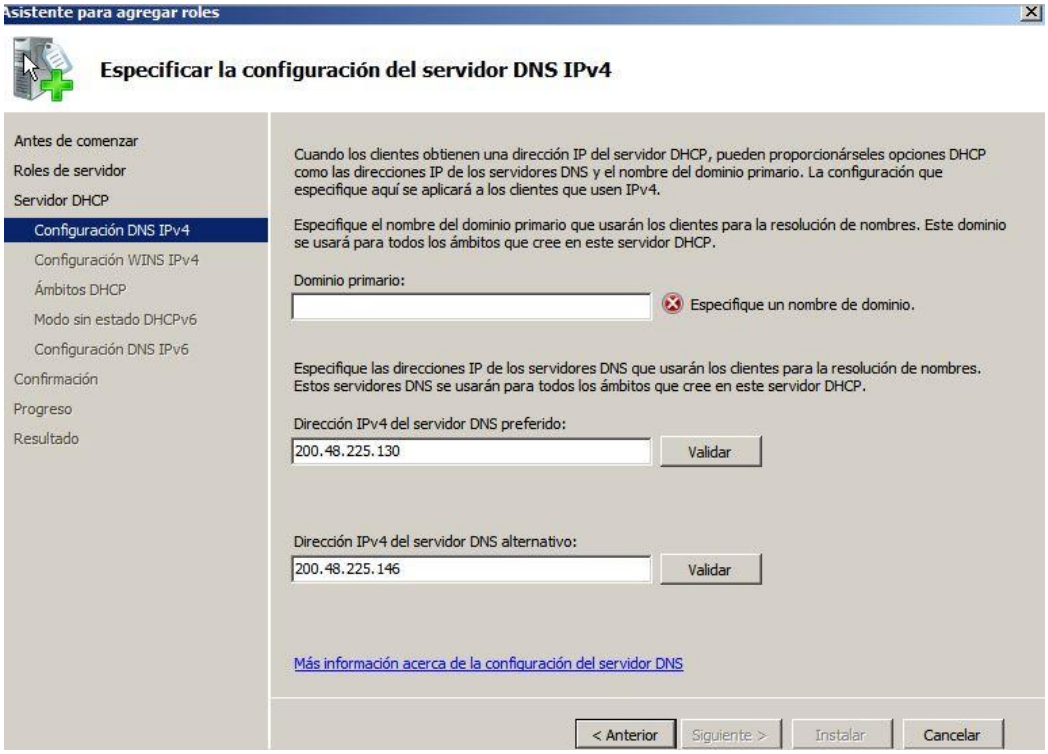
Service – WINS para esta red, se habilitó el DHCPv4 modo estático para este servidor, se configuró el IPv4 DNS, se autorizó el certificado del dominio administrador del servidor DHCP en el Active Directory y se finalizó la instalación.

Figura 21: Creación del servidor DHCP



Fuente: Elaboración propia

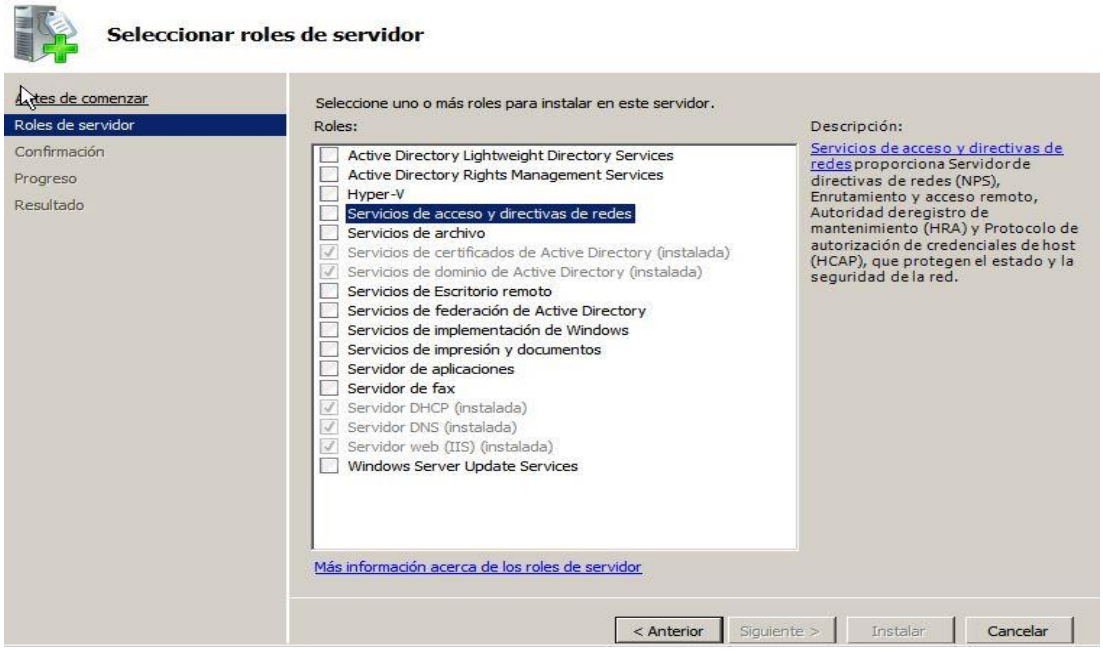
Figura 22: Instalación del servidor DNS



Fuente: Elaboración propia

Se instaló y configuró en el servidor los certificados de autenticación del servidor, teniendo en cuenta que el certificado del servidor debe ser emitido por la entidad de certificación publica que sea de confianza para el equipo cliente, debe existir dentro de la carpeta de certificación raíz de confianza del almacén de certificados de equipo cliente; dando inicio agregando el rol de Active Directory Certificate Services (Ver figura 22), se seleccionó el certificado de autorización que es usado para emitir y gestionar certificados, donde se especificó que el tipo de certificado que se tiene que usar es Enterprise dado que el CA utiliza los datos del Active Directory, se seleccionó el Root CA porque va hacer la primera y la única autoridad de certificación en una infraestructura de clave pública (Ver figura 22), se creó una clave privada, se configura la criptografía del Certificado de Autorización, por default se dejó el nombre del certificado, se indicó el periodo de validez del certificado, por default se dejó la ubicación de la base de datos donde se almacenara el CA y se finalizó con la instalación del certificado de autorización.

Figura 23: Configuración de los roles del servidor

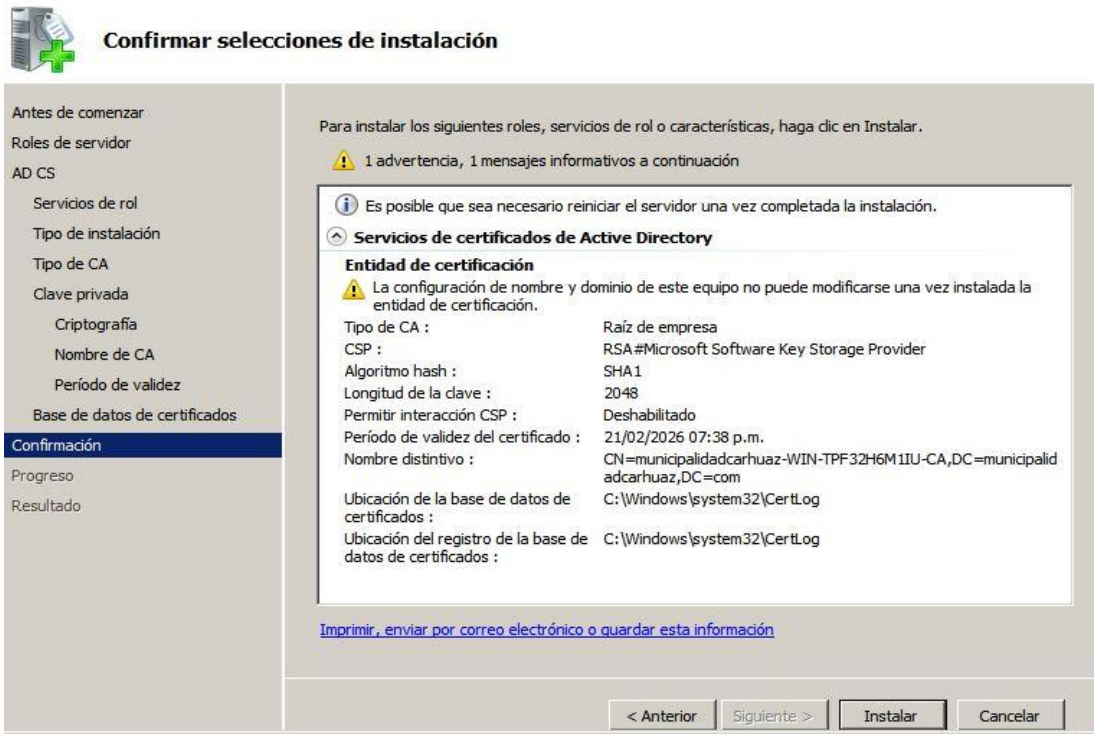


Fuente: Elaboración propia

Luego conectar e ingresar a los usuarios al dominio se agregó certificado en la cuenta del equipo local. Seguidamente instalar el Network Policy Server (NPS) que es usado en el servidor RADIUS para autenticar a los clientes Wireless con la autenticación PEAP, se agregó el rol Network Policy and Access Services, se agregó el Network Policy Server y el Routing and Remote Access Services y se instaló.

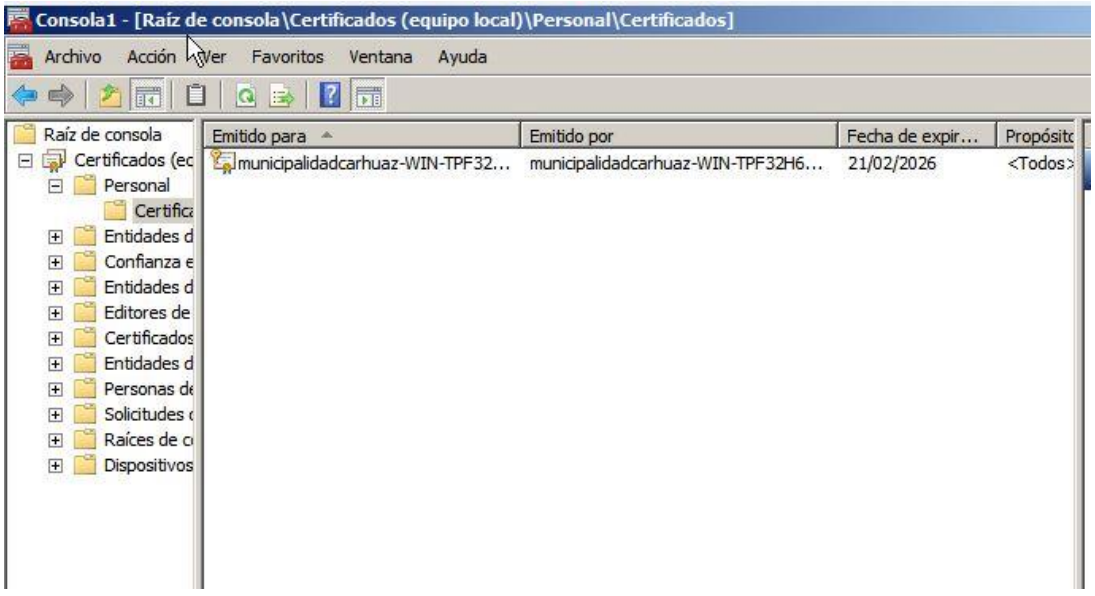
Se agregaron los certificados en la cuenta de la computadora local, en los certificados de la computadora local que se encuentra en Microsoft Management Console (MMC), dentro de la carpeta Personal se encuentra la carpeta certificada, en la cual se crea el certificado Domain Controller.

Figura 24: Adición de los certificados de seguridad



Fuente: Elaboración propia

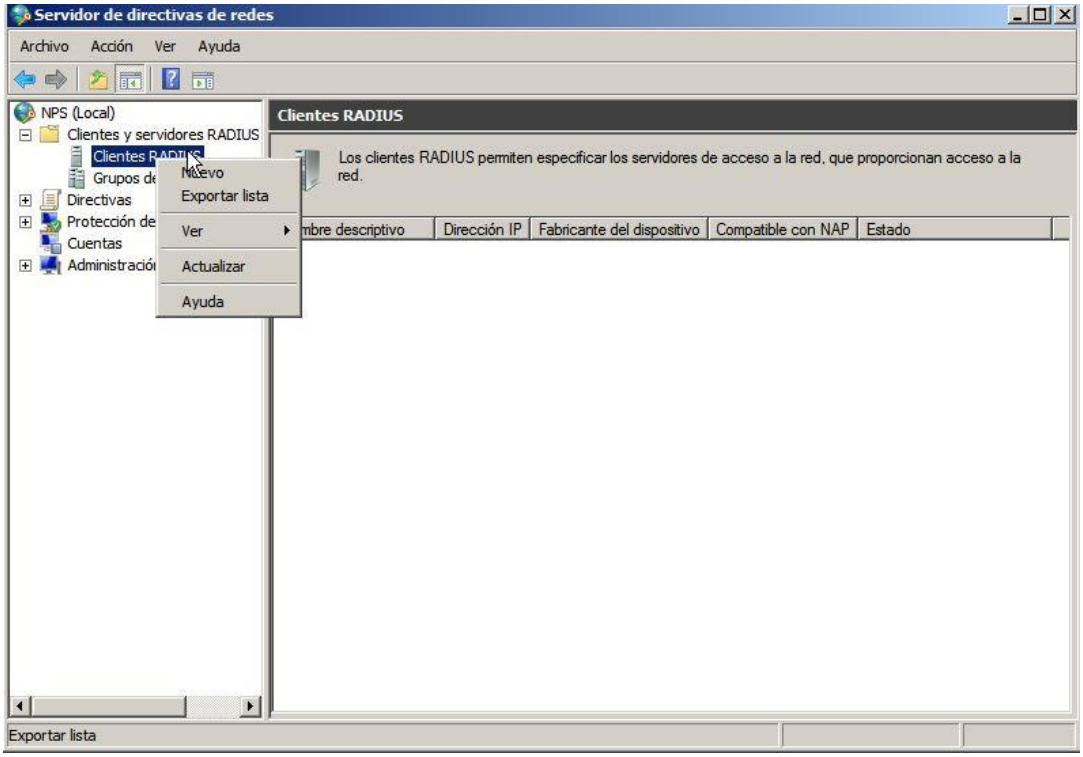
Figura 25: Vista de los certificados instalados



Fuente: Elaboración propia

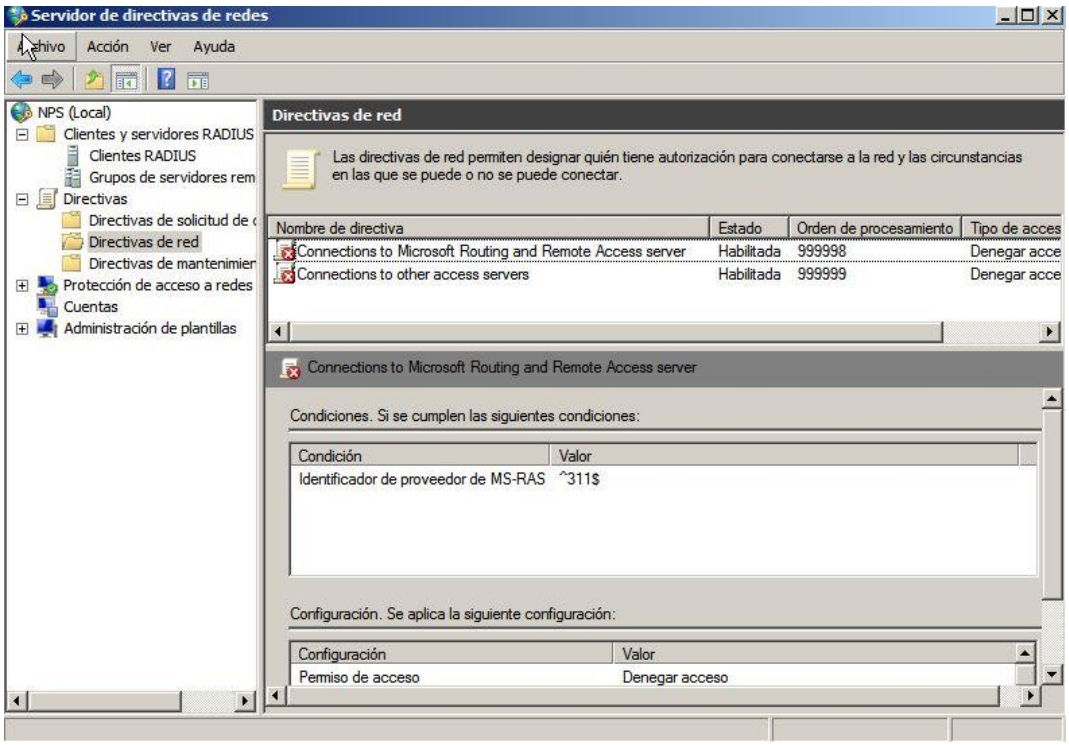
Se registró el NPS en el Active Directory, se añade la Wireless LAN Controller como cliente en el NPS, políticas de red Wireless para los usuarios, se agregaron las políticas de red y se configuró el método de autenticación agregando el Microsoft Protected EAP (PEAP).

Figura 26: Registro de NPS



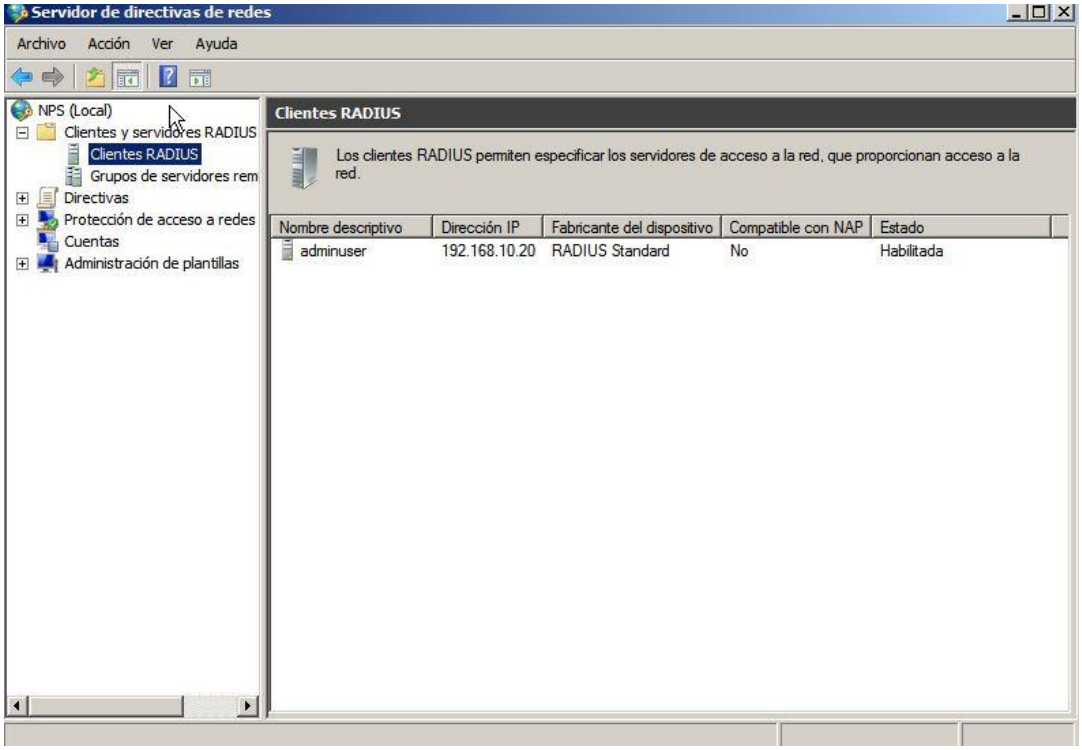
Fuente: Elaboración propia

Figura 27: Configuración de políticas de seguridad



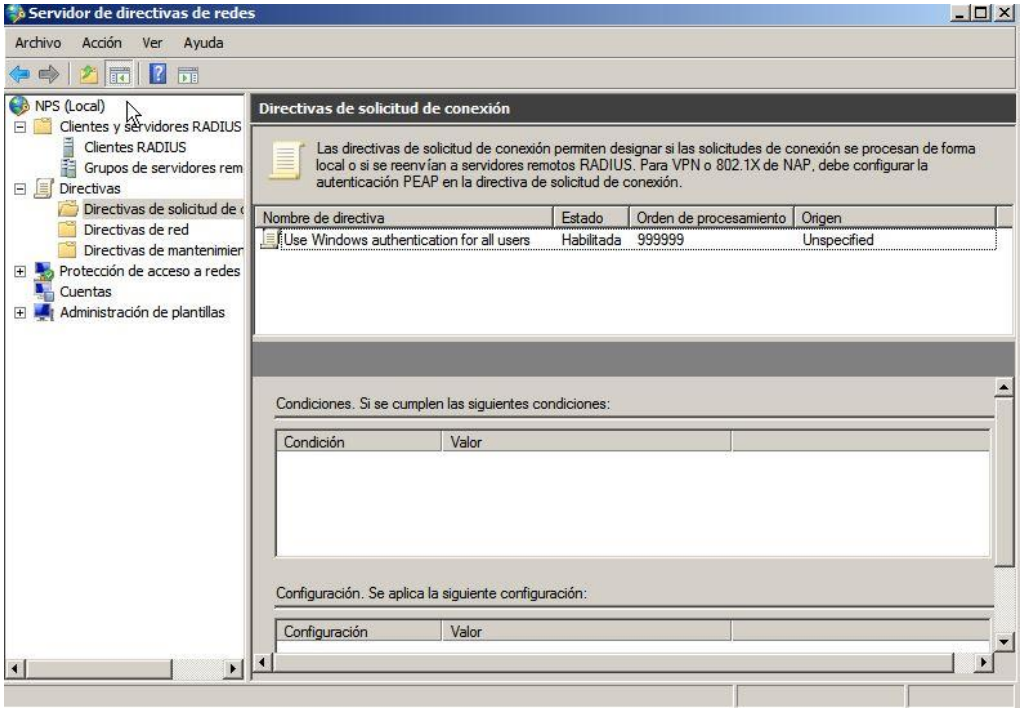
Fuente: Elaboración propia

Figura 28: Creación del Servidor Radius



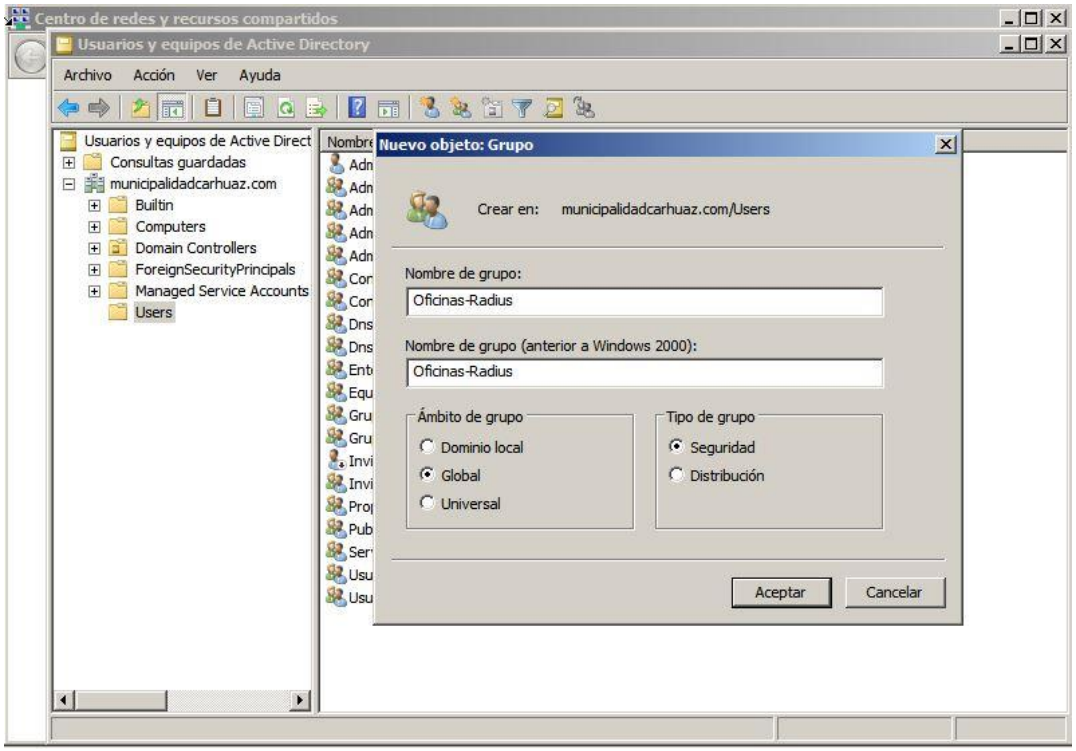
Fuente: Elaboración propia

Figura 29: Importación de las políticas de seguridad al servidor Radius



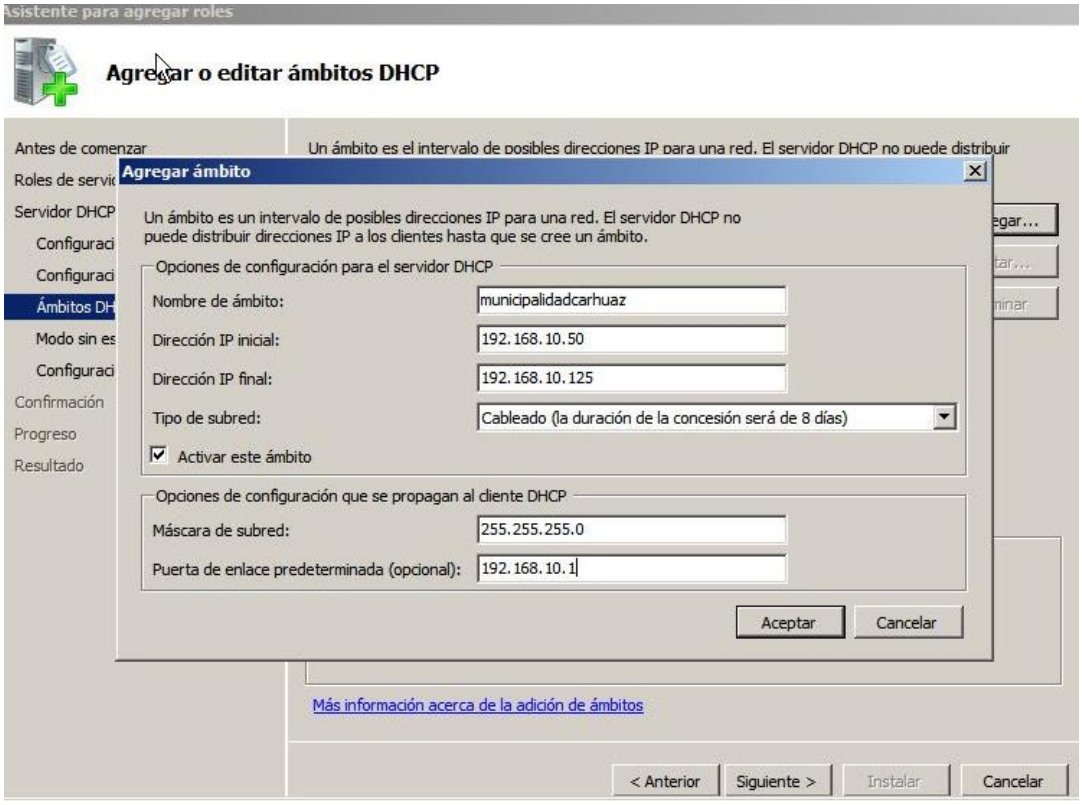
Fuente: Elaboración propia

Figura 30: Creación de grupos en Radius



Fuente: Elaboración propia

Figura 31: Creación del ámbito para las políticas del protocolo Radius

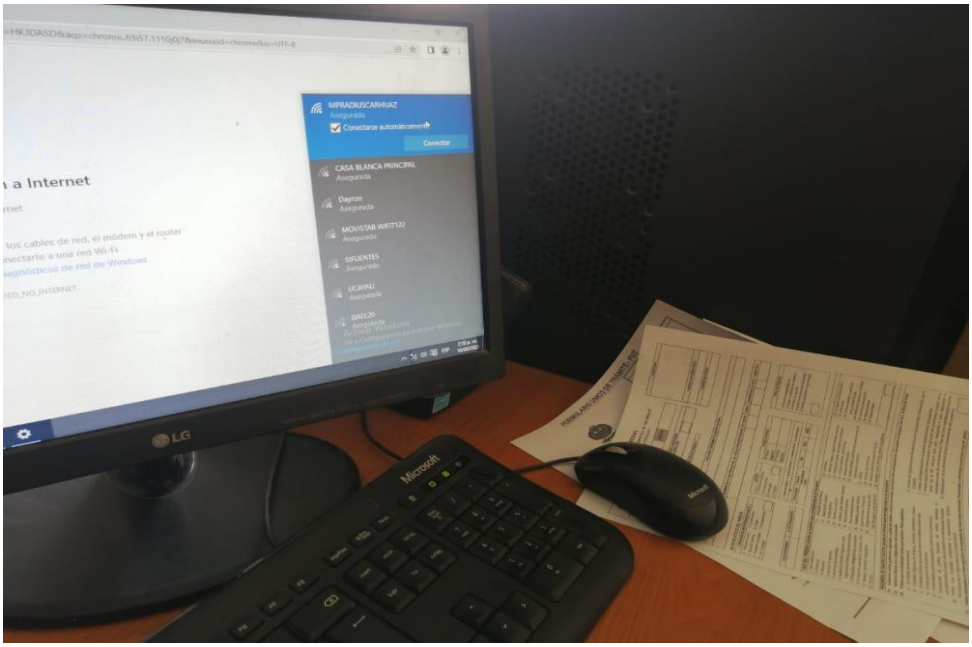


Fuente: Elaboración propia

Se puede visualizar que dentro de la aplicación se visualiza el nombre de los equipos que cumplen con los parámetros que se tiene para identificar las funciones que cumple cada una de los equipos registrados en el aplicativo antes mencionado, por esta razón se ha trabajado en conjunto con el jefe de infraestructura tecnológica (Departamento de Redes), de modo que se culmina demostrando que dicho servidor queda instalado y operativo en el municipio.

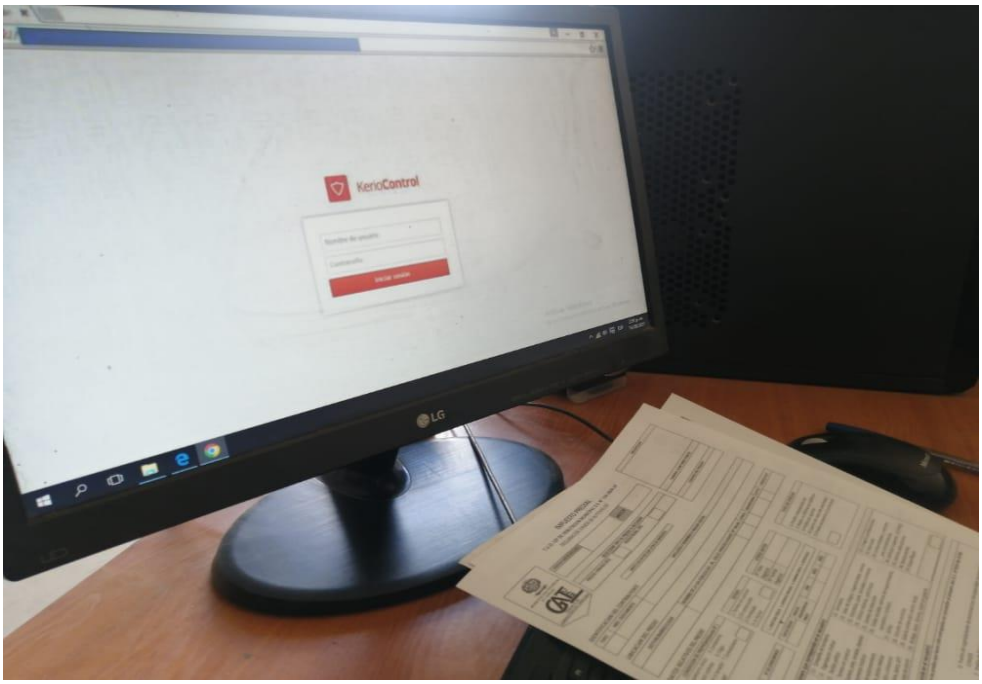
Posterior a ello se simuló una conexión para las pruebas, siendo la prueba con el usuario pruebaCarhuaz el mismo que se pudo conectar desde la computadora de escritorio al Access Point con el SSID 'MPRADIUSCARHUAZ', en la figura se puede observar la intensidad de la señal, el tipo de seguridad y tipo de radio del Access Point conectado y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al Internet.

Figura 32: Lista de redes disponibles en la prueba



Fuente: Elaboración propia

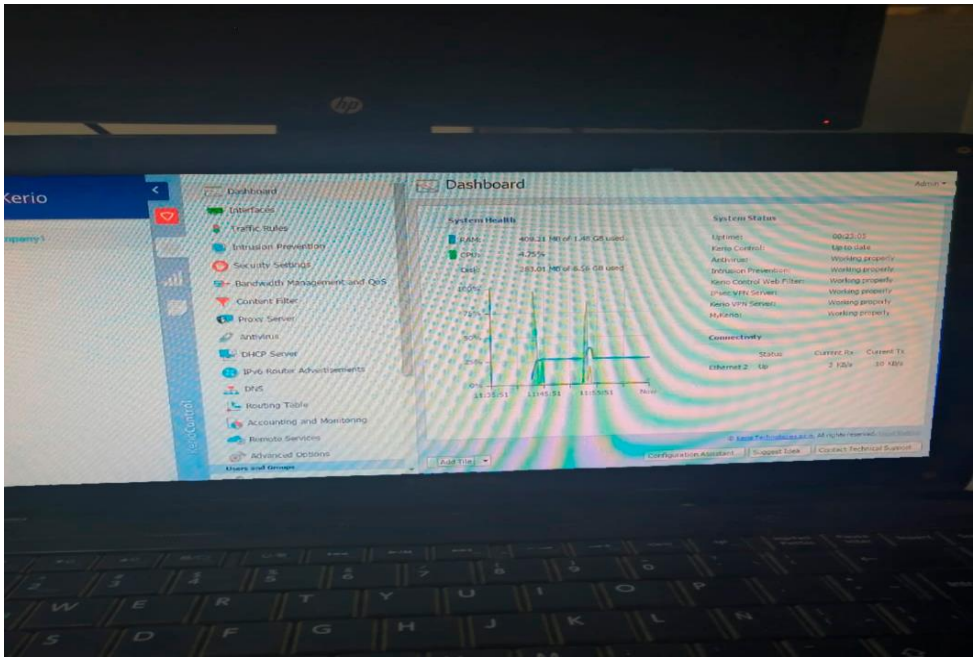
Figura 33: Interfaz de acceso a la red



Fuente: Elaboración propia

En el Kerio Control Centro se puede visualizar cuantos equipos se han inicializado la sesión con la cuenta de pruebaCarhuaz y las estadísticas del usuario.

Figura 34: Vista de administrador de la red



Fuente: Elaboración propia

Figura 35: Administración de usuarios en la red

Fuente: Elaboración propia

Posterior a la implementación del sistema de seguridad de redes bajo el protocolo RADIUS se procedió a la capacitación de los usuarios en cuanto al sistema de uso de seguridad.

Figura 36: Capacitación de usuarios del sistema de seguridad

Fuente: Elaboración propia

En cuanto al procedimiento para el acceso a la red de datos se indicó a los usuarios que deben de ingresar el usuario y la clave de acuerdo a la lista especificada en la figura 19, en la que se crean los usuarios de RADIUS.

Posteriormente a la implementación se comenzó a realizó un cambio en la red para dejar de utilizar el cableado estructurado y explotar más las redes inalámbricas debido a que ahora la red es segura por el uso de RADIUS

4.1.4. Objetivo específico 4: Evaluación del sistema de seguridad de redes

Pasados tres meses a la implementación del sistema de seguridad de redes basado en el protocolo RADIUS se realizó la evaluación del nivel de satisfacción de la administración de acceso a la red mediante la aplicación del cuestionario de administración de la red sobre la muestra del pre test con el fin de determinar el cambio en el grado de satisfacción. Tras el procesamiento de los datos recolectados con los baremos establecidos en el punto 4.1. los resultados hallados fueron:

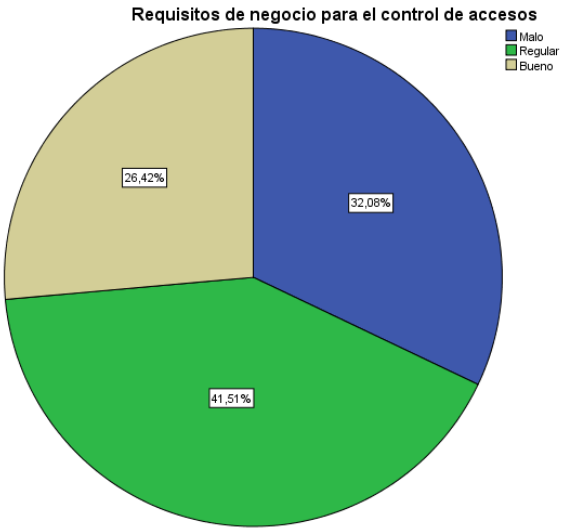
En lo que respecta a la dimensión requisitos de negocio para el control de acceso se hallaron los siguientes resultados:

Cuadro 26: Calificación de los requisitos de negocio para el control de acceso

	Frecuencia	Porcentaje
Bueno	14	32,1%
Regular	22	41,5%
Malo	17	26,4%

Fuente: Elaboración propia

Figura 37: Calificación de la dimensión requisitos de negocio para el control de accesos



Fuente: Elaboración propia

En el cuadro 26 y figura 34 se observa que la mayoría de encuestados, representados por el 41,5% del total califican a los requisitos de negocio para el control de accesos de la administración de acceso a la red como regular, seguidamente un 26,4% la califican como malo y finalmente un 32,1% lo califican como bueno.

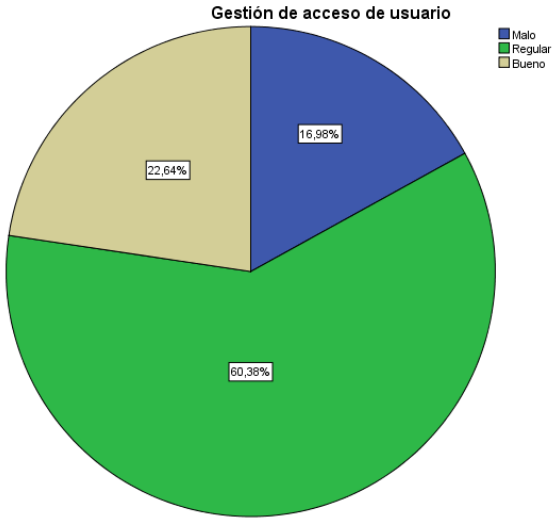
En lo que respecta a la dimensión gestión de acceso de usuario se hallaron los siguientes resultados:

Cuadro 27: Calificación de la gestión de acceso de usuario

	Frecuencia	**Porcentaje**
Bueno	12	22,6%
Regular	32	60,4%
Malo	9	17,0%

Fuente: Elaboración propia

Figura 38: Calificación de la dimensión gestión de acceso de usuario



Fuente: Elaboración propia

En el cuadro 27 y figura 35 se observa que la mayoría de encuestados, representados por el 60,4% del total califican a la gestión de acceso de usuario de la administración de acceso a la red como regular, seguidamente un 22,6% la califican como buena y finalmente un 17,0% lo califican como mala.

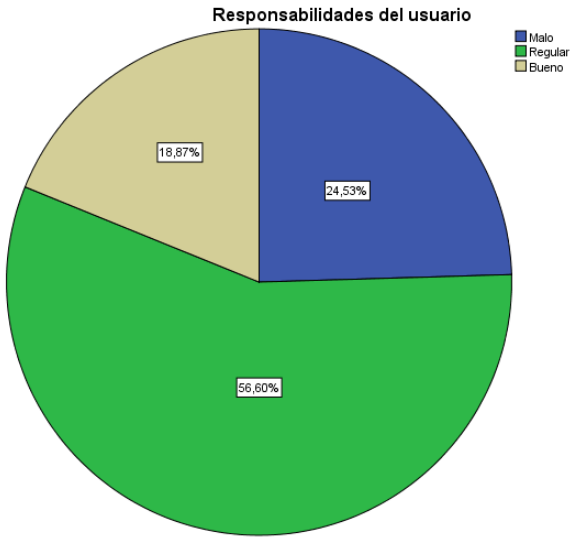
En lo que respecta a la dimensión responsabilidades del usuario se hallaron los siguientes resultados:

Cuadro 28: Calificación de las responsabilidades del usuario

	Frecuencia	Porcentaje
Bueno	10	18,9%
Regular	30	56,6%
Malo	13	24,5%

Fuente: Elaboración propia

Figura 39: Calificación de la dimensión responsabilidades del usuario



Fuente: Elaboración propia

En el cuadro 28 y figura 36 se observa que la mayoría de encuestados, representados por el 56,6% del total califican a las responsabilidades del usuario en la administración del acceso a la red como regular, mientras que el 24,5% lo califican como mala y finalmente un 18,9% lo califican como buena.

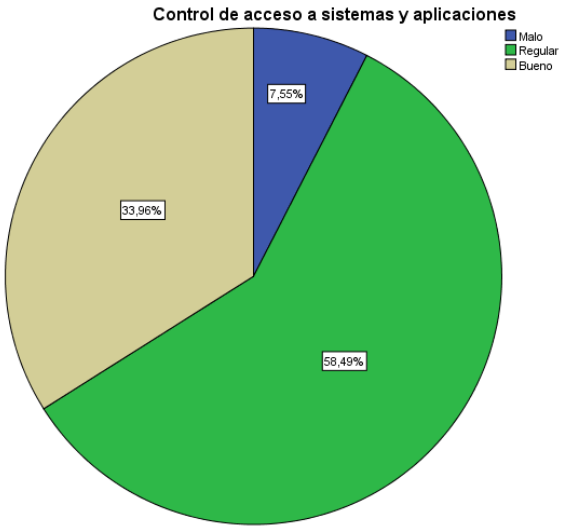
En lo que respecta a la dimensión control de acceso a sistemas y aplicaciones se hallaron los siguientes resultados:

Cuadro 29: Calificación del control de acceso a sistemas y aplicaciones

	Frecuencia	Porcentaje
Bueno	18	34,0%
Regular	31	58,5%
Malo	4	7,5%

Fuente: Elaboración propia

Figura 40: Calificación de la dimensión control de acceso a sistemas y aplicaciones



Fuente: Elaboración propia

En el cuadro 29 y figura 37 se observa que la mayoría de encuestados, representados por el 58,5% del total califican al control de acceso a sistemas y aplicaciones en la administración del acceso a la red como regular, seguidamente el 34,0% la califican como buena y finalmente un 7,5% lo califican como mala.

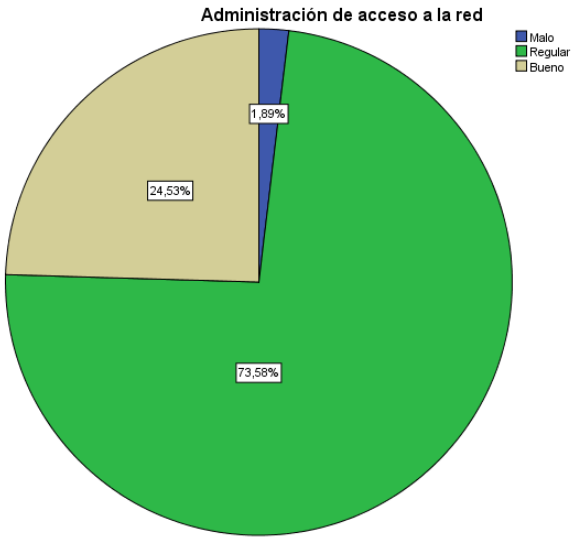
En cuanto al estudio de la variable administración de acceso a la red se hallaron los siguientes resultados:

Cuadro 30: Calificación de la administración de acceso a la red

	Frecuencia	Porcentaje
Bueno	13	24,5%
Regular	39	73,6%
Malo	1	1,9%

Fuente: Elaboración propia

Figura 41: Calificación de la variable administración de acceso a la red



Fuente: Elaboración propia

En el cuadro 30 y figura 38 se observa que la mayoría de encuestados, representados por el 73,6% del total califican a la administración del acceso a la red como regular, seguidamente el 24,5% la califican como buena y finalmente un 1,9% lo califican como mala.

4.2. Prueba de hipótesis

4.2.1. Contrastación de hipótesis general

Para la contrastación de la hipótesis general que indica que el diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019, se realizó una comparación entre los resultados hallados en el pre test y post test permitiendo determinar el cambio en cuanto a la percepción de la mejora en la administración de accesos a la red.

De acuerdo a los datos recolectados del pre test (Apartado 4.1.1) y el pos test (Apartado 4.1.4) se realizó la aplicación de estadísticos, los cual sirvió de contrastar la hipótesis planteada en la investigación, hallándose:

Cuadro 31 Estadísticos descriptivos de la administración de acceso a la red

Variable	Estadístico		Valor	Error estándar
Administración de acceso a la red Pre test	Media		66,49	1,812
	95% de intervalo de confianza para la media	Límite inferior	62,85	
		Límite superior	70,13	
	Media recortada al 5%		65,54	
	Mediana		61,00	
	Varianza		174,024	
	Desviación estándar		13,192	
Administración de acceso a la red Post test	Media		92,85	2,187
	95% de intervalo de confianza para la media	Límite inferior	88,46	
		Límite superior	97,24	
	Media recortada al 5%		92,64	
	Mediana		87,00	
	Varianza		253,477	
	Desviación estándar		15,921	

Fuente: SPSS v. 23

En el cuadro del análisis descriptivo de la variable dependiente administración de acceso a la red, se puede observar que antes de la implementación del sistema de seguridad de redes basado en el protocolo RADIUS, se tenía una Media de 66,49 a viéndose un incremento al 92,85 tras su implementación.

Para la contrastación de la hipótesis de la investigación se establecen la hipótesis alterna y la hipótesis nula, siendo estos:

H_0: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS no mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

H_1: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

Para lograr contrastar la hipótesis general, es necesario determinar si los datos que corresponden a las series de la administración de acceso a la red antes y después tienen un comportamiento paramétrico, para tal fin y en vista que las series de ambos datos son en cantidad mayor a 30, se procederá al análisis de normalidad mediante el estadígrafo de Kolmorov – Smirnov de acuerdo a la regla de decisión:

$$Si\ p_{valor} \leq 0{,}05\ los\ datos\ tienen\ un\ comportamiento\ no\ paramétrico$$

$$Si\ p_{valor} \geq 0{,}05\ los\ datos\ tienen\ un\ comportamiento\ paramétrico$$

Cuadro 32 Prueba de normalidad de la administración de acceso a la red

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Administración de acceso a la red Pre test	,190	53	,000
Administración de acceso a la red Pos test	,153	53	,003

Fuente: SPSS v. 23

Del cuadro 32 se puede verificar que la significancia de las pruebas pre y pos test de la administración de acceso a la red, tienen valores menores a 0.05, por consiguiente y de acuerdo a la regla de decisión, queda demostrado que tienen comportamientos no paramétricos. Dado que lo que se quiere es saber si la administración de acceso a la red ha mejorado, se procederá al análisis con el estadígrafo de Wilcoxon para muestras relacionadas en la contrastación de la hipótesis.

H_0: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS no mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

H_1: El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

Para ello se aplicará la regla de decisión:

$$Si\ p_{valor} \leq 0{,}05\ se\ rechaza\ H_0 \text{ y se acepta } H_1$$

$$Si\ p_{valor} > 0{,}05\ no\ se\ rechaza\ H_0 \text{ y se acepta } H_1$$

Tras el análisis estadístico para la prueba Wilcoxon para muestras relacionadas se muestra en las tablas presentadas a continuación:

Cuadro 33 Datos descriptivos de la prueba de Wilconxon

		N	Rango promedio	Suma de rangos
Post test – Pretest	Rangos negativos	0[a]	26,50	1378,00
	Rangos positivos	52[b]	,00	,00
	Empates	1[c]		
	Total	53		

a. Post test < Pretest
b. Post test > Pretest
c. Post test = Pretest

Fuente: SPSS V.23

Del cuadro la cuadro 33 se puede observar que la calificación de la administración de acceso a la red “después” (Pos test) en la mayoría de casos (52) cuenta con un valor mayor a la calificación de la administración de acceso a la red “antes” (Pre test), por consiguiente, según la regla de decisión se acepta la hipótesis alterna siendo rechazada la hipótesis nula.

A fin de confirmar que el análisis es el correcto, se procede al análisis mediante el p valor o significancia de los resultados de la aplicación de la prueba de Wilcoxon para muestras relacionadas.

Cuadro 34 Resultados de la prueba de Wilcoxon para muestras relacionadas

	Post test - Pretest
Z	6,276[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Fuente: SPSS V.23

De acuerdo a los datos expresados en el cuadro 32 se puede afirmar que la significancia que es de 0,000 es menor que 0,05, por lo cual se reafirma la aceptación de la hipótesis alterna y se niega la hipótesis nula, quedando demostrado estadísticamente que el diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.

4.2.2. Contrastación de hipótesis específicas

En cuanto a la primera hipótesis específica que indica que: Existe una deficiente administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz, se evidenció que 64,1% calificó la administración de acceso a la red anterior como malo, lo cual fue evidenciado y detallado de manera más profunda en la presentación de los resultados expuestos en el punto 4.1.1., dándose así contrastada la hipótesis específica.

La segunda hipótesis específica indica que: Se realizó el desarrollo del sistema de seguridad de redes basado en el protocolo RADIUS para la mejora del control de accesos; es en tal sentido que en el punto 4.1.2 se detalló el procedimiento de diseño

de la red de datos basado en el protocolo RADIUS partiendo del diagnóstico y la recolección de requerimientos hasta concluir con el diseño físico y de arquitectura de la red, es mediante este procedimiento que se descarta la hipótesis nula en la que se sostiene que no se logró con el diseño quedando aceptada la segunda hipótesis específica.

La tercera hipótesis específica sostiene que: Se implementó el sistema de seguridad de redes basado en el protocolo RADIUS para la mejora de la gestión de acceso de usuarios. Dicho procedimiento fue detallado en el punto 4.1.3 en el cual se presentaron capturas de pantalla del procedimiento efectuado para implementar el sistema en la Municipalidad Provincial de Carhuaz, el cual fue desarrollado de manera exitosa lo cual es evidenciado en los Anexos 5, 6 y 7. Es en tal sentido que es posible descartar la hipótesis nula quedando aceptada la hipótesis alterna.

Finalmente, El sistema de seguridad de redes basado en el protocolo RADIUS influye positiva y significativamente sobre la mejora del control de acceso a sistemas y aplicaciones, se evidenció que **e**l funcionamiento del sistema de seguridad de redes basado en el protocolo RADIUS mejora notablemente la administración de accesos a la red en la Municipalidad Provincial de Carhuaz; la cual fue contrastada en la presentación de los resultados del post test en la que se observa el incremento en la satisfacción de la administración de accesos teniéndose un 73,6% que la califican como regular y un 24,5% que la califican como buena.

4.3. Discusión de resultados

En lo que respecta al objetivo general de desarrollar el sistema de seguridad para la administración de accesos a la red usando el protocolo RADIUS en la Municipalidad Provincial de Carhuaz, se procedió inicialmente con el análisis del desempeño de la

administración de acceso a la Red que venía funcionado (pre test), posteriormente se realizó la recolección de requerimientos, diseño e implementación del sistema, luego de ello se realizó la recolección de datos de la administración de acceso a la red actual (post test) para determinar la existencia de una mejora siendo que, de acuerdo a la aplicación de la prueba de Wilcoxon para muestras relacionadas existe una diferencia significativa (p – valor = 0,000 < 0,05) y positiva (Z = 6,276) en la administración de acceso a la red tras la implementación del sistema de seguridad utilizando el protocolo RADIUS, dándose conformidad a los requerimientos establecidos en la presente investigación.

Los resultados hallados coinciden con los hallados por Tobar y Mora (2016), quienes en su investigación refieren que la construcción del diseño propuesto realizado en su tesis va acorde a las necesidades de brindar cobertura a los sitios remotos garantizando autentificación y control en el acceso inalámbrico a los recursos de red. A su vez el proyecto de implementación resultó más económico para el Gobierno Provincial de Guayas que cubrió con los gatos de implementación. A su vez los resultados hallados guardan coherencia con la investigación de Espinoza (2018), quien en sus conclusiones señala que el servidor RADIUS ha mostrado ser un mecanismo de protección y salvaguardo de información, empleando los estándares de seguridad, y juntamente a Eduroam brinda un valor agregado a la institución catalogándola como una institución de confianza a nivel internacional y a su vez los usuarios dispondrán de acceso a este servicio desde cualquier parte de la institución.

En lo concerniente a la teoría hallada en la presente investigación se tiene a la normativa ISO (2018), en la cual se especifica que la norma ISO 27001 indica que la administración de accesos a la red es la encargada del control de accesos para prevenir y no dejar entrar a las personas no autorizadas a través de controles los cuales podrán

registra y revocar permisos a los usuarios; así mismo Vinay (2015) menciona que el protocolo RADIUS, se encarga de la autentificación de los usuarios que se conectan remotamente a Internet mediante líneas conmutadas, además cuentan con el servicio de servicio de Autentificación, Autorización y Contabilidad (AAA), pudiendo ser empleado para trabajar en una red LAN, MAN o WAN.

En base a los datos expuestos en párrafos anteriores es posible vislumbrar una problemática en la Municipalidad Provincial de Carhuaz en lo que respecta a la administración de acceso a la red, siendo que muchos de los usuarios identifican que estos problemas son comunes en el municipio; es en base a ello que se realizó el diagnóstico a fin de identificar los requerimientos de la red actual y rescatar los puntos fuertes que tiene esta, teniéndose como resultado el diseño de la red planteada.

En cuanto al objetivo específico de Evaluar la administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz, 2019, se logró determinar que el 64,1% de los encuestados califican a la administración de acceso a la red de la red previa a la implementación del sistema como mala, mientras que el 34,0% indican que esta es regular y tan solo un 1,9% la califican como buena. Estos resultados guardan coherencia con los hallados por Ortega (2017) quien en su investigación manifiesta que el nivel de insatisfacción de los trabajadores en el pre test fue de 67,5% debido a que perciben que la red se encuentra poco disponible, vulnerable, con errores de transmisión y accesos limitados; en lo concerniente a la teoría hallada la revista Seguridad en América (2017) indica que los sistemas de seguridad deben de ir incorporando los cambios y avances tecnológicos para lograr mejorar su alcance y eficiencia, por ello es necesario que las entidades incorporen nuevas herramientas para la protección de datos, siendo el caso de la Municipalidad Provincial de Carhuaz uno de los casos donde no se realizaron cambios en el sistema de seguridad por lo cual la

seguridad en los últimos años ha ido quedando desfasada. De acuerdo a lo expuesto es posible afirmar que el sistema de seguridad de redes que venía funcionando en la Municipalidad Provincial de Carhuaz presentaba una serie de deficiencias en cuanto a la administración de acceso a la red, ello debido a la propia opinión de los colaboradores del municipio, quienes manifestaron problemas como la falta de políticas para el acceso a la red, la ausencia de credenciales o mecanismos de seguridad y la poca atención a la protección de información confidencial.

En relación al objetivo de desarrollar el sistema de seguridad de redes basado en el protocolo RADIUS para la mejora de la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019, se logró identificar que el sistema de seguridad para la administración de accesos requiere de una gestión de acceso a los usuarios, el establecimiento de responsabilidades del usuario, el control de acceso a la red mediante 6 módulos y la integración de ordenadores portátiles. Este resultado guarda similitud con el de Chávez (2016) quien indica que en la municipalidad de Carhuaz se requieren de mecanismos de seguridad por medio de un servidor de datos que permita la administración y control de accesos permitiendo una mejor respuesta a las solicitudes de acceso por parte de los usuarios, en cuanto a la teoría relacionada CISCO (2018) sostiene que los sistemas de seguridad tienen como fin el mejorar el control y acceso a los recursos de red permitiendo que únicamente los usuarios autorizados puedan acceder a la red de datos y solicitar aquella información a la que tienen acceso. De acuerdo a lo expresado es posible afirmar que la red de la Municipalidad Provincial de Carhuaz requiere de un sistema de seguridad de redes que permita gestionar y controlar los accesos, establecer responsabilidades e integrar los diferentes dispositivos a la red brindando así un mejor control y acceso a los recursos informáticos. De acuerdo a CISCO (2006) RADIUS trabaja bajo el protocolo

cliente/servidor, el cual permite que el servidor proporcione el servicio de autentificación, autorización y administración, así mismo este protocolo permite la conexión alámbrica e inalámbrica de los dispositivos sin la necesidad de emplear dispositivos en específico, siendo gracias a ello uno de los sistemas más económicos para su implementación. En base a lo descrito es posible afirmar que el diseño del sistema de seguridad bajo el protocolo RADIUS incorpora una serie de componentes al sistema ya existente, dado que el municipio ya cuenta con el servidor y algunos de los equipos necesarios para su funcionamiento, razón por la cual la solución empleada es económicamente viable.

En cuanto al objetivo específico de implementar el sistema de seguridad de redes basado en el protocolo RADIUS para la mejora de la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019, se realizó la implementación del sistema de seguridad de redes de manera paulatina, iniciando con la instalación del servidor RADIUS en el servidor principal de la Municipalidad Provincial de Carhuaz, posteriormente se realizó la configuración dentro del Windows Server 2008 estableciendo las políticas, las credenciales de usuario y parámetros de control que rigen la administración de acceso a la red. Los resultados descritos guardan similitud a lo descrito por Albujar (2017) quien en su investigación indica que la red que implementó fortaleció la seguridad, integrando la configuración de VLAN y reduciendo las vulnerabilidades existentes debido a la falta de optimización de los servicios de banda ancha y acceso a la red interna, por su parte Microsoft (2017) señala que los servidores RADIUS basado en el Servicio de Autenticación de Internet (IAS) requieren de acciones de monitoreo y control para que se garantice la implementación y disponibilidad continua del servicio y la seguridad de la red, no obstante, es necesario determinar estrategias para la administración de la red, por lo que es necesario

capacitar y equipar al personal para que administre la infraestructura de RADIUS. En base a los descrito es posible afirmar que la implementación del sistema de seguridad basado en el protocolo RADIUS se desarrolló en cumplimiento del diseño, para ello se inició con la incorporación de los protocolos y credenciales de usuario dentro del servidor principal del municipio cuyo sistema operativo es el Windows Server 2008, posteriormente se realizaron acciones de capacitación para el personal encargado de la administración de la red, ello con la finalidad de darle soporte una vez el servidor se encuentre en operación.

Finalmente, en cuanto al objetivo específico de evaluar la influencia del sistema de seguridad de redes basado en el protocolo RADIUS sobre la mejora de la administración de accesos a la red en la Municipalidad Provincial de Carhuaz se aplicó un post test sobre el personal administrativo con el fin de evaluar el cambio de percepción tres meses después de implementado el sistema de seguridad hallándose que el 73,6% califican como regular a la administración de acceso a la red, el 24,5% califican como buena a la administración de acceso a la red y tan solo el 1,9% calificaron como mala a la administración de acceso a la red; tras la comparación con el pre test se halló un incremento en la media del puntaje de calificación de 66,49 a 92,85 lo cual con un Z de Wilcoxon de 6,276 y p-valor de 0,00 indican que es un cambio significativo y positivo. Este resultado guarda similitud con el hallado por Bardales (2015) quien en su investigación tuvo en el pre test un puntaje promedio de 12,67 y en el post test un 25,75 por lo que tras la aplicación del coeficiente de T de Student con un valor de t=13,74 se determinó un cambio en la satisfacción de los usuarios; en cuanto a la teoría la ISO 27001 (2018) indica que la administración de accesos a la red permite mejorar la prevención de infiltraciones y vulneraciones a la seguridad, dado que al no dejar entrar a las personas no autorizadas se minimizar el

riesgo de la manipulación de datos sin un registro de cambios y a su vez se activan mecanismos de bloqueo de accesos al detectarse una infiltración. Los resultados descritos evidencian la mejora de la administración de acceso a la red tras la implementación del sistema de seguridad, lo cual es observador por el personal administrativo dado a que actualmente se cuentan con credenciales de usuarios, protocolos de conexión y control de accesos, lo cual no solo sirvió para limitar accesos no autorizados, sino que permitió la mejora de la cobertura del servicio de red.

V. CONCLUSIONES

1. El sistema de seguridad de redes basado en el protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, lo cual fue contrastado mediante la aplicación de la prueba de Wilcoxon dando como respuesta un Z = 6,276 con un p-valor de 0,000 estableciéndose una mejora significativa entre el antes (pre test) y el después de la implementación (post test).
2. La administración de acceso a la red en la Municipalidad Provincial de Huaraz previa a la implementación de la solución planteada en la presente fue calificada por el 64,1% la califican como mala y como regular por el 34% del personal administrativo, lo cual reflejó la necesidad de implementar el sistema desarrollado.
3. Se determinó que los requerimientos de la administración de la red mediante la aplicación del protocolo RADIUS son mejorar la gestión de los usuarios mediante un servidor RADIUS, determinar las responsabilidades de los usuarios mediante políticas internas, mejorar el control de acceso a la red apoyado en el servidor RADIUS, y realizar el diseño con la integración de ordenadores portátiles. El diseño de la Red RADIUS comprende un total de 34 Access point de la marca Cisco de series Airnet 1600 los que son administrados por la controladora, esto permite la gestión oportuna y precisa de la red inalámbrica.
4. Se realizó la implementación del sistema de seguridad de redes basado en el protocolo RADIUS comprobándose el correcto funcionamiento del servidor y la aplicación de las políticas de acuerdo a los roles de los usuarios, así mismo se determinó la viabilidad económica debido a que se realizará la recuperación de la inversión tras 4 años.

5. Se desarrolló la evaluación de la satisfacción de la administración de accesos a la red hallándose que el 73,6% del personal califica a la administración de accesos como regular, seguidamente el 24,5% la calificó como buena y el 1,9% la calificó como mala, comprobándose así un cambio positivo tras la implementación del sistema de seguridad de redes basado en el protocolo RADIUS.

VI. RECOMENDACIONES

1. La Municipalidad Provincial de Carhuaz debe de continuar con el uso y mejorar con el tiempo al sistema implementado en la presente investigación, ello debido a que administración de acceso a la red con el protocolo RADIUS ha significado una mejora para el personal administrativo.
2. Se deben de desarrollar cursos de capacitación al personal administrativo de la Municipalidad Provincial de Carhuaz con respecto a temas de seguridad de datos, cuidados en el uso de equipos y prevenciones frente al uso de ingeniería social.
3. Es indispensable que la Municipalidad Provincial de Carhuaz explote más las tecnologías inalámbricas a fin de potencializar otros servicios como VoIP, sistemas de vigilancia; así mismo trasladar el Access point del centro tecnológico popular sobre las ventanillas de atención al público lo que permitirá brindar cobertura a la sala de sesiones de juntas.
4. Debido a la cantidad de usuarios que se encuentran en las oficinas, se recomienda utilizar un ancho de banda igual o superior a los 2 Mbps y manejar un plan de contingencia en caso de que la red inalámbrica presente fallas, este plan deberá incluir equipos Access point de Backup.
5. Al implementarse la red se recomienda realizar actualizaciones periódicas, para asegurar un correcto rendimiento de los equipos, además realizar mantenimientos periódicos al servidor RADIUS y el Active Directory, así como revisar el estado físico del equipo de cómputo donde residen estos servidores.

VII. REFERENCIAS BIBLIOGRÁFICAS

Albujar Moreno, O. (2017). *Diseño de un Sistema de Seguridad de Red Basado en la Integración de los Servidores RADIUS - LDAP en Linux para Fortalecer el Acceso de la Red de la Clínica Millenium Chiclayo 2016*. Universidad Nacional Pedro Ruiz Gallo.

América, R. S. (2017). Seguridad en Empresas, Control de Accesos. *Revista Seguridad En América*, *Vol. 15*, 22–56.

Bardales Ramírez, M. (2015). *Sistema de Gestión de Acceso a una Red Wi-Fi Utilizando Software Libre para Mejorar el Nivel de Seguridad del Acceso a la Información*. Universidad César Vallejo.

Chavéz Gonzales, E. (2016). *Diseño de un Cableado Estructurado para Mejorar la Comunicación de datos de la Municipalidad Provincial de Carhuaz, Departamento de Ancash 2016*. Universidad Católica los Ángeles de Chimbote.

CISCO. (2006). *¿Cómo el RADIUS Trabaja?* Notas Técnicas de Troubleshooting. https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

CISCO. (2014). *Acceso del Administrador TACACS al Ejemplo de Configuración Convergido de los Reguladores del Wireless LAN del acceso*. Notas Técnicas y Ejemplos de Configuración. https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/117711-config-tacacs-00.html

CISCO. (2018). *Sistema de Administración de Red: Informe oficial de Mejores Prácticas*. White Paper de Tecnología. https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15114-NMS-bestpractice.html

Cobos Velasco, J., & Gutiérres Constante, G. (2016). *Redes de Computadores I*. Universidad Central de Ecuador.

Diario Gestión. (2016). *Empresas Invierten Cada vez más en Sistemas de Seguridad Informática*. Noticias de Tecnología. https://gestion.pe/tecnologia/empresas-invierten-vez-sistemas-seguridad-informatica-144913-noticia/

Dordoigne, J. (2015). *Redes Informáticas*. Ediciones ENI.

Espinoza Arana, E. (2018). *Desarrollo e Implementación de un Sistema de Control de Acceso a Redes Inalámbricas Mediante RADIUS*. Universidad Nacional Mayor de San Marcos.

Gómez Vieites, A. (2014). *Enciclopedia de la Seguridad Informática*. Ediciones RA-MA.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ta ed). McGraw-Hill.

McGuinness, D. (2017). *Cómo Uno de los Primeros Ciberataques de Origen Ruso de la Historia Transformó a un País*. BB Noticias. https://www.bbc.com/mundo/noticias-39800133

Mendoza Loor, J., & Andrade Acosta, N. (2016). Los Dispositivos Interconectados en el Acceso de Información. *Revista Cientifica Dominio de Las Ciencias*, *Vol. 3*, *Nr*, 313–315.

Microsoft. (2017). *Introducción a Active Directory Domain Service*. Identidad y Acceso Active Directory Domain Services. https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft. (2018). *Diseño de una Infraestructura de RADIUS para la Seguridad de LAN inalámbricas*. Documentación de Microsoft. https://docs.microsoft.com/es-es/security-

updates/security/guadeplaneamientodiseodeunainfraestructuraderadiusparalaseguridad delaninalmbricas

Murillo Safont, J. (2015). *Diseño e Implantación de una Red Inalámbrica Unificada en el Colegio Nuestra Señora de Fátima de Valencia*. Universidad Politecnica de Valencia.

Organisno Internacional de Normalización. (2018). *ISO/IEC 27000*. Normativas. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

Ortega De La Cruz, M. (2017). *Diseño de un Cableado Estructurado bajo la Metodología Top Down Network Design Aplicando Políticas de Seguridad para el Colegio El Pinar de la Ciudad de Huaraz 2017*. Universidad Católica los Angeles Chimbote.

Pazmiño Palma, M., & Pinargote Santana, J. (2016). *Servidor para Autenticación en la Red de Comunicación de datos del GAD Municipal del Cantón Bolívar*. Escuela Superior Politécnica Agropecuaria Calceta de Ecuador.

Pérez, S., & Facchini, H. (2017). *Dispositivos y Protocolos de Redes LAN y WAN*. UTN Regional Mendoza.

Ramírez, T. (2009). *¿Cómo Hacer una Investigación?* PANAPO.

Riofrío, M. (2018). *Las Inversiones en Seguridad Informática no son aún una Prioridad en Perú*. Publicaciones de El Comercio. https://elcomercio.pe/economia/ejecutivos/inversiones-seguridad-informatica-son-prioridad-peru-noticia-541276-noticia/

RPP Noticias. (2018). *Redes y Seguridad Informática: su Impacto en el Futuro de las Empresas*. Publicaciones de Noticias. https://rpp.pe/campanas/contenido-patrocinado/redes-y-seguridad-informatica-su-impacto-en-el-futuro-de-las-empresas-

noticia-1164480

Ruiz, A. (2014). *Redes LAN*. Ministerio de educación del gobierno de España.

Soriano, M. (2014). *Seguridad en Redes y Seguridad de la Información*. Universidad Técnica Checa.

Tamayo, M. (2012). *El Proceso de la Investigación Científica*. Limusa S.A.

Tobar Espinoza, Y., & Mora Cedeño, G. (2016). *Implementación de un Servidor Radius en Windows Server para Centralizar la Administración de Nuevos Access Point en las Oficinas Remotas de Galpones y Huertos del Gobiernos Autónomo Descentralizado de Guayas*. Universidad Politécnica Salesiana.

Vinay Kumar, P. (2015). Role of Diameter Based Protocol in enhancing of new and Upcoming Technologies. *Procedia Computer Science ELSEVIER*, *Vol. 78*, 415–422.

ANEXOS

Anexo 1: Matriz de consistencia

Título	Problemática	Objetivo general y especifico	Hipótesis	Variables e indicadores	Diseño de investigación	Métodos y técnicas de investigación	Población y muestra de estudio
"Diseño del sistema de seguridad de redes basado en el protocolo RADIUS para mejorar la administración de acceso a la red de la municipalidad provincial de Carhuaz, 2019"	¿Cuál debe de ser el diseño del sistema de seguridad de redes para la administración de accesos usando el protocolo RADIUS en la municipalidad provincial de Carhuaz, 2019?	OG: Desarrollar una propuesta de un sistema de seguridad para la administración de accesos a la red usando el protocolo RADIUS en la Municipalidad Provincial de Carhuaz. Objetivos específicos Oe1: Realizar el diagnóstico de la administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz. Oe2: Determinar los requerimientos para el sistema de seguridad para la administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz Oe3: Realizar el diseño del sistema de seguridad para la administración de accesos a la red actual en la	El diseño del sistema de seguridad de redes basado en el Protocolo RADIUS mejora la administración de acceso a la red de la Municipalidad Provincial de Carhuaz, 2019.	Variable 1: Diseño del sistema de seguridad basado en el protocolo RADIUS: D1: Utilización del servicio de autentificación para la administración de acceso a la red D2: Identificación de los requisitos previos de la solución D3: Diseño de la infraestructura RADIUS D4: Plan de administración Variable 2: Administración de acceso a la Red.	No experimental, transeccional descriptiva	Métodos: Estadístico Inferencial Técnicas: De muestreo: Estadística De Recolección de datos: Entrevistas Encuestas De procesamiento: Guía de entrevista Cuestionarios	Población: 53 empleados. Muestra: 53 empleados. Tipo de muestra: No probabilística Censal

		Municipalidad Provincial de Carhuaz Oe4: Desarrollar un prototipo del sistema de seguridad para la administración de accesos a la red actual en la Municipalidad Provincial de Carhuaz		D1: Requisitos de negocio para el control de accesos D2: Gestión de acceso de usuario D3: Responsabilidades del usuario D4: Control de acceso a sistemas y aplicaciones			

Fuente: Elaboración propia

Anexo 2: Instrumento de recolección de requerimientos

Ficha de recolección de información sobre el estado de la Red de Datos de la Municipalidad Provincial de Carhuaz.

1. ¿Cuál es la cantidad de computadoras y laptops conectadas a la red de la Municipalidad Provincial de Carhuaz?

   .....

2. La asignación de las IP es realizada de manera:

   a. Manual

   b. Automática (DHCP)

3. El rango o clase de las direcciones IP empleadas en la red son:

   a. 10.0.0.0 – 10.255.255.255 (Clase A)

   b. 172.16.0.0 – 172.31.225.255 (Clase B)

   c. 192.168.0.0 – 192.168.255.255 (Clase C)

4. Cuantos de los siguientes dispositivos se disponen en el municipio:

   a. Routers: .....

   b. Switchs: .....

   c. Access Points: .....

5. ¿La red de la Municipalidad Provincial de Carhuaz se encuentra segmentada por áreas o departamentos?

   .....

6. ¿Cuántas áreas o departamentos físicos poseen la Municipalidad Provincial de Carhuaz?

   .....

7. ¿Cuántas redes públicas de libre conexión tiene la Municipalidad Provincial de Carhuaz?

   .....

8. ¿Cuánto es el ancho de banda disponible para la red de la Municipalidad Provincial de Carhuaz?

   .....

9. ¿El ancho de banda se encuentra distribuido para cada usuario o dependencia de la Municipalidad Provincial de Carhuaz?

   .....

10. Marque cuales son los servicios instalados en la infraestructura de la Municipalidad Provincial de Carhuaz

    a. Servidor web
    b. Firewall
    c. Servidor proxy
    d. Servidor de correo
    e. Otros .....

Anexo 3: Cuestionario sobre la Administración de accesos de red

A continuación, encontrará una serie de preguntas destinadas a conocer su opinión sobre diversos aspectos se la administración de accesos. Para saber que piensa el personal sobre esta temática.

El cuestionario tiene cuatro secciones. Por favor lea las instrucciones y conteste la alternativa que más se acerca a lo que usted piensa.

Instrucciones: Se evaluará en una escala de 1 a 3, donde 1 Muy en desacuerdo, 2 No vierte opinión (ni de acuerdo ni en desacuerdo), y 3 Muy de acuerdo. Por favor marque con una "X" la alternativa que más se parece a lo que usted piensa.

Sección 1: Requisitos de negocio para el control de accesos

Preguntas	Nivel de conocimiento		
	1	2	3
La municipalidad Provincial de Carhuaz difunde las políticas relacionadas al acceso a la red.			
Los trabajadores de la municipalidad cumplen con las políticas relacionadas al acceso a la red.			
Durante la incorporación de nuevos equipos, estos son formateados y revisados adecuadamente.			
El área de informática monitorea constantemente el funcionamiento de los equipos conectados a la red.			

Sección 2: Gestión de acceso de usuario

Preguntas			
	1	2	3
Existe una lista o registro de los usuarios activos de la red de la municipalidad.			
El personal de área de informática registra los equipos de los nuevos usuarios			
Cada usuario de la red municipal tiene acceso solo a ciertos recursos de la red.			
Los recursos de red con los que dispone son los pertinentes con respecto a sus labores			
Los usuarios externos o invitados son registrados por el área de informática			
Existe una adecuada administración de permisos de los usuarios externos o invitados			

Preguntas			
	1	2	3
Existen políticas o normas que regulan la confidencialidad de los datos personales de los usuarios de la red.			
Los trabajadores son responsables en cuanto al acceso a sus equipos y cuentas			
Los trabajadores conocen sus derechos y responsabilidades en cuanto al uso de sus equipos y recursos de red.			
El MOF y el ROF comprenden las funciones de los trabajadores y los recursos empleados para cumplirlos.			

Sección 3: Responsabilidades del usuario

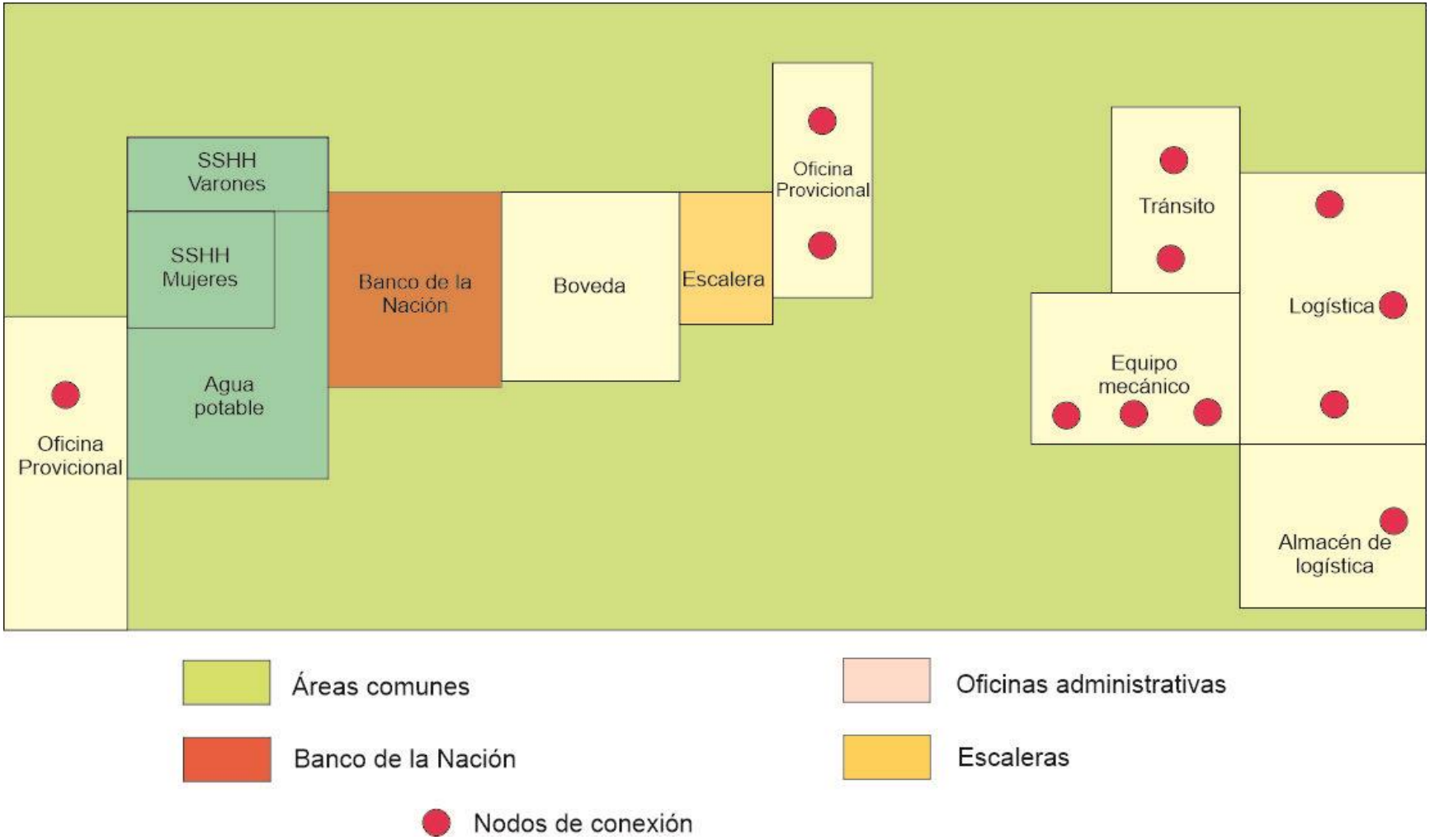
Preguntas	Nivel de conocimiento		
	1	2	3
Los trabajadores usan sus credenciales de acceso a recursos de red de manera personal			
Los trabajadores conocen los riesgos de compartir sus credenciales de acceso con los demás.			
Los trabajadores utilizan claves personales para acceder a sus equipos y a sus cuentas.			
Existen políticas que permiten asegurar la seguridad de datos confidenciales en la municipalidad.			
Los trabajadores dan cumplimiento a las normas y políticas establecidas sobre el uso de los equipos y recursos de red.			
El alcalde, los gerentes y regidores comprenden la necesidad de cumplir con las normas y políticas sobre el uso de equipos y recursos de red.			

Sección 4: Control de acceso a sistemas y aplicaciones

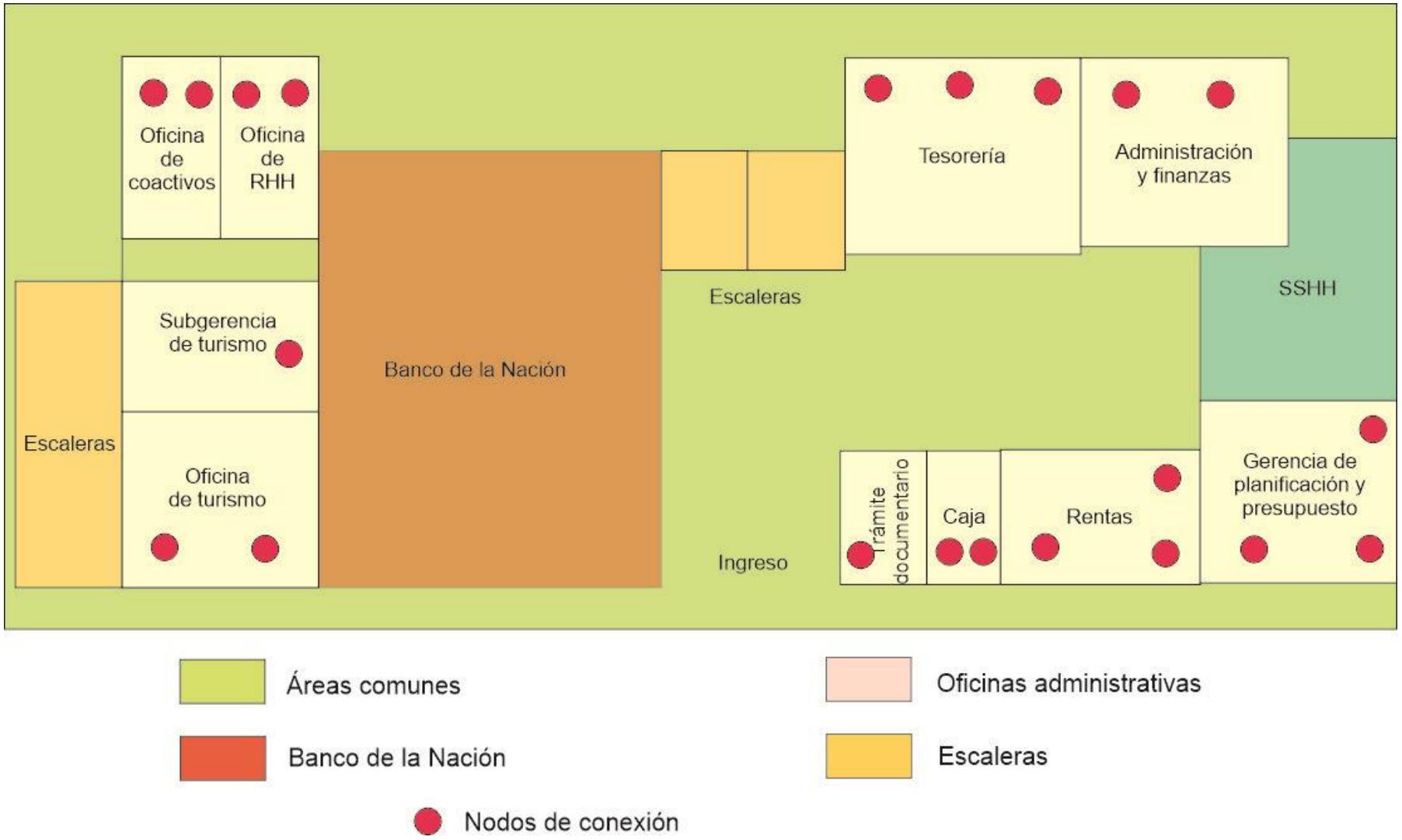
Preguntas	Nivel de conocimiento		
	1	2	3
El área de informática restringe el acceso a información confidencial de la municipalidad.			
Los usuarios externos o invitados requieren del permiso del área de informática.			
Se cuenta con manuales e instructivos para el uso de equipos y acceso a los recursos de red.			

Preguntas	Nivel de conocimiento		
	1	2	3
El personal conoce las pautas para crear y recordarse de sus credenciales de usuario.			
Sus contraseñas son impuestas por el área de informática o por los recursos a los cuales desea acceder.			
Cuenta con las opciones para modificar las contraseñas sin depender del área de informática.			
Cuenta con una opción para recuperar sus contraseñas de manera segura.			
Se cuenta con un soporte técnico para solucionar problemas de acceso a la red.			
Existen políticas y herramientas para la gestión de riesgos (en caso de pérdida de datos, vulnerabilidad, intrusiones o algún otro riesgo)			
Se cuentan con herramientas y software de ayuda para resolver los inconvenientes en el uso de plataformas virtuales.			

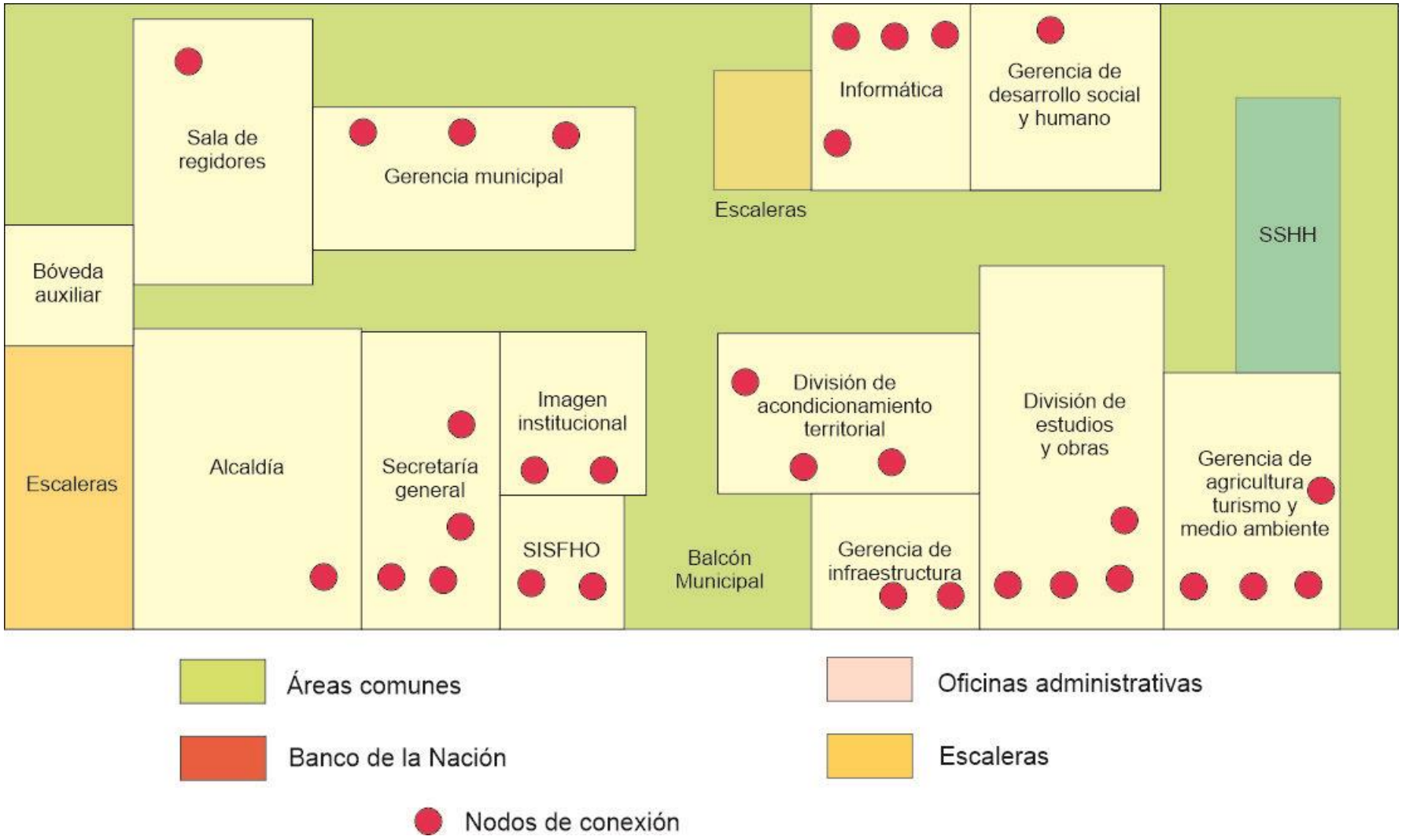
Anexo 4: Plano de ubicación de las antenas inalámbricas



PLANO DEL SÓTANO

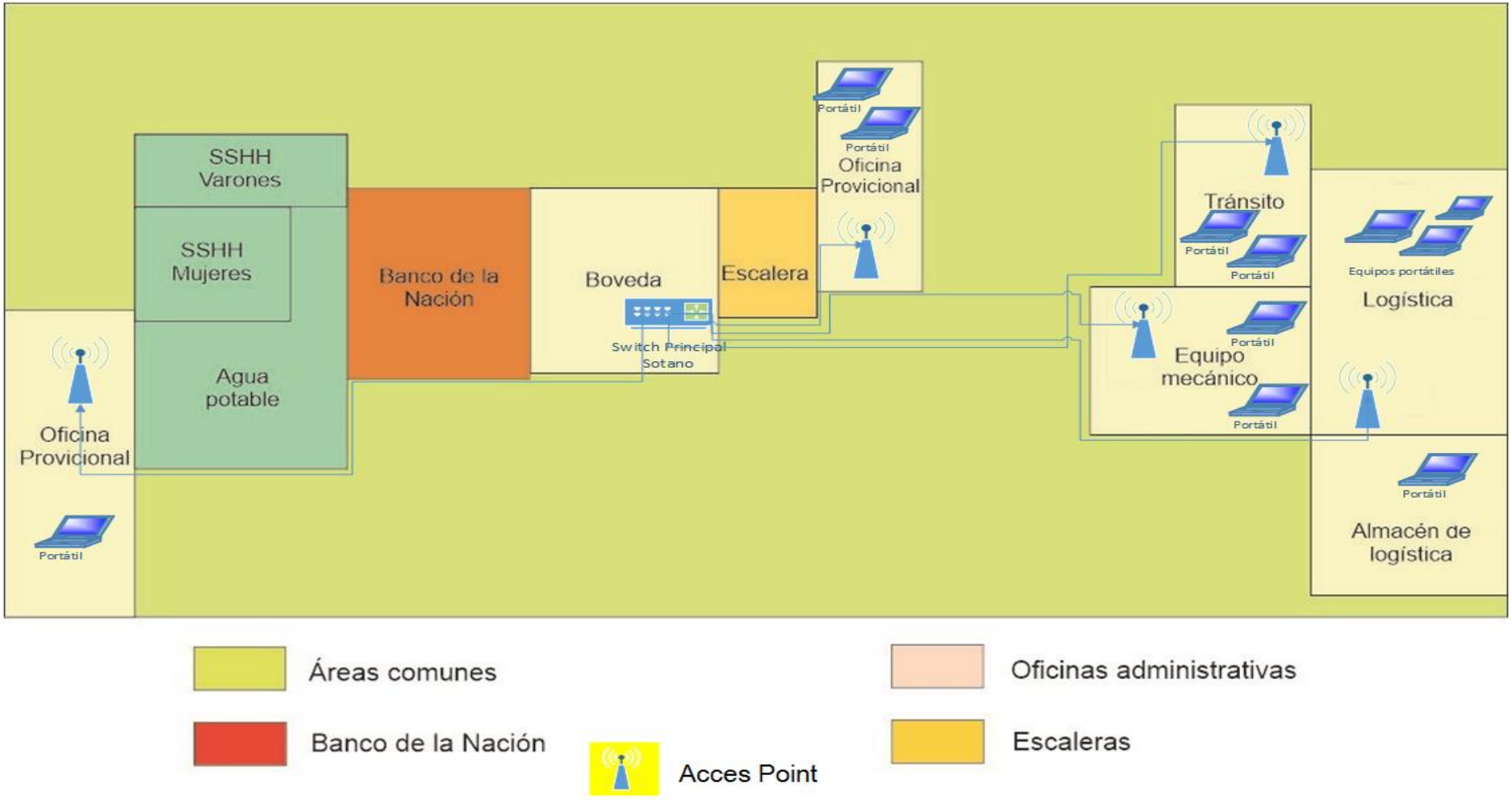


PLANO DEL PRIMER PISO



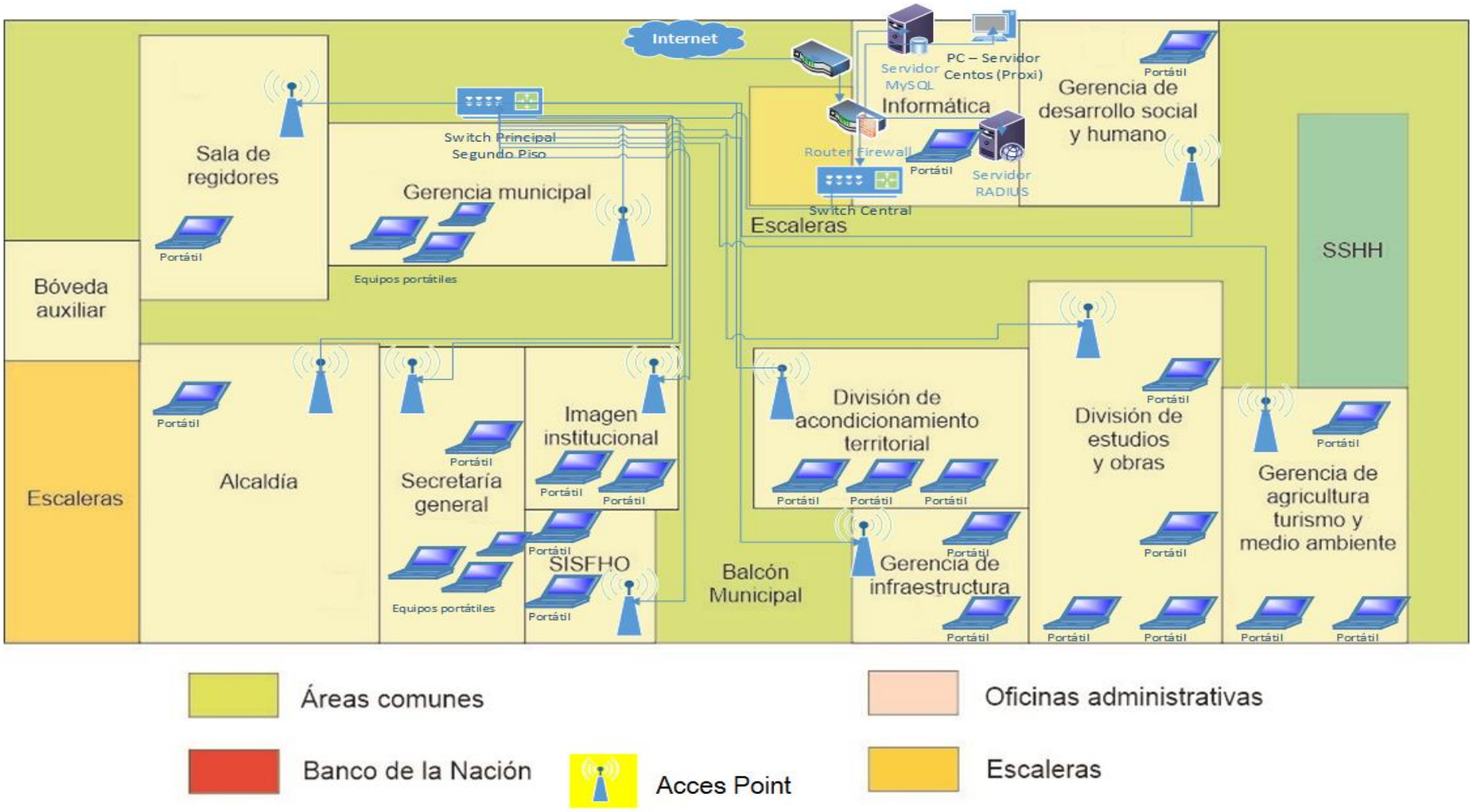
PLANO DEL SEGUNDO PISO

Anexo 5: Plano de la infraestructura de la red



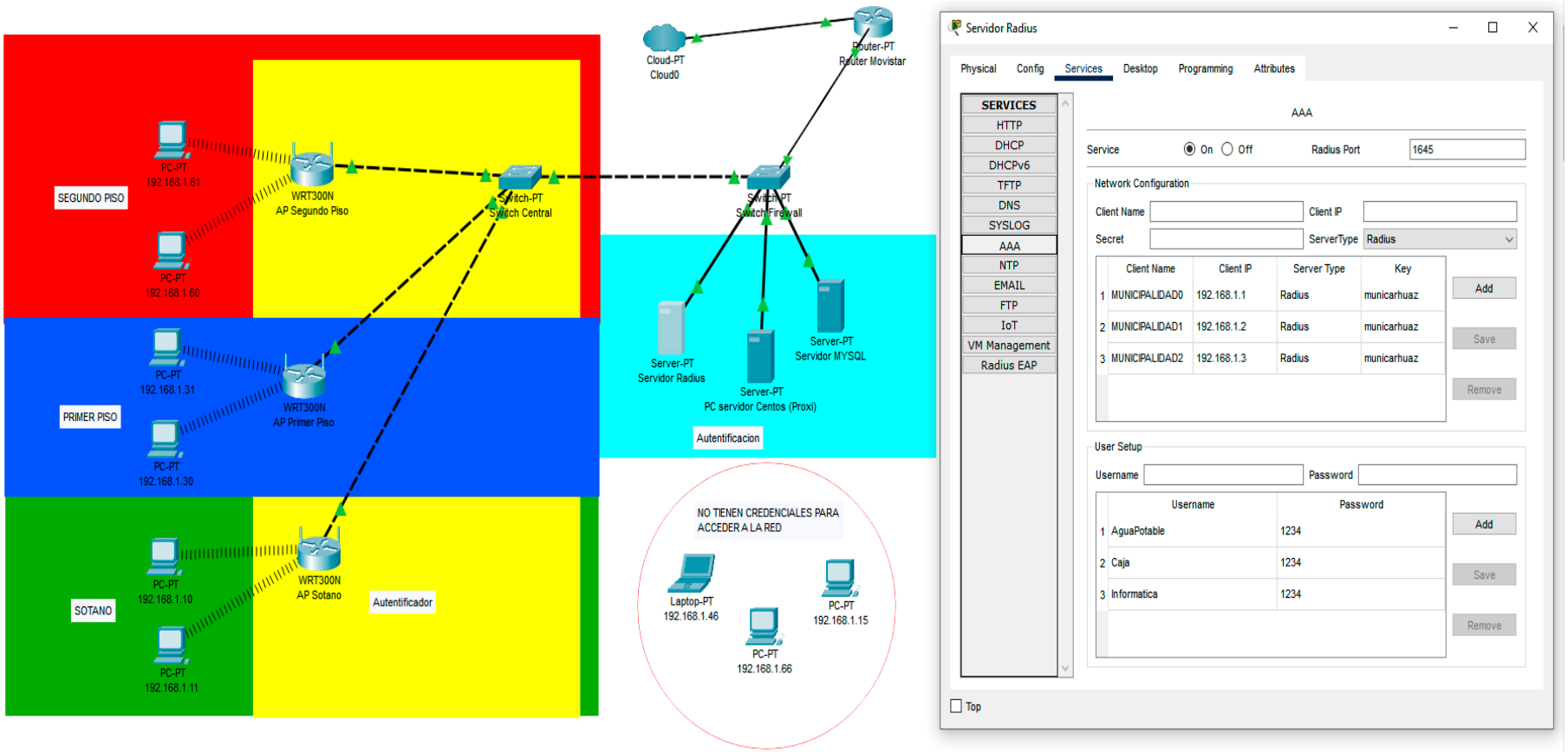
PLANO DEL SÓTANO

PLANO DEL PRIMER PISO



PLANO DEL SEGUNDO PISO

Anexo 6: Desarrollo del diseño y asignación de permisos de usuarios



DISEÑO DE LA RED CLIENTE/SERVIDOR RADIUS

PLANIFICACIÓN DE CUENTAS DE USUARIO

GRUPOS LOCALES

GL1: Alcaldía

GL2: Secretaria general

GL3: Regidores

GL4: Imagen institucional

GL5: Gerencia municipal

GL6: Informática

GL7: División de acondicionamiento territorial

GL8: División de estudios y obras

GL9: Gerencia de agricultura turismo y medio ambiente

GL10: Tesorería

GL11: Administración y finanzas

GL12: Rentas

GL13: Caja

GL14: Gerencia de planificación y presupuestos

GL15: Turismo

GL16: RR. HH.

GL17: Coactivo

GL18: Logística

GL19: Agua potable

GL20: Transito

GRUPOS GLOBALES

GG1: Alcaldía

GG2: Gerencia municipal

GG3: Informática

GG4: Gerencia de agricultura turismo y medio ambiente

GG5: Tesorería

NOMBRE DE LOS SISTEMAS DE INFORMACIÓN

SI1: SI de gestión general

SI2: SI de Logística y Almacén

SI3: SI de Trámite Documentario

SI4: SI de gestión municipal

SI5: SI de manejo de personal

SI6: SI de Caja

SI7: SIAF

SI8: SISFO

SI9: SI de Catastro

SI10: SI de informática y publicidad

SI11: SI de Rentas, Impuesto Predial y Arbitrios

Planificación de usuario, grupos locales y grupos globales

USUARIOS CON GRUPOS LOCALES																				
USUARIOS	**GRUPOS LOCALES**																			
	GL 1	**GL 2**	**GL 3**	**GL 4**	**GL 5**	**GL 6**	**GL 7**	**GL 8**	**GL 9**	**GL 10**	**GL 11**	**GL 12**	**GL 13**	**GL 14**	**GL 15**	**GL 16**	**GL 17**	**GL 18**	**GL 19**	**GL 20**
Usuario 1	X																			
Usuario 2		X																		
Usuario 3		X																		
Usuario 4		X																		
Usuario 5		X																		
Usuario 6			X																	
Usuario 7				X																
Usuario 8				X																

Usuario 9					X														
Usuario 10					X														
Usuario 11					X														
Usuario 12						X													
Usuario 13						X													
Usuario 14						X													
Usuario 15							X												
Usuario 16							X												
Usuario 17							X												
Usuario 18							X												
Usuario 19								X											
Usuario 20								X											
Usuario 21								X											
Usuario 22								X											
Usuario 23									X										

Usuario 24									X										
Usuario 25									X										
Usuario 26									X										
Usuario 27									X										
Usuario 28										X									
Usuario 29										X									
Usuario 30										X									
Usuario 31											X								
Usuario 32											X								
Usuario 33												X							
Usuario 34												X							
Usuario 35												X							
Usuario 36												X							
Usuario 37												X							
Usuario 38													X						

Usuario 39														X					
Usuario 40														X					
Usuario 41														X					
Usuario 42															X				
Usuario 43																X			
Usuario 44																X			
Usuario 45																	X		
Usuario 46																	X		
Usuario 47																		X	
Usuario 48																		X	
Usuario 49																		X	
Usuario 50																		X	
Usuario 51																			X
Usuario 52																			X
Usuario 53																			X

USUARIOS CON GRUPOS GLOBALES					
USUARIOS	**GRUPOS GLOBALES**				
	GG1	**GG2**	**GG3**	**GG4**	**GG5**
Usuario 1	X				
Usuario 9		X			
Usuario 12			X		
Usuario 23				X	
Usuario 28					X

Definición de usuarios

Usuarios		Contraseñas
Usuario 1	Alcaldía	Alcal12
Usuario 2	Gerente secretaria general	Gesege22
Usuario 3	Asesor de secretaria general	Asesege32
Usuario 4	Asistente secretaria general 1	asisege11
Usuario 5	Asistente secretaria general 2	asisege22
Usuario 6	Encargado sala de regidores	salreg62
Usuario 7	Imagen institucional	imains72
Usuario 8	Asistente imagen institucional	asiimains82
Usuario 9	Gerencia municipal	gemuni92
Usuario 10	Sub gerencia municipal	subgemu03
Usuario 11	Asistente gerencia municipal	asigemu13
Usuario 12	Informática	info23
Usuario 13	Asistente informática	asisinfo33
Usuario 14	Soporte informática	sopoinfo43
Usuario 15	División de acondicionamiento territorial	diacote53
Usuario 16	SJ. División de acondicionamiento territorial	sjsiaco63
Usuario 17	A. división de acondicionamiento territorial 1	adiaco73
Usuario 18	A. división de acondicionamiento territorial 2	adiaco83
Usuario 19	G. División de estudios y obras	gobras93
Usuario 20	SG. División de estudios y obras	sdiesob04
Usuario 21	A. División de estudios y obras 1	adiobra14
Usuario 22	A. División de estudios y obras 2	aobra24
Usuario 23	Gerencia de agricultura turismo y medio ambiente	gturiamb34
Usuario 24	Sg. Agricultura	sgagri44
Usuario 25	A. Agricultura	aagri54
Usuario 26	Sg, Medio ambiente	sgmedamb64
Usuario 27	A. Medio ambiente	amedamb74
Usuario 28	Tesorería	teso84
Usuario 29	J. Tesorería	jte94
Usuario 30	A. Tesorería	ates05
Usuario 31	Administración de finanzas	fina15
Usuario 32	A. Administración de finanzas	admifina25
Usuario 33	Rentas	ren35
Usuario 34	SJ. Rentas	sjre45
Usuario 35	C. Rentas	cren55
Usuario 36	A. Rentas 1	aren65
Usuario 37	A. Rentas 2	aren75
Usuario 38	Caja	caj85
Usuario 39	Gerencia de planificación y presupuesto	gepre95
Usuario 40	Sub Gerencia de planificación y presupuesto	sgpla06

Usuario 41	A. Gerencia de planificación y presupuesto	ageplan16
Usuario 42	Turismo	Turi26
Usuario 43	RR. HH.	frh36
Usuario 44	A. RR. HH.	arh46
Usuario 45	Coactivo	coac56
Usuario 46	A. Coactivo	acoc65
Usuario 47	Logística	log75
Usuario 48	SJ. Logística	sjlogi85
Usuario 49	A. Logística 1	aslog95
Usuario 50	A. Logística 2	asilogi06
Usuario 51	Agua Potable	agupot61
Usuario 52	Transito	tran62
Usuario 53	SJ. Transito	sjtransi63

Planificación de restricciones, permisos y acceso

	GG1																				
	GL1							GL2							GL3						
	SISTEMA DE INFORMACIÓN 1														SISTEMA DE INFORMACIÓN 3						
	P		A			R		P		A			R		P		A			R	
	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T
Usuario 1	X	X		X				X	X		X				X	X		X			
Usuario 2								X	X		X				X				X		X
Usuario 3								X	X	X			X		X				X		X
Usuario 4								X				X	X		X				X		X
Usuario 5								X				X	X		X				X		X
Usuario 6															X		X				X

	GG2																				
	GL5							GL16							GL18						
	SISTEMA DE INFORMACIÓN 2							SISTEMA DE INFORMACIÓN 4							SISTEMA DE INFORMACIÓN 5						
	P		A			R		P		A			R		P		A			R	
	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T
Usuario 9	X	X		X				X	X		X				X	X		X			
Usuario 10								X	X	X			X		X				X	X	
Usuario 11								X				X	X		X				X		X
Usuario 43															X	X		X			
Usuario 44															X				X	X	
Usuario 47	X	X		X				X		X			X		X				X	X	
Usuario 48	X	X	X					X				X		X	X				X		X
Usuario 49	X				X	X															
Usuario 50	X				X		X														

	GG3													
	GL4							GL6						
	SISTEMA DE INFORMACIÓN 10													
	P		A			R		P		A			R	
	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T
Usuario 7								X	X		X		X	
Usuario 8								X	X	X			X	
Usuario 12	X	X		X				X		X			X	
Usuario 13	X		X			X								
Usuario 14	X		X				X							

	GG4																												
	GL9							GL7							GL8							GL15								
	SISTEMA DE INFORMACIÓN 8							SISTEMA DE INFORMACIÓN 9																					
	P		A			R		P		A			R		P		A			R		P		A			R		
	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T	L	E	U	ADM	I	P	T	
Usuario 23	X	X		X				X	X		X				X	X		X											
Usuario 24	X		X					X		X			X		X		X			X									
Usuario 25	X				X		X	X				X		X	X				X		X								
Usuario 26	X		X					X		X			X		X		X			X									
Usuario 27	X				X		X	X				X		X	X				X		X								

Usuario 15								X	X		X				X		X												
Usuario 16								X	X	X			X																
Usuario 17								X				X		X															
Usuario 18								X				X		X															
Usuario 19								X				X	X		X	X		X											
Usuario 20															X	X	X		X										
Usuario 21															X				X	X									
Usuario 21															X				X	X									
Usuario 42																						X	X		X				

	GG5																												
	GL10							**GL13**							**GL11**							**GL12**								
	SISTEMA DE INFORMACIÓN 6														**SISTEMA DE INFORMACIÓN 11**														
	P		**A**			**R**		**P**		**A**			**R**		**P**		**A**			**R**		**P**		**A**			**R**		
	L	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**
Usuario 28	X	X		X																									
Usuario 29	X	X	X			X																							

Usuario 30	X				X		X																					
Usuario 31															X	X		X										
Usuario 32															X				X	X								
Usuario 33																						X	X		X			
Usuario 34																						X	X	X				
Usuario 35																						X	X	X			X	
Usuario 36																						X				X		X
Usuario 37																						X				X		X
Usuario 38								X	X		X																	

	GG5																											
	GL14							**GL17**							**GL19**							**GL20**						
	SISTEMA DE INFORMACIÓN 7														**SISTEMA DE INFORMACIÓN 6**													
	P		**A**			**R**		**P**		**A**			**R**		**P**		**A**			**R**		**P**		**A**			**R**	
	L	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**	**L**	**E**	**U**	**ADM**	**I**	**P**	**T**
Usuario 39	X	X		X																								
Usuario 40	X	X	X			X																						

Usuario 41	X				X		X																					
Usuario 45								X	X		X																	
Usuario 46								X				X	X															
Usuario 51															X	X	X											
Usuario 52																					X	X		X				
Usuario 53																					X				X	X		

LEYENDA:

P: Permisos (Lectura: **L**, Escritura: **E**)

A: Accesos (Usuario: **U**, Administrador: **ADM**, Invitado: **I**)

R: Restricciones (Parcial: **P**, Total: **T**)

Plantilla para la identificación de grupos

Identificación de grupos		
Número de Usuarios		
Tipo de usuario:		
Tipo de grupo: □ Local □ Global		
Nombre del grupo	# de Usuarios	Comentarios

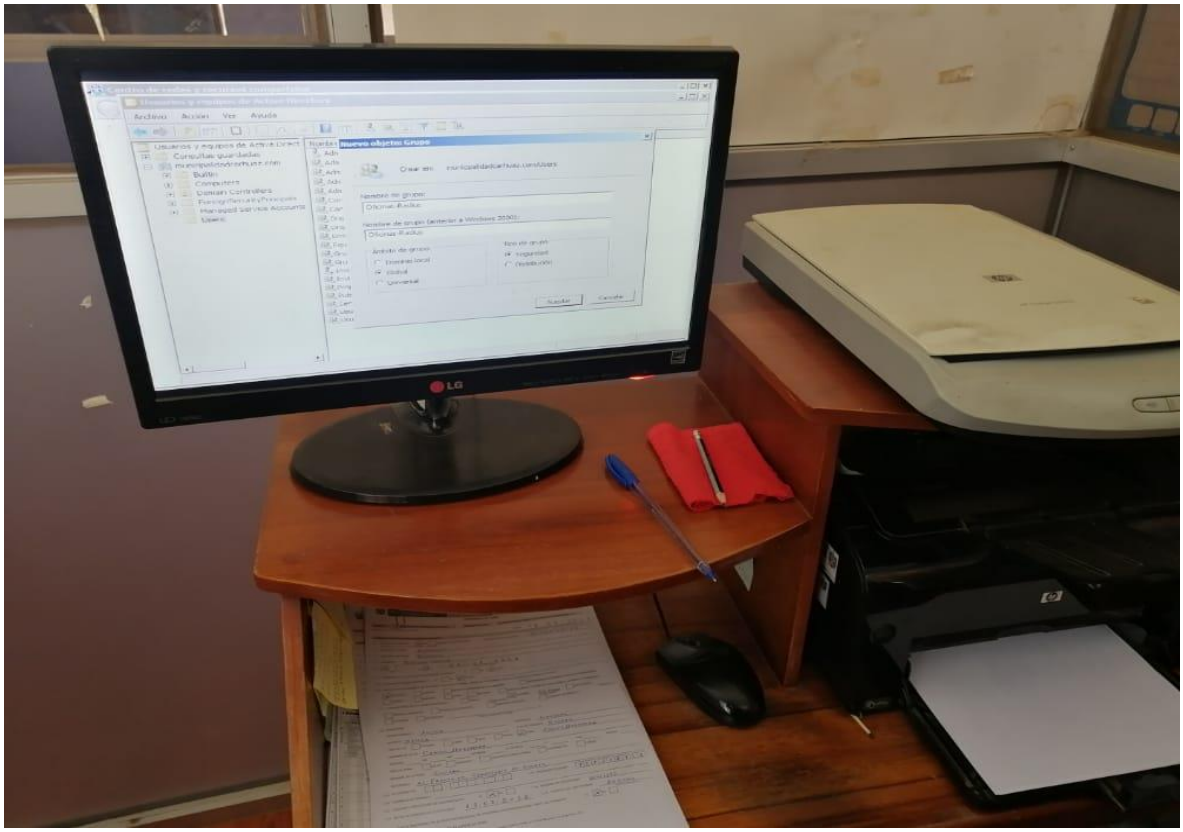
Para la identificación de dominio y usuarios por área

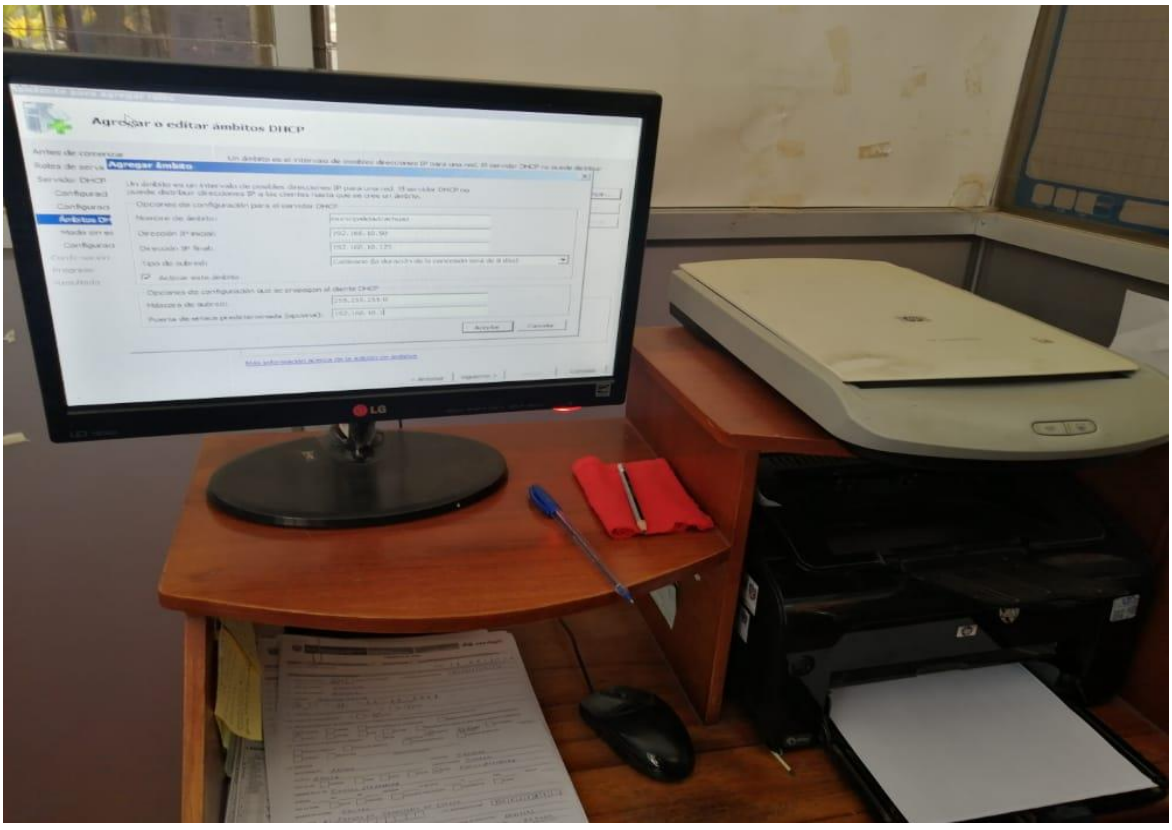
Dominio y usuarios en cada grupo		
Área	Dominios	Usuarios por Dominio
Notas		

Para la asignación de IP

Nombre del usuario	Área	Dirección IP
Notas		

Anexo 7: Fotos de la implementación





Anexo 8: Fotos de capacitación

Anexo 9: Constancia de implementación

Municipalidad Provincial de Carhuaz

"Año del Bicentenario del Perú: 200 años de Independencia"

CONSTANCIA

(CPPP. N° 024-2021 MPC-GAF-RRHH)

El que suscribe, **JEFE DE LA OFICINA DE RECURSOS HUMANOS** de La Municipalidad Provincial de Carhuaz, **CONSTA:**

Que, el Bachiller; **ROJAS MENDEZ JIMMY WILFREDO**, identificado con DNI N° 72204907, Bachiller de la Especialidad de **INGENIERIA DE SISTEMAS E INFORMÁTICA** de la **"UNIVERSIDAD SANTIAGO ANTUNEZ DE MAYOLO – HUARAZ"**, quien ha realizado la **IMPLEMENTACION DE SU TESIS "DISEÑO DEL SISTEMA DE SEGURIDAD DE REDES BASADO EN EL PROTOCOLO RADIUS PARA MEJORAR LA ADMINISTRACION DE ACCESO A LA RED DE LA MUNICIPALIDAD PROVINCIAL DE CARHUAZ, 2019",** en esta institución, las cuales iniciaron el **13 de Agosto del 2021** hasta la culminación de la misma en nuestra Entidad.

Es propio citar que el mencionado Bachiller demostró: puntualidad, responsabilidad, eficiencia y sobre todo proactividad durante el desarrollo de los encargos asignados, lo que le hace recomendable para cualquier efecto de este mismo orden.

Se expide el presente para los fines que el interesado estime por conveniente.

Carhuaz, 07 de Setiembre del 2021.

MUNICIPALIDAD PROVINCIAL DE CARHUAZ

C.P.C. VICTOR ANANIAS RAMIREZ ALBERTO
JEFE DE RECURSOS HUMANOS

C.C. Archivo RRHH.