FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL

INGENIERÍA DE SISTEMAS

SISTEMA DE GESTIÓN DE ACCESO A UNA RED WI-FI UTILIZANDO SOFTWARE LIBRE PARA MEJORAR EL NIVEL DE SEGURIDAD DEL ACCESO A LA INFORMACIÓN

TESIS PARA OBTENER EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

AUTOR:

Br. Bardales Ramírez Odiaga, Milton Rodolfo

ASESOR:

Ing. Edwin Mendoza Torres

LINEA DE INVESTIGACIÓN:

Infraestructura y Servicios de Redes y Comunicación

TRUJILLO – PERU

2015

PÁGINA DEL JURADO

El Presidente y los miembros de Jurado evaluador designado por la escuela de Ingeniería de Sistemas

APRUEBAN:

La tesis denominada:

"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 por:

_____

Br. BARDALES RAMÍREZ ODIAGA, MILTON RODOLFO

_____

MG. ALCÁNTARA MORENO OSCAR

PRESIDENTE DEL JURADO

_____

ING. VEGA GAVIDIA EDWARD

SECRETARIO

_____

DR. PACHECO TORRES JUAN FRANCISCO

VOCAL

Dedicatoria

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis Padres:

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

Milton Bardales Ramírez Odiaga.

Agradecimientos

A DIOS, que nos da la vida y la salud para poder servirle y ser cada vez mejores personas, y así poder esforzarnos para alcanzar nuestras metas y objetivos.

A mis familiares, aquellos que siempre nos apoyan en los momentos buenos y más difíciles de nuestras vidas.

A la Municipalidad Distrital de la Esperanza, por todo su apoyo en la realización de la presente investigación.

A los Ing. Edwin Mendoza Torres y José Luis Madrid Rentería, por la orientación y paciencia en el presente proyecto, gracias por brindarme su apoyo constante.

A todos los docentes, la ocasión es propicia para testimoniar mi sincero y profundo agradecimiento a ellos que con sus conocimientos impartidos, sus consejos, paciencia y tiempo han contribuido valiosa y enormemente a mi formación académica – profesional, sin lo cual no hubiese podido realizar el presente trabajo.

Y sin más, a todas las personas que de una forma u otra apoyaron para que el presente trabajo pueda ser desarrollado.

Milton Rodolfo Bardales Ramírez Odiaga.

Declaración de Autenticidad

Yo Milton Rodolfo Bardales Ramírez Odiaga con DNI N° 42757197, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por el cual me someto a lo dispuesto en las normas académicas de la Universidad César Vallejo.

Trujillo, Julio Del 2015

Br. Bardales Ramírez Odiaga, Milton Rodolfo

Presentación

Señores Miembros del Jurado:

En cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la Tesis 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**". La misma que someto a vuestra consideración y espero que cumpla con los requisitos de aprobación para obtener el título Profesional de Ingeniero de Sistemas.

Milton Rodolfo Bardales Ramírez Odiaga

Índice General

Resumen

La presente investigación denominada **"SISTEMA DE GESTIÓN DE ACCESO A UNA RED WI-FI UTILIZANDO SOFTWARE LIBRE, PARA MEJORAR EL NIVEL SEGURIDAD DEL ACCESO A LA INFORMACIÓN",** tiene como propósito mejorar el nivel de seguridad en el acceso a la información de la Municipalidad Distrital de la Esperanza. Para ello, se obtuvo información a través de entrevistas, observación y encuestas al personal, la cual fue sumamente importante para el análisis de requerimientos enfocados a resolver los objetivos planteados, controlar el acceso inalámbrico para los usuarios autorizados a conectarse a los servicios que ofrece la red y elevar el nivel de satisfacción de los usuarios. Se utilizó como método de análisis de datos la Prueba Z de diferencia de medias, de esta forma el indicador de nivel de satisfacción se aplicó la prueba t Student y la metodología de Jerry FitzGerald se creyó la mejor opción para el desarrollo del proyecto. De acuerdo al objetivo principal planteado en esta investigación, luego de implementado el sistema se redujo el número de intentos para acceder al control del acceso inalámbrico para los usuarios en un 19.25%; además se incrementó la velocidad de la información en un 29.56 %; así mismo, se logró elevar el nivel de satisfacción de los usuarios en un 43.8 %. El sistema implementado permitió el control de los usuarios en el acceso y mejorar la velocidad de la información en la institución. Se concluyó que con la implementación del sistema se ha logrado mejorar significativamente el nivel de seguridad de la información.

Palabras Claves: Gestión de acceso, software libre, seguridad.

Abstract

This research called "MANAGEMENT SYSTEM ACCESS NETWORK USING WI-FI FREE SOFTWARE TO IMPROVE SAFETY LEVEL ACCESS TO INFORMATION", aims to improve the security level of access to information of the District Municipality Hope. To do this, information was obtained through interviews, observation and surveys of staff, which was extremely important for requirements analysis focused on solving the objectives, control wireless access to authorized to connect users to the services offered by the network and raise the level of user satisfaction. It was used as a method of data analysis Test mean difference Z, thus the indicator of satisfaction the Student t test and the methodology applied Jerry FitzGerald the best choice for the project was believed. According to the main objective raised in this research, it implemented the system after the number of attempts decreased to access the wireless access control for users in 19.25%; also the speed of information is increased by 29.56%; Likewise, it was possible to raise the level of user satisfaction in 43.8%. The implemented control system allowed users to access and improving the speed of information in the institution. It was concluded that with the implementation of the system has managed to significantly improve the level of information security.

Keywords: access management, free software, security.

CAPÍTULO I

INTRODUCCIÓN

I. INTRODUCCIÓN

En la actualidad el tema de las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy, debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta el difícil acceso o imposible brindar servicio con una red LAN. La tecnología inalámbrica va desde redes de voz y datos, que permite a los usuarios establecer conexiones mediante la tecnología de luz infrarroja y ondas de radio de alta frecuencia, creando canales de comunicación entre hosts para conexiones inalámbricas de área global o distancias cortas.

La creciente demanda e implementación de redes inalámbricas en entornos educativos y en el ámbito personal, ofrece ventajas a diferencias de las redes tradicionales cableadas, entre las cuales encontramos: la flexibilidad, la movilidad, la facilidad de instalación, la reducción de costo y la escalabilidad que nos proporciona este tipo de tecnología inalámbrica. Asimismo, la seguridad es un punto muy importante a la hora de implementar este medio de comunicación ya que se deben de tener en cuenta diversas prevenciones que eviten las vulnerabilidades que se pueden presentar sino se tiene cuidado.

En muchos casos, los usuarios finales de esta red pasan por alto la seguridad, dejándola en un segundo plano, siendo uno de los motivos más frecuentes la falta de conocimiento de buenas prácticas y políticas para mantener la integridad, disponibilidad y accesibilidad de los recursos de una red.

A medida que evoluciona esta tecnología se han propuesto varias recomendaciones para dotar de un nivel de seguridad adecuado, actualmente se están desarrollando propuestas más concretas de mecanismos que permiten mejorar este nivel.

Entre las soluciones de seguridad más eficientes para el control de acceso a los recursos y la protección de la información en redes inalámbricas, se describe una de las más eficientes, la cual se basa en el uso de autenticación para el acceso a la red y en el uso de encripción en las comunicaciones sobre este tipo de redes.

Teniendo en cuenta lo antes mencionado, se genera la necesidad de implementar un sistema de gestión de acceso a una red wi-fi utilizando software libre; se presenta como antecedentes los trabajos de investigación relacionados con el sistema de gestión de acceso en una organización, uno de los trabajos revisados se titula: "**Diseño e implementación de una red Lan y wlan con sistema de control de acceso mediante servidores AAA**" (García, 2012) el cual describe todas las tecnologías que se emplean en la implementación y cuál fue la evolución tecnológica para llegar a ellas, también me sirve para aportar ideas con los que respecta a la seguridad de la información y al uso adecuado de los recursos de la red.

También fue considerada la tesis titulada: "**Instalación y configuración de un servidor Radius para mejorar el servicio de autenticación y control del servicio WIFI en el Grupo Educativo ITN"** (Santisteban Rengifo, 2011)**,** la cual se realizó en ciudad de Trujillo en el año 2011, donde explica RADIUS como un servicio empleado para controlar el acceso a servicios en red. FreeRADIUS como una solución de código abierto, el cual nos servirá para entender lo que respecta a autenticación de redes a través del protocolo 802.1x & 802.1x-EAP y sobre las ventajas del uso de RADIUS.

Otro tema que fue necesario investigar fue el uso de un sistema en una plataforma de software libre tal es el caso de la tesis titulada : "**Instalación y Configuración de Equipos Informáticos bajo software libre para la Biblioteca de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí** (Bailón Giler, y otros, 2010)**,** la investigacion antes mencionda fue presentada en el país de Colombia en el año 2010, menciona como Instalar y configurar equipos informáticos bajo software libre. La relación que guarda esta tesis con el desarrollo de esta investigación se basa en la aplicación de software libre en el sistema de gestión de acceso la cual beneficiara a la entidad en la reduccion de costos, licencias y en brindar mayor seguridad en la informacion.

Sin duda alguna la propuesta que se presenta en esta investigación desarrolla un sistema capaz de autenticar de manera amigable tratando que la interfaz utilizada sea lo más parecido al entorno con el que los usuarios estaban acostumbrados, brindando mayor seguridad y a la vez reduciendo la filtración de usuarios no autorizados, y por ende incrementando la satisfacción de los usuarios con el óptimo funcionamiento de la red Wi-fi.

La realización de esta investigacion se justifica socialmente debido a que la Municipalidad Distrital de la Esperanza requiere el mejoramiente del nivel de seguridad del acceso a la informacion, contribuyendo al mejoramiento de la confiabilidad e integridad de los datos (trámites, contribuciones, etc.) incrementando el rendimiento de los trabajadores en beneficio de la población.

Su justificación tecnológica se basa en que para la implementación de un Sistema de Gestión de Acceso a una red Wi-fi utilizando software libre, permite el mayor control y seguridad de la información en las diferentes áreas y aumentar así la satisfacción en los clientes.

Debido a las necesidades que hay actualmente en las redes de las telecomunicaciones y en especial en el tema de seguridad WIFI, se debe promover a la investigación en temas que ayuden a mejorar y a evolucionar en estos niveles, es así como se ha abordado este tema como una búsqueda a mejorar un problema como lo es la inseguridad de las comunicaciones WIFI, es muy importante tener en cuenta que para abordar una investigación tecnológica se debe de pensar en un tema de constante investigación, ya que las tecnologías están en constante evolución. Por esta razón se ha abordado este tema como uno de los de suma importancia y de gran a porte a la tecnología.

Actualmente los sistemas inalámbricos disponen de mecanismos de seguridad que permiten garantizar la seguridad, disponibilidad e integridad del acceso al internet por lo tanto fue factible llevar a cabo el proyecto ya que se dispone de diferentes tipos de herramientas para poder desarrollarlo, entre ellas tenemos la EEE 802.11b, EEE 802.11a, EEE 11g, EEE11n, así como también diversos servidores tales como: Radius, AAA, etc. De esta manera se puede desarrollar herramientas tecnológicas comparativas en relación a otras instituciones. Operacionalmente se justifica puesto que permite una rápida adaptación al uso del sistema desarrollado, brindando mayor seguridad y a la vez reduciendo la filtración de usuarios no autorizados a las diferentes áreas de la Municipalidad Distrital de la Esperanza, y por ende incrementar la satisfacción de los usuarios con el óptimo funcionamiento de la red inalámbrica.

En el ámbito económico, el proyecto no genera un gasto adicional a la entidad y busca la manera rentable de realizar esta labor, mejorar el nivel de seguridad del acceso a la información a través de un Sistema de Gestión de Acceso, el cual permite reducir tiempo y ser eficiente, eficaz en la ejecución de las actividades en la gerencia del sistema. Además ya que el sistema se desarrolla con software libre no incurrirá en costo por algún tipo de licencia, lo cual es beneficioso para el proyecto.

Sin estas herramientas no podremos ser competitivos en el mundo actual, y que una vez implementadas y desarrolladas correctamente conducen inevitablemente a un mayor beneficio institucional. A continuación se dan a conocer fundamentos teóricos necesarios sobre los cuales se sustenta la investigación, los cuales harán posible el mejor entendimiento, comprensión y desarrollo del mismo.

Para comprender la investigación es necesario conocer: ¿Qué es una LAN inalámbrica? Según Cisco (CCNA Exploration 4.0, 2009)**,** en términos sencillos, una red de área local inalámbrica (WLAN) hace exactamente lo que el nombre implica. Proporciona todas las funciones y beneficios de las tecnologías LAN tradicionales, como Ethernet y Token Ring, pero sin las limitaciones impuestas por los alambres o cables. De esta forma, las WLANs redefinen la forma en la cual la industria contempla las LANs. Conectividad ya no significa conexión física. Las áreas locales ya no se miden en pies ni en metros, sino en millas o kilómetros. Una infraestructura no necesita estar enterrada u oculta detrás de los muros, sino que puede desplazarse y cambiar según las necesidades de una organización.

Una WLAN, al igual que una LAN, requiere un medio físico a través del cual pasan las señales de transmisión. En lugar de utilizar par trenzado o cable de fibra óptica, las WLANs utilizan luz infrarroja (IR) o frecuencias de radio (RFs). El uso de la RF es mucho más popular debido a su mayor alcance, mayor ancho de banda y más amplia cobertura, las wlan utilizan las bandas de frecuencia de 2,4 Gigahertz (GHz) y de 5 GHz. Estas porciones del espectro de RF están reservadas en la mayor parte del mundo para dispositivos sin licencia. El networking inalámbrico proporciona la libertad y la flexibilidad para operar dentro de edificios y entre edificios.

Entre las ventajas de las redes inalámbricas a corto y largo plazo, se incluyen: la **Accesibilidad:** en el cual todos los equipos portátiles y la mayoría de los teléfonos móviles vienen equipados con la tecnología Wi-fi necesaria para conectarse directamente a una LAN inalámbrica, donde los empleados pueden acceder de forma segura a sus recursos de red desde cualquier ubicación dentro de su área de cobertura. Generalmente, el área de cobertura es su instalación, aunque se puede ampliar más de un edificio. Otra ventaja de una red inalámbrica tenemos la **Movilidad** nos permite que los empleados pueden permanecer conectados a la red incluso cuando no se encuentren en sus mesas. Los asistentes de una reunión pueden acceder a documentos y aplicaciones. Los vendedores pueden consultar la red para obtener información importante desde cualquier ubicación.

Asimismo tenemos la **Productividad,** el acceso a la información y a las aplicaciones clave de su compañía ayuda a su personal a realizar su trabajo y fomenta la colaboración. Los visitantes (como clientes, contratistas o vendedores) pueden tener acceso de invitado seguro a internet y a sus datos de empresa. También tenemos la **Fácil configuración,** al no tener que colocar cables físicos en una ubicación, la instalación puede ser más rápida y rentable.

Las redes LAN inalámbricas también facilitan la conectividad de red en ubicaciones de difícil acceso, como en un almacén o en una fábrica. **Escalabilidad:** Conforme crecen sus operaciones comerciales, puede que necesite ampliar su red rápidamente. Generalmente, las redes inalámbricas se pueden ampliar con el equipo existente, mientras que una red cableada puede necesitar cable adicional.

Otra ventaja que nos brinda las wlan es **la Seguridad:** El control y la administración del acceso a su red inalámbrica es importante para su éxito. Los avances en tecnología Wi-Fi proporcionan protecciones de seguridad sólidas para que sus datos sólo estén disponibles para las personas a las que se les permita el acceso. Los **Costos** ya que se eliminan o se reducen los costos de cableado durante los traslados de oficina, nuevas configuraciones o expansiones. (Mérigo Hernández)

Las redes inalámbricas son vulnerables a diferentes tipos de ataques debido a que el aire es un medio de acceso para cualquier persona que se encuentre en la cobertura de un punto de acceso a la red, dejando la posibilidad de interceptar la transmisión de datos. Para garantizar la seguridad en este tipo de redes es necesario el cifrado de la información antes de ser enviada y la autenticación de los usuarios antes de acceder a la red.

A continuación se detallan los estándares y los protocolos utilizados en la implementación de la presente tesis. El estándar IEEE 802.11i, permite la implementación de una WLAN más segura a través del uso de la encriptación y la autenticación mediante los protocolos WPA,TKIP , CCMP , EAP-TLS y el estándar IEEE 802.1X.

Estándar IEEE 802.11X, es el estándar que más ha destacado es la especificación de la IEEE: 802.11, es la más utilizada ya que brinda a sus usuarios flexibilidad, simplicidad de uso y efectividad de costos. Este estándar especifica los parámetros de dos capas del modelo OSI: la capa física (PHY) y la capa de control de acceso al medio (MAC). La capa MAC tiene tres funciones principales: controlar el canal de acceso, mantener la calidad de servicio (QoS) y proveer seguridad. La capa MAC del IEEE 802.11 soporta servicios de seguridad para las aplicaciones de las capas superiores tales como la autentificación y la privacidad, pero la especificación IEEE 802.11 sólo da un método débil de autentificación y para asegurar la privacidad cuenta con una opción llamada Wired Equivalent Privacy (WEP) que no ha cumplido con su propósito. Al inicio, el 802.11 especificaba un bajo índice de transferencia real, hasta de 2Mbps.El estándar ha sido mejorado en dos diferentes especificaciones: el estándar 802.11b conocido como Wi-Fi, que permite, en teoría, una funcionalidad inalámbrica comparable con Ethernet con un índice de transferencia real de hasta 11Mbps en la banda comercial y el estándar 802.11a que permite hasta 54Mbps .

La arquitectura de una WLAN IEEE 802.11 consiste, generalmente, de un conjunto de servicios básicos (BSS) que se interconectan a un sistema de distribución (DS) para formar un conjunto de servicios extendidos (ESS). Cada estación puede transmitir directamente a cualquier otra estación en el mismo BSS (modo ad-hoc). Por otro lado, para transmitir a estaciones pertenecientes a diferentes BSS, las estaciones pasan a través de un punto de acceso (PA) que es una unidad de enlace que implementa ambos protocolos MAC, el de la IEEE 802.11 y el del DS (modo de infraestructura).

Según (ISECOM) y la IEEE , nos dice "en la actualidad existen varios estándares IEEE 802.11", a continuación mencionaremos : a) **IEEE 802.11a** , el cual opera en el rango de 5 GHz, es capaz de transmitir datos a velocidades de transmisión mucho más altas, pero es más susceptible a interferencias. La tasa de datos es de 54 Mbps. b) **IEEE 802.11b**, rectificado como estándar en septiembre de 1999. Tiene dos formas básicas. Los sistemas de espectro disperso de secuencia directa (DSSS, direct-sequence spread-spectrum), el cual transmiten señales a través de un amplio espectro de frecuencias de radio simultáneamente (en la banda 2.4 GHz). La señal se divide en muchas partes diferentes y se envía sobre diferentes frecuencias simultáneamente. Debido a que varios dispositivos de radio podrían estar operando en estas mismas bandas (teléfonos inalámbricos, hornos microondas...), los dispositivos agregan un código especial a cada bit transmitido que identifica de manera única la señal y permite que el receptor al que se envía la señal la identifique.

Los sistemas de espectro disperso de salto de frecuencias (FHSS, frecuency- hopping spread-spectrum) transmiten señales a través del mismo amplio espectro de frecuencias de radio, pero utilizan cada frecuencia en turnos. Una pequeña ráfaga de datos se envía a una frecuencia (generalmente menos de medio segundo) y luego el emisor cambia a otra frecuencia seudo aleatoria y transmite otra ráfaga de datos antes de cambiar a otra frecuencia, y así sucesivamente.
c) IEEE 802.11g, Estandarizado en Junio del 2003, provee mayores anchos de banda a 2.4GHz, las velocidades son similares a las de 802.11a, y tiene compatibilidad con el estándar IEEE 802.11b.
d) IEEE 802.11n , es la cuarta generación en los sistemas inalámbricas Wi-Fi, compatible en gran parte con los estándares anteriores, trabaja en la frecuencia de 2.4 Ghz y 5 Ghz. la mejora respecto a los anteriores es el uso de varias antenas de transmisión y recepción (MIMO=Múltiple IN, Múltiple OUT) lo que mejora las características de la señal y permite anchos de banda de 300 Mbps (está propuesto a 540 Mbps).

Una característica importante es la capacidad de poder usar una antena exclusivamente para transmitir y otra para recibir, a diferencia de sus predecesoras que usaban la misma antena para ambas acciones, debiendo el transmisor cambiar a modo receptor cada cierto tiempo o usar filtros adicionales. Esto hace que el 802.11n sea ideal para altas velocidades.

En esta investigación también debemos tener conocimientos sobre los Protocolos de Encriptación, estos han pasado por un proceso evolutivo desde WEP hasta contar actualmente con WPA2 desarrollado dentro del estándar IEEE 802.11i. **WEP** (Wired Equivalent Privacy) es el protocolo de encriptación incluido originalmente en el estándar IEEE 802.11, emplea CRC (Cyclic Redundancy Check) como algoritmo de verificación de integridad, y como algoritmo de encriptación utiliza RC4, el cual viene acompañado de una clave secreta de 40 o 104 bits que es combinada con el vector de inicialización (IV) de 24 bits. El envío de la clave es en texto plano, lo que lo hace vulnerable a ataques basados en el uso de analizadores de tramas (sniffers) y decodificadores de código WEP (WEP crackers). (Lehembre, 2015)

También tenemos el protocolo **WPA** (Wi-Fi Protected Access) el cual fortalece el algoritmo de encriptación utilizado por el WEP con el incremento de la clave secreta de 104 a 128 bits, el incremento del vector de inicialización de 24 a 48 bits y la implementación del protocolo de claves dinámicas TKIP (Temporal Key Integrity Protocol), de esta forma se soluciona el problema del tamaño y reutilización del vector, con esto se evita los ataques estadísticos que permiten recuperar la clave WEP, también implementa el código MIC (Message Integrity Code) para el control de integridad, debido a que el control CRC (Cyclic Redundancy Check usado por el WEP) es inseguro al permitir alterar la información sin conocer la clave WEP para luego actualizar el CRC haciendo que el cambio no sea perceptible.

Además incluye un contador de tramas para la protección contra ataques de repetición (reply attacks), su principal mejora fue incorporar un proceso de autenticación que implementa el EAP (Extensible Authentication Protocol) y el estándar 802.1X para distribuir claves diferentes a cada usuario mediante un servidor de autenticación; sin embargo, también se puede utilizar claves precompartidas (PSK - Pre Shared Key) para usuarios domésticos.
El protocolo **WPA2**, el cual está basado en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i (ratificado en Junio de 2004). La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1X/EAP como WPA Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de AP apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard), con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2.este protocolo de encriptación está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI (Tecnologías de la Información) la seguridad que la tecnología cumple con estándares de interoperatividad" declaró el Director de la Wi-Fi Alliance, si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i (siempre y cuando se utilice una clave los suficientemente larga y compleja como para no ser comprometida por ataques de diccionario y/o de fuerza bruta).

En el tema de los estándares de autenticación tenemos: IEEE 802.1x también conocido como Port-Based Network Access Control, originalmente fue desarrollado para redes cableadas, ahora también ha sido adoptado por las redes inalámbricas. Establece una capa entre la capa de acceso y los diferentes algoritmos de autenticación, donde traduce las tramas enviadas a un formato entendible por el sistema de autenticación que utilice la red. Para autenticar al cliente móvil usa el protocolo EAP y para controlar el proceso de autenticación en la red usa PAE (Port Authentication Entity).

Está compuesta por tres entidades funcionales: el usuario (suplicante), el NAS (Network Access Server) o autenticador y el servidor de autenticación. La autenticación de mensajes se incorpora para asegurar que el usuario y el NAS calculen sus claves secretas y activen la encriptación antes de acceder a la red, se comunican mediante el protocolo EAP. El NAS cumple un rol pasivo, pues se limita a enviar los mensajes al servidor de autenticación, EAP es un entorno para el transporte de varios métodos de autenticación, una vez terminado el proceso ambas entidades tendrá una clave maestra secreta (MK). EAP es transportado por el protocolo EAPOL (EAP Over LAN).

La comunicación entre NAS y servidor de autenticación requiere un protocolo de capa más alta, como RADIUS si usamos un servidor RADIUS. Este proceso finaliza cuando el servidor envíe un mensaje “Radius Accept” que contiene la MK y un mensaje final “EAP Success” para el usuario.

Este estándar trae las siguientes ventajas: entre las principales tenemos: Alto nivel de seguridad porque puede usar nombres de usuarios y contraseñas, certificados de usuario, cifrado más seguro, Autenticación y cohesión a la WLAN transparentes, Autenticación por separado de usuarios y de equipos, bajo costo de hardware de red.

Otro punto en el cual la investigación se ha realizado es sobre la **Autenticación en Redes Inalámbricas,** la autenticación es un proceso en el cual se verifica la identidad de una persona o equipo, también se define como el acto o proceso de calificar algo como válido o auténtico. Para la autentificación, el 802.11 especifica dos modalidades: OSA (Autentificación de Sistema Abierto) y la Autentificación de Llave Compartida. La modalidad de autentificación OSA está predispuesta a los ataques debido al uso de llaves previamente compartidas, no utiliza la criptografía de llave pública para obtener una llave en un medio inseguro, de hecho, no se utiliza ningún protocolo de intercambio de llaves, lo cual implica en la práctica, que no hay autentificación verdadera. Por otra parte, la autentificación de llave compartida únicamente admite a aquellas terminales móviles que posean una llave cifrada estática.

Por lo regular la forma más común de autenticación está basada en una combinación de un identificador y una contraseña, esta contraseña debe de ser secreta y sólo el usuario al que se le asignó debe de tener conocimiento de ella, ya que con ésta se podrán acceder a ciertos recursos.
Es una parte fundamental del ***control de acceso***, que es la habilidad de permitir o denegar el uso de un recurso específico a una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, recursos lógicos o recursos digitales. El control de acceso es un mecanismo por el cual un sistema otorga o revoca el derecho de acceder a los datos o realizar acciones. Normalmente, un usuario debe identificarse y posteriormente autenticarse, y para eso se requiere de la existencia de un registro.

El control de acceso se apoya de la gestión del acceso de usuarios, gestión de identificadores de usuarios, registro de usuarios, comprobación de acceso, gestión de privilegios, gestión de contraseñas, entre otras cosas. Los controles de accesos son necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos. Los métodos de autentificación se clasifican en cinco tipos: a) **Autentificación del origen de datos**, es un tipo de autentificación donde la identidad de una de las partes es corroborada con la fuente original de datos específicos creados en algún momento (típicamente sin ser señalado) en el pasado. Este tipo de autentificación incluye integridad de datos. b) **Autentificación de mensaje**, esto sucede cuando se quiere garantizar la procedencia de un mensaje conocido, de forma que se pueda asegurar que no ha sido falsificado, nos provee autentificación del origen de los datos con respecto a la fuente del mensaje original, también provee integridad de datos pero no una garantía sobre la línea del tiempo. c) **Autentificación de transacción**, denota autentificación de mensajes aunado a una garantía de existencia única y temporal, es decir, que identifique el momento preciso de creación.

d) **Autentificación de entidad** nos menciona que es el proceso por el cual una de las partes, mediante la adquisición de evidencia que se puede corroborar, está seguro de la identidad de la otra parte involucrada en el protocolo, y que esa otra parte está activa en ese justo momento. Los términos Identificación y Autentificación de entidad se usan comúnmente como sinónimos. La identificación está basada en una o más de estas características: algo que se conozca (contraseña, NIP, etc.); algo que se posea (por ejemplo, una tarjeta de identificación); y algo que sea inherente a un individuo (huellas digitales u otras características biométricas). e) **Autentificación de llave**, es la propiedad por la cual, una parte, está segura de que ninguna otra entidad además de una segunda parte identificada (o un conjunto de partes confiables) tiene acceso a una llave secreta particular. (Reyes Montiel)

Como servidor a utilizar en este proyecto es RADIUS, el cual gestiona el acceso a las redes, utiliza principalmente por los proveedores de servicios de Internet para gestionar acceso a Internet a sus clientes. El nombre RADIUS es en realidad un acrónimo de "Remote Authentication Dial In User Service" (Dial de autenticación remoto para acceso a servicios). El protocolo no sólo logra acceso a la red, sino también a la gestión de cuentas del usuario. Las funciones de un servidor RADIUS se resumen con las siglas "AAA" que significan: Autenticación, Autorización y Anotación (Registro).
Veamos a continuación a qué se refiere cada uno de estos términos: **Autenticación** hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. Este proceso se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.
Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son: Autenticación de sistema (system authentication), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd; los protocolos PAP (Password Authentication Protocol), y su versión segura CHAP (Challenge Handshake Authentication Protocol), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP; LDAP (Lightweight Directory Access Protocol) que es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.Habitualmente, almacena la información de login o acceso a un sistema (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, Kerberos, el famoso método de autenticación diseñado por el MIT; EAP (Extensible Authentication Protocol), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto; por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

Otra función de Radius es la **Autorización,** el cual se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario. El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor. No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

Por ultimo tenemos el **Registro,** se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio. Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado (aunque posiblemente jerarquizado por medio de diversos servidores RADIUS).

Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas de tecnologías de red (incluyendo módems, xDSL, VPNs y redes inalámbricas) no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet (como e-mail, Web o incluso dentro del proceso de señalización SIP en VoIP). (WEB002)

Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta investigación, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño. RADIUS es un servicio de daemon que se ejecuta en una de las múltiples plataformas y que permanece de forma masiva a la escucha de solicitudes de autenticación hasta que estas se producen. Para ello utiliza el protocolo UDP (y no TCP o SCTP que permitiría mayor control y seguridad en transporte) y permanece a la escucha en los puertos 1812 0 1645 para autenticación y 1813 o 1646 para la contabilidad. Algunos servidores como Freeradius utilizan el puerto UDP 1814 para la escucha de las respuestas proxy RADIUS de otros servidores, pero esto no está contemplado en ningún RFC, y está en conflicto con el puerto utilizado por TDP Suite (Telocator Data Protocol), protocolo de comunicaciones para localizadores de buscapersonas.

Está basado en un modelo cliente-servidor, ya que RADIUS escucha y espera de forma pasiva las solicitudes de sus clientes o NAS, las que responderá de forma inmediata. En este modelo el cliente es el responsable del envió y de la correcta recepción de las solicitudes de acceso, y es el servidor RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, debe enviar al NAS (Network Access Server) los parámetros de conexión necesarios para prestar el servicio. El motivo por el cual RADIUS justifica el uso de UDP sobre TCP en su RFC es por el aprovechamiento de la normativa del protocolo UDP, que mantiene una copia del paquete de solicitud sobre la capa de transporte a fin de poder recuperarlo para reenviarlo, si fuera necesario, a otro servidor RADIUS si el primero no estuviera disponible. De esa manera se simplifica el diseño de protocolos, evitando que hacerse cargo del control de llegada de esos paquetes a su destino. Para aprovechar esta simplicidad se utiliza las características de UDP de ser “stateless” o “connectionless”. Las retransmisiones se pueden hacer más rápidamente hacia otros servidores, ya que el puerto no quedara colapsado por el control de la conexión, evitándose las esperas necesarias en el protocolo TCP.

Cabe recordar que la implementación de la investigación está basada sobre soluciones libres (software libre); para el cual una de sus grandes ventajas es que nos permite poder acceder al código para poder modificarlo de acuerdo a nuestras necesidades y así ser capaces de amoldarlo a la solución más óptima posible. Para este caso, estamos utilizando como plataforma al sistema operativo Ubuntu Desktop, en su versión 15.04 .Como gestor de bases de datos se usó MySQL, es sencillo de usar y rápido. También es uno de los motores de base de datos más usados en Internet, la principal razón de esto es que es gratuito para aplicaciones no comerciales.

Entre sus principales características de MySQL tenemos: Es un gestor de base de datos. Una base de datos es un conjunto de datos y un gestor de base de datos es una aplicación capaz de manejar este conjunto de datos de manera eficiente y cómoda. Es una base de datos relacional. Una base de datos relacional es un conjunto de datos que están almacenados en tablas entre las cuales se establecen unas relaciones para manejar los datos de una forma eficiente y segura. Para usar y gestionar una base de datos relacional se usa el lenguaje estándar de programación SQL. Es de código abierto. El código fuente de MySQL se puede descargar y está accesible a cualquiera, por otra parte, usa la licencia GPL para aplicaciones no comerciales. Es una base de datos muy rápida, segura y fácil de usar.

Para el desarrollo del sistema, se hace uso de la metodología de Jerry FitzGerald, ya que esta da una propuesta completa para desarrollar el proyecto los cuales está constituido por diez pasos de los cuales solo se utilizaron 5 pasos de estos, los cuales definen el problema y los requerimientos necesarios para el sistema, así como también el diseño de la propuesta del sistema para así su posterior validación.

1.1 Problema

Luego de realizada una exhaustiva investigación se obtuvo información relevante que sirve como base para el análisis de requerimientos del sistema propuesto:

- Dificultad en la comunicación y lentitud en la transferencia de información en las computadoras de la institución, por el excesivo tráfico de datos en un mismo segmento de Red, debido al incremento de usuarios de la Red sin el cumplimiento de los estándares de cableado estructurado, topología ancho de banda, entre otros**. (ANEXO 2)**

- Acceso inseguro a la Información disponible en las computadoras de la Red LAN de la institución, al no existir políticas de seguridad, los usuarios internos y externos no autorizados tienen acceso libre a la información y recursos importantes de la Institución y pueden vulnerar sus niveles de protección y confiabilidad. **(ANEXO 3)**

- Libre acceso del personal administrativo a servicios y aplicaciones de Internet no autorizadas por la institución, provocando la disminución de la productividad laboral. **(ANEXO 3)**

- Escasez de personal para el mantenimiento preventivo y correctivo de los equipos de cómputo e impresoras generando inoperatividad de los equipos y la lentitud en las unidades afectadas**. (ANEXO 2)**

Ante estos problemas, se plantean diversos escenarios en los que se proyecta la realización de diversas alternativas de solución y de los cuáles se selecciona, el escenario que trate de mejorar el nivel de seguridad de la información.

Teniendo en cuenta lo expresado anteriormente surge la interrogante, ¿De qué manera un Sistema Gestión de Acceso a una Red Wi-fi utilizando Software Libre, mejorará el nivel de seguridad en el acceso a la información en la Municipalidad Distrital de la Esperanza en el año 2015?

1.2 Objetivos

1.2.1 Objetivo General.

Mejorar el Nivel de seguridad del acceso a la información de la Municipalidad Distrital de la Esperanza, a través de un Sistema Gestión de Acceso a una Red Wi-fi utilizando Software Libre.

1.2.2 Objetivo Específico

- Diseñar e implementar una red inalámbrica en la Municipalidad
- Controlar el acceso inalámbrico para los usuarios autorizados a conectarse a los servicios que ofrece la red en la Municipalidad Distrital de la Esperanza
- Incrementar la velocidad de acceso a la información.
- Elevar el nivel de satisfacción de los usuarios con respecto al acceso a la red Wi-Fi.

CAPITULO II

MARCO METODOLÓGICO

II. MARCO METODOLÓGICO

2.1 Hipótesis

El diseño e implementación de un Sistema de Gestión de Acceso a una Red Wi-fi utilizando Software Libre mejora significativamente el nivel de Seguridad del acceso a la información en la Municipalidad Distrital de la Esperanza.

2.2 Variables

- **Variable Independiente (VI):** Sistema de Gestión de Acceso a una Red Wi-fi.

- **Variable dependiente (VD):** Nivel de Seguridad del acceso a la información.

2.3 Operacionalización de Variables

Tabla 2.1: Operacionalización de Variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	ESCALA DE MEDICIÓN
Sistema de Gestión de Acceso	Un sistema de gestión es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización	Beneficiará en el registro de las actividades de los usuarios y en la restricción de algunos recursos.	Controlar el acceso inalámbrico para Los usuarios autorizados	RAZÓN
Nivel de Seguridad de la Información	La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.	Verificar la seguridad de la información, Confiabilidad, integridad y disponibilidad de la información,	Velocidad de la Información	RAZÓN
			Nivel de Satisfacción de los usuarios	RAZÓN

Tabla 2.2: Descripción de Indicadores

N°	INDICADOR	DESCRIPCION	OBJETIVO	TECNICA / INSTRUMENTO	UNIDAD DE MEDIDA	MODO DE CALCULO
1	Control del acceso inalámbrico para los Usuarios autorizados	Este indicador determinada el número de intentos del usuario al conectarse al sistema.	Mejorar el control del acceso y el nivel de seguridad de la información en la institución	Reportes del Sistema	Porcentaje	$Nsi = \frac{\sum_{i=1}^{n} Iair}{n}$ Nsi: Nivel de seguridad de información debe ser menor que 5 Iair: Bloqueos a intentos de acceso a información restringida n: número de usuarios que intentan acceder a información restringida
2	Velocidad de acceso a la información	Tiempo que demora un usuario en acceder al sistema informático de la institución	Reducir el tiempo que demora la búsqueda de información corporativa por motivo del desorden del mismo.	Medición de Tiempo/Cronómetro	Segundos	$\Delta Vai = \frac{S}{T2} - \frac{S}{T1}$ ΔVai: Incremento de Velocidad de acceso. S : Tamaño de archivo en bits T1: tiempo que demora en enviar el archivo antes de implementar el sistema T2: tiempo que demora en enviar el archivo después de implementar el sistema
3	Nivel de satisfacción de los trabajadores	Este indicador determina el nivel de satisfacción de los usuarios con respecto a la búsqueda de información en la institución	Mejorar el nivel de satisfacción de los trabajadores con respecto a la búsqueda de la información corporativa.	Encuesta	Porcentaje	$st = \frac{\sum_{i=1}^{n} (ts)_i}{n}$ st: Satisfacción del trabajador ts: Trabajador satisfecho n: número de trabajadores

2.4 Metodología

En la presente investigación la metodología utilizada es experimental ya que existe la relación causa y efecto entre la variable dependiente (Nivel de Seguridad del acceso a la información en la Municipalidad Distrital de la Esperanza.) y la variable independiente (Sistema de Gestión de Acceso a una Red Wi-fi utilizando software libre). Así mismo la Metodología a utilizar es Metodologia De Jerry Fitzgerald.

- **Metodologia De Jerry Fitzgerald** (Angulo Díaz, y otros, 2011)

Esta metodología considera las fases siguientes:

Fase I. Consideraciones Técnicas

En esta etapa se analiza la situación problemática actual de la empresa para el procesamiento de información, así como la factibilidad y las características de la red actual.

Subfases:

- Análisis de la Empresa
- Estudio de la Factibilidad

Fase II. Diseño de la Red

En esta etapa se define el alcance geográfico de la red, los mensajes que se transmitirán entre las oficinas de la institución, así como la carga de tráfico para la optimización de la red.

Subfases:

- Alcance de la red.
- Transmisión de la información por medio de la red.

Fase III. Configuración de la Red

En esta etapa se definen las características técnicas de la red, la distribución física de los usuarios, así como las especificaciones para el enlace de comunicaciones entre las regiones.

Subfases:

- Definición de las características técnicas de la red.
- Distribución física de los usuarios.

Fase IV. Consideraciones de Hardware/Software y Seguridad

En esta etapa se definen características del Hardware y Software necesarios para la implementación de la red, así como los niveles de seguridad para el manejo y confiabilidad de la información.

Subfases:

- Definición de las características del hardware y software.
- Definición de niveles de seguridad.

Fase V. Consideraciones de Implementación y Costos

Se evalúan las especificaciones finales del proyecto, así como la estructura de costos que implica la implementación de la red en la empresa.

Subfases:

- Evaluar las especificaciones finales del proyecto.
- Costos de la implementación de la red.
- Implementación de la red.

2.5 Tipo de Estudio

- **Por el Tipo de Investigación: Aplicada**

Debido a que aplicaremos los conocimientos obtenidos durante el proceso de formación Profesional, logrando alcanzar dar solución integral a un problema específico.

- **Según el Nivel o Alcance: Experimental**

Porque nos permite introducir determinadas variables de estudio para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas por el investigador.

2.6 Diseño de Investigación

Para la contrastación de la hipótesis se utilizara el método de diseño en sucesión o en línea llamando también método PRE –TEST –POST-TEST, el que consiste en:

- Una medición previa de la variable dependiente a ser utilizada. (Pre-test).
- La aplicación de la variable independiente a los sujetos del grupo, el cual está afectada por una variable por una variable interviniente.
- Una nueva medición de la variable dependiente en los sujetos. (Post-test)

Diseño de la Investigación.

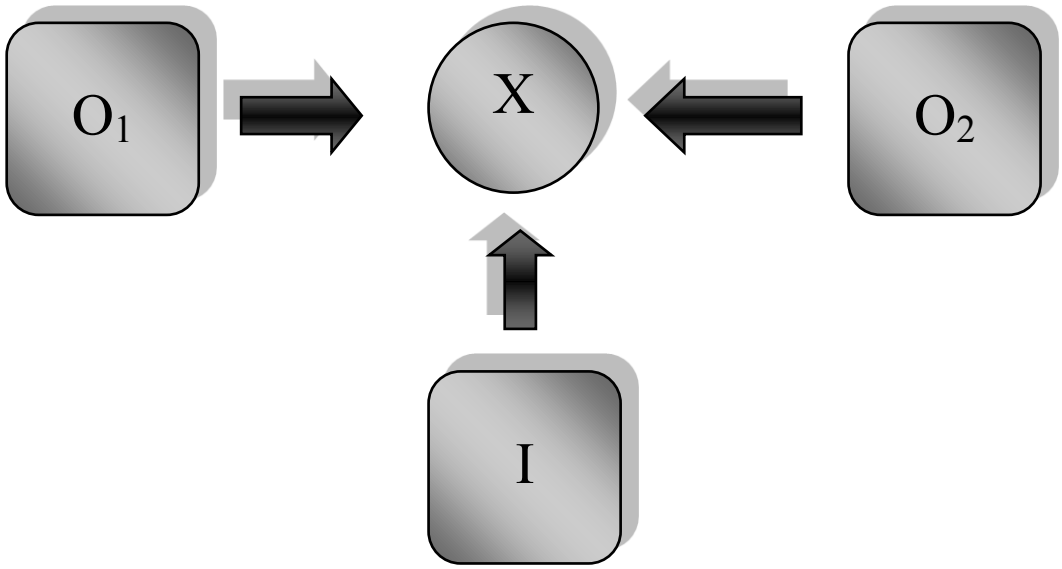


Fig. 2.1: Diseño de la Investigación.

Donde

O_1: Nivel de Seguridad en el acceso de la información, antes de la implementación del Sistema de Gestión de Acceso a una red Wi-fi utilizando software libre.

X: Diseño e implementación del Sistema de Gestión de Acceso a una red Wi-fi utilizando software libre.

O_2: Nivel de Seguridad en el acceso de la información, después de la implementación del Sistema de Gestión de Acceso a una red Wi-fi utilizando software libre.

I: Metodología De Jerry FitzGerald

Al finalizar se establecerán las diferencias entre $\mathbf{O_1}$ y $\mathbf{O_2}$, para determinar si hay mejora o no en el nivel de Seguridad en el acceso de la información en la Municipalidad Distrital de la Esperanza con los resultados obtenidos.

2.7 Población , Muestra y Muestreo

2.7.1 Población

La población para el proyecto de tesis está conformada por los trabajadores de la Municipalidad Distrital de la Esperanza, los cuales están distribuidos de la siguiente manera.

Tabla 2.3: Distribución de los trabajadores del Palacio Municipal

ÁREAS	N° DE TRABAJADORES
ARCHIVO	2
GERENCIA DE ASESORÍA JURÍDICA	4
SECRETARIA DE DEFENSA CIVIL Y GESTIÓN DEL RIESGO DE DESASTRES	2
PROCURADURIA PÚBLICA MUNICIPAL	3
SERVICIO SOCIAL	2
DEMUNA	2
SUBGERENCIA DE LOGÍSTICA Y SERVICIOS GENERALES	7
SUBGERENCIA DE CONTABILIDAD Y CONTROL PATRIMONIAL	6
SUBGERENCIA DE TESORERÍA	4
SECRETARÍA DE RELACIONES PÚBLICAS Y COMUNICACIONES	5
SECRETARIA GENERAL	6
SECRETARÍA DE ALCALDÍA	3
ALCALDÍA	1
GERENCIA MUNICIPAL	3
PROCURADURIA PÚBLICA MUNICIPAL	3
DIVISIÓN DE PROGRAMACIÓN E INVERSIONES	2
GERENCIA PLANEAMIENTO, PRESUPUESTO Y RACIONALIZACIÓN	2
SUBGERENCIA DE PRESUPUESTO Y	2

ESTADÍSTICA	
SUBGERENCIA DE LA PLANIFICACIÓN ORGANIZACIÓN Y MÉTODOS	1
SUBGERENCIA DE RECURSOS HUMANOS	8
DIVISIÓN DE REGISTRO CIVIL	4
SECRETARÍA DE TRÁMITE DOCUMENTARIO Y ARCHIVO	4
GERENCIA DE ADMINISTRACIÓN TRIBUTARIA	12
SUBGERENCIA DE INFORMÁTICA Y SISTEMAS	4
DIVISIÓN DE EJECUCIÓN COACTIVA	2
ÓRGANO CONTROL INSTITUCIONAL	2
TOTAL :	**96**

Tabla 2.4: Distribución de los trabajadores Anexo 1

ÁREAS	**N° DE TRABAJADORES**
SECRETARÍA DE PARTICIPACIÓN VECINAL	1
SUBGERENCIA DE ORNATO Y ÁREAS VERDES	1
SUBGERENCIA DE JUVENTUD, DEPORTE Y RECREACIÓN	3
GERENCIA DE DESARROLLO URBANO Y PLANEAMIENTO TERRITORIAL	1
SERVICIO SOCIAL	2
ALMACÉN	2
SUBGERENCIAS DE OBRAS	4
SUBGERENCIA DE HABILITACIÓN URBANA Y CATASTRO	3
TOTAL :	**17**

Tabla 2.5: Distribución de los trabajadores Anexo 2

ÁREAS	N° DE TRABAJADORES
SUBGERENCIA DE ACTIVIDADES ECONÓMICAS Y LICENCIAS	2
SECRETARÍA DE DEFENSA CIVIL Y GESTIÓN DEL RIESGO DE DESASTRES	2
SUBGERENCIA DE TRANSPORTE, TRÁNSITO Y SEGURIDAD VIAL	2
GERENCIA DE DESARROLLO ECONÓMICO LOCAL	3
TOTAL :	**9**

La población total de la Municipalidad Distrital de la Esperanza está representada por:

N = 122 Usuarios

2.7.2 Muestra

Se calcula a partir de la población, la misma que al representar una cantidad muy alta, nos vemos precisados a establecer una muestra, la misma que se representa en una formula en general.

$$M = \frac{N * z^2 * P * Q}{(N-1) * E^2 + z^2 * P * Q}$$

Dónde:

M = Tamaño de la Muestra.

N = Tamaño de la Población; N = 122

E = Margen de error 5%: E = 0.05

Z = Coeficiente de Nivel de Confianza es de 95 % Z = 1.96

P = Probabilidad de éxito; P = 0.5

Q = Probabilidad de fracaso; Q = 0.5

$$M = \frac{122 * 1.96^2 * 0.5 * 0.5}{(122-1) * 0.05^2 + 1.96^2 * 0.5 * 0.5}$$

M = 92.7

M = 93 usuarios

La muestra simple obtenida para el estudio es de 93 usuarios, trabajadores de la Municipalidad Distrital de la Esperanza.

2.7.3 Muestreo

El muestreo es de tipo probabilístico y se utilizó el muestreo aleatorio simple.

2.7.4 Población, muestra y muestreo por cada indicador

Por cada indicador ser calcularon las siguientes muestras:

a) **Indicador N° 1:** Controlar el acceso inalámbrico para los usuarios autorizados a conectarse a los servicios que ofrece la red en la Municipalidad Distrital de la Esperanza

Para este indicador se evaluará el número de intentos de los usuarios al ingresar al sistema implementado.

Población= 122 usuarios

Reemplazando los valores en la fórmula de muestreo:

$$M = \frac{122 * 1.96^2 * 0.5 * 0.5}{(122-1) * 0.05^2 + 1.96^2 * 0.5 * 0.5}$$

M = 93 Usuarios.

Muestra: 93

Muestreo: El muestreo es de tipo probabilístico y se utilizó el muestreo aleatorio simple.

b) **Indicador N° 2:** Velocidad de acceso a la Información.

Para este indicador se evaluará el tiempo que demora un usuario en acceder al sistema de gestión de acceso de la institución.

Población = 122 usuarios

Reemplazando los valores en la fórmula de muestreo:

$$M = \frac{122 * 1.96^2 * 0.5 * 0.5}{(122-1) * 0.05^2 + 1.96^2 * 0.5 * 0.5}$$

M = 93 Usuarios.

Muestra: 93 usuarios

Muestreo: El muestreo es de tipo probabilístico y se utilizó el muestreo aleatorio simple.

c) **Indicador N° 3:** Nivel de satisfacción de los trabajadores.

Para este indicador se utilizará la declaración de cada usuario sobre su sobre su nivel de satisfacción con el sistema de gestión de acceso a la red inalámbrica de la municipalidad.

Población = 122 usuarios

Reemplazando los valores en la fórmula de muestreo:

$$M = \frac{122 * 1.96^2 * 0.5 * 0.5}{(122-1) * 0.05^2 + 1.96^2 * 0.5 * 0.5}$$

M = 93 Usuarios.

Muestra: 93 usuarios

Muestreo: El muestreo es de tipo probabilístico y se utilizó el muestreo aleatorio simple.

2.8 Técnicas e Instrumentos De Recolección De Datos.

Las técnicas empleadas para la recolección de información son las siguientes:

Tabla 2.6: Técnicas e instrumentos de recolección de datos.

TÉCNICA	INSTRUMENTOS	INFORMANTES
Encuesta	Cuestionario	Trabajadores de la institución
Entrevista	Cuestionario	Jefe del Área de Sistemas
Observación	Análisis	Áreas de Trabajo de la institución

2.9 Métodos de análisis de datos

Para realizar el contraste de la hipótesis y determinar si es aceptada o rechazada, se analizará el antes y el después de las variables luego de haber sido expuestas al estímulo; para ello se efectuará la prueba de distribución Z para muestras mayores a 30 y T Student para los indicadores menores iguales a 30:

Si n < 30 → Prueba T Student para diferencia de medias

Si n >= 30 → Prueba Z para diferencia de medias.

A. Para un indicador n < 30

Tabla 2.7: Prueba T Student

Nro.	I_a	I_p	D_i	D_i^2
1	$I1_a$	$I1_d$		
2	$I2_a$	$I2_d$		
3	$I3_a$	$I3_d$		
4	$I4_a$	$I4_d$		
			$\sum_{i=1}^{n} Di$	$\sum_{i=1}^{n} Di^2$

Procedimiento:

1. **Definición de Variables**

Ia=Indicador del Sistema Actual

Ip= Indicador del Sistema Propuesto

2. **Hipótesis Estadística**

Hipótesis H0:

H0 = Ia– Ip<=0

El indicador del Sistema actual es mejor que el indicador del sistema propuesto.

Hipótesis Ha:

Ha = Ia– Ip> 0

El indicador del Sistema propuesto es mejor que el indicador del Sistema actual.

3. **Nivel de Significancia**

X = 5% (ERROR)

Nivel de confiabilidad ((1-X)=0.95)

4. **Estadística de la Prueba**

$$t = \frac{\overline{D}\sqrt{n}}{SD}$$

Dónde:

$\overline{D}$ = Diferencia de Promedio

n =Muestra

SD = Desviación Estándar

5. Región de Rechazo

La Región Rechazo es $t = t_x$

Donde t_x es tal que:

$P [T > T_x] = 0.05$

Donde t_x= Valor Tabular

Luego Región de rechazo: $t > t_x$

- **Diferencia de Promedios**

$$\bar{D} = \frac{\sum_{i=1}^{n} Di}{n}$$

- **Desviación Estándar**

$$Sp = \sqrt{\frac{n\sum_{i=1}^{n} Di^2 - (\sum_{i-1}^{n} Di)^2}{n(n-1)}}$$

Distribución T Student

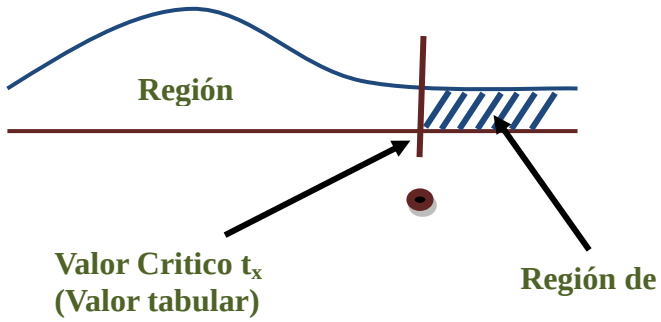


Fig. 2.2: Distribución T Student.

B. Para un indicador n >= 30

Prueba Z diferencia de medias

Nro.	I_a	I_p	$I_{ai} - \overline{Ia}$	$I_{pi} - \overline{Ip}$	$(I_{ai} - \overline{Ia})^2$	$(I_{pi} - \overline{Ip})^2$
1	$I1_a$	$I1_p$				
2	$I2_a$	$I2_p$				
3	$I3_a$	$I3_p$				
4	$I4_a$	$I4_p$				
			$\sum_{i=1}^{n}(Ia - \overline{Ia})$	$\sum_{i=1}^{n}(Ipi - \overline{Ip})$	$\sum_{i=1}^{n}(Iai - \overline{Ia})2$	$\sum_{i=1}^{n}(Ipi - \overline{Ip})2$

$$\overline{Ia} = \frac{\sum_{i=1}^{n} Iai}{n} \qquad \overline{Ip} = \frac{\sum_{i=1}^{n} Ipi}{n}$$

Fig. 2.3: Prueba Z Diferencia de medias.

Procedimiento:

1. **Definición de Variables**

   I_a=Indicador del Sistema Actual

   I_p= Indicador del Sistema Propuesto

2. **Hipótesis Estadística**

   Hipótesis H_0:

   $$H_0 = I_a - I_p <= 0$$

   El indicador del Sistema actual es mejor que el indicador del sistema propuesto.

   Hipótesis H_a:

   $$H_a = I_a - I_p > 0$$

   El indicador del Sistema propuesto es mejor que el indicador del Sistema actual.

3. **Nivel de Significancia**

X = 5% (ERROR)

Nivel de confiabilidad ((1-X)=0.95)

4. **Estadística de prueba**

$$Zc = \frac{(\overline{Xa} - \overline{Xp})}{\sqrt{\frac{\sigma a^2}{na} + \frac{\sigma p^2}{np}}}$$

5. **Región de rechazo**

La región de rechazo es **Z = Zx**, donde **Zx** es tal que:

P [Z >Zx] = 0.05, donde Zx = Valor Tabular

Luego Región de rechazo:

Z >Zxz<

- **Promedio**

$$\overline{x} = \frac{\sum_{i=1}^{n} Xi}{n}$$

- **Desviación Estándar**

$$S^2 = \frac{\sum_{i=1}^{n} (Xi - \overline{x})^2}{n-1}$$

"Distribución Z (Normal)"

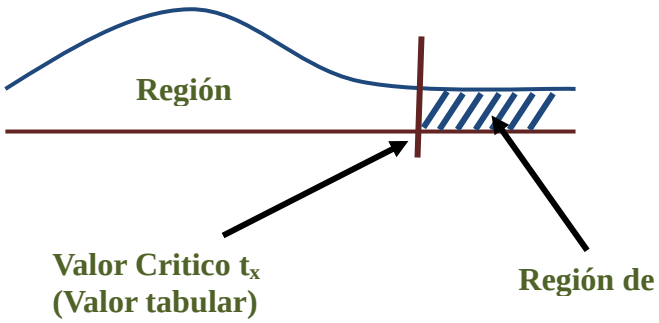


Fig. 2.4: Distribución de Z

Capítulo III

RESULTADOS

III. RESULTADOS

El estudio realizado hace uso de la Metodología de Jerry FitzGerald, para ello se siguen diversas Fases.

3.1 Desarrollo de la Metodología de Jerry FitzGerald

3.1.1 Fase I Consideraciones técnicas

3.1.1.1 Estudio de la Factibilidad

Flujo de Caja

Tabla 3.23: Flujo de Caja

PERIÓDO / INGRESOS	Año 0	Año 1	Año 2	Año 3
INGRESOS	**0**	**8,160.00**	**8,435.00**	**8,760.00**
Ahorro en Horas de Trabajo		7,560.00	7,560.00	7,560.00
Ingresos Proyectados		600.00	875.00	1,200.00
EGRESOS	**11,025.09**	**1,384.69**	**1,384.69**	**1,384.69**
Costo de Inversión y Desarrollo	**11,025.09**			
Hardware	3,865.00			
Software	0			
Materiales	308.40			
Recursos Humanos	6,800.00			
Consumo Eléctrico	51.69			
Costos de Operación		**1,384.69**	**1,384.69**	**1,384.69**
Consumo Eléctrico		51.69	51.69	51.69
Mantenimiento		560.00	560.00	560.00
Depreciación		773.00	773.00	773.00
Flujo de Caja	**-11,025.09**	**6,775.31**	**7,050.31**	**7,375.31**
Flujo de Caja Acumulado	**-11,025.09**	**-4,249.78**	**2,800.53**	**10,175.84**

1. Análisis de Rentabilidad

A. VAN (Valor Anual Neto)

Criterio de Evaluación:

VAN < 0 → No conviene ejecutar el proyecto. El valor actual de costos supera a los beneficios; por lo que el capital invertido no rinde los beneficios suficientes para hacer frente a sus costos financieros.

- VAN > 0 → Conviene ejecutar el proyecto.
- VAN=0 → Es indiferente la oportunidad de inversión.

La Tasa mínima aceptable de rendimiento:

- Tasa (TMAR)= 15% - Fuente: Banco de Crédito

Formula:

$$VAN = -I_0 + \frac{(B-C)}{(1+i)} + \frac{(B-C)}{(1+i)^2} + \frac{(B-C)}{(1+i)^3}$$

Dónde:

- $\boldsymbol{I_0}$**:** Inversión inicial o flujo de caja en el periodo 0.
- **B=**Total de beneficios tangibles
- **C=**Total de costos operaciones
- **n=**Número de años (período)

Reemplazamos los beneficios y costos totales obtenidos en el flujo de caja tenemos:

$$\boldsymbol{VAN} = -11{,}025.09 + \frac{(8{,}160.00 - 1{,}384.69)}{(1+0.15)} + \frac{(8{,}435.00 - 1{,}384.69)}{(1+0.15)^2} + \frac{(8{,}760.00 - 1{,}384.69)}{(1+0.15)^3}$$

$$\boldsymbol{VAN = 5046.91}$$

B. Relación Beneficio/Costo (B/C)

La relación costo beneficio toma los ingresos y egresos presentes netos del estado de resultado, para determinar cuáles son los beneficios por cada nuevo sol que se invierte en el proyecto.

Formula:

$$\frac{B}{C} = \frac{VAB}{VAC}$$

Dónde:

- **VAB:** Valor Actual de Beneficios.
- **VAC:** Valor Actual de Costos.

Fórmula para Hallar VAB:

$$VAB = \frac{B}{(1+i)} + \frac{B}{(1+i)^2} + \frac{B}{(1+i)^3}$$

Reemplazamos los beneficios obtenidos en el flujo de caja tenemos:

$$VAB = \frac{(8{,}160.00)}{(1+0.15)} + \frac{(8{,}435.00)}{(1+0.15)^2} + \frac{(8{,}760.00)}{(1+0.15)^3}$$

$$\boldsymbol{VAB = 16{,}072.00}$$

Fórmula para Hallar VAC:

$$VAC = I_0 + \frac{C}{(1+i)} + \frac{C}{(1+i)^2} + \frac{C}{(1+i)^3}$$

Reemplazamos los beneficios obtenidos en el flujo de caja tenemos:

$$VAC = 11{,}025.09 + \frac{1{,}384.69}{(1+0.15)} + \frac{1{,}384.69}{(1+0.15)^2} + \frac{1{,}384.69}{(1+0.15)^3}$$

$$\boldsymbol{VAC = 14{,}186.64}$$

Reemplazamos los valores de VAB y VAC

$$\boldsymbol{B/C = \frac{16{,}072.00}{14{,}186.64}}$$

$$\boldsymbol{\frac{B}{C} = 1.13}$$

C. TIR (Tasa interna de retorno)

La tasa interna de retorno o tasa interna de rentabilidad (TIR) de una inversión, está definida como la tasa de interés con la cual el valor actual neto o valor presente neto (VAN o VPN) es igual a cero. El VAN o VPN es calculado a partir del flujo de caja anual, trasladando todas las cantidades futuras al presente. Es un indicador de la rentabilidad de un proyecto, a mayor TIR, mayor rentabilidad.

$$0 = -I_0 + \frac{(B-C)}{(1+i)} + \frac{(B-C)}{(1+i)^2} + \frac{(B-C)}{(1+i)^3}$$

Usando la fórmula de Excel obtenemos el siguiente resultado:

Flujo de Caja	**-11,025.09**	**6,775.31**	**7,050.31**	**7,375.31**

abla 3.24: Tasa Interna de Retorno

TIR = 41%

D. Tiempo de Recuperación de Capital

Esto indicador nos permitirá conocer el tiempo en el cual recuperaremos la inversión (años / meses / días).

Fórmula:

$$\boldsymbol{TR = \frac{I_0}{(B - C)}}$$

Dónde:

- **Io:** Capital Invertido
- **B:** Beneficios generados por el proyecto
- **C:** Costos Generados por el proyecto

Reemplazando los datos, obtenemos el siguiente resultado:

$$\boldsymbol{TR} = \frac{\mathbf{11,025.09}}{(\mathbf{8,160.00 - 1,384.69})}$$

$$\boldsymbol{TR} = \mathbf{1.62}$$

1 año

0.62 *12 = 7.44, es decir 7 meses

0.44 *30 = 13.2, es decir 13 días

3.1.2 Fase II Diseño de la Red

3.1.2.1 Alcance de la Red

Fig. 3.11: Diagrama Físico de la Red de Datos - Palacio Municipal (Primer Piso)

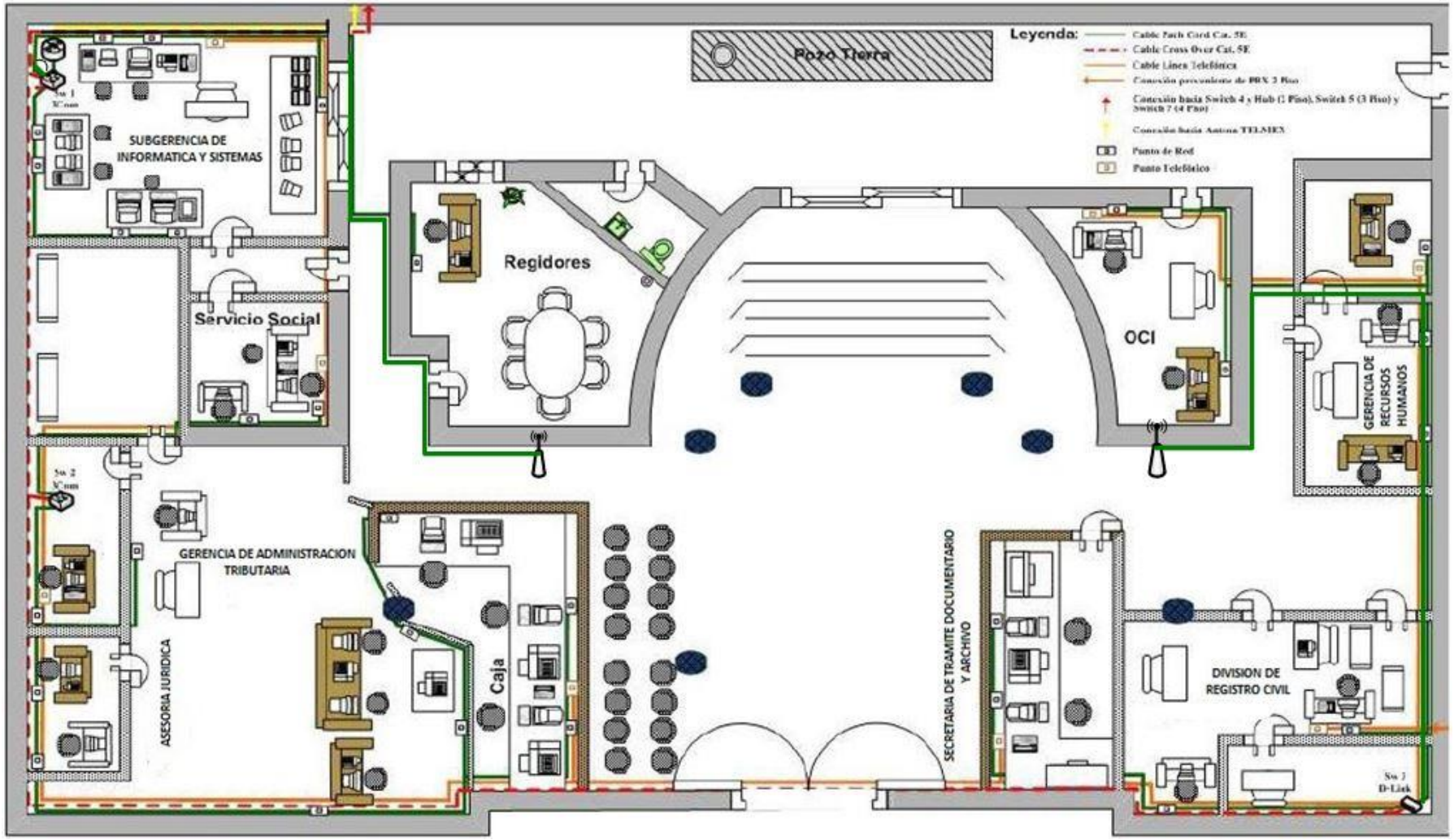


Fig. 3.12: Diagrama Físico de la Red de Datos - Palacio Municipal (Segundo Piso)

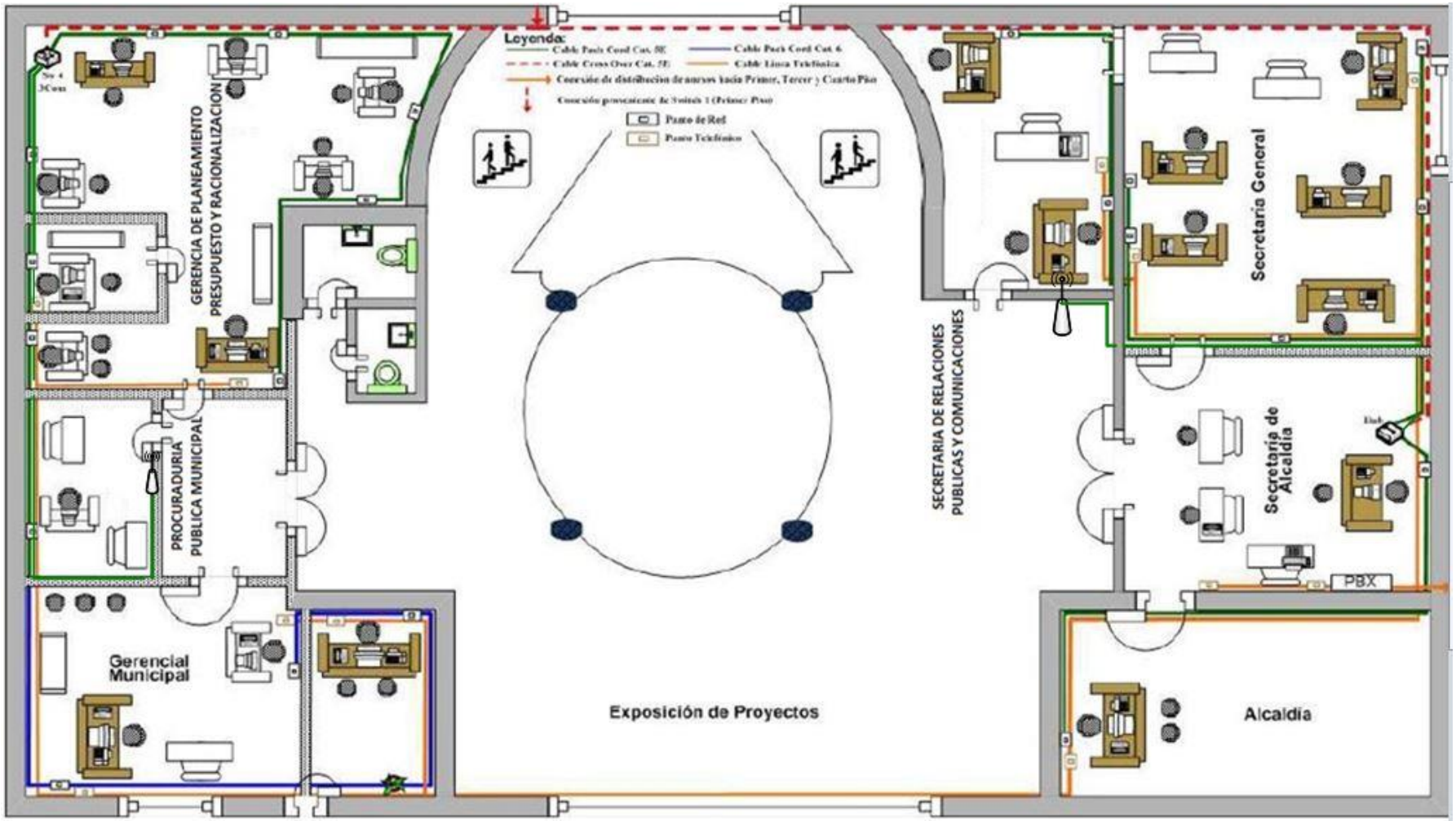


Fig. 3.13 Diagrama Físico de la Red de Datos - Palacio Municipal (Tercer Piso)

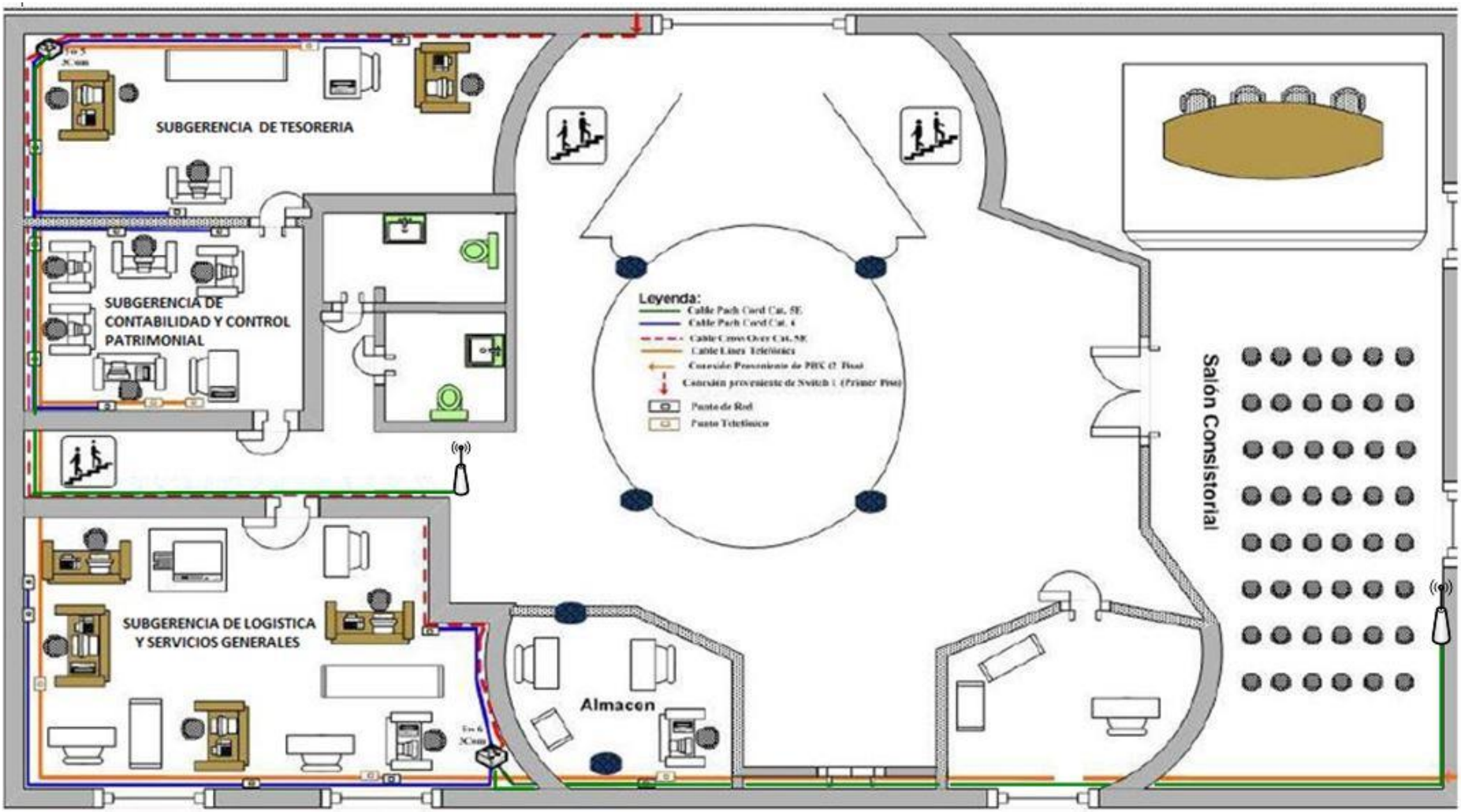
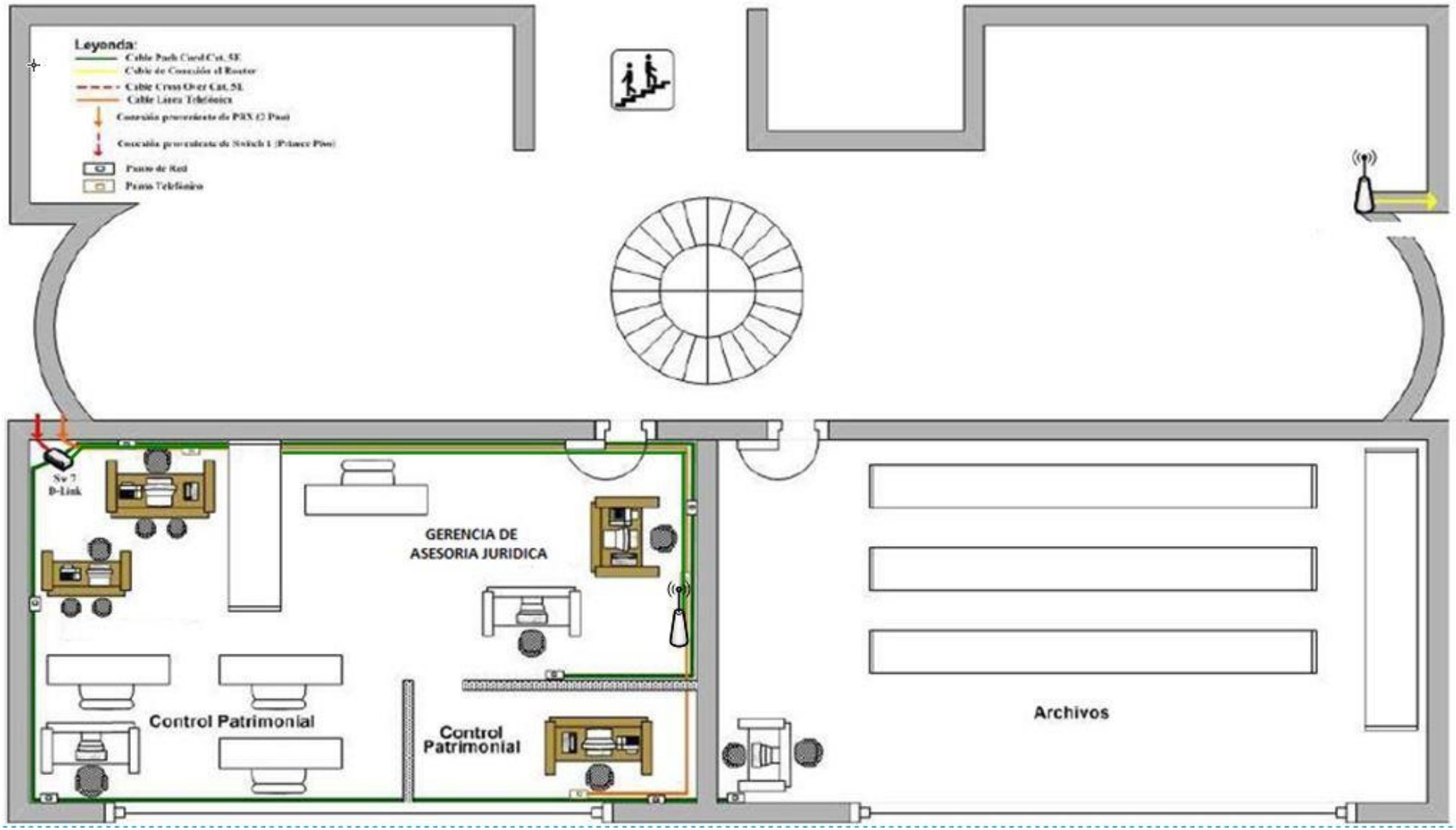


Fig. 3.14: Diagrama Físico de la Red de Datos - Palacio Municipal (Cuarto Piso)



3.1.2.2 Transmisión de la información por medio de la red

Para verificar la manera de transmisión de información en la Municipalidad Distrital de la Esperanza se utilizaron herramientas de testeo de red:

- ✓ Advanced IP Scanner
- ✓ Colasoft Ping Tool
- ✓ Free Port Scanner
- ✓ Wireshark Network Analyzer

En las siguientes pantallas se muestra la taza de transferencia de información con la red actual de la municipalidad, obtenidas con el software descrito anteriormente.

Utilizando Software: Advanced Ip Scanner: Es una herramienta con la cual se obtiene todos los datos disponibles de las IP que se encuentran conectados en tu misma red como el nombre de red, dirección MAC, nombre del equipo.

Fig. 3.20: Escaneo de red con Advanced IP Scanner

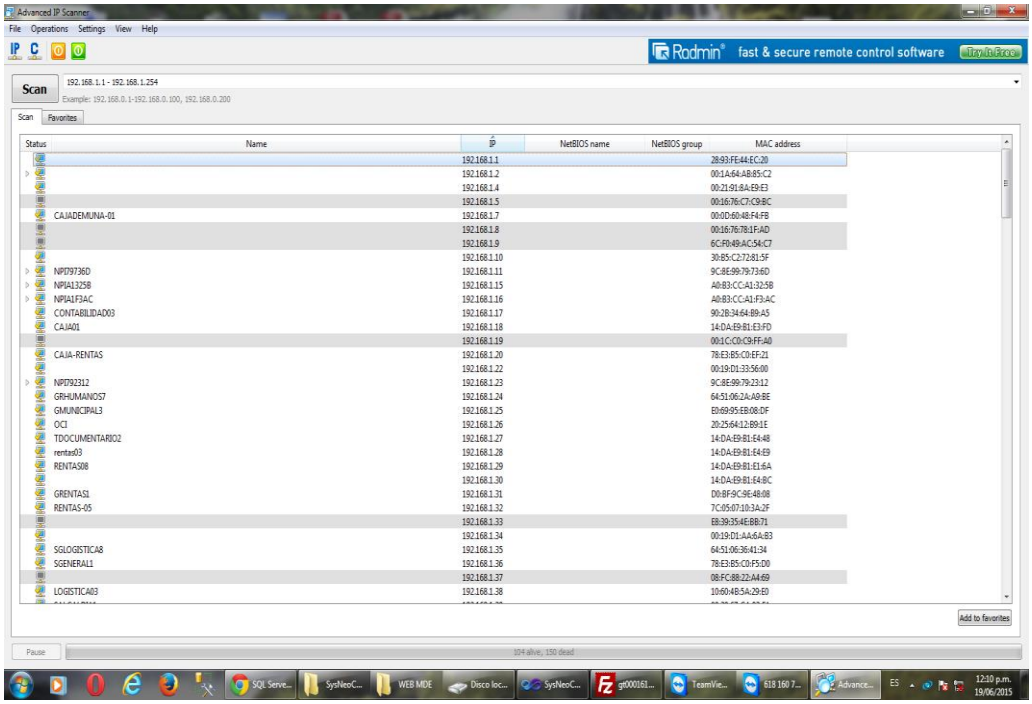
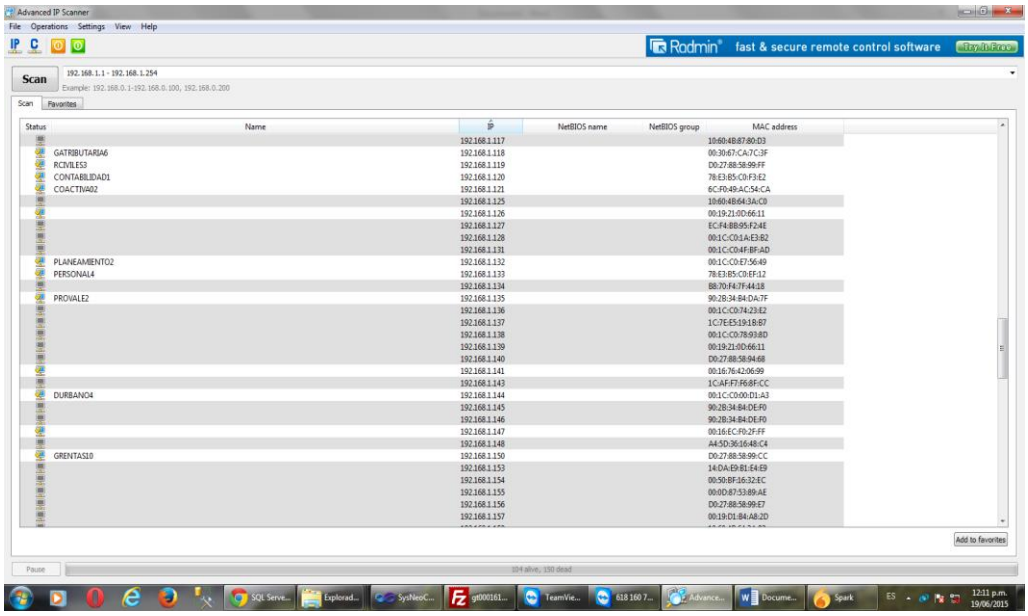


Fig. 3.21: Escaneo de red con Advanced IP Scanner



Utilizando Ping Tool: Esta es una herramienta que permite testear la velocidad de transmisión a través de la red cableada en la Municipalidad Distrital de la Esperanza.

Fig. 3.22: Escaneo de red con Ping Tool

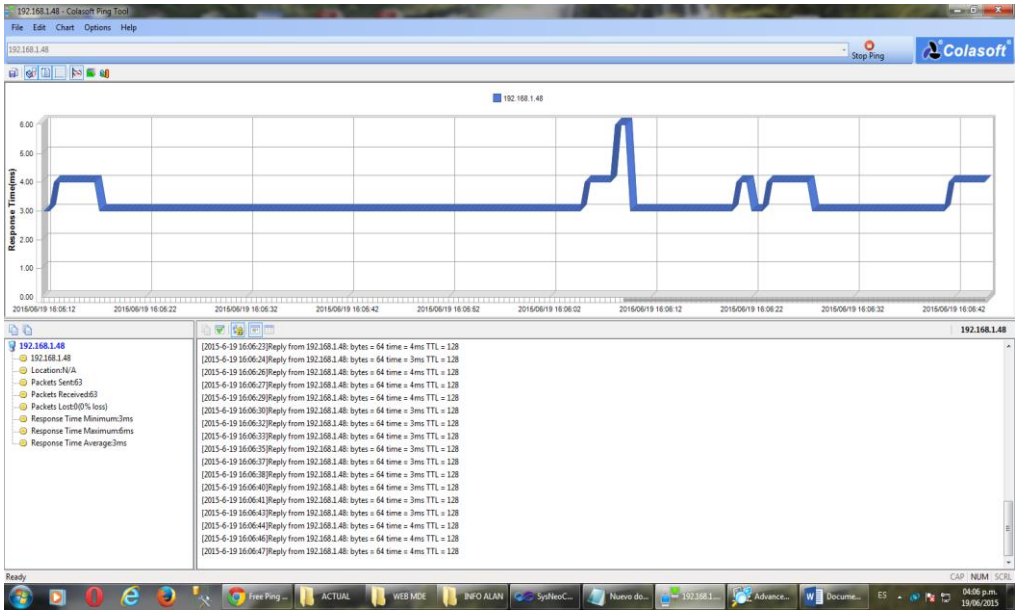
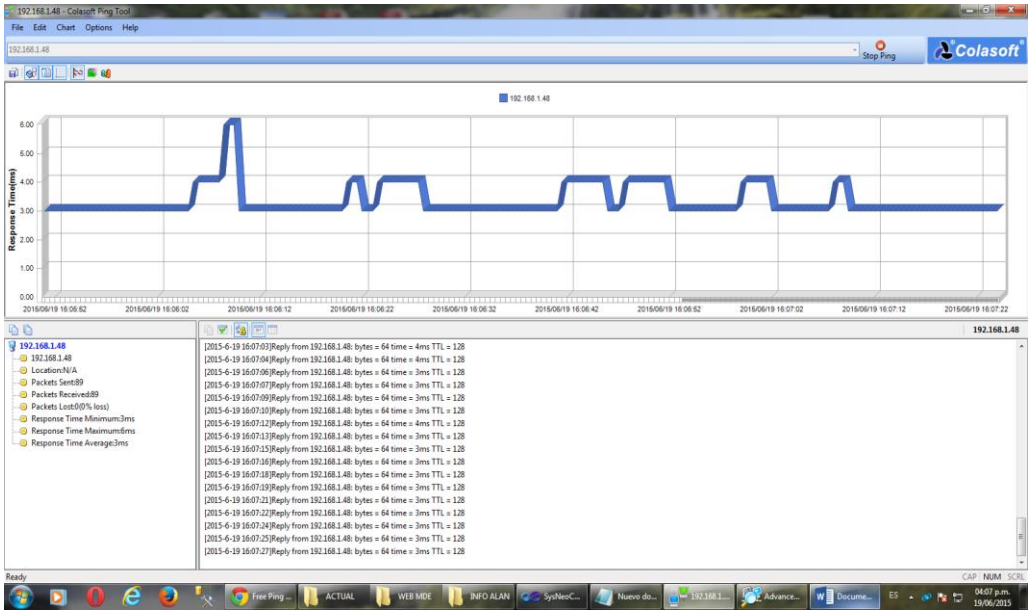
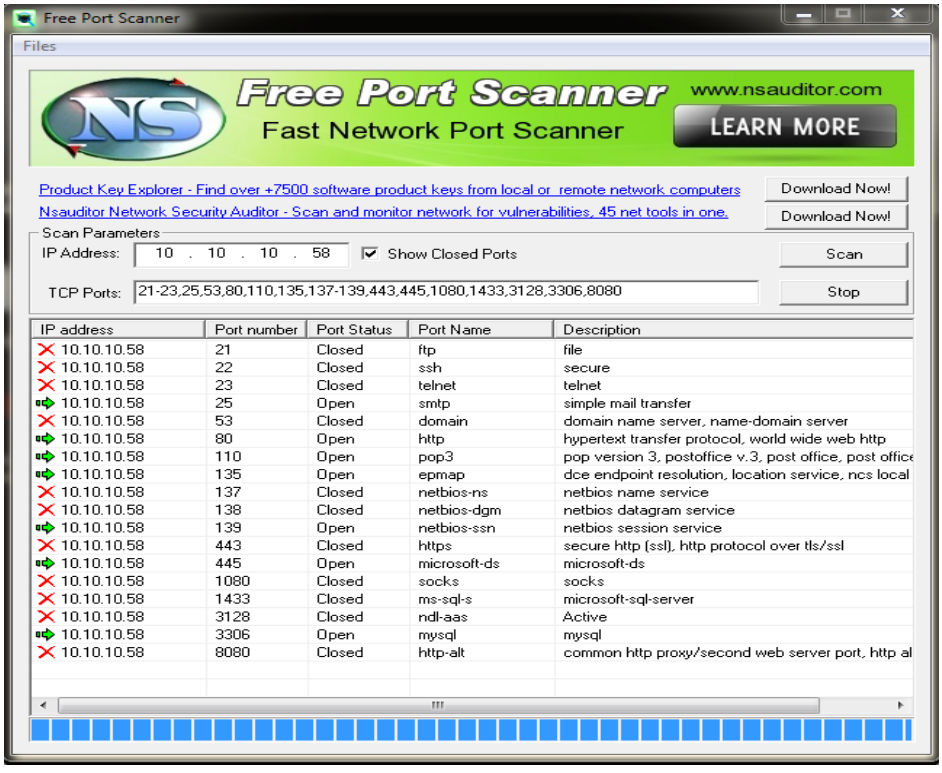


Figura 3.23: Escaneo transferencia de datos con Ping Tool



Utilizando Free Port Scanner: Herramienta usada para verificar los puertos abiertos al momento de la transmisión de información. Se ejecutó la herramienta al acceder al servicio de Internet desde una PC perteneciente a la Subgerencia de informática y Sistemas.

Fig. 3.24: Monitoreo de transmisión de información con Free Port Scanner



Utilizando Wireshark Network Analyzer: Analizador de red. Esta herramienta nos permite identificar los paquetes transmitidos y perdidos al momento de realizar el proceso de transmisión de información en la municipalidad

Pantalla de resultados de paquetes enviados y paquetes recibidos:

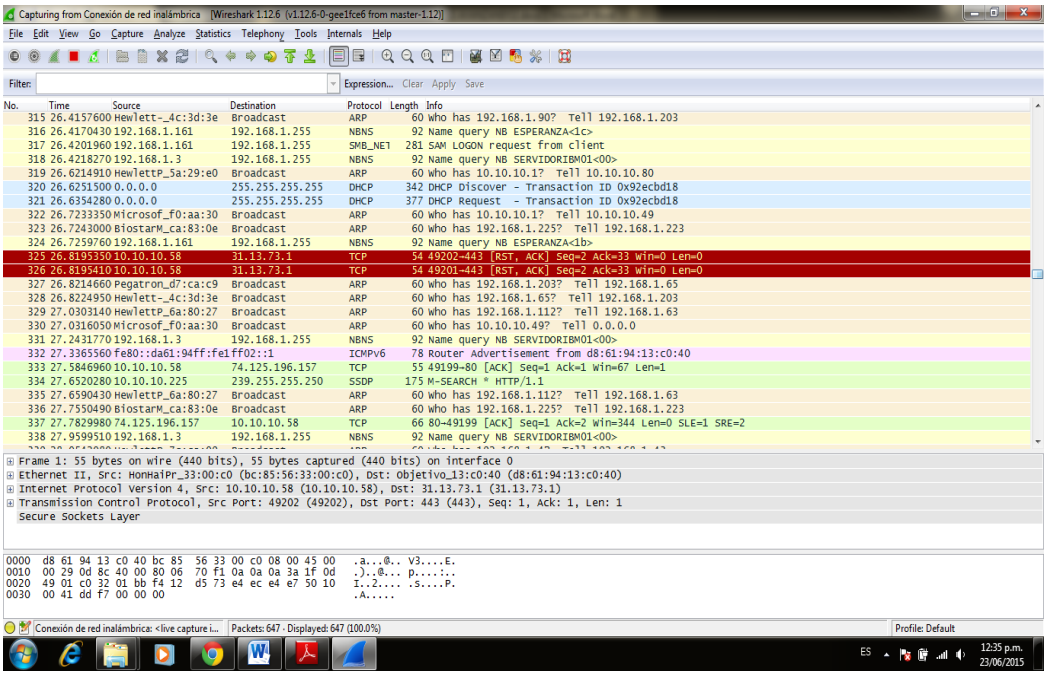


Fig. 3.25**:** Monitoreo de paquetes transmitidos con red inalámbrica

Escaneando protocolos de red, durante el proceso de transmisión de información en la municipalidad, a través de la red inalámbrica.

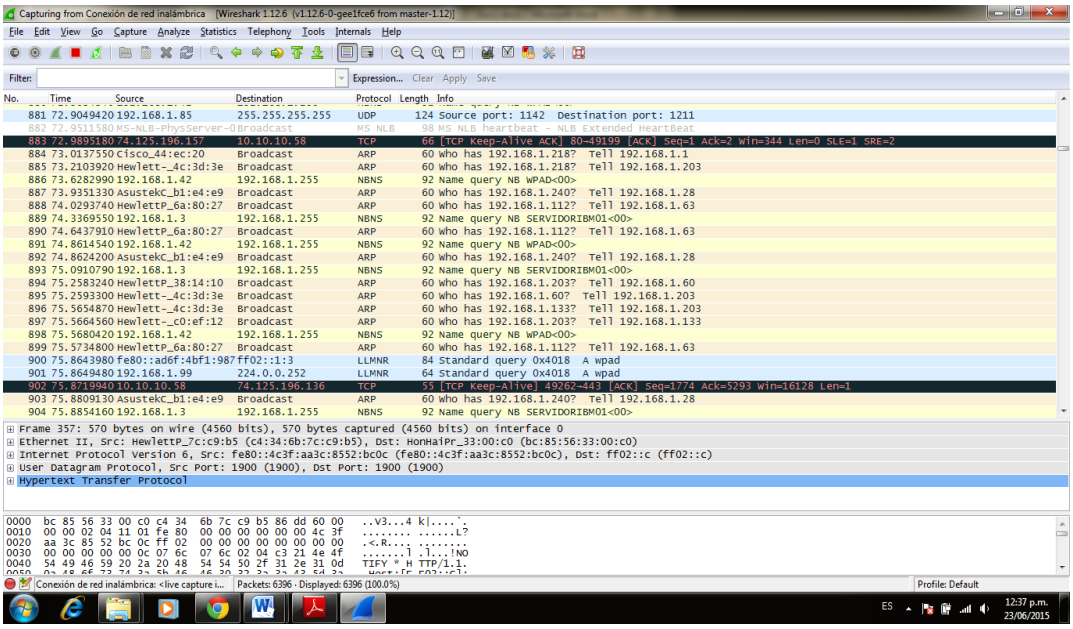


Fig. 3.26: Monitoreo de protocolos usando la red inalámbrica

3.1.3 Fase III Configuración de la Red

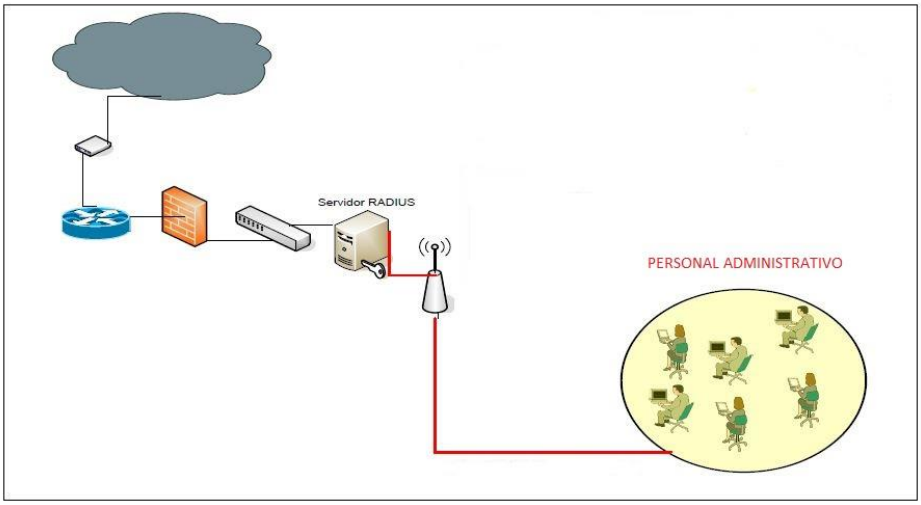
3.1.3.1 Distribución física de los usuarios.

Para nuestra realidad se han identificado solo un tipo de usuario que harán uso la red inalámbrica: personal administrativo pertenecientes a la Municipalidad Distrital de la Esperanza, con diferentes políticas se seguridad para los mismos.

- **Personal Administrativo**

  Este grupo de usuarios es aquel conformado por los trabajadores de la Municipalidad Distrital de la Esperanza, los cuales diariamente se encuentran intercambiando información, por lo que se ha visto conveniente crearle una, sistema de gestión de acceso, el cual los usuarios deberán registrarse previamente en el Servidor Radius que será implementado para la autenticación de usuarios.

Fig. 3.34: Diagrama del personal con servidor Radius.



3.1.4 Fase IV Consideraciones de Hardware/Software y Seguridad

Para el presente proyecto se han evaluado los recursos de hardware y software necesarios los mismos que describimos a continuación.

3.1.4.1 Definición de las características del Hardware y Software

1. Características del Hardware

a. Solución con Access Point TP-Link TL-WA7210N

Fig. 3.35: Access Point TP LINK- TL-WA7210N

3.1.4.2 Definición de niveles de seguridad

Fig. 3.41: Configuración de WPA/WPA2 en Access Point

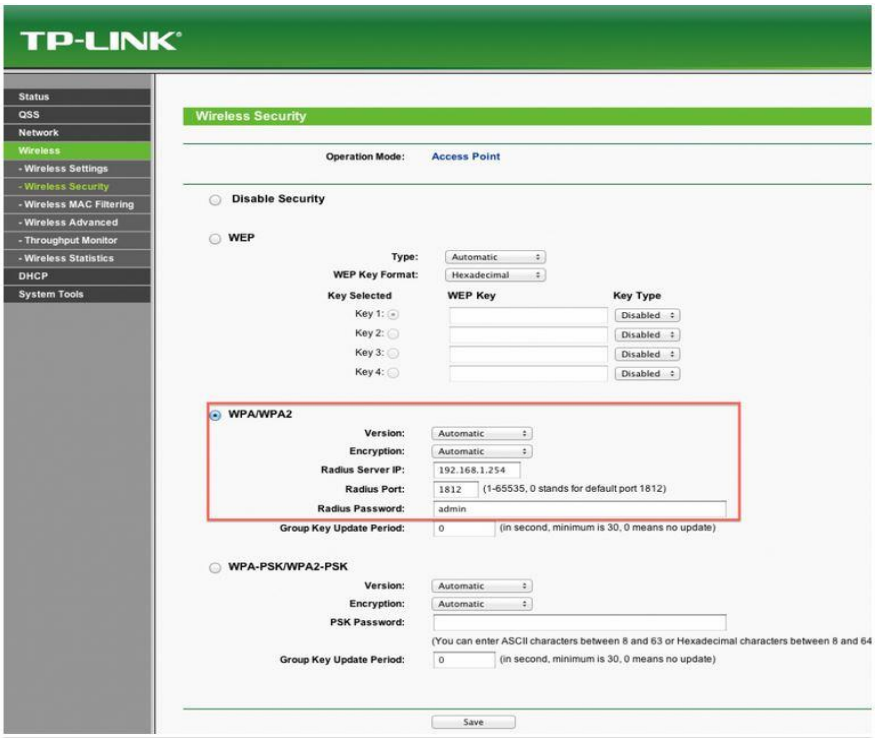
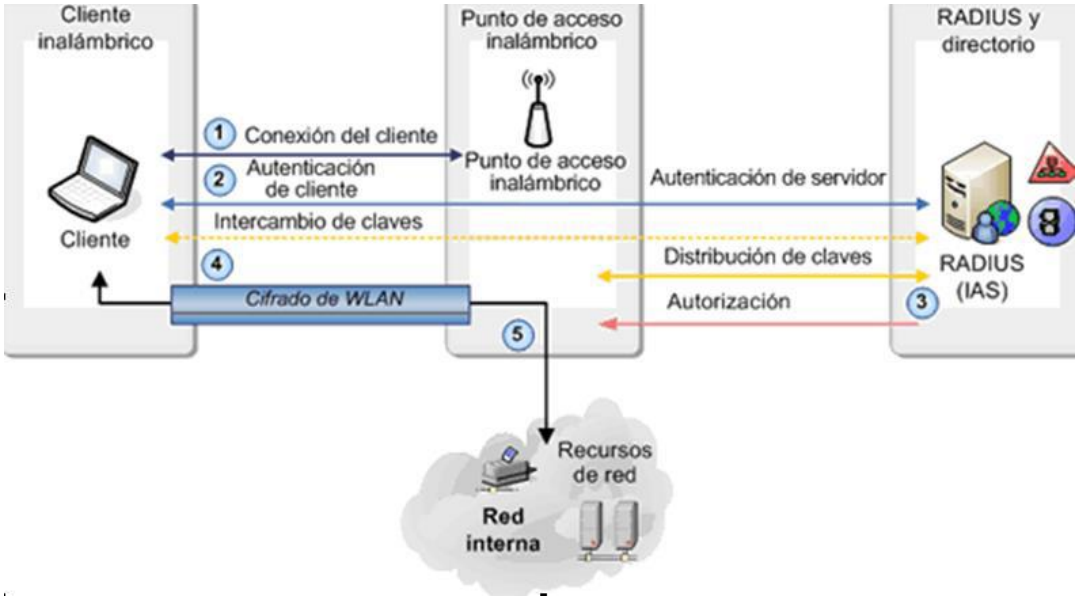


Fig. 3.42: Funcionamiento de Servidor Radius



3.1.5 Fase V Consideraciones de Implementación y Costos

3.1.5.1 Implementación de la red.

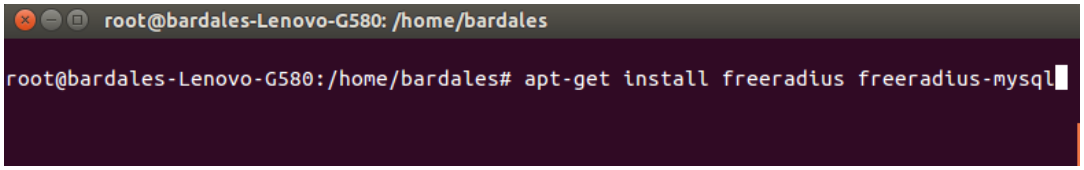
Instalación y configuración del Servidor Radius

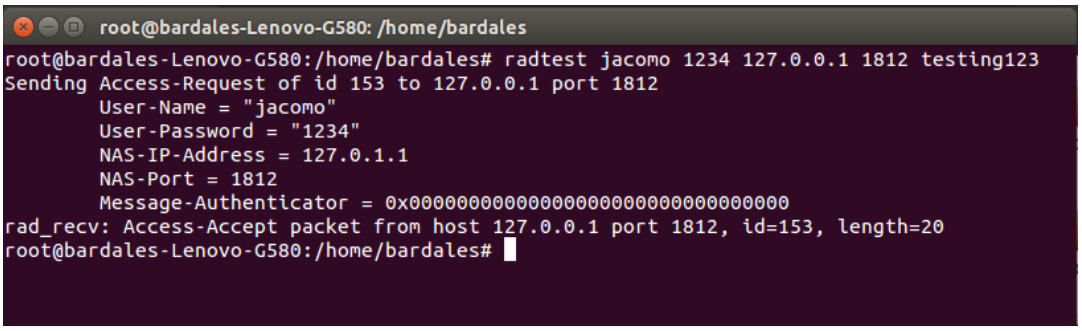
Los pasos que usaremos para lograrlo son los siguientes:

1. Instalación de FreeRadius
2. Instalación de Daloradius :Administrador de Radius

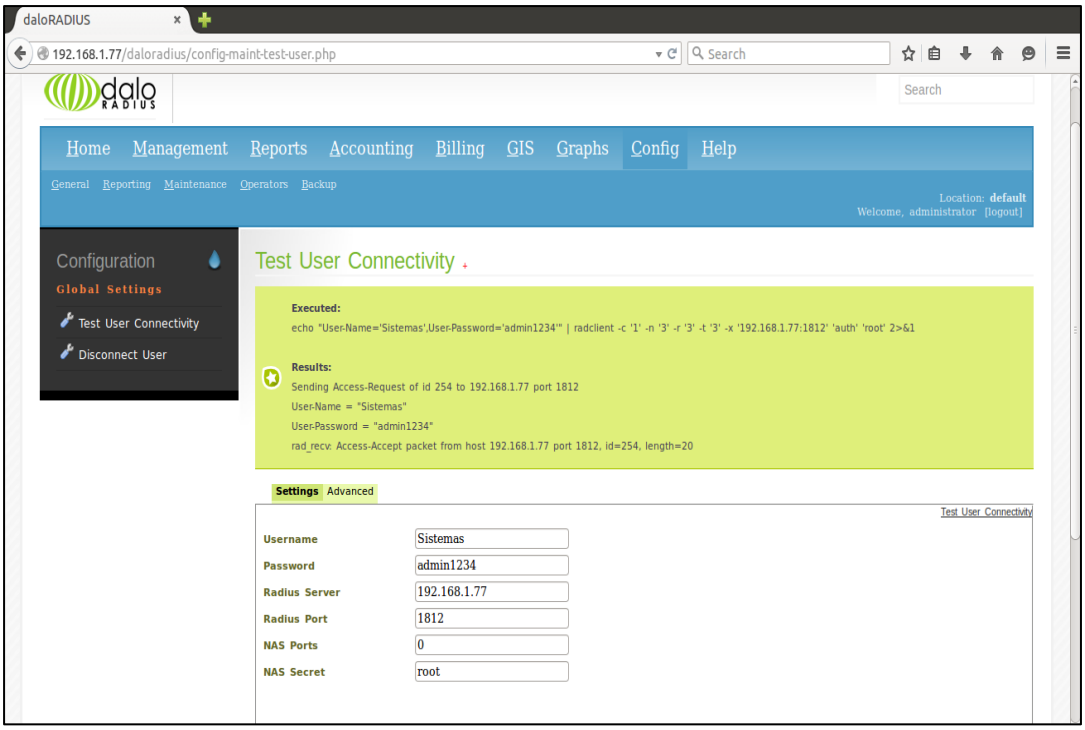
I. INSTALACIÓN DE FREERADIUS

Instalación y Verificación de FreeRadius.





II. DALORADIUS : ADMINISTRADOR DEL SERVIDOR RADIUS



3.2 Contrastación de Hipótesis

3.2.1 Nivel de Satisfacción de los Trabajadores.

a) Cálculo para hallar el nivel de satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza antes de implementación el sistema propuesto.

Se realizó una encuesta a los trabajadores de la municipalidad. Los datos obtenidos han sido tabulados, para calcular los resultados pertinentes en la investigación teniendo en cuenta los siguientes rangos:

Tabla 3.25 Escala de Likert

Rango	Nivel de Satisfacción	Peso
MB	Muy Bueno	5
B	Bueno	4
R	Regular	3
M	Malo	2
MM	Muy Malo	1

Los valores se calcularon en base a las respuestas proporcionadas por 93 trabajadores (muestra).

Para realizar la ponderación correspondiente de las preguntas aplicadas en las encuestas se tomó como base la escala de Likert (rango de ponderación: [1-5]).

Para cada pregunta se contabilizó una frecuencia de ocurrencia; para cada una de las posibles respuestas (05) por cada encuestado (93), luego se procedió a realizar el cálculo del puntaje total y puntaje promedio, como se detalla.

Se tiene que:

$$PT_i = \sum_{j=1}^{5} \left(F_{ij} * P_j\right)$$

Dónde:

$\boldsymbol{PT_i} =$ Puntaje Total de la pregunta i $-$ ésima
$\boldsymbol{F_{ij}} =$ Frecuencia j $-$ ésima de la Pregunta i $-$ ésima
$\boldsymbol{P_j} =$ Peso j $-$ ésima.

El cálculo del promedio ponderado por cada pregunta vendría a ser:

$$\overline{PP_i} = \frac{PT_i}{n}$$

Dónde:

$\overline{PP_i} =$ Promedio de Puntaje Total de la pregunta $\quad$ i − ésima.

$n \;=\; 93$ trabajadores.

En la tabla siguiente tabla podemos observar la ponderación de los criterios de evaluación del Indicador Cualitativo de Nivel Satisfacción del Cliente con los valores obtenidos en las encuestas realizadas con el Sistema Actual.

Tabla 3.26: Tabulación del nivel de Satisfacción de los Trabajadores (Pre-test)

		MB	B	R	M	MM	Puntaje	Puntaje
Nº	Pregunta	5	4	3	2	1	Total	Promedio
1	El nivel de seguridad de la información de la institución es adecuada	8	7	11	36	31	204	2.19
2	¿Cómo calificaría el servicio de internet	5	10	10	41	27	204	2.19
3	¿Cómo calificaría el tiempo que demora en acceder al sistema informático de la institución	3	12	15	40	23	211	2.27
4	¿Obtiene información a tiempo?	0	15	11	33	34	193	2.08
5	¿Cómo considera el tiempo de descarga de archivos?	0	12	10	31	40	180	1.94
6	¿Cómo calificaría el sistema con el que cuenta actualmente?	0	8	16	37	32	186	2.00
						∑	1178	12.67

b) Cálculo para hallar el nivel de satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza con la implementación del sistema propuesto.

A continuación, se muestra los resultados de la encuesta aplicada para conocer el Nivel de Satisfacción de los clientes con el Sistema propuesto.

Tabla 3.27: Tabulación del nivel de Satisfacción de los Trabajadores (Post-test)

		MB	B	R	M	MM	Puntaje	Puntaje
Nº	Pregunta	5	4	3	2	1	Total	Promedio
1	El nivel de seguridad de la información de la institución es adecuada	45	35	13	0	0	404	4.34
2	¿Cómo calificaría el servicio de internet	38	40	15	0	0	395	4.25
3	¿Cómo calificaría el tiempo que demora en acceder al sistema informático de la institución	48	36	9	0	0	411	4.42
4	¿Obtiene información a tiempo?	42	31	20	0	0	394	4.24
5	¿Cómo considera el tiempo de descarga de archivos?	30	37	26	0	0	376	4.04
6	¿Cómo calificaría el sistema con el que cuenta actualmente?	48	40	5	0	0	415	4.46
						∑	2395	25.75

En la siguiente tabla se podrá observar la contrastación de los resultados de las pruebas realizadas de Pre-Test y Post-Test.

Tabla 3.28: Contrastación de Pres & Post test

Pregunta	PRE TEST	POST TEST	Di	Di^2
1	2.19	4.34	-2.15	4.62
2	2.19	4.25	-2.06	4.24
3	2.27	4.42	-2.15	4.62
4	2.08	4.24	-2.16	4.66
5	1.94	4.04	-2.10	4.41
6	2.00	4.46	-2.46	6.05
∑	**12.67**	**25.75**	**-13.08**	**28.60**

Calculamos los niveles de satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza tanto para el sistema actual como para el sistema propuesto:

$$\boldsymbol{NSP_a} = \frac{\sum_{i=1}^{n} \boldsymbol{NSP_i}}{\boldsymbol{n}} = \frac{12.67}{6} = 2.11$$

$$\boldsymbol{NSP_s} = \frac{\sum_{i=1}^{n} \boldsymbol{NSP_i}}{\boldsymbol{n}} = \frac{25.75}{6} = 4.29$$

c) Definición de Variables

$\boldsymbol{NSP_a}$**:** Nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el sistema Actual.

$\boldsymbol{NSP_s}$**:** Nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el Sistema Propuesto.

d) Hipótesis Estadísticas

Hipótesis H0: 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.

H0: NSPa – NSPp >= 0

Hipótesis Ha: Nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el sistema actual es menor que el Nivel de satisfacción de trabajadores de la Municipalidad Distrital de la Esperanza con el sistema propuesto.

Ha: NSPIa – NSPp < 0

e) Nivel de significancia

El margen de error, ***Confiabilidad 95%,***

Haciendo uso de un nivel de significancia ***(α = 0.05) del 5%.*** Por lo tanto el ***nivel de confianza (1- α = 0.95)***, que representa al 95%.

Valor Crítico:

$$\boldsymbol{t_{\alpha=0.05}} = -2.015$$

Como = 0.05 y n-1 = 6 - 1 = 5 grados de libertad, la región de rechazo

consiste en aquellos valores de ***t*** menores que ***–t0.05*** = - 2.015 .

f) Resultados de la Hipótesis Estadística

Diferencia Promedio

$$\bar{D} = \frac{\sum_{i=1}^{n} D_i}{n}$$

$$\bar{D} = \frac{\sum_{i=1}^{n} D_i}{6} = \frac{-13{,}8}{6}$$

$$\bar{D} = -2.3$$

Desviación Estándar

$$S_D{}^2 = \frac{n\sum_{i=1}^{n} D_i{}^2 - (n\sum_{i=1}^{n} D_i)^2}{n(n-1)}$$

$$S_D{}^2 = \frac{6(28{,}60) - (-13.08)^2}{6(6-1)}$$

$$S_D{}^2 = 0.17$$

Cálculo de T

$$t = \frac{\bar{D}\sqrt{n}}{\sqrt{S_D}} = \frac{(-2.3)\sqrt{6}}{\sqrt{0.17}}$$

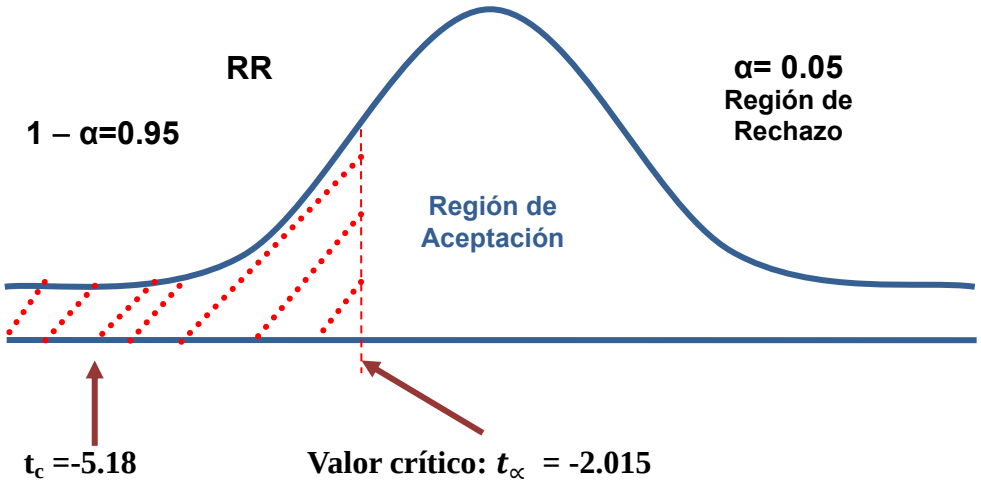
$$t = \frac{(-2.3)\sqrt{6}}{0.41}$$

$$t = -13.74$$

g) Conclusión

Puesto que: *tc* = -13.74 (*t*calculado) < *tα* = -2.015 (*t*tabular), estando este valor dentro de la región de rechazo, se concluye que Va – Vp < 0, se rechaza **H0** y **Ha** es aceptada, por lo tanto se prueba la validez de la hipótesis con un nivel de error de 5% (= 0.05), siendo la implementación del sistema propuesto mejoraría el nivel de satisfacción de

los trabajadores de la Municipalidad Distrital de la Esperanza.

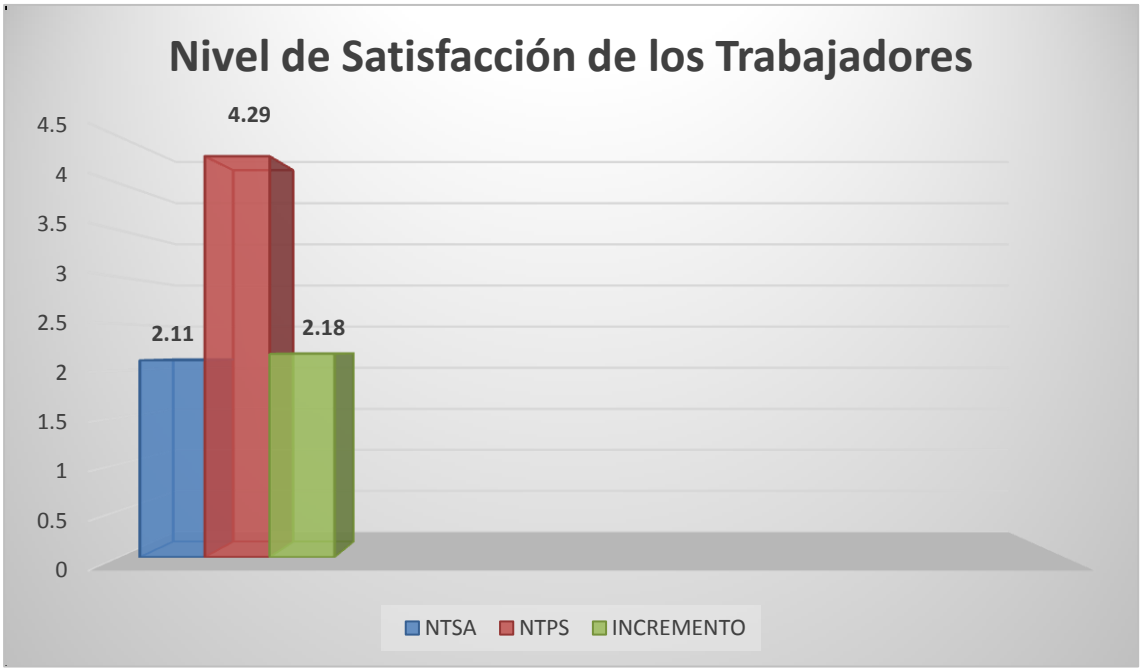


Comparación del Indicador Nivel De Satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza con el sistema actual (NTSA) y Nivel De Satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza con el propuesto (NTSP).

Tabla 3.29: Comparación del Indicador NSPA y NSPS

NTSA		NTSP		Incremento	
(1 - 5)	%	(1 - 5)	%	(1 - 5)	%
2.11	42.2	4.29	85.8	2.18	43.6

Gráfico 3.1: Nivel de Satisfacción de los trabajadores



3.2.2 Controlar el acceso inalámbrico para los usuarios autorizados a conectarse a los servicios que ofrece la red

a) Definición de las variables.

Ca = Control del acceso inalámbrico para los usuarios autorizados con el sistema actual.

Cp = Control del acceso inalámbrico para los usuarios autorizados con el sistema propuesto.

b) Hipótesis estadística

Hipótesis nula: Control del acceso inalámbrico para los usuarios autorizados con el sistema actual antes de implementado el sistema propuesto es menor o igual al Control el acceso inalámbrico para los usuarios autorizados luego de implementar el sistema propuesto.

$$\boldsymbol{H_0 = C_a - C_p \leq 0}$$

Hipótesis alternativa: Control del acceso inalámbrico para los usuarios autorizados con el sistema actual antes de implementado el sistema propuesto mayor al Control el acceso inalámbrico para los usuarios autorizados luego de implementar el sistema propuesto.

$$\boldsymbol{H_a = C_a - C_p > 0}$$

c) Nivel de Significancia

Se define el margen de error, **confiabilidad 95%.**

Usando un nivel de significancia **($\propto$ = 0.05)** del 5%. Por lo tanto el nivel de confianza **(1 - $\propto$ = 0.95)** será del 95%.

d) Estadística de prueba

Debido a que la muestra es 93 (n=93), se usará la distribución normal (Z).

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

$$\sigma^2 = \frac{\sum_{i=1}^{n} X_i - \bar{X}}{n}$$

$$Z_c = \frac{\overline{X_A} - \overline{X_D} + X_A - X_D}{\sqrt{\left(\frac{{\sigma_A}^2}{n_A} + \frac{{\sigma_D}^2}{n_D}\right)}}$$

Para calcular el control del acceso inalámbrico para los usuarios autorizados de Municipalidad Distrital de la Esperanza se ha estimado un universo de 93 reportes, por cada uno de los trabajadores que fueron extraídos de la muestra, los cuáles se estudiarán el acceso a información en minutos, tomadas en un periodo de un mes.

Tabla 3. 30: Control del acceso inalámbrico para los usuarios

Nº	ANTES	DESPUÉS	ANTES	DESPUÉS	ANTES	DESPUÉS
	C_{ai}	C_{pi}	$C_{ai} - \overrightarrow{C_a}$	$C_{pi} - \overrightarrow{C_p}$	$(C_{ai} - \overrightarrow{C_a})^2$	$(C_{pi} - \overrightarrow{C_p})^2$
1	75	66	6.09	10.35	37.04	107.22
2	66	52	-2.91	-3.65	8.49	13.29
3	96	73	27.09	17.35	733.65	301.19
4	63	48	-5.91	-7.65	34.98	58.45
5	88	66	19.09	10.35	364.28	107.22
6	66	42	-2.91	-13.65	8.49	186.19
7	82	65	13.09	9.35	171.24	87.51
8	52	42	-16.91	-13.65	286.08	186.19
9	46	35	-22.91	-20.65	525.05	426.22
10	52	39	-16.91	-16.65	286.08	277.06
11	62	43	-6.91	-12.65	47.80	159.90
12	78	61	9.09	5.35	82.56	28.67
13	62	58	-6.91	2.35	47.80	5.55
14	94	77	25.09	21.35	629.31	456.03
15	60	56	-8.91	0.35	79.46	0.13
16	82	68	13.09	12.35	171.24	152.64
17	69	52	0.09	-3.65	0.01	13.29
18	82	59	13.09	3.35	171.24	11.25
19	73	63	4.09	7.35	16.70	54.09
20	83	72	14.09	16.35	198.42	267.48
21	56	52	-12.91	-3.65	166.77	13.29
22	62	50	-6.91	-5.65	47.80	31.87
23	53	48	-15.91	-7.65	253.25	58.45
24	48	38	-20.91	-17.65	437.39	311.35
25	66	53	-2.91	-2.65	8.49	7.00
26	74	60	5.09	4.35	25.87	18.96

27	58	42	-10.91	-13.65	119.11	186.19
28	64	55	-4.91	-0.65	24.15	0.42
29	57	44	-11.91	-11.65	141.94	135.61
30	52	35	-16.91	-20.65	286.08	426.22
31	67	53	-1.91	-2.65	3.66	7.00
32	62	59	-6.91	3.35	47.80	11.25
33	70	62	1.09	6.35	1.18	40.38
34	81	66	12.09	10.35	146.07	107.22
35	69	56	0.09	0.35	0.01	0.13
36	62	48	-6.91	-7.65	47.80	58.45
37	68	60	-0.91	4.35	0.84	18.96
38	72	60	3.09	4.35	9.52	18.96
39	88	66	19.09	10.35	364.28	107.22
40	85	64	16.09	8.35	258.76	69.80
41	94	78	25.09	22.35	629.31	499.74
42	60	49	-8.91	-6.65	79.46	44.16
43	82	65	13.09	9.35	171.24	87.51
44	69	45	0.09	-10.65	0.01	113.32
45	82	69	13.09	13.35	171.24	178.35
46	76	60	7.09	4.35	50.21	18.96
47	83	62	14.09	6.35	198.42	40.38
48	57	39	-11.91	-16.65	141.94	277.06
49	62	52	-6.91	-3.65	47.80	13.29
50	53	37	-15.91	-18.65	253.25	347.64
51	49	41	-19.91	-14.65	396.57	214.48
52	65	50	-3.91	-5.65	15.32	31.87
53	72	63	3.09	7.35	9.52	54.09
54	50	42	-18.91	-13.65	357.74	186.19
55	69	66	0.09	10.35	0.01	107.22
56	75	60	6.09	4.35	37.04	18.96
57	66	56	-2.91	0.35	8.49	0.13
58	96	79	27.09	23.35	733.65	545.45
59	63	54	-5.91	-1.65	34.98	2.71
60	88	62	19.09	6.35	364.28	40.38
61	66	48	-2.91	-7.65	8.49	58.45
62	82	66	13.09	10.35	171.24	107.22
63	55	44	-13.91	-11.65	193.60	135.61
64	64	50	-4.91	-5.65	24.15	31.87
65	52	48	-16.91	-7.65	286.08	58.45
66	62	40	-6.91	-15.65	47.80	244.77
67	78	67	9.09	11.35	82.56	128.93

68	62	55	-6.91	-0.65	47.80	0.42
69	55	46	-13.91	-9.65	193.60	93.03
70	92	77	23.09	21.35	532.96	456.03
71	84	62	15.09	6.35	227.59	40.38
72	62	43	-6.91	-12.65	47.80	159.90
73	82	68	13.09	12.35	171.24	152.64
74	76	66	7.09	10.35	50.21	107.22
75	83	77	14.09	21.35	198.42	456.03
76	57	48	-11.91	-7.65	141.94	58.45
77	62	45	-6.91	-10.65	47.80	113.32
78	56	43	-12.91	-12.65	166.77	159.90
79	49	38	-19.91	-17.65	396.57	311.35
80	65	55	-3.91	-0.65	15.32	0.42
81	72	68	3.09	12.35	9.52	152.64
82	56	44	-12.91	-11.65	166.77	135.61
83	69	58	0.09	2.35	0.01	5.55
84	75	54	6.09	-1.65	37.04	2.71
85	83	65	14.09	9.35	198.42	87.51
86	90	77	21.09	21.35	444.62	456.03
87	63	58	-5.91	2.35	34.98	5.55
88	64	56	-4.91	0.35	24.15	0.13
89	51	45	-17.91	-10.65	320.91	113.32
90	58	44	-10.91	-11.65	119.11	135.61
91	69	52	0.09	-3.65	0.01	13.29
92	82	69	13.09	13.35	171.24	178.35
93	77	62	8.09	6.35	65.38	40.38
Sumatoria	6409	5175			**14635.31**	**11551.29**
Promedio	68.91	55.65				
Varianza					**157.37**	**124.21**

En la tabla 3.2 denominada Control del acceso inalámbrico para los usuarios, muestra en la primera columna la cantidad (N) de reportes de ingresos al sistemas durante el mes, antes de implementado el sistema (Ca) se calcula a partir de los datos obtenido de la observación, y luego se compara con el promedio obtenido del mismo dato después de implementado el sistema (Cp).Se calcula que la varianza de los datos obtenidos en la observación

Promedio:

$$\overline{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

$$\overline{N_a} = \frac{\sum_{i=1}^{n} C_{ai}}{n_a} = \frac{6409}{93} = 68.91$$

$$\overline{N_p} = \frac{\sum_{i=1}^{n} C_{pi}}{n_s} = \frac{5175}{93} = 55.65$$

Varianza:

$$\sigma_a{}^2 = \frac{\sum_{i=1}^{n} C_{ai} - \overline{C_a}^2}{n_a} = \frac{14635.31}{93} = 157.37$$

$$\sigma_s{}^2 = \frac{\sum_{i=1}^{n} C_{pi} - \overline{C_p}^2}{n_s} = \frac{11551.29}{93} = 124.21$$

Cálculo de Z:

$$Z_c = \frac{\overline{C_a} - \overline{C_p}}{\sqrt{\left(\frac{\sigma_a{}^2}{n_a} + \frac{\sigma_s{}^2}{n_s}\right)}}$$

$$Z_c = \frac{(68.91 - 55.65)}{1.74} = 7.62$$

e) Región crítica

Para α =0.05, en la Tabla N° 5.2, (Anexo N° 13) encontramos Zα = 1.645. Entonces la región critica de la prueba es Zc = < 1.645 >.

f) Conclusión

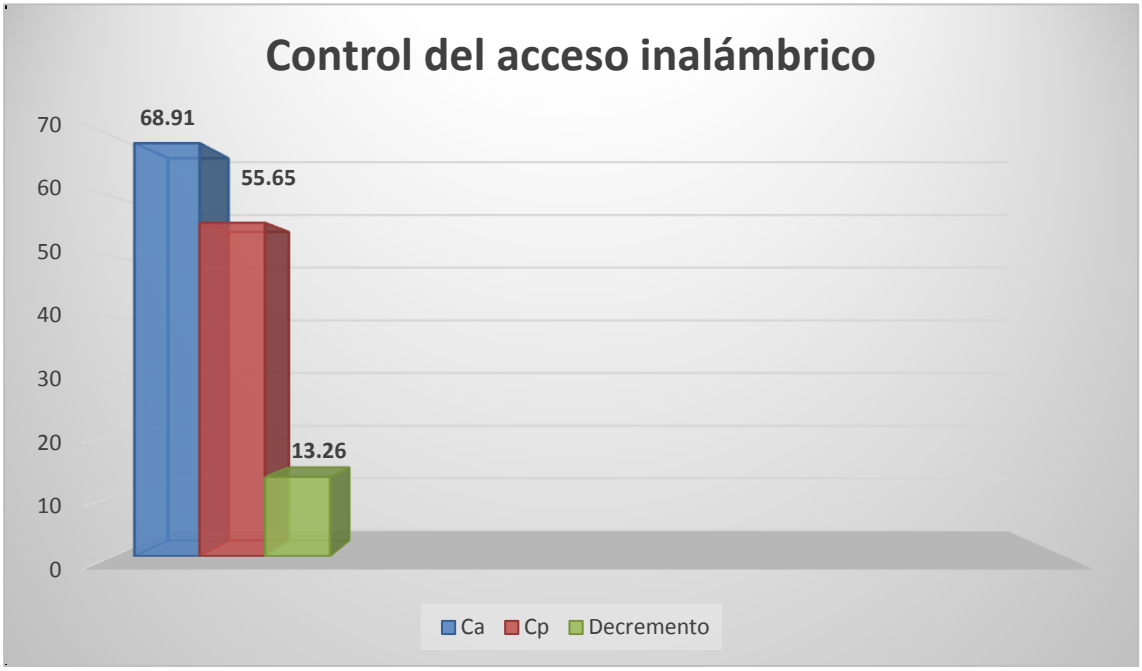
Puesto que ZC = 7.62 calculado, es mayor que Zα = 1.645 y estando este valor dentro de la región de rechazo < 1.645, >, entonces se rechaza H0 y por consiguiente se acepta Ha.

Comparación del Indicador Control del acceso inalámbrico para los usuarios autorizados el sistema actual (Ca) y Control del acceso inalámbrico para los usuarios autorizados con el sistema Propuesto (Cp) , dado en minutos.

Tabla 3.31: Comparación del Indicador Ca y Cp

Ca		Cp		Decremento	
	%		%		%
68.91	100.00	55.65	80.75	13.26	19.25

Gráfico 3. 1: Control del Acceso Inalámbrico



3.2.3 Velocidad de la Información

a) Definición de las variables.

Va = Velocidad de la información con el sistema actual

Vp = Velocidad de la información con la Implementación del Sistema propuesto.

b) Hipótesis estadística

Hipótesis nula: Velocidad de la información de los trabajadores de la Municipalidad Distrital dela Esperanza antes de implementado el sistema propuesto es menor o igual a la velocidad de la información de los trabajadores luego de implementar el sistema propuesto.

$$\boldsymbol{H_0 = V_a - V_p \leq 0}$$

Hipótesis alternativa: Velocidad de la información de los trabajadores de la Municipalidad Distrital de la Esperanza antes de implementado el sistema propuesto es mayor a la velocidad de la información de los trabajadores luego de implementar el sistema propuesto.

$$\boldsymbol{H_a = V_a - V_p > 0}$$

c) Nivel de Significancia

Se define el margen de error, **confiabilidad 95%.**

Usando un nivel de significancia **($\propto$ = 0.05)** del 5%. Por lo tanto el nivel de confianza **(1 - $\propto$ = 0.95)** será del 95%.

d) Estadística de prueba

Debido a que la muestra es 93 (n=93), se usará la distribución normal (Z).

$$\overline{\boldsymbol{X}} = \frac{\sum_{i=1}^{n} \boldsymbol{X_i}}{\boldsymbol{n}}$$

$$\boldsymbol{\sigma^2} = \frac{\sum_{i=1}^{n} \boldsymbol{X_i} - \overline{\boldsymbol{X}}}{\boldsymbol{n}}$$

$$\boldsymbol{Z_c} = \frac{\overline{\boldsymbol{X_A}} - \overline{\boldsymbol{X_D}} + \boldsymbol{X_A} - \boldsymbol{X_D}}{\sqrt{\left(\frac{\boldsymbol{\sigma_A}^2}{\boldsymbol{n_A}} + \frac{\boldsymbol{\sigma_D}^2}{\boldsymbol{n_D}}\right)}}$$

Para calcular la velocidad de la información de los trabajadores de la Municipalidad Distrital de la Esperanza se ha estimado un universo de 93 reportes, por cada uno de los trabajadores que fueron extraídos de la muestra, los cuáles se estudiarán en la búsqueda de la información en segundos, tomadas en un periodo de un mes.

Tabla 3. 32: Velocidad de la Información

Nº	ANTES	DESPUÉS	ANTES	DESPUÉS	ANTES	DESPUÉS
	V_{ai}	V_{pi}	$V_{ai} - \overrightarrow{V_a}$	$V_{pi} - \overrightarrow{V_p}$	$(V_{ai} - \overrightarrow{V_a})^2$	$(V_{pi} - \overrightarrow{V_p})^2$
1	1440	1100	-919.75	-562.43	845945.01	316327.63
2	1728	1000	-631.75	-662.43	399111.46	438813.65
3	1152	900	-1207.75	-762.43	1458666.56	581299.67
4	1402	920	-957.75	-742.43	917290.21	551202.46
5	2550	1400	190.25	-262.43	36194.04	68869.56
6	1950	1202	-409.75	-460.43	167897.27	211995.88
7	1500	1100	-859.75	-562.43	739174.68	316327.63
8	2700	1500	340.25	-162.43	115768.23	26383.54
9	2100	1520	-259.75	-142.43	67471.46	20286.34
10	2275	1602	-84.75	-60.43	7183.02	3651.80
11	1575	1300	-784.75	-362.43	615836.78	131355.58
12	1750	1228	-609.75	-434.43	371798.34	188729.52
13	1800	1080	-559.75	-582.43	313323.07	339224.83
14	1830	1320	-529.75	-342.43	280637.91	117258.38
15	2850	1500	490.25	-162.43	240342.43	26383.54
16	2250	1600	-109.75	-62.43	12045.65	3897.52
17	1710	1650	-649.75	-12.43	422178.56	154.51
18	1865	1220	-494.75	-442.43	244780.22	195744.40
19	1708	1030	-651.75	-632.43	424781.57	399967.84
20	1816	1008	-543.75	-654.43	295666.99	428278.77
21	1753	1222	-606.75	-440.43	368148.82	193978.68
22	2820	2210	460.25	547.57	211827.59	299832.79
23	1810	1250	-549.75	-412.43	302228.02	170098.59
24	2770	2060	410.25	397.57	168302.86	158061.82
25	1804	1610	-555.75	-52.43	308861.05	2748.92
26	2820	2040	460.25	377.57	211827.59	142559.02
27	1620	1207	-739.75	-455.43	547234.04	207416.58
28	1862	1515	-497.75	-147.43	247757.74	21735.64
29	2680	2252	320.25	589.57	102558.34	347592.66
30	1696	1360	-663.75	-302.43	440567.63	91463.97

31	2670	2132	310.25	469.57	96253.39	220495.88
32	1440	1271	-919.75	-391.43	845945.01	153217.53
33	1830	1270	-529.75	-392.43	280637.91	154001.39
34	2100	1618	-259.75	-44.43	67471.46	1974.03
35	2400	2287	40.25	624.57	1619.85	390087.55
36	1800	1600	-559.75	-62.43	313323.07	3897.52
37	2850	2400	490.25	737.57	240342.43	544009.35
38	1440	1200	-919.75	-462.43	845945.01	213841.60
39	1728	1400	-631.75	-262.43	399111.46	68869.56
40	1152	950	-1207.75	-712.43	1458666.56	507556.66
41	1200	1020	-1159.75	-642.43	1345026.30	412716.44
42	2550	1904	190.25	241.57	36194.04	58356.01
43	1950	1218	-409.75	-444.43	167897.27	197518.12
44	1560	1316	-799.75	-346.43	639604.36	120013.82
45	2710	2290	350.25	627.57	122673.18	393843.97
46	2100	1815	-259.75	152.57	67471.46	23277.57
47	2275	2118	-84.75	455.57	7183.02	207543.93
48	1570	1256	-789.75	-406.43	623709.31	165185.43
49	1650	1498	-709.75	-164.43	503748.88	27037.26
50	1776	1234	-583.75	-428.43	340767.20	183552.36
51	2840	2444	480.25	781.57	230637.48	610851.50
52	2698	2045	338.25	382.57	114411.24	146359.72
53	1730	1204	-629.75	-458.43	396588.45	210158.16
54	1890	2280	-469.75	617.57	220667.59	381392.57
55	2632	2296	272.25	633.57	74118.60	401410.81
56	2890	2032	530.25	369.57	281162.21	136581.91
57	2600	2211	240.25	548.57	57718.77	300928.93
58	2200	1804	-159.75	141.57	25520.92	20042.03
59	2120	1980	-239.75	317.57	57481.35	100850.64
60	1642	1456	-717.75	-206.43	515168.92	42613.39
61	1868	1607	-491.75	-55.43	241820.71	3072.50
62	2642	2452	282.25	789.57	79663.55	623420.62
63	2810	2330	450.25	667.57	202722.64	445649.56
64	1650	1472	-709.75	-190.43	503748.88	36263.63
65	1440	1260	-919.75	-402.43	845945.01	161949.99
66	1728	1690	-631.75	27.57	399111.46	760.10
67	2550	2210	190.25	547.57	36194.04	299832.79
68	2700	2080	340.25	417.57	115768.23	174364.62
69	2275	2012	-84.75	349.57	7183.02	122199.11
70	1750	1442	-609.75	-220.43	371798.34	48589.43
71	1830	1666	-529.75	3.57	280637.91	12.74

72	2850	2490	490.25	827.57	240342.43	684871.93
73	1710	1522	-649.75	-140.43	422178.56	19720.62
74	1753	1300	-606.75	-362.43	368148.82	131355.58
75	2770	2400	410.25	737.57	168302.86	544009.35
76	1804	1420	-555.75	-242.43	308861.05	58772.36
77	2820	2464	460.25	801.57	211827.59	642514.29
78	1862	1448	-497.75	-214.43	247757.74	45980.27
79	2680	2260	320.25	597.57	102558.34	357089.78
80	1696	1452	-663.75	-210.43	440567.63	44280.83
81	2650	2110	290.25	447.57	84243.50	200318.81
82	1450	1280	-909.75	-382.43	827649.95	146252.79
83	1820	1520	-539.75	-142.43	291332.96	20286.34
84	2760	2200	400.25	537.57	160197.91	288981.39
85	2226	1902	-133.75	239.57	17889.78	57393.73
86	1890	1620	-469.75	-42.43	220667.59	1800.31
87	2100	1822	-259.75	159.57	67471.46	25462.55
88	2988	2588	628.25	925.57	394694.68	856679.63
89	29100	2810	26740.25	1147.57	715040826.30	1316916.66
90	1900	1524	-459.75	-138.43	211372.53	19162.89
91	1540	1252	-819.75	-410.43	671994.47	168452.87
92	1776	1388	-583.75	-274.43	340767.20	75311.88
93	2490	2158	130.25	495.57	16964.36	245589.52
Sumatoria	219457	154606			**745203685.31**	**20267146.80**
Promedio	2359.75	1662.43				
Varianza					**8012942.85**	**217926.31**

En la tabla 3.32 denominada velocidad de la información de los trabajadores de la Municipalidad Distrital de la Esperanza, muestra en la primera columna la cantidad (N) de reportes de ingresos al sistemas durante el mes, antes de implementado el sistema (Va) se calcula a partir de los datos obtenido de la observación, y luego se compara con el promedio obtenido del mismo dato después de implementado el sistema (Vp).Se calcula que la varianza de los datos obtenidos en la observación

Promedio:

$$\overline{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

$$\overline{V_a} = \frac{\sum_{i=1}^{n} V_{ai}}{n_a} = \frac{219457}{93} = 2359.75$$

$$\overline{V_p} = \frac{\sum_{i=1}^{n} V_{pi}}{n_s} = \frac{154606}{93} = 1662.43$$

Varianza:

$$\sigma_a{}^2 = \frac{\sum_{i=1}^{n} V_{ai} - \overline{V_a}^2}{n_a} = \frac{745203685.31}{93} = 8012942.85$$

$$\sigma_s{}^2 = \frac{\sum_{i=1}^{n} V_{pi} - \overline{V_p}^2}{n_s} = \frac{20267146.80}{93} = 217926.31$$

Cálculo de Z:

$$Z_c = \frac{\overline{V_a} - \overline{V_p}}{\sqrt{\left(\frac{\sigma_a{}^2}{n_a} + \frac{\sigma_s{}^2}{n_s}\right)}}$$

$$Z_c = \frac{(2359.75 - 1662.43)}{297.49} = 2.34$$

e) Región crítica

Para α =0.05, en la Tabla N° 5.2, (Anexo N° 13) encontramos Zα = 1.645. Entonces la región critica de la prueba es Zc = < 1.645 >.

f) Conclusión

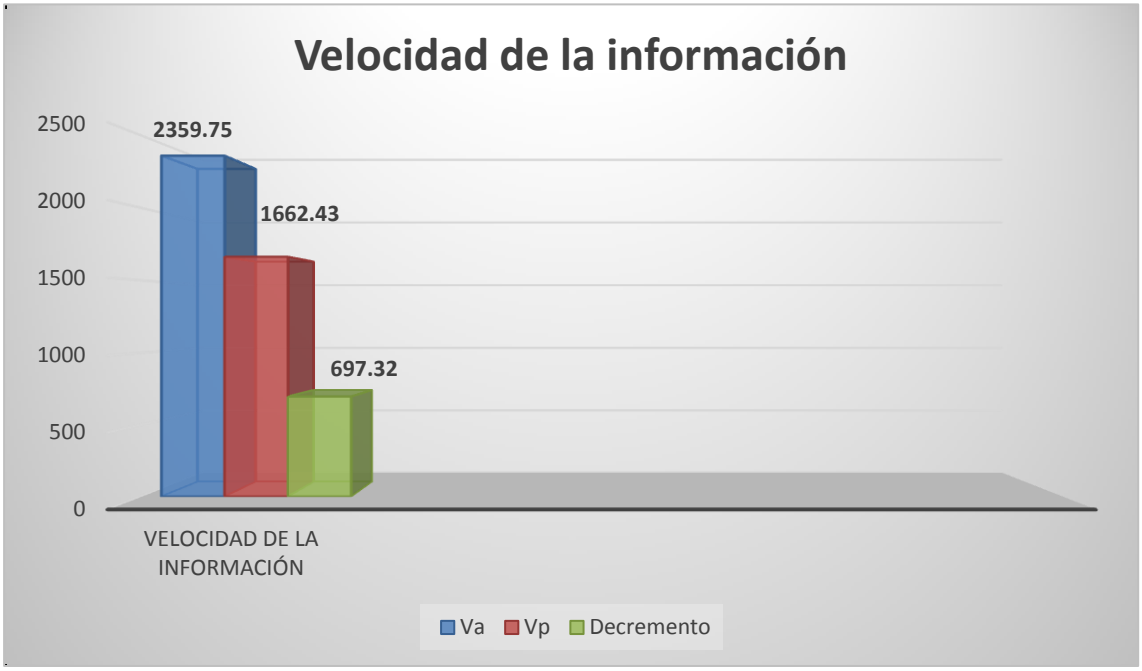
Puesto que ZC = 2.34 calculado, es mayor que Zα = 1.645 y estando este valor dentro de la región de rechazo < 1.645, >, entonces se rechaza H0 y por consiguiente se acepta Ha.

Comparación del Indicador de la Velocidad de la Información de los trabajadores de la Municipalidad Distrital de la Esperanza con el sistema actual (Va) y la velocidad de la Información de los trabajadores de la Municipalidad Distrital de la Esperanza con el sistema Propuesto (Vp) dado en segundos.

Tabla 3. 13: Comparación del Indicador Va y Vp

Va		Vp		Decremento	
	%		%		%
2359.75	100.00	1662.43	70.44	697.32	29.56

Gráfico 3. 2: Velocidad de la Información



CAPITULO IV

DISCUSIÓN

IV. DISCUSIÓN

Para empezar esta investigación, se aplicó encuestas y entrevistas con el fin de conocer la actualidad sobre el nivel de seguridad del acceso a la información del personal que labora en la municipalidad, como lo muestra en el anexo 2, al no existir políticas de seguridad, los usuarios internos y externos no autorizados tienen acceso libre a la información y recursos importantes de la Institución y pueden vulnerar sus niveles de protección y confiabilidad; de esa manera se logró un análisis profundo de la situación actual de la municipalidad para luego implementar la metodología de Jerry FitzGerald , con lo cual se obtuvo como producto el sistema propuesto.

Por lo tanto dentro de la Fase I denominada Consideraciones técnicas, en esta etapa se analizó la situación problemática actual de la municipalidad, la cual se obtuvo a partir de las entrevistas realizadas y a través de la observación, así como las características de la red actual, se puede observar en la tablas 3.8, 3.9 y 3.10 titulada Relación de equipos de comunicación en el Palacio Municipal, anexo 1 y anexo 2, sus diagramas físicos de la redes de dichos locales

En relación al estudio de factibilidad es uno de los aspectos más importantes durante el desarrollo de un proyecto porque permite saber si debe continuar o no con el desarrollo, el objetivo es evaluar y demostrar la viabilidad económica de la implementación de un sistema de gestión de acceso a una red wi-fi utilizando software libre para mejorar el nivel de seguridad del acceso a la información de los costos de este proyecto donde la tabla 3.23 titulada Flujo de Caja resume todos los ingresos y egresos proyectados en un periodo de 3 años. Se logró un valor anual neto de S/. 5046.01 Nuevos soles. Debido a que el VAN es mayor a cero (en VAN pág. 45.), se puede afirmar que es rentable el proyecto, se identificó la relación de beneficios y costo (B/C) al reemplazar los valores de VAB y VAC(pág. 46) por cada nuevo sol que se invierte, obtendremos una ganancia de S/.0.13, de acuerdo al flujo de caja se obtuvo el 41% de la tasa interna de retorno (TIR) es mayor que el BCP (15%) asumiendo que el proyecto es más rentable que colocar el capital invertido en un banco, mientras la tasa recuperación (1.62) representa que el capital invertido en el presente proyecto se recuperará en 1 año, 0.62*12 = 7 meses y 13 días. Los indicadores económicos corroboran la información obtenida en el flujo de caja.

Continuando con el desarrollo de la Metodología de Jerry FitzGerald, en la Fase II de Diseño de la Red se procedió a determinar el alcance de la red mediante los diagramas físicos de la red de datos propuestos para la implementación en el palacio municipal, anexos 1 y 2, como nos muestra en la fig. 3.11 al 3.19, así como la transmisión de la información por medio de la red, que se realizó mediante herramientas de testeo tales como Advanced Ip IP Scanner, Free Ports Scanner Ping Tool las cuales están graficadas en la Fig 3.20-al 3.14.

Luego se continuó con el desarrollo de la metodología, en la Fase III denominada Configuración de la Red, nos muestra las características técnicas de la red inalámbrica a implementarse, como su topología, tecnología, tipo seguridad, las cuáles son importantes para evitar la vulnerabilidad de la red ante ataques maliciosos, culminando con el desarrollo de esta etapa se pudo observar en la Fig. 3.34, la distribución física de los usuarios en este caso se identificó un usuario, el personal administrativo, con diferentes políticas de seguridad

Siguiendo con la Fase IV denominada Consideraciones de Hardware/Software y Seguridad se definió características del Hardware y Software necesarios para la implementación de la red tal como muestra la Fig. 3.35 titulada Access Point TP LINK- TL-WA7210N, donde describe las características y sus especificaciones generales, culminando con el desarrollo de la fase 4 en la Fig. 3.41: Configuración de WPA/WPA2 en Access Point definimos el nivel de seguridad con el cual vamos a llevar la implementación en nuestra caso emplearemos WPA/WPA2 con servidor Radius.

Por último la Fase V denominada Consideraciones de implementación y costos, se evaluaron las especificaciones finales del proyecto, así como la estructura de costos que implica la implementación de la red inalámbrica en la municipalidad los cuales están especificados en el estudio de factibilidad económica Ver Págs. 44. , y la implementación del sistema con un gestor web Daloradius que nos permitirá administrar nuestra servidor Radius desde un entorno gráfico (Ver pág. 90)

Así como se comprobó en la investigación realizada de **(Santisteban Rengifo, 2011)** , la instalación de un servidor Radius mejora el control del acceso a los servicios en red. En la presente investigación se determinó que control del acceso inalámbrico de los usuarios a conectarse a los servicios que ofrece la red de la Municipalidad Distrital de la Esperanza antes de implementado el sistema propuesto era de 68.91 minutos, lo que representa el 100 % y con el sistema propuesto es de 55.65 el cual representa el 80.71, es decir existe un decremento de 13.26 minutos, lo que representa un 19.25 % menos.

Luego de evaluar los resultados, se puede llegar a algo similar a la que se llegó en la investigación realizado por (García, 2012) la implementación de una WLAN con sistema de control mediante servidores AAA, mejora el rendimiento y la seguridad de la red , en el cual esta investigación se incrementó notoriamente como podemos observar en la Velocidad de la información de los trabajadores antes de implementado era de 2359.75 segundos, estos datos fueron tomados en un período de un mes mediante reportes, y con el sistema es de 1662.43 segundos, lo que representa un decremento de 697.32 segundos lo que representa el 29.56 % .

Otro punto importante de esta investigación es que se realizó con el servidor Radius y bajo una plataforma de software libre (Ubuntu 15.04), el cual no nos generó gastos en las licencias, a diferencia de la investigación mencionada la cual utilizo Servidor TACCAS que tiene licencia CISCO.

El relación al desempeño del personal manifiestan su malestar en el tiempo de demora y del servicio, según las encuestas mostradas en (Anexo 4) ,estas han sido tabuladas, de manera que se calculen los resultados obtenidos de acuerdo a los rangos que se presentan en la tabla 3.25 titulada Escala de Likert , podemos ver el rango de valores para evaluar el nivel de satisfacción del personal con el sistema actual, los valores se calcularon en base a las respuestas proporcionadas por el personal de al azar, ya que ellos se encuentran inmersos en el manejo del sistema actual.

De acuerdo a los resultados obtenidos mostraron que el nivel de satisfacción de los trabajadores de la municipalidad con el sistema actual es de 2.11, lo que representa el 42.2 % del puntaje máximo y con el sistema propuesto es de 4.29 es decir el 85.8 % , lo cual infiere que existe un incremento de 2.18 lo que representa un 43.8 % como se muestra en la tabla 3.28 titulada Contrastación de Pres & Post test

CAPITULO V

CONCLUSIONES

V. CONCLUSIONES

a) Con respecto a controlar el acceso inalámbrico para los usuarios autorizados a conectarse a los servicios que ofrece la red en la Municipalidad Distrital de la Esperanza con el sistema actual es de 68.91 minutos, en comparación al sistema propuesto que es 55.65 minutos , lo que determina una reducción de tiempo de 13.26 minutos , lo cual se redujo el número de intentos para acceder al control dela acceso en un 19.25 % con el Sistema De Gestión De Acceso A Una Red Wi-Fi Utilizando Software Libre para Mejorar El Nivel De Seguridad Del Acceso A La Información.

b) Se ha determinado que el indicador la velocidad de la información de los trabajadores de la Municipalidad Distrital de la Esperanza con el Sistema De Gestión De Acceso A Una Red Wi-Fi Utilizando Software Libre Para Mejorar El Nivel De Seguridad Del Acceso A La Información, se redujo el tiempo de búsqueda de la información en un 29.56 % después de implementado el sistema propuestos.

c) El indicador de nivel de satisfacción de los trabajadores de la Municipalidad Distrital de la Esperanza, siendo la implementación del sistema propuesto una mejoría en el incremento del nivel de satisfacción en un 43.6% debido al Sistema De Gestión De Acceso A Una Red Wi-Fi Utilizando Software Libre para Mejorar El Nivel De Seguridad Del Acceso A La Información.

d) En función a los resultados obtenidos se mejorará el Nivel de seguridad del acceso a la información de la Municipalidad Distrital de la Esperanza, a través de un Sistema Gestión de Acceso a una Red Wi-fi utilizando Software Libre.

CAPITULO VI

RECOMENDACIONES

VI. RECOMENDACIONES

1. En aplicaciones donde se necesite una seguridad más fuerte, el servidor de autenticación RADIUS, puede estar configurado para trabajar con certificados

2. Se recomienda que si el número de usuarios es más grande al planteado en él, se implementa un directorio activo en una base de datos externa a los servidores para optimizar los tiempos de respuesta de las peticiones dentro de la red.

3. Segmentación con redes virtuales y priorización del ancho de banda.

4. Se recomienda usar los servidores en modo Proxy para equilibrar la carga de tráfico de solicitudes de autenticación y conmutar a otro servidor si uno falla.

5. Se debe concientizar a todo el personal de la municipalidad. Sobre la importancia de implementar métodos para elevar la seguridad en una red inalámbrica para dispositivos móviles ya que son vulnerables por intrusos

CAPITULO VII

REFERENCIAS BIBLIOGRÁFICAS

VII. REFERENCIAS BIBLIOGRÁFICAS

(García, 2012). *Diseño e implementación de una red Lan y Wlan con sistema de control de acceso mediante servidores AAA* Lima: tesis.
http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1445/LAZO_GARCIA_NUTTSY_SERVIDORES_AAA.pdf?sequence=1

(CCNA Exploration 4.0, 2009) *Cisco Networking Academy Program***.**
http://www.escuelafolklore.edu.pe/ccna/wireless/ch1/1_1_1/index.html

(Bailón Giler, y otros, 2010), *Instalación y Configuración de Equipos Informáticos bajo software libre para la Biblioteca de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí.*
http://www.academia.edu/5779454/Lets_Keep_Walking

(Lehembre, 2015) *Seguridad Wi-Fi – WEP, WPA y WPA2*
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

(Reyes Montiel) *Estudio, diseño y evaluación de protocolos de autenticación para redes Inalámbricas.*
http://delta.cs.cinvestav.mx/~francisco/Repository/tesisItzelt.pdf

(WEB002) *INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR RADIUS.*
http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

(ISECOM) *OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad.*
http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

(Mérigo Hernández) *Seguridad en la conexión a redes inalámbricas en lugares públicos.*
http://es.slideshare.net/rosanicastillo/seguridad-en-laconexinaredesinalmbricasenlugarespblicos

CAPITULO VIII

ANEXOS

VIII. ANEXOS

ANEXO I

MUNICIPALIDAD DISTRITAL DE LA ESPERANZA
CREADO EL 29 DE ENERO DE 1965 - LEY Nº 15418
Jr. C.M. Alvear Nº 999 - Telefax 272478 - 483330 - 272345 - 271744
TRUJILLO - PERÚ

EL GERENTE DE RECURSOS HUMANOS DE LA MUNICIPALIDAD DISTRITAL DE LA ESPERANZA, EXTIENDE:

CARTA DE ACEPTACIÓN

La Esperanza, 20 de abril de 2015.

ING. LIC. GROVER EDUARDO VILLANUEVA SÁNCHEZ
Director de la Escuela de Ingeniería en Sistemas
Universidad Cesar Vallejo

Presente

Tengo el agrado de dirigirme a Usted, con la finalidad de hacer de su conocimiento que el Sr. **MILTON RODOLFO BARDALES RAMIREZ ODIAGA,** identificado con **DNI N° 42757197,** Alumno de la Escuela Profesional de INGENIERIA DE SISTEMAS, de la Institución Universitaria que usted representa, ha sido **AUTORIZADO** para realizar su trabajo de investigación denominado " **Sistema de Gestión de Acceso a una Red Wifi utilizando Software Libre para Mejorar el Nivel de Seguridad del Acceso a la Información",** en la Sub Gerencia de Informática y Sistemas, de Nuestra Institución. a partir del **21.04.15**,

Aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente,

MUNICIPALIDAD DISTRITAL DE LA ESPERANZA
GERENCIA DE RECURSOS HUMANOS
Mg. José R. Martínez Ulloa
GERENTE

JRMU/jkcp
Archivo

ANEXO 2

ENTREVISTA DIRIGIDA A LOS JEFES DE LAS ÁREAS DE LA MUNICIPALIDAD DISTRITAL DE LA ESPERANZA

DATOS DE LA ENCUESTA:

Fecha: ___/___/___ Hora: ___:___:___
Lugar: _____
Duración Aproximada: _____

CONTENIDO DE LA ENCUESTA:

1.- ¿Cuál es la función que usted desempeña en la municipalidad?

2.- ¿Cuáles son los problemas más comunes que presenta la red actual en la municipalidad y como afectan estos en el desempeño de las labores de los trabajadores de la municipalidad?

3.- ¿Cuál cree que es la causa de estos problemas?

4.- ¿Considera que el tiempo de descarga de información es el adecuado?

5.- ¿Cree que la red actual con la que cuenta la municipalidad necesita una reestructuración?

6.- ¿Por qué la municipalidad no cuenta con una red inalámbrica?

7.- ¿Estaría de acuerdo con la implementación de una red inalámbrica para mejorar la comunicación y el servicio de red?

8.- ¿Estaría de acuerdo con la implementación de un sistema de gestión de acceso mediante una red Wi-Fi para mejorar el nivel de seguridad de la información?

ANEXO 3

ENTREVISTA PARA EL JEFE DE LA OFICINA DE INFORMATICA Y SISTEMAS DE LA MUNICIPALIDADD DISTRITAL DE LA ESPERANZA

DATOS DE LA ENCUESTA:

Fecha: ___/___/___ Hora: ___:___:___
Lugar: _____
Duración Aproximada: _____

CONTENIDO DE LA ENCUESTA:

1.- ¿El lugar donde se encuentra el área de Sistemas e Informática es el adecuado para el funcionamiento de los servidores, y/o equipos de cómputo?

2.- ¿La institución cuenta con un plan de mantenimiento preventivo de los recursos de procesamiento de información?

3.- ¿El Personal que labora en la institución cuenta con autorización para poder ingresar al sistema?

4.- ¿Existen ficheros de log que registren los accesos a personas autorizadas y los intentos de acceso licito?

5.- ¿Realiza un registro adecuado de las actividades que realizan los usuarios en el sistema?

6.- ¿Existen políticas definidas para el acceso a internet?

5.- ¿El sistema operativo que actualmente utilizan es licenciado?¿Cree Ud. Que utilizando herramientas de software libre beneficiaran a la institución ?

6.- ¿Existe el interés por parte de la institución en adquirir nuevos y mejores activos de procesamiento de información?

ANEXO 4

CUESTIONARIO DE SATISFACCIÓN DEL USUARIO

Encuesta dirigida a los usuarios de la Municipalidad Distrital De la Esperanza

1.- El nivel de seguridad de la información de la institución es adecuada

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

2.- ¿Cómo calificaría el servicio de internet?

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

3.- ¿Cómo calificaría el tiempo que demora en acceder al sistema informático de la institución?

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

4.- Obtiene información a tiempo.

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

5.- ¿Cómo considera el tiempo de descarga de archivos?

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

6.- ¿Cómo calificaría el sistema con el que cuenta actualmente?

☐ Muy Bueno ☐ Bueno ☐ Regular ☐ Malo ☐ Muy Malo

Anexo 5: Metodología de FitzGerald

El estudio realizado hace uso de la Metodología de Jerry FitzGerald, para ello se siguen diversas Fases.

I. Fase I Consideraciones técnicas

- **Análisis de la Empresa**

La Municipalidad Distrital de La Esperanza, es un Gobierno Local promotor del Desarrollo Local, que emana de la voluntad popular. Tiene personería jurídica de derecho público con autonomía política, económica y administrativa en los asuntos municipales de su competencia, es promotor del desarrollo local con plena capacidad para el cumplimiento de sus fines; ejerce las funciones y atribuciones que le señala la Constitución Política del Perú y la Ley Orgánica de Municipalidades.

Se encuentra ubicada en la parte no centro de la provincia de Trujillo, en la región La Libertad, limita por el Norte y Oeste con el distrito de Huanchaco, por el Este con el distrito de Florencia de Mora y por el Sur con el distrito de Trujillo, entre las coordenadas 08º04'39" de latitud sur y 79º02'38" de longitud oeste, a una distancia aproximada de seis kilómetros de la capital de la provincia con respecto a la Plaza de Armas del distrito.

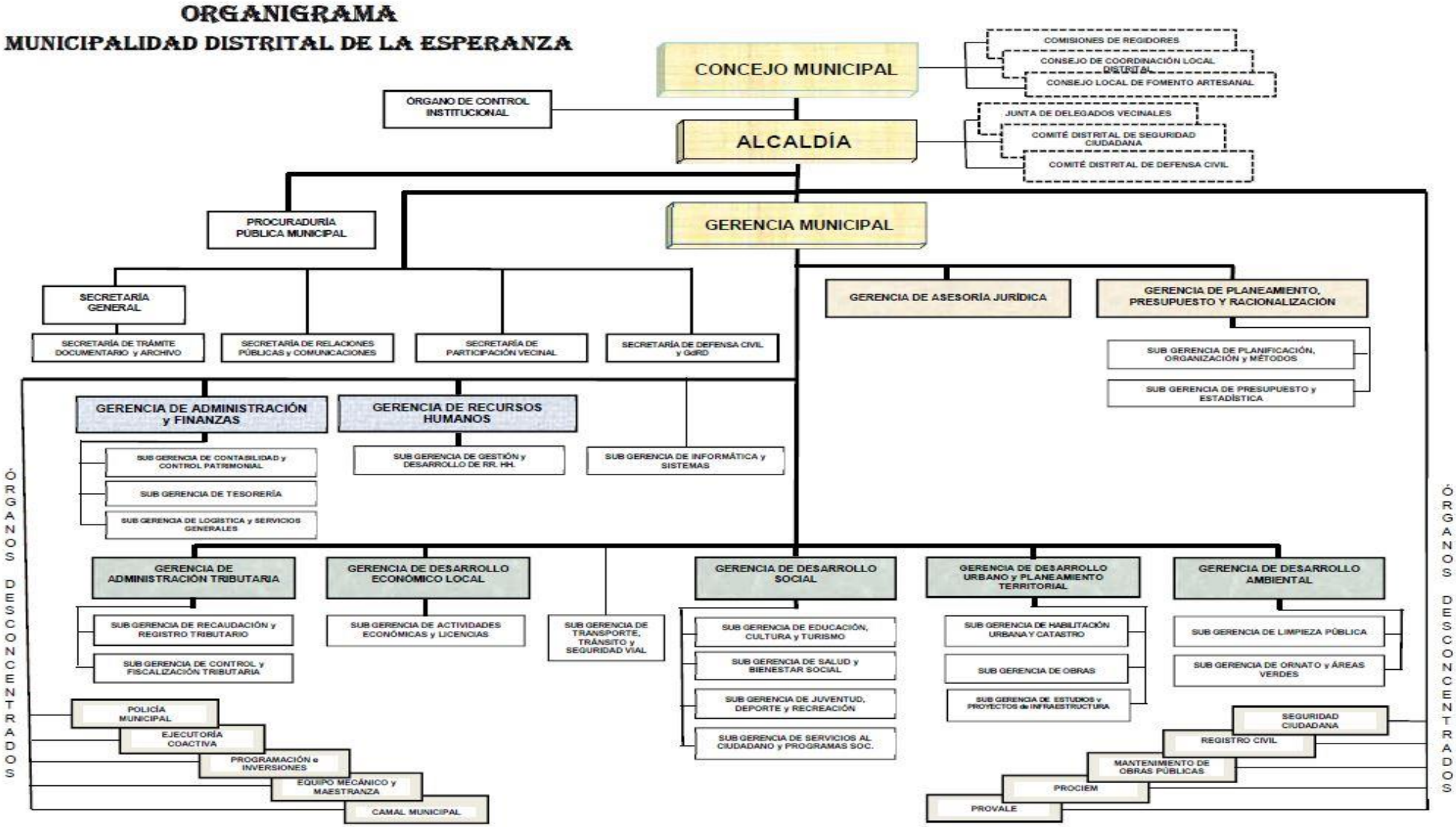
Misión

La Municipalidad Distrital de La Esperanza tiene como Misión la Gobernabilidad del distrito La Esperanza, representando a su vecindario, promoviendo la adecuada prestación de los servicios públicos locales, fomentando el bienestar de los vecinos y liderando activamente el desarrollo integral, armónico y sostenible de las circunscripciones de su jurisdicción.

Visión

La Municipalidad Distrital de La Esperanza, es una Institución líder, abierta al diálogo, que con legitimidad conduce, orienta, coordina y evalúa la formulación y aplicación de las políticas de gobierno local, generando y asegurando la gobernabilidad y desarrollo del distrito, con óptima gestión de recursos públicos, en la búsqueda de una ciudad moderna, ordenada y democrática, con equidad.

Fig 3.1 Organigrama de la Municipalidad Distrital de la Esperanza



A. Realidad Problemática

La Municipalidad Distrital de la Esperanza en la actualidad cuenta con una infraestructura de red cableada, la misma que le permite comunicarse con sus diferentes áreas del palacio municipal, el cableado no cumple con las normas y estándares establecidos por la ANSI/TIA/EIA, ISO, IEEE, propios de una certificación de calidad total.

En el palacio municipal y en los anexos de la municipalidad con el paso de los años han ocurrido problemas de red tales como la dificultad para encontrar la ubicación de un punto de red en los switches principales. La no existencia de acceso inalámbrico, que permita el acceso inmediato al servicio de Internet en el Palacio Municipal no cumple con los requerimientos y materiales para cubrir unos eventos, o algunas actividades donde las personas requieran del servicio y al no existir este servicio se le improvisaba en el momento una red cableada para cumplir con el propósito.

Los equipos inalámbricos con los que cuenta la Municipalidad no tienen el alcance de cobertura suficiente para abarcar el área geográfica que la comprende, esto es tercer piso y cuarto piso del palacio municipal. En la encuesta realizada para ver la viabilidad de la implementación de la red inalámbrica en el municipio, los jefes de cada área y el personal que labora respondieron en un 100% que era necesaria y conveniente la utilización de dicha tecnología de red. Se han observado los siguientes inconvenientes con respecto al manejo de la información:

Dificultad en la comunicación y lentitud en la transferencia de información en las computadoras de la institución, por el excesivo tráfico de datos en un mismo segmento de Red, debido al incremento de usuarios de la Red sin el cumplimiento de los estándares de cableado estructurado, topología ancho de banda, entre otros**.(ANEXO 1)**

Acceso inseguro a la Información disponible en las computadoras de la Red LAN de la institución, al no existir políticas de seguridad, los usuarios internos y externos no autorizados tienen acceso libre a la información y recursos importantes de la Institución y pueden vulnerar sus niveles de protección y confiabilidad. **(ANEXO 3)**

Escasez de personal para el mantenimiento preventivo y correctivo de los equipos de cómputo e impresoras generando inoperatividad de los equipos y la lentitud en las unidades afectadas**. (ANEXO 2)**

B. Tecnología Existente en la Municipalidad Distrital de la Esperanza

La Municipalidad Distrital de la Esperanza cuenta con recursos tecnológicos para la comunicación e integración de sus áreas organizacionales, recursos hardware que le permiten albergar sus servicios electrónicos, descritos en los siguientes cuadros.

Hardware:

Servidores:

1 Servidor de Dominio:

Tabla Nº 3.1: Tabla de descripción servidor de Dominio

CARACTERÍSTICAS	FUNCIÓN
CPU INTEL INTEL DG31PR INTEL CORE 2 DUO 3.00 GHZ MEMORIA RAM 4 GB CPU ADAPTADO COMO SERVIDOR **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: WINDOWS SERVER 2012 R2	**Servidor de Dominio** 

Fuente: Sub Gerencia de Informática y Sistemas

1 Servidor de Base de Datos:

Tabla Nº 3.2: Tabla de descripción servidor de Datos

CARACTERÍSTICAS	FUNCIÓN
CPU BIOSTARH61MGC INTEL CORE i5 2.8 GHZ MEMORIA RAM 8 GB CPU ADAPTADO COMO SERVIDOR **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS 7 ULTIMATE	**Servidor de Base de Datos (Servidor de Área de Caja)** 

Fuente: Sub Gerencia de Informática y Sistemas

1 Servidor IBM de Base de Datos:

Tabla Nº 3.3: Tabla de descripción servidor de Base de Datos

CARACTERÍSTICAS	FUNCIÓN
SERVIDOR IBM SYSTEM X3200 INTEL XEON 2.13 GHZ MEMORIA RAM 4 GB **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS SERVER 2003 R2	**Servidor de Base de Datos (Servidor de la MDE)** 

Fuente: Sub Gerencia de Informática y Sistemas

1 Servidor HP PROLIANT:

Tabla Nº 3.4: Tabla de descripción servidor de SIAF

CARACTERÍSTICAS	FUNCIÓN
SERVIDOR HP PROLIAN ML350G6 NTEL XEON 2.40 GHZ MEMORIA RAM 6 GB SERVIDOR SIAF **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS SERVER 2008	**Servidor de SIAF** 

Fuente: Sub Gerencia de Informática y Sistemas

1 Servidor HP PROLIANT:

Tabla Nº 3.5: Tabla de descripción servidor de Dominio (Nuevo)

CARACTERÍSTICAS	FUNCIÓN
SERVIDOR HP PROLIANT DL320e Gen 8 V2 INTEL XEON 3.10 GHZ MEMORIA RAM 16 GB **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS SERVER 2012 **1**	**Servidor de Dominio (Nuevo)** 

Fuente: Sub Gerencia de Informática y Sistemas

Servidor HP PROLIANT:

Tabla Nº 3.6: Tabla de descripción servidor HP -DATA (RENTAS)

CARACTERÍSTICAS	FUNCIÓN
SERVIDOR HP PROLIANT DL380p INTEL XEON E5-2630 2.30 GHZ MEMORIA RAM 24 GB SERVER-RENTAS **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS SERVER 2008 R2	**Servidor HP -DATA (RENTAS)** 

Fuente: Sub Gerencia de Informática y Sistemas

1 Servidor IBM RENTAS:

Tabla Nº 3.7: Tabla de descripción servidor IBM-RENTAS (CONSULTAS ONLINE)

CARACTERÍSTICAS	FUNCIÓN
SYSTEM X3200 INTEL XEON CPU X3430 2.40 GHZ 6 GB SERVIDOR-RENTAS NECESITA SER REPARADO **SOFTWARE INSTALADO:** SISTEMA OPERATIVO: MICROSOFT WINDOWS SERVER 2008 R2	**Servidor IBM -RENTAS (CONSULTAS ONLINE)** 

Fuente: Sub Gerencia de Informática y Sistemas

C. Descripción de la Red actual de la Municipalidad Distrital de la Esperanza.

La Municipalidad Distrital de la Esperanza actualmente cuenta con tres redes de datos separadas geográficamente la red principal que se encuentra en el Palacio Municipal y las otras en sus anexos; y cada uno de estos locales cuenta con su propia servicio telefónico y servicio de internet, a continuación se describirán la administración, topología, el hardware, estándares, servicios de conectividad, estado de los equipos de comunicación, distribución de direccionamiento de IPs y la respectiva estructura física y lógica (diagramas) de las redes de dichos locales.

1.- Administración:

La forma de trabajo administrativo se traslada a la aplicación de grupos de trabajo, bajo un solo dominio llamado muniesperanza.

Estos grupos de trabajo, han sido determinados según las áreas funcionales de la organización, con el objeto de ofrecer un desempeño coherente con la estructura institucional.

Cada trabajador que usa una computadora de la red, tiene asignado un password, que lo reconoce como usuario de la red y que lo habilita para realizar su trabajo con el debido resguardo de la información que maneja de la misma forma, como política

del trabajo informático, se tiene señalado que toda la información que se procesa bajo la red, debe ser guardado en uno de los servidores habilitados para tal actividad. En cuanto con la administración de los dispositivos de comunicación (Switches) no existen configuraciones establecidas en dichos dispositivos.

2.- Topología:

La Municipalidad Distrital de la Esperanza actualmente tiene implementada su red de datos con la topología estrella; y sus respectivos locales-anexos de igual forma (en el punto estructura lógica y física se apreciara esta topología), los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red (Switch), quien se encarga de gestionar las transmisiones de información por toda la red.

3.- Hardware de comunicación:

Tabla 3.8: Relación de equipos de comunicación Palacio Municipal

Área	Nivel	Descripción	Cantidad	Marca	Modelo	Características	Estado
Sub Gerencia de Informática y Sistemas	PRIME R PISO	Router	1	Cisco	Serie 850	- 1 Puerto consola - 4 Puertos FastEthernet - 1 Puerto Wan	OPERATIVO
		Switch	1	Hp	Switch HP 2530	- 24 Puertos FastEthernet 10/100/1000 Mbits/s. - 4 puertos Gigabit SFP -1 Puerto Consola.	
		Switch	1	3Com	Baseline Switch 2924 SFP Plus	- 24 Puertos FastEthernet 10/100/1000 Mbits/s. - 4 puertos Gigabit SFP -1 Puerto Consola.	
Gerencia de Administración Tributaria (Caja)		Switch	1	3Com	Baseline Switch 2816	-16 Puertos FastEthernet 10/100/1000 Mbits/s.	
Gerencia de Administración Tributaria (Rentas)		Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
SubGerencia de Recursos Humanos		Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
División de Registro Civil		Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
Secretaria de Alcaldía	SE G	Switch	1	3Com	Baseline Switch	- 24 Puertos FastEthernet	

					2824	10/100/1000 Mbits/s.	
Secretaría General		Switch	1	D-Link	DES-1016D	- 16 Puertos FastEthernet 10/100 Mbits/s.	
Secretaría de Relaciones Publicas y Comunicaciones		Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
Gerencia de Planeamiento, presupuesto Y Racionalización		Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
Subgerencia de Contabilidad y Control Patrimonial	**TERCER PISO**	Switch	1	3Com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s.	
Subgerencia de Logística y Servicios Generales		Switch	1	3Com	Baseline Switch 2924 SFP Plus	- 24 Puertos FastEthernet 10/100/1000 Mbits/s. - 1 Puerto Consola.	
Gerencia de Administración y Finanzas		Switch	1	3com	Baseline Switch 2924 SFP Plus	- 24 Puertos FastEthernet 10/100/1000 Mbits/s. - 4 puertos Gigabit SFP - 1 Puerto Consola.	
Gerencia de Asesoría Jurídica	**CUARTO PISO**	Switch	1	D-Link	DES-1016D	- 16 Puertos FastEthernet 10/100 Mbits/s.	

Tabla 3.9: Relación de equipos de comunicación Anexo 1

Área	Nivel	Descripción	Cantidad	Marca	Modelo	Características	Estado
Subgerencia de Obras	PRIMER PISO	Router Anexo 1	1	Cisco	850	-1 Puerto Consola. - 4 Puertos FastEthernet. - 1 Puerto WAN	OPERATIVO
Subgerencia de habilitación urbana y catastro		SwAnexo 1	1	3com	Baseline Switch 2824	- 24 Puertos FastEthernet 10/100/1000 Mbits/s. - Soporta MDI/MDIX.	
Subgerencia De Estudios Y Proyectos De Infraestructura							
División De Mantenimiento De Obras Públicas							
Liquidación de obras							
Gerencia De Desarrollo Urbano Y Planeamiento Territorial							
Almacén							
Subgerencia De Juventud, Deporte Y Recreación							
Liquidación de Obras							
Demuna							
Servicio social		SwAnexo 1-2	1	d-Link	DES-1024D	- 24 Puertos FastEthernet 10/100 Mbits/s. - Puertos MDI/MDIX. - Soporta Full/Half duplex.	
Subgerencia de ornato y áreas verdes							
Subgerencia de educación, cultura y turismo							
Secretaria de participación vecinal							
Provale	SEGUNDO PISO	Hub	1	DLINk	10Base-T	- 8 Puertos FastEthernet 10 Mbits/s. - Soporta Full/Half duplex.	

Tabla 3.10: Relación de equipos de comunicación Anexo 2

Área	Nivel	Descripción	Cantidad	Marca	Modelo	Características	Estado
Gerencia de desarrollo económico local	PRIMER PISO SEGUNDO PISO TERCER PISO	Router	1	Cisco	850	-1 Puerto Consola. - 4 Puertos FastEthernet. - 1 Puerto WAN	0OPERATIVO
Subgerencia de transporte, tránsito y seguridad vial		Switch	1	3Com	Baseline Switch 2024 Plus	-24 Puertos FastEthernet 10/100 Mbits/s.	
Secretaría de Defensa Civil y gestión del riesgo de desastres							
Subgerencia de actividades económicas y licencias							
División De Ejecutoría Coactiva							

4.- Listado de Aplicaciones:

El listado de aplicaciones que se muestra a continuación es general para todos los locales de la Municipalidad.

Tabla N° 3.11: Lista de Sistemas Operativos.

Nombre del Programa	Versión	Estado	Licencia
Microsoft Windows XP	SP3	Instalado	No
Microsoft Windows 7 Ultimate	Ultimate	Instalado	No
Microsoft Windows 2003 Server	2003	Instalado	No
Microsoft Windows 2012 Server	2008	Instalado	No
Microsoft Windows 8	8 Pro	Instalado	No

Tabla N° 3.12: Lista de Programas Actuales.

Nombre del Programa	Versión	Estado	Licencia
Microsoft Office	2010	Instalado	No
Microsoft Office	2013	Instalado	No
Microsoft Office	2007	Instalado	No
Winzip	4.0	Gratuita	No
Eset Nod 32 Endpoint Security	5	Instalado	Si
S10	2005	Instalado	Si
Autocad	2008-12-14-15	Instalado	No
Adobe Reader	XI	Instalado	No
SAP 2000	v17	Instalado	No
Corel Draw	X6	Instalado	No
Ccleaner	3.27	Instalado	No
Winrar	4.20	Instalado	No
Spark	2.70	Instalado	No
Nero Essentials	7	Instalado	No
Nitro Pro	8	Instalado	No
Visual Studio	2012	Instalado	No
VNC Server	5.0.5	Instalado	No

Tabla N° 3.13: Lista de Sistemas de Información.

Nombre del Programa	Lenguaje de Programación	Estado	Licencia
Sistema de trámite Documentario	Visual Studio 6.0	Instalado	Si
Sistema de Rentas	Visual Basic 6.0	Instalado	Si
SIAF	Visual Fox Pro	Instalado	Si
Sistema de Almacén	Visual Basic 6.0	Instalado	Si
Sistema de Caja	Visual Basic 6.0	Instalado	Si
Sistema de Registros Civiles	Visual Basic 6.0	Instalado	Si
SISFOG	Visual Fox Pro	Instalado	Si
Clariza	Visual Fox Pro	Instalado	Si
Meliza	Visual Fox Pro	Instalado	Si
Sistema COA	DOS	Instalado	Si
Sistema de Provale	Visual Studio 6.0	Instalado	Si
Sistema de Audiencia	Visual Studio 6.0	Instalado	Si
Sistema de Transportes	Visual Studio 6.0	Instalado	Si
Sistema de Participación Vecinal	Visual Studio 6.0	Instalado	Si
Sistema de Abastecimiento	Visual Basic 6.0	Instalado	Si

5.- Estructura Lógica y Física de la Red

Fig. 3.2: Diagrama Lógico de la Red de Datos – Palacio Municipal

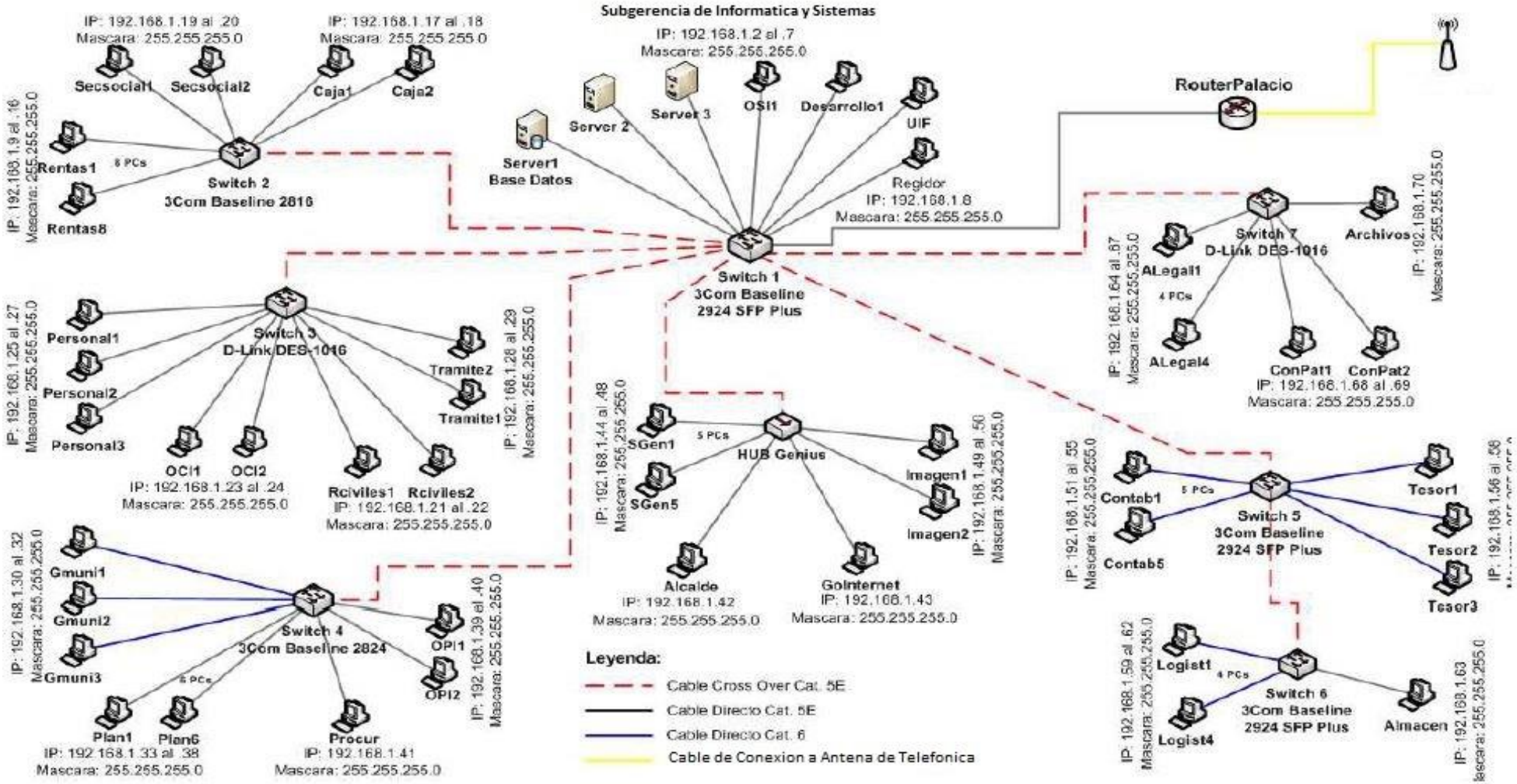


Fig. 3.3: Diagrama Físico de la Red de Datos - Palacio Municipal (Primer Piso)

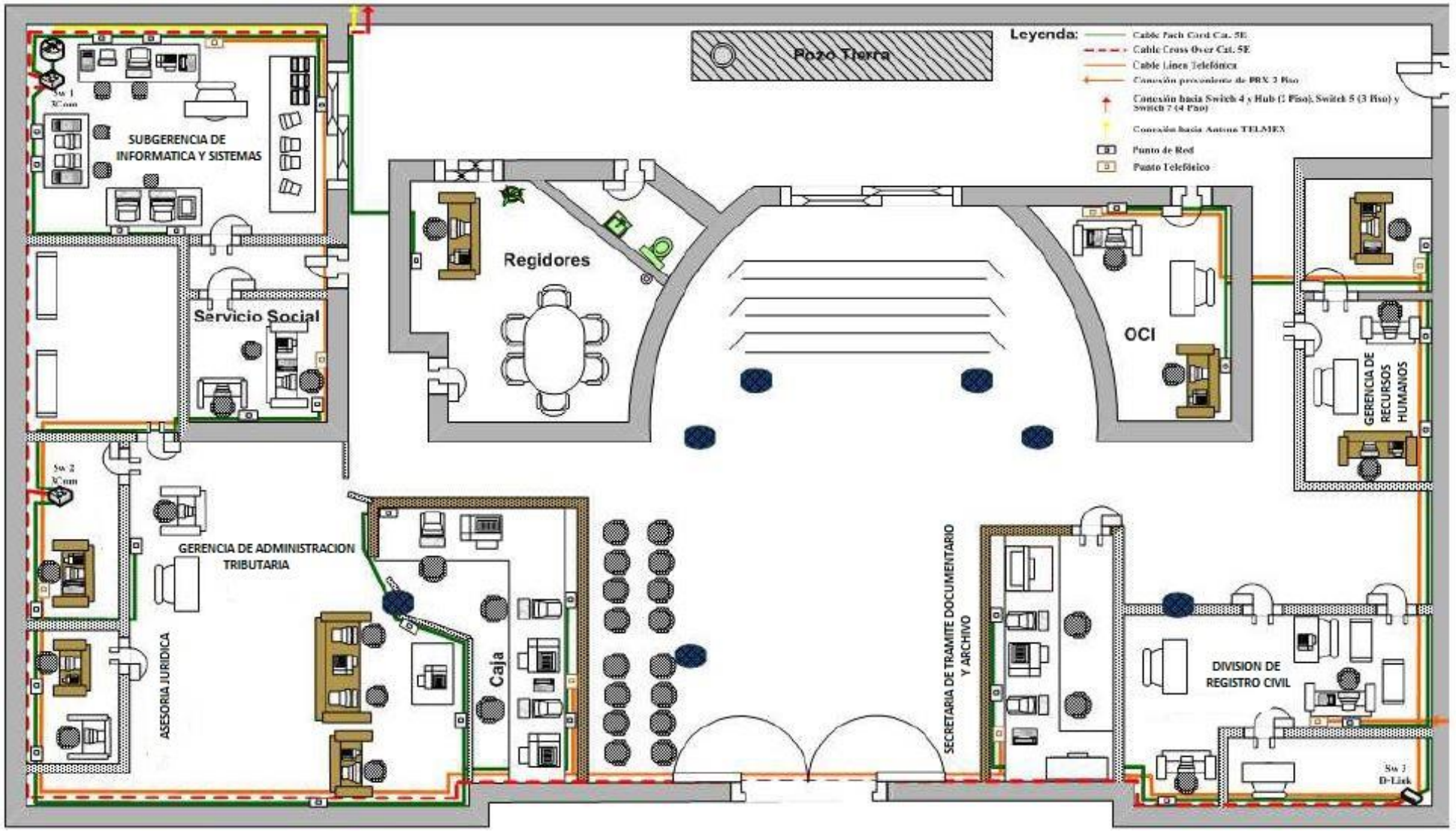


Fig. 3.4: Diagrama Físico de la Red de Datos - Palacio Municipal (Segundo Piso)

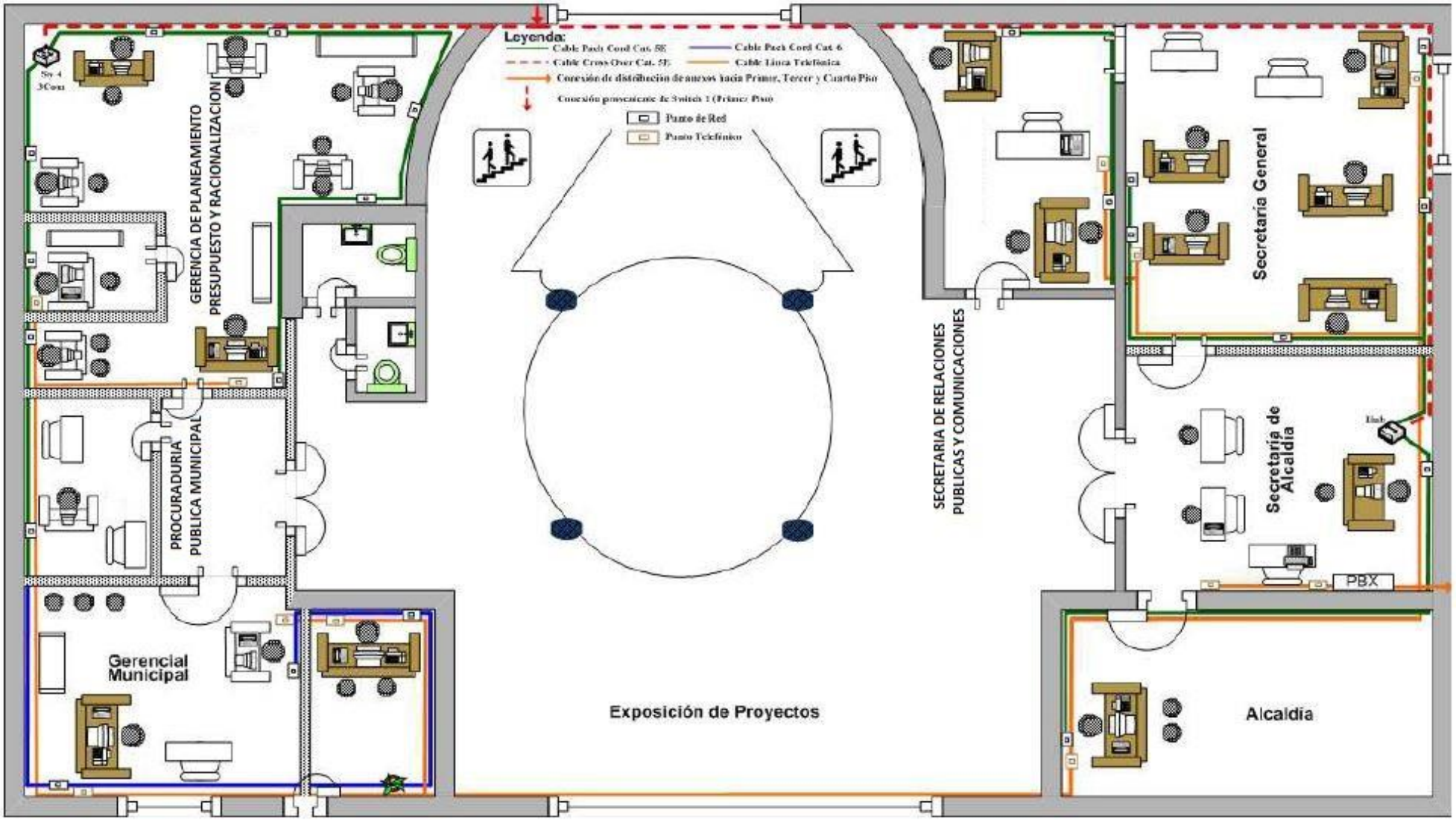


Fig. 3.5: Diagrama Físico de la Red de Datos - Palacio Municipal (Tercer Piso)

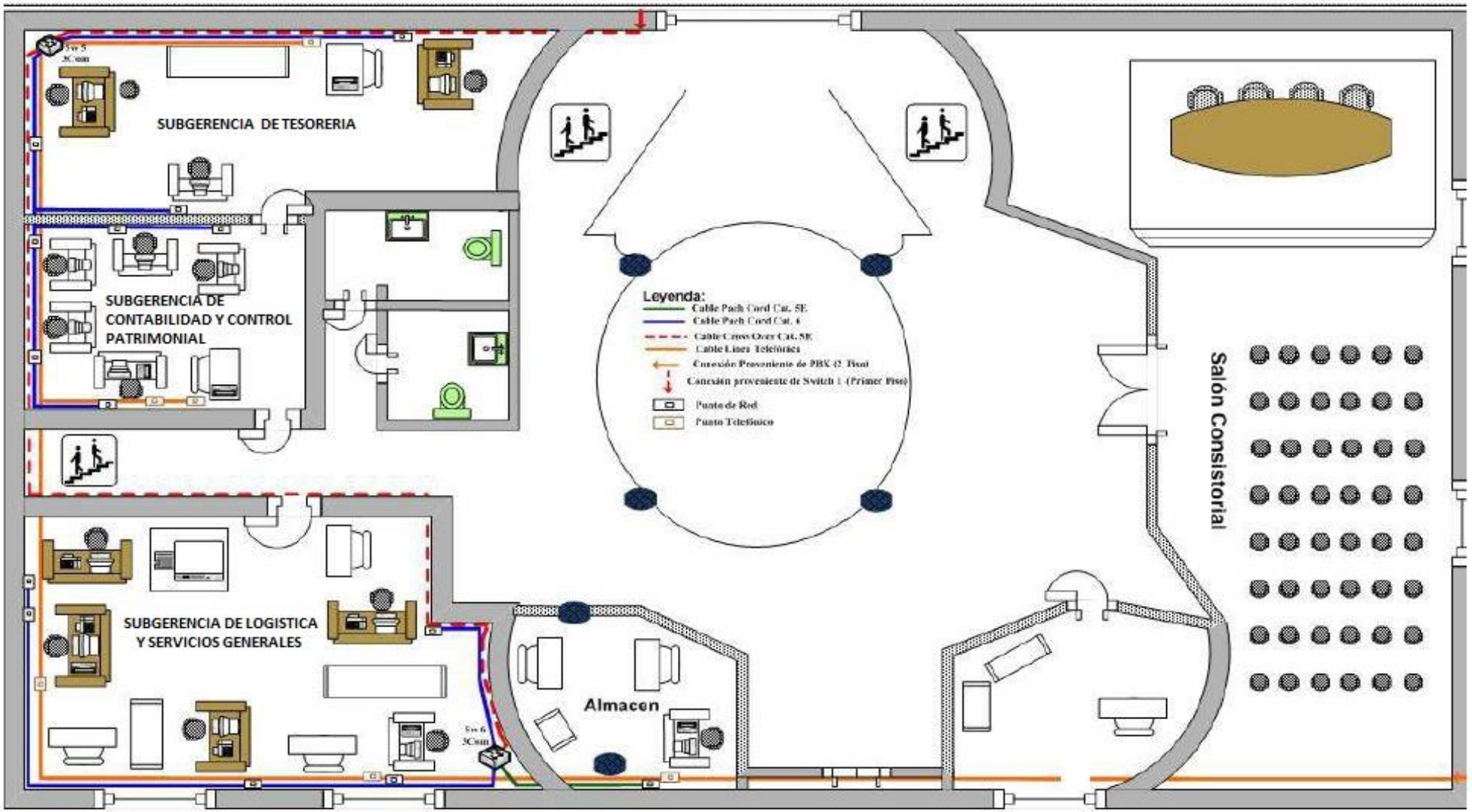


Fig. 3.6: Diagrama Físico de la Red de Datos - Palacio Municipal (Cuarto Piso)

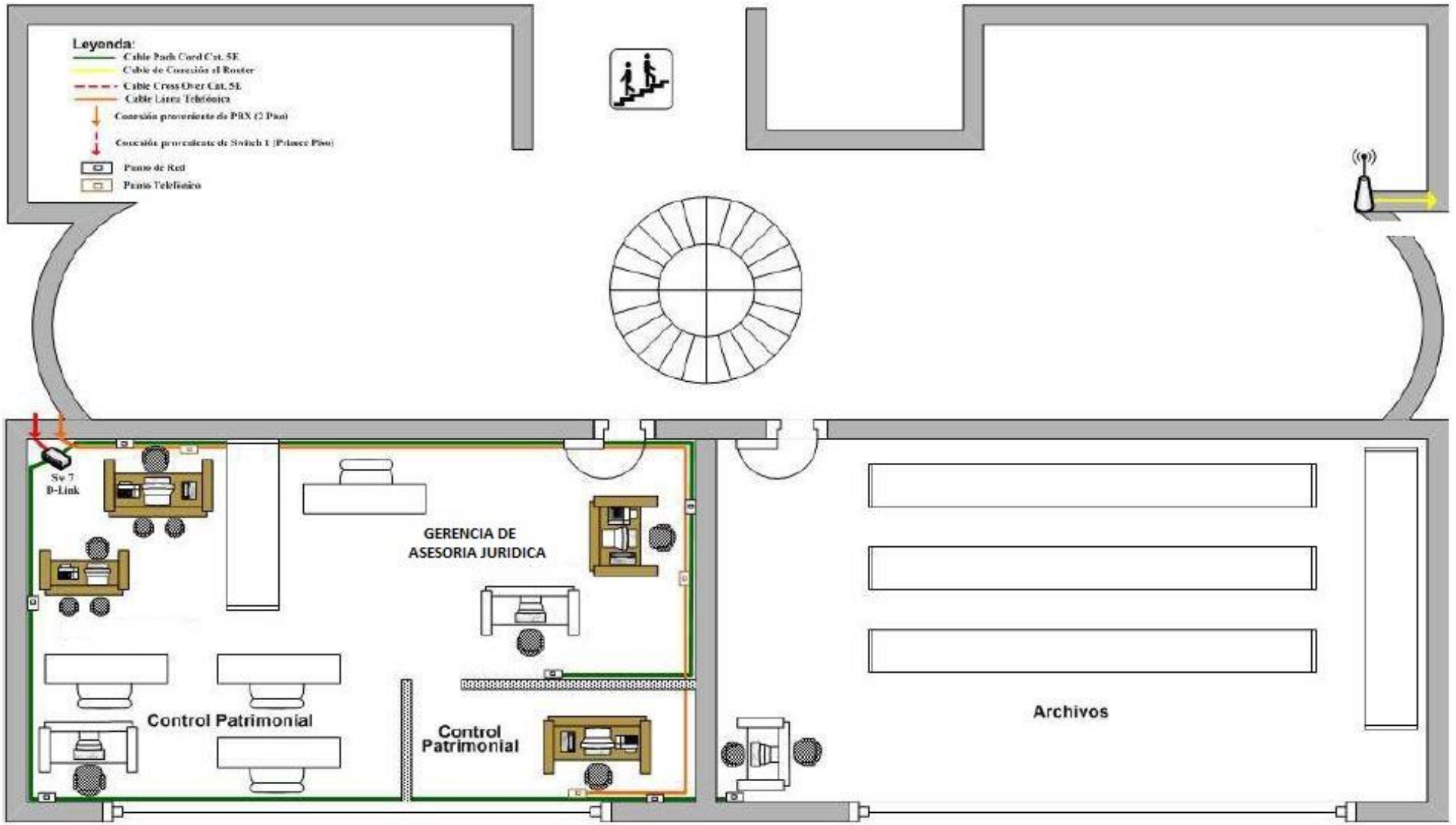


Fig. 3.7: Diagrama Físico de la Red de Datos - Anexo 1 (Primer Piso)

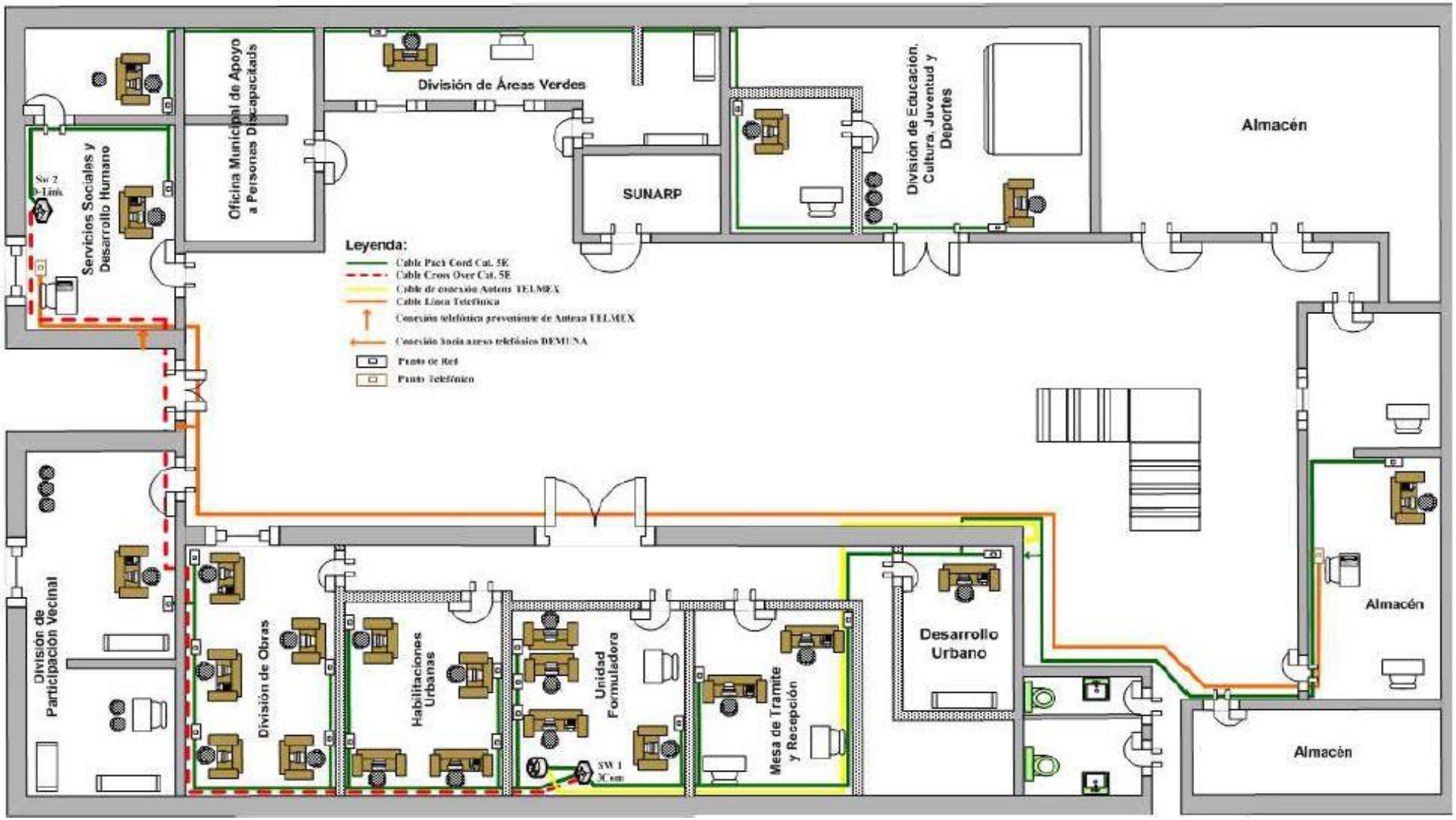


Fig. 3.8: Diagrama Físico de la Red de Datos - Anexo 1 (Segundo Piso)

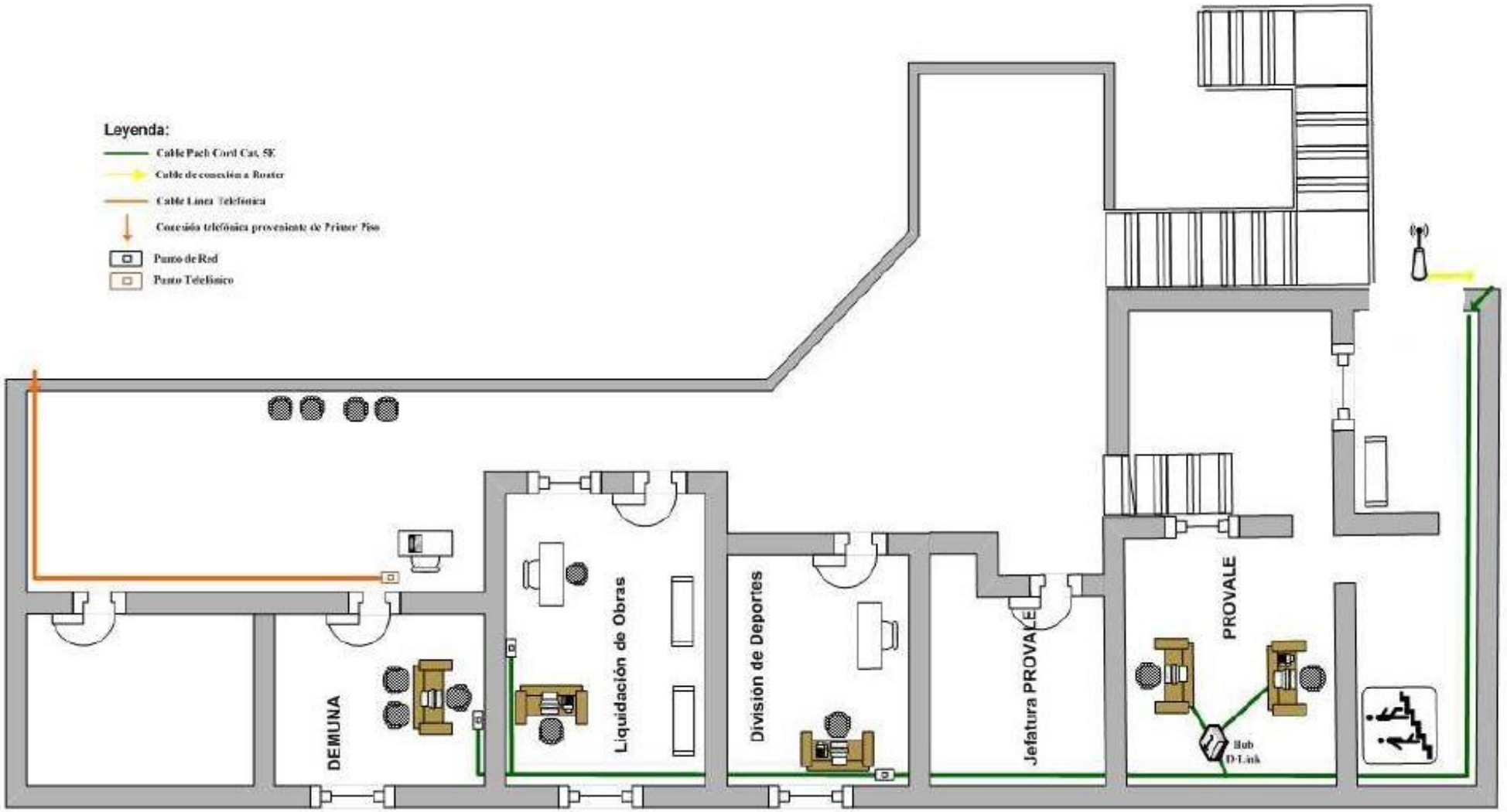


Fig. 3.9: Diagrama Físico de la Red de Datos - Anexo 2 (Primer Piso)

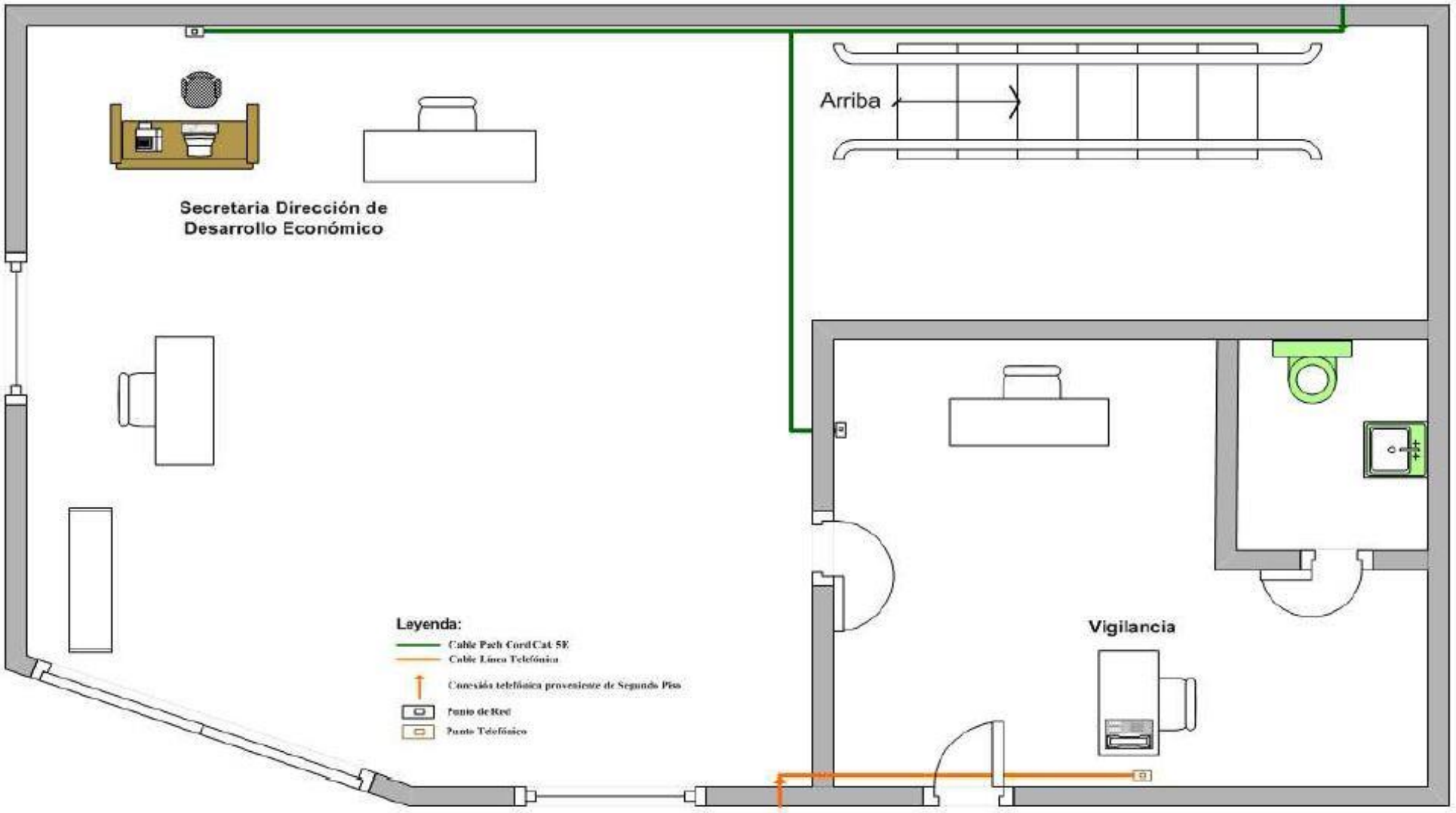
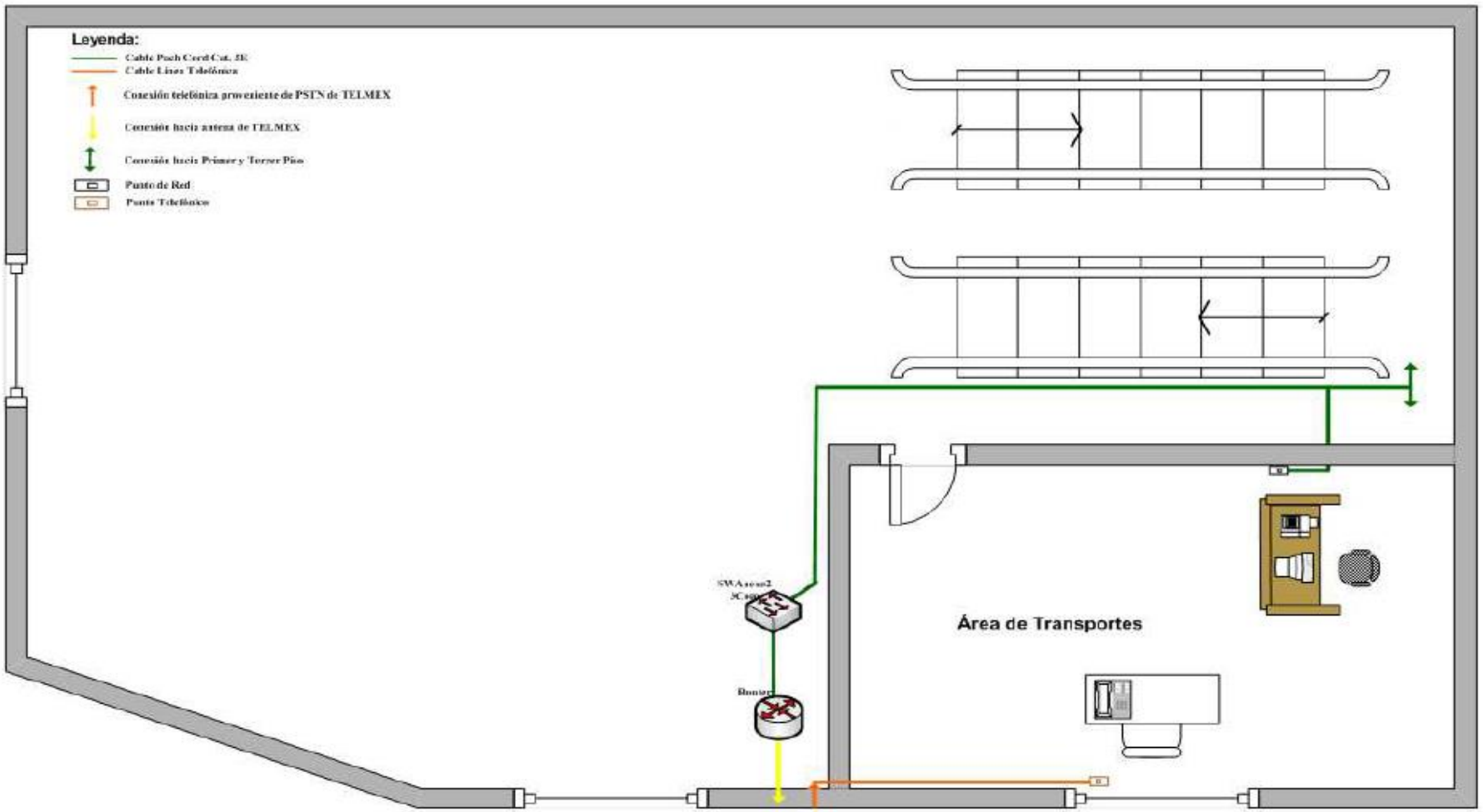


Fig. 3.10 Diagrama Físico de la Red de Datos - Anexo 2 (Segundo Piso)



- **Estudio de la Factibilidad**

1. **Estructura de Costos**

a) Costos de Inversión

- **Hardware**

Tabla 3.14: Costos de Inversión - Hardware

RECURSO	CANTIDAD	PRECIO UNITARIO (S/.)	TOTAL (S/.)
Computadora	1	2,500.00	2,500.00
Access Point	6	1200.00	1200.00
Impresora	1	165.00	165.00
		COSTO TOTAL	**S/. 3,865.00**

- **Software**

Tabla 3.15: Costos de Inversión - Software

LICENCIAS	NOMBRE	VERSIÓN	TOTAL S/.
Herramienta de Programación	Ubuntu	15.04	00.00
Gestor de Base de Datos	My SQL	5.6	00.00
Gestor Servicio Web	Daloradius	0.9	00.00
		COSTO TOTAL	S/. 00.00

- **Recursos Humanos**

Tabla 3.16: Costos de Inversión – Recursos Humanos

PERSONAL	FUNCIÓN	PAGO MENSUAL	N° MESES	TOTAL
Milton Bardales Ramírez Odiaga	Tesista	S/. 750.00	8	S/. 6,000.00
Ing. Edwin Mendoza Torres	Asesor	S/. 100.00	8	S/. 800.00
			TOTAL	**S/. 6,800.00**

- **Materiales**

Tabla 3.17: Costos de Inversión - Materiales

MATERIAL	UNIDAD DE MEDIDA	CANTIDAD	PRECIO UNITARIO (S/.)	TOTAL (S/.)
Papel	Millar	2	12.50	25.00
Lapiceros	Unidad	5	0.80	4.00
Corrector	Unidad	2	1.20	2.40
Folder Manila	Unidad	10	0.70	7.00
Cartucho negro HP	Unidad	4	40.00	160.00
Cartucho color HP	Unidad	1	80.00	80.00
DVD	Unidad	10	3.00	30.00
			TOTAL	**S/. 308.40**

- **Consumo Eléctrico**

  Para el consumo eléctrico tomaremos en cuenta las 400 horas de desarrollo del proyecto.

Tabla 3.18: Costos de Inversión – Consumo Eléctrico

EQUIPO	CANTIDAD	Potencia		Frecuencia	Consumo	Costo(S/.)	IGV (19%)	TOTAL
		Watts	KW	Horas	KW/H	KW/H		
Computadora	1	200	0.40	400	203.78	0.3856	0.19	S/. 39.16
Impresora	1	150	0.15	100	76.42	0.3856	0.19	S/. 12.53
							TOTAL	**S/. 51.69**

Fuente: Datos de potencia y costo: Hidrandina S.A

- **Costos de Mantenimiento**

Tabla 3.19: Costos de Inversión – Costos de Mantenimiento

DESCRIPCIÓN	Nº DE VECES	COSTO UNITARIO (S/.)	TOTAL (S/.)
Computadora	9	30	S/. 270.00
Access Point	4	50	S/.200.00
Impresora	3	30	S/. 90. 00
TOTAL			**S/. 560.00**

- **Costos de Depreciación**

Tabla 3.20: Costos de Inversión – Costos de Depreciación

DESCRIPCIÓN	COSTO INICIAL	PORCENTAJE DE DEPRECIACIÓN	TOTAL (S/.)
Computadora	2,500.00	20%	500.00
Access Point	1200.00	20%	240.00
Impresora	165.00	20%	33.00
TOTAL			**S/. 773.00**

2. Beneficios del Proyecto

a) Proyección de Beneficios Tangibles

- **Tiempo de Ahorro en Horas de Trabajo Mensual**

Tabla 3.21: Tiempo de Ahorro en Horas de Trabajo Mensual

PERSONAL	SUELDO HORA (S/.)	TIEMPO AHORRADO ESTIMADO MENSUALES (HORAS)	MONTO AHORRADO (S/.)
Administrador	35.00	18	630.00
		Total	S/. 630.00

- **Ingresos Proyectados**

Como consecuencia de la implementación del Sistema propuesto se proyecta mejorar los ingresos de la municipalidad de la siguiente manera:

Tabla 3.22: Ingresos Proyectados

AÑO	INGRESO PROYECTADO	PORCENTAJE DE AUMENTO EN INGRESOS	BENEFICIOS PROYECTADOS
2015	S/. 30,000.00	2.0%	S/. 600.00
2016	S/.35,000.00	2.5%	S/. 875.00
2017	S/. 40,000.00	3.0%	S/. 1,200.00

b) Beneficios Intangibles

- Mejorar el nivel de satisfacción de los trabajadores de la municipalidad.
- Obtener información pertinente en el momento que sea necesario.
- Mejorar el nivel de seguridad de la información de la municipalidad
- Mejorar la calidad del servicio

II. Fase II Diseño de la Red

- **Alcance de la Red**

  - **Local**

La Red Inalámbrica propuesta, debe estar diseñada con el fin de conectar a todas las áreas de la municipalidad y la interconexión de los anexos, así como mejorar la comunicación y la transmisión de información.

  - **Identificación del alcance geográfico**

El alcance de la red inalámbrica para el presente proyecto ha sido determinado por el espacio geográfico que comprende el palacio del municipio y los anexos de la Municipalidad Distrital de la Esperanza.

III. Fase III Configuración de la Red

A. Definición de las características de la red

Esta etapa describe las características técnicas de la red inalámbrica a implementarse en la Municipalidad Distrital de la Esperanza.

Entre las características más resaltantes de una infraestructura inalámbrica tenemos:

- Movilidad.
- Simplicidad y rapidez de instalación.
- Flexibilidad de instalación.
- Bajo coste de instalación.
- Escalabilidad.

Para la ejecución de nuestro proyecto se han definido las siguientes características técnicas:

- **Topología WLAN**

  La Red Inalámbrica que se implementará en la Municipalidad distrital de la Esperanza, será:

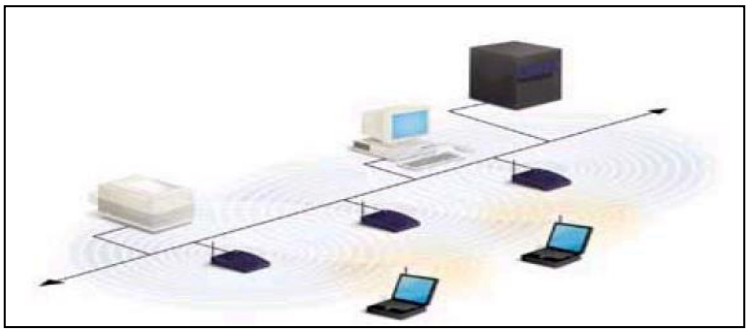
  Infraestructura Network.

  La comunicación entre las estaciones es a través de Access Point, los cuáles a su vez se conectan al cableado estructurado de la red. La WLAN se utiliza como una extensión a la infraestructura de red basada en cable.

  Los Access Point actúan como clientes que solicitan servicios a nodos conectados a la infraestructura inalámbrica.

Fig. 3.27: Topología – Infraestructura Network

Fig. 3.28: Utilización de varios puntos de acceso

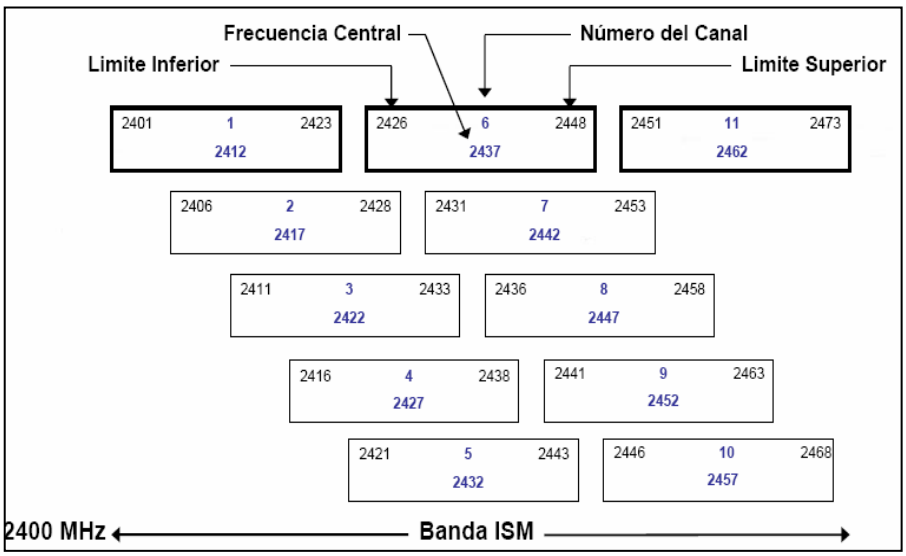


- **Tecnología Inalámbrica**

  Se ha definido la Radio Frecuencia para la transmisión de información como tecnología inalámbrica adecuada para nuestra realidad.

  Se transmite y se recibe en una banda específica de frecuencias para el paso de la información, de tal manera que los usuarios tengas distintas frecuencias de comunicación para evitar las interferencias. La frecuencia usada será **2.4 Ghz.**

Fig. 3.29: Distribución de canales y frecuencias correspondientes



- **Categoría de red Inalámbrica**

  Utilizadas en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy alejados entre sí y en el interior de edificios.

  En el caso de la aplicación de nuestro proyecto la categoría de la red inalámbrica será de corta distancia **Wi-fi,** ya que el área de cobertura que cubrirá la red está comprendida en el palacio municipal**.**

- **Tipo de red Inalámbrica**

  El tipo de red para nuestra realidad de acuerdo al alcance y la distancia que cubrirá es una Red de Área Local LAN, basándonos en el siguiente cuadro mostrado por la empresa DLINK.

Fig. 3.30: Clasificación de redes inalámbricas

Basada en la Norma del Instituto de Ingenieros Eléctricos y Electrónicos IEEE:

- **IEEE 802.11,** que presenta dos grandes esquemas:
- **IEEE 802.11 a:** tiene velocidad hasta 54 Mbps en distancias cortas y utiliza la radiofrecuencia de 5 Ghz.
- **IEEE 802.11 b:** permite la transmisión de datos a 11Mpbs y utiliza la radiofrecuencia de 2.4 Ghz la que puede llegar hasta 2.5 Km.

Fig. 3.31: Clasificación y tipos de redes inalámbricas

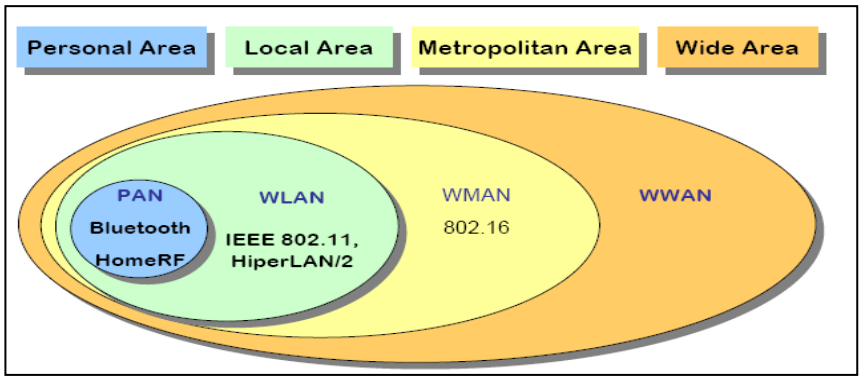
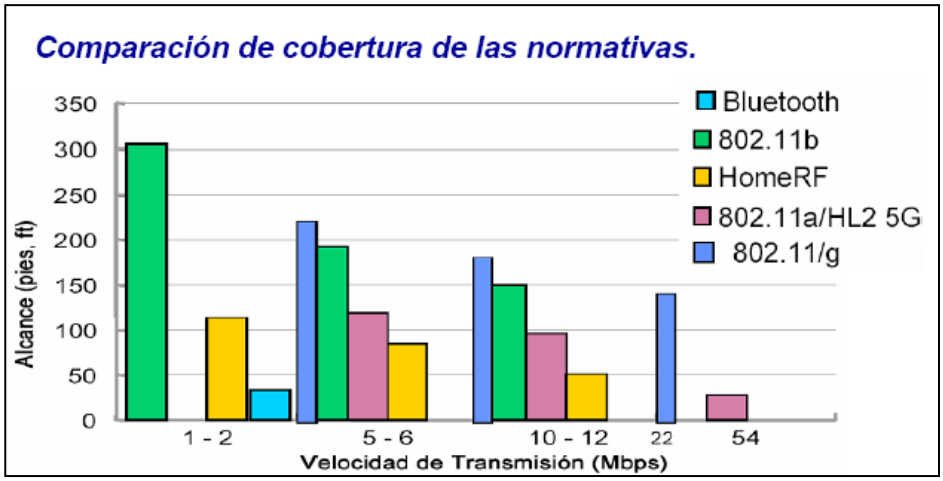
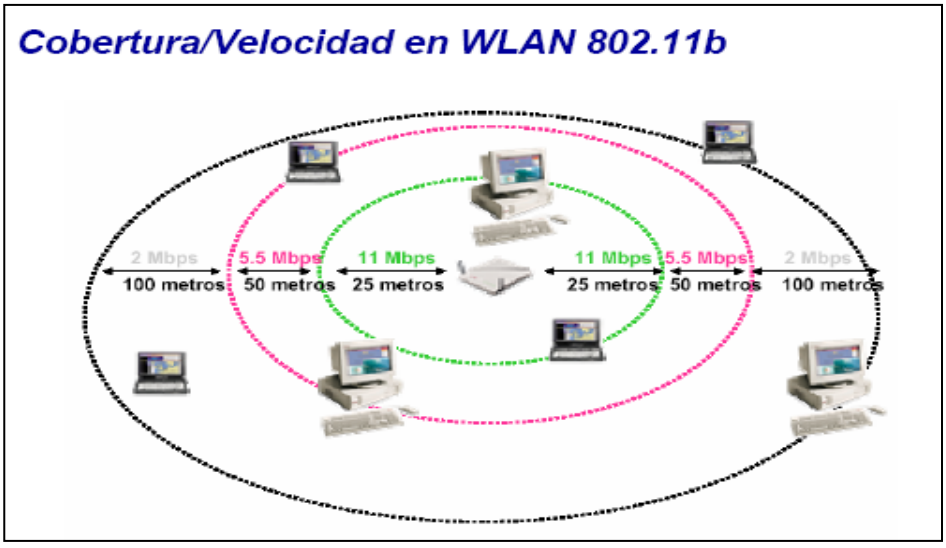


Fig. 3.32: Cuadro comparativo de las tecnologías inalámbricas



Fuente: WEB

Fig. 3.33**:** Diagrama de cobertura de la Norma IEEE 802.11b



Fuente: WEB

- **Seguridad**

  Para la implementación de la red inalámbrica se han definido utilizar el protocolo de seguridad **WPA-** Wifi Protected Access.

  WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x), con una clave de 128 bits y un vector de inicialización de 48 bits.

  La Norma **IEEE 802.1X** es una norma de la IEEE para Control de Admisión de Red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos.

  El protocolo 802.1x está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software *suplicante*. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

  Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación solo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

IV. Fase IV Consideraciones de Hardware/Software y Seguridad

Para el presente proyecto se han evaluado los recursos de hardware y software necesarios los mismos que describimos a continuación.

- **Definición de las características del Hardware y Software**

1. Características del Hardware

a. Solución con Access Point TP-Link TL-WA7210N

Esta solución consta de dos equipos Access Point, punto de acceso inalámbrico **TP-Link TL- WA7210N**

El Punto de Acceso Inalámbrico de Alta Potencia de TP-LINK, el TL-WA7210N está dedicado para las soluciones de WISP CPE y las soluciones de red inalámbrica de larga distancia. Posee una potencia de transmisión inalámbrica de 500mw y cuenta con una antena polarizada dual de 12dBi que proporciona una forma eficiente para captar y mantener una señal estable para una conexión de red inalámbrica que abarca múltiples kilómetros.

Fig. 3.35: Access Point TP LINK- TL-WA7210N

Características Generales

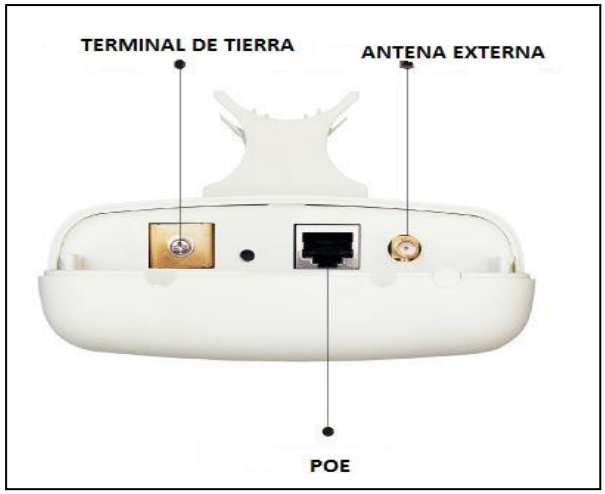
- ✓ La antena direccional de 12dBi con doble polarización incrementa el alcance inalámbrico
- ✓ El amplificador de potencia dedicado y el amplificador de bajo ruido mejora el rendimiento radio
- ✓ Hasta 500mW de potencia (solo países fuera de la Unión Europea) para transmisión a larga distancia
- ✓ Carcasa impermeable, protección contra rayos de 4KV, terminal de puesta a tierra integrado y protección ESD de 15KV
- ✓ Compatible con IEEE 802.11b/g/n, velocidad inalámbrica hasta 150Mbps
- ✓ Soporta los modos de funcionamiento Router Cliente de AP (Cliente WISP), Router con AP y AP
- ✓ Hasta 60 metros (200 pies) de despliegue flexible con el inyector Power over Ethernet incluido
- ✓ Conector RP-SMA externo para de antena de más alta ganancia
- ✓ Soporta Alineamiento de antena, Configuración de distancia, Ping Watch Dog y Test de velocidad inalámbrica

Ejemplo de implementación:

Fig. 3.36: Ejemplo de implementación de TP LINK –TL WA7210N

Fuente Web

Fig. 3.37: Componentes de TP LINK-TL- WA7210N



Fuente Web

b. Solución con DWA-140 (hardware)

Solución que consta de 20 tarjetas inalámbricas USB para el municipio distrital de la esperanza.

Fig. 3.38**:** USB Wireless N DWA-140

Fuente Web

Características Generales

- ✓ Banda de frecuencia de 2,4 GHz.
- ✓ Puede establecer una conexión segura con una red inalámbrica mediante WPA™/WPA2™ (acceso protegido Wi-Fi®), los estándares de cifrado que ofrecen el nivel de seguridad de datos y comunicaciones más elevado disponible hasta la fecha.
- ✓ Puede colocar el DWA-140 en prácticamente cualquier parte de su espacio de trabajo para lograr la mejor recepción posible.
- ✓ Especificación para LAN inalámbrica draft 802.11n, compatible con los dispositivos 802.11b/g.
- ✓ Conexión Fast USB 2.0 para ordenador de sobremesa o notebook.
- ✓ Tasa de transferencia de datos bruta de 300 Mbps.
- ✓ Se activa a través del puerto USB; no necesita ninguna fuente de alimentación externa.
- ✓ Soporte para los sistemas operativos Windows 7/VISTA/XP/2000.
- ✓ Dos antenas internas integradas.
- ✓ Gestor inalámbrico de D-Link para el fácil acceso a las redes a las que se accede frecuentemente.
- ✓ Admite redes de infraestructura a través de un punto de acceso o router inalámbrico.

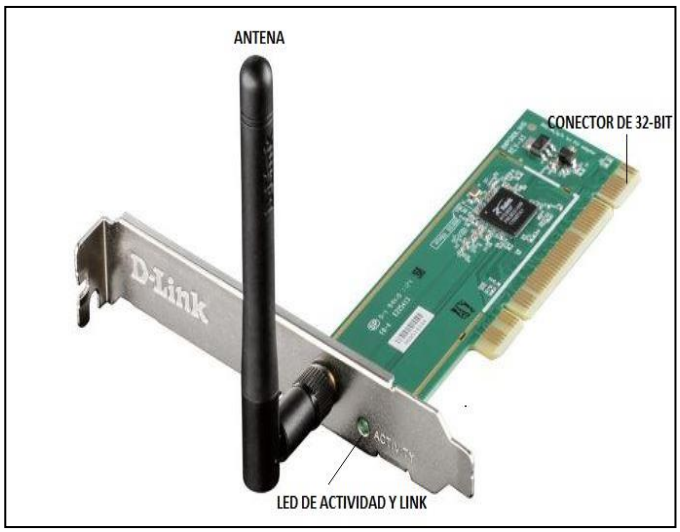
c. Solución con Dlink – Wireless N DWA-525

Solución con tarjetas inalámbricas tipo PCI, para implementarse en el municipio distrital de la Esperanza.

Fig. 3.39**:** Tarjeta Wireless D-Link Wireless N DWA-525

Fuente Web

Fig. 3.40**:** Descripción de la Tarjeta Wireless D-Link Wireless N DWA-525



Fuente Web

Características Generales

- ✓ Banda de frecuencia de 2,4 GHz.
- ✓ Permite conexión inalámbrica hasta 150 Mbps
- ✓ Compatible con 802.11 b/g/n
- ✓ Proporciona hasta 11 para 802.11b, 54Mbps para 802.11g, 150Mbps para 802.11n
- ✓ Soporta WEP, WPA-Personal/Empresa, WPA2-Personal/Empresa, WPS
- ✓ Antena de 2dbi reemplazable

2. Características del Software

El software de instalación de los equipos Access Point viene incluidos en los productos o hardware de los equipos ya presentados anteriormente.

A continuación se muestra las pantallas de instalación y configuración de los equipos Access Point utilizados en el proyecto. ***Ver pantallas de Instalación y configuración de equipos Access Point. Págs. 99,100.***

- **Definición de niveles de seguridad**

Para alcanzar un buen nivel de seguridad en una red inalámbrica, es necesario combinar los mecanismos propios de las redes inalámbricas, con mecanismos empleados en una red cableada. Dichos métodos se pueden englobar en dos grupos. Un grupo de métodos los cuales podremos considerar básicos**,** y que estaría compuesto por WEP, WPA, SSID, filtrado de direcciones MAC. Y un segundo grupo de métodos más avanzados**,** que mejorarían el nivel de seguridad junto con los primeros. Este segundo grupo englobaría TIKP, EAP, LEAP.

Para el presente proyecto se han definido los mecanismos de seguridad WPA-Enterprise, que vienen incluidos en los equipos Access Point **TP-Link TL-WA7210N** y uso de EAP a través de un Servidor Radius para brindar mayor seguridad a la información.

Uso de WPA/WPA2

WPA2 o IEEE 802.11: incluye un algoritmo de cifrado AES (Adavanced Encryption Estándar), desarrollado por el NIS, se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. El cual, requiere un hardware potente para analizar sus algoritmos.

Wpa: Soluciona gran parte de las debilidades de WEP y se considera suficientemente seguro

Se distingue por tener una distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autenticación.

WPA incluye las siguientes tecnologías:

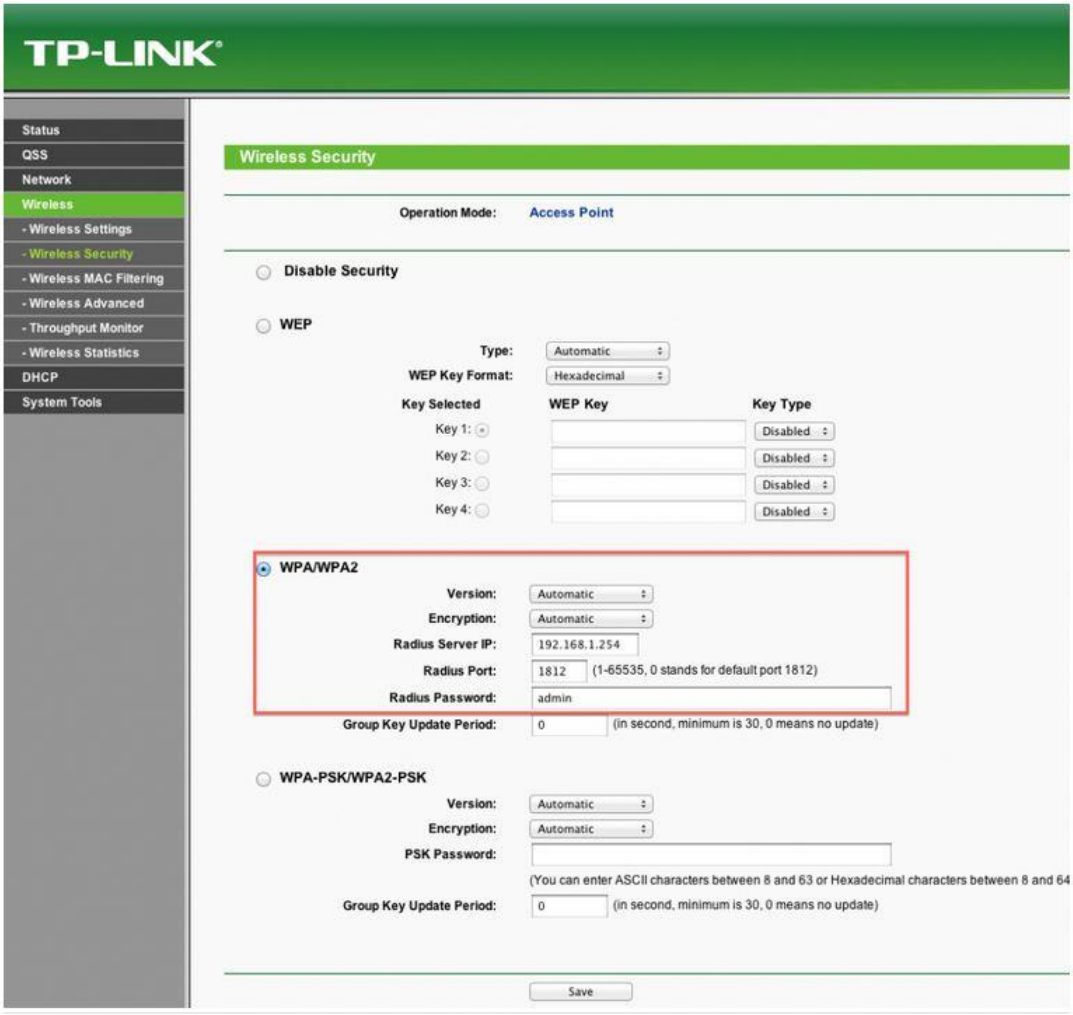
IEEE 802.1X. Estándar del IEEE que proporciona un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*), como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso.

EAP: Definido en la RFC 2284, es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*).

TKIP (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

MIC (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

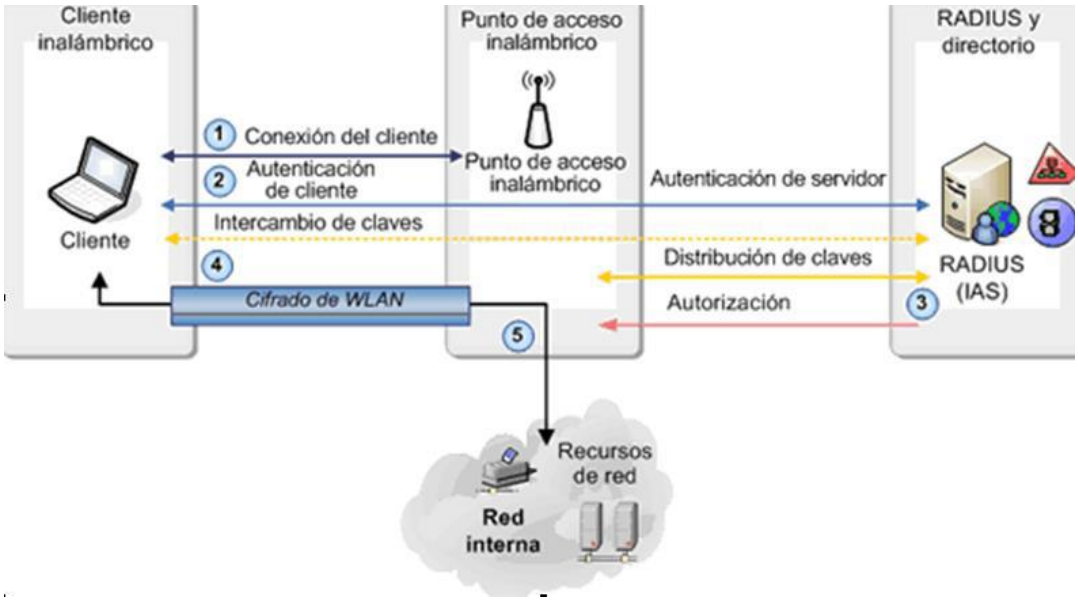
Fig. 3.41: Configuración de WPA/WPA2 en Access Point



La autenticación se realizara de la siguiente manera.

1. Un ordenador portátil solicita acceso a la red WiFi (punto de acceso TP-LINK) mediante un usuario y password, proporcionado por el departamento de informática del centro.
2. El punto de acceso enviará las credenciales al servidor RADIUS para que sean autenticadas. Si no son válidas, no se concederá la autorización para acceder a la red y se informará al cliente (autenticación incorrecta)
3. En caso que las credenciales del usuario sean correctas, el servidor Radius autorizará al cliente al acceso a la red, comunicándoselo al punto de acceso.
4. El punto de acceso permitirá al dispositivo móvil establecer una conexión con él.

Fig. 3.42: Funcionamiento de Servidor Radius



V. Fase V Consideraciones de Implementación y Costos

1. Evaluar las especificaciones del proyecto

Se evaluaron, las configuraciones de los equipos Access Point, servidor RADIUS, normativas de seguridad a utilizarse, como son WPA, WPA2 a utilizarse en la implementación de nuestra red inalámbrica para la Municipalidad Distrital de la Esperanza.

2. Costos de la Implementación de la red.

Se consideró para la implementación de la Red Inalámbrica a equipos Access Point **TP-Link TL- WA7210N**, así como para algunas áreas de la municipalidad se tomó en cuenta equipos, las tarjetas adaptadoras para cada Pc's. Para la implementación de la misma.

Todos los costos de implementación están especificados en el estudio de factibilidad económica. Ver Factibilidad Económica. Págs. 65-72

3. Implementación de la red.

A continuación se muestran las pantallas de instalación y configuración del Servidor de Seguridad Radius, la autenticación de usuarios con el PEAP, y configuración de los equipos Access Point utilizado en el proyecto.

Ámbito de aplicación: Municipalidad Distrital de la Esperanza
Alcance: Indoor 100mts; Outdoor 400mtrs
Tecnología de red: IEEE 802.11b/g/n, radiofrecuencia, 2.4ghz
Tipología: WLAN / WI-FI
Topología: Punto de Acceso / Infraestructura
Seguridad: WPA-WPA2 /

INSTALACIÓN DE SERVIDOR RADIUS

Los pasos que usaremos para lograrlo son los siguientes:

- ✓ Instalación de FreeRadius
- ✓ Configuración de FreeRadius
- ✓ Configuración del Punto AP
- ✓ Configuración de los clientes windows 7, para autenticar en FreeRadius.
- ✓ Configuración de los clientes Android, para autenticar en FreeRadius.

A. INSTALACIÓN DE FREERADIUS

En la instalación del FreeRadius utilizamos como plataforma el sistema operativo Ubuntu Desktop 15.04

Fig.3.43: Versión Ubuntu 15.04

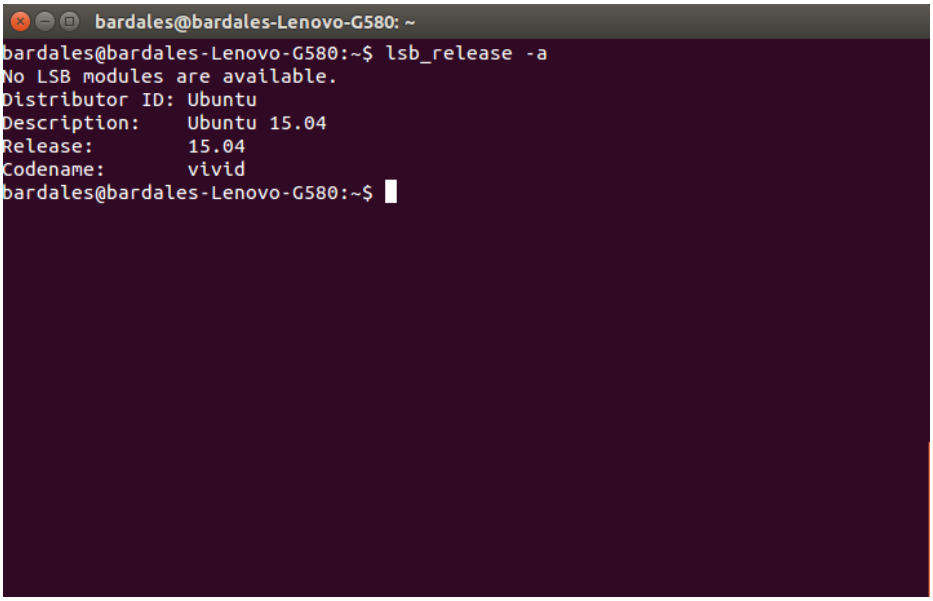
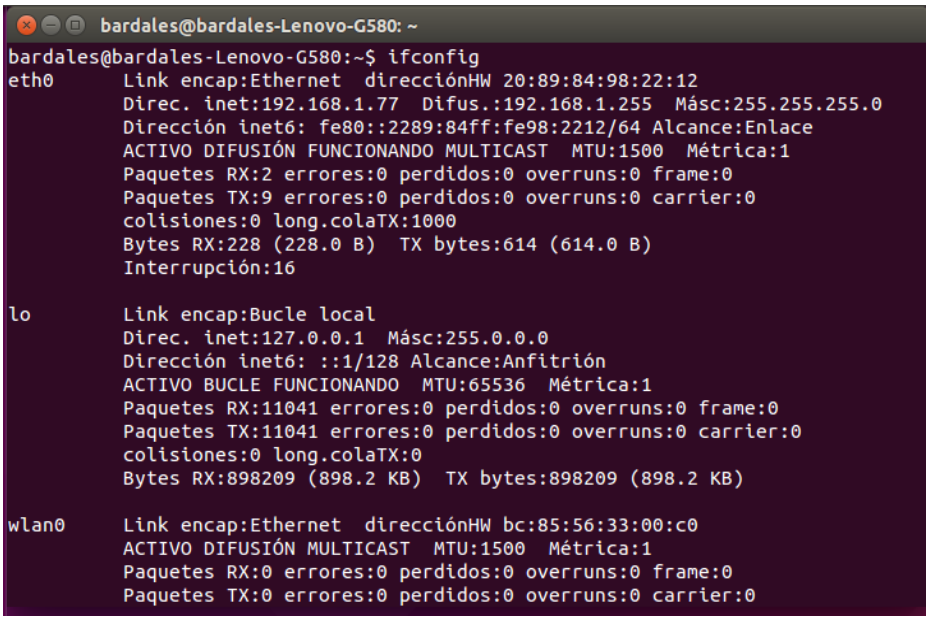


Fig. 3.44: Configuración de red Ubuntu 15.04



Para comenzar la instalación del servidor FreeRadius, debemos tener instalado Apache, PHP y Mysql. Abrimos un terminal en nuestro Ubuntu 15.04. Y ejecutamos los siguientes comandos.

- **Instalación Apache**

1. Instalamos Apache

```
root@bardales-Lenovo-G580:/home/bardales# apt-get install apache2
```

2. Reiniciamos Apache

```
root@bardales-Lenovo-G580:/home/bardales#  /etc/init.d/apache2 start
```

3. El directorio donde se almacenan tus documentos web es: **/var/www/html**

Para comprobar que todo se instaló correctamente, escribimos en la barra de direcciones de nuestro navegador lo siguiente: **http://localhost**

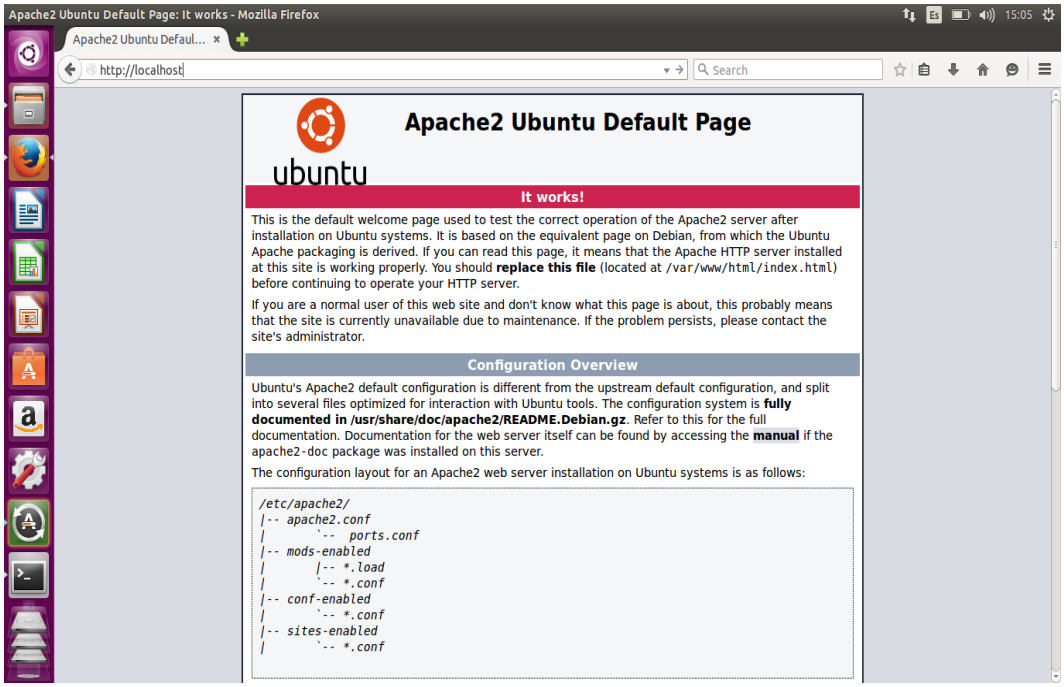
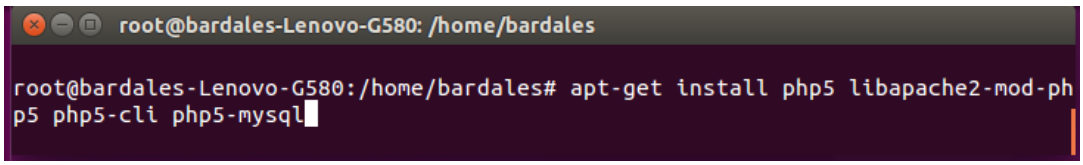
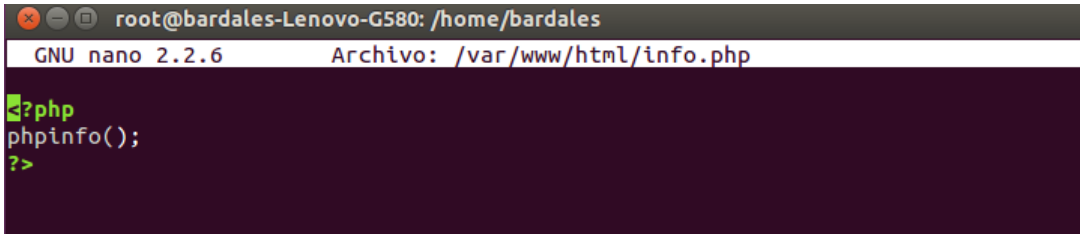


Fig.3.45**:** Verificación Instalación Apache2

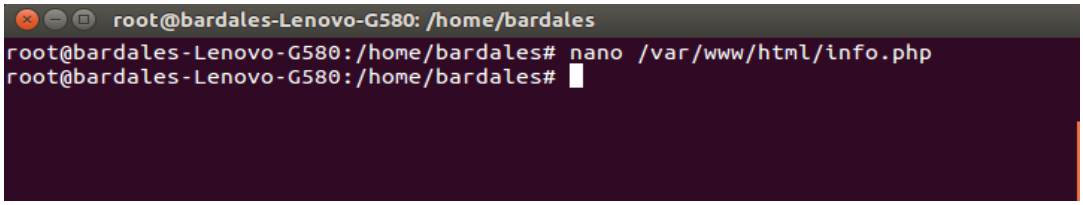
- **Instalación de php**

1. Instalamos librerías

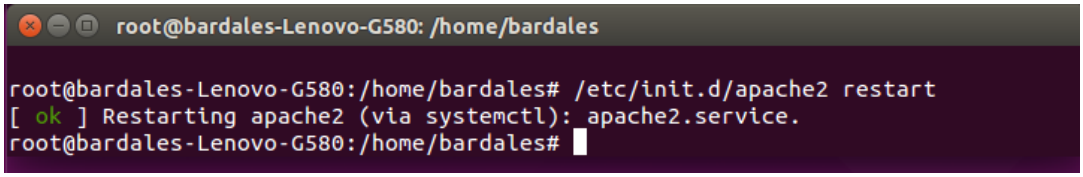




2. Editamos una página de demostración:

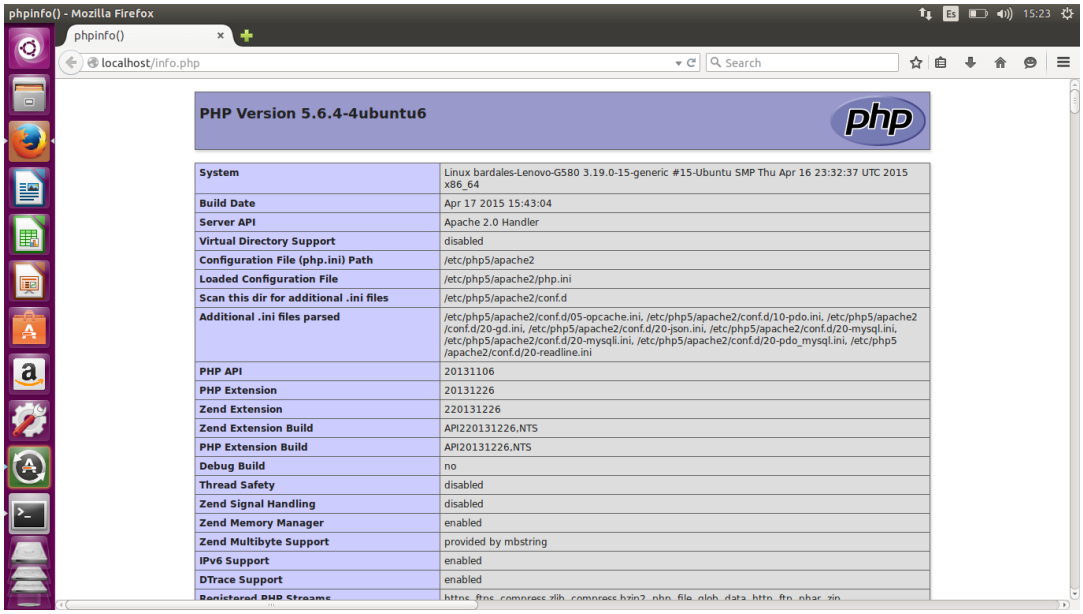


3. Reiniciamos PHP



4. Para ejecutar el script ve a esta dirección: http://localhost/info.php

Debes ver una página con información sobre tu instalación de PHP.

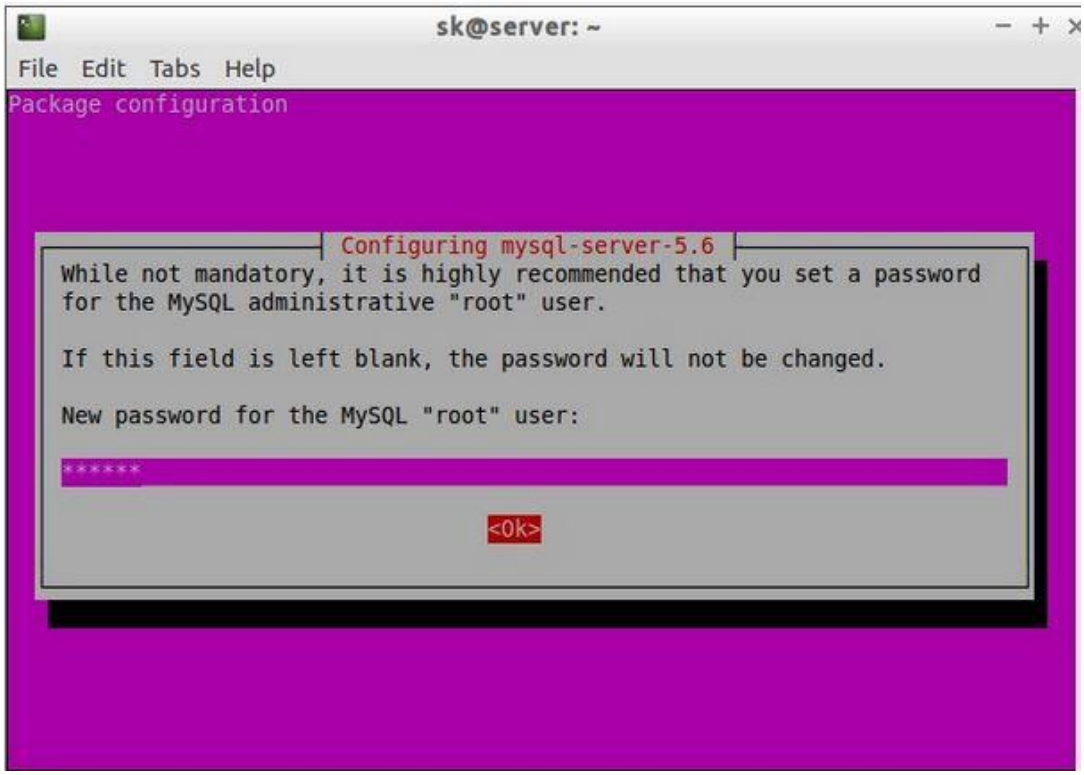


➢ Instalación de Mysql

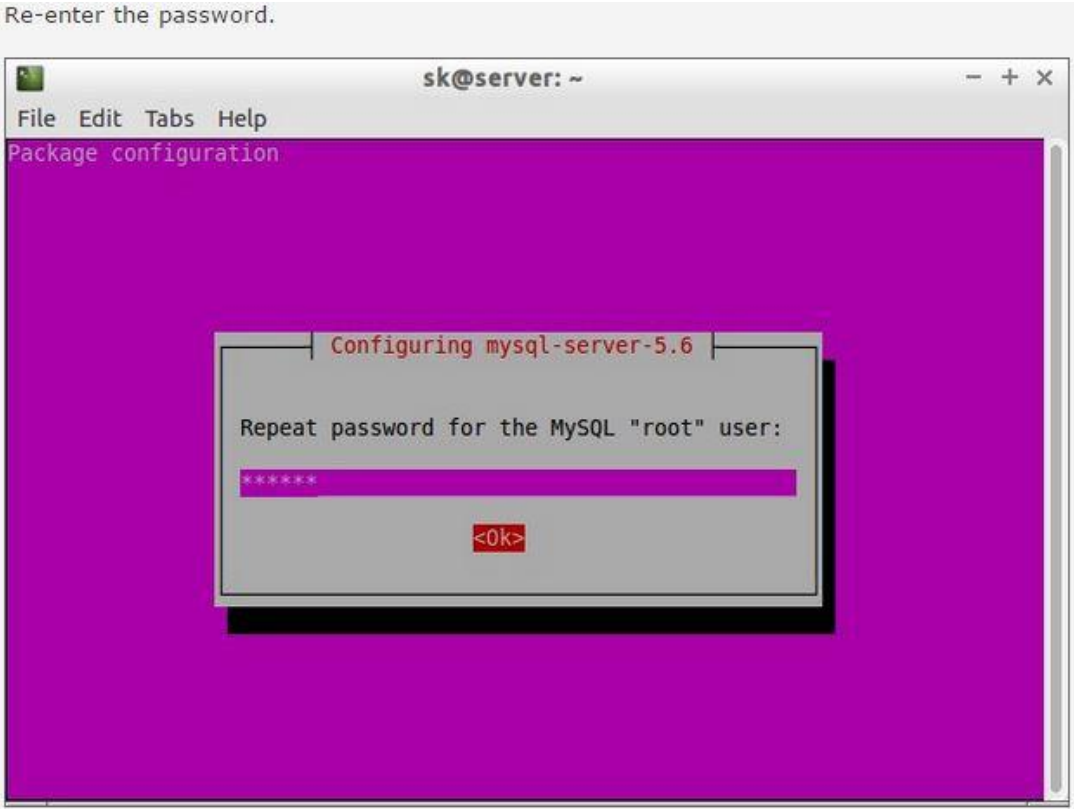
1.- Instalamos Mysql

```
root@bardales-Lenovo-G580:/home/bardales# apt-get install mysql-server mysql-client
```

Durante la instalación, te preguntará por un password el cual ingresarás.

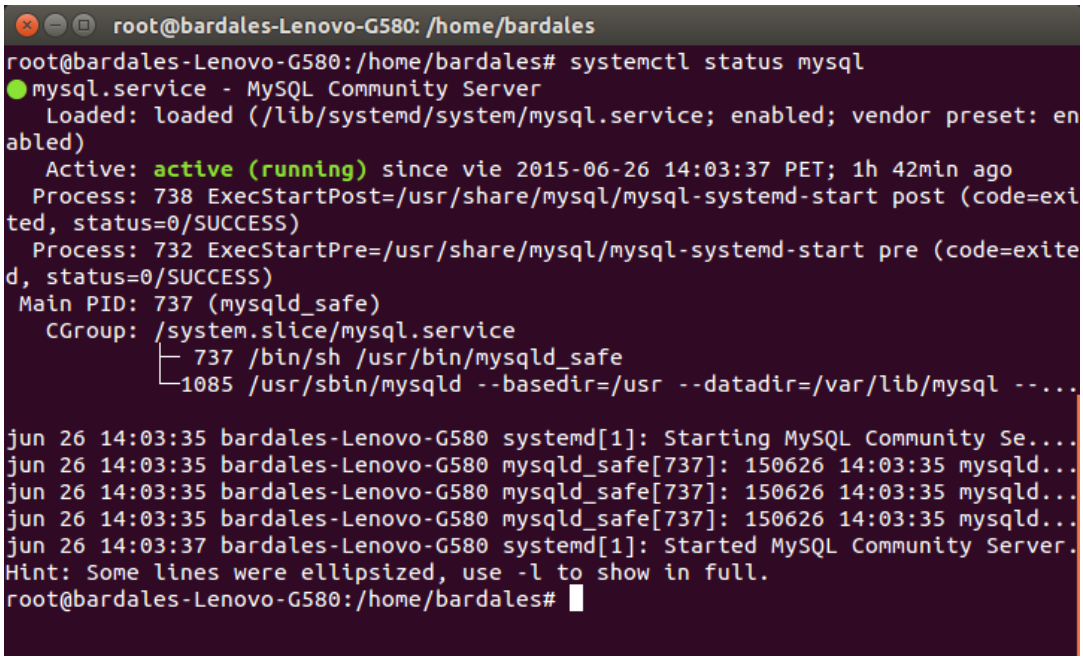


2.-Colocar nuevamente el password ingresado anteriormente.



3.- Verificamos el estado de MYSQL

```
root@bardales-Lenovo-G580:/home/bardales# systemctl status mysql
```

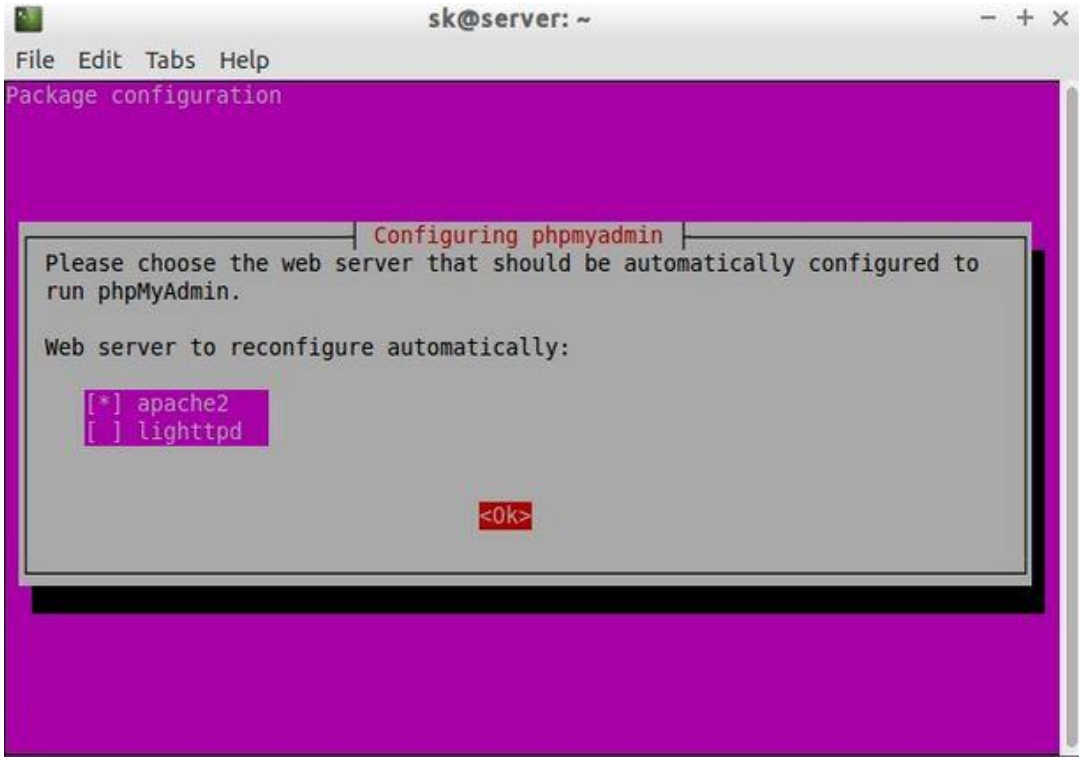


- **Instalación de Phpmyadmin**

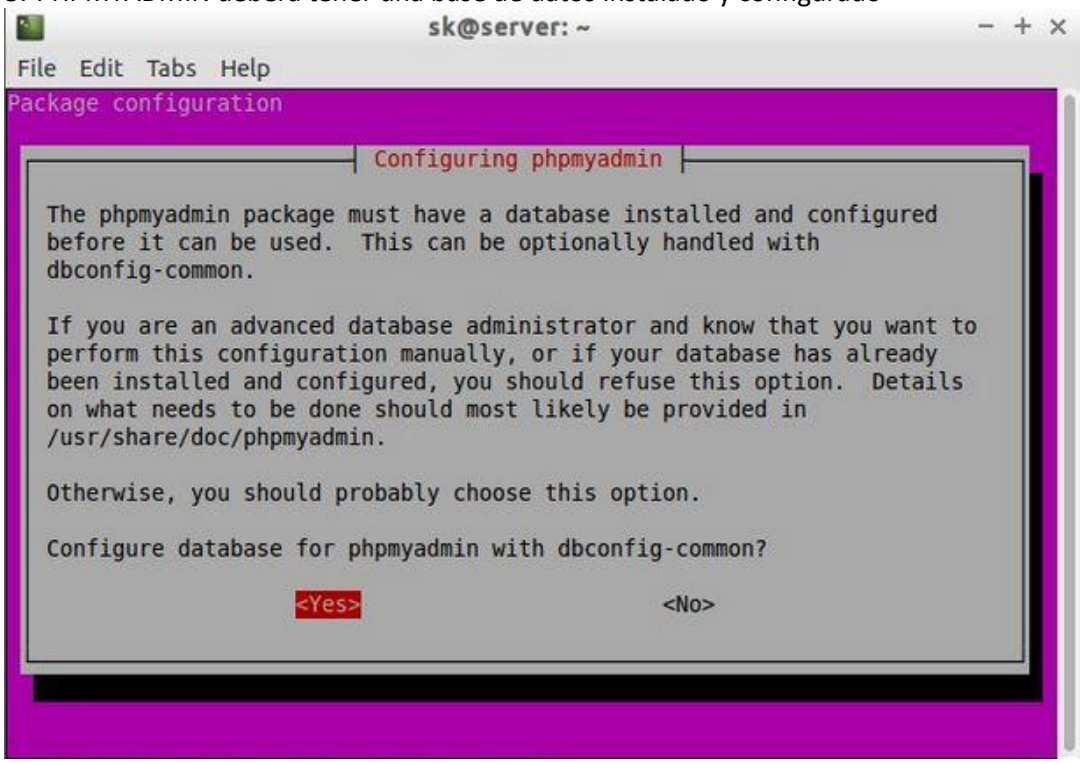
1.- Instalamos Phpmyadmin

```
root@bardales-Lenovo-G580:/home/bardales# apt-get install phpmyadmin
```

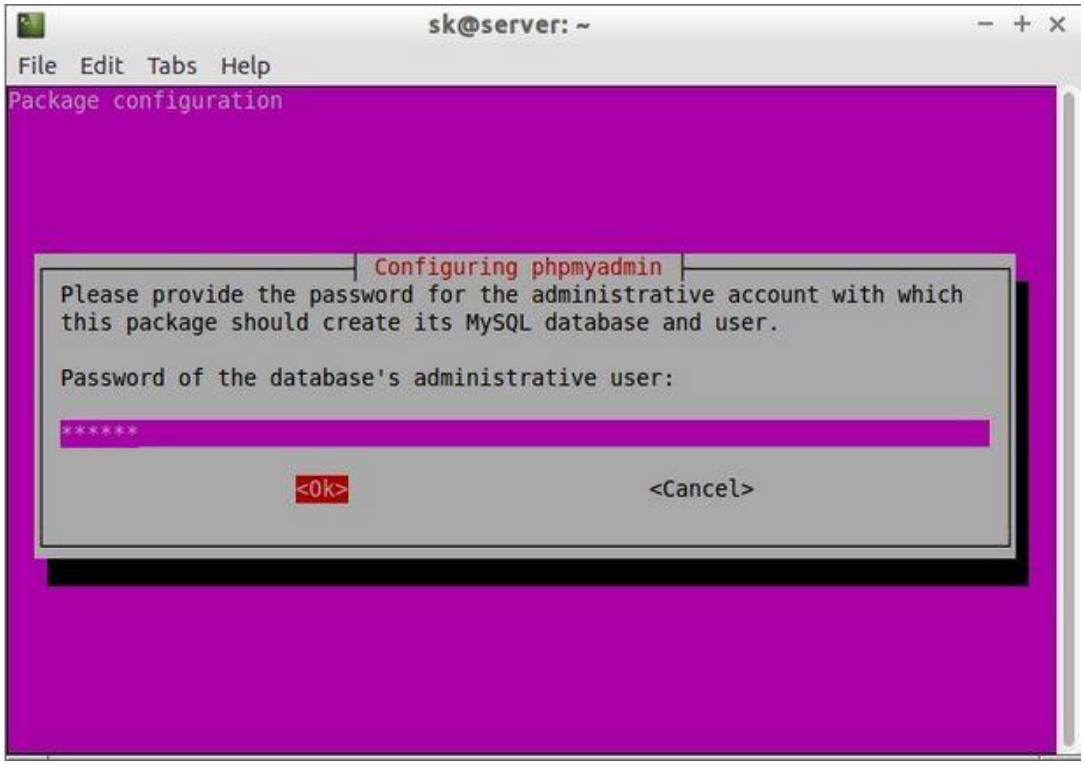
2.-Seleccionar Servidor Web para configurar Phymyadmin : Apache2



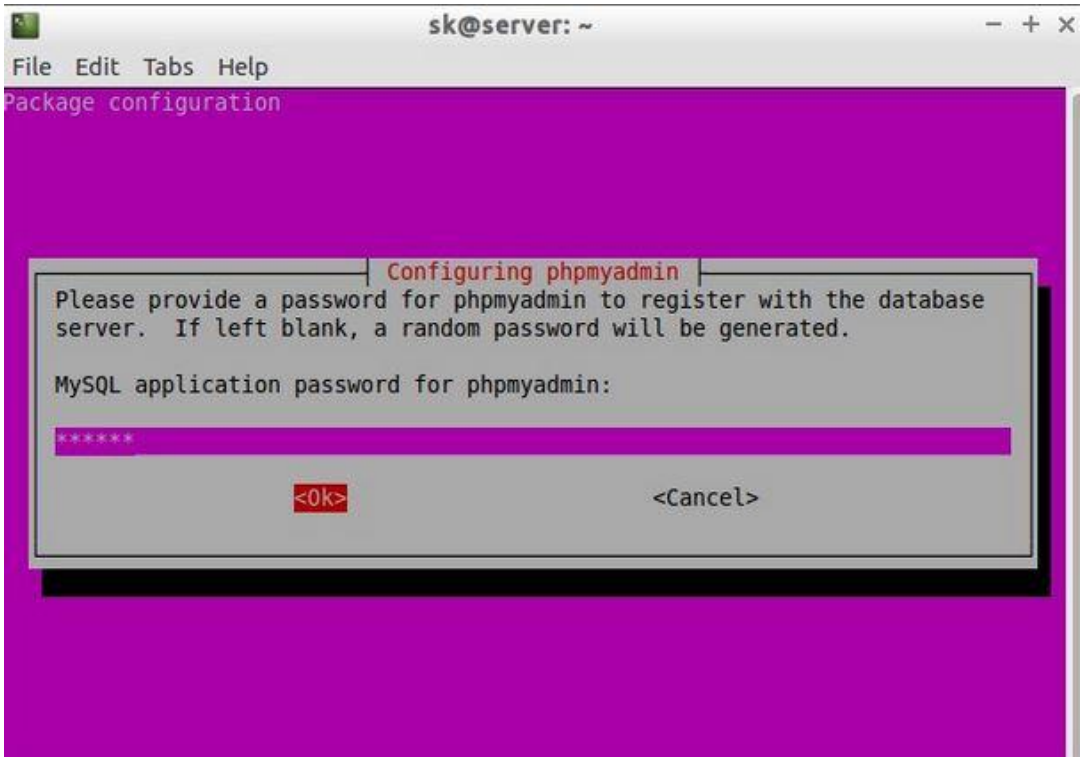
3.-PHPMYADMIN deberá tener una base de datos instalado y configurado



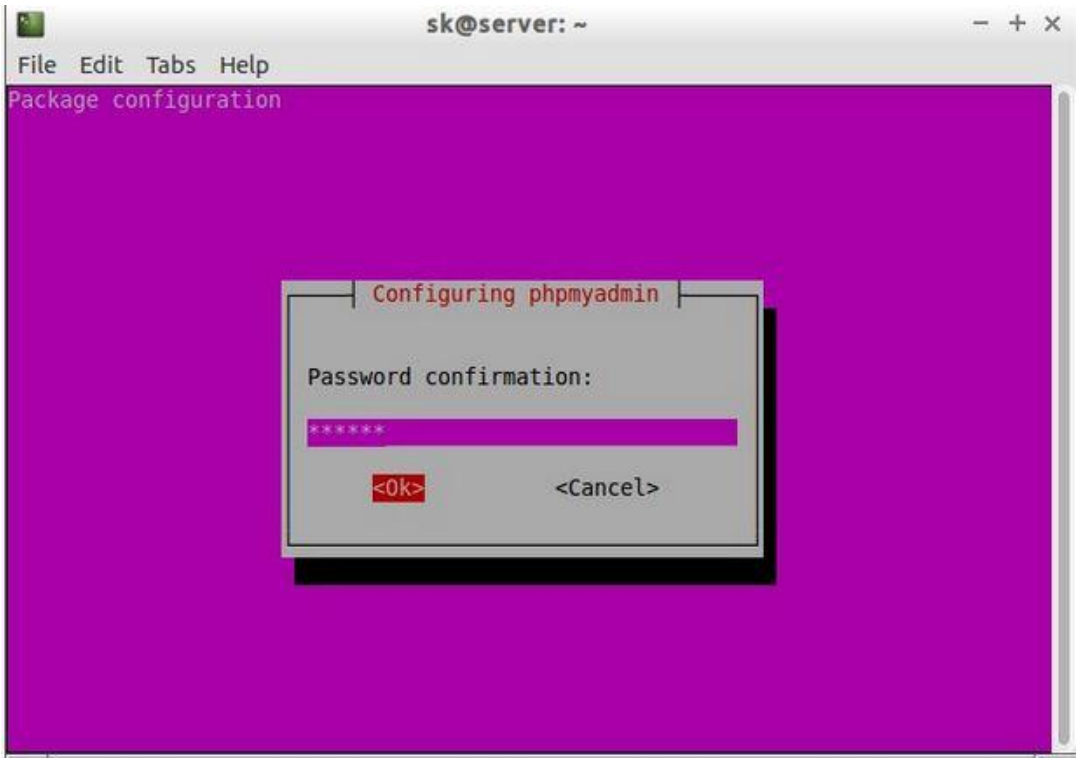
4.-Ingresar el password (root) de la base de datos



5.-Ingresar el password para phpmyadmin

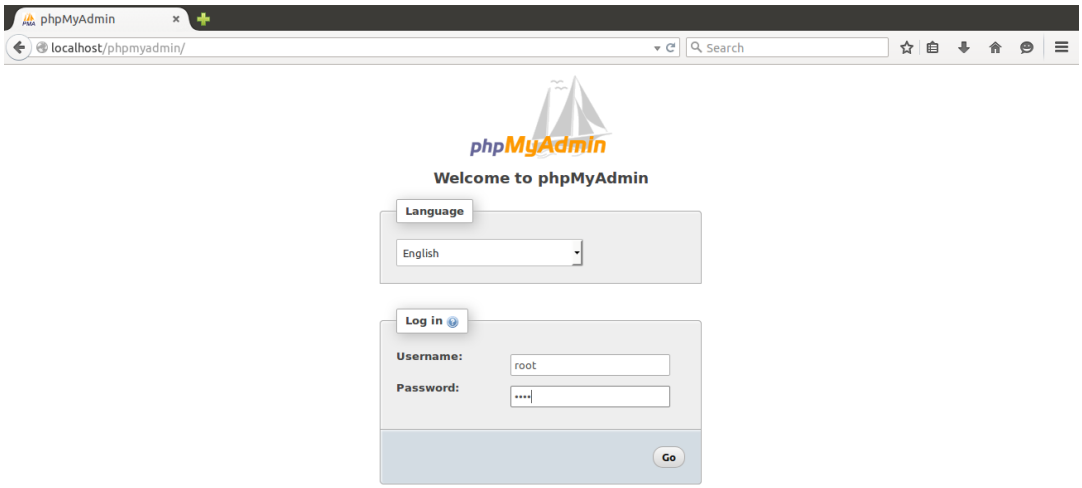


6.- Reingresar password



6.- Verificamos PHPMYADMIN en un navegador de Internet

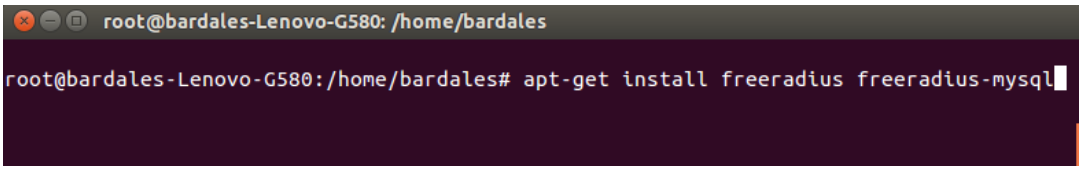
http://localhost/phpmyadmin



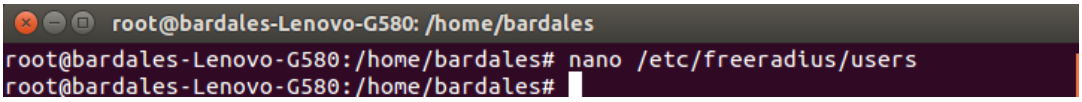
B. CONFIGURACIÓN FREERADIUS

FREERADIUS como servidor de autenticación ofrece un rendimiento y potencia muy elevada, es compatible con casi cualquier plataforma o sistema operativo (Windows, Linux,MacOS,etc) y da soporte para gran cantidad de módulos de autenticación.

1.- Con el comando apt-get, instalaremos el paquete freeRadius, junto con el paquete freeRadius-mysql que nos permitirá la integración de freeRadius en la base de datos:

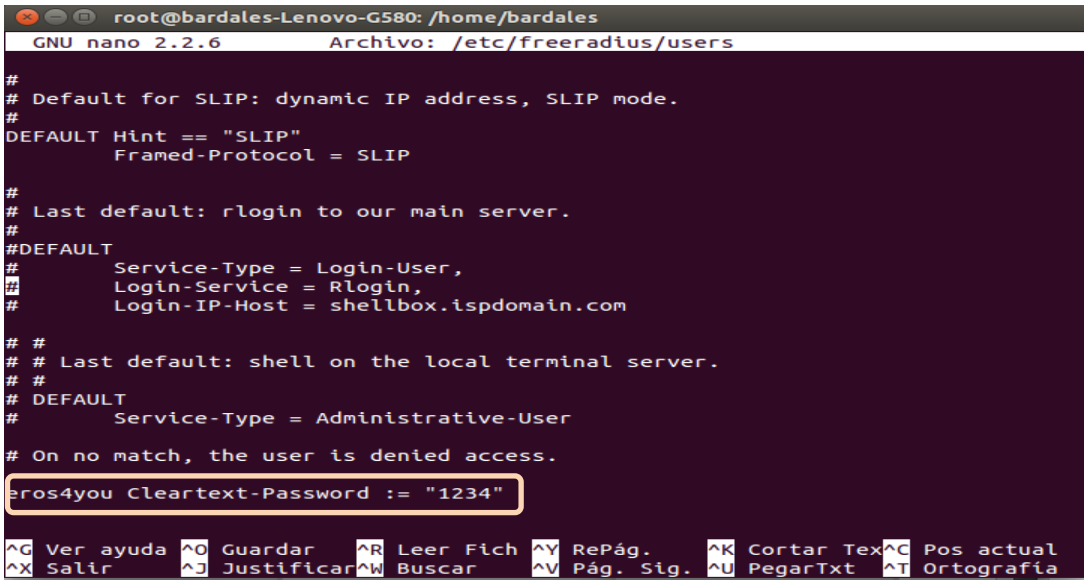


2.-Editamos (por ejemplo, con el editor de texto nano) el archivo /etc/freeradius/users y creamos un usuario para hacer las pruebas del funcionamiento correcto del servidor freeRadius:

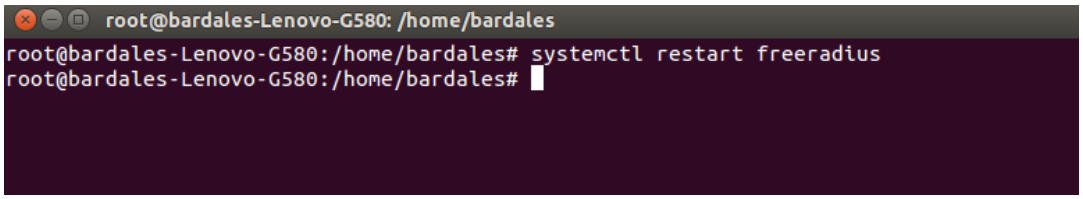


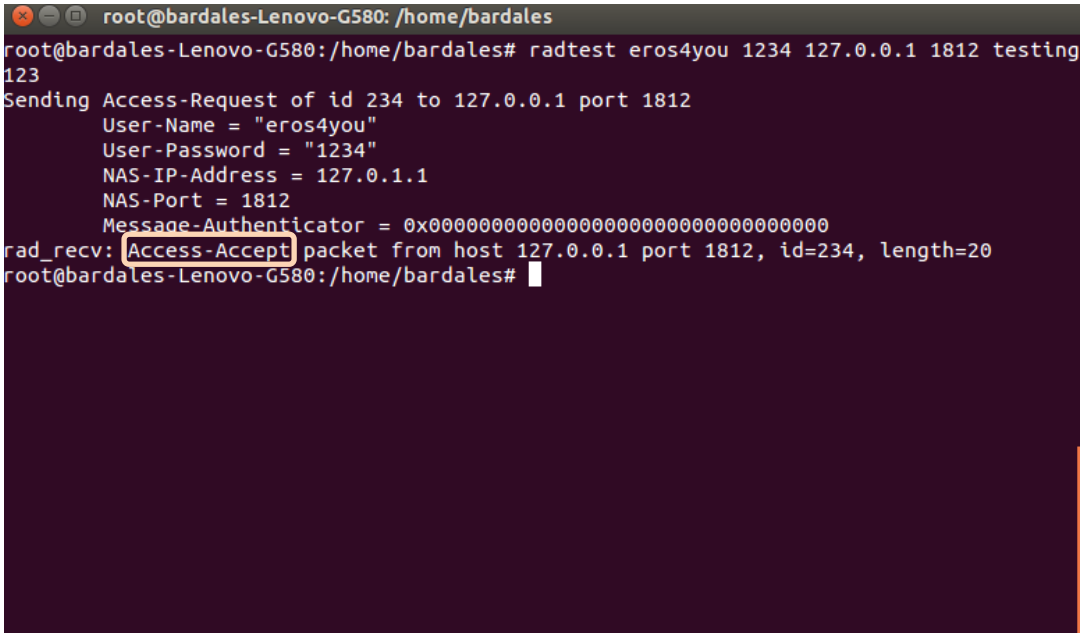
3.- En el archivo /etc/freeradius/users hay varios ejemplos, ya creados, de diferentes tipos de usuarios los cuales podemos reutilizar para la prueba. Podemos descomentar (quitar el carácter # de delante de la línea) uno de estos usuarios o bien, crear uno nuevo con nuestros propios datos y lo ponemos al final del archivo. La siguiente pantalla muestra el que yo he usado:

eros4you Cleartext-Password := “1234”



4.- Una vez modificado el fichero anterior, probaremos mediante la utilidad propia de freeRadius, denominada radtest, si funciona la autenticación. Pero antes, es importante reiniciar el servidor para que los cambios hechos en el fichero surtan efecto.



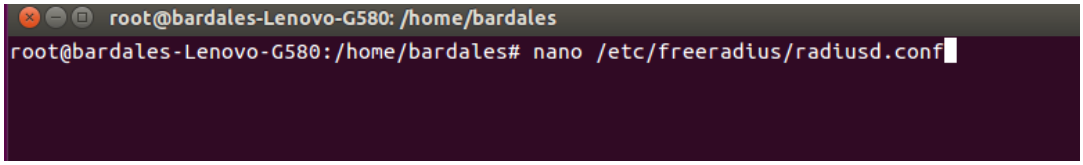


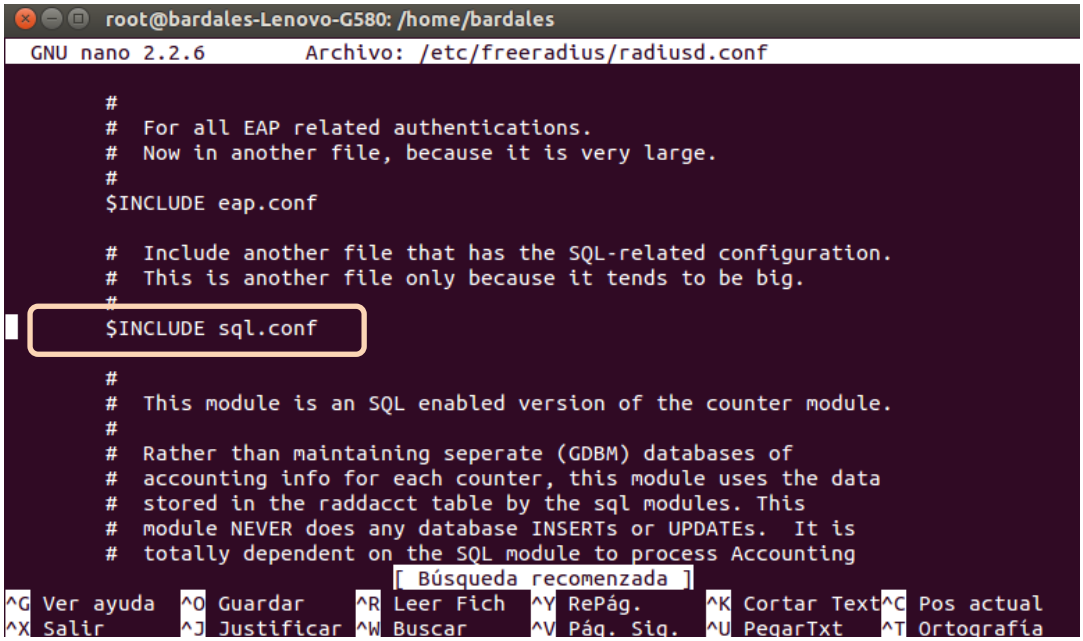
Si todo está configurado correctamente, debemos ver en el terminal de Ubuntu la información mostrada en la siguiente imagen. Es muy importante asegurarnos de recibir un Access-Accept del Access-Request que se ha enviado.

Inicialmente vemos que funciona correctamente, ahora lo siguiente será integrarlo con MySQL para utilizar los usuarios de base de datos, en lugar del usuario de pruebas del fichero users.

- **Integración De Freeradius Con Mysql**

1.-Configuramos seguidamente el servidor freeRadius para que pueda leer los datos desde MySQL. En este punto, es necesario editar el archivo /etc/freeradius/radiusd.conf y descomentar la línea $INCLUDE sql.conf

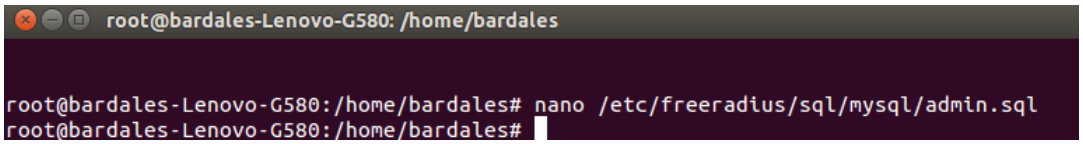


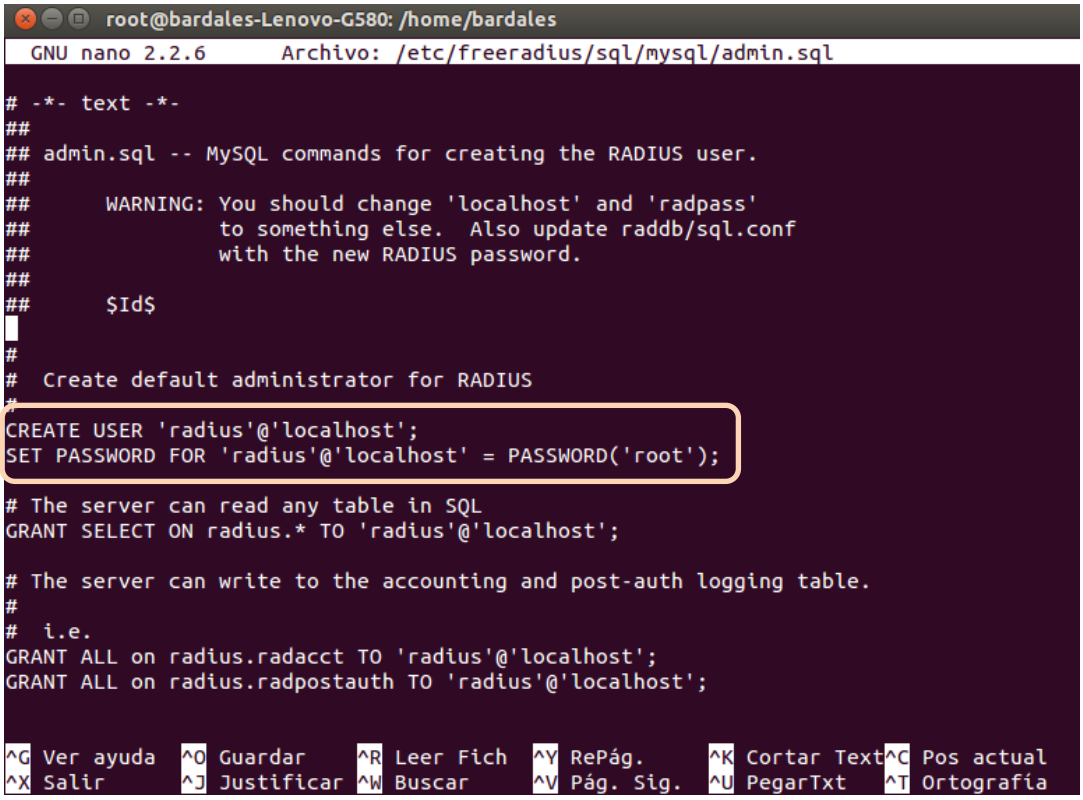


2.- Accedemos a la administración de MySQL y creamos la base de datos que albergará la configuración de freeRadius y un usuario para la misma. En este caso asumimos que la base de datos se llama radius:

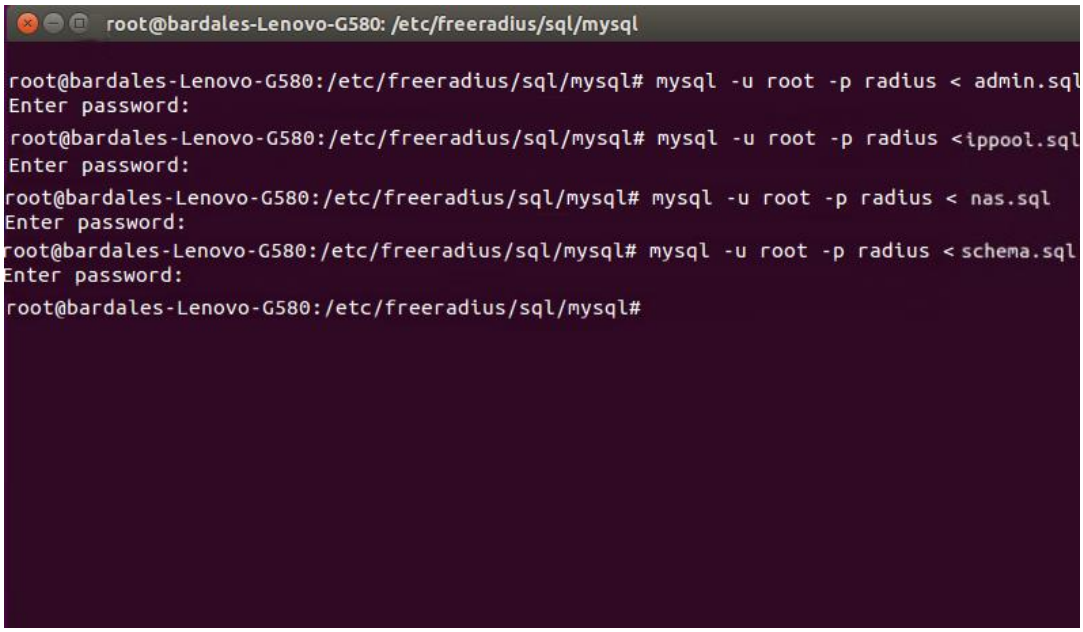
```
root@bardales-Lenovo-G580:/home/bardales# mysql -u root –p
Enter password:
mysql > CREATE DATABASE radius;
mysql > exit;
```

Para el usuario, editaremos el fichero /etc/freeradius/sql/mysql/admin.sql con el fin de que quede de la siguiente manera. Nótese que el usuario, para la base de datos creada, se llama radius y su clave es root:





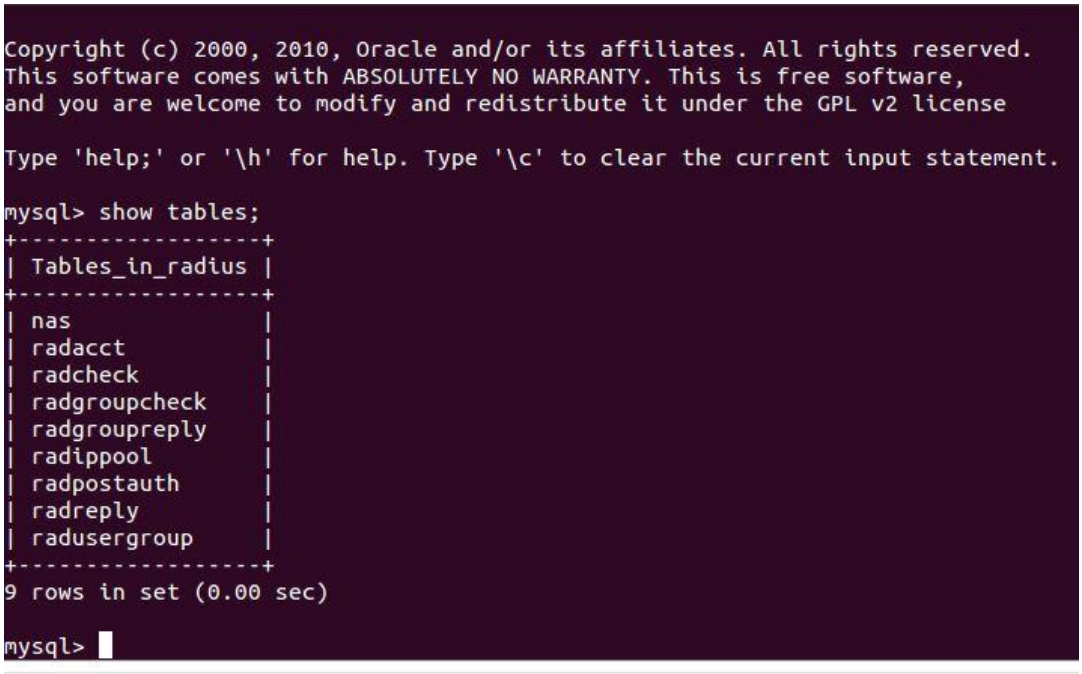
3.- Ahora introduciremos, mediante 4 scripts de base de datos, los datos de las tablas SQL de freeRadius en MySQL para el correcto funcionamiento del servidor. Estos scripts, están situados dentro del directorio /etc/freeradius/sql/mysql/



4. Verificamos si las tablas SQL se han creado correctamente, podemos hacer lo siguiente:

```
root@bardales-Lenovo-G580:/home/bardales# mysql -u root -p radius
Enter password:
mysql > show tables;
mysql > exit;
```

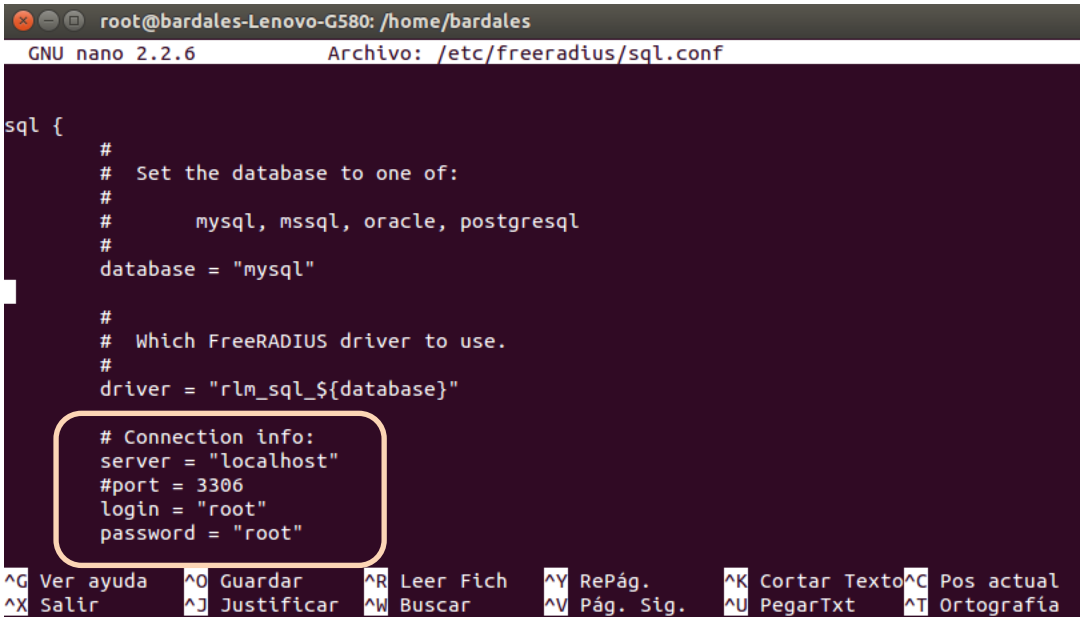
Si vemos los datos tal y como los muestra la siguiente ventana, todo habrá salido correctamente:



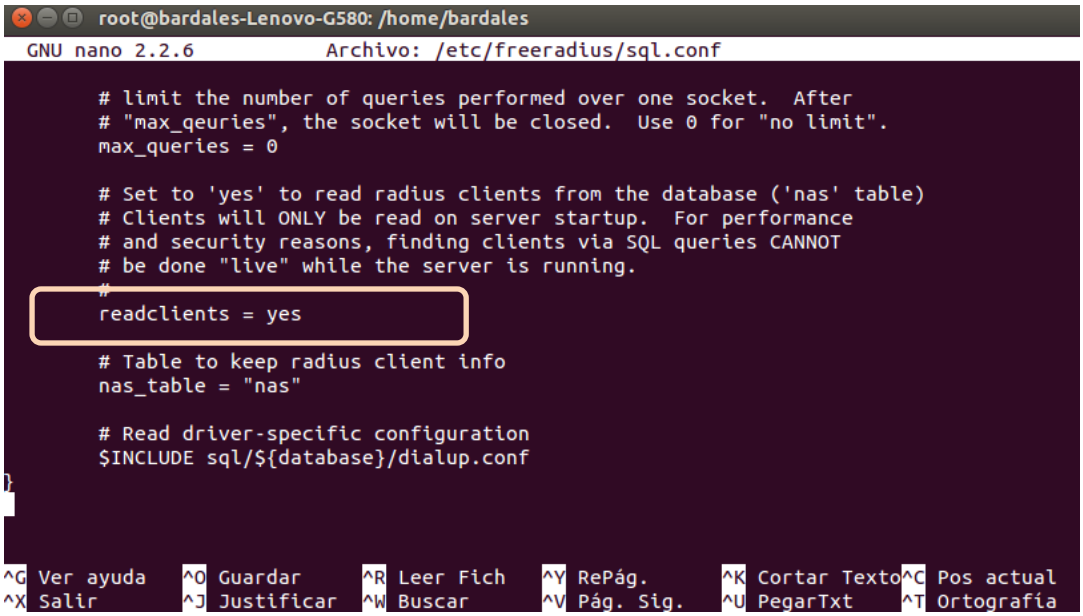
5.- Editamos el archivo /etc/freeradius/sql.conf para establecer una conexión entre nuestro servidor freeRadius y la base de datos MySQL.

```
root@bardales-Lenovo-G580:/home/bardales# nano /etc/freeradius/sql.conf
```

Buscamos la etiqueta Connection info y la dejamos como sigue:

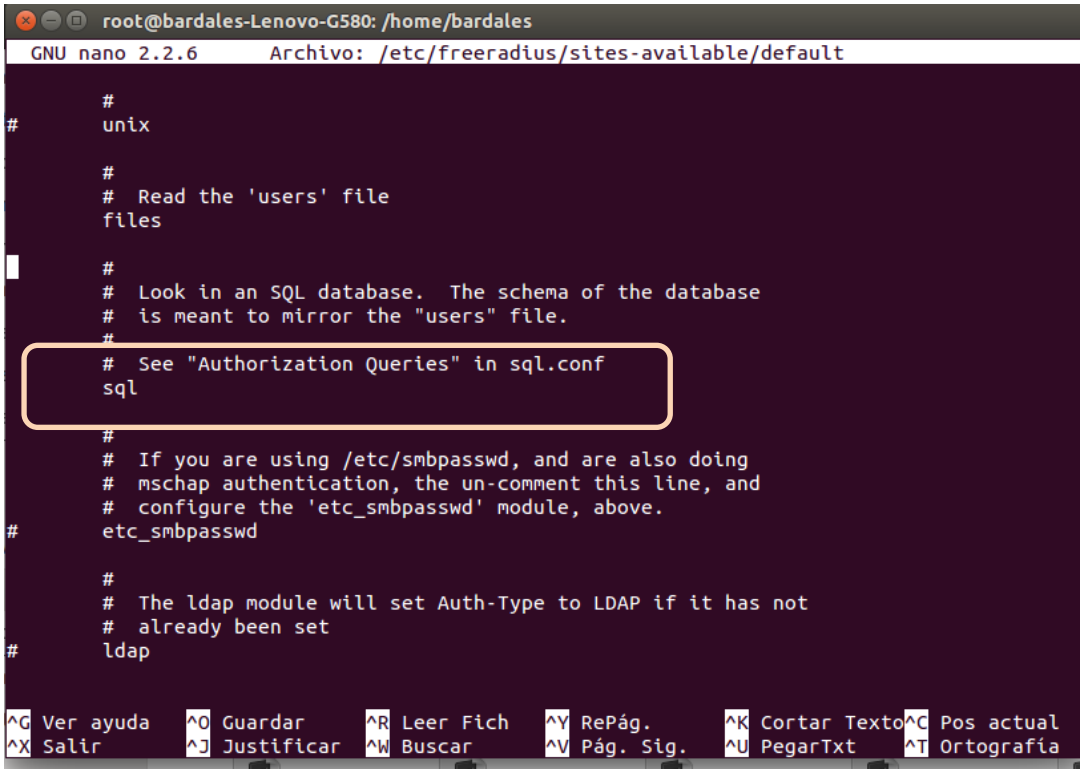


Y también, en el mismo fichero, descomentamos la línea readclients = yes , esto permite que radius lea los usuarios de la tabla nas de la base de datos.



6. Editamos el archivo /etc/freeradius/sites-available/default y descomentar la variable sql en las secciones authorize{} y accounting{}.Esto es necesario para que el servidor pueda obtener los datos desde las tablas SQL de la base de datos radius y así poder autenticar y autorizar los usuarios que creemos:

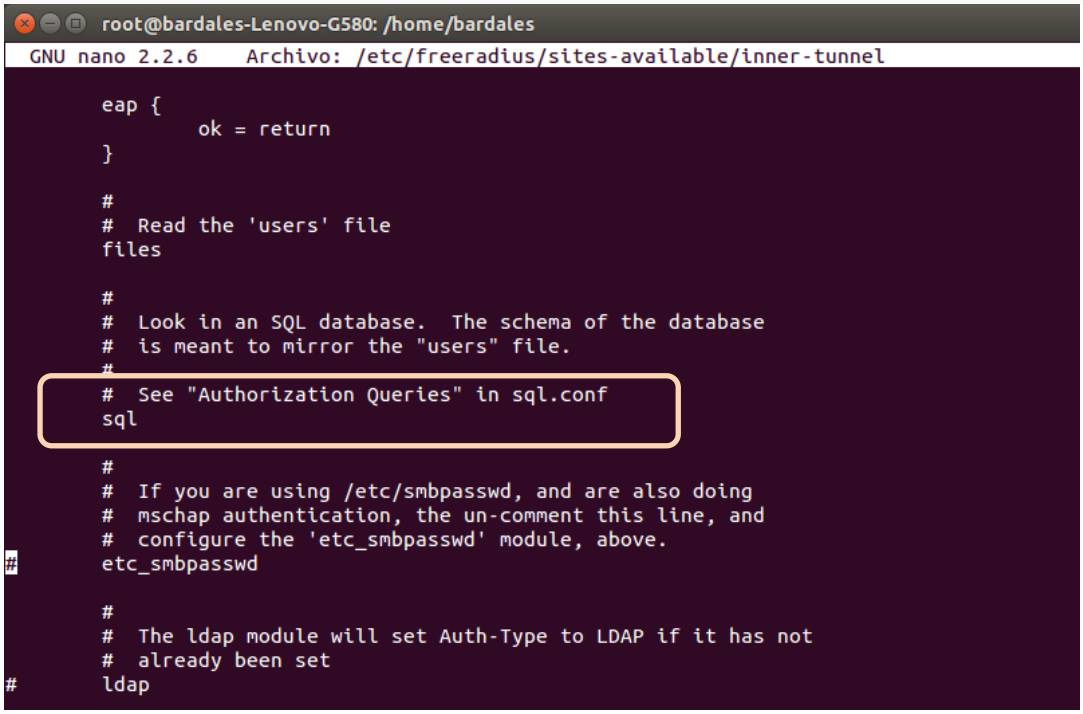
```
root@bardales-Lenovo-G580:/home/bardales# nano /etc/freeradius/sites-available/default
```


root@bardales-Lenovo-G580: /home/bardales
GNU nano 2.2.6 Archivo: /etc/freeradius/sites-available/default
unix
Read the 'users' file
files
Look in an SQL database. The schema of the database
is meant to mirror the "users" file.
See "Authorization Queries" in sql.conf
sql
If you are using /etc/smbpasswd, and are also doing
mschap authentication, the un-comment this line, and
configure the 'etc_smbpasswd' module, above.
etc_smbpasswd
The ldap module will set Auth-Type to LDAP if it has not
already been set
ldap
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Texto ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía


root@bardales-Lenovo-G580: /home/bardales
GNU nano 2.2.6 Archivo: /etc/freeradius/sites-available/default
Return an address to the IP Pool when we see a stop record.
main_pool
Log traffic to an SQL database.
See "Accounting queries" in sql.conf
sql
If you receive stop packets with zero session length,
they will NOT be logged in the database. The SQL module
will print a message (only in debugging mode), and will
return "noop".
You can ignore these packets by uncommenting the following
three lines. Otherwise, the server will not respond to the
accounting request, and the NAS will retransmit.
if (noop) {
ok
}

7. Se procederá de la misma forma con el archivo /etc/freeradius/sites-available/inner-tunnel en la sección authorize{}

```
root@bardales-Lenovo-G580:/home/bardales# nano /etc/freeradius/sites-available/inner-tunnel
```



8. Ahora procederemos a insertar un nuevo usuario en la base de datos. Este usuario nos servirá para poder autenticarnos desde un equipo, por ejemplo con Windows XP/7, contra el servidor freeRadius:

```
root@bardales-Lenovo-G580:/home/bardales# mysql -u root -p radius;
Enter password:
mysql > INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('jacomo', 'Cleartext-Password', '1234');
```

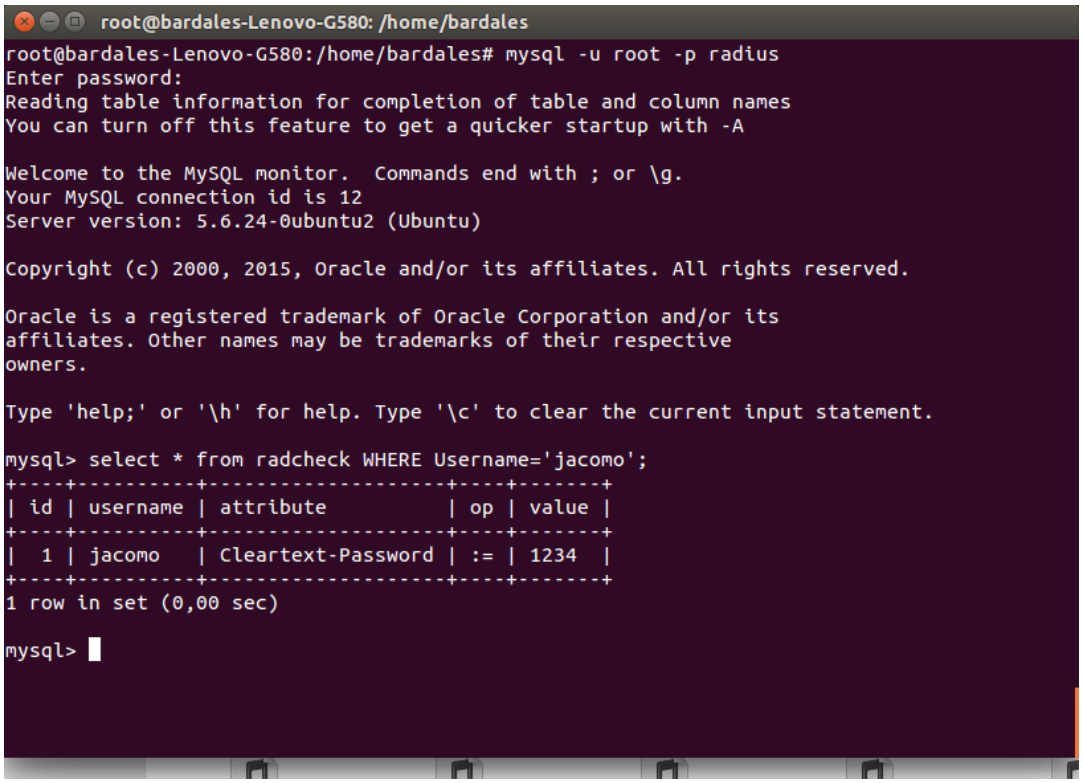
9. Verificamos que el usuario se ha creado correctamente con la siguiente sentencia SQL. En este caso debe aparecer el usuario que hemos creado en la tabla radcheck.

```
mysql > SELECT * from radcheck WHERE UserName='jacomo';
```

10. Con el fin de evitar problemas en la autenticación de radius actualizaremos el campo op del usuario recién creado al valor ':='. Para ello ejecutamos en MySQL la sentencia:

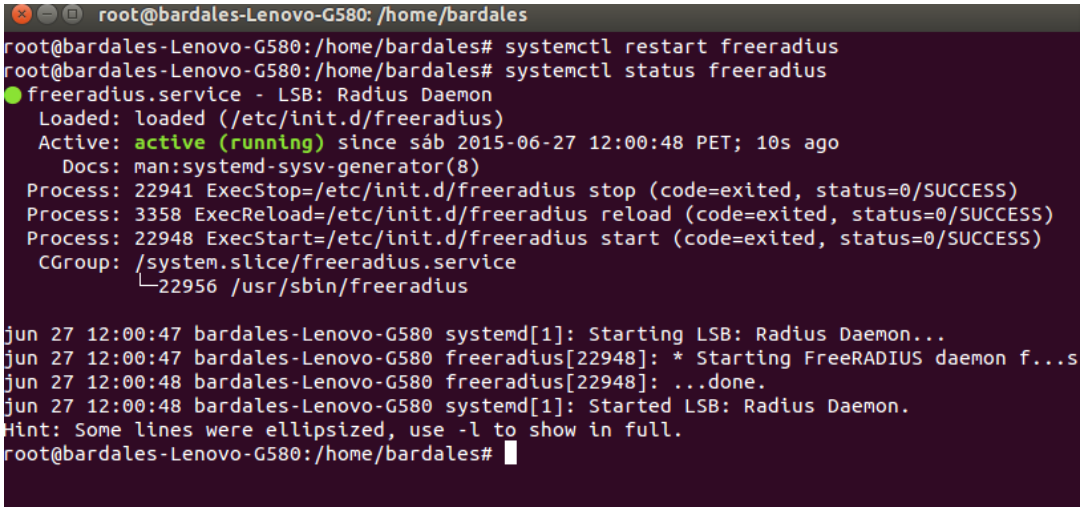
```
mysql > UPDATE radcheck SET op =':=' WHERE username = 'jacomo';
```

El resultado es el que nos muestra la siguiente imagen:



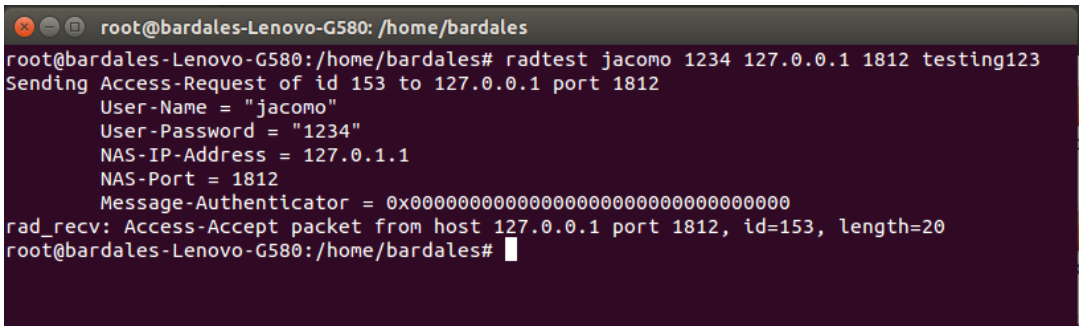
11. Para probar que todo está ok, y que podemos autenticarnos con el usuario recién creado, reiniciamos freeRadius y usamos nuevamente la utilidad radtest.

```
root@bardales-Lenovo-G580:/home/bardales# systemctl restart freeradius;
root@bardales-Lenovo-G580:/home/bardales# systemctl status freeradius;
```



Verificamos usuario creado:

```
root@bardales-Lenovo-G580:/home/bardales# radtest  jacomo  1234  127.0.0.1  1812
testing123
```



C. INSTALACIÓN DE DALORADIUS

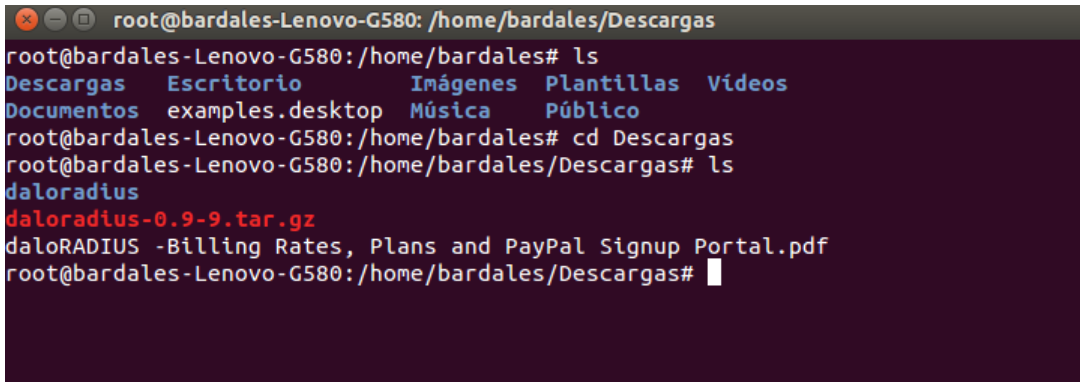
DALORADIUS, es una aplicación avanzada de gestión de RADIUS web destinadas a la gestión de puntos de acceso y las implementaciones de proveedor de internet para fines generales. Es una interfaz web que permite configurar y administrar mi servidor freeRadius.

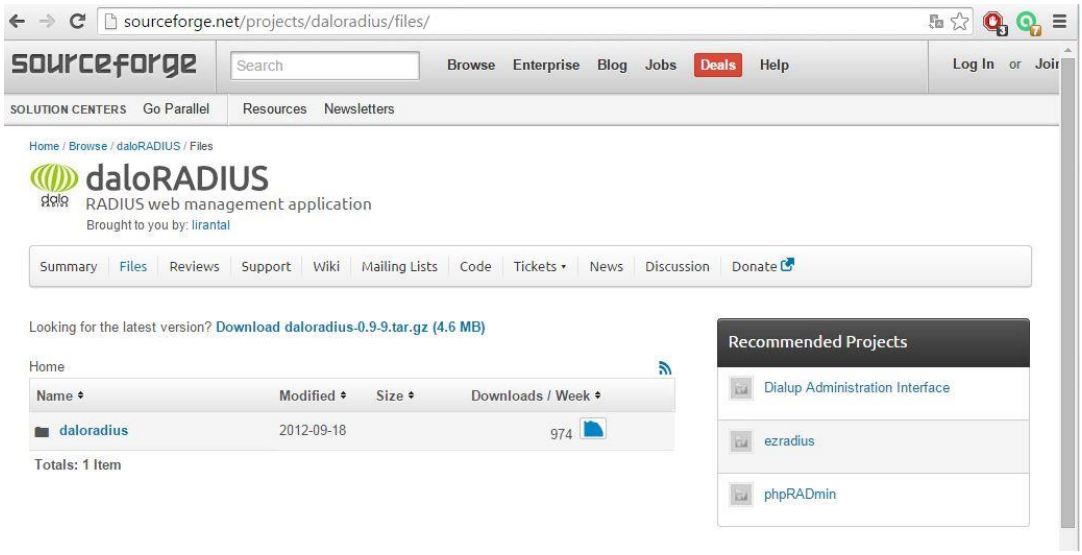
1.- Descargamos la versión más reciente de este paquete, podemos bajarlo desde:

http://sourceforge.net/projects/daloradius/files/

Si damos el camando "ls" podremos ver el archivo daloradius-0.9-8.tar.gz el cual será necesario descomprimir con el siguiente comando:

```
root@bardales-Lenovo-G580:/home/bardales# tar - zxvf daloradius-0.9-9.tar.gz
```





2.- Copiamos este archivo bajo el directorio de publicación del servidor web.

Como en nuestro caso estamos trabajando con una distribución de Ubuntu (15.04), el directorio de publicación por defecto es: /var/www/html/. Entonces hacemos lo siguiente:

```
root@bardales-Lenovo-G580:/home/bardales/Descargas# cp  daloradius
/var/www/html/ -R
```

3.-Luego instalamos algunas librerías que son necesarias para el buen funcionamiento de la aplicación:

```
root@bardales-Lenovo-G580:/home/bardales# apt-get install php5 php5-mysql php-pear
php5-gd php-DB
```

4.- Ahora cambiamos los permisos y propiedades del directorio de daloradius.

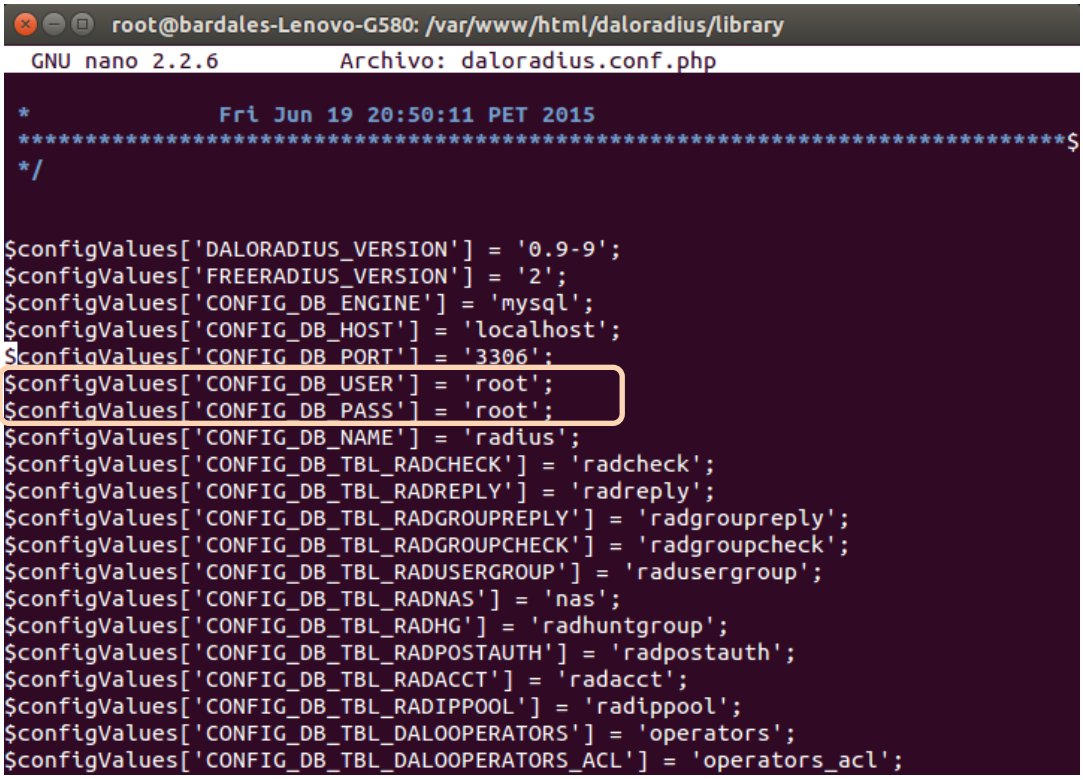
```
root@bardales-Lenovo-G580:/home/bardales# chown www-data:www-
data /var/www/html/daloradius/ -R
```

5.-Cambiamos los permisos del archivo:

```
root@bardales-Lenovo-G580:/home/bardales# chmod 644
/var/www/html/daloradius/library/daloradius.conf.php
```

6.-Ingresamos al directorio cd /var/www/html/daloradius/library y listado todos los archivos y editamos con nano el archivo daloradius.conf.php ; aquí se almacena toda la información acerca de las tablas y acerca del usuario de la base de datos.

Modificamos el usuario y contraseña ingresado anteriormente.



Para que Daloradius funcione correctamente, se requiere agregar algunas tablas más a la base de datos de MySQL.

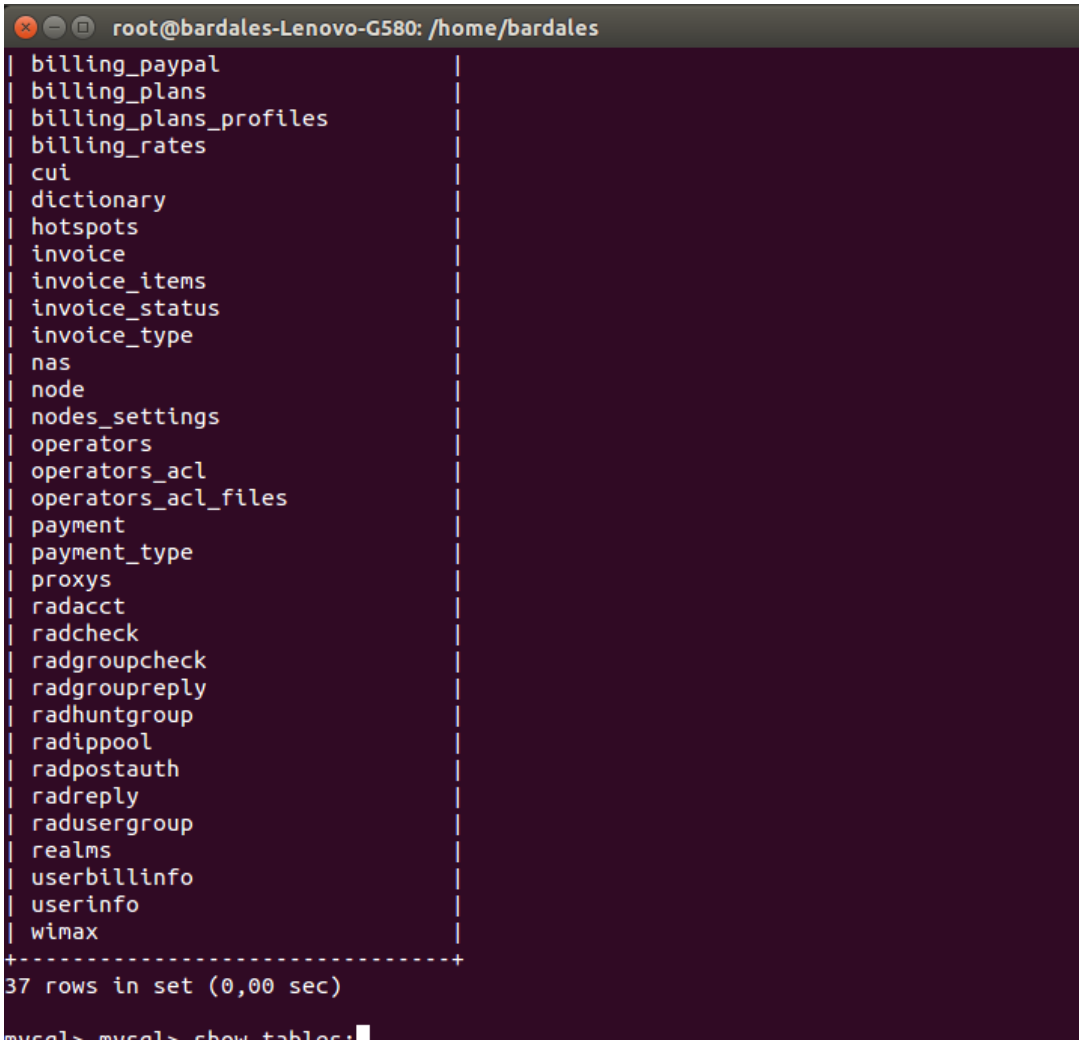
Estas tablas ya están incluidas en el directorio de DaloRadius, por lo que solo es necesario ejecutar el siguiente comando:

```
root@bardales-Lenovo-G580:/var/www/html/daloradius/contrib/db#mysql -u root -p < mysql-daloradius.sql
```

Verificamos las tablas ingresadas:

```
root@bardales-Lenovo-G580:/home/bardales# mysql –u root –p radius
Enter password:
mysql> show tables;
```

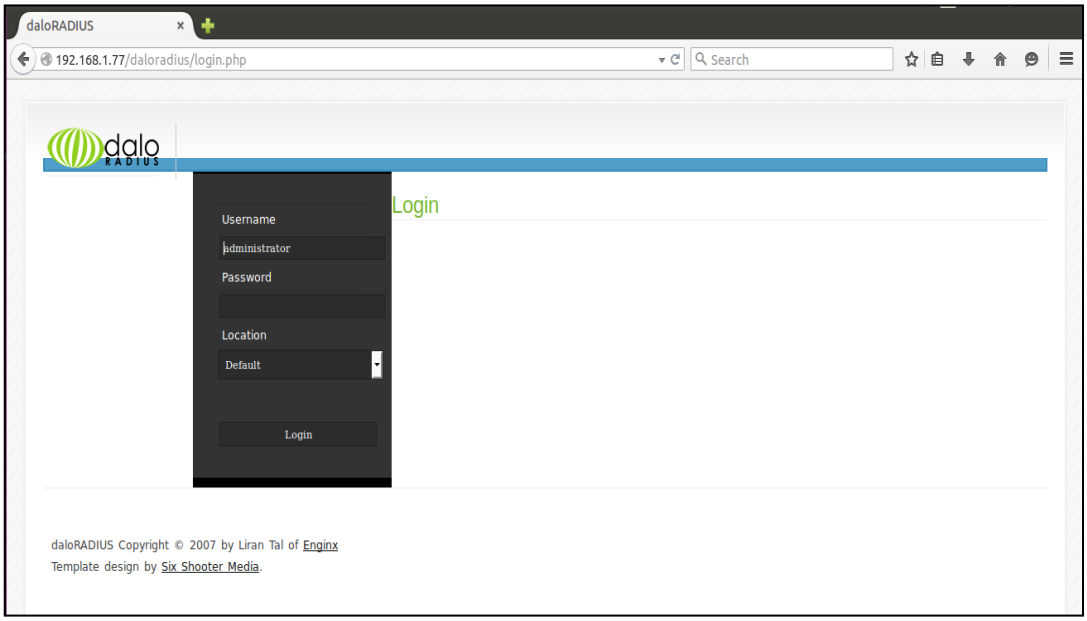
Nos aparece un listado como este:



8.- Ahora nos dirigimos al explorador y colocamos en la barra de direcciones

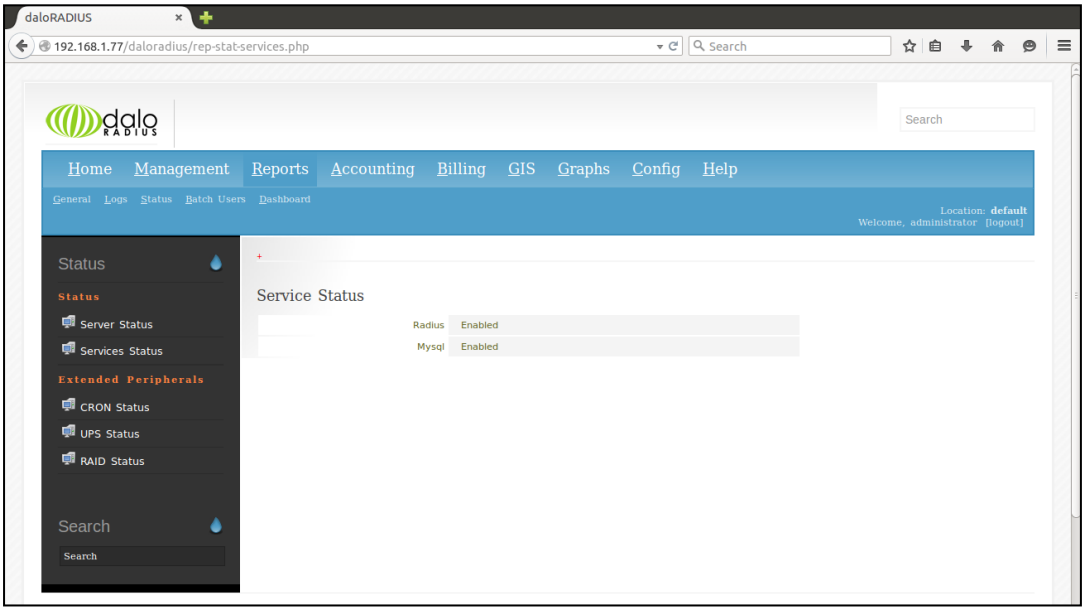
Ingresamos nuestro ip del servidor radius en este caso es 192.168.1.77

http://192.168.1.77/daloradius



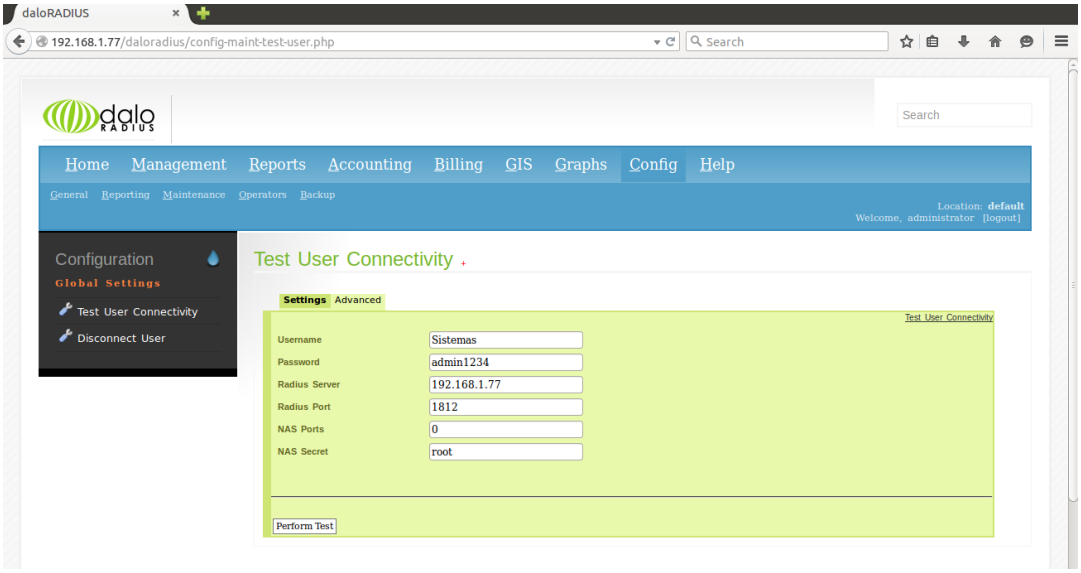
9.-Por defecto el usuario es administrador e ingresamos la contraseña que es **radius**

Verificamos el estado de los servicios.

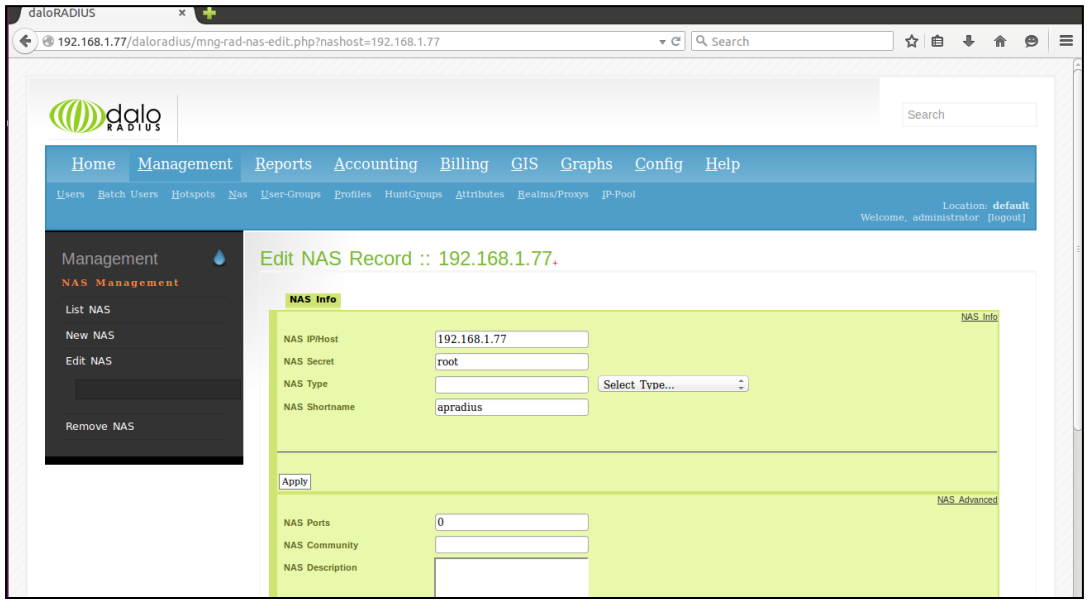


10.- Creamos un usuario para poder testear si funciona correctamente.

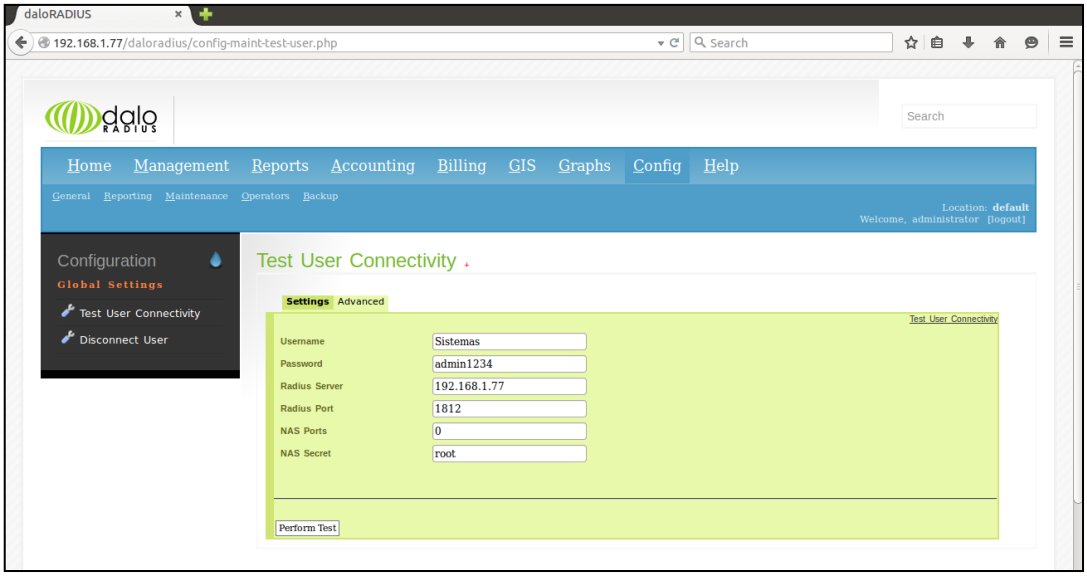
El usuario que crearemos será: Sistemas



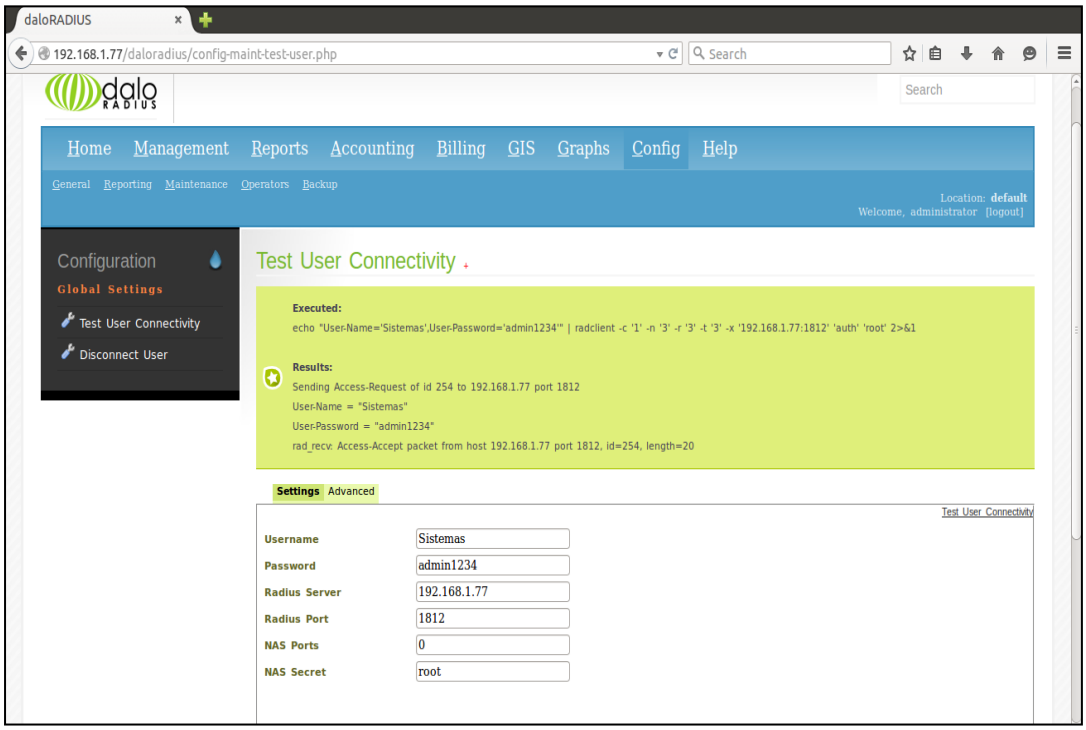
11.- Ingresamos nuestro ip de servidor radius, password y el nombre de nuestro apradius en la pestaña NAS (Networt Access Server)



12.- Verificamos el usuario creado en la pestaña de Config, en Test User Connectivity.



13.- Usuario está conectado satisfactoriamente



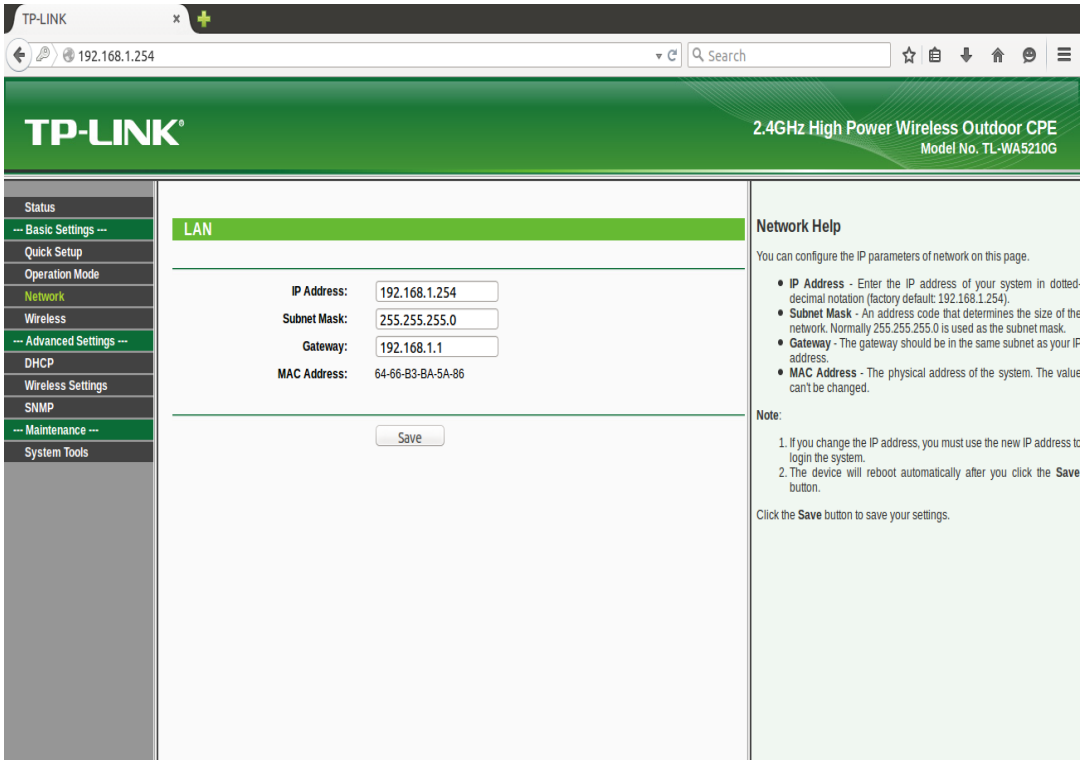
D. CONFIGURACIÓN DE ACCESS POINT

Configuraremos el punto de acceso a través de la administración web del mismo. Para ello tendremos en cuenta los siguientes parámetros: IP privada, SSID de la WiFi y por último la configuración de la seguridad para que apunte al servidor freeRadius.

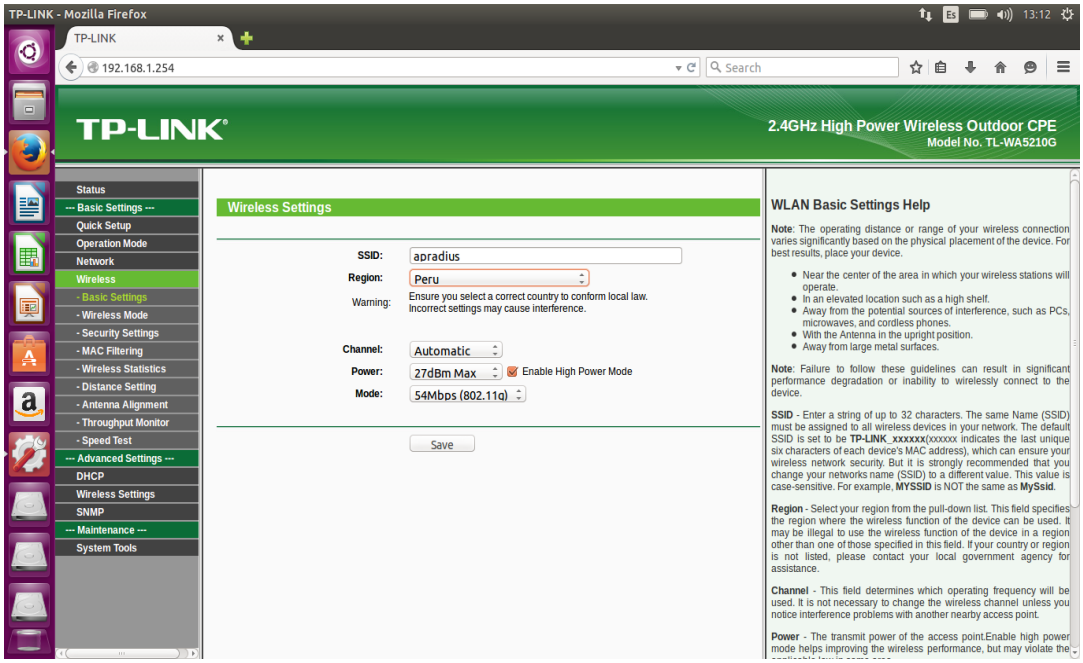
NOTA: Usaremos un navegador de Internet, pondremos la IP 192.168.1.254 y las credenciales por defecto admin/admin.

Empezaremos configurando la IP del punto de acceso en el apartado Network. En nuestro caso hemos elegido la 192.168.1.254, que está en el rango de direcciones de la red clase C de nuestro router ADSL y que además fue añadida con anterioridad a la tabla SQL nas.

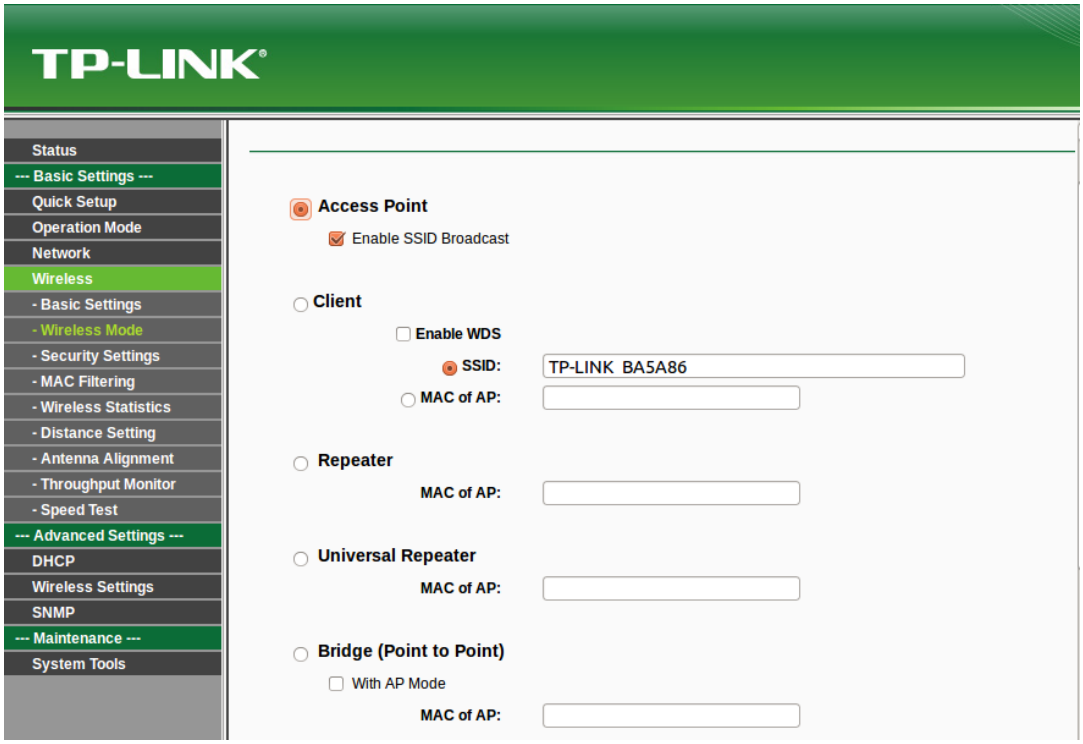
La puerta de enlace (Gateway) será la IP privada del Router ADSL, en nuestro caso la IP 192.168.1.1. Así, el punto de acceso podrá tener salida a Internet. Para acabar, pulsaremos el botón Save para reiniciar. Todos los datos comentados los podemos ver en la siguiente imagen.



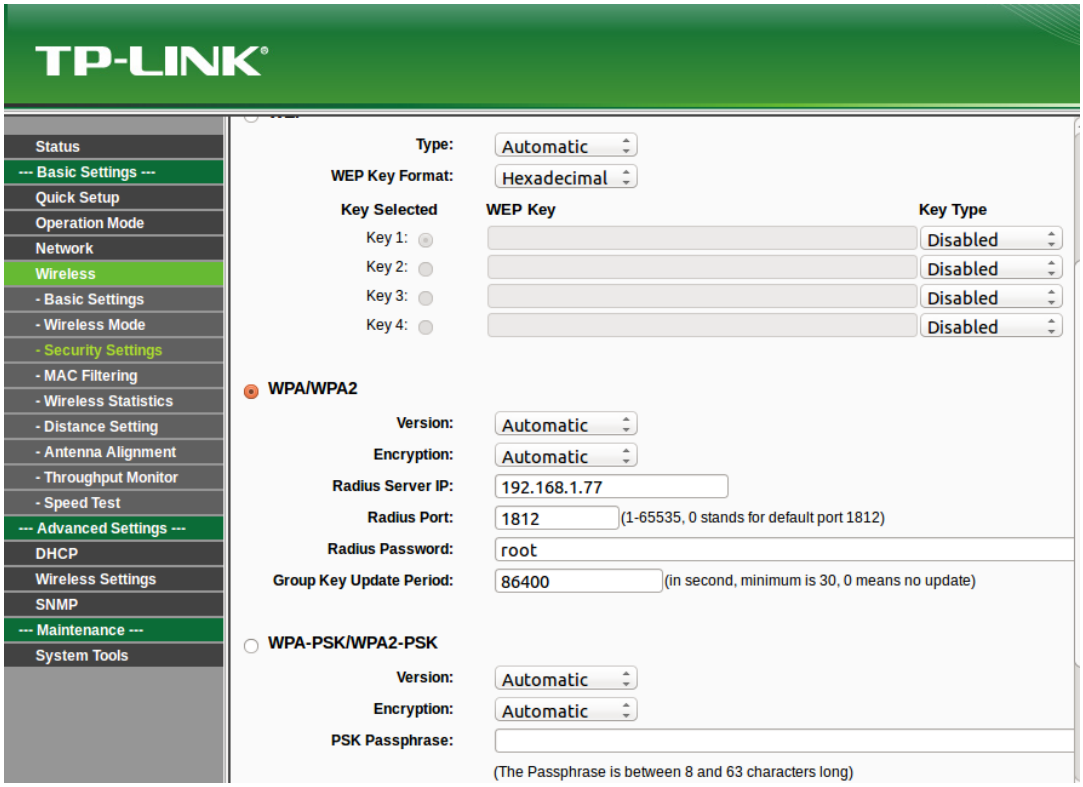
Ahora, en el apartado Wireless Settings, nos tocará configurar el nombre del SSID de la red, que en nuestro caso será apradius. Una vez hecho esto, pulsamos sobre el botón Save y reiniciamos nuevamente el punto de acceso.



Ahora, en el apartado Wireless Settings, nos tocará configurar el modo de operación, que nosotros dejaremos por defecto (Access Point).



Lo último, y más importante, que nos queda de configurar en el punto de acceso es la seguridad WPA/WPA2 del mismo para que valide contra el servidor freeRadius. En este caso, en el apartado Wireless Security, sólo tenemos que configurar la IP 192.168.1.77 de nuestro servidor Radius y la clave del usuario radius de MySQL, que si recordamos era root. Pulsamos sobre el botón Save y reiniciamos el punto de acceso.

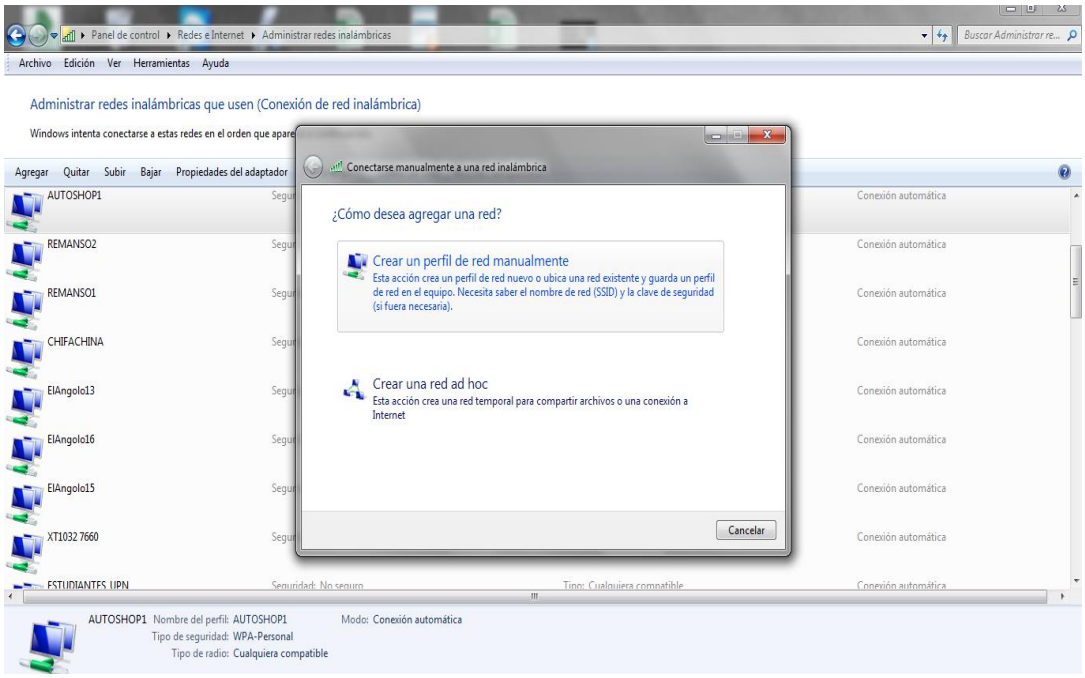


E. CONFIGURACIÓN DE LOS CLIENTES WINDOWS 7 , PARA AUTENTICAR EN FREERADIUS

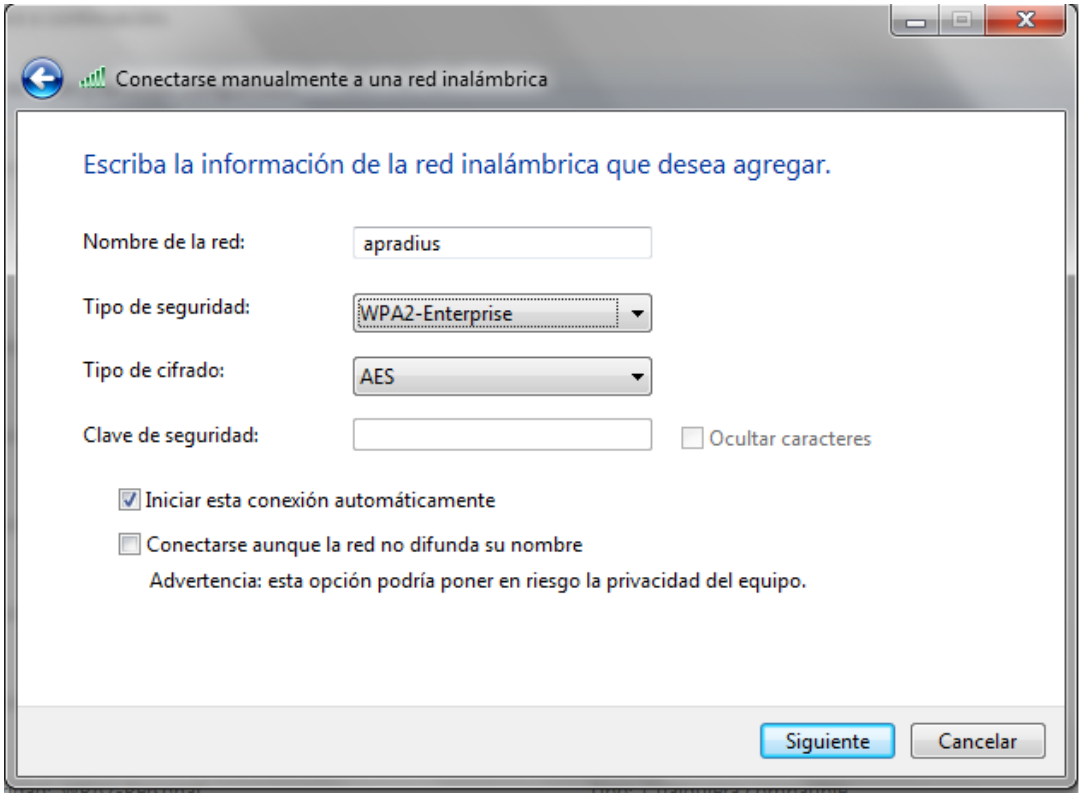
La configuración del cliente radius será la siguiente:

1. Lo primero que haremos es acceder al **Panel de control | Redes e Internet | Administrar redes inalámbricas** y pulsamos sobre el botón Agregar, tal y como se muestra en la siguiente imagen.

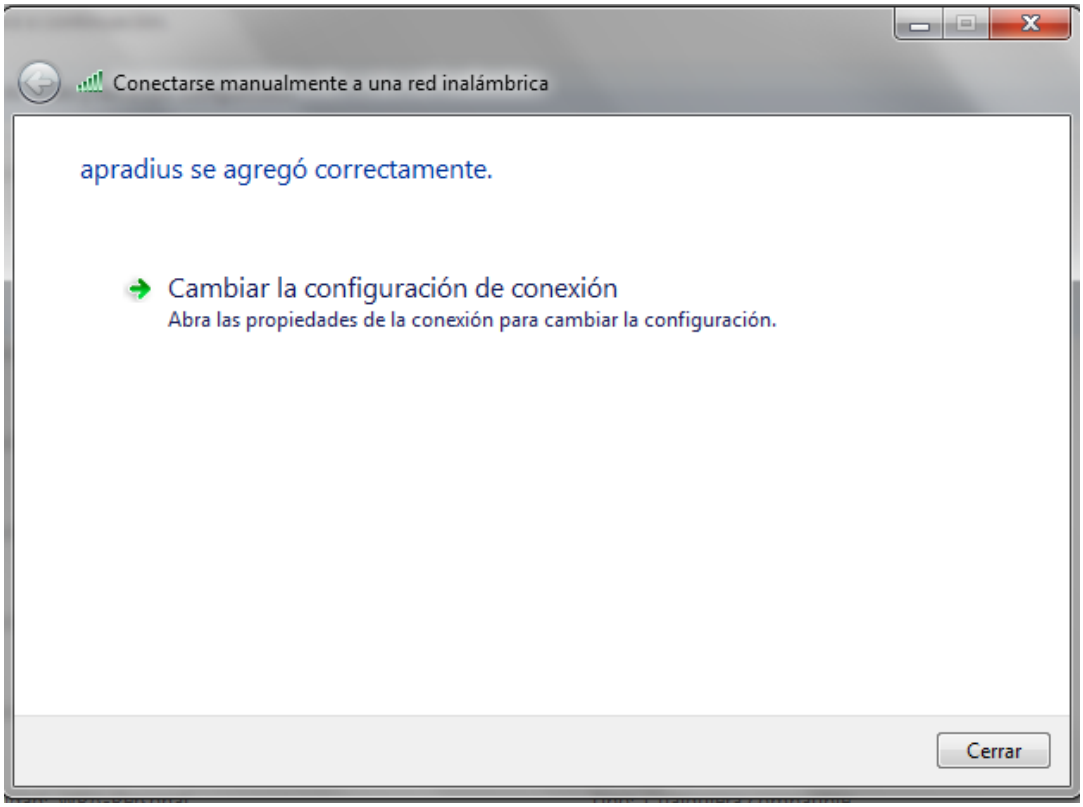
En la ventana que se abre, crearemos un nuevo perfil de red de forma manual. Para ello, pulsaremos en el área señalada de la siguiente imagen:



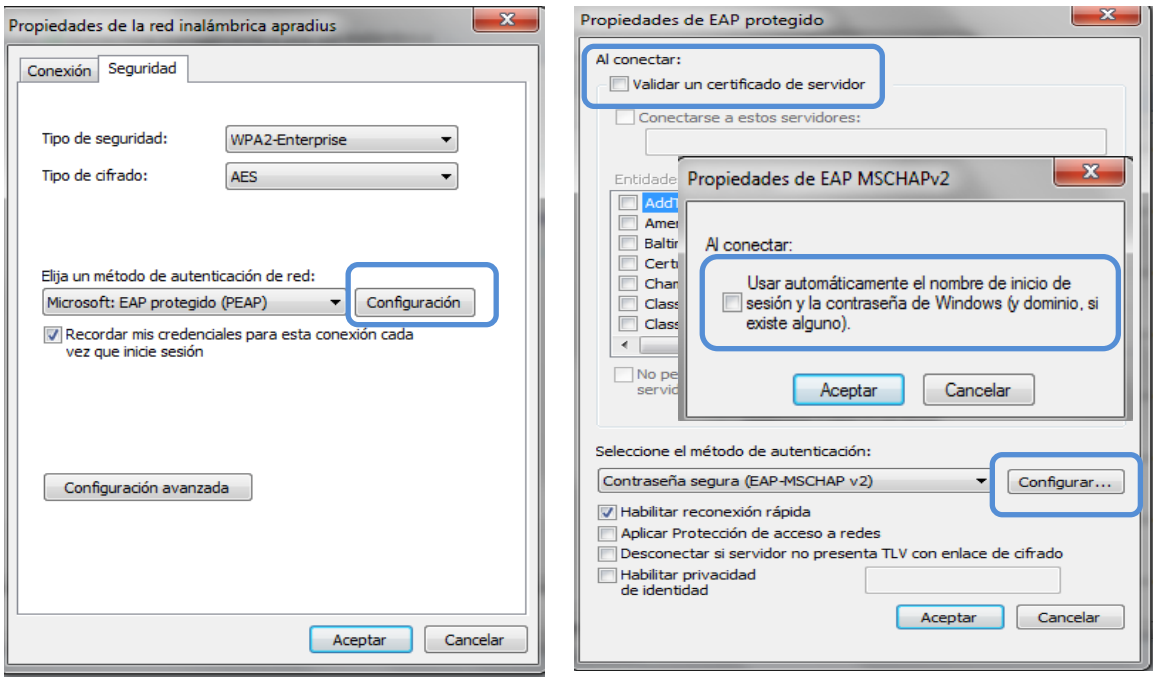
2. Ahora, introduciremos el Nombre de la red inalámbrica (SSID del punto de acceso), en nuestro caso apradius y en el Tipo de seguridad seleccionaremos WPA2-Entreprise. Por último, en el Tipo de cifrado elegiremos el valor AES. El resto de opciones de la ventana las dejaremos como están.



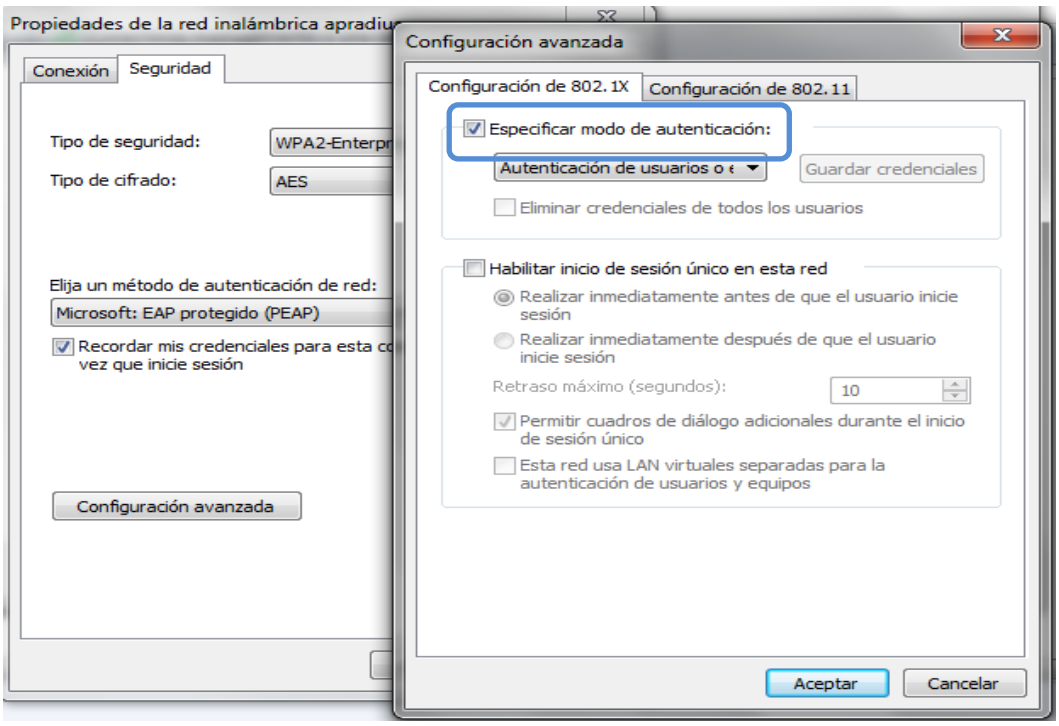
3. El siguiente paso, consiste en Cambiar la configuración de conexión, para ello sólo tenemos que pulsar el correspondiente enlace, señalado en rojo en la siguiente ventana.



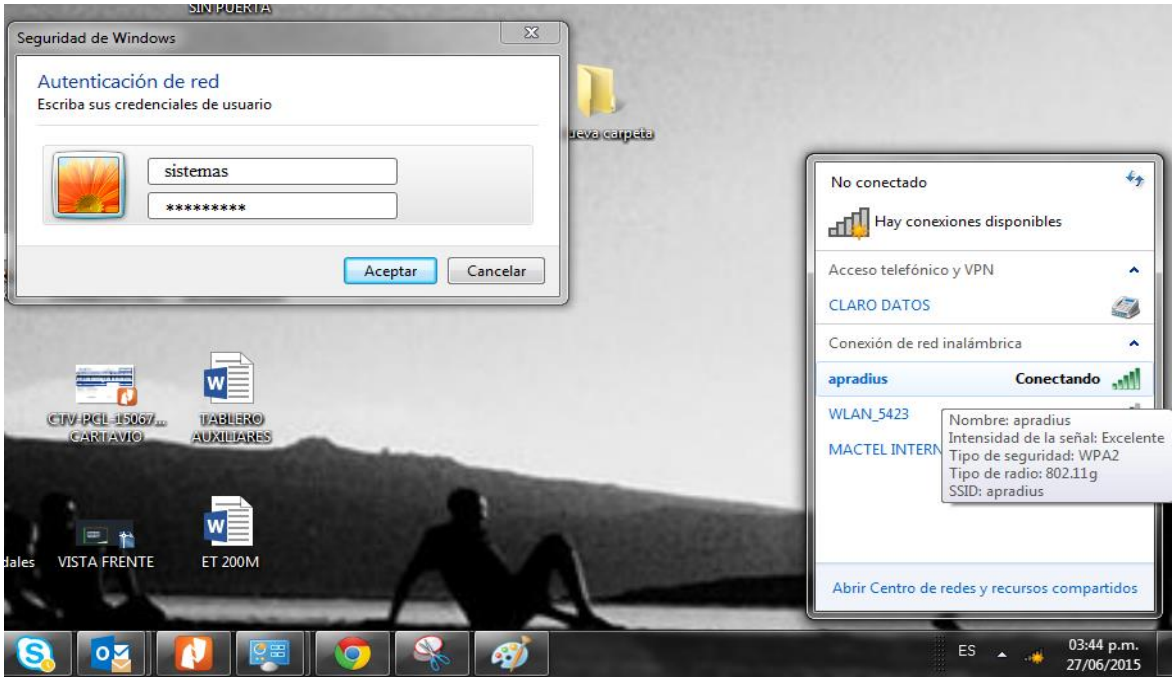
4. En la pestaña Seguridad de la ventana que se nos abre, es pulsar en el botón Configuración. Después desmarcamos la casilla Validad un certificado de servidor, pulsamos configurar y desmarcamos la opción de utilizar el usuario de Windows para validarnos. Aceptamos y Aceptamos, para volver a la ventana inicial.



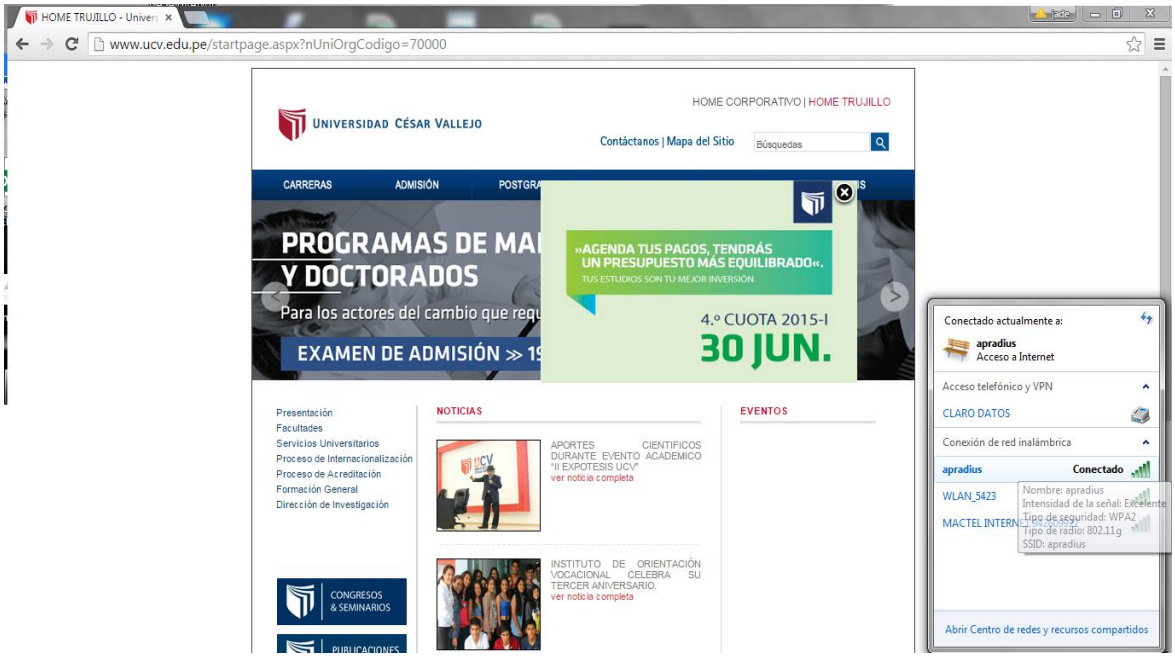
4. En la pestaña Seguridad de la ventana que se nos abre, es pulsar en el botón Configuración Avanzada. Después marcamos la casilla Especificar modo de autenticación para que se conecte de forma automática a la red.



5. Ahora nos conectamos a la red WiFi con el usuario creado sistemas.



6. Verificamos la conexión apradius si está correctamente establecida.



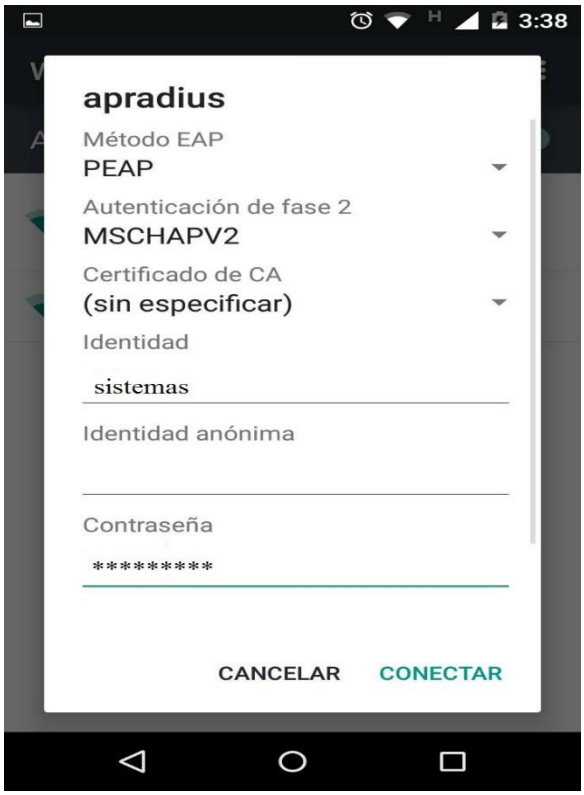
F. CONFIGURACIÓN DE LOS CLIENTES ANDROID, PARA AUTENTICAR EN FREERADIUS.

1. Ingresamos a Settings

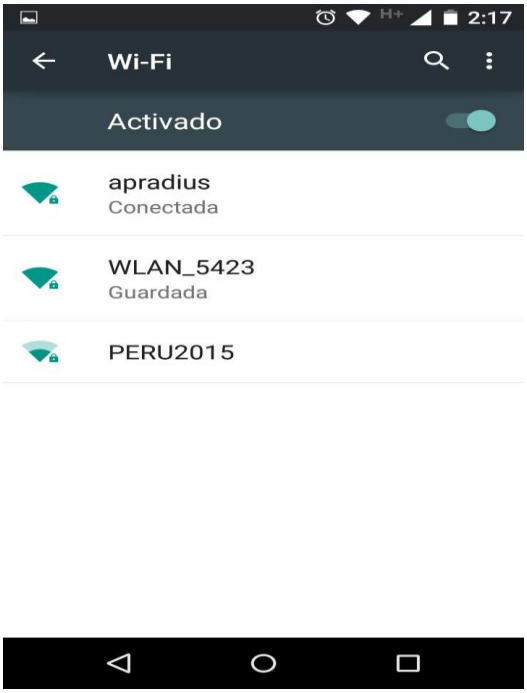
2.- Buscamos en Wi-Fi, nuestro servidor radius, apradius

2.- Buscamos en Wi-Fi , nuestro servidor radius, apradius

- ✓ Elegimos **PEAP** en el Método EAP
- ✓ Elegimos **MSCHAPV2 en Autenticación de fase 2**.
- ✓ Ingresamos el usuario en este caso sistemas en identidad.
- ✓ Ingresamos la contraseña correspondiente del usuario en contraseña.
- ✓ En certificado de CA e identidad anónimas no ingresamos datos.
- ✓ Presionar conectar .



3.- Verificamos la conexión establecida

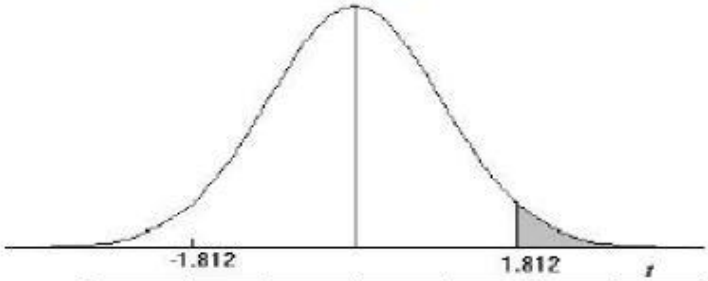


4.- Ingresamos a una página web para verificar conexión

ANEXO 6

TABLA 2: DISTRIBUCIÓN t DE STUDENT

Puntos de porcentaje de la distribución t



Ejemplo

Para ϕ = 10 grados de libertad:

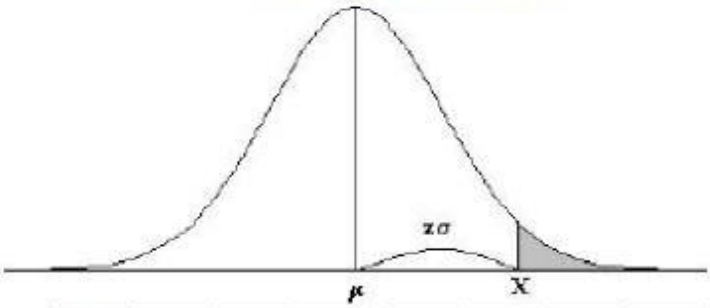
$P[t > 1.812] = 0.05$
$P[t < -1.812] = 0.05$

α / r	0,25	0,2	0,15	0,1	0,05	0,025	0,01	0,005	0,0005
1	1,000	1,376	1,963	3,078	6,314	12,706	31,821	63,656	636,578
2	0,816	1,061	1,386	1,886	2,920	4,303	6,965	9,925	31,600
3	0,765	0,978	1,250	1,638	2,353	3,182	4,541	5,841	12,924
4	0,741	0,941	1,190	1,533	2,132	2,776	3,747	4,604	8,610
5	0,727	0,920	1,156	1,476	2,015	2,571	3,365	4,032	6,869
6	0,718	0,906	1,134	1,440	1,943	2,447	3,143	3,707	5,959
7	0,711	0,896	1,119	1,415	1,895	2,365	2,998	3,499	5,408
8	0,706	0,889	1,108	1,397	1,860	2,306	2,896	3,355	5,041
9	0,703	0,883	1,100	1,383	1,833	2,262	2,821	3,250	4,781
10	0,700	0,879	1,093	1,372	1,812	2,228	2,764	3,169	4,587
11	0,697	0,876	1,088	1,363	1,796	2,201	2,718	3,106	4,437
12	0,695	0,873	1,083	1,356	1,782	2,179	2,681	3,055	4,318
13	0,694	0,870	1,079	1,350	1,771	2,160	2,650	3,012	4,221
14	0,692	0,868	1,076	1,345	1,761	2,145	2,624	2,977	4,140
15	0,691	0,866	1,074	1,341	1,753	2,131	2,602	2,947	4,073
16	0,690	0,865	1,071	1,337	1,746	2,120	2,583	2,921	4,015
17	0,689	0,863	1,069	1,333	1,740	2,110	2,567	2,898	3,965
18	0,688	0,862	1,067	1,330	1,734	2,101	2,552	2,878	3,922
19	0,688	0,861	1,066	1,328	1,729	2,093	2,539	2,861	3,883
20	0,687	0,860	1,064	1,325	1,725	2,086	2,528	2,845	3,850
21	0,686	0,859	1,063	1,323	1,721	2,080	2,518	2,831	3,819
22	0,686	0,858	1,061	1,321	1,717	2,074	2,508	2,819	3,792
23	0,685	0,858	1,060	1,319	1,714	2,069	2,500	2,807	3,768
24	0,685	0,857	1,059	1,318	1,711	2,064	2,492	2,797	3,745
25	0,684	0,856	1,058	1,316	1,708	2,060	2,485	2,787	3,725
26	0,684	0,856	1,058	1,315	1,706	2,056	2,479	2,779	3,707
27	0,684	0,855	1,057	1,314	1,703	2,052	2,473	2,771	3,689
28	0,683	0,855	1,056	1,313	1,701	2,048	2,467	2,763	3,674
29	0,683	0,854	1,055	1,311	1,699	2,045	2,462	2,756	3,660
30	0,683	0,854	1,055	1,310	1,697	2,042	2,457	2,750	3,646
40	0,681	0,851	1,050	1,303	1,684	2,021	2,423	2,704	3,551
60	0,679	0,848	1,045	1,296	1,671	2,000	2,390	2,660	3,460
120	0,677	0,845	1,041	1,289	1,658	1,980	2,358	2,617	3,373
∞	0,674	0,842	1,036	1,282	1,645	1,960	2,326	2,576	3,290

ANEXO 7

TABLA 1: DISTRIBUCIÓN NORMAL

Áreas bajo la curva normal



Ejemplo:

$$Z = \frac{X - \mu}{\sigma}$$

P [Z > 1] = 0.1587
P [Z > 1.96] = 0.0250

Desv. normal x	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.5000	0.4960	0.4920	0.4880	0.4840	0.4801	0.4761	0.4721	0.4681	0.4641
0.1	0.4602	0.4562	0.4522	0.4483	0.4443	0.4404	0.4364	0.4325	0.4286	0.4247
0.2	0.4207	0.4168	0.4129	0.4090	0.4052	0.4013	0.3974	0.3936	0.3897	0.3859
0.3	0.3821	0.3783	0.3745	0.3707	0.3669	0.3632	0.3594	0.3557	0.3520	0.3483
0.4	0.3446	0.3409	0.3372	0.3336	0.3300	0.3264	0.3228	0.3192	0.3156	0.3121
0.5	0.3085	0.3050	0.3015	0.2981	0.2946	0.2912	0.2877	0.2843	0.2810	0.2776
0.6	0.2743	0.2709	0.2676	0.2643	0.2611	0.2578	0.2546	0.2514	0.2483	0.2451
0.7	0.2420	0.2389	0.2358	0.2327	0.2296	0.2266	0.2236	0.2206	0.2177	0.2148
0.8	0.2119	0.2090	0.2061	0.2033	0.2005	0.1977	0.1949	0.1922	0.1894	0.1867
0.9	0.1841	0.1814	0.1788	0.1762	0.1736	0.1711	0.1685	0.1660	0.1635	0.1611
1.0	0.1587	0.1562	0.1539	0.1515	0.1492	0.1469	0.1446	0.1423	0.1401	0.1379
1.1	0.1357	0.1335	0.1314	0.1292	0.1271	0.1251	0.1230	0.1210	0.1190	0.1170
1.2	0.1151	0.1131	0.1112	0.1093	0.1075	0.1056	0.1038	0.1020	0.1003	0.0985
1.3	0.0968	0.0951	0.0934	0.0918	0.0901	0.0885	0.0869	0.0853	0.0838	0.0823
1.4	0.0808	0.0793	0.0778	0.0764	0.0749	0.0735	0.0721	0.0708	0.0694	0.0681
1.5	0.0668	0.0655	0.0643	0.0630	0.0618	0.0606	0.0594	0.0582	0.0571	0.0559
1.6	0.0548	0.0537	0.0526	0.0516	0.0505	0.0495	0.0485	0.0475	0.0465	0.0455
1.7	0.0446	0.0436	0.0427	0.0418	0.0409	0.0401	0.0392	0.0384	0.0375	0.0367
1.8	0.0359	0.0351	0.0344	0.0336	0.0329	0.0322	0.0314	0.0307	0.0301	0.0294
1.9	0.0287	0.0281	0.0274	0.0268	0.0262	0.0256	0.0250	0.0244	0.0239	0.0233
2.0	0.0228	0.0222	0.0217	0.0212	0.0207	0.0202	0.0197	0.0192	0.0188	0.0183
2.1	0.0179	0.0174	0.0170	0.0166	0.0162	0.0158	0.0154	0.0150	0.0146	0.0143
2.2	0.0139	0.0136	0.0132	0.0129	0.0125	0.0122	0.0119	0.0116	0.0113	0.0110
2.3	0.0107	0.0104	0.0102	0.0099	0.0096	0.0094	0.0091	0.0089	0.0087	0.0084
2.4	0.0082	0.0080	0.0078	0.0075	0.0073	0.0071	0.0069	0.0068	0.0066	0.0064
2.5	0.0062	0.0060	0.0059	0.0057	0.0055	0.0054	0.0052	0.0051	0.0049	0.0048
2.6	0.0047	0.0045	0.0044	0.0043	0.0041	0.0040	0.0039	0.0038	0.0037	0.0036
2.7	0.0035	0.0034	0.0033	0.0032	0.0031	0.0030	0.0029	0.0028	0.0027	0.0026
2.8	0.0026	0.0025	0.0024	0.0023	0.0023	0.0022	0.0021	0.0021	0.0020	0.0019
2.9	0.0019	0.0018	0.0018	0.0017	0.0016	0.0016	0.0015	0.0015	0.0014	0.0014
3.0	0.0013	0.0013	0.0013	0.0012	0.0012	0.0011	0.0011	0.0011	0.0010	0.0010

ANEXO 8


POWER