UNIVERSIDAD DE HUÁNUCO

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

"IMPLEMENTACIÓN DE LA NORMA IEEE 802.1X PARA LA MEJORA EN LA SEGURIDAD DE LA RED WLAN DE LA EMPRESA SEDA HUANUCO S.A 2016."

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR

Bach. Demetrio Lino, FRETEL MALPARTIDA

ASESOR

Ing. Luis Andres, MEZA ORDOÑEZ

HUÁNUCO- PERÚ

2018

UNIVERSIDAD DE HUANUCO
Facultad de Ingeniería

E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMATICA

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO(A) DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 17:00 horas del día 11 del mes de Diciembre del año 2018, en el Auditorio de la Facultad de Ingeniería, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron los Jurados Calificadores Nombrados mediante la Resolución N° 1171-2018-D-FI-UDH integrado por los docentes:

Mg. Omar Iván Sulca C. (Presidente)
Mg. Héctor R Zacarías V. (Secretario)
Ing. José A. Nuñez Vicente (Vocal)

Para calificar el Trabajo de Suficiencia Profesional solicitado por el (la) Bachiller Demetrio Lino Fretel Malpartida para optar el Título Profesional de Ingeniero(a) de Sistemas e Informática.

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas: precediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo (a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de 15 y cualitativo de BUENO

Siendo las 18:20 horas del día 11 del mes de Diciembre del año 2018, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Presidente

Secretario

Vocal

DEDICATORIA

A Dios por permitirme tener una familia que siempre creyó en mí y por ser la motivación para cada día llegar más lejos en mi vida personal y carrera profesional.

AGRADECIMIENTOS

A la Universidad de Huánuco por formarme como Profesional, a todos los docentes y administrativos que fueron participes de este proceso de formación.

A la Directora de la Escuela de Ingeniería de Sistemas e Informática Ing. Bertha Campos Ríos por el constante incentivo de lograr mis objetivos.

Y finalmente a los que invirtieron su tiempo para revisar el proyecto de Tesina, infinitas gracias a todos ellos.

INDICE

RESUMEN

El objetivo fundamental del presente estudio fue el de investigar y comprobar la mejora ante la implementación y uso del estándar 802.1x en la seguridad de la red inalámbrica de la empresa SEDA Huánuco. La metodología que se empleó en la investigación corresponde a un enfoque cuantitativo, el tipo de investigación es experimental, de nivel aplicativo y el diseño de investigación es cuasi experimental de pre y post evaluación con un solo grupo. El tamaño de la muestra está compuesto por 05 trabajadores de la OMS de la empresa SEDA Huánuco, se obtuvo la muestra de forma no aleatoria, e intencional, escogiendo a los 05 trabajadores que conforman la oficina de Organización, métodos y sistemas. Para la recolección de los datos se utilizó como técnica la encuesta y su instrumento el cuestionario. Los resultados fueron procesados mediante el paquete estadístico SPSS. Se concluye a nivel global, una influencia muy favorable del uso e implementación del estándar 802.1x en la mejora de la de la seguridad de la red inalámbrica de la institución, se evidencia que la mejora radica en cuanto a los controles de acceso empleados al momento de la autenticación en la red.

Por consiguiente, después de haber comprobado de forma positiva la hipótesis de la investigación, se concluye la importancia de la investigación ya que es de carácter práctico y aplicativo dando solución al problema de la inseguridad de la red inalámbrica de la empresa SEDA Huánuco S.A.

Palabras clave: 802.1x, Radius, Servidor de autenticación, AAA.

ABSTRACT

The main objective of this study was to investigate and verify the improvement in the implementation and use of the 802.1x standard in the security of the wireless network of the company SEDA Huánuco. The methodology used in the research corresponds to a quantitative approach, the type of research is experimental, application level and the research design is quasi experimental and the design is pre and post evaluation with a single group. The sample size is composed of 05 WHO workers from the company SEDA Huánuco, the sample was obtained in a non-random and intentional way, choosing the 05 workers that make up the Organization's office, methods and systems. The survey questionnaire was used to collect the data. The results were processed using the SPSS statistical package. It is concluded at the global level, a very favorable influence of the use and implementation of the 802.1x standard in the improvement of the security of the wireless network of the institution, it is evident that the improvement lies in the access controls used at the moment Of the authentication in the network.

Therefore, after having tested positively the research hypothesis, the importance of the investigation is concluded since it is of a practical and practical nature, giving solution to the problem of the insecurity of the wireless network of the company SEDA Huánuco S.A.

Keywords: 802.1x, Radius, Authentication Server, AAA.

INTRODUCCIÓN

La presente investigación se refiere al tema de las redes inalámbricas de área local (WLAN), que van ganando un espacio primordial y crucial en las comunicaciones del mundo actual, ya que, por su facilidad de instalación y conexión, se han convertido en una buena alternativa para realizar conectividad en lugares donde resulta imposible brindar servicio con una red cableada. La popularidad de estas redes ha crecido a tal punto que los diferentes dispositivos ya vienen con un receptor y emisor inalámbrico embebido. Las WLAN son redes de computadoras que su característica principal es de establecer la conexión usado las ondas de radio, mejor dicho, no necesitan de un medio guiado para operar, esto permite que cualquier host conectado a la red pueda tener acceso a los recursos de la red desde cualquier lugar, siempre y cuando este dentro de la cobertura del Access point.

Así como mencionamos implícitamente aquellas ventajas de una WLAN, también podemos mencionar algunas desventajas, y una de las más principales está relacionada en cuanto al factor de la seguridad, sabemos hoy en día que el problema de la seguridad está presente en todos los sistemas de comunicación e información, esto implica que estos sistemas están expuestos a diferentes riesgos, debido a las vulnerabilidades de los mismo, y ante la cantidad de ataques realizados por agentes extraños cuyo objetivo es causar daño y robar información o simplemente acceder a los recursos de la red sin permiso y gratuitamente.

Afortunadamente existen mecanismo estandarizados para asegurar la información y los recursos de una red, por ende el estándar 802.1x asegura el proceso de autenticación de una WLAN, permitiendo que los usuarios solo puedan conectarse a la red si es que poseen las credenciales de ingreso como son una nombre de usuario y una contraseña y todo esto validado por un servidor de autenticación que este caso es RADIUS, de esta forma con este mecanismo de protección se pueden evitar los riesgos y reforzar aquellas vulnerabilidades inherentes de un red inalámbrica.

Con respecto al estudio de investigación se ha visto por conveniente implementar dicho mecanismo de seguridad para la WLAN de la empresa

SEDA Huánuco para evitar accesos no permitidos a la red y también asegurar la información y recursos de dicha red, de esta forma solo podrán ingresar a la WLAN aquellos usuarios a los cuales se le asignó un nombre de usuario y una contraseña, dichas credenciales serán administradas desde un servidor, el cual realizará el proceso de autenticación.

El informe de investigación está divido en 5 capítulos y se resumen a continuación: En el capítulo I se trata sobre la descripción del problema, relacionado a la vulnerabilidad de la red inalámbrica de la empresa, teniendo como problema principal: ¿De qué manera la implementación de la norma IEEE 802.1x mejorará la seguridad de la WLAN de la Empresa SEDA HUÁNUCO S.A.? y ante esta pregunta se plantea el objetivo de Implementar la norma IEEE 802.1x para mejorar la seguridad de la red WLAN de la Empresa. Se da a conocer también por qué y para que, del estudio, y así mismo se fijan las limitaciones la viabilidad del presente estudio. En el capítulo II se da a conocer los trabajos de investigación relacionados, así como también la estructura teórica y se platea la hipótesis: “La implementación de la norma IEEE 802.1x mejora la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.” para poner en prueba la hipótesis. En el capítulo III se establece la metodología, bajo el nivel aplicativo y usando el diseño cuasi-experimental con grupo de pre y post prueba. En el capítulo IV se muestra los resultados procesados en el software SPSS y también se pone a prueba la hipótesis en base al diseño planteado en el capítulo III y finalmente, En el capítulo V se realiza las discusiones de los resultados en base a los resultados obtenidos.

Finalmente, desde el punto de vista económico, la implementación de este mecanismo de seguridad no generara gastos excesivos ya que la implementación de dicho mecanismo es usando software libre, en este caso se usó el sistema operativo Linux, evitando la compra de licencias, es así como podemos hablar de un estudio de investigación que soluciona el problema usando tecnología actual, es sustentable y viable y genera beneficios a la institución.

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del Problema

En estos días la seguridad se ha convertido en un factor determinante en la calidad de servicio y de producto de cualquier empresa y/o organización, se habla de seguridad ciudadana, seguridad ambiental, seguridad en el trabajo, seguridad vial, seguridad, seguridad de la información y entre otros, dentro de estos ámbitos las ciencias de la seguridad se encargan de evaluar, estudiar y analizar los riesgos que se encuentran adheridos a una persona, objetos o situación, para poder así minimizar los riesgos y asegurar la continuidad del negocio de una empresa y organización.

Así mismo, la seguridad de la información, según ISO 27001, se ocupa de la confidencialidad, la integridad y la disponibilidad de la información y los datos sensibles para la organización, independientemente del formato que tengan, estos pueden ser: físicos, electrónicos, etc. Unos de los tipos de seguridad es la seguridad lógica, y desde el punto de vista de capas, hablamos de la seguridad de la capa de red, que es la encargada de proveer aquellos mecanismos de protección para proteger la información que fluye en una red de computadoras, independiente del medio, ya sea físico o no, ya sean redes cableadas o inalámbricas.

La Empresa SEDA HUÁNUCO S.A. es una organización que actúa con autonomía administrativa, financiera y presupuestaria cuyo objeto social es la Prestación de Servicios de Saneamiento, los cuales están comprendidos por los siguientes sistemas: Servicio de Agua Potable y Servicio de Alcantarillado Sanitario y Pluvial. Teniendo bajo su responsabilidad la prestación de los servicios en las localidades de Huánuco, Amarilis, y las localidades de Tingo María y Aucayacu. A su vez la Empresa cuenta con tres áreas indispensables el área administrativa, el área operacional y el área Comercial, esta última tiene entre sus filas la oficina de OMS (Organización Métodos y Sistemas) el cual se encarga de brindar cobertura y seguridad de todos los datos de la población consumidora por medio de consultas y búsquedas de facturaciones, reclamos y contratos de nuevos servicios, generados constantemente por medio de la intranet de la empresa. Actualmente, esta oficina posee una

infraestructura de red y comunicación dividida en tres partes en la matriz localizada de la empresa, a través de la topología estrella con red de fibra óptica.

Ante el uso masivo de la tecnología de la información y comunicación en el ámbito empresarial y desde el punto de vista de la seguridad de la información, las organizaciones son cada vez más susceptibles a riesgos en cuanto al uso de la información; así mismo la empresa Seda Huánuco también está expuesta a una serie de riesgos en cuanto a la confidencialidad y disponibilidad de su red local inalámbrica que desde ahora la denominaremos WLAN, en este caso el riesgo radica en la probabilidad de ataques por parte de los hackers, que puedan intentar descifrar las contraseñas Wi-Fi con el fin de obtener acceso a la red, y así poder hacer uso de la red y acceder a los recursos de aquella. Estos riesgos surgen debido a las siguientes causas: mala implementación de los protocolos de seguridad de la red, el desconocimiento de ellos, y la negligencia por parte de los trabajadores de la OMS, por ende, esto genera diferentes consecuencias como la saturación de la red debido a los diferentes accesos no permitidos, la caída de la misma red por la saturación excesiva de clientes conectados no autorizados al punto de acceso, la filtración de información sensible de las áreas de la empresa, entre otras. Los riesgos mencionados anteriormente fueron comprobados mediante análisis previos y conversaciones con los encargados del área técnica y también previa revisión de algunos documentos y registros de incidencias donde se da a conocer que en la red inalámbrica ha sido accedida sin las autorizaciones correspondientes.

Por lo tanto, el presente trabajo de investigación planteo la solución para garantizar la seguridad de la WLAN de la empresa Seda Huánuco, con la finalidad de lograr un acceso seguro a la red inalámbrica mediante la identificación y autenticación de los clientes en el punto de acceso, y esto se logró mediante la implementación de la norma IEEE 802.1X, también conocido como protocolo o servidor RADIUS.

1.2 Formulación del Problema

1.2.1 Problema Principal

¿De qué manera la implementación de la norma IEEE 802.1x mejorará la seguridad de la WLAN de la Empresa SEDA HUÁNUCO S.A.?

1.2.2 Problemas Secundarios

P.E 01: ¿De qué manera la Implementación de un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejorará la Autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A.?

P.E 02: ¿De qué manera la Implementación de un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejorará la Autorización de la WLAN de la Empresa SEDA HUÁNUCO S.A.?

1.3 Objetivo General

Determinar la norma IEEE 802.1X para mejorar la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.

1.4 Objetivos Específicos

O.E.1: Determinar la mejora de Implementar un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES para mejorar la Autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A.

O.E.2: Determinar la mejora de Implementar un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES para mejorar la Autorización de la WLAN de la Empresa SEDA HUÁNUCO S.A.

1.5 Justificación de la investigación

1.5.1 Justificación Teórica:

Desde la perspectiva teórica se fundamenta la justificación del estudio en base a la información disponible sobre el estándar IEEE 802.1x, así mismo se procesa y se resume en el anexo el procedimiento manual de la parte teórica para su posterior aplicación en cualquier escenario siempre y cuando el objetivo sea utilizar un servidor Radius para el control de acceso de una red inalámbrica.

1.5.2 Justificación Práctica:

El presente trabajo de investigación se justifica a raíz de la creciente demanda de acciones de mejora en temas de seguridad, en este caso en la seguridad de la información, y a consecuencia de los diferentes riesgos que está expuesto la WLAN de la empresa SEDA Huánuco, y de comprometer sus procesos inmersos en el uso de esta tecnología. Con la implementación de la norma IEEE 802.1x que se desarrollará en la presente investigación, se conseguirá mejorar la seguridad en cuanto al acceso a la WLAN de la empresa SEDA Huánuco.

1.5.3 Justificación Metodológica:

Existe la metodología que nos permite la realización y aplicación de este tipo de estudio aplicado utilizando la tecnología, la metodología consiste en la instalación, configuración, administración y soporte del Servidor, dicha metodología se aplica a diferentes entornos en el cual se opta el uso de un servidor para la solución de un problema en particular.

1.6 Limitaciones de la investigación

Las limitaciones encontradas para realizar la presente investigación son:

- Se debe contar con la presencia de los trabajadores del área de la OMS para lograr una correcta recolección de información, ya que son considerados como integrantes de la muestra; para ello se debe citarlos previamente para poder tener su disponibilidad en cuanto a tiempo.
- Escasa bibliografía sobre la norma IEEE 802.1X e implementación en entornos de software libre.

1.7 Viabilidad de la investigación

La presente investigación resulta viable, a razón de las siguientes premisas:

- Se tiene conocimiento y recursos bibliográficos (físicos y virtuales) para la realización de la investigación, en lo relacionado a la implementación de la norma IEEE 802.1X.
- Se cuenta con los permisos correspondientes, por parte de la gerencia del área, así como con la venia de las autoridades de empresa SEDA Huánuco.
- Se dispone del tiempo suficiente para desarrollar la investigación los próximos meses del presente año.
- Todos los gastos desembolsables para desarrollar la investigación, están dentro del presupuesto y alcance del investigador.
- Se cuenta con los recursos físicos y tecnológicos para el normal desarrollo de la investigación.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

Antecedentes Internacionales

a. (García, 2012) realizo la investigación: Implementación de un Servidor Radius en la Escuela Superior de Ingeniería Mecánica Y Eléctrica de la Ciudad de México. La investigación llego a las principales conclusiones:
   - La autentificación es una parte Fundamental en la informática y la seguridad de la información ya que permite la compartición de recursos informáticos de manera confiable, la informática y las tecnologías de la información demandan una mayor asertividad en la identificación de usuarios, es por este motivo que la implementación de este servidor de autenticación es en gran medida una forma de comprender esta necesidad y es porque solo mediante la conjunción de los diversos protocolos de autenticación y envío de mensajes que es posible.
   - Es en este caso el poder ver y entender de una manera muy fácil el protocolo de autenticación por desafío y compartimiento de secreto, y el protocolo PAP (Password Authentication Protocol) que es uno de los más necesarios y más sencillos, entre otras cosas, vimos que un mismo protocolo puede estar dado en más de una plataforma tecnológica que en este caso el Radius tiene la característica de poderse encontrar en forma gratuita en FreeRadius y En el servidor de Windows como el Internet Authentication Server. En fin esta poderosísima herramienta nos permite tener una pequeña red en casa que nos puede servir para tener cámara IP conectadas a nuestra RED, o bien incluso hasta un café Internet.

b. (López, 2012) realizo la investigación: Implementación de un portal cautivo para la autenticación de usuarios en redes usando herramientas de software libre. México. La investigación llego a las principales conclusiones:

- Actualmente la autenticación es un mecanismo muy importante para proteger el acceso a los recursos de información. Por otra parte, existen muchas herramientas que permiten llevar a cabo la autenticación de usuarios en una red, cada una de éstas tiene ventajas y a la vez desventajas.
- Dichas herramientas pueden ir desde un simple software hasta un protocolo complejo, es importante, conocer la existencia de dichas herramientas ya que pueden ser de gran utilidad. En el área de seguridad, se concluye que nada puede ser totalmente seguro, ya que algunas de las desventajas que existen en las herramientas, son ocasionadas por la naturaleza del protocolo que se usa. En otras implementaciones el punto más débil del mecanismo de autenticación es el propio usuario.
- La herramienta NoCat es una implementación de portal cautivo que ofrece gran compatibilidad con protocolos de autenticación. La complejidad de la instalación y configuración de una infraestructura de red que autentique con esta herramienta depende mucho del servidor de autenticación que se utilice, ya que no es lo mismo instalar un servidor LDAP, que uno de RADIUS, uno de SAMBA o simplemente un servidor de base de datos.
- La arquitectura empleada en un mecanismo de autenticación es un factor muy importante para poder generar un sistema robusto, ya que al separar los servicios en equipos físicos distintos, se vuelve más complejo el poder vulnerar dicho sistema, debido a que se requiere comprometer más equipos con configuraciones diferentes cada uno. Por otra parte con la instalación y configuración de varios servicios de autenticación, comprendí que muchos de estos servicios se pueden complementar para generar un servicio más robusto, y que realizar estás configuraciones requiere de un conocimiento especializado, a mayor complejidad del servicio, mayor es el conocimiento requerido. La elaboración de este trabajo me permitió adquirir conocimientos más sólidos, en el área de redes y seguridad, principalmente sobre los mecanismos de autenticación, así como, conocer con más detalle algunos de los

protocolos de autenticación robustos, administración y configuración de servidores Linux y arquitecturas de red. Por otra parte me permitió poner en práctica conocimientos que he adquirido durante mi estancia en la Universidad Nacional Autónoma de México.

c. (Tapia, 2012) realizo la investigación: Implementación de un Portal Cautivo que permita el Control de Acceso al Servicio de Internet a los estudiantes del Colegio San Luis Gonzaga a través de una Autenticación de los usuarios mediante un servicio AAA implementado en un Servidor que trabaje con Protocolo Radius en la Universidad Politécnica Salesiana de la ciudad de Quito. La investigación llego a las principales conclusiones:
   - El control del ingreso de los usuarios al servicio del internet se puede administrar y cuantificar, por lo que es posible adoptar nuevas políticas de uso según se vaya trabajando en el Portal Cautivo del Colegio San Luis Gonzaga.
   - El Portal Cautivo del Colegio San Luis Gonzaga permite utilizar una encriptación básica de los datos de los usuarios que viajan en la red inalámbrica para el uso del internet a un nivel de tipo académico, esta implementación de seguridad en la institución es suficiente en cuanto al nivel de seguridad planteada. Este tipo de soluciones en cuanto a seguridad de redes no son tan viables en empresas o instituciones que requieran un alto nivel de seguridad y protección para los datos de los usuarios, para lo cual se cuenta con distintos tipos de soluciones de hardware y software a una escala mucho mayor.
   - La restricción y administración de los sitios web permitidos para el Colegio San Luis Gonzaga se realizó en conjunto con un Firewall Cisco el cual administra la red utilizando WebFilters y limitadores de ancho de banda.
   - Chillispot no ofrece la opción de limitaciones de tiempo para los usuarios conectados al Portal Cautivo, pero la configuración actual

está totalmente acorde con la política del Colegio San Luis Gonzaga de que el servicio de internet esté libre por ser un servicio meramente de investigación y con esta premisa no se debería limitar el tiempo de la indagación de conocimientos e información académica.

- Al trabajar en conjunto los distintos tipos de software, proveen de total disponibilidad e integridad del servicio en cuanto a la conectividad de red a través del portal cautivo para los usuarios de la Red Inalámbrica del Colegio San Luis Gonzaga.
- Al centralizar la instalación de todos los programas en un mismo servidor físico, la comunicación entre el software de autenticación y el software de administración de usuarios, se ejecuta más efectivamente, debido a que utiliza el ancho de banda del bus de datos propio del servidor implementado, asegurando una respuesta mucho más rápida de la verificación de los datos del usuario.
- El control administrativo del portal cautivo es totalmente adaptable a una red específica, por lo que su implementación resulta bondadosa en cuanto a costo/beneficio, debido a su bajo costo de implementación y gran utilidad para el control de los usuarios de una wlan.

Antecedentes Nacionales

a. (Mori, 2008) , realizo la investigación: Diseño e implementación de un Sistema de gestión de accesos a una Red WI-FI utilizando software libre en la Universidad Pontifica Católica del Perú. La investigación llego a las principales conclusiones:

- Es posible la integración de todas las herramientas de software libre utilizadas en la presente tesis (FreeRADIUS, OpenLDAP, SAMBA, MySQL) con un dominio desarrollado con Microsoft Windows. Es decir, en el caso de que se le desee implementar en una red ya existente y que utilice herramientas comerciales (tales como MS Windows 2003 Server y/o MS Active Directory) bastaría con

modificar algunos parámetros en los archivos de configuración de las herramientas de software libre utilizadas para poder lograr la integración y trabajo entre todos estos.

- La implementación de este prototipo no contempla mecanismos de seguridad que aseguren ataques provenientes desde el interior de la red (la red cableada). Lo que se plantea aquí es garantizar un medio de acceso seguro entre el cliente móvil y el punto de acceso a la red (AP); más no entre éste y los elementos de la red interna (tales como servidores de correo, web, archivos, entre otros).
- La implementación se ha optimizado para los clientes móviles que cuenten con una notebook con sistema operativo MS Windows XP SP2 o MS Windows Vista; ya que de acuerdo al escenario inicial planteado todos los clientes de esta organización cuentan con dicho sistema operativo. Sin embargo, también hubiese sido posible brindar soporte para clientes con otros sistemas operativos, tales como distribuciones libres de GNU Linux (Ubuntu 6.06 Desktop Edition, CentOS, etc.). Sin embargo, lo que no se hubiese soportado es a aquellos clientes móviles con otros tipos de equipo portátiles (tales como PDAs, Pocket PC, smartphones, etc.) que no contaran con soporte de WPA2 Enterprise (como es el caso de las PDA de la marca Palm, a excepción del modelo T|X que cuenta con un upgrade para poder soportar esto).

b. (Hernan, 2007) , realizo la investigación: Diseño de una red local inalámbrica utilizando un sistema de seguridad basado en los protocolos WPA Y 802.1X para un complejo hotelero en la Universidad Pontifica Católica del Perú. La investigación llego a las principales conclusiones:

- Las soluciones basadas en redes inalámbricas están disponibles hoy en día y es sólo el principio de una tendencia creciente. El estándar 802.11g prometen un gran ancho de banda para permitir un buen número de nuevas aplicaciones; aunque aún existen varios obstáculos que se tiene que vencer como la seguridad e

interferencia, las Redes inalámbricas ofrecen por lo pronto una comunicación eficiente tanto en interiores como exteriores.

- El diseño de una Red Inalámbrica de área local es una solución versátil que permite el intercambio de información y acceso a Internet, pudiendo ser instalada en distintos lugares, donde el cableado no pueda ser accesible.
- Un factor importante al realizar el diseño de una Red Inalámbrica de área local es la pérdida de potencia de la señal de radiofrecuencia al encontrar obstáculos como vidrio, ladrillo, madera, etc.
- La ubicación de uno o más Puntos de Acceso y los obstáculos que tendrá que pasar determinan la zona de cobertura de la red inalámbrica.
- El ancho de banda que posea un usuario haciendo uso de la red inalámbrica está directamente relacionada con la cantidad de potencia que reciba del Punto de Acceso. Se podrá mejorar la potencia instalando más Puntos de Acceso, por lo cual se tendrá que hacer un balance entre velocidad y cobertura y costo.
- La seguridad es un factor importante al diseñar una Red Inalámbrica. Una Red Inalámbrica sin seguridad permitirá el acceso de personas sin autorización, exposición de nuestra información y la mal configuración de los equipos.
- Los precios de los productos para implementar Redes Inalámbricas han estado reduciendo enormemente, y continuarán bajando conforme se alcance el consumo masivo de software y hardware basados en tecnologías inalámbricas.
- Cuando se evalúa una solución inalámbrica que pueda satisfacer las necesidades de comunicación es muy importante tener en cuenta los estándares y tecnologías de más penetración. Esta decisión ahorrará dinero, tiempo y problemas de incompatibilidad y brindará una comunicación rápida, eficiente, segura y transparente.

c. (Leon, 2012), realizo la investigación: Buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo. Chiclayo. La investigación llego a las principales conclusiones:

- Al presentar esta investigación, se propone buenas prácticas para el desarrollo de auditorías de redes inalámbricas aplicadas a las empresas del rubro hotelero. La propuesta está basada en el estudio de las empresas del rubro hotelero de la ciudad de Chiclayo con el fin de mejorar la disponibilidad, confiabilidad e integridad de la información, cotejando metodologías existentes que ayuden auditar redes inalámbricas, y desarrollando la propuesta de las buenas prácticas. En base a las metodologías COBIT 4.1, NTP – ISO – I
- EC 27001, NTP – ISO – IEC 27002, Osstmm Wireless 2.9, ENISA, RED-M, Information networks planning and design (INPD) y metodología para administrar redes 3.0., se elaboraron buenas prácticas para auditar redes inalámbricas. Como parte de las buenas prácticas se encuentra, los dominios Diseño, Administración y Seguridad, y cada una presenta sus buenas prácticas, a la vez cada de estas tiene su objetivo, actividades o tareas, herramientas de apoyo y un Checklist para auditar la red inalámbrica. Se utilizó la entrevista, encuesta, análisis de la red inalámbrica y documentos para recaudar información a través de los archivos históricos referentes a la aplicación de metodologías o guías de auditoría en la red inalámbrica.
- Se realizó un estudio pre experimental, realizándose una encuesta a las entidades hoteleras para poder determinar si cuentan con una red inalámbrica, si se realizaron auditorías a la red inalámbrica, si se basaron en algún documento, norma o guía de buenas prácticas, etc.; basándose en la información recopilada anteriormente se determinó una entidad hotelera para desarrollar y aplicar la propuesta para las buenas prácticas en la auditoría de la red

inalámbrica, y por último evaluar si lo hecho sirve para cualquier institución.

Antecedentes Nacionales

Después de haber realizado una revisión en las diferentes universidades e institutos de la localidad sobre temas de investigación relacionados o parecidos al presente, se puede afirmar que no se encontraron trabajos similares al presente estudio de investigación.

2.2 Bases Teóricas

2.2.1 Redes WI-FI

Redes: (Millahual, 2012), Llamamos red a un conjunto de computadoras que están conectadas entre sí por algún medio que puede ser físico (cables) o no (ondas electromagnéticas). El objetivo principal de la red es que se puedan compartir recursos e información entre todos los elementos que la integran, y tener flexibilidad para así optimizar tareas o procesos que los usuarios realizan. Las redes de computadoras evolucionan para obtener mayor movilidad y/o rendimiento de las tareas.

Redes de Área Local: (Tanenbaum, 2003), Las redes de área local (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LANs son diferentes de otros tipos de redes en tres aspectos: 1) tamaño; 2) tecnología de transmisión, y 3) topología.

Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de

antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red. Las LANs podrían utilizar una tecnología de transmisión que consiste en un cable al cual están unidas todas las máquinas, como alguna vez lo estuvo parte de las líneas de las compañías telefónicas en áreas rurales. Las LANs tradicionales se ejecutan a una velocidad de 10 a 100 Mbps, tienen un retardo bajo (microsegundos o nanosegundos) y cometen muy pocos errores. Las LANs más nuevas funcionan hasta a 10 Gbps. En este libro continuaremos con lo tradicional y mediremos las velocidades de las líneas en megabits por segundo (1 Mbps es igual a 1,000,000 de bits por segundo) y gigabits por segundo (1 Gbps es igual a 1,000,000,000 de bits por segundo).

Redes Inalámbricas: (Stallings, 2004), Como su propio nombre indica, una red LAN inalámbrica es aquella que hace uso de un medio de transmisión inalámbrico. Hasta hace relativamente poco tiempo, las redes LAN inalámbricas eran poco usadas debido a su alto precio, la baja velocidad de transmisión, la existencia de problemas de seguridad y la necesidad de licencias. A medida que estos problemas se han ido solucionando, la popularidad de las LAN inalámbricas ha crecido rápidamente.

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total entre las estaciones pertenecientes a la red y capacidad de difusión. Además de las mencionadas, existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- Rendimiento: el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio inalámbrico para maximizar la capacidad.

- Número de nodos: las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.
- Conexión a la LAN troncal: en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas ad hoc.
- Área de servicio: una zona de cobertura para una red LAN inalámbrica tiene un diámetro típico de entre 100 y 300 metros.

Redes WLAN IEEE 802.11: El componente elemental de una red LAN inalámbrica es un conjunto básico de servicios (BSS, Basic Service Set), consistente en un número de estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. Un BSS puede funcionar aisladamente o bien estar conectado a un sistema troncal de distribución (DS, Distribution System) a través de un punto de acceso (AP, Access Point) que efectúa las funciones de puente. El protocolo MAC puede ser completamente distribuido o bien estar controlado por una función central de coordinación ubicada en el punto de acceso. Generalmente, el BSS se corresponde con lo que en la bibliografía es referido como «celda». Por otro lado, el DS puede ser un conmutador, una red cableada tradicional u otra red inalámbrica.

La configuración más simple posible es la que cada estación pertenece a un BSS aislado; esto es, cada estación se encuentra dentro del rango de otras estaciones que pertenecen al mismo BSS. Es igualmente posible que exista un solapamiento geográfico entre dos BSS, de manera que una estación podría formar parte de más de un BSS. Además, la asociación entre una estación y un BSS es dinámica, puesto que una estación puede apagarse, salirse de la distancia máxima permitida o incorporarse de nuevo. Un conjunto extendido de servicios (ESS, Extended Service Set) consiste en dos o más conjuntos

básicos de servicios interconectados mediante un sistema de distribución. Este último es, por lo general, una LAN cableada troncal, aunque puede tratarse de cualquier red de comunicaciones. El conjunto extendido de servicios aparece a nivel de control de enlace lógico (LLC) como una única red LAN lógica.

Un AP se implementa como parte de una estación. El AP constituye la lógica dentro de la estación que proporciona el acceso al DS a través de los servicios de distribución, además de servir como estación. La integración de una arquitectura 802.11 con una red LAN cableada tradicional se realiza a través de un portal. La lógica del portal se implementa en un elemento, como un puente o un dispositivo de encaminamiento, que forme parte de la LAN cableada y que se encuentre conectado al DS.

Servicios de IEEE 802.11: La normativa IEEE 802.11 define nueve servicios que deben ser proporcionados por una red inalámbrica para ofrecer una funcionalidad equivalente a la inherente a una LAN cableada tradicional:

1. El proveedor de servicios puede ser tanto la estación como el DS. Los servicios de la estación son implementados en cada estación IEEE 802.11, incluyendo la estación que constituye el AP. Los servicios de distribución son proporcionados entre BSS diferentes y deben ser implementados en un AP o en cualquier otro dispositivo de propósito específico conectado al sistema de distribución.

2. Tres de los servicios enumerados se emplean para controlar el acceso a una LAN IEEE 802.11 y para proporcionar confidencialidad. Los seis servicios restantes dan soporte a la entrega de unidades de datos de servicio MAC (MSDU, MAC Service Data Units) entre estaciones. Una MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en la forma de una PDU LLC. Si una MSDU es demasiado grande para ser transmitida en una sola

trama MAC, puede ser fragmentada y transmitida en una serie de tramas.

Topología de redes inalámbricas WLAN: (Tanenbaum, 2003), Como en la mayoría de redes LAN, en las redes WLAN (Redes Inalámbricas de Área local) podemos encontrar dos tipos de topologías: Red Ad-Hoc y Red Modo Infraestructura, que define el conjunto de estándares 802.11.

Topología Ad-Hoc

La topología ad hoc, conocida como punto a punto, es un modo de conexión para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo ad hoc, no se requiere involucrar un punto de acceso central. Los dispositivos que conformen una red ad hoc se pueden comunicar directamente con otros clientes.

Para este modo de operación y conexión, cada dispositivo cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico en modo ad hoc y usar el mismos SSID (Service Set IDentifiel) conocido como nombre de la red y “numero de canal” de la red.

Una red de tipo ad hoc normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca uno de otro. El rendimiento es menor a medida que el número de nodos crece. Para el estándar 802.11 el modo ad hoc se denota como Conjunto de Servicios Básicos Independientes (IBSS –Independent Basic Service Set)

Topología modo infraestructura

La forma de operación más común de las redes inalámbricas WLAN es el modo infraestructura. En modo infraestructura a comparación del modo ad hoc, hay un elemento central de “coordinación”: un punto de acceso o estación base. Las estaciones inalámbricas no se pueden comunicar directamente, todos los datos deben pasar a través del AP (punto de acceso) La función AP actúa como puente hacia la red

cableada y hacia las estaciones inalámbricas, permitiendo el servicio y comunicación hacia los clientes conectados. Para el estándar 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos (BSS –Basic Service Set) conocido o maestro y cliente.

Arquitectura de WLAN IEEE 802.11: (Martínez, 2005), La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. Diferentes tecnologías de capa física se definen para transmitir por el medio inalámbrico

Capas de IEEE 802.11: (Rodríguez, 2001) El estándar IEEE 802.11 (Instituto de Ingenieros Eléctricos y Electrónicos) norma las comunicaciones a nivel MAC (Capa de acceso al medio) y PHY (capa física) para dispositivos móviles y portátiles. Los dispositivos portátiles se mueven de un sitio a otro, pero acceden a la red desde puntos fijos. Para los dispositivos móviles el acceso a la red se da cuando están en movimiento.

Capa Física (PHY)

La capa física proporciona una serie de servicios a la capa MAC (capa de acceso al medio). Diferentes tecnologías de capa física se definen para transmitir por el medio inalámbrico. La capa física de servicios consiste en dos protocolos:

- Una función de convergencia de capa física, que adapta las capacidades del sistema físico depende del medio PMD (Physical Medium Dependent). Esta función es implementada por el protocolo PLCP (Physical Layer Convergence Protocol), que define una forma de mapear MPDUs (MAC Protocol Data Unit) en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones a través de la capa PMD.

- Un sistema PMD (Physical Medium Dependent), cuya función define las características y un medio de transmisión y recibir a través de un medio sin cables entre dos o más estaciones. La

comunicación entre capas de de acceso al medio de diferentes estaciones se realiza a través de la capa física mediante una seria de puntos de acceso al servicio

Técnicas de transmisión capa física

La capa física del estándar 802.11 define diferentes técnicas de transmisión, mediante la cual se propaga la red inalámbrica de área local

Técnicas de transmisión Infrarrojo

La técnica de transmisión infrarrojo utiliza una transmisión difusa (es decir, no requiere línea visual) a 0.85 o 0.95 micras. Se permite dos velocidades: 1 y 2 Mbps A 1 Mbps se utiliza un esquema de codificación en el cual un grupo de 4 bits se codifica como una palabra de 16 bits, que contiene quince 0s y un 1, mediante código de Gray. Este código tiene la propiedad de que un pequeño error en la sincronización en el tiempo lleva a un solo error de bits en la salida. Las señales de infrarrojo no pueden penetrar las paredes, por lo que las celdas en los diferentes cuartos están bien aisladas entre sí. Sin embargo, debido al bajo ancho de banda (y al hecho de que la luz solar afecta las señales de infrarrojo), esta no es una opción muy popular.

Técnica de transmisión FHSS (Espectro Disperso con Salto de Frecuencia).

Esta técnica utiliza 79 canales, cada uno de los canales tiene un ancho de banda de 1HMGz, iniciando en el extremo más bajo de la banda ISM de 2.4 GHz Para producir la secuencia de frecuencia a saltar, se utiliza un generador de números pseudoaleatorios. Siempre y cuando todas las estaciones utilicen las mismas semillas para el generador de números pseudoaleatorios y permanezcan sincronizadas, saltarán de manera simultánea a la misma frecuencia. La aleatorización de FHSS proporciona una forma justa de asignar espectro en la banda ISM no regulada. También proporciona algo de seguridad pues un intruso que

no sepa la secuencia de saltos o el tiempo de permanecía no puede espiar las transmisiones

Técnicas de transmisión DSSS (Espectro Disperso de Secuencia Directa)

Esta técnica consiste en la combinación de la señal a transmitir en una secuencia de bits a mayor velocidad de transmisión. A esta secuencia se le conoce como chipping code o “código de troceado” y no es más que un patrón redundante de bits asignados a cada bit a enviar, que divide la información del usuario acorde a un “radio de esparcimiento” Spread Ratio. Cuando se desea enviar la información, realmente se transmite los códigos correspondientes. Si uno o más bits del patrón sufren interferencias durante la transmisión, el receptor podría reconstruir el dato enviado, gracias a la reducción del chipping code (menor número de canales)

Técnicas de transmisión OFDM (Multiplexado por División de Frecuencia Ortogonal).

En una comunicación inalámbrica a alta tasa de bits, se requiere un gran

ancho de banda; en estos casos el canal es susceptible a presentar desvanecimientos selectivos en frecuencia (no plano). Además, esta técnica se constituye como una de las candidatas más probables

para la tecnología móvil de cuarta generación. Por otro lado, la técnica OFDM fue seleccionada para la transmisión en redes de área local de alto rendimiento (HIPERLAN) y forma parte del estándar IEEE 802.11 para redes de área local no guiada (WLAN). En comunicaciones guiadas, OFDM se emplea en la línea digital asimétrica del abonado (ADSL, Asymetric Digital Suscriber Line) y la línea digital de alta velocidad del abonado.

2.2.2 Seguridad en Redes WI-FI

Riesgos de las redes inalámbricas: (INTECO, 2012), Las redes inalámbricas Wi-Fi han posibilitado la sustitución de los cables por ondas de radio. De este modo, se eliminan las ataduras y limitaciones de los dispositivos de conexión. Pero también permiten una mayor facilidad para que cualquiera tenga acceso a los datos que circulan por la red. Si con los cables un atacante debía obtener acceso físico a un punto de acceso para poder realizar alguna acción, con las redes inalámbricas esta tarea se vuelve trivial. Al eliminarse el componente físico que podía llegar a proteger los datos, éstos quedan mucho más expuestos.

Por tanto, si se quiere hacer un uso responsable y seguro de esta tecnología, el modelo de redes inalámbricas debe centrarse en el cifrado de los datos. A continuación, se exponen los riesgos a los que están expuestas estas redes:

a) Redes abiertas

Las redes abiertas se definen o caracterizan por no tener implementado ningún sistema de autenticación o cifrado, dando acceso a cualquier usuario que tenga la facilidad de conexión mediante algún dispositivo inalámbrico, permitiendo el acceso total de dicho AP (punto de acceso). Y que facilita la conexión a Internet. Para las redes abiertas los únicos elementos de seguridad que se pueden implementar y que proporcionan un cierto grado de confianza, es la implementación de:

- Direcciones MAC
- Direcciones IP
- El ESSID de la red

b) Romper ACL (Listas de Control de Acceso) basado en MAC

Las listas de control de acceso fueron la primera medida de seguridad implementada en redes inalámbricas, y siguen siendo, el filtro de conexión por dirección MAC. El mecanismo de ACL, consiste en definir si cierta dirección o cierta subred tienen privilegio de acceso o

denegación a la conexión del punto de acceso para permitir la salida a Internet.

La ruptura de ACL basadas en MAC se lleva a cabo mediante el mecanismo de un ataque tipo DoS (Denegación de Servicio) a la computadora, basado en cambiar la MAC (control de acceso al medio) de autentificación mediante la MAC de otro equipo.

c) Ataque de denegación de servicios (DoS)

La implementación del ataque de denegación de servicios en una red inalámbrica, como objetivo fundamental, es impedir la comunicación entre el AP y una terminal. Para lograr esto sólo hemos de hacernos pasar por el AP poniendo la dirección MAC que lo identifica (la obtención de la MAC se puede obtener mediante un sniffer negando la comunicación a la terminal o terminales que se conecten mediante envió de notificaciones de asociación).

d) Descubriendo ESSID Ocultos

La filosofía de ESSID (Extended Service Set IDentifier) ocultos está basada en seguridad por oscuridad (STO, segurity through obscurity) la cual consiste en ocultar ESSID mejor conocido como nombre de red, como método para aumenta la invisibilidad de dicha red; sin embargo, una vez más se ha demostrado que este tipo de mecanismo utilizado en redes abiertas no resulta efectivo. En la mayoría de puntos de acceso se puede encontrar la opción de configuración para deshabilitar él envió de ESSID en los paquetes o desactivar los BEACOM FRAMES. Aun implementada esta medida de seguridad, un presunto ataque tendría dos opciones:

- Husmear la red durante un tiempo indefinido con objeto de conseguir el nombre de red mediante una nueva conexión a través de las tramas PROVE REQUEST del cliente.
- Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque dos, pero sin mantener al cliente desconectado.

e) Ataque Man in the middle

Basado en la traducción al español seria “Hombre en Medio,” se define como a la persona que se encuentra en medio de la comunicación entre el origen y el destino. La habilidad que se posee mediante este mecanismo es que puede observar, interceptar, modificar y retransmitir la información que viaja entre el origen y el destino, originando los siguientes posibles ataques.

f) Sniffing

El objetivo de este medio es poner la tarjeta de red en un estado conocido como “modo promiscuo o modo monitor” ya que de esta manera se puede capturar todo el tráfico que viaja por la red, logrando la obtención de la siguiente información; credenciales enviadas (Users, Passwords, Ccs.), Información enviada (archivos, páginas) y poder observar el comportamiento del usuario en base al tráfico de la red.

g) Spoofing

Se define como: “Creación de respuestas o señales para mantener una sesión activa y evitar tiempos de espera. Algunas acciones que se pueden ejecutar con Spoofing (Suplantación de Identidad) son las siguientes:

- El atacante puede enviar datos como si fuera el origen
- Realizar operaciones con los datos del cliente
- Mostrar páginas falsas
- Enviar datos a destinos diferentes

Protocolos de seguridad WLAN: (Pellejero, 2006), Entre los protocolos de seguridad usados en las WLAN tenemos:

WEP (Wired Equivalent Privacy)

EL IEEE publicó un mecanismo opcional de seguridad, denominado WEP (Wired Equivalent Privacy), en la norma de redes inalámbricas 802.11 (ANSI/IEEE Std 802.11, 1999). Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha

convertido en una protección inservible. Por otro lado, WEP es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permiten cifrar la información que se transmite. El protocolo WEP proporciona cifrado a nivel 2. Está basado en algoritmos de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización IV) o de 128 bits (104 bits más 24 bits de IV).
El protocolo WEP se basa en dos componentes para cifrar las tramas de circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

El problema con WEP no está en RC4, sino en cómo lo implementa. WEP no crea bien el vector de iniciación del algoritmo, y hace que los vectores sean predecibles para incrementar el vector de un paquete a otro. Además, existe un problema con el tamaño de los vectores de iniciación. Todo esto ha hecho que WEP se considere inseguro, y que existan numerosas herramientas capaces de averiguar en cuestión de minutos la clave con la que están cifrados los datos. Para limitar estos ataques, se creó WEP+.

Por otro lado, una de las grandes desventajas en este protocolo de seguridad es que utiliza llaves estáticas lo que implica que todos y cada uno de los usuarios tienen que usar la misma clave. Este método suele provocar que las claves no se cambien durante meses, facilitando su obtención. El hecho de que el IV (vector de inicialización) se transmita sin encriptar y de que se pueda repetir cada cierto tiempo, además de que el algoritmo que genera este vector presenta ciertos caracteres de predictibilidad, hace que sea un sistema perfecto para romper por fuerza bruta. Algunos tipos de ataques que se utilizan para este tipo de encriptación son los siguientes:

- Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico.
- Ataques activos basados en la introducción de paquetes.
- Ataques activos basados en el ataque/engaño al punto de acceso
- Ataque de diccionario

El ISAAC (Internet Security, Application, Authentication and Cryptography) hizo un estudio profundo acerca de los problemas y debilidades del protocolo WEP llegando a las siguientes conclusiones:

- Los ataques de Sniffing se basan sólo en obtener la clave WEP que es cambiada infrecuentemente.
- Una longitud de claves de 64 0 128 bits hoy en día no es suficiente garantizar un buen nivel de seguridad.
- Los algoritmos de cifrado son vulnerables al análisis si se utiliza frecuentemente los mismos keystreams.
- El cambio infrecuente de las claves permite a los atacantes usar las técnicas de ataque por diccionario.
- El protocolo WEP utiliza CRC para garantizar la integridad de los frames
- enviados. Aunque el CRC es encriptado por el algoritmo de RC4, y los CRC no son criptográficamente seguros.

a) WPA (Wireless Protected Access)

WPA (Wireless Protected Access) tiene sus orígenes en los problemas detectados en el anterior sistema de seguridad para las redes inalámbricas. La idea fundamental al desarrollar este protocolo fue crear un sistema de seguridad que hiciera de puente entre WEB y el estándar 802.11i (WPA2). Este mecanismo utiliza el protocolo TKIP (Temporal Key Integrity Protocol) y mecanismo 802.1X. La combinación de estos dos sistemas proporciona una encriptación dinámica y un proceso de autentificación mutuo. Así pues, WPA involucra dos

aspectos: un sistema de encriptación mediante TKIP y un proceso de autentificación mediante 802.1X.

WPA implementa la mayoría del estándar IEEE 802.11i y fue creado por Wi-Fi Alliance para corregir WEP de forma transitoria. Se necesitaba algo que corrigiera WEP, pero que a su vez fuese compatible con el hardware del momento. Mientras se esperaba a que estuviese preparado y definido WPA2, la alianza creó un sistema intermedio. WPA fue diseñado para utilizar un servidor de autenticación (normalmente Radius), que distribuye claves diferentes a cada usuario. También se puede utilizar en modo de clave pre-compartida (PSK, Pre-Shared Key), menos seguro que con el servidor Radius.

La información es cifrada utilizando el algoritmo RC4 (porque debía ser compatible con lo ya existente) pero mejorado y bien implementado. La clave es de 128 bits y el vector de inicialización de 48 bits. Una de las mejoras fundamentales sobre WEP es la implementación del Protocolo de Integridad de Clave Temporal (TKIP o Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Fue específicamente diseñado, junto con un vector de inicialización (IV) mucho más grande, para evitar los ataques ya conocidos contra WEP. Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información. Con CRC era posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad mejorado (MIC o Message Integrity Code), también conocido como Michael. Además, WPA previene contra ataques de repetición, puesto que incluye un contador de tramas.

Privacidad e integridad con TKIP

Temporal Key Integrity Protocol (TKIP) es el protocolo elegido con el objetivo de sustituir al sistema de encriptación WEB y solucionar los problemas de seguridad que éste plantea. TKIP usa el algoritmo RC4 proporcionado por RSA Security para encripatar el cuerpo del frame así

como el CRC antes de la transmisión. Así como características mejoradas destacar la ampliación de la clave a 128 bits y el cambio del carácter de la misma de llave estática a llaves dinámicas; cambiando por usuario, sesión y paquete y añadiendo temporalidad. El vector de inicialización pasa de 24 bits a 48 bits, minimizando la reutilización de claves. Y como colofón se han añadido claves para tráfico de difusión y multidifusión

Autenticación mediante 802.1X/EAP

El plus principal del estándar 802.11x es encapsular los protocolos de autentificación sobre los protocolos de la capa de enlace de datos (MAC) y permite emplear el protocolo de autentificación Extensible (EAP) para autentificar al usuario de varias maneras. El estándar IEEE 802.11x define 3 entidades:

- El solicitante (supplicant), reside en la estación inalámbrica
- El autentificado (authenticador), reside en el punto de acceso
- El servidor de autentificación, reside en un servidor AAA (Authentication, Authorization, and Accounting) como RADIUS

El funcionamiento basado en el estándar 802.11x se centra en la denegación de cualquier tráfico que no sea hacia el servidor de autentificación hasta que el cliente no se haya autentificado correctamente. El método del autenticador es crear un puerto por cliente que define dos caminos, uno autorizado y otro no autorizado; manteniendo el primero cerrado hasta que el servidor de autentificación le comunique que el cliente tiene acceso al camino autorizado. Los métodos de autentificación empleados en el protocolo WPA son los siguientes: EAP-TLS, EAP.TTLS y PEAP. Se basas en el método de Infraestructura pública (PKI) para autentificar al usuario y al servidor de autenticación mediante certificados digitales. Para ello se emplea la existencia de una Autoridad de Certificados (CA), sea empresaria o pública.

EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)

El mecanismo que mantiene (EAP-TLS) es mediante la de certificados digitales por parte del cliente y el servidor de autentificación; el proceso de autenticación comienza con envió de su identificación (nombre de usuario) por parte del solicitante hacia el servidor de autentificación, tras esto, el servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo propio. Si el certificado del solicitante es validado, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado, la cual es enviada al punto de acceso por el servidor de autentificación para que pueda comenzar la comunicación segura

PEAP y EAP-TLS

El protocolo de autenticación extensible protegido en sus siglas en inglés (PEAP) es un nuevo miembro de la familia de protocolos de Protección de Autentificación Extensible (EAP). PEAP utiliza seguridad de nivel de transporte (TLS) para crear un canal cifrado entre el cliente de autenticación PEAR, como un equipo inalámbrico, y un autenticador PEAP, como un servicio de autenticación de internet (IAS) o un servidor del servicio de usuario de acceso telefónico de autenticación remota (RADIUS). PEAP no específica un método de autenticación, sino que proporciona seguridad adicional para otros protocolos de autenticación EAP. PEAP se utiliza como método de autentificación para los equipos clientes inalámbricos 802.11, pero no se admite en clientes de red privada virtual (VPN) u otros clientes de acceso remoto. La implementación inalámbrica 802.11 con PEAP puede elegir entre dos mecanismos de EAP para usar con PEAP: EAP-MS-CHAPv2 o EAP-TLS. Para EAP-MS-CHAPv2 usa credenciales para la autentificación de usuarios, y un certificado del almacén de certificados del equipo cliente o una tarjeta inteligente para la autentificación del usuario y equipo cliente, y un certificado de alance de certificados del equipo servidor para la autentificación del servicio. Los certificados de clave pública proporcionan un método de autentificación más seguro que los

que utilizan credenciales basadas con contraseña. PEAP con EAPTLS utiliza certificados para la autentificación de servidores y certificados o tarjetas inteligentes para la autenticación de usuarios y quipos clientes. Para utilizar PEAP-EAP-TLS, se debe implementar una infraestructura PKI (Public Key Infrastructure). El inconveniente al implementar el uso de EAP-TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de ellos puede ser difícil y costosa. Para la corrección de este defecto se crearon PEAP (Protected EAP) y EAP-TTLS que únicamente requieren certificados de servicio. La idea fundamental de utilizar estos métodos, es empleando el certificado del servicio previamente validado, el cliente pueda enviar sus datos de autentificación cifrado a través de un túnel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden crear una clave de sesión segura.

b) WPA2

WPA2 está basado en el estándar IEEE 802.11i. WPA2 es la implementación aprobada por Wi-Fi Alliance de estándar 802.11i y es compatible con WPA. WPA2 provee un alto nivel de seguridad incluyendo el algoritmo AES (Sistema Avanzado de Encriptación). WPA2 Personal protege de acceso no autorizado a la red utilizando una contraseña estable. WPA2 enterprise verifica a los usuarios de la red a través de un servidor. El Sistema Avanzado de Encriptación de llave temporal de 128 bits y un vector de inicialización de 48 bits en el proceso de encriptación. Los métodos de autentificación utilizados por el 802.11i utiliza el estándar IEEE 802.11x y el protocolo TKIP.

c) WPA-PSK

Los métodos soportados por EAP necesitan de una cierta infraestructura, fundamentalmente de un servidor RADIUS, lo que puede limitar su implementación en redes pequeñas. Wireless ofrece los beneficios de WPA mediante el uso de una clave pre-compartida

(PSK, pre-shared key). El estándar permite claves de hasta 256 bits, lo que proporciona una seguridad muy elevada. Sin embargo, el escoger claves sencillas y cortas puede hacer vulnerable el sistema frente a ataques de fuerza bruta o ataque de diccionario. Retomando el estándar IEEE 802.1x, específica el protocolo PSK como método de control de acceso para las redes Wi-Fi de empresas. Puede utilizar también el protocolo PSK en entornos de oficinas de reducido tamaño y en entornos domésticos en los que no es posible configurar la autenticación basada en servidores

d) WPA-RADIUS

El sistema RADIUS (Remote Authentication Dial-In User Service) se utiliza frecuentemente para proporcionar servicios de autorización, autentificación y auditoría (AAA) que se utiliza cuando un cliente de acceso telefónico AAA inicia o finaliza una sesión en un Servidor de acceso a redes. RADIUS almacena información de identificación sobre todos los usuarios de la red con contr1aseñas y perfiles individuales, que pueden incluir restricciones de acceso. A continuación, se describen cada una de las fases AAA de servicios que proporciona RADIUS:

- Fase de autentificación: Verifica el nombre de usuario y la contraseña en una base de datos local. Después de verificar las credenciales, se inicia el proceso de autorización.
- Fase de autorización: Determina si se permite que una solicitud tenga acceso a un recurso. Se asigna una dirección IP al cliente de acceso telefónico.
- Fase de auditoría: Recopila información sobre el uso de los recursos para el análisis de tendencias, la auditoría, el cobro de tiempo de las sesiones o la asignación de costos.

A continuación, se describen cada uno de los procesos que se realizan al ejecutar la autentificación mediante el método EAPoL RADIUS:

- La autentificación del cliente se lleva a cabo mediante el protocolo de EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente forma.
- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (o logra enlazarse y asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL
- (EAP over LAN), que es el requerido para efectuar la autenticación.
- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.
- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Reques/Identify.
- La estación se identifica mediante un mensaje EAP-Response/Identify.
- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUS Access- Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.

- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS. El plus de seguridad que se aplica en RADIUS, es la no transmisión de contraseñas en texto claro entre el NAS y un servidor RADIUS. Más bien, un secreto compartido se utiliza con el MD5 algoritmo de hashing de contraseñas para confundir.

2.3 Definición de Términos Básicos

AAA: En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.
ACL: Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

ADSL: Consiste en la transmisión analógica de datos digitales apoyada en el cable de pares simétricos de cobre que lleva la línea telefónica convencional o línea de abonado (Red Telefónica Conmutada, PSTN), siempre y cuando la longitud de línea sea de hasta inclusive 5,5 km medidos desde la central telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

AP: Un punto de acceso inalámbrico (en inglés: wireless access point, conocido por las siglas WAP o AP), en una red de computadoras, es un

dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

ARPANET: Red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales. El primer nodo fue creado en la Universidad de California en Los Ángeles (UCLA), y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP, iniciada en 1983.

D_OD: Es un departamento del brazo ejecutivo del gobierno federal de Estados Unidos encargado de coordinar y supervisar todas las agencias y funciones del gobierno relacionadas directamente con la seguridad nacional y las Fuerzas Armadas de los Estados Unidos.

DOS: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

HANDOFF: Se denomina handover o traspaso (también handoff o transferencia) al sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones. Este mecanismo garantiza la realización del servicio cuando un móvil se traslada a lo largo de su zona de cobertura.

IEEE: El Instituto de Ingeniería Eléctrica y Electrónica es una asociación mundial de ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.

ISM: Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (e.g. Wi-Fi) o WPAN (e.g. Bluetooth).

ISO: La Organización Internacional de Normalización es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

MAC: En informática y telecomunicaciones, el control de acceso al medio (conocido por las siglas MAC, del inglés: Media Access Control) es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios "interlocutores" (dispositivos en una red, como computadoras, teléfonos móviles, etcétera) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico o fibra óptica, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema).

PSK: En criptografía, una clave previamente compartida, clave pre compartida o PSK (en inglés pre-shared key) es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice. Para crear una clave de secreto compartido, se debe utilizar la función de derivación de claves. Estos sistemas utilizan casi siempre algoritmos criptográficos de clave simétrica. El término PSK se utiliza en cifrado Wi-Fi como WEP o WPA, donde tanto el punto de acceso inalámbrico (AP) como todos los clientes comparten la misma clave.

ROAMING: La itinerancia (popularmente se usa el vocablo inglés roaming, róming, que significa vagar, rondar) es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

SSID: El SSID (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres, que la mayoría de las veces son alfanuméricos (aunque el estándar no lo específica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID**.**

TCP/IP: La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

TKIP: TKIP (Temporal Key Integrity Protocol) es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Esto era necesario porque la ruptura de WEP había dejado a las redes WiFi sin seguridad en la capa de enlace, y se necesitaba una solución para el hardware ya desplegado**.**

VPN: Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

2.4 Hipótesis

Hipótesis General

La implementación de la norma IEEE 802.1X mejora la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.

Hipótesis Específicas

H1: La implementación de un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejorará la Autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A.

H2: La implementación de un Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejorará la Autorización de la WLAN de la Empresa SEDA HUÁNUCO S.A.

2.5 Variables

2.5.1 Variable Independiente

X: Norma IEEE 802.1x

2.5.2 Variable Dependiente

Y: Seguridad de la WLAN de la empresa SEDA Huánuco S.A.

2.6 Operacionalización de las variables

VARIABLES	DIMENSIONES	INDICADORES
Variable de Medición Seguridad de la red WLAN	• Autenticación • Autorización • Actualización	• Ocultación del SSID • Filtrado de MAC • DHCP desactivado • Autenticación • Robustez de contraseña • Cifrado • Actualización de Firmware
Variable de Calibración Norma IEEE 802.1X	Protocolo Radius.	• Tipos de Autenticación • Flexibilidad • Administración • Interfaz • Auditoria

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo de Investigación

3.1.1 Enfoque

El enfoque de dicha investigación es cuantitativo ya que según los autores Hernández, Fernández y Baptista, en su libro Metodología de la Investigación (2010). Explica sobre el enfoque cuantitativo, y menciona que una investigación es cuantitativa cuando los datos producto de los instrumentos de recolección son calificativos numéricos de 0 a 100. Con lo cual se puede probar estadísticamente la hipótesis y volcar los resultados en los cuadros estadísticos que respalden la información.

3.1.2 Alcance

Esta investigación por su naturaleza es una investigación aplicativa, ya que se aplicará la tecnología para resolver un problema a nivel técnico.

3.1.3 Diseño

El diseño que presenta el estudio de investigación es el cuasi experimental de pre y post prueba en el grupo de la investigación, teniendo en cuenta el siguiente diseño:

G O1 X O2

Dónde:

G = Grupo de investigación (Trabajadores del área OMS)

X = Aplicación (Norma 802.1x)

$\mathbf{O_1}$ = Pre Observación

$\mathbf{O_2}$ = Post Observación

3.2 Población y Muestra

La población está conformada por todas las áreas de la empresa: Administrativa, Gerencia, Cobros, Soporte, Logística y el área de Organización de Métodos y sistemas; siendo un total de 87 trabajadores de los cuales para la muestra se tomó el número total de empleados que laboran en el área de OMS de la empresa SEDA Huánuco, en este caso conformado por 5 personas. La determinación de la muestra fue no probabilística.

$$n = 5$$

3.3 Técnicas e instrumentos de recolección de datos

Para el presente trabajo de investigación se utilizará el cuestionario de encuesta como principal instrumento de recolección de datos, siendo la encuesta la técnica a usarse; en cuanto a la utilización de dicho instrumento será aplicado a los trabajadores del OMS para que puedan verter sus opiniones correspondientes al manejo del servidor Radius, es así que este cuestionario se aplicara tanto antes y después de la implementación

3.4 Técnicas para el procesamiento y análisis de los datos

Para realizar la presentación de los datos procedentes del instrumento de recolección, se va emplear la estadística descriptiva, por medio de la media, varianza, moda, la tabla de frecuencias con sus respectivas frecuencias relativas y acumuladas. Para ello, se va emplear el paquete informático SPSS, en su versión 20. El cual nos permitirá mostrar los resultados obtenidos mediante tablas y gráficos y con su correspondiente interpretación, esto también nos servirá para poner en prueba la hipótesis.

CAPÍTULO IV: RESULTADOS

4.1 Procesamiento de Datos

Datos tabulados de las respuestas del Pre Test

	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
1	1.00	1.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	1.50
2	1.00	1.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	1.50
3	1.50	1.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	1.00
4	1.00	1.00	1.00	1.00	0.00	0.00	0.00	1.50	0.00	1.50
5	0.00	1.50	1.00	0.00	0.00	0.00	0.00	1.00	0.00	1.50

Datos tabulados de las respuestas del Post Test

	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
1	1.5	1.5	1	1	2	2	2	1	2	2
2	2	2	1	1	1	2	1	2	1	2
3	2	1.5	1	2	1	2	1	1	1	2
4	2	1.5	2	1	1	2	1	1	2	2
5	1.5	2	1	2	2	2	1	1.5	1	2

Matriz de puntuación de instrumentos

Instrumento	*Pregunta*	*Alternativa*	*Puntaje*
Cuestionario sobre la Seguridad de la WLAN	1	Ninguno	0
		WEP	1
		WPA	1.5
		WPA2	2
	2	Baja	1
		Media	1.5
		Alta	2
	3	Básica	1
		Completa	2
	4	No realiza	0
		Semana	1
		Mensual	2
	5	Si	2
		No	0
	6	Si	2
		No	0
	7	Si	2
		No	0
	8	Básica	1
		Media	1.5
		Avanzada	2
	9	Si	2
		No	0
	10	0 – 20	2
		21 – 40	1.5
		41 – 60	1
		61 a más	0

PRE TEST – OMS

Resultados en cuadros y gráficos estadísticos:

En el cuadro # 01, se presentan los resultados de la pregunta número 1 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Ninguno, WEP, WPA Y WPA2. La alternativa WEP posee el 60% de las respuestas.

¿En cuanto a los protocolos de seguridad cuál de ellos se utiliza para el proceso de autenticación en la WLAN?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Ninguno	1	20,0	20,0	20,0
	WEP	3	60,0	60,0	80,0
	WPA	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 01 – Resultados del proceso de autenticación de la WLAN

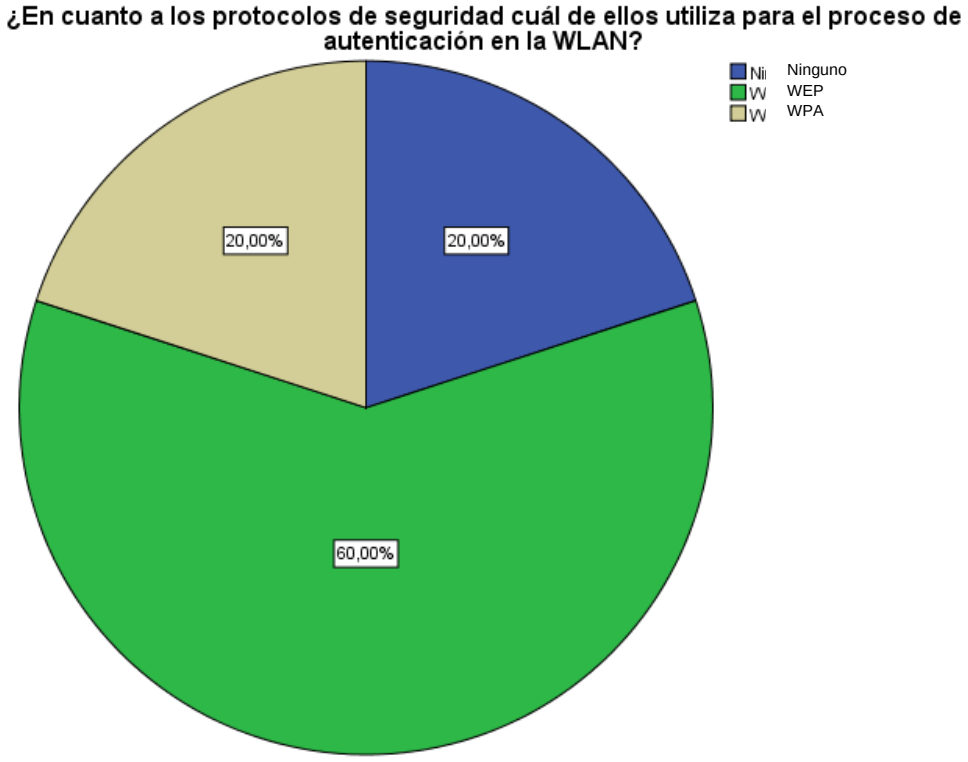


Gráfico # 01 – Resultados del proceso de autenticación de la WLAN

En el cuadro # 02, se presentan los resultados de la pregunta número 2 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: alta, media y baja. La alternativa baja posee el 80%.

Indique Ud. la frecuencia de cambio de contraseña del AP

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Baja	4	80,0	80,0	80,0
	Media	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 02 – Resultados de la frecuencia de cambio de contraseña de la WLAN

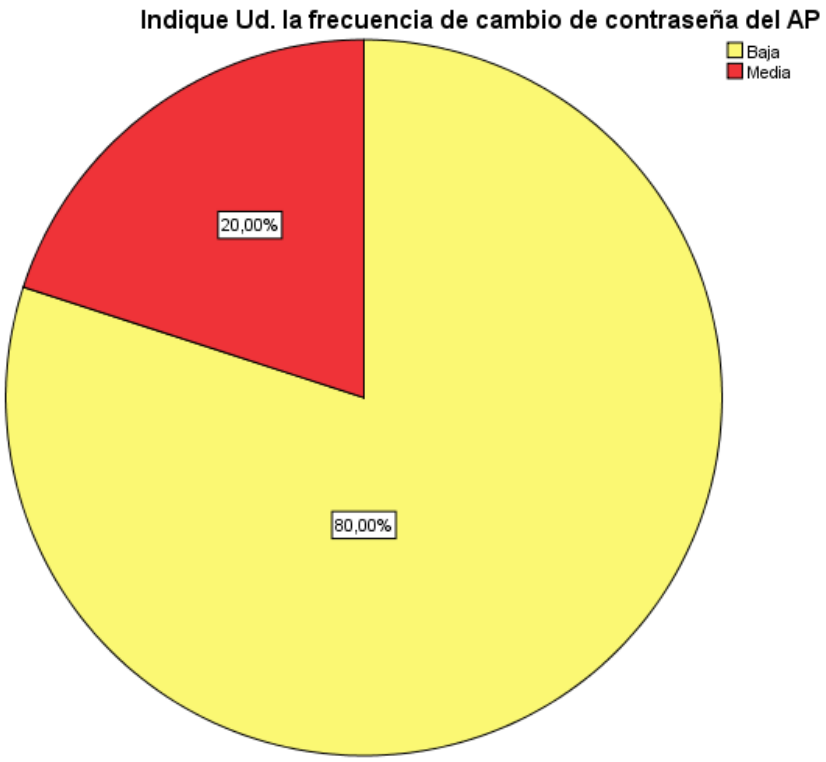


Gráfico # 02 – Resultados de la frecuencia de cambio de contraseña de la WLAN

En el cuadro # 03, se presentan los resultados de la pregunta número 3 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: básica y avanzada. La alternativa básica posee el 100% de las respuestas.

¿En cuanto a los ajustes de configuración del dispositivo AP en qué estado se encuentra?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Básica	5	100,0	100,0	100,0

Cuadro # 03 – Resultados de los ajustes de configuración del AP de la WLAN

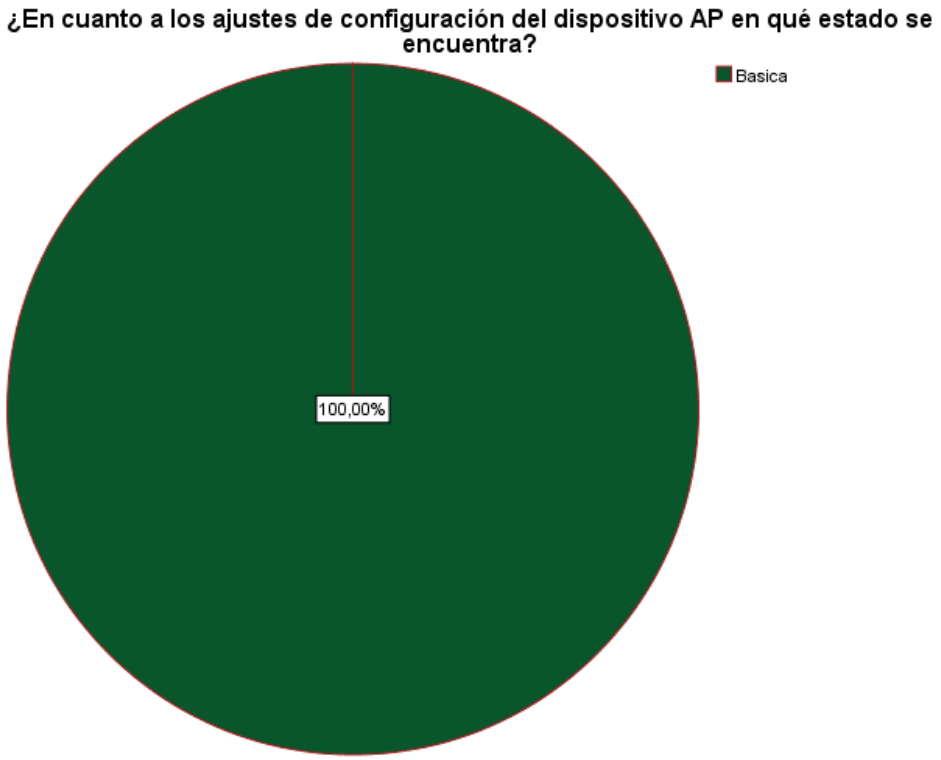


Gráfico # 03 – Resultados de los ajustes de configuración del AP de la WLAN

En el cuadro # 04, se presentan los resultados de la pregunta número 4 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: No realiza, semanal y mensual. La alternativa “No realiza” posee el 80% de las respuestas

¿Cuál es la frecuencia que se realiza para la actualización del firmware del dispositivo AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No realiza	4	80,0	80,0	80,0
	Mensual	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 04 – Resultados de la frecuencia de actualización del firmware del AP de la WLAN

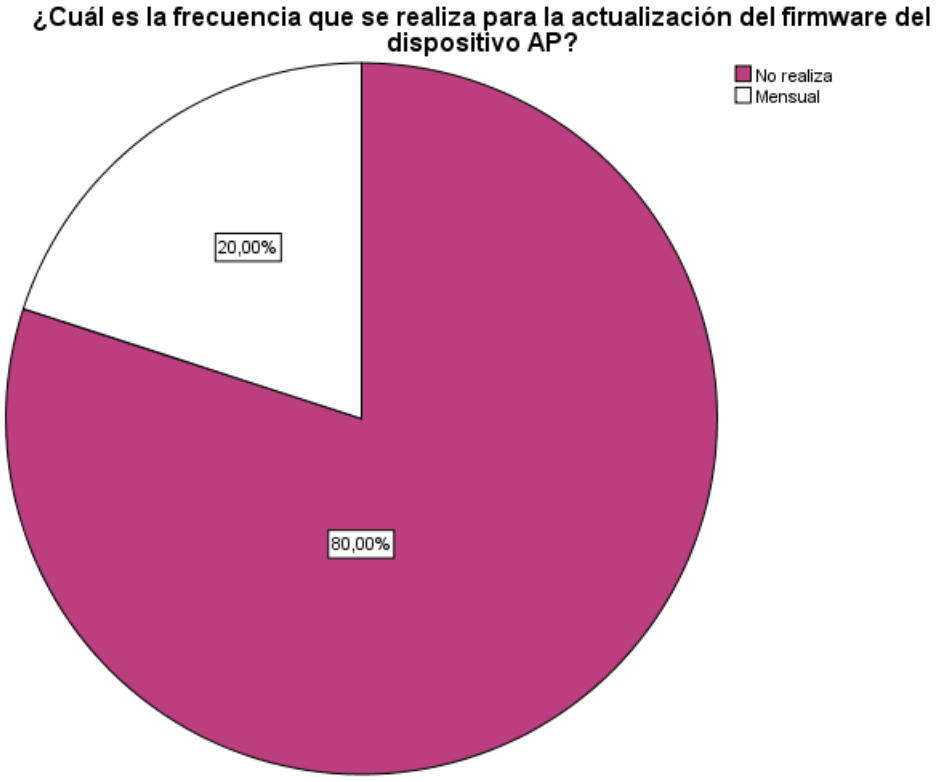


Gráfico # 04 – Resultados de la frecuencia de actualización del firmware del AP de la WLAN

En el cuadro # 05, se presentan los resultados de la pregunta número 5 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 100% de las respuestas.

¿Con respecto a las listas de control de acceso realiza el filtrado de direcciones MAC?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	5	100,0	100,0	100,0

Cuadro # 05 – Resultados del filtrado de direcciones MAC de la WLAN

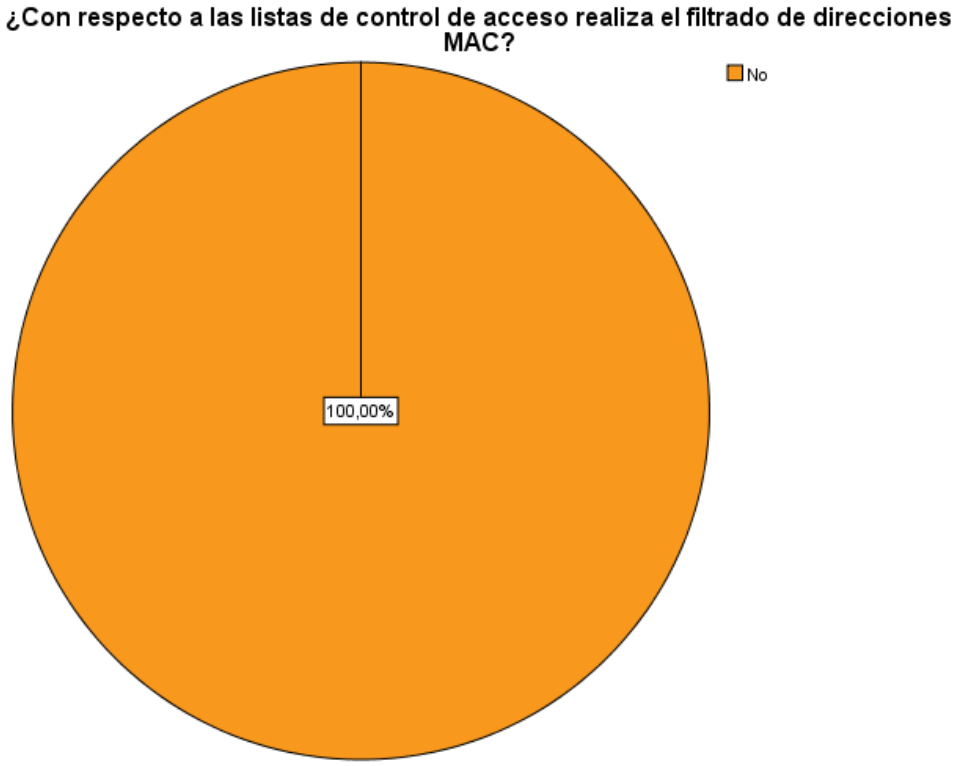


Gráfico # 05 – Resultados del filtrado de direcciones MAC de la WLAN

En el cuadro # 06, se presentan los resultados de la pregunta número 6 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 100% de las respuestas.

¿Realiza la ocultación del nombre de la red (SSID) del dispositivo AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	5	100,0	100,0	100,0

Cuadro # 06 – Resultados la ocultación del SSID del AP de la WLAN

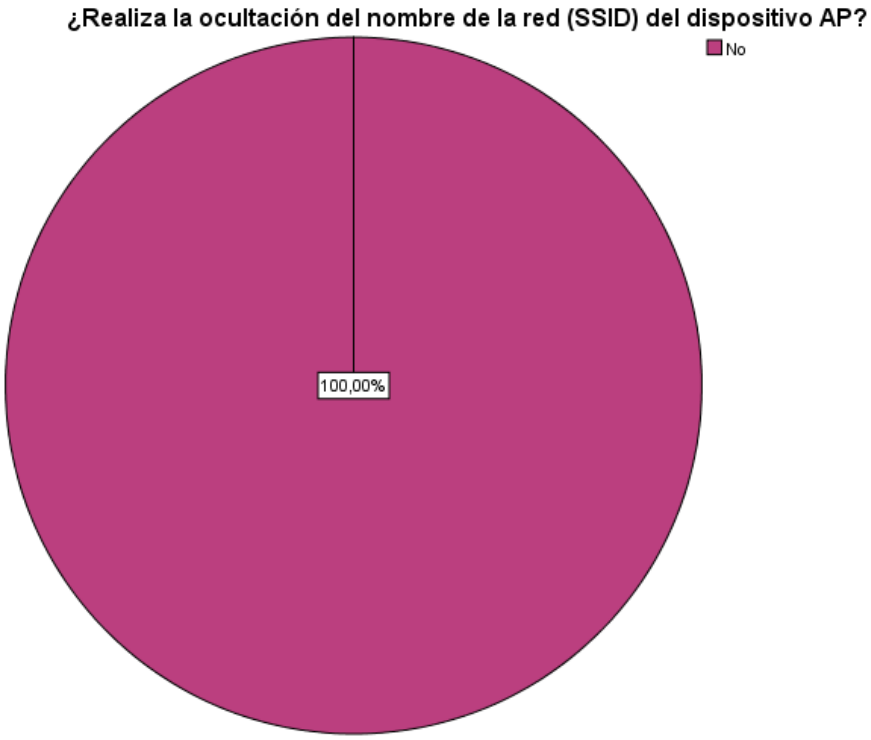


Gráfico # 06 – Resultados la ocultación del SSID del AP de la WLAN

En el cuadro # 07, se presentan los resultados de la pregunta número 7 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 100% de las respuestas.

¿Mantiene el servicio DHCP del dispositivo AP desactivado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	5	100,0	100,0	100,0

Cuadro # 07 – Resultados de la desactivación del servidor DHCP de la WLAN

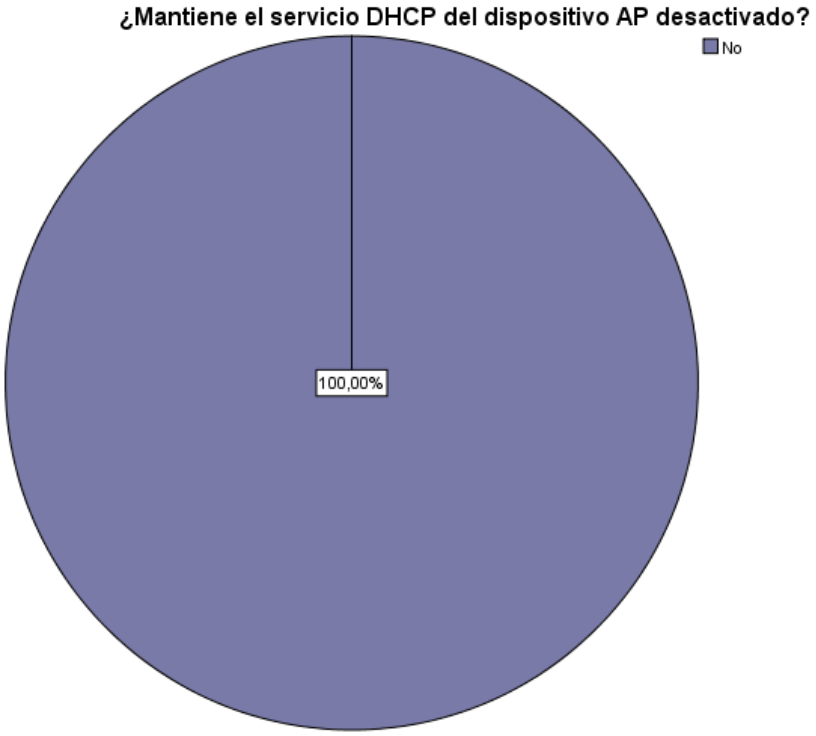


Gráfico # 07 – Resultados de la desactivación del servidor DHCP de la WLAN

En el cuadro # 08, se presentan los resultados de la pregunta número 8 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: básica. media y avanzada. La alternativa “básica” posee el 80% de las respuestas.

¿Qué tipo de contraseñas utiliza para asegurar la red del AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Básica	4	80,0	80,0	80,0
	Media	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 08 – Resultados del tipo de contraseña del AP de la WLAN

Gráfico # 08 – Resultados del tipo de contraseña del AP de la WLAN

En el cuadro # 09, se presentan los resultados de la pregunta número 9 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 100% de las respuestas.

¿Utiliza mecanismo de cifrado con autenticación de usuarios?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	5	100,0	100,0	100,0

Cuadro # 09 – Resultados del mecanismo de cifrado del AP de la WLAN

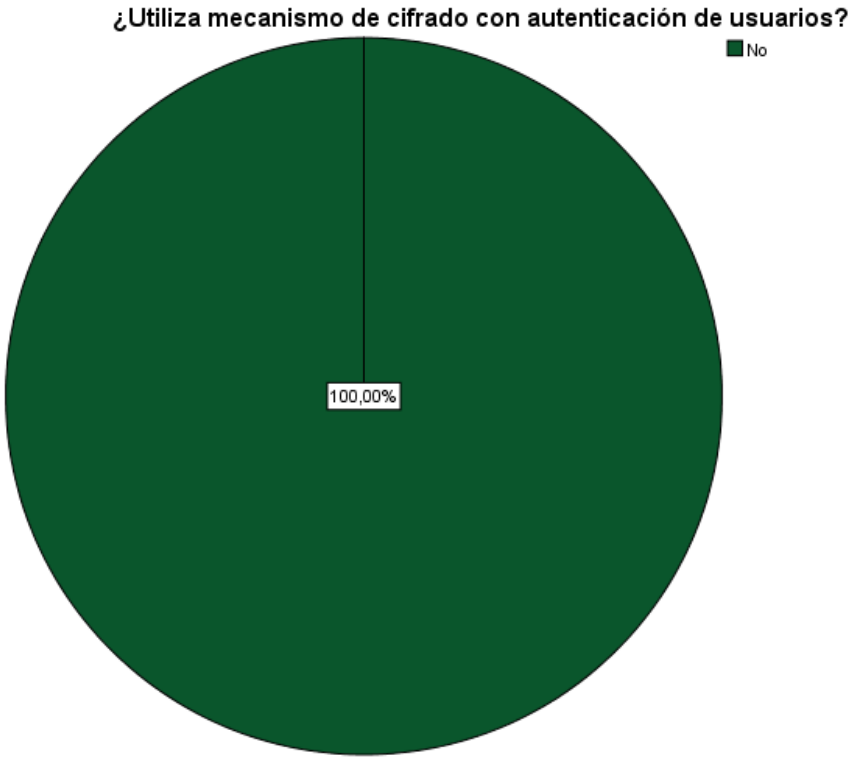


Gráfico # 09 – Resultados del mecanismo de cifrado del AP de la WLAN

En el cuadro # 10, se presentan los resultados de la pregunta número 10 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por los rangos de alternativas: 0-20, 21-40, 41-60 y 60 a más. El rango “21-40” posee el 40% de las respuestas mientras que el rango 41-60 tiene el 60%.

¿Cuál es la cantidad de usuarios conectados no autorizados al AP en un día?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	41-60	1	20,0	20,0	20,0
	21-40	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Cuadro # 10 – Resultados de la cantidad de usuarios conectados a la WLAN

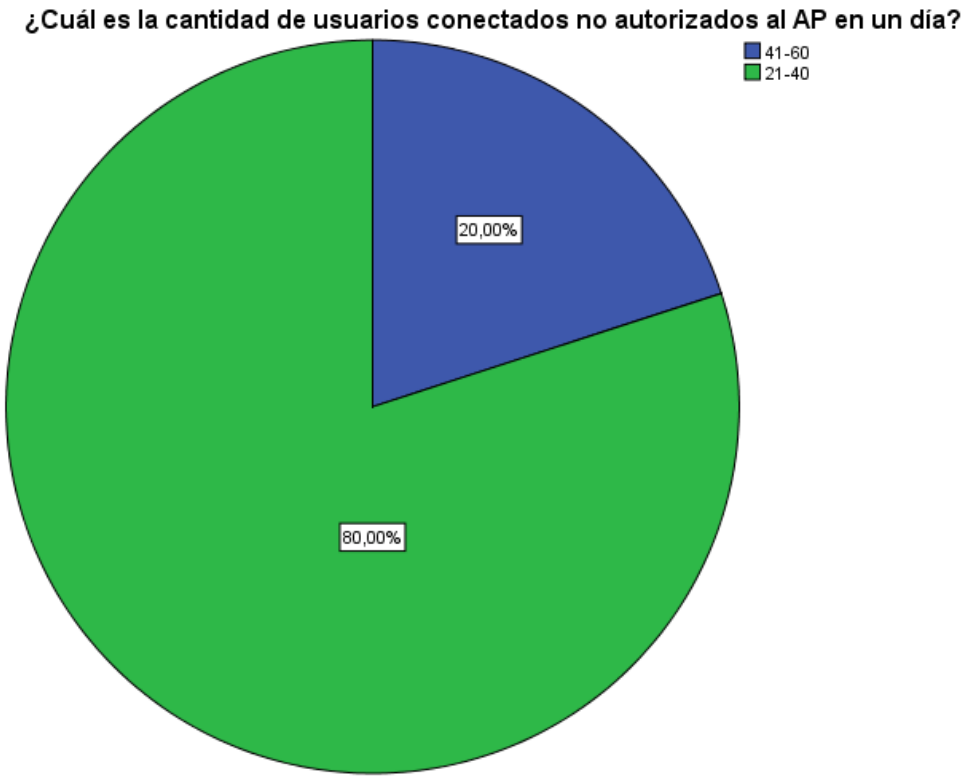


Gráfico # 10 – Resultados de la cantidad de usuarios conectados a la WLAN

POST TEST – OMS

Resultados en cuadros y gráficos estadísticos:

En el cuadro # 11, se presentan los resultados de la pregunta número 1 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: WEP, WPA Y WPA2. La alternativa WPA2 posee el 60% de las respuestas.

¿En cuanto a los protocolos de seguridad cuál de ellos utiliza para el proceso de autenticación en la WLAN?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	WPA	2	40,0	40,0	40,0
	WPA2	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Cuadro # 11 – Resultados del proceso de autenticación de la WLAN

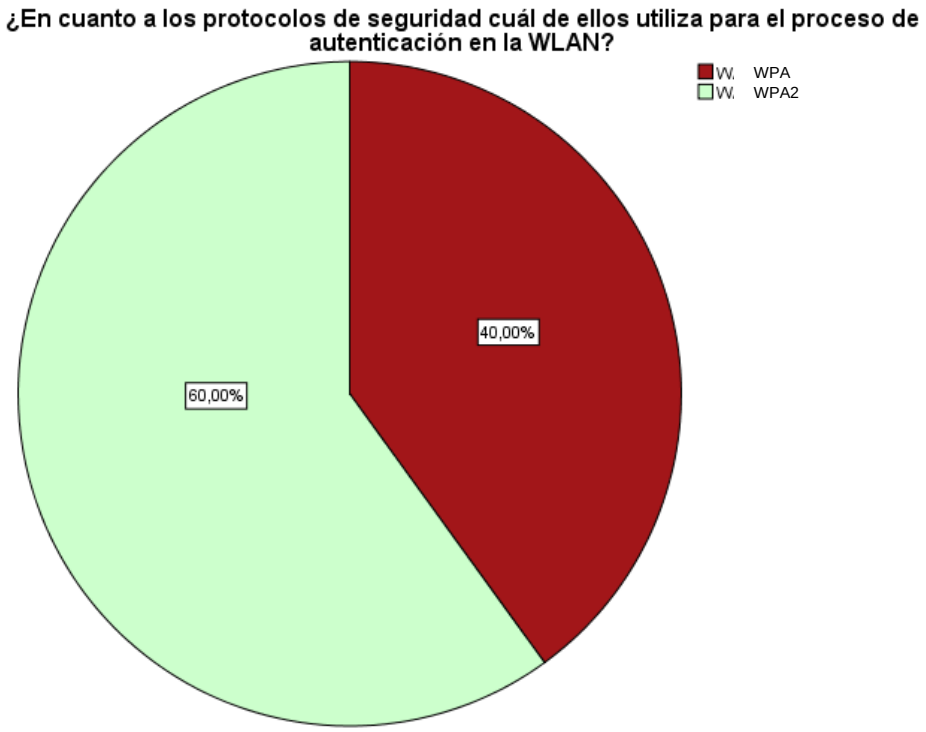


Gráfico # 11 – Resultados del proceso de autenticación de la WLAN

En el cuadro # 12, se presentan los resultados de la pregunta número 2 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: alta, media y baja. La alternativa media posee el 60% de las respuestas.

Indique Ud. la frecuencia de cambio de contraseña del AP

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Media	3	60,0	60,0	60,0
	Alta	2	40,0	40,0	100,0
	Total	5	100,0	100,0	

Cuadro # 12 – Resultados de la frecuencia de cambio de contraseña de la WLAN

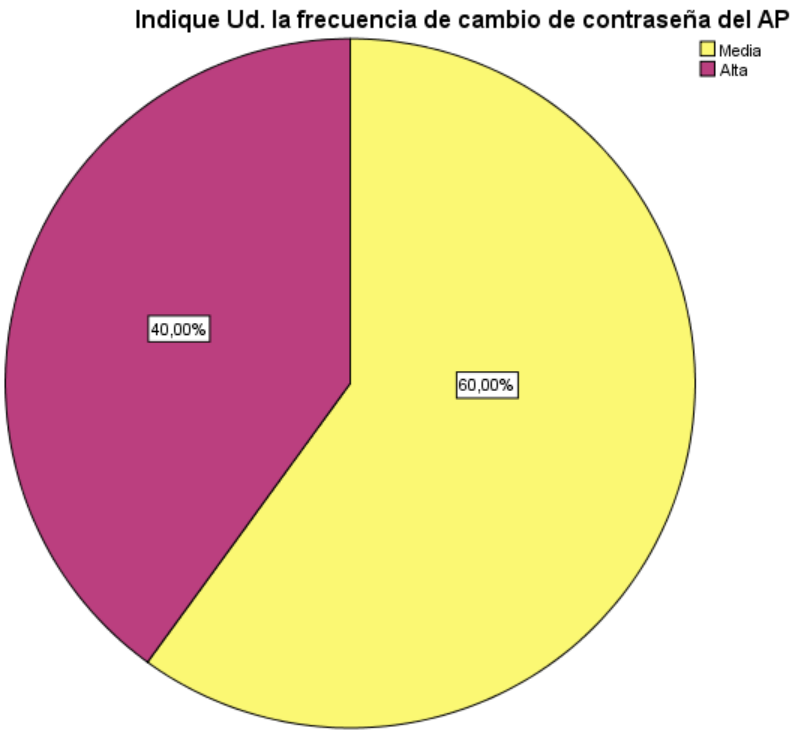


Gráfico # 12 – Resultados de la frecuencia de cambio de contraseña de la WLAN

En el cuadro # 13, se presentan los resultados de la pregunta número 3 del pre test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: básica y avanzada. La alternativa básica posee el 80% de las respuestas.

¿En cuanto a los ajustes de configuración del dispositivo AP en qué estado se encuentra?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Básica	4	80,0	80,0	80,0
	Completa	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 13 – Resultados de los ajustes de configuración del AP de la WLAN

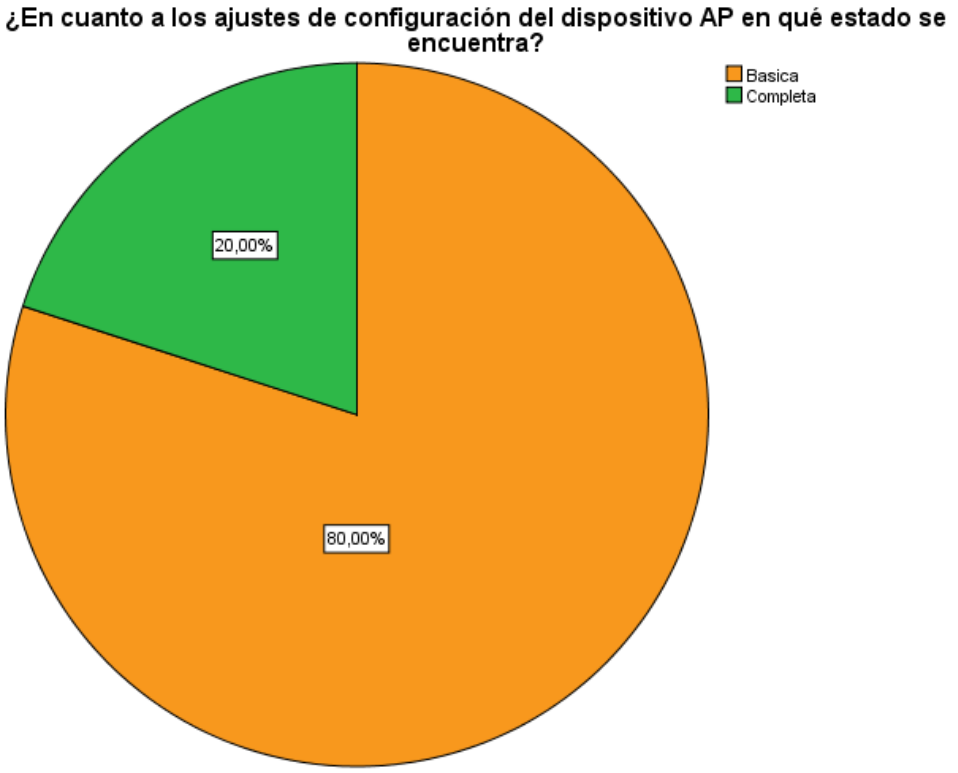


Gráfico # 13 – Resultados de los ajustes de configuración del AP de la WLAN

En el cuadro # 14, se presentan los resultados de la pregunta número 4 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: No realiza, semanal y mensual. La alternativa “Mensual” posee el 60% de las respuestas

¿Cuál es la frecuencia que se realiza para la actualización del firmware del dispositivo AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Mensual	3	60,0	60,0	60,0
	Semanal	2	40,0	40,0	100,0
	Total	5	100,0	100,0	

Cuadro # 14 – Resultados de la frecuencia de actualización del firmware del AP de la WLAN

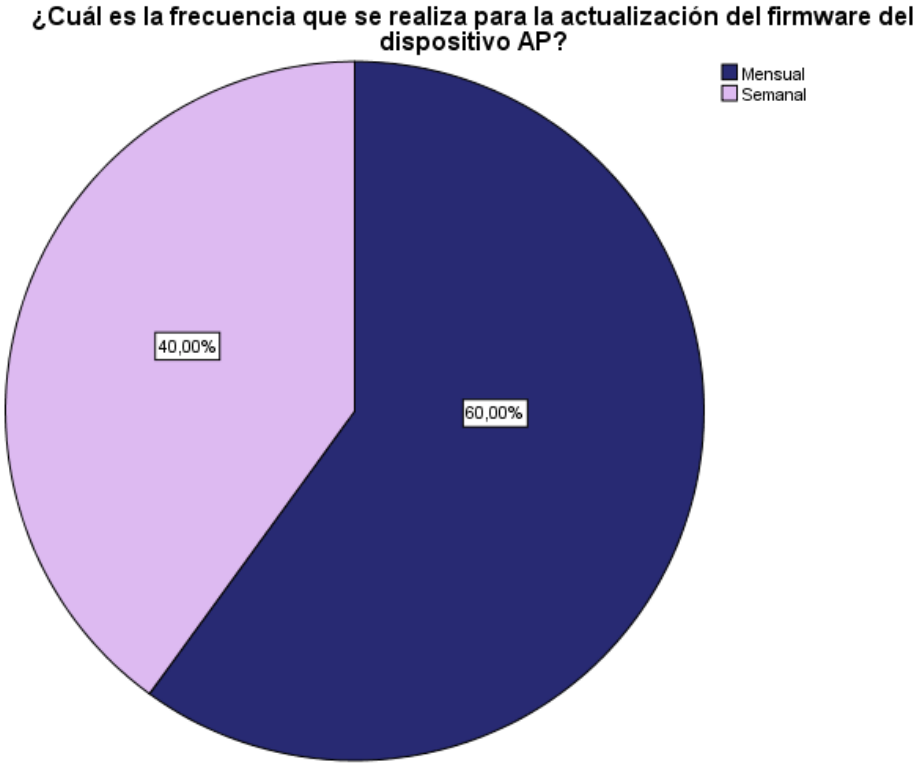


Gráfico # 04 – Resultados de la frecuencia de actualización del firmware del AP de la WLAN

En el cuadro # 15, se presentan los resultados de la pregunta número 5 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 100% de las respuestas.

¿Con respecto a las listas de control de acceso realiza el filtrado de direcciones MAC?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Si	5	100,0	100,0	100,0

Cuadro # 05 – Resultados del filtrado de direcciones MAC de la WLAN

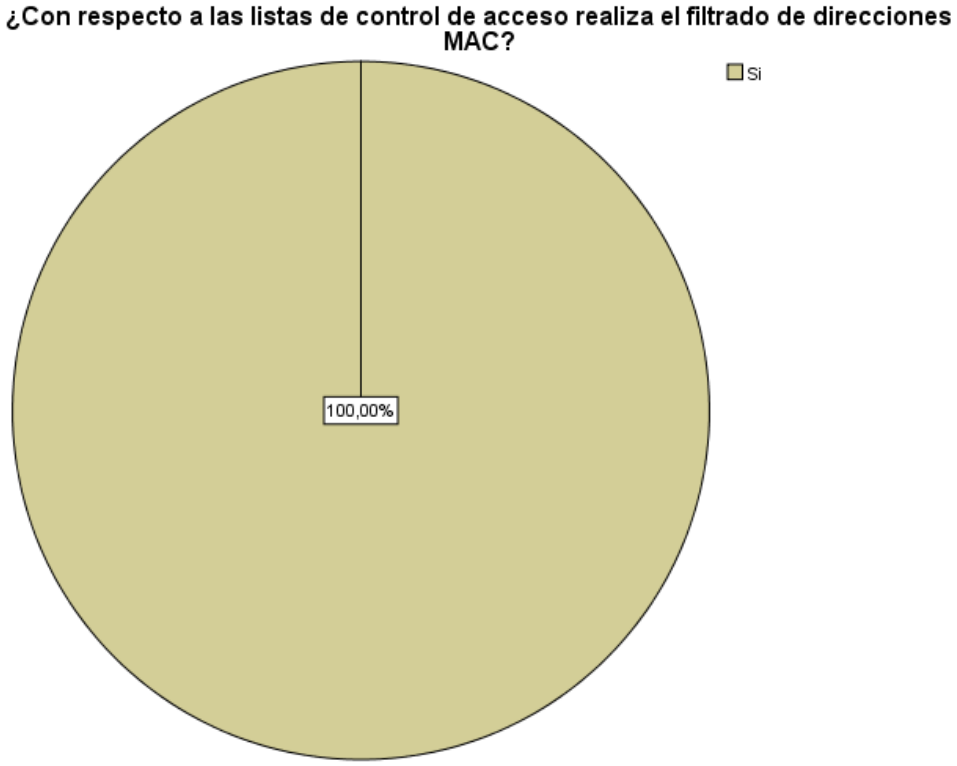


Gráfico # 05 – Resultados del filtrado de direcciones MAC de la WLAN

En el cuadro # 16, se presentan los resultados de la pregunta número 6 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 40% de las respuestas.

¿Realiza la ocultación del nombre de la red (SSID) del dispositivo AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	3	60,0	60,0	60,0
	Si	2	40,0	40,0	100,0
	Total	5	100,0	100,0	

Cuadro # 16 – Resultados la ocultación del SSID del AP de la WLAN

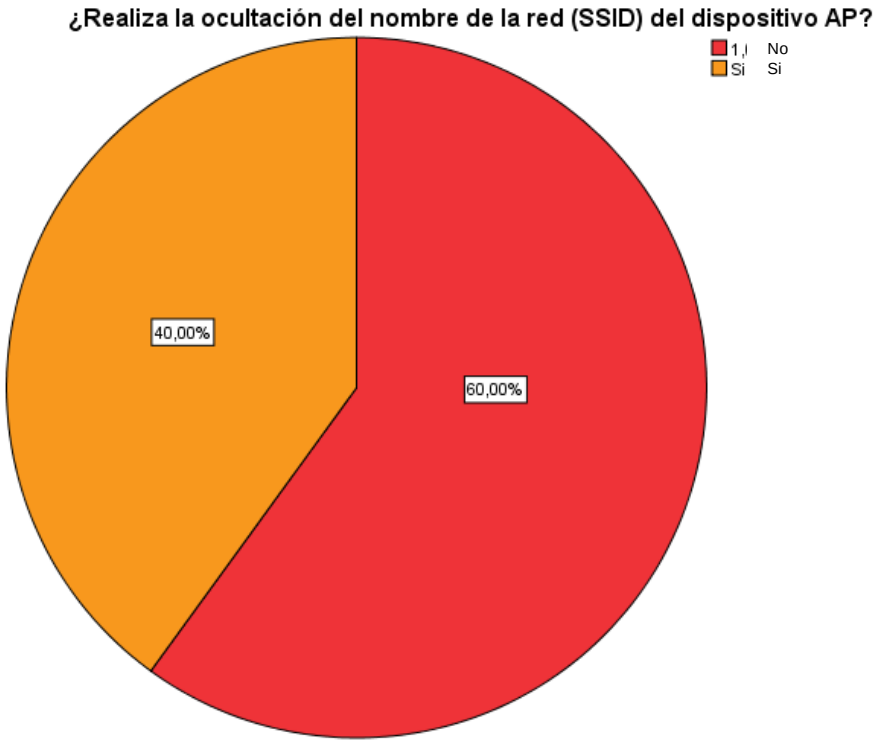


Gráfico # 16 – Resultados la ocultación del SSID del AP de la WLAN

En el cuadro # 17, se presentan los resultados de la pregunta número 7 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “No” posee el 80% de las respuestas.

¿Mantiene el servicio DHCP del dispositivo AP desactivado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 17 – Resultados de la desactivación del servidor DHCP de la WLAN

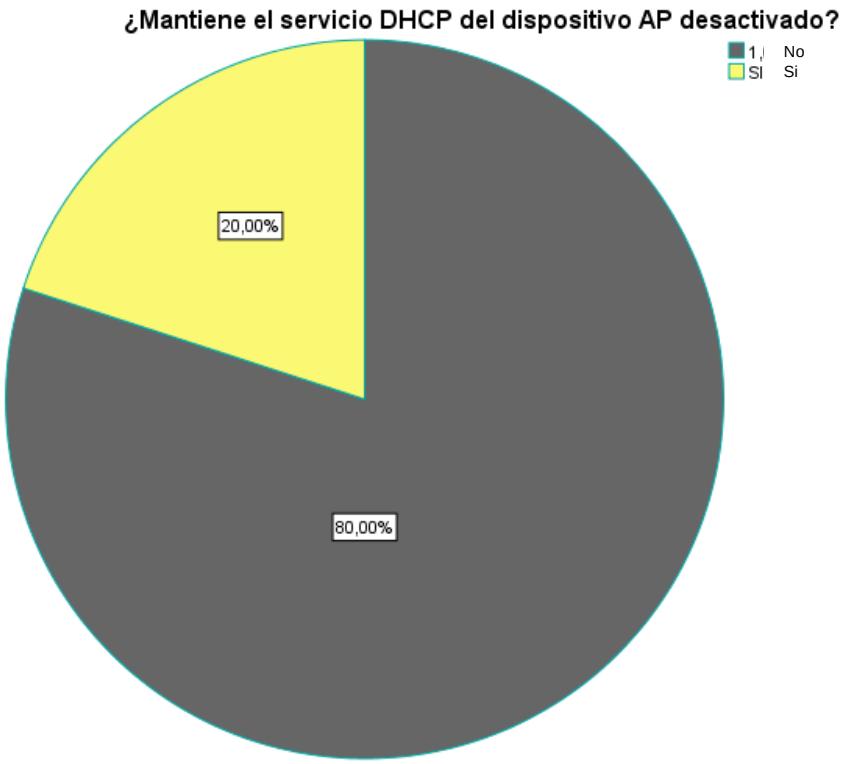


Gráfico # 17 – Resultados de la desactivación del servidor DHCP de la WLAN

En el cuadro # 18, se presentan los resultados de la pregunta número 8 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: básica. media y avanzada. La alternativa “avanzada” posee el 80% de las respuestas mientras que la alternativa media posee el 20%.

¿Qué tipo de contraseñas utiliza para asegurar la red del AP?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Básica	3	60,0	60,0	60,0
	Media	1	20,0	20,0	80,0
	Avanzada	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Cuadro # 18 – Resultados del tipo de contraseña del AP de la WLAN

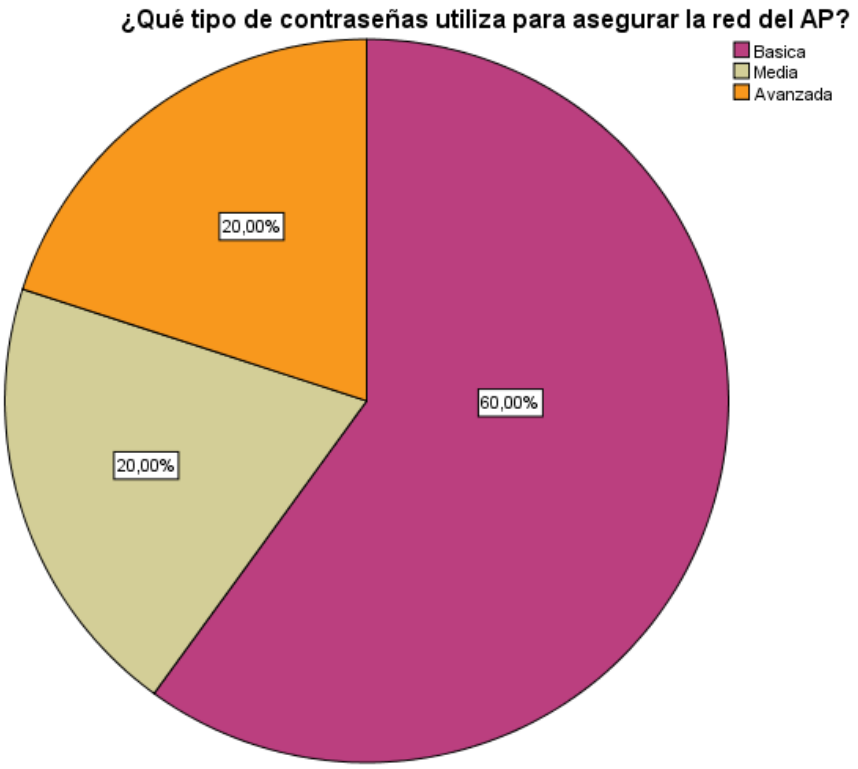


Gráfico # 18 – Resultados del tipo de contraseña del AP de la WLAN

En el cuadro # 19, se presentan los resultados de la pregunta número 9 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por las alternativas: Sí y No. La alternativa “Si” posee el 40% de las respuestas.

¿Utiliza mecanismo de cifrado con autenticación de usuarios?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	No	3	60,0	60,0	60,0
	Si	2	40,0	40,0	100,0
	Total	5	100,0	100,0	

Cuadro # 19 – Resultados del mecanismo de cifrado del AP de la WLAN

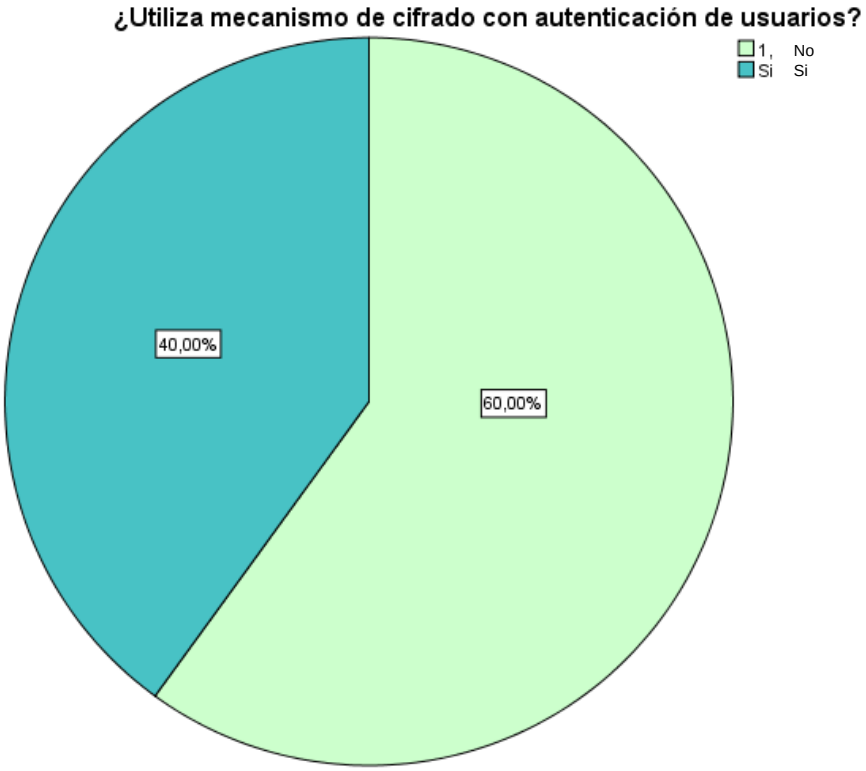


Gráfico # 19 – Resultados del mecanismo de cifrado del AP de la WLAN

En el cuadro # 20, se presentan los resultados de la pregunta número 10 del post test aplicado al personal de la OMS para evaluar el nivel de la seguridad de la WLAN. Está compuesto por los rangos de alternativas: 0-20, 21-40, 41-60 y 60 a más. El rango “0-20” posee el 100% de las respuestas.

¿Cuál es la cantidad de usuarios conectados no autorizados al AP en un día?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	0-20	5	100,0	100,0	100,0

Cuadro # 20 – Resultados de la cantidad de usuarios conectados a la WLAN

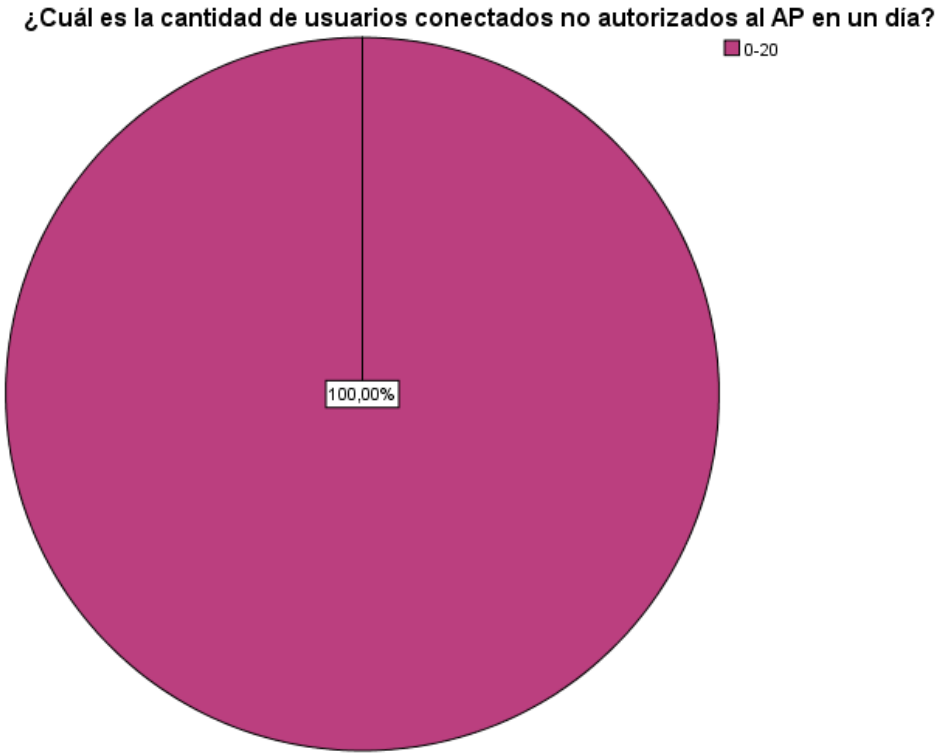


Gráfico # 20 – Resultados de la cantidad de usuarios conectados a la WLAN

4.2 Prueba de hipótesis

Todo contraste de hipótesis se basa en la formulación de dos hipótesis exhaustivas y mutuamente exclusivas. Para la presente investigación las hipótesis quedan definidas de la siguiente manera:

Hipótesis

Existe diferencia significativa en los promedios de calificación antes y después de aplicar la norma IEEE 802.1X para mejorar la seguridad de la red WLAN

Hipótesis nula (H0): No existe diferencias estadísticamente significativas en los promedios de calificación antes y después de la intervención

Hipótesis alternativa (H1): Existe diferencias estadísticamente significativas en los promedios de calificación antes y después de la intervención.

Nivel de confianza: 95%

Por medio del software estadístico SPSS (Statistical Package for the Social Science), en su versión 20 se realizó la inferencia estadística. Es uno de los programas estadísticos más conocidos teniendo en cuenta su capacidad para trabajar con grandes bases de datos y un sencillo interface para la mayoría de los análisis.

Los resultados obtenidos se muestran a continuación:

Estadísticos de muestras relacionadas

	Media	N	Desviación típ.	Error típ. de la media
Pre_Test	9.125	12	1.8844	.5440
Post_Test	16.958	12	1.3049	.3767

Estadísticos descriptivos

	N	Media		Desv. típ.
	Estadístico	Estadístico	Error típico	Estadístico
Puntajes totales del Pre	5	5,7000	,33912	,75829
Puntajes totales del Post	5	19,5000	,22361	,50000
N válido (según lista)	5			

Prueba de muestras relacionadas

	Diferencias relacionadas					t	gl	Sig. (bilateral)
	Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
				Inferior	Superior			
Puntajes totales del Pre - Puntajes totales del Post	-9,00000	1,03682	,00000	-10,00000	-8,00000	-20,000	4	,000

Para realizar la prueba de hipótesis antes se recodifico los valores cualitativos a cuantitativos dándole un valor numérico equivalente, como se observa en la Matriz de puntuación de instrumentos, se utilizará la prueba paramétrica T de Student previo análisis de la distribución normal de los datos:

Prueba de normalidad: Siendo n<30 se escoge Shapiro Wilk

P-Valor (Antes) = 0,07 > α =0.05

P-Valor (Después) = 0,421 > α =0.05

Conclusión:

Los datos provienen de una distribución normal

La fórmula de la prueba T de student para muestras relacionadas, se muestra a continuación:

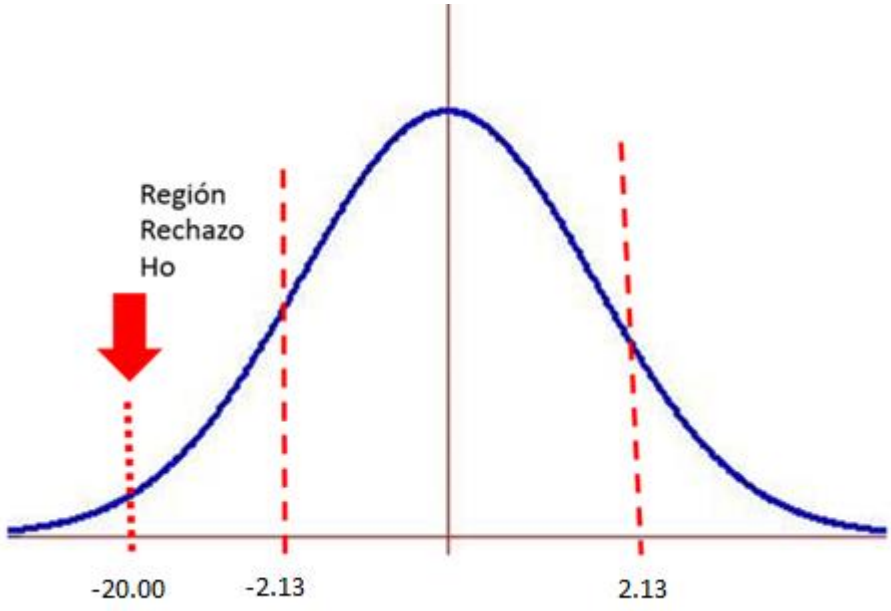
$$t_0 = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{s^2 \times \left[\frac{1}{n_1} + \frac{1}{n_2}\right]}}$$

Una vez que se obtiene el valor de T_0, se procede a evaluarlo con el valor procedente de la tabla t de student según los grados de libertad.

Grados de libertad	0.25	0.1	0.05	0.025	0.01	0.005
1	1.0000	3.0777	6.3137	12.7062	31.8210	63.6559
2	0.8165	1.8856	2.9200	4.3027	6.9645	9.9250
3	0.7649	1.6377	2.3534	3.1824	4.5407	5.8408
4	0.7407	1.5332	2.1318	2.7765	3.7469	4.6041
5	0.7267	1.4759	2.0150	2.5706	3.3649	4.0321
6	0.7176	1.4398	1.9432	2.4469	3.1427	3.7074
7	0.7111	1.4149	1.8946	2.3646	2.9979	3.4995
8	0.7064	1.3968	1.8595	2.3060	2.8965	3.3554
9	0.7027	1.3830	1.8331	2.2622	2.8214	3.2498
10	0.6998	1.3722	1.8125	2.2281	2.7638	3.1693
11	0.6974	1.3634	1.7959	2.2010	2.7181	3.1058
12	0.6955	1.3562	1.7823	2.1788	2.6810	3.0545
13	0.6938	1.3502	1.7709	2.1604	2.6503	3.0123
14	0.6924	1.3450	1.7613	2.1448	2.6245	2.9768
15	0.6912	1.3406	1.7531	2.1315	2.6025	2.9467
16	0.6901	1.3368	1.7459	2.1199	2.5835	2.9208
17	0.6892	1.3334	1.7396	2.1098	2.5669	2.8982
18	0.6884	1.3304	1.7341	2.1009	2.5524	2.8784
19	0.6876	1.3277	1.7291	2.0930	2.5395	2.8609
20	0.6870	1.3253	1.7247	2.0860	2.5280	2.8453

g.l. = n – 1 = g.l = (5) – 1 = 4, Grados de libertad, a un nivel de significancia del 0.05, es igual a 2.13.

A continuación, se procede a realizar el contraste según la campana de gauss:



A raíz de que el valor calculado de la ecuación es de -20.00, este se encuentra más a la derecha del valor de la tabla (-2.13). Por lo que se sostiene que se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Sí existen diferencias de medias. El resultado de la Prueba T de Student, se simplifica en la sigma bilateral, para posteriormente, realizar la contrastación respectiva con el nivel de significancia de la investigación (95% = 0.05). La sigma bilateral es de 0.00. Por lo tanto, al ser la sigma bilateral de la prueba, inferior al nivel de significancia, se sostiene que se rechaza la hipótesis nula y se acepta la hipótesis de investigación.

Por lo tanto, existe diferencia entre las medias del pre y post test. Por lo existe una mejora significante en la seguridad de la wlan de la empresa SEDA Huánuco.

CAPÍTULO V: DISCUSIÓN DE RESULTADOS

Esta investigación tuvo como propósito de mejoras la seguridad de la red inalámbrica de la empresa SEDA Huánuco, a continuación, iremos mostrando los apartados específicos de cada discusión:

En cuanto a la mejora del proceso de autenticación de la red se ha mejorado ya que se vienen usando los protocolos actuales como WPA y WPA2, también podemos afirmar que la frecuencia del cambio de contraseñas ha aumentado de baja a media en un 60%, así mismo se pudo incrementar el nivel de configuración del punto de acceso.

Con respecto a la actualización del software del equipo se pudo observar que la frecuencia de actualización cambia drásticamente de casi nunca a semana y mensual en un 40% y 60% respectivamente, en relación al filtrado de direcciones MAC, tanto en el pre como en el post test, este proceso siempre se ha venido realizando en un 100% ya que la política de la empresa es que solo puedan acceder equipos que hayan sido identificados previamente por su dirección física, también se realiza la ocultación del SSID para que solo aquellos usuarios con conocimiento del nombre de la red puedan conectarse, se procedió así mismo a mejorar la calidad de las contraseñas, y finalmente se determinó una disminución de usuarios no autorizados conectados a la red.

Hasta este punto podemos decir que si existe diferencias estadísticamente significativas entre los puntajes promedios de la mejora de la seguridad de la WLAN ya que en la prueba de hipótesis tenemos un nivel de significancia del 0.05, por lo que se sostiene que se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Sí existen diferencias de medias. El resultado de la Prueba T de Student, se simplifica en el sigma bilateral, para posteriormente, realizar la contrastación respectiva con el nivel de significancia de la investigación (95% = 0.05). El sigma bilateral es de 0.00. Por lo tanto, al ser el sigma bilateral de la prueba, inferior al nivel de significancia, se sostiene que se rechaza la hipótesis nula y se acepta la hipótesis de investigación.

Por lo tanto, existe diferencia entre las medias del pre y post test. En consecuencia, una mejora significante en la mejora de la seguridad de la WLAN, de la empresa SEDA Huánuco.

CONCLUSIONES

De los resultados obtenidos se detallan las conclusiones como producto de la implementación de la norma 802.1x para la mejora de la seguridad de la WLAN**:**

1. Se Implemento la norma IEEE 802.1X mediante el uso de un servidor Radius en el área de Organización de Métodos y de Sistemas y en consecuencia se mejoró la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.

2. La Implementación del Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejoro notablemente la Autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A. ya que actualmente los usuarios deben registrarse en el área y se les asigna un nombre de usuario y su contraseña para que posteriormente puedan ingresar a la red inalámbrica de la empresa.

3. La Implementación del Servidor bajo el protocolo RADIUS conjuntamente con el cifrado TPK/AES mejoro notablemente la Autorización de la WLAN de la Empresa SEDA HUÁNUCO S.A. esto se debe a que el servidor controla los tiempos de acceso, las direcciones físicas y lógicas de los clientes, últimos accesos, tiempos de acceso e incluso horarios a los que se pueden acceder. De esta forma se ha disminuido la cantidad de accesos no autorizados a la red, por ende, se ha optimizando el flujo de comunicación de la red. Así mismo se ha podido concientizar al personal de la oficina OMS para que tomen en cuenta y aplique los mecanismos de seguridad para proteger la WLAN de ataques internos y externos.

RECOMENDACIONES

1. Se debe contar con una política de seguridad en el cual estipule la frecuencia del actualización y mantenimiento del servidor Radius, ya que su funcionalidad y aseguramiento de la red también dependerá de las actualizaciones realizadas en el servidor.

2. Los trabadores de la OMS deben organizar capacitaciones graduales para los trabajadores de las demás áreas y concientizar sobre el uso de la red inalámbrica y el uso exclusivo de sus credenciales, para que no puedan ser usados por otras personas.

3. Se recomienda a los trabajadores del área de la OMS también realizar un seguimiento del funcionamiento del servidor de seguridad y realizar una bitácora en el cual se anoten las incidencias relacionadas en cuanto al acceso y autorización de la red para futuras soluciones en cuanto al tema de la seguridad de la WLAN.

REFERENCIAS BIBLIOGRÁFICAS

García, E. C. (2012). *Implementación de un servidor Radius.* Mexico.

Hernan, L. I. (2007). *Diseño de una red local inalámbrica utilizando un sistema de seguridad basado en los protocolos WPA Y 802.1X para un complejo hotelero.* Lima.

INTECO. (2012). *Riegos de las Redes Inalámbricas.* España.

Leon, G. M. (2012). *Buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo.* Chiclayo.

López, J. H. (2012). *Implementación de un portal cautivo para la autenticación de usuarios en redes usando herramientas de software libre.* México.

Martínez, D. R. (2005). *Comunicaciones en redes WLAN: WiFi, VoIP, Multimedia, Seguridad.* Creaciones Copyright.

Millahual, C. A. (2012). *Redes Wi-Fi en entornos Windows.* Buenos Aires: Fox andina.

Mori, A. L. (2008). *Diseño e implementación de un sistema de gestión de accesos a una red wi-fi utilizando software libre.* Lima.

Pellejero, I. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica.* Marcombo.

Rodríguez, D. L. (2001). *Sistemas inalámbricos de comunicaciones personales.* Marcombo.

Stallings, W. (2004). *Comunicaciones y Redes de computadoras.* Madrid: Pearson Educación.

Tanenbaum, A. S. (2003). *Redes de computadoras.* Mexico: Pearson Educación.

Tapia, A. M. (2012). *Implementación de un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del colegio San Luis Gonzaga a través de una autenticación de los usuarios mediante un servicio aaa implementado en un servidor.* Quito.

ANEXOS

ANEXO1: MATRIZ DE CONSISTENCIA

IMPLEMENTACIÓN DE LA NORMA IEEE 802.1X PARA LA MEJORA EN LA SEGURIDAD DE LA RED WLAN DE LA EMPRESA SEDA HUÁNUCO S.A

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
Problema General ¿De qué manera la implementación de la norma IEEE 802.1X mejorará la seguridad de la WLAN de la Empresa SEDA HUÁNUCO S.A.?	**Objetivo General** Implementar la norma IEEE 802.1X para mejorar la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.	**Hipótesis General** La implementación de la norma IEEE 802.1X mejora la seguridad de la red WLAN de la Empresa SEDA HUÁNUCO S.A.	**Dependiente** Seguridad de la red WLAN	***Seguridad de nivel lógico***	• Ocultación del SSID • Filtrado de MAC • DHCP desactivado • Autenticación • Robustez de contraseña • Cifrado • Actualización de Firmware	**Enfoque:** Cuantitativo **Tipo:** Aplicativo **Diseño:** Pre-Experimental
Problema Específico **P.E 01:** ¿Cuál es la situación actual de la red WLAN de la empresa SEDA HUÁNUCO S.A.? **P.E 02:** ¿De qué manera la implementación del protocolo RADIUS mejorará la autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A.?	**Objetivos Específico** **O.E.1:** Diagnosticar la situación actual de la seguridad de la red WLAN de la empresa SEDA HUÁNUCO S.A. **O.E.2:** Implementar el protocolo RADIUS conjuntamente con el cifrado TPK/AES para mejorar la autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A	**Hipótesis Especifica** **H1:** La situación actual de la seguridad de la red WLAN de la empresa SEDA HUÁNUCO S.A. de la ciudad de Huánuco es vulnerable y deficiente. **H2:** La implementación del protocolo RADIUS mejora la autenticación de la WLAN de la Empresa SEDA HUÁNUCO S.A.	**Independiente** Norma IEEE 802.1X	***Protocolo Radius.***	• Autenticación • Autorización • Anotación	**Esquema del Diseño:** G: O1 X O2 •Donde: G= Grupo de investigación (Trabajadores del área de Sistemas) X= Aplicación de la variable O1, O2, = Medición de Observación

ANEXO 02:

Cuestionario de Evaluación de la implementación de la norma IEEE 802.1X

1. ¿En cuanto a los protocolos de seguridad cuál de ellos utiliza para el proceso de autenticación en la WLAN?
   - ☐ WEP
   - ☐ WPA
   - ☐ WPA2

2. Indique Ud. la frecuencia de cambio de contraseña del AP
   - ☐ Alta
   - ☐ Media
   - ☐ Baja

3. ¿En cuanto a los ajustes de configuración del dispositivo AP en qué estado se encuentra?
   - ☐ Ajustada básicamente
   - ☐ Ajustada completamente

4. ¿Cuál es la frecuencia que se realiza para la actualización del firmware del dispositivo AP?
   - ☐ Mensual
   - ☐ Semanal
   - ☐ No se realiza

5. ¿Realiza la ocultación del nombre de la red (SSID) del dispositivo AP?
   - ☐ Si
   - ☐ No

6. ¿Con respecto a las listas de control de acceso realiza el filtrado de direcciones MAC?
   - ☐ Si
   - ☐ No

7. ¿Mantiene el servicio DHCP del dispositivo AP desactivado?

   ☐ Si

   ☐ No

8. ¿Qué tipo de contraseñas utiliza para asegurar la red del AP?

   ☐ Básica

   ☐ Media

   ☐ Avanzada

9. ¿Utiliza mecanismo de cifrado con autenticación de usuarios?

   ☐ Si

   ☐ No

10. ¿Cuál es la cantidad de usuarios conectados no autorizados al AP en un día?

    ☐ 0 – 20

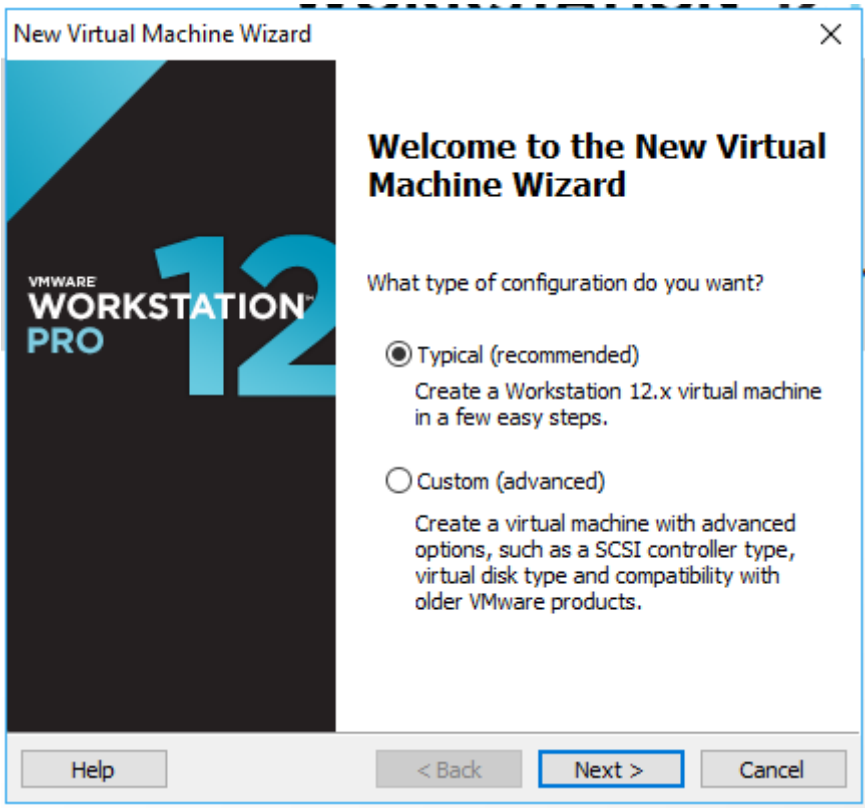
    ☐ 21 – 40

    ☐ 41 – 60

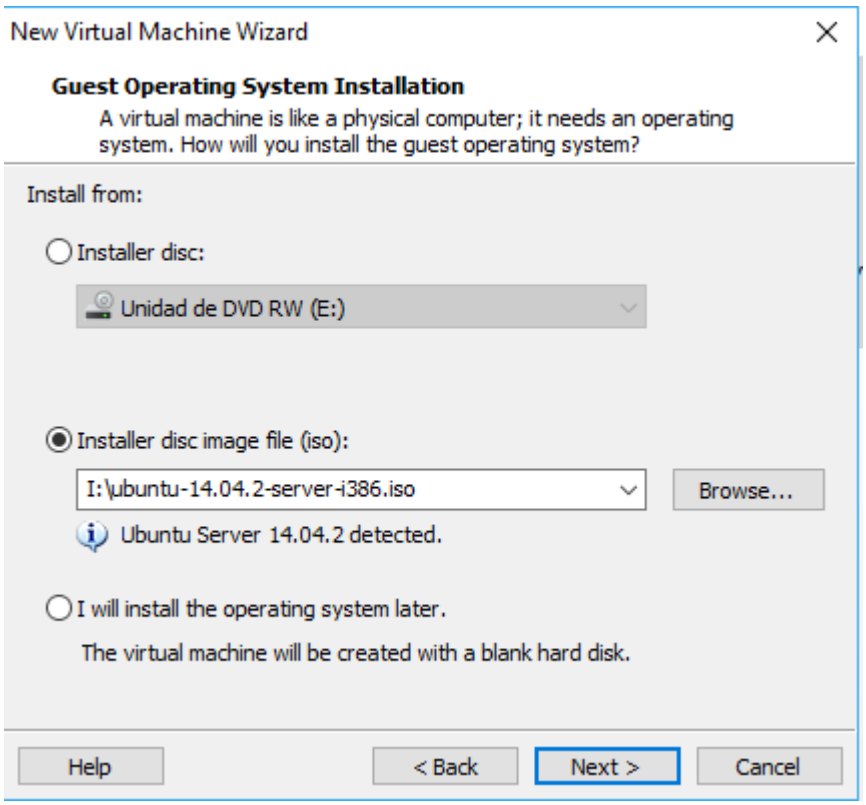
    ☐ 60 a mas

ANEXO 03: DESARROLLO DE LA PARTE APLICATIVA

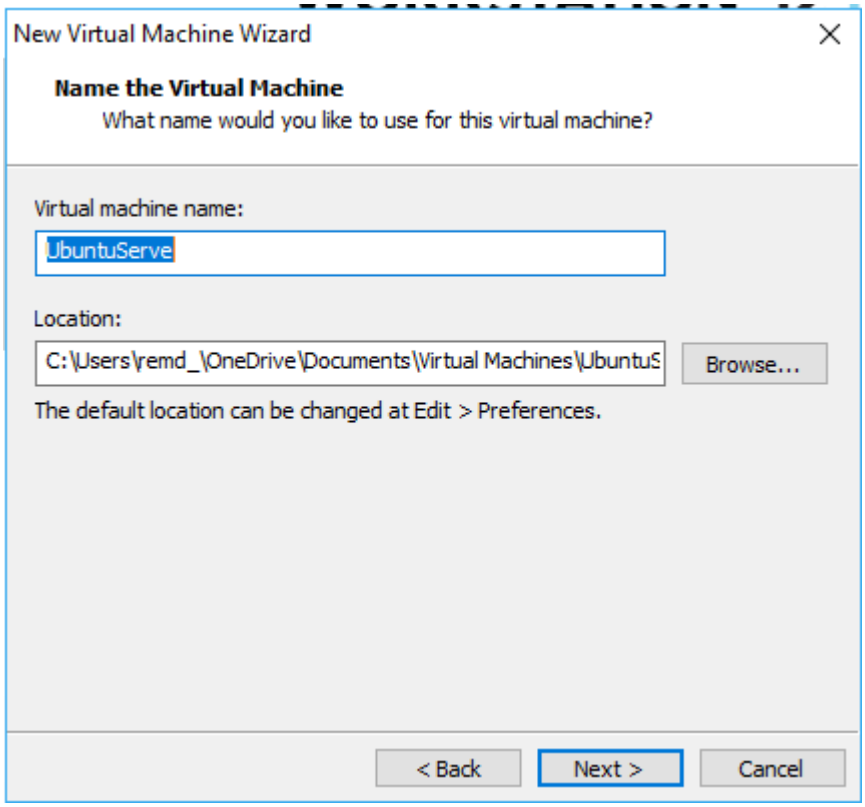
Instalación de la Maquina virtual



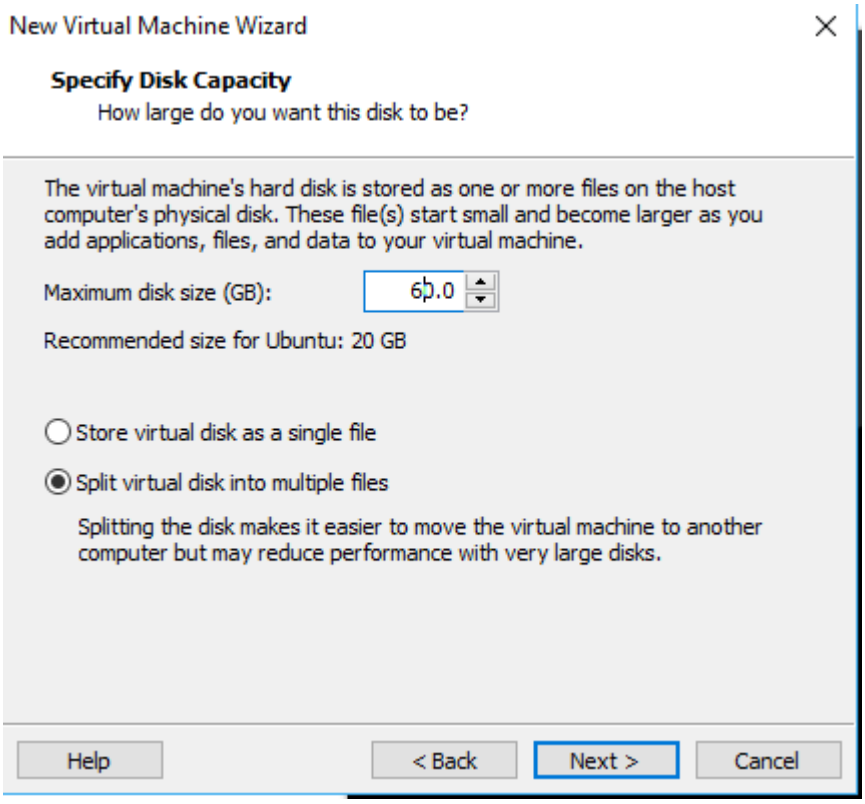
Escogemos la ISO. Damos a siguiente.



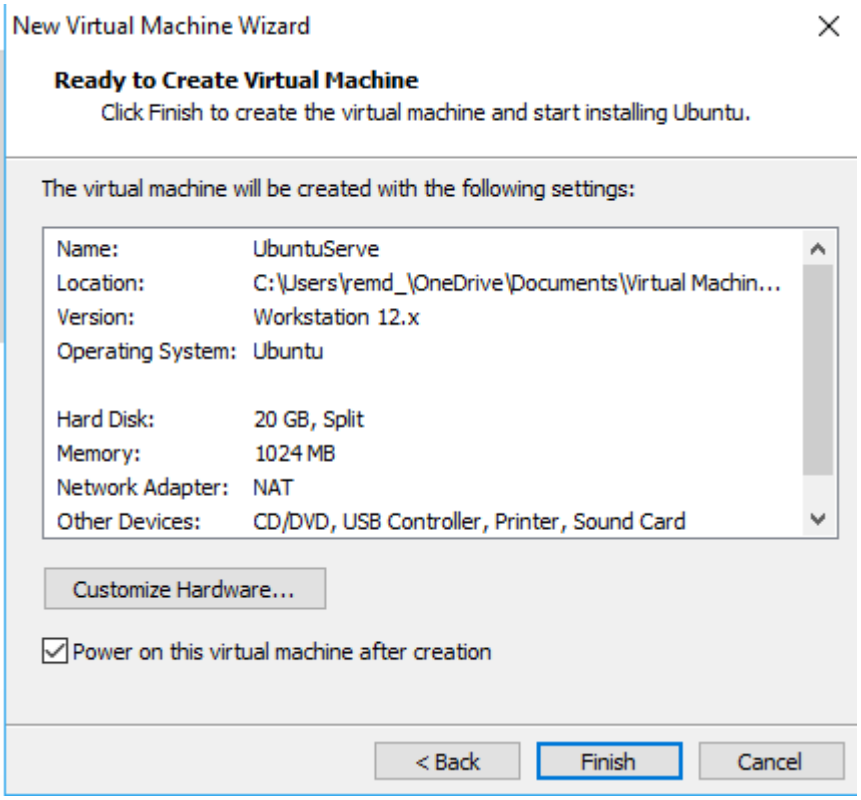
Ponemos un nombre a la máquina virtual



Damos clic en siguiente



Damos clic en finish para terminar de crear la máquina virtual

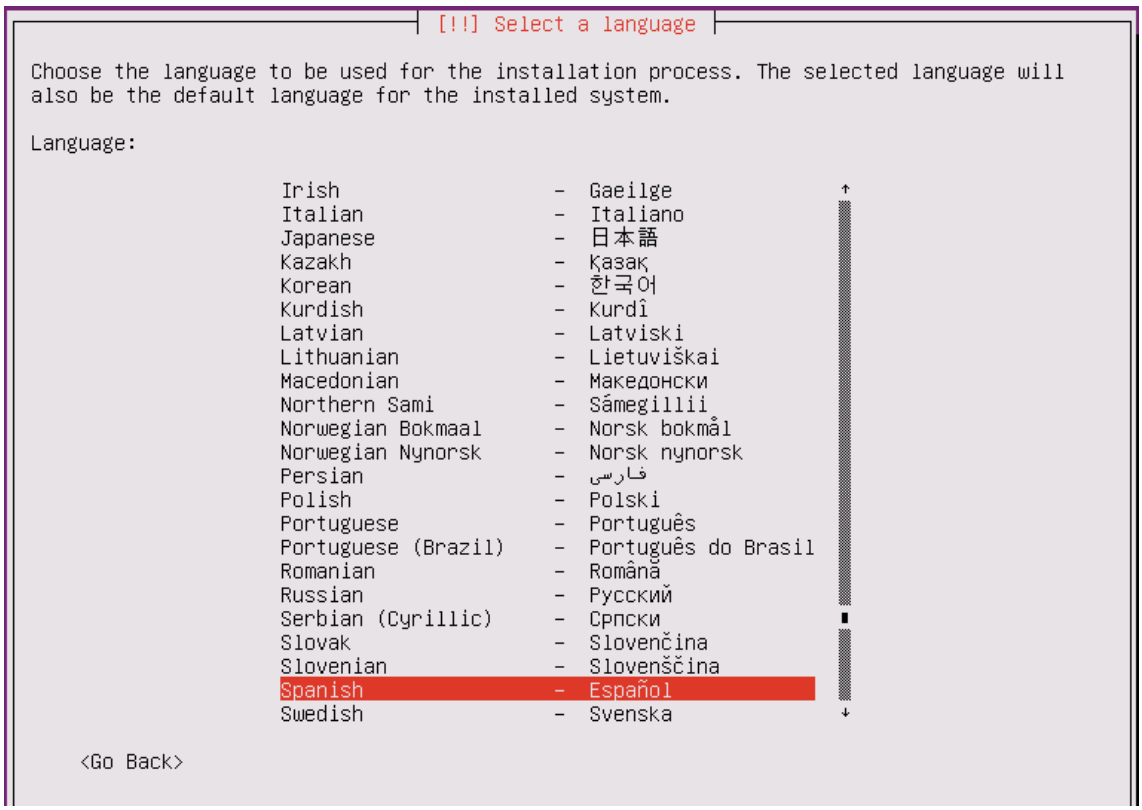


Instalación de Ubuntu Serve 14

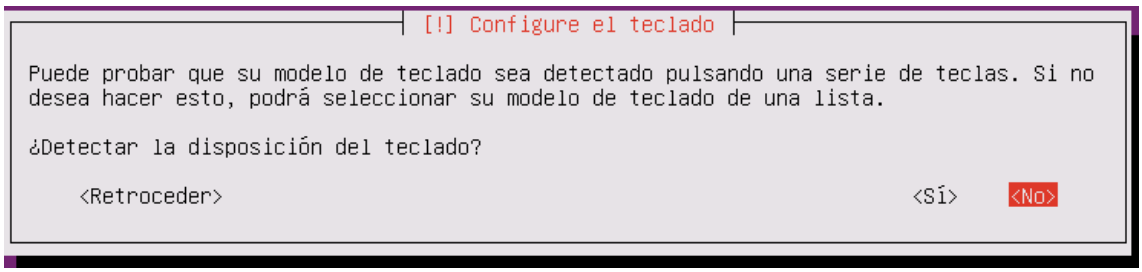
Escogemos el idioma

Escogemos instalar Ubuntu Server

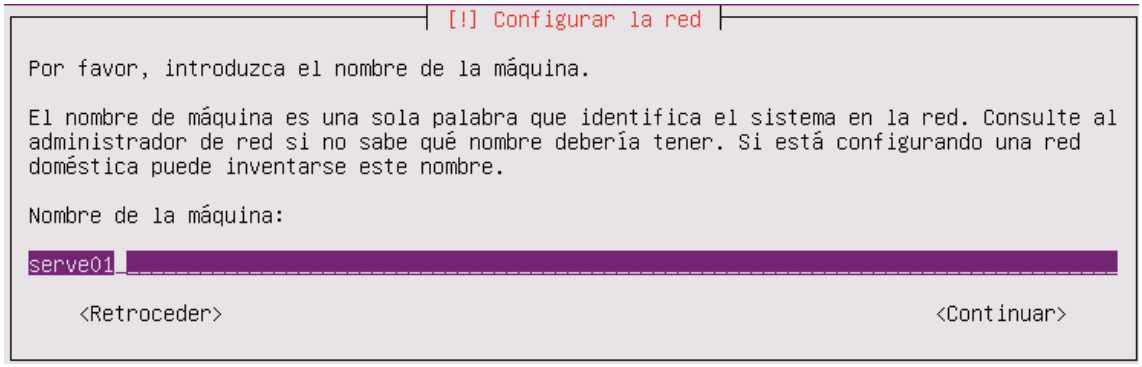
Seleccionamos el lenguaje



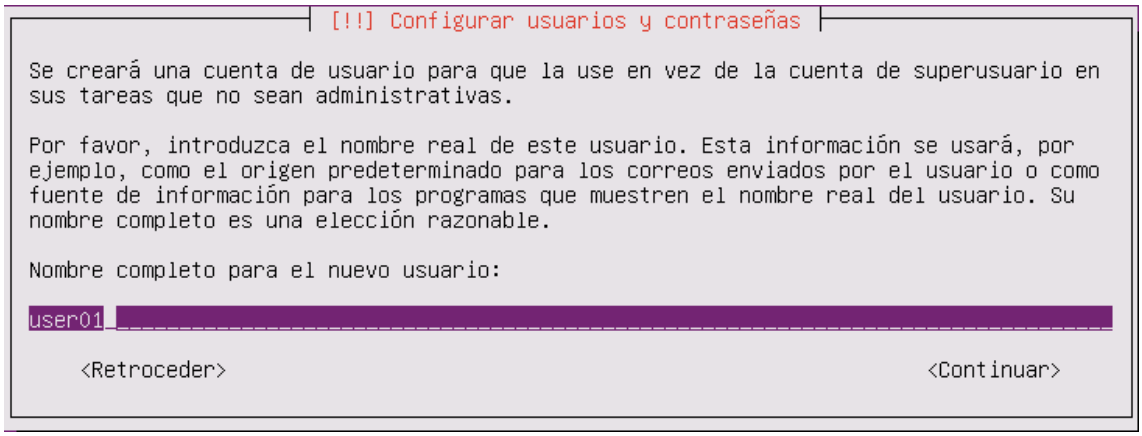
Debemos probar la configuración del teclado le damos que si



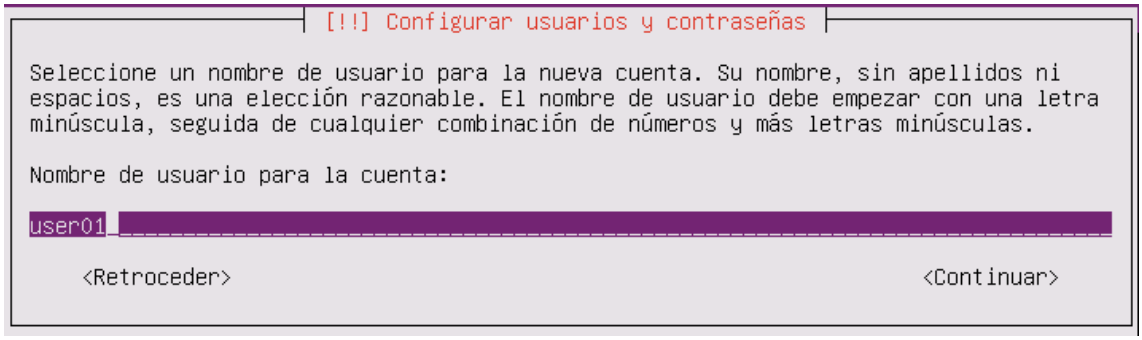
Ponemos el nombre de la máquina virtual



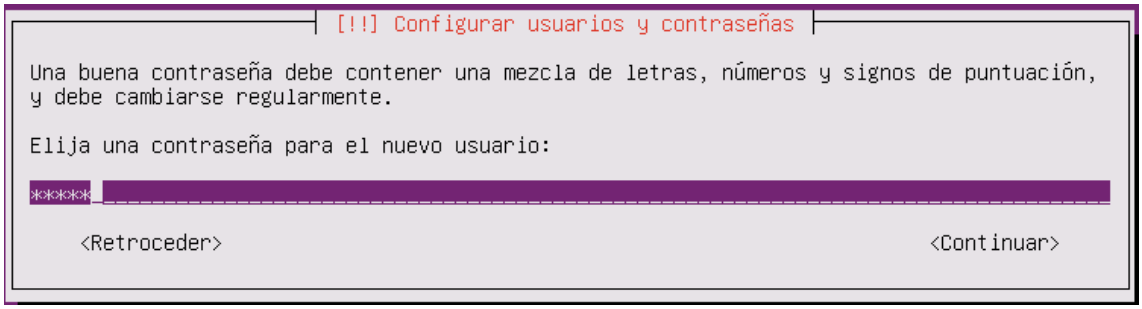
Ponemos el nombre del usuario



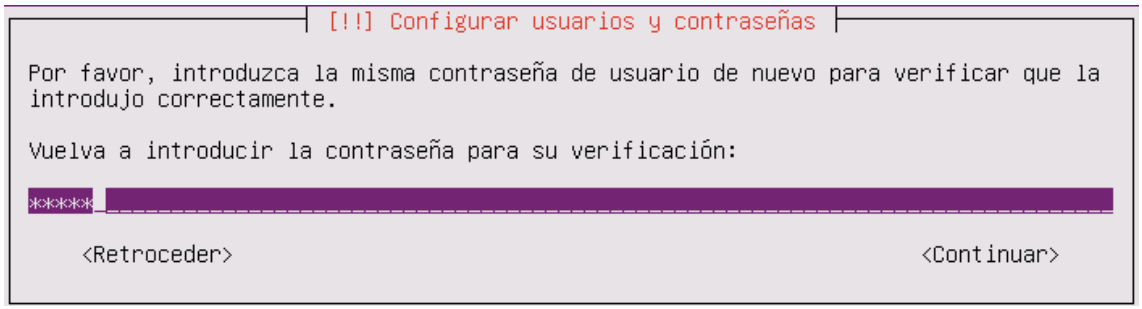
Lo dejamos como esta



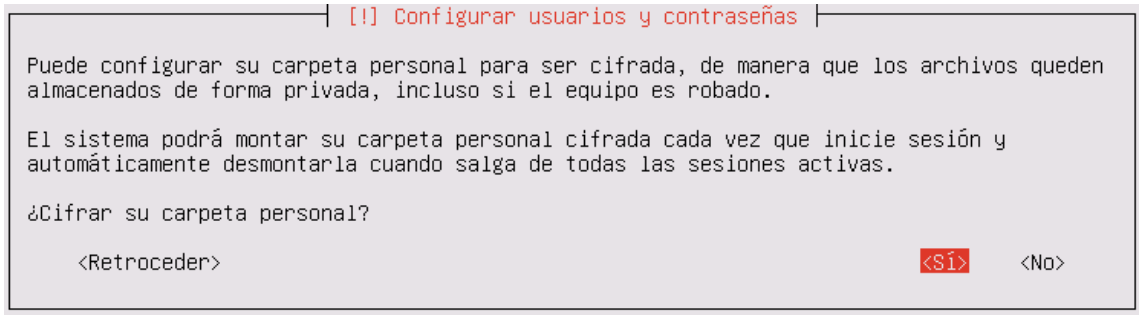
Ponemos una contraseña



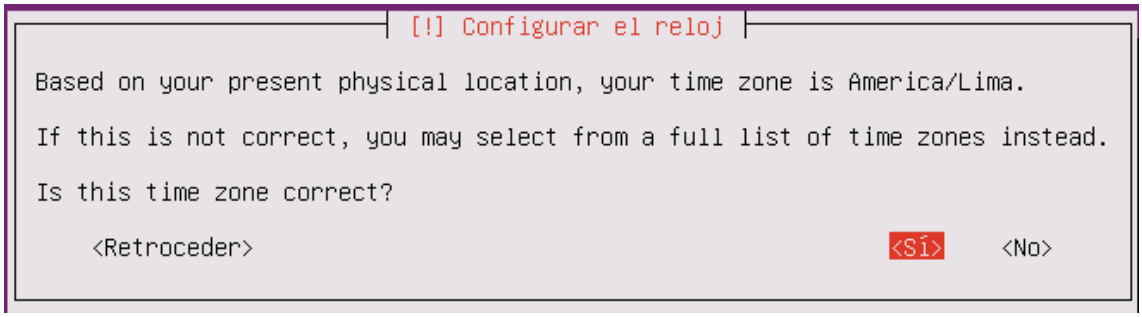
Volvemos a introducir la contraseña



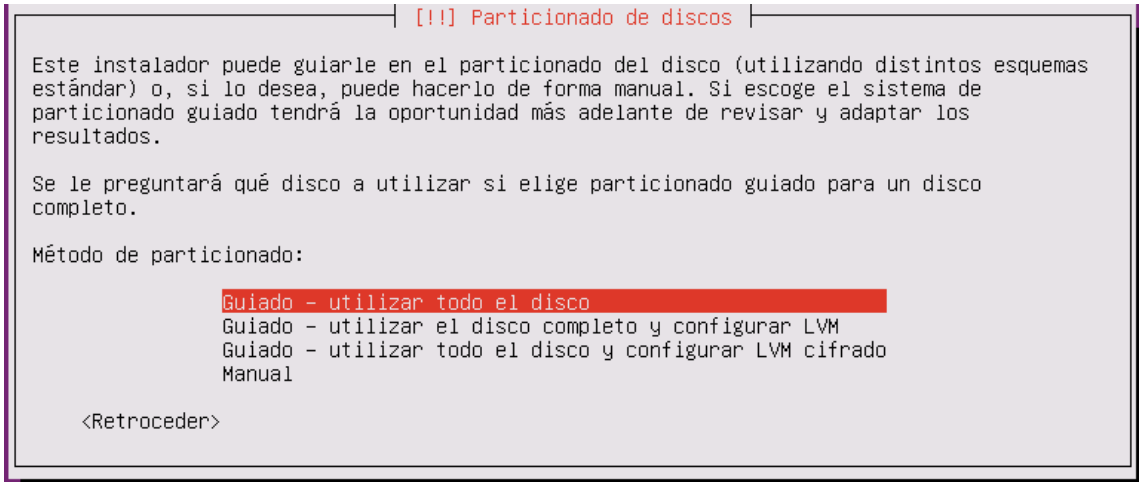
Elegimos en si



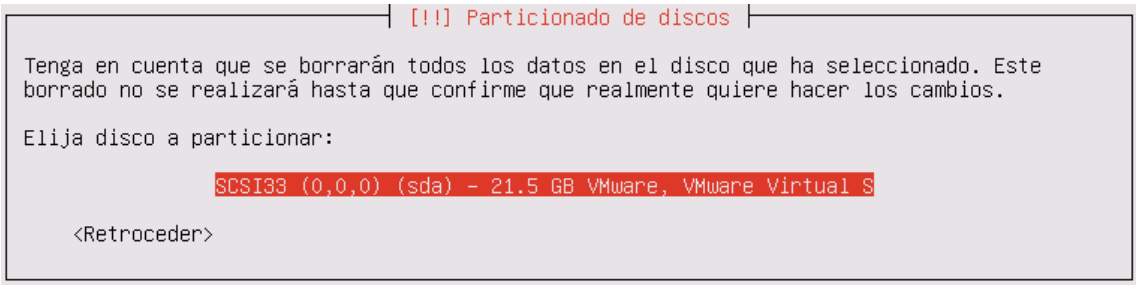
Elegimos que si



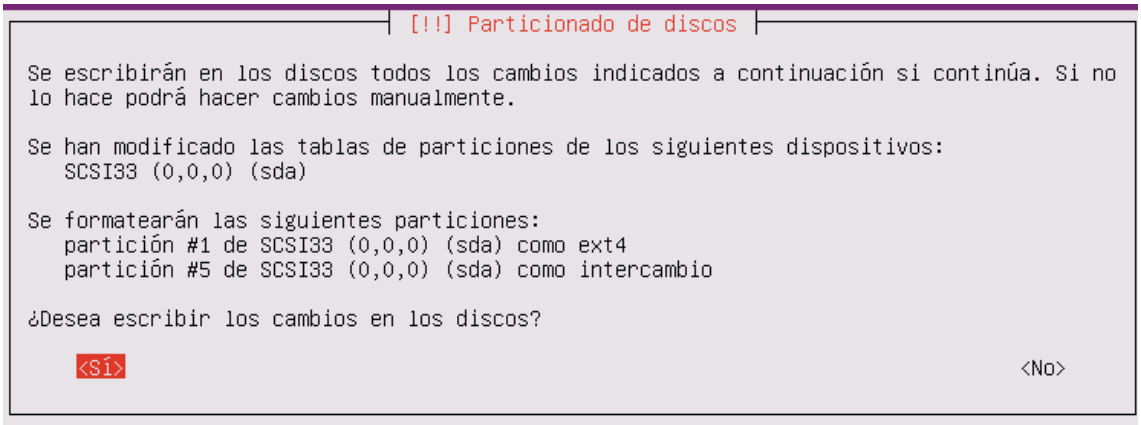
Seleccionamos lo siguiente



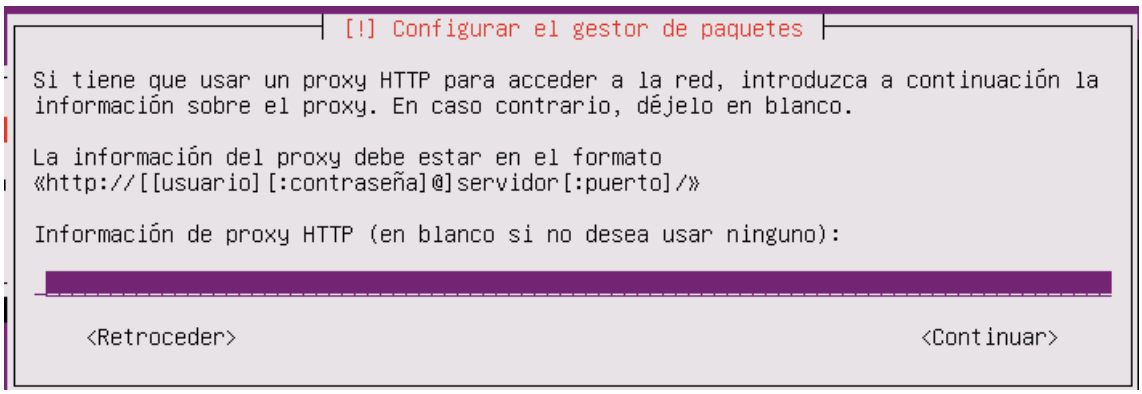
Elegimos la partición



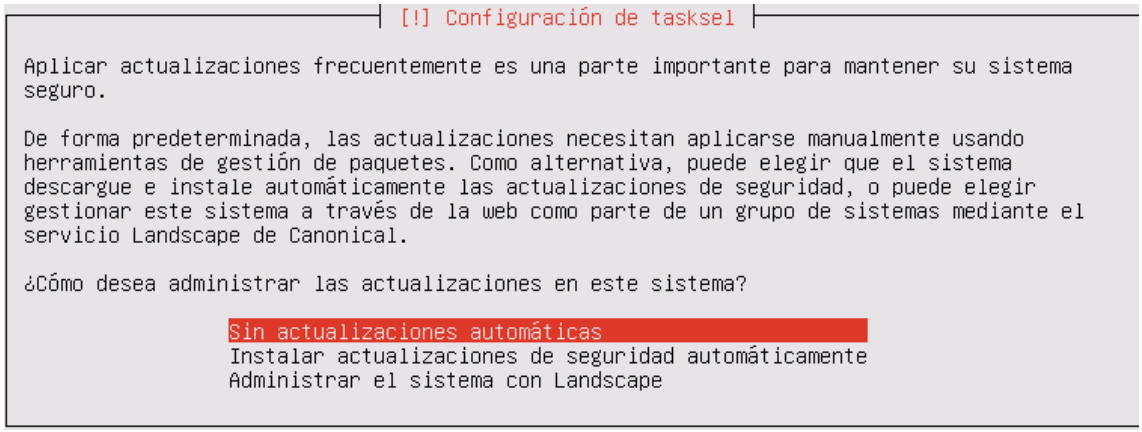
Elegimos que si



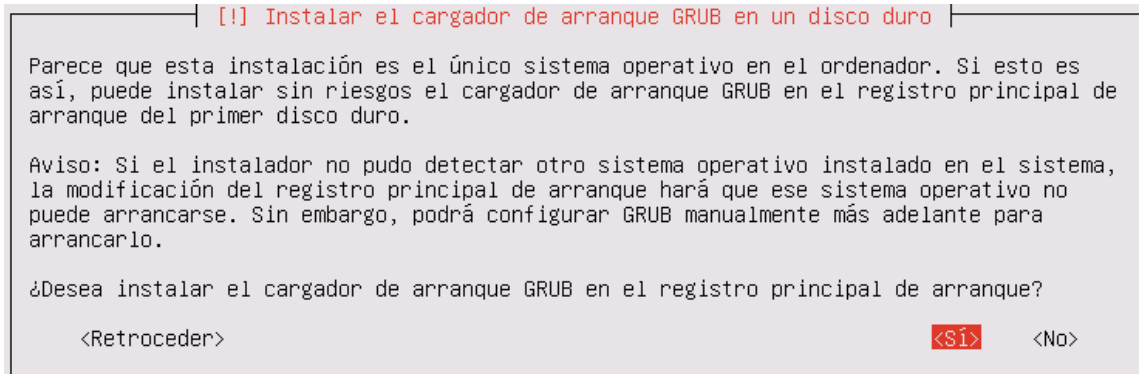
Elegimos continuar



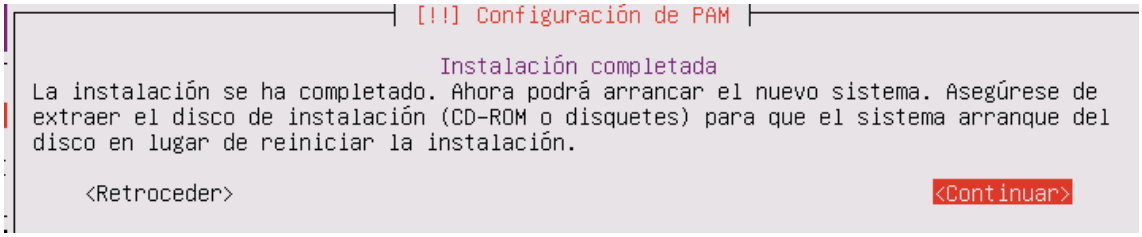
Elegimos sin instalar actualizaciones automáticas



Elegimos que si



Elegimos en continuar



Configuración del Ubuntu

Entramos a la siguiente ubicación

```
user01@serve01:~$ sudo nano /etc/network/interfaces
[sudo] password for user01:
```

Ponemos lo siguiente

```
  GNU nano 2.2.6                File: /etc/network/interfaces

# This file describes the network interfaces available on your sys
# and how to activate them. For more information, see interfaces(5

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.254
netmask 255.255.255.0
network 192.168.1.0
gateway 192.168.1.1
broadcast 192.168.1.255

dns-nameservers 200.48.225.130 200.48.225.146
```

Instalación del freeradius

Antes de instalar el freeradius ponemos los siguientes comandos:

- apt-get upgrade
- apt-get update

Al comenzando la instalación ponemos el siguiente comando, para que el freeradius valla a instalarse

```
root@serve01:~# apt-get install freeradius
```

Elegimos buscar el archivo de usuarios

```
root@serve01:~# cd /etc/freeradius/
root@serve01:/etc/freeradius# ls
acct_users                certs             huntgroups      proxy.conf       templates.conf
attrs                     clients.conf      ldap.attrmap    radiusd.conf     users
attrs.access_challenge    dictionary        modules         sites-available
attrs.access_reject       eap.conf          policy.conf     sites-enabled
attrs.accounting_response experimental.conf policy.txt      sql.conf
attrs.pre-proxy           hints             preproxy_users  sqlippool.conf
root@serve01:/etc/freeradius# nano users
```

Bajamos hasta el final y creamos los siguientes usuarios

```
# On no match, the user is denied access.

rafael Cleartext-Password := "admin123"
admin1 Cleartext-Password := "admin234"
admin2 Cleartext-Password := "admin345"
```

Salimos de la ruta de freeradius y reiniciamos el equipo

```
root@serve01:/etc/freeradius# /etc/init.d/freeradius restart
 * Stopping FreeRADIUS daemon freeradius                                [ OK ]
 * Starting FreeRADIUS daemon freeradius                                [ OK ]
root@serve01:/etc/freeradius# _
```

Ahora configuramos el archivo clients para los clientes

```
root@serve01:~# nano /etc/freeradius/clients.conf
```

Configuramos de la siguiente manera y guardamos

```
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}

clients 192.168.1.253{
    secret = 123321
    shortname = TP-LINK_FA3822
}
```

Hacemos ping para configurar si existe conexión con el router en Ubuntu y Windows como se muestra en las imágenes respectivamente

```
root@serve01:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=5.98 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.16 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.82 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.45 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.77 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=1.52 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=1.55 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=1.63 ms
^C
--- 192.168.1.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7017ms
rtt min/avg/max/mdev = 1.523/2.489/5.984/1.392 ms
root@serve01:~#
```

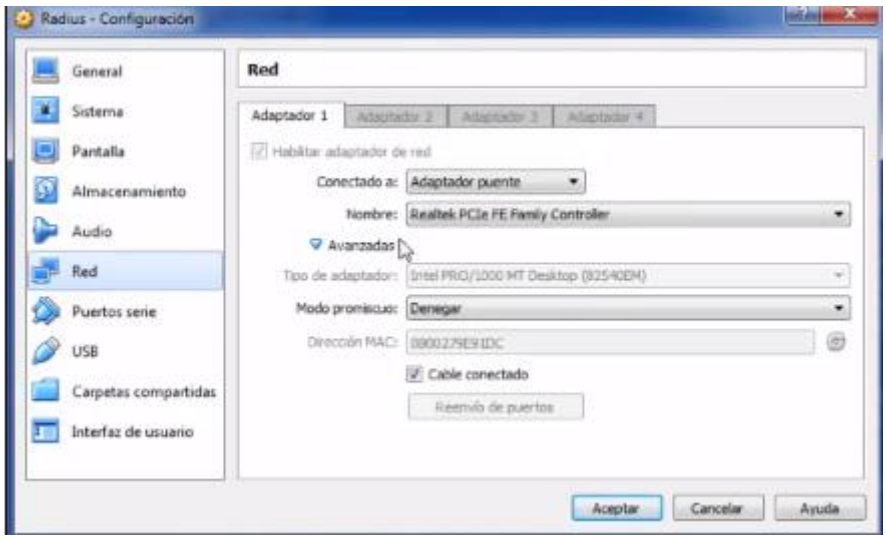
```
C:\Users\remd_>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

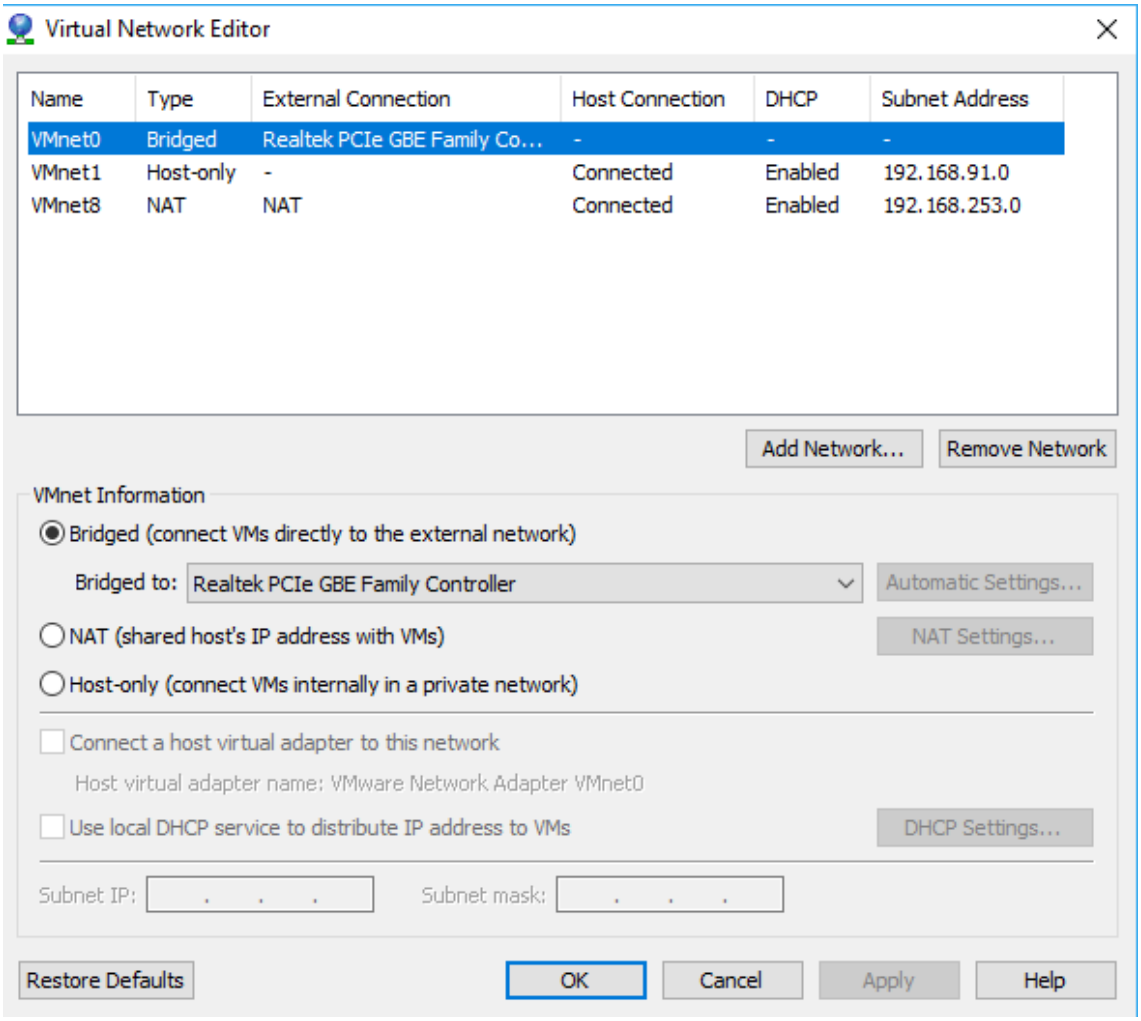
Nota: si el Ubuntu no se conecta revisa la siguiente configuración y asegurase de que este como se muestra en la imagen

En virtualbox



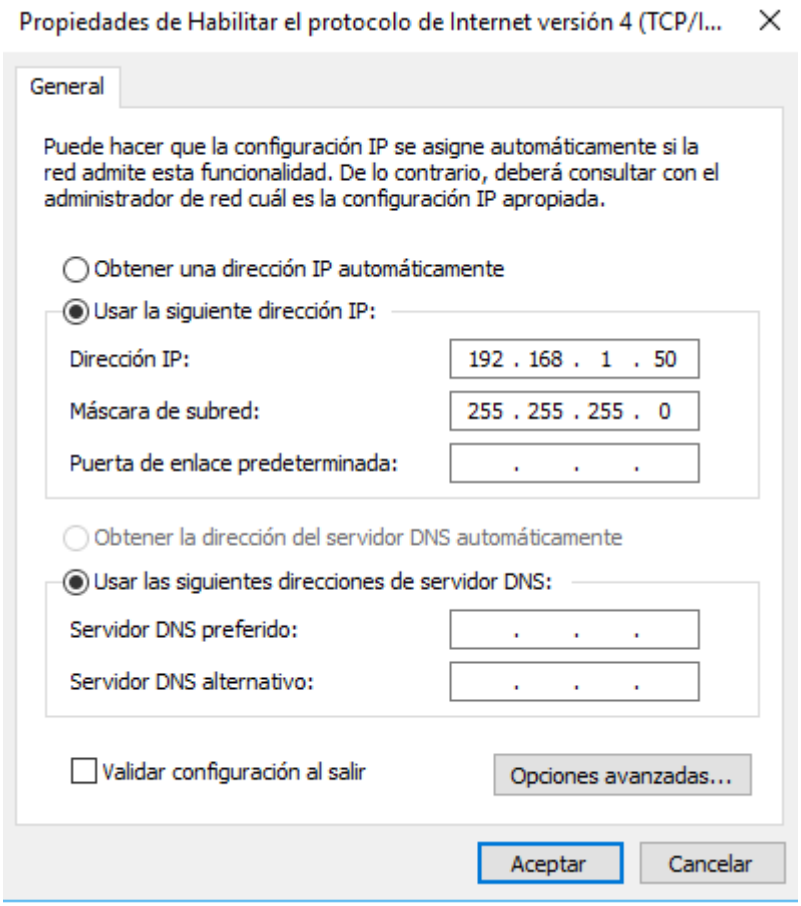
En Vmware:

Entre en edit => Virtual Netword Editor

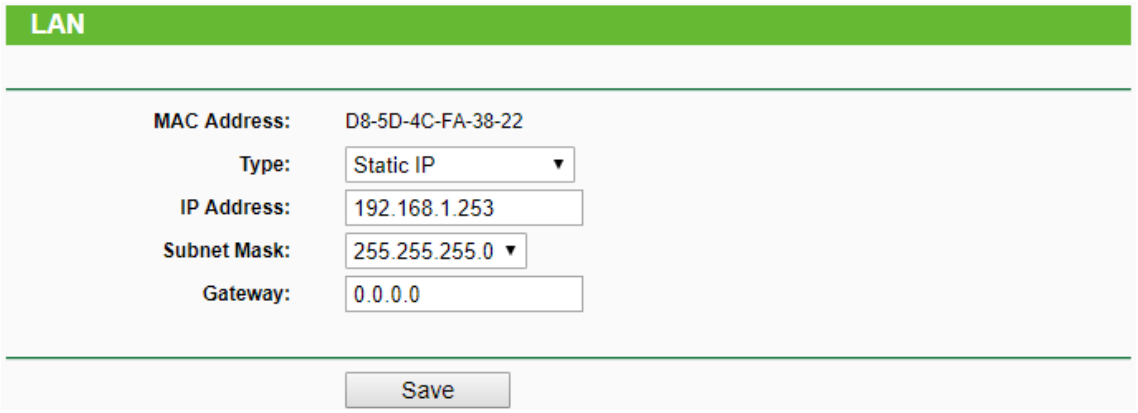


Configuramos el acces point

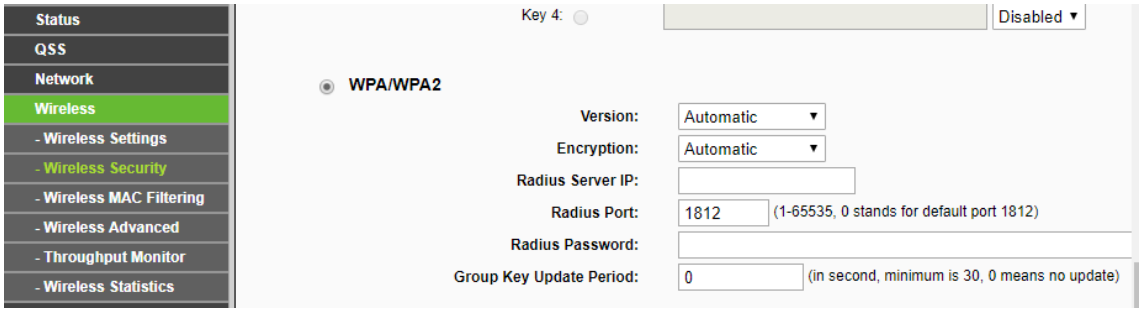
Configuramos la ip de muestra pc



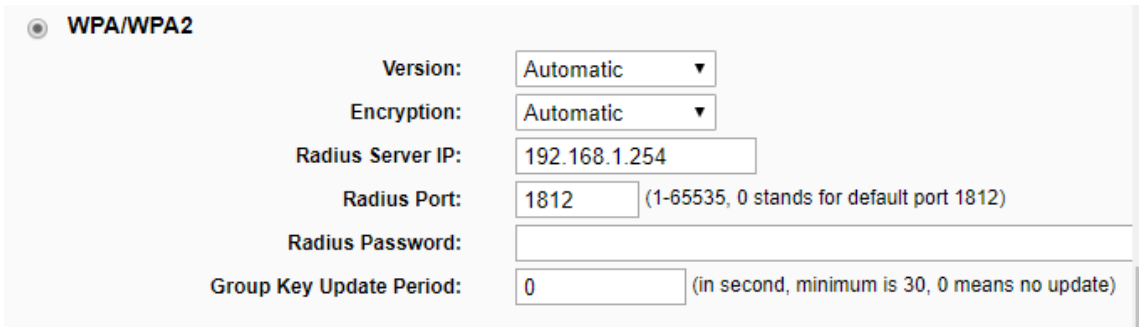
Cambiamos la ip



Entramos a Wireless => Wireless Segurity. Y configuramos esta parte



Ponemos la dirección Ip del Ubuntu Serve y guardamos



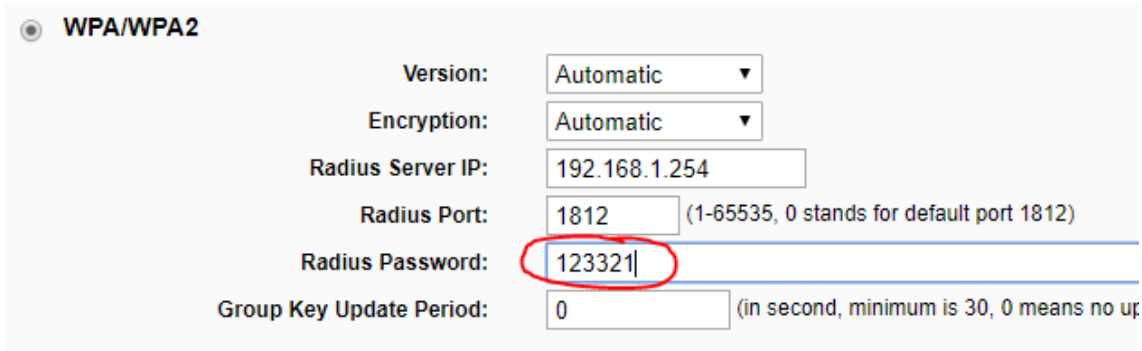
Ejecutamos el servidor Freeradius

```
root@serve01:~# freeradius -X
```

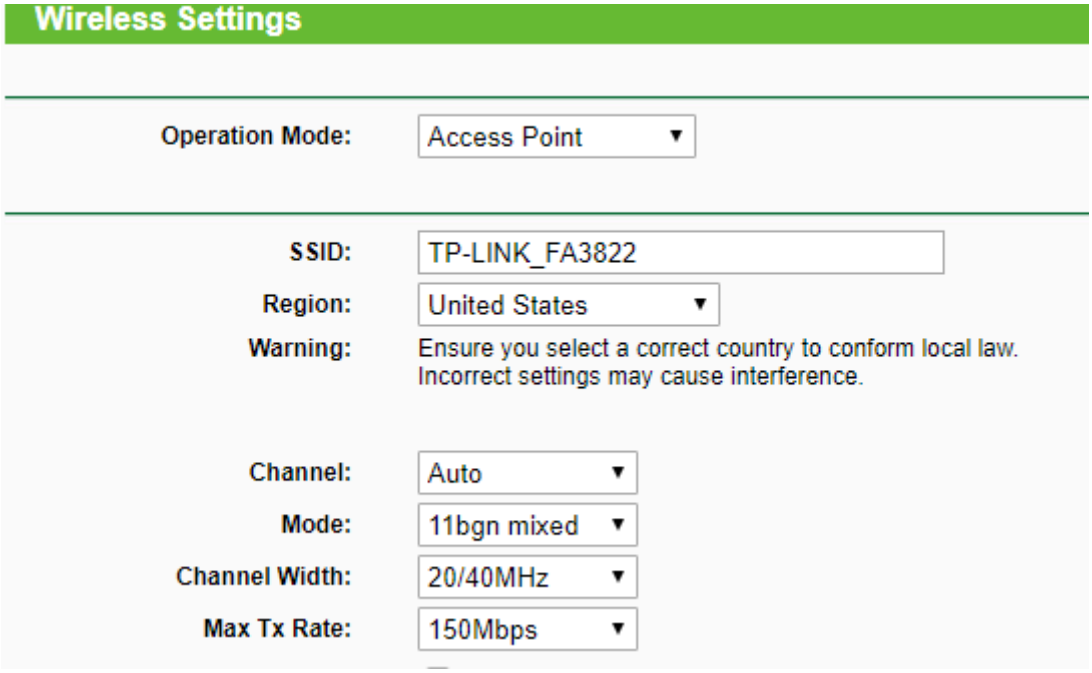
Y comprobamos que el puerto es el mismo que el Access point

```
... adding new socket proxy address * port 39421
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

Comprobar que la contraseña sea la misma que el client.conf de Access Point



En wireless => Wireless Settings SSID debe de ser igual que el shortname de client.conf




```
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}

clients 192.168.1.253{
    secret = 123321
    shortname = TP-LINK_FA3822
}
```

Volvemos a entra al servidor Freeradius y lo dejamos asi

```
root@serve01:~# freeradius -X
```

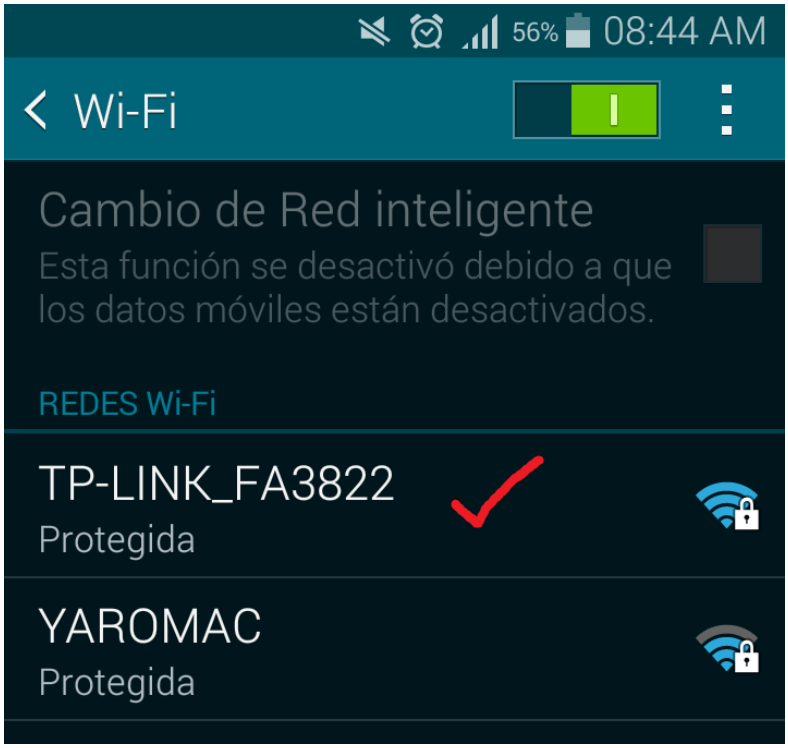
Comprobando que el usuario es aceptado

```
root@serve01:/etc/freeradius# radtest rafael admin123 localhost 0 testing123
Sending Access-Request of id 247 to 127.0.0.1 port 1812
        User-Name = "rafael"
        User-Password = "admin123"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=247, length=20
root@serve01:/etc/freeradius#
```

Después de haber terminado todas las configuraciones se recomienda reiniciar tanto en Ubuntu server como el Access Point y rauter

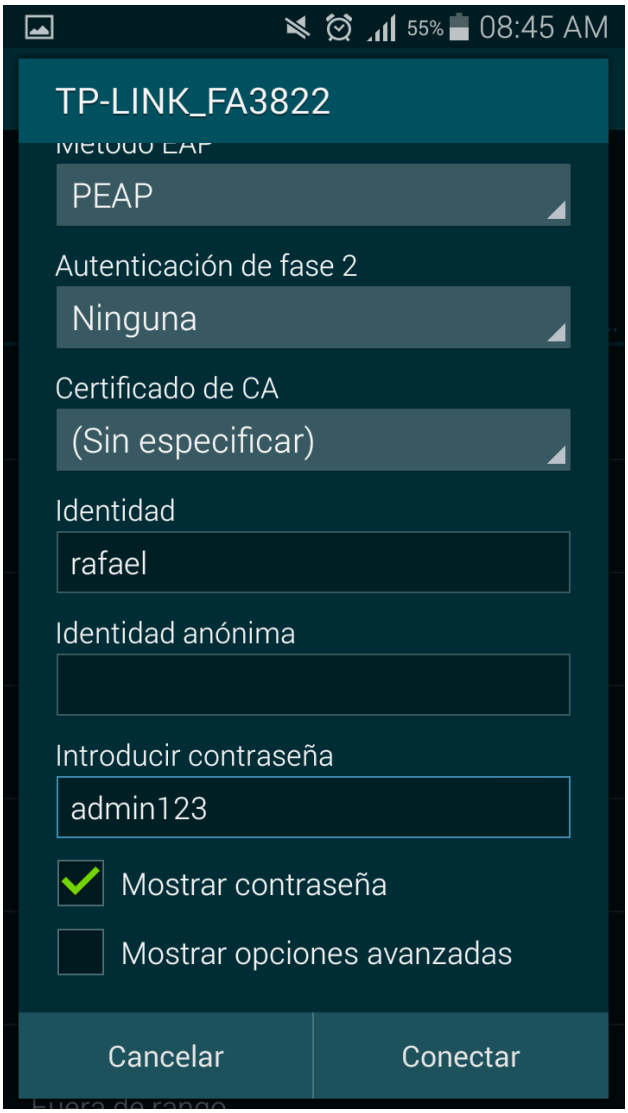
En el celular

Buscar el wifi:

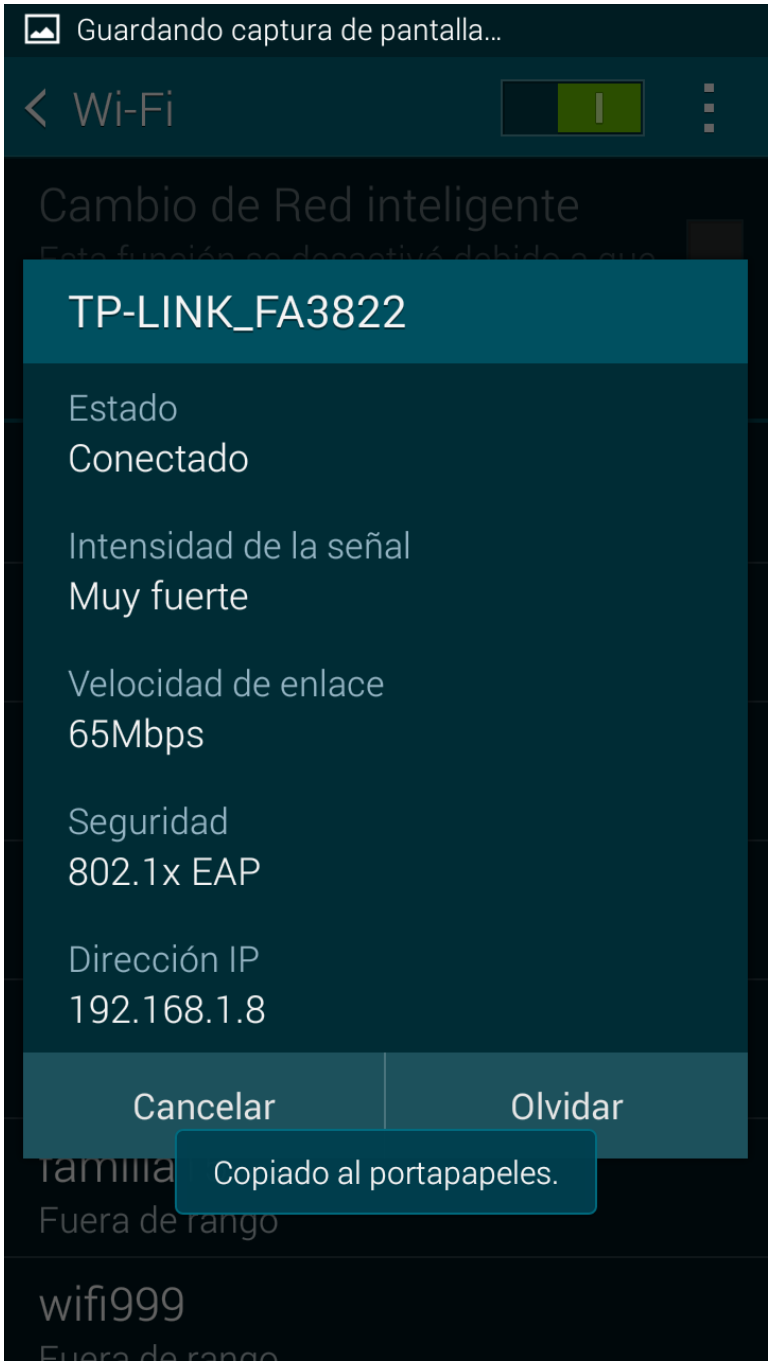


1. **Usuario Autentificado**

Ponemos nuestro login y password



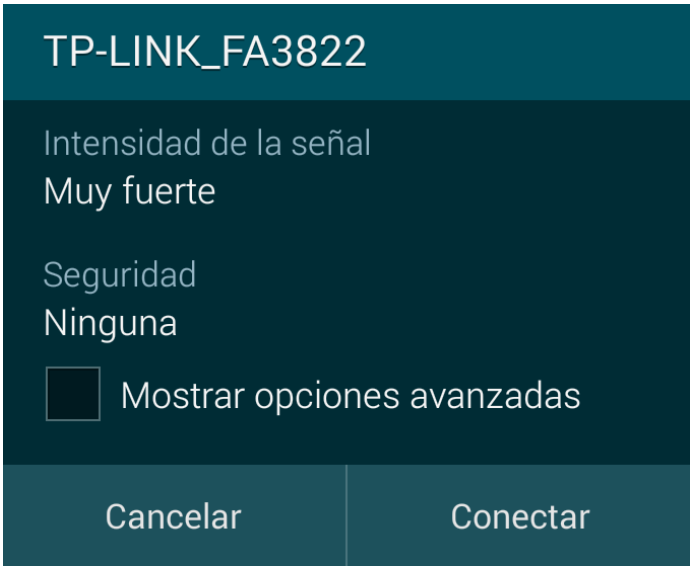
Y luego accederemos de nuevo al wifi y nos mostrara de esta forma



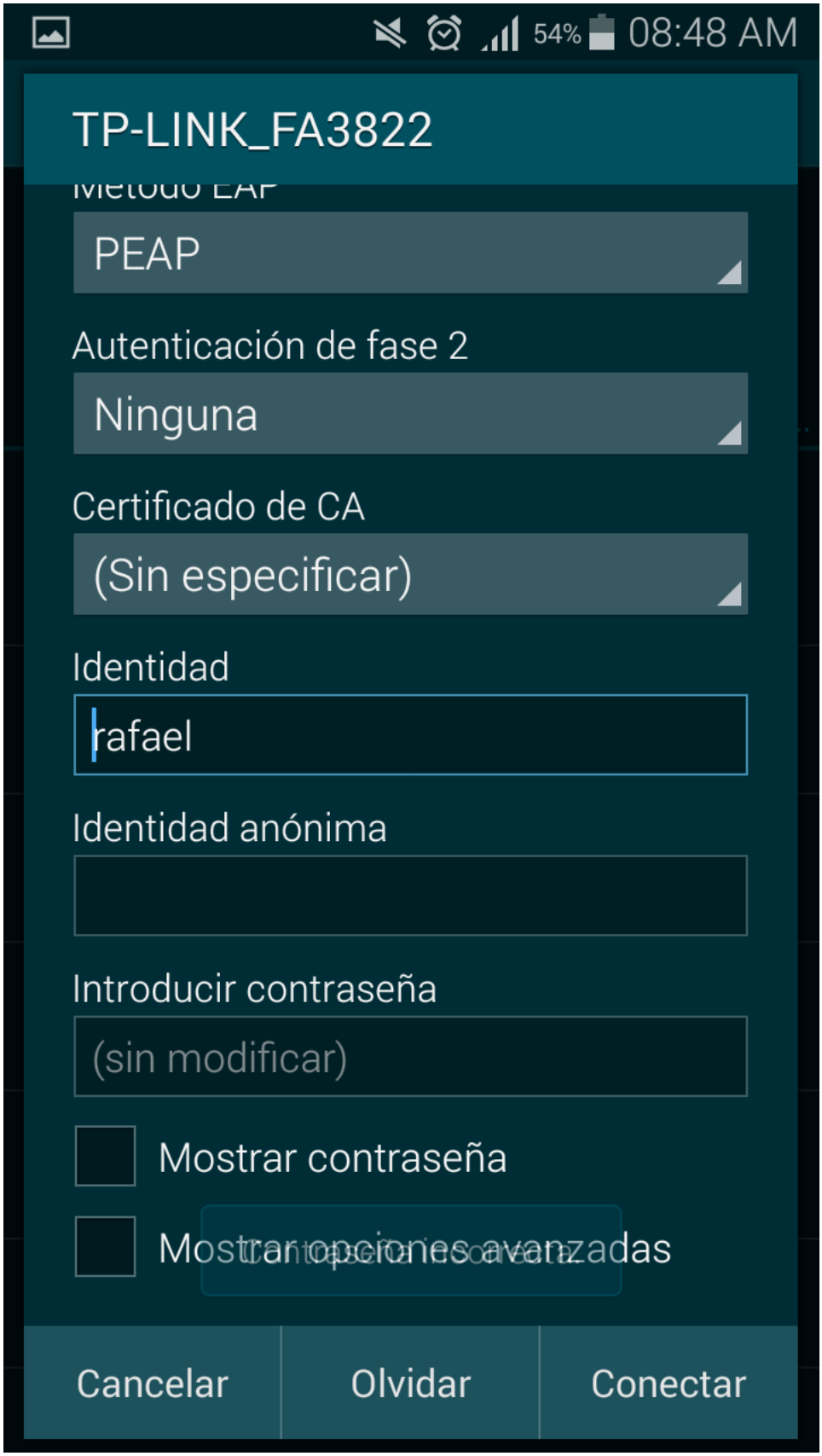
Y así accedemos a Google

2. Usuario no Autentificado

Al ingresar al wifi de nuevo después de iniciar sección incorrectamente nos saldrá de esta forma



Oh de la siguiente forma donde nos pida ingresar la contraseña de nuevo



NOTA: desactivar el firewall o cualquier antivirus o software que pueda ocasionar problemas en la red.

Diagrama de conexión