ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ

MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN EN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD: PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

ACCESO A REDES INALÁMBRICAS DE LA ESPAM MFL MEDIANTE UN SERVIDOR RADIUS

AUTOR:

JOSÉ RUBÉN LOOR ANCHUNDIA

TUTOR:

ING. JOFFRE RAMÓN MOREIRA PICO, M.Sc,

COTUTOR:

ING. JAVIER HERNÁN LÓPEZ ZAMBRANO, M.Sc,

CALCETA, SEPTIEMBRE 2019

DERECHOS DE AUTORÍA

JOSÉ RUBÉN LOOR ANCHUNDIA, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____

JOSÉ RUBÉN LOOR ANCHUNDIA

CERTIFICACIÓN DE TUTOR

ING. JOFFRE RAMÓN MOREIRA PICO, M.Sc, certifica haber tutelado el trabajo de titulación, que ha sido desarrollada por **JOSÉ RUBÉN LOOR ANCHUNDIA**, previa la obtención del título de Magister en Tecnologías de la Información con mención en Redes y Sistemas Distribuidos de acuerdo al **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

_____

ING. JOFFRE RAMÓN MOREIRA PICO, M.Sc,

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **ACCESO A REDES INALÁMBRICAS DE LA ESPAM MFL MEDIANTE UN SERVIDOR RADIUS** que ha sido propuesto, desarrollado por **JOSÉ RUBÉN LOR ANCHUNDIA**, previa la obtención del título de Magister en Tecnologías de la Información con mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

DR. INF. JORGE PÁRRAGA ÁLAVA
MIEMBRO

DR. INF. JORGE HERRERA TAPIA
MIEMBRO

ING. JÉSSICA MORALES CARILLO., M.Sc
PRESIDENTA

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que me dio la oportunidad de crecer como ser humano a través de una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día;

A Dios por ser el motor espiritual para seguir luchando por mis objetivos personales y profesionales;

A mis padres, que han sido mi ejemplo de vida para forjarme con valores y principios, y

A mi tutor, cotutor y tribunales por su asesoramiento durante el desarrollo de este trabajo, gracias por su valioso aporte.

El autor

DEDICATORIA

A Dios, mi creador y soporte espiritual.

A mis padres, por su gran apoyo durante estos años.

A mi hermana y hermanos, compañeros de vida.

A mis sobrinas y sobrinos, mi mayor tesoro.

A todos quienes, de una u otra manera, me han apoyado durante este largo camino.

El autor

CONTENIDO GENERAL

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

CONTENIDO DE GRÁFICOS

RESUMEN

La presente investigación se trata de la implementación de un servidor RADIUS en el Sector 8 de la ESPAM MFL, frente a la problemática actual que se pudo observar desde un contexto social - organizacional el incumplimiento de políticas, procedimientos y procesos para el control del acceso de las redes la implementación de mecanismos para su gestión y administración. Para el desarrollo se utilizó la metodología EDER (estudio, diseño, ejecución y revisión), la cual define procesos y procedimientos claramente definidos para la aplicación de proyectos de infraestructura tecnológica, el método utilizado para el muestreo fue de tipo dirigido. Para la recopilación de la información se realizó entrevistas al personal de Unidad de Tecnología y encuestas a los usuarios de la institución (docentes, personal administrativo y estudiantes) lo que permitió conocer la situación actual de las redes inalámbricas. Para el monitoreo y caracterización de las redes inalámbricas y los puntos de acceso se utilizó el Software Acrylac Wi-Fi Home y Acrylac Wi-Fi HeadMaps 4.1. Se instalaron Oracle VM Virtual Box 6.0, CentOS 7, daloRADIUS 1.0-0 entre otros programas y se realizaron las configuraciones de los equipos inalámbricos de acceso y las pruebas respectivas para la implementación del servidor RADIUS. Se muestran los principales resultados de la investigación sobre el la forma de acceso a las redes inalámbricas y a los recursos académicos y no académicos y la percepción del nivel de seguridad de la información institucional que tienen los usuarios; y por último se presenta la discusión, las conclusiones y recomendaciones.

.

PALABRAS CLAVE

Wi-Fi, AUTENTICACIÓN, AUTORIZACIÓN, AUDITORÍA, EDER

ABSTRACT

The present investigation is about the implementation of a RADIUS server in Sector 8 at ESPAM MFL, against the current problem that could be observed from a social - organizational context the breach of policies, procedures and processes for the control of the access of the networks the implementation of mechanisms for their management and administration. For the development we used the EDER methodology (study, design, execution and review), which clearly defines the processes and procedures for the application of technological infrastructure projects, the method used for sampling was directed. In order to gather the information, interviews were carried out with the staff of the Technology Unit and surveys of the users of the institution (teachers, administrative staff and students), which allowed to know the current situation of the wireless networks. The Acrylac Wi-Fi Home Software and Acrylac Wi-Fi HeadMaps 4.1 were used to monitor and characterize the wireless networks and access points. Oracle VM Virtual Box 6.0, CentOS 7, daloRADIUS 1.0-0 among other programs were installed; the wireless access equipment configurations and the respective tests for the RADIUS server implementation were performed. The main results of the research on the way of access to wireless networks and academic and non-academic resources and the perception of the level of security of institutional information that users have are shown; and finally the discussion, conclusions and recommendations are presented.

KEY WORDS

WI-FI, EDER, AUTHENTICATION, AUTHORIZATION, ACCOUNTING.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACION DEL PROBLEMA

Gutiérrez, (2012), sostiene que la seguridad en las redes se ha convertido en un factor de mucha importancia dentro de la gestión y administración de estas. Particularmente en las redes inalámbricas, la seguridad debe consistir en la aplicación de políticas, procedimientos o mecanismos que ayuden a prevenir y supervisar el acceso no autorizado para el uso de los recursos disponibles, pero muchas veces los mecanismos implementados no son los adecuados o simplemente no son bien implementados para su efecto, lo que representa serias desventajas en la seguridad de las redes inalámbricas.

Según *González, et al.* (2017), en el caso de las universidades, además del riesgo de sufrir ataques desde fuera de su perímetro, se ofrecen servicios a distintos tipos de clientes: usuarios administrativos, no docentes, y usuarios del ámbito académico, compuestos por profesores, investigadores y estudiantes, algunos de los cuales pueden ser personas con conocimientos sobre cómo vulnerar la seguridad de la red. En este sentido, resulta imprescindible disponer de políticas de seguridad para este tipo de entorno, de manera que permitan garantizar a un nivel aceptable, la autenticidad, disponibilidad y confidencialidad de la información que se genera y se transmite y con ello el funcionamiento de la red.

Según datos obtenidos de las unidades académicas y administrativas pertenecientes al Sector 8 de la ESPAM MFL, actualmente se cuenta con una gran cantidad de redes inalámbricas distribuidas en todas sus áreas, entre los edificios de Biblioteca, Carrera de Computación y de Posgrado y a medida que pasa el tiempo los recursos de red disponibles en este sector se ven cada día más solicitados por la alta demanda de usuarios, ya que a pesar de que existen protocolos de seguridad utilizados para su acceso, tales como WEP (Wireless Encryption Protocol), WPA (WiFi Protect Access), WPA2 (WiFi Protect Access

2), muchas de estas redes son de libre acceso lo que las hace vulnerables a ataques.

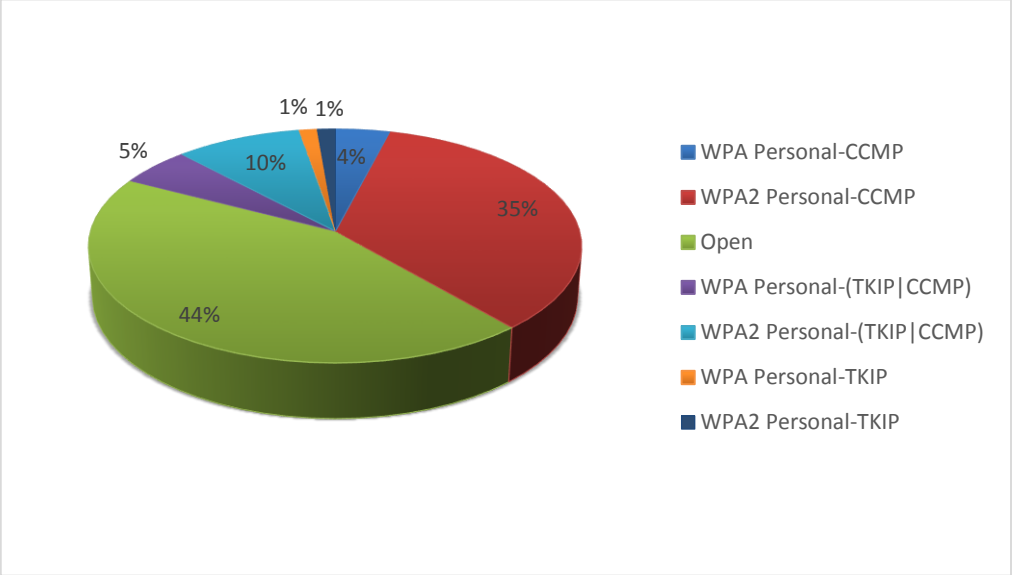


Gráfico 1. 1. Modo de cifrado de seguridad

Fuente: El autor

Se puede observar en el gráfico anterior que el 44% de las redes inalámbricas del Sector 8 de la ESPAM MFL tienen un modo de cifrado de seguridad abierto.

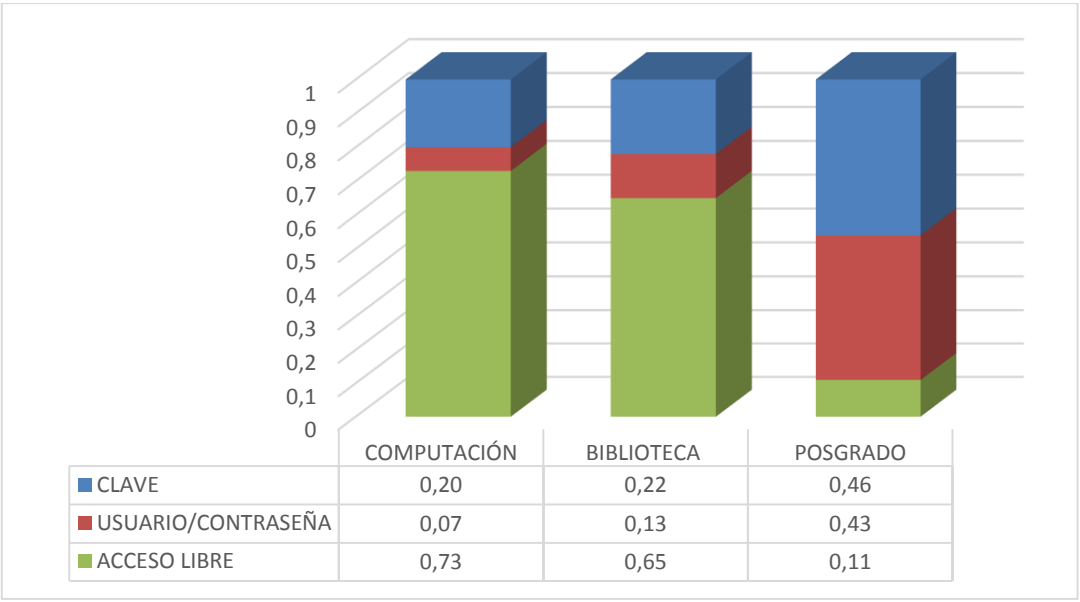


Gráfico 1. 2. Modo de acceso a redes inalámbricas

Fuente: El autor

De acuerdo con datos obtenidos en la encuesta realizada el 73% de los usuarios en el edificio de la Carrera de Computación, el 65% del edificio de Biblioteca y el 11% del edificio de Posgrado respectivamente acceden libremente a una red inalámbrica.

Por otra parte, Mendoza *et al.* 2017, expresan que un factor que impide un buen rendimiento en la red es el tipo de cifrado que se utiliza para conectar a los usuarios ya que en la práctica solo le preocupa contar con una clave de acceso (comúnmente por defecto), sin conocer cuál es el tipo de cifrado con el que cuenta el módem, access-point o router. Otros factores que determinan el rendimiento de una red inalámbrica con conexión a internet se pueden mencionar: el servicio de ancho de banda que el usuario contrata con el proveedor, el cual a su vez determina la velocidad promedio o máxima con la que se podrá contar, la cantidad de usuarios conectados, la ubicación en el área destinada, los obstáculos físicos, entre otros.

Otros datos obtenidos de la encuesta se puede observar que al 61% de los usuarios le comparten la clave de seguridad al conectarse a una red inalámbrica, mientras que el 46% de los usuarios pide autorización.

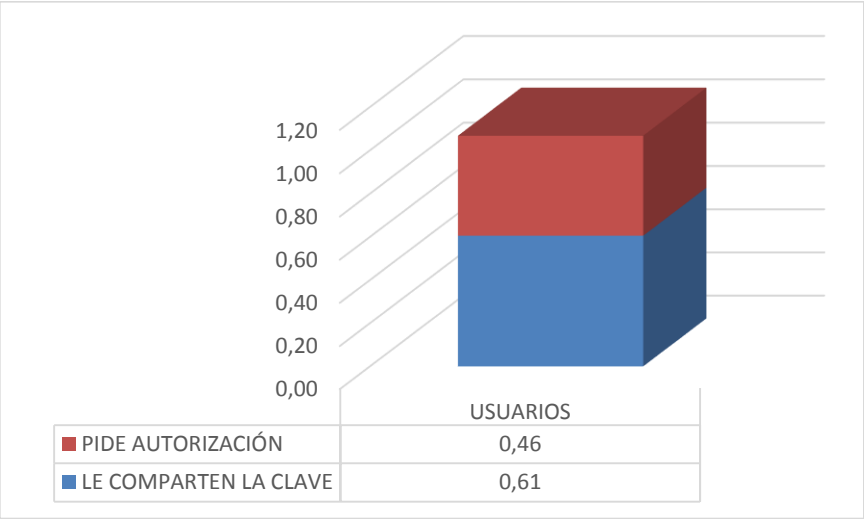


Gráfico 1. 3. Acceso a Redes inalámbricas por clave de seguridad

Fuente: El autor

La propagación de las claves de seguridad en las redes inalámbricas del Sector 8 quizás se deba por que las mismas son muy predecibles para los usuarios, y estos las puedan compartir ya que en muchas de ellas se utiliza la misma clave y en otras se sigue casi siempre un mismo patrón, tal como se lo muestra en la tabla siguiente:

Tabla 1. 1. Claves de seguridad de las redes inalámbricas del Sector 8 de la ESPAM MFL

Edificio	Red inalámbrica	Clave de seguridad
Bibliotecas	Talento Humano	tt-hh@123*0.
	Coordinacion academica	espamespam*0.
	Investigacion E	Investigacion001_
	Acreditacion	acreditacion@123*0.
	Planificacion	planificacion@123*0.
	Idiomas	idioma@2009
Computación	UDC desarrollo	Udcespam2019
Posgrado	Administracion -A	mespam@123*0.
	Administracion -B	mespam@123*0.
	Agroindustria - I	mespam@123*0.
	Agroindustria - II	mespam@123*0.
	Zootecnia	mespam@123*0.
	Turismo	mespam@123*0.
	E-posgrado	posgrado@123*0.

Fuente: El autor

Por otro lado, el 59% de las conexiones se realizan mediante el uso de dispositivos como Smartphones, Tabletas u otros dispositivos.

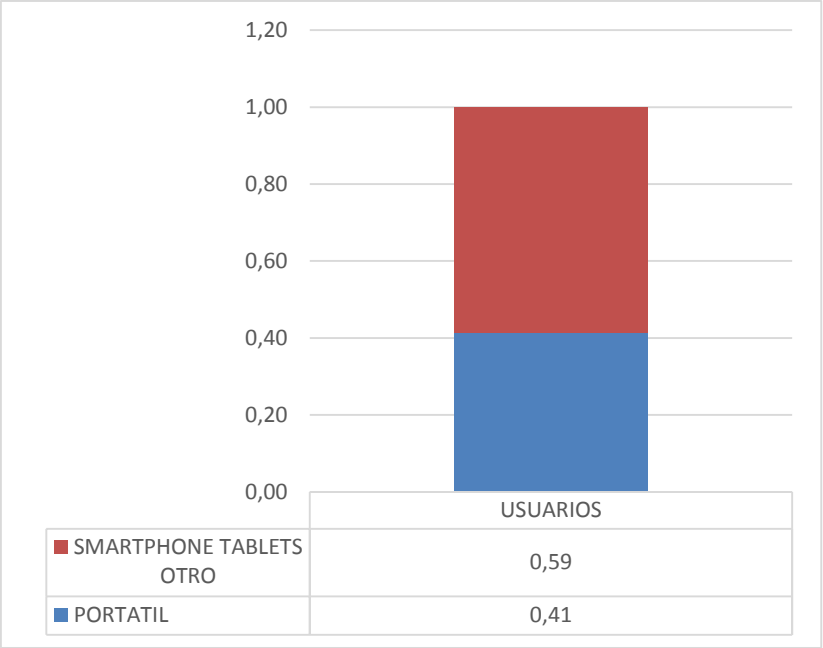


Gráfico 1. 4. Dispositivos utilizados por los usuarios para el acceso a las redes inalámbricas

Fuente: El autor

El 41% de consumo de internet es en servicios y recursos no académicos tales como: juegos en línea, páginas de descargas de películas, redes sociales, Youtube, páginas con contenido sexual entre otros.

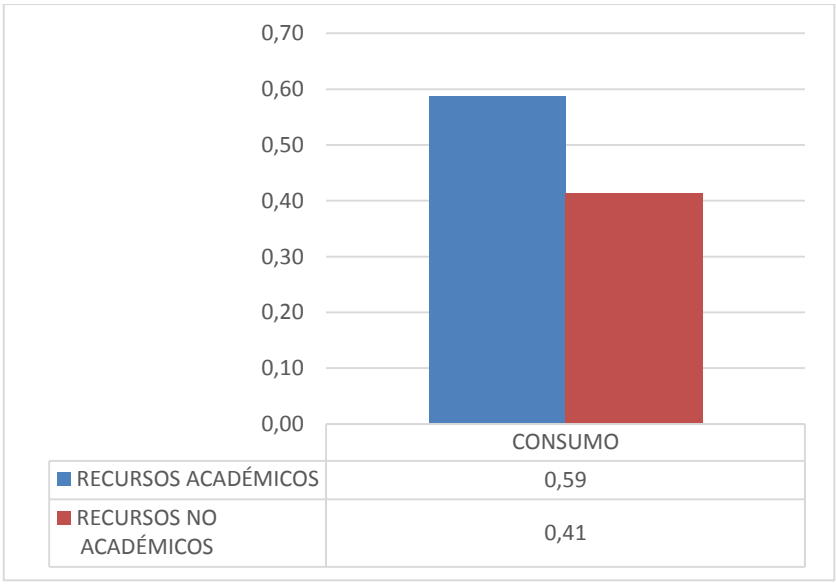


Gráfico 1. 5. Consumo de internet en el Sector 8

Fuente: El autor

Ante estos antecedentes mencionados se ve la necesidad de implementar un mecanismo de control de acceso a las redes inalámbricas, que permita una conexión más segura y que brinde un modo de autenticación más efectivo, y que no solo restringirá el acceso a usuarios no autorizados, sino que también registre las actividades de los usuarios al ser uso de la red mediante una administración eficiente de credenciales de acceso, por lo que el autor se formula la siguiente interrogante:

¿Qué mecanismo se debe implementar para mejorar el control de acceso a las redes inalámbricas de la ESPAM-MFL?

1.2. JUSTIFICACIÓN

Vallejo (2010), expresa que se han desarrollado muchas estrategias para controlar el acceso a las redes inalámbricas, la mayoría basadas principalmente en el cifrado de las comunicaciones (WEP, WPA, WPA2), la debilidad de estos mecanismos de seguridad es conocida hoy en la actualidad ya que existen muchas maneras de romper y conocer las claves de acceso. También existen otro tipo de medidas de protección como el filtrado de direcciones MAC, o bien medidas de protección más robustas basadas en el estándar IEEE 802.1x. Además de las desventajas citadas anteriormente, otro problema de las redes inalámbricas es la falta de integración de estos mecanismos.

Según Martínez y Oñate (2017), en las universidades es necesario aplicar estrategias enfocadas a la protección de la información crítica de la institución, por este motivo se toma como guía las estrategias que están siendo aplicadas en las empresas a nivel mundial como son las políticas de seguridad en las redes inalámbricas, con la finalidad de disponer un acceso seguro a la información y los servicios que brinda.

Siendo la ESPAM MFL parte del sistema de educación superior del Ecuador, en miras de la mejora continua de su realidad como Universidad, dentro de su quehacer institucional y haciendo mención en lo establecido en el modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas del Ecuador 2018, presentado por el Consejo de aseguramiento de la calidad de la Educación Superior (CACES), en su criterio 5: Recursos e infraestructura, subcriterio 5.1. Infraestructura, Ítem 5.1.3. Sistemas informáticos, considera como un elemento fundamental que las IES apliquen políticas y protocolos de seguridad y gestión de la información, que garantizan la confiabilidad y la confidencialidad de la información, **por esta razón y por la situación problemática anteriormente descrita**, se ve la necesidad de implementar un mecanismo de acceso a las redes inalámbricas y a sus recursos que establezca un mayor nivel de seguridad, que está basado en el estándar IEEE 802.1X y ofrece una

autenticación más segura, al mismo tiempo permite registrar las actividades de los usuarios garantizando un control más eficiente y reutilizando la infraestructura tecnología existente lo que no generará costos adicionales para su implementación, como solución tecnológica se propone un servidor RADIUS, el cual es un servidor de autenticación para el acceso a las rede inalámbricas, donde una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificar cuándo comienza y termina una conexión, determinar el consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un servidor RADIUS para controlar el acceso a las redes inalámbricas en el Sector 8 de la ESPAM MFL.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar la situación actual sobre el acceso y seguridad de las redes inalámbricas de la ESPAM MFL.
- Diseñar la arquitectura del servidor RADIUS.
- Poner en funcionamiento el servidor RADIUS en la infraestructura tecnológica de la ESPAM MFL.

1.4. IDEA PARA DEFENDER

¿La implementación de un servidor RADIUS mejorará el control de acceso a las redes inalámbricas de la ESPAM MFL?

CAPITULO II. REVISIÓN BIBLIOGRÁFICA

El presente trabajo tiene como finalidad la implementación de un servidor RADIUS como mecanismo de control de acceso a las redes inalámbricas del Sector 8 de la ESPAM MFL. En este capítulo se realizó la revisión bibliográfica que se divide en tres partes:

- **1:** Análisis de investigaciones relacionadas a la política de seguridad de la información, normativas, implantación y mecanismos utilizados en el acceso a las redes inalámbricas.
- **2:** Análisis de investigaciones relacionadas con servidores AAA (autenticación, autorización y auditoría) y estándar IEEE 802.1 X.
- **3:** Análisis de investigaciones relacionadas donde se implementó RADIUS como mecanismo de control de acceso a las redes inalámbricas.

2.1. ANÁLISIS DE INVESTIGACIONES RELACIONADAS A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, NORMATIVAS, IMPLANTACIÓN Y MECANISMOS UTILIZADOS EN EL ACCESO A LAS REDES INALÁMBRICAS.

A continuación se citan algunos autores que dentro de sus investigaciones expresan de manera general la importancia que tienen las redes inalámbricas dentro de las organizaciones y los diferentes riesgos y vulnerabilidades a las que se encuentran expuestas, así como también la implementación de políticas, procedimientos y otros lineamientos a seguir para lograr un mejor nivel de seguridad enfocados dentro de una cultura organizacional del buen uso de la red inalámbrica. Por otra parte, enfatizan en el acceso a las redes inalámbricas dado por la utilización de las claves de seguridad (WEP WPA, WPA2) como mecanismo utilizado, presentando ciertas deficiencias de las mismas y resaltan la implementación del estándar IEEE 802.1X como una solución a estos problemas.

Chaparro y Fajardo (2007), sostienen que las redes inalámbricas de área local, debido a sus múltiples aplicaciones, cada vez cobran una mayor importancia, en especial aquellas orientadas a usuarios móviles. En particular, las redes inalámbricas de área local se están convirtiendo rápidamente en una alternativa eficiente y confiable para todo tipo de organizaciones comerciales, industriales, gubernamentales, educativas, de salud, de servicios, entre otras. No obstante, las redes inalámbricas de área local aún presentan muchas vulnerabilidades en cuanto a la seguridad. Por su parte Vaca (2015), expresa que actualmente existen muchos riesgos de seguridad relacionados con las redes de comunicación, técnicas de ingeniería social, ataques de negación de servicio, uso indebido de aplicaciones, hasta la sustracción de datos, amenazas que pueden originarse desde fuera de la empresa o de propios empleados que intencionalmente o por falta de conocimientos pudieran llegar a comprometer la operatividad de toda la infraestructura de red, es allí la importancia de tener comunicaciones seguras en redes inalámbricas para establecer enlaces de intercambio de información confidencial (Gutiérrez, 2012).

Morales (2014), manifiesta que lo primero para la implementación de una red inalámbrica es desarrollar una adecuada política de acceso. Los usuarios, como principal elemento de una política de seguridad, deben ser educados y formar parte proactiva de dicha seguridad, esto concuerda con lo expresado por *Espinosa, et al.* (2018), que antes de comenzar a diseñar la red o evaluar los mecanismos de autenticación, es indispensable crear una política corporativa sobre la implementación y el uso de la red inalámbrica.

Según el Centro Criptológico Nacional (2017), dentro de esta política deberán incluirse, al menos, los siguientes aspectos:

• **Uso aceptable de la red inalámbrica:** Aspectos relacionados con el uso apropiado e inapropiado de la red inalámbrica y las medidas disciplinarias correspondientes. Se indicará lo que se puede hacer a través de la red inalámbrica y a qué recursos se puede acceder. Se incluirán los requisitos de

autenticación de usuario para el acceso a la red inalámbrica, requisitos sobre los dispositivos cliente, requisitos específicos de la conexión, entre otros.

• **Requisitos de seguridad de la infraestructura inalámbrica:** Consideraciones relativas a la asignación de roles y responsabilidades para la dirección, gestión y explotación de la red inalámbrica; tipo de información que podrá y que no podrá ser transmitida por la red inalámbrica; requisitos de seguridad física para los componentes de la infraestructura; configuración de seguridad de los elementos de la infraestructura; mecanismos de protección de la comunicación inalámbrica, incluyendo requisitos sobre cifrado, autenticación y gestión de claves criptográficas; entre otros.

• **Requisitos de seguridad de los dispositivos cliente:** Elementos relacionados con las condiciones de uso permitido de los dispositivos clientes, es decir, cómo, cuándo y dónde se pueden utilizar para acceder a la red inalámbrica; tipos de dispositivos cliente autorizados; configuraciones de seguridad, entre otros.

Dussan (2006), sostiene que para que la política sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: la cultura organizacional, las herramientas y el monitoreo, lo que involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.

Según Morales (2014), las redes inalámbricas cuentan con numerosos mecanismos y protocolos que aunque no garantizan de forma absoluta la integridad y confidencialidad de la información que por ellas transita, sí proporcionan barreras que reducen de forma considerable la cantidad de personas capaces (por sus conocimientos y recursos) de efectuar ataques

exitosos que llegan al punto de competir con muchas de las soluciones cableadas actualmente disponibles.

Para Capcha *et al.* (2017), la implementación de nuevas tecnologías y la adquisición e instalación de equipamiento informático requiere de un marco normativo que aporte las medidas inherentes a la seguridad; en el cual se plasmen mecanismos que resguarden su estado físico, su acabildad, uso y aprovechamiento; ya que es común encontrar redes WLAN sin seguridad de acceso o con seguridad WEP lo cual representa una gran deficiencia en su estructura de seguridad y una vulnerabilidad fuertemente expuesta a ser atacada, las redes abiertas están expuestas a ser suplantadas fácilmente y las protegidas bajo WEP son fuertemente vulnerables en su autenticación. Otro esquema de encriptación es WPA, que aunque es más robusto en su esquema de seguridad, simplemente retarda el mecanismo de vulnerabilidad a un par de horas adicionales de procesamiento para encontrar la llave de acceso a la red; como solución y medida adoptada para la solución a estas deficiencias, la IEEE desarrolló una arquitectura de seguridad, especificada bajo el estándar IEEE 802.1x, particularmente el estándar IEEE 802.11i especifica cómo se implementa la seguridad en redes inalámbricas (Monsalve *et al*., 2016). Este protocolo define el control de acceso a la red basado en puertos, facilita la autenticación y autorización de dispositivos que están conectados a un puerto LAN (red cableada), a través de redes inalámbricas y a través de puertos virtuales, ya sea para permitir o denegar el acceso a dicho puerto (Valdivieso, 2015).

Soriano (2014), manifiesta que el control de acceso se refiere a la prevención del uso no autorizado de un recurso, por lo tanto, abarca una variedad de mecanismos que establecen la política de derechos de acceso a los recursos y requieren la autenticación y posteriormente la autorización para acceder a los recursos que se desee proteger. Reyes (2016), expresa que es aquí donde el concepto de servidor de autenticación toma fuerza, ya que este elemento ofrece alternativas de protección en el acceso a una red de telecomunicaciones, a pesar de la existencia de muchas alternativas que cumplen esta función, un servidor Radius cuenta con las condiciones necesarias para cumplir este objetivo a fin de

brindar nuevas alternativas de acceso a una red corporativa, lo que concuerda con lo expresado por Enaceanu y Garais (2010), que la seguridad de la WLAN se puede fortalecer significativamente usando IEEE 802.1X para controlar el acceso a los puntos de acceso y entregar claves dinámicas a los usuarios autenticados. Los servidores de autenticación(AS) basados en el protocolo RADIUS desempeñan un papel clave en IEEE 802.1X; Cubillos (2013), el AS realiza la autenticación real de las credenciales proporcionadas por el cliente y hasta que un cliente no se valide no tiene acceso a los servicios ofrecidos por la red y Zhang *et al.* (2015), que sostiene que la autenticación IEEE 802.1X realiza la autorización, la autenticación y la contabilidad, y realiza un control efectivo para el acceso a la red de los usuarios de LAN. Por lo tanto, la configuración del sistema AAA que soporta la autenticación IEEE 802.1x proporciona tecnología para una investigación particular y una mejora adicional.

2.2. ANÁLISIS DE INVESTIGACIONES RELACIONADAS CON SERVIDORES AAA Y ESTÁNDAR IEEE 802.1X

Con base a las siguientes investigaciones citadas se pueden presentar las características de la arquitectura AAA y del estándar IEEE 802.1X sus ventajas y desventajas y así como también una comparativa entre este estándar frente a los demás mecanismos de seguridad, seguidamente se muestran diferentes comparativas entre los métodos de autenticación soportados por IEEE 802.1X, las características de un servidor RADIUS, los servidores que soportan el protocolo RADIUS con sus requerimientos técnicos y finalmente una comparativa entre RADIUS y otros servidores de autenticación.

En la tabla siguiente se muestran las principales características de la arquitectura AAA (autenticación, autorización y auditoría) y los principales beneficios de su implementación.

Tabla 2. 1. Características de la arquitectura AAA.

Características de arquitectura AAA	
Autenticidad	Proporciona el método de identificación de usuarios, incluyendo nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería y, según el protocolo de seguridad que seleccione, puede ofrecer cifrado.
Autorización	Provee el método de control de acceso remoto, incluyendo autorización total o autorización para cada servicio, lista de cuentas y perfil por usuario, soporte para grupos de usuarios, y soporte para IP, IPX, ARA y Telnet.
Auditoría	Posee un método de recolección y envío de información al servidor de seguridad, el cual es usado para facturar, auditar y reportar: nombres de usuario, tiempo de inicio y final, comandos ejecutado (como PPP), cantidad de paquetes enviados, y número de bytes.
Beneficios	• Incrementación de flexibilidad y control de configuración de acceso. • Escalabilidad. • Métodos de autorización estandarizados, como RADIUS, TACACS+ o Kerberos. • Múltiples sistemas de backup.
Tema: Diseño de implementación de arquitectura de conectividad y seguridad AAA en UDNET (Authentication, Authorization and Accounting) (Mauricio,M. 2010)	

Fuente: El autor

Seguidamente se presentan los puntos claves del control de acceso a la red mediante el estándar IEEE 802.1X, las ventajas que tiene y las funcionalidades que brinda, así como también la seguridad requerida dependiendo el tipo de y tamaño de la organización.

Tabla 2. 2. Características del estándar IEEE 802.1x.

Características del estándar IEEE 802.1X					
Puntos Clave	Realiza el control de acceso a una red mediante un proceso de autenticación.	Requiere de: Usuario o "suplicante", Punto de acceso o "Autenticador" y Servidor de autenticación.	Hace referencia al uso del protocolo de autenticación extensible EAP.	La implementación de 802.1x para redes inalámbricas utiliza un servidor de autenticación como el RADIUS.	
Porque 802.1X?	Evitar la difusión del identificador de red o SSID.	Establecer listas de control de acceso por direcciones físicas.	Utilizar cifrado en las conexiones.	Segmentar los puntos de acceso inalámbricos.	Combinar mecanismo de autenticación a la red y cifrado de datos.

Ventajas	Costos asociados, ya que se puede utilizar servidores de autenticación (RADIUS, IAS6).	Es fácilmente adaptable a los cambios o crecimientos de las infraestructuras tecnológicas.	Se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.
Funcionalidad	Ofrecer acceso a los servicios tecnológicos.	Brindar acceso a algunos servicios para invitados, clientes o socios de negocio.	Habilitar el acceso a los recursos informáticos para usuarios que requieren movilidad.
Seguridad Requerida	Puede variar ampliamente entre una y otra organización.	Tamaño de las organizaciones y su limitación en recursos pueden conllevar a que se implementen mecanismos de seguridad menos robustos.	
Tema: "Implementación de Active Directory aplicando el estándar 802.1x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja" (Ocampo, et al. 2016)			

Fuente: El autor

En la siguiente tabla se muestran las ventajas y desventajas del estándar IEEE 802.1X.

Tabla 2. 3. Ventajas y desventajas del estándar IEEE 802.1x

Ventajas y desventajas del estándar IEEE 802.1X	
Ventajas	**Desventajas**
Nivel de seguridad alto: **Se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuarios y contraseñas.**	**Interoperabilidad:** Aunque IEEE 802.1x disfruta de una aceptación casi universal, el uso de distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada.
Autenticación de usuarios y de equipos: **Permite la autenticación por separado de usuario y de equipo. La autenticación permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.**	
Transparencia: **Proporciona una autenticación y una conexión a la WLAN transparentes.**	
Cifrado más seguro: **Permite un cifrado muy seguro de los datos de la red.**	**Disponibilidad:** Por ser compleja la configuración en lo que respecta a la seguridad de WLAN, muchas de las empresas no disponen del estándar IEEE 802.1x.
Bajo coste: **Bajo coste del hardware de red.**	
Alto rendimiento: **Dado que el cifrado se lleva a cabo en el hardware de WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.**	
Tema: Diseño de un modelo de autenticación Radius para reforzar los niveles de seguridad en el diseño de redes inalámbricas IEEE 802.11 x para la Cooperativa de Ahorro y Crédito Tumán(Guanilo,2010)	

Fuente: El autor

A continuación, se muestra una tabla comparativa entre las opciones tecnológicas para un esquema de seguridad, como se puede observar el estándar IEEE 802.1X en los diferentes parámetros presenta ventajas frente a las demás opciones.

Tabla 2. 4. Comparativa entre opciones tecnológicas para esquema de seguridad

Comparativa entre opciones tecnológicas para un esquema de seguridad				
Características	**IEEE 802.1X**	**WEP Estático**	**VPN**	**Ipsec**
Autenticación	Si	No	Sí, pero las VPNS no usan la autenticación de clave compartida.	Sí, si se usa la autenticación Kerberos o certificados.
Encriptación de datos robusta	Si	No	Si	Si
Conexión y reconexión transparente a la WLAN	Si	Si	No	Si
Autenticación de usuario	Si	No	Si	Si
Autenticación de computadora	Si	Si	No	Si
Tráfico "broadcast"y "multicast" protegido	Si	Si	Si	No
Depositivos adicionales de red requeridos	Servidores RADIUS.	No	Servidores VPN, Servidores RADIUS.	No
Acceso seguro a la WLAN	Si	Si	No	No
Tema: Control de acceso a una red inalámbrica privada con administración centralizada basada en 802.1x (Casanova,2010)				

Fuente: *El autor*

En esta tabla se realiza una comparativa entre los diferentes métodos de autenticación para el estándar IEEE 802.1X, donde el método PEAP se presenta como el más idóneo según lo enunciado.

Tabla 2. 5. Comparativa entre métodos de autenticación para IEEE 802.1X

Comparativa entre los métodos de autenticación para IEEE 802.1X			
Característica	**PEAP**	**EAP-TLS**	**EAP-MD5**
Autenticación Mutua	Autenticación de cliente y usuario.	Autenticación de cliente y usuario.	Solo autenticación del cliente.
Generación dinámica en clave	Generación durante la autenticación y regeneración en intervalos de tiempo.	Generación durante la autenticación y regeneración en intervalos de tiempo.	No tiene generación dinámica de claves. Posee claves fijas.
Nivel de seguridad	Uso de autenticación de contraseñas fuertes o certificados digitales.	Autenticación fuerte.	Seguridad débil.

Protección de credenciales de usuario	Protegido por el túnel de seguridad de Capa de transparente (TLS).	Autenticación basada en certificados protegida por el tunel de seguridad de Capa de Transporte (TLS).	Abierto a ataques basados en texto conocido (ataques de diccionario).
Facilidad de implementación	Soportado por clientes Windows.	Requiere una infraestructura de llave pública (PKI). Soportado por clientes Windows.	Simple, no recomendado para soluciones inalámbricas.
Flexibilidad de las credenciales	Cualquier método EAP con Túnel TLS, como el método basado en contraseñas (EAP - MSCHAPV2).	Solamente certificados digitales.	Solamente contraseñas.
Tema: Control de acceso a una red inalámbrica privada con administración centralizada basada en 802.1x (Casanova,2010)			

Fuente: El autor

A continuación, se presentan características de un servidor RADIUS en el funcionamiento dentro de una red inalámbrica.

Tabla 2. 6. Características del servidor RADIUS

Características del servidor RADIUS	
Seguridad	Las transacciones entre el cliente y el servidor RADIUS son autentificadas mediante el uso de un secreto compartido.
Flexibilidad	El servidor RADIUS puede soportar una variedad de métodos para autentificar un usuario, puede soportar PPP PAP P CHAP, acceso UNIX, y otros mecanismos de autentificación.
Administración simple	El servidor RADIUS provee seguridad a la información en archivos de textos en una locación central; se pueden agregar nuevos usuarios a la base de datos o modificar información de usuario existente.
Capacidad extensiva de auditoria	RADIUS provee una extensiva capacidad de contabilidad, referida como contabilidad RADIUS. La información colectada en un archivo bitácora puede ser analizada para proyectar seguridad o usada para facturar.
Tema: Acceso WiFi mediante servidor centralizado implementando puntos de acceso basados en Open-WRT (Martinez, 2015)	

Fuente: El autor

Los servidores de software que implementan el protocolo RADIUS son diversos, a continuación, se muestran una gama de ellos, según lo observado FreeRADIUS y DolaRADIUS son los más versátiles y flexibles con los requerimientos funcionales.

Tabla 2. 7. Comparativa de diferentes servidores que implementan el protocolo RADIUS

Comparativa de diferentes servidores que implementan el protocolo RADIUS			
Servidores de Software	**Sistema operativo**	**Encriptación que soporta**	**Base de Datos**
Networld Policy Server (NPS-RADIUS)	Windows Server 2008-Server 2008R2 y Windows Server 2012-20012R2, Windows Server 2016.	Tarjetas inteligentes, Certificados, EAP, EAP-MSCHAP v2, PEAP, PEAP TLS.	SQL Server, LDAP.
TekRADIUS	Windows	MD5, PEAP Y TLS.	LDAP, SQL, PostgreSQL.
EmeraldV5	Windows, Linux.	PEAP, TTLS Y LEAP.	LDAP, SQL, PostgreSQL.
RAD-series	Windows	MD5, TLS, PEAP, TTLS Y LEAP.	LDAP, SQL, PostgreSQL.
Odyssey	Windows	MD5, TLS, PEAP, TTLS Y LEAP.	LDAP, SQL, PostgreSQL.
Steef Belted RADIUS 4.0	Windows, Sun Solaris.	MD5, TLS, PEAP, TTLS Y LEAP.	LDAP, SQL, PostgreSQL.
Zeroshell	Windows, Linux.	EAP-TLS, EAP-TTLS Y PEAP.	LDAP, SQL, PostgreSQL.
FreeRADIUS	Linux, Debian, Ubuntu, Suse, Mandriva, FedoraCore,FeeBSD, MacOS, OpenBSD, Solaris Windows.	MD5, TLS, PEAP, TTLS Y LEAP.	LDAP, OpenLDAP, SQL, MySQL, PosrgreSQL.
DaloRADIUS	Linux, Debian, Ubuntu, Suse, Mandriva.	MD5, TLS, PEAP, TTLS.	LDAP,OpenLDAP, SQL.
Tema: Mecanismos de seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos (González,2017)			

Fuente: El autor

En la siguiente tabla comparativa se describen las funcionalidades del servidor TACACS+ y RADIUS, donde este último presenta algunas ventajas dentro de sus funcionalidades para su implementación dentro de una red inalámbrica.

Tabla 2. 8. Comparativa entre TACACS+ Y RADIUS

Comparativa entre TACACS+ Y RADIUS		
FUNCIONALIDAD	**TACACS+**	**RADIUS**
Autenticación	El proceso de Autorización es independiente del proceso de autenticación.	Combina la Autenticación y la Autorización.
Estándar	Cisco Systems.	Estándar abierto.

Confidencialidad	Encripta el paquete completo, incluido el nombre de usuario, la contraseña y otros atributos.	Solo en la contraseña en el paquete de solicitud de acceso.
Granular Comandos de Autorización	Permite flexibilidad adicional y controles de acceso granular sobre quién puede ejecutar qué comandos en dispositivos específicos. Por usuario o por grupo.	No tienen esta opción para autorizar comandos por usuario o por grupo.
Auditoría	Tiene suporte para auditoría, pero limitada.	Proporciona mayor soporte para auditoría que TACACS+.
Requerimiento de equipos	Alto	Medio
Precio	Alto	Gratis
Tema: AN ANALYTICAL AND EXPERIMENTAL STUDY OF AAA MODEL WITH SPECIAL REFERENCE TO RADIUS AND TACACS+(Sikarwar y Saxena,2017)		

Fuente: El autor

De igual forma en esta tabla comparativa se describen las funcionalidades del servidor DIAMETER y RADIUS, donde también RADIUS presenta algunas ventajas dentro de sus funcionalidades para su implementación dentro de una red inalámbrica.

Tabla 2. 9. Comparativa entre DIAMETER Y RADIUS.

Comparativa entre DIAMETER Y RADIUS		
FUNCIONALIDAD	**DIAMETER**	**RADIUS**
Autenticación	El proceso de Autorización es independiente del proceso de autenticación.	Combina la Autenticación y la Autorización.
Estándar	Estándar abierto.	Estándar abierto.
Confidencialidad	Encripta el paquete completo.	Solo en la contraseña en el paquete de solicitud de acceso.
Autorización	Se pueden dar restricciones de autorización, reglas de acceso y filtros.	Se pueden dar restricciones de autorización, reglas de acceso y filtros.
Auditoría	Dirige la contabilidad en tiempo real, es decir, envían el informe de los eventos que ocurren en una escala de segundos en vivo de forma síncrona, la contabilidad es más dinámica.	Dirige la contabilidad en tiempo real, es decir, envían el informe de los eventos que ocurren en una escala de segundos en vivo de forma síncrona.
Tema: Role of Diameter Based Protocol in enhancing of new and Upcoming Technologies (*Kuma, et al. 2016*)		

Fuente: El autor

Finalmente se presenta una comparativa entre RADIUS, TACACS+ Y DIAMETER.

Tabla 2. 10. Comparativa entre RADIUS, TACACS+ Y DIAMETER

Comparativa entre RADIUS, TACACS+ Y DIAMETER			
Parámetros	**RADIUS**	**TACACS+**	**DIAMETER**
Protocolo ID de transporte	UDP	TCP	TCP o SCTP con TLS o IPSEC
Tipo de protocolo	Cliente /servidor.		Peer to peer.
Tipo de mensajes	Solicitud/Respuesta del cliente al servidor.		Solicitud/Respuesta de una parte a otra.
Encriptación de paquetes	Solo la contraseña en las respuestas al acceso. Otra información esta vulnerable a ser capturada.	Todo el cuerpo del paquete excepto la cabecera estándar.	Todo el cuerpo del paquete.
Algoritmo de encriptación	Secreto compartido con MD5.		Secreto Compartido con HMAC-MD5.
Autenticación y autorización	Combinado en un mismo perfil de usuario. Los paquetes de acceso aceptando generados por el servidor para el cliente contienen información de autorización.	Independiente Empleo de arquitectura AAA permitiendo separar en servidores diferentes las soluciones AAA.	Independientes
Tema: Protocolos de control de acceso RADIUS (Escalona, 2012)			

Fuente: El autor

2.3. ANÁLISIS DE INVESTIGACIONES RELACIONADAS CON LA IMPLEMENTACIÓN DE SERVIDOR RADIUS

A continuación se presentan las investigaciones realizadas por diferentes autores donde **se revisó de manera minuciosa** cada una de ellas y se describen el objetivo/alcance general de las mismas, hardware/ software utilizado, las principales conclusiones o resultados de las mismas, lo que fundamenta de manera práctica los beneficios(ventajas) que se pueden obtener al usar RADIUS como servidor de autenticación dentro de una organización, finalmente se presentan los datos relevantes de la implementación de RADIUS como una solución eficiente para solucionar los problemas de control de acceso a las redes inalámbricas. En definitiva, en esta parte se muestran las mejoras

realizadas y las principales contribuciones de los trabajos según el objeto de estudio planteado.

Tabla 2. 11. Trabajos relacionados con la implementación de un Servidor RADIUS

TEMA:	OBJETIVO/ALCANCE	HARDWARE/SOFWARE UTILIZADO	RESULTADOS/CONCLUSIONES	DATOS RELEVANTES
Implementation of network access control using authentication, authorization and accounting protocols (Arana, et al.2013).	Diseño e implementación de un sistema de control de acceso a la red que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA) usando software libre, empleando los protocolos estándar IEEE 802.1x y RADIUS**.**	**Hardware:** Switch Cisco 2950-24, 300 estaciones de trabajos. **Software:** Ubuntu 10.4, FreeRADIUS, MySQL, OpenSSL, OpenLDAP (licencia GNU) y Directorio Activo (AD) Windows.	El sistema se logró: Tres métodos de autenticación mediante el uso de EAP-TLS, PEAP y EAP TTLS. La administración segura de la información, concerniente a los usuarios que pueden acceder la red y los permisos que cada uno de ellos posee; El uso de certificados digitales para demostrar la identidad de un usuario o de un equipo que ejecute cualquiera de los sistemas operativos más populares. (Windows en las versiones XP, Vista y 7, MAC OSX versiones 10.5 a 10.6 y Ubuntu en la versión 10.4.)	Se configuró un servidor RADIUS para que use dos puntos de información de políticas; un servidor de directorio OpenLDAP y el Directorio Activo de Microsoft. Lo anterior posibilita un control de acceso a red escalable, sin demandar un alto presupuesto. Al comparar la solución AAA propuesta con soluciones de control de acceso a red comerciales (por ejemplo, aquellas basadas en dispositivos de los fabricantes Bradford, Fortinet o Cisco), tienen funciones de seguridad adicionales muy particulares, a veces exclusivas, cuyo funcionamiento se complementa (no compite) con la solución planteada.
Implementación de un plan piloto de seguridad bajo el protocolo IEEE 802.X para el Departamento de Gestión Tecnológica del Ministerio de Telecomunicaciones y Sociedad de la Información (Paredes, 2013).	Implementar un nuevo sistema de autenticación y de seguridad para la administración de la red para tener un control de acceso más seguro.	**Hardware:** Switch Cisco 2960 **Software:** Ubuntu 11.04, MySQL, FreeRADIUS, DALO RADIUS.	Se logró con la implementación del estándar IEEE 802.1X mayor seguridad a los recursos que forman parte de la red de la institución. El servidor AAA instalado funciona de acuerdo con los parámetros configurados, dando acceso a todos los usuarios dentro de la base de datos y denegando el ingreso a los servicios a los usuarios que no lo están.	El administrador web que se utilizó para el servidor RADIUS fue DALORADIUS que permitió tener un control eficaz en la red por medio de gráficas ver el consumo de ancho de banda, cantidad de usuarios conectados, los permisos que pueden tener dentro de la red, los recursos de red que los usuarios intentan ingresar y el registro que indica la hora y fecha de los usuarios que están ocupando la red. Los métodos de autenticación que permite el estándar 802.1X son varios, se escogió como métodos ideales por sus características de configuración y seguridad en encriptación y cifrado a EAP-

				MD5 y PEAP, que pueden ser implementadas en conexiones alámbricas e inalámbricas. Los dispositivos que forma parte de la topología de la red son compatibles con el estándar IEEE802.1X, haciendo que la integración con la nueva forma de autenticación sea posible y todos estos puedan tener el acceso a la red.
Diseño de un Modelo de Autenticación RADIUS para reforzar los niveles de seguridad en el díselo de redes inalámbricas IEEE 802.1x para la Cooperativa de Ahorro y Crédito Tumán (Cuanilo y Gonzáles,2013)	Ofrecer un modelo de seguridad en la transferencia de datos de modo seguro, a través de la autenticación RADIUS de tal manera que permita la seguridad de enviar y recibir información.	**Hardware:** Access Point TP-Link TLWA501G AP. **Software:** Ubuntu 11.10, FreeRADIUS 2.1.12, MySQL 5.1, Dolaradius 0.9-9, Apache 2.4.1 y PHP 5.4.0	Con el diseño del modelo se puede evitar la vulnerabilidad en las redes inalámbricas teniendo como defensa a un servidor RADIUS al momento que se conectan los usuarios correspondientes por autenticación, autorización, dado que el modelo brinda una mejor seguridad para la seguridad de datos y conexiones de usuarios ajenos a la red.	La encriptación a nivel de capa de enlace (WEP, WPA, WPA2) es una medida de seguridad comúnmente utilizada pero no garantiza la confiabilidad que debería haber en una red inalámbrica. La supresión del anuncio SSID y el fritado mediante direcciones Mac no son métodos de autenticación seguros. Es necesario un método de seguridad de alto nivel como un servidor RADIUS.
Despliegue del Servicio eduroam en el Campus Universitario de la UNMSM (Calienes, 2015)	Implementar una solución wireless cuya finalidad será permitir el acceso a los usuarios docentes, administrativos y alumnos a los servicios de red por el medio inalámbrico.	**Hardware:** Access Point Cisco 1700 y 3700, switches. Wireless LAN Controller Cisco modelo 5508, estación de trabajo con 1GB de Memoria RAM y un espacio de Disco de 8 GB. **Software:** Secure W2, Sistema Operativo Linux Debian v. 6.0, Sofare de gestión y monitoreo Cisco Prime Infraestructure v. 2.1	El servicio de movilidad eduroam implementado en la UNMSM facilitó el acceso a la información de manera sencilla y segura a investigadores, docentes y estudiantes.	El despliegue del proyecto eduroam en la UNMSM, consiste en registrar los dispositivos access point, ubicados en las Facultades y Dependencias de la Universidad (que soporten el protocolo de autenticación IEEE 802.1x) al servidor RADIUS. La solución cuenta con funcionalidades de Autenticación segura, cifrado y control de acceso usando 802.1x con WPA-Enterprise y WPA2-Enterprise. Soporta los siguientes servidores de autenticación: Base de datos interna, LDAP o SSL Secure LDAP, RADIUS, TACACS.
Diseño e implementación de un sistema de autenticación y	Diseñar e implementar un sistema de autenticación y políticas de	**Hardware:** Switch Core Cisco Modelo 4507, Access Point Cisco AIR-	La implementación de un mecanismo de acceso seguro y	Mediante el uso de los protocolos de autenticación RADIUS, TACACS+ y MAB,

políticas de seguridad mediante un servidor AAA, haciendo uso del estándar IEEE 802.1x y los protocolos RADIUS y TACACS+ para la red corporativa de la empresa proyectos integrales del Ecuador PIL S.A. (Valdivieso, 2015)	seguridad para la red corporativa de la empresa Proyectos integrales del Ecuador PIL.S.A.	CAP2602I-AK9, Router Cisco 2911-V/K9, Controladora Cisco AIR CT2504-15K9, Switch Cisco WS-C4507R+E. **Software:** Secure ACS Cisco, Firewall ASA Cisco.	conjuntamente con las políticas de seguridad Cisco ACS, y los dispositivos utilizados, incremento la movilidad y dos niveles de seguridad al mecanismo de acceso seguro actual con respecto al esquema anterior a nivel LAN y WLAN.	previamente levantados en el servidor de autenticación ACS, se pudo crear diferentes tipos de usuarios previamente registrados en el directorio activo, asociados a políticas de seguridad y autenticación.
Propuesta de una red segura para la interconexión y cooperación de las comisarías y municipalidades de Arequipa utilizando los protocolos VPN Y OLSR con servidor RADIUS y monitoreo NAGIOS (Cárdenas y Quispe, 2015)	Propuesta de una red segura para la interconexión y Cooperación de las Comisarias y Municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor RADIUS y monitoreo NAGIOS.	**Hardware:** Antena Ubiquiti M5, Router Cisco 2811 Wired Router, Acces point TP Linkw8901g, Switch Cisco 2940. **Software:** Sistema de supervisión de red Nagios, DALORADIUS.	Se comprobó la efectividad que brindó el protocolo VPN y servidor RADIUS mediante las pruebas de ejecución para intercomunicar las Municipalidades y Comisarías de la ciudad de Arequipa, en la encriptación de datos y la autenticación de puntos de conexión servidor y cliente.	Que la propuesta de una red segura para la interconexión y cooperación de las Comisarias y Municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor RADIUS y monitoreo NAGIOS, ha sido efectiva en el sentido de la Seguridad de la Red, ya que no cualquier individuo se puede contactarse a la red, sin previa autenticación. Mediante el programa NAGIOS se identificó las fallas más frecuentes y problemas en la arquitectura de la Red a firmando que uno de los problemas más frecuentes es la mala manipulación a los equipos de interconexión.
Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT(Aryeh, et al. 2016)	Administrar la autenticación de usuarios en la Universidad Red inalámbrica de Mines and Technology (UMaT).	**Hardware:** Laptop Dell y router Cisco. **Software:** Virtual Machine, Microsoft Windows 10, FreeBSD, Windows Server 2012 R2, Windows 7 and Windows 8.	El método de autenticación RADIUS combinado con tecnología de portal cautivo fue capaz de lograr los objetivos establecidos de este trabajo. Por lo tanto, no habría ninguna instancia donde las mismas credenciales serían utilizadas por múltiples usuarios.	El experimento realizado demostró cómo lograr la configuración de pfSense portal cautivo y un servidor local RADIUS para usuarios autenticados en una red inalámbrica y asegurar sus credenciales. Solo usuarios con las credenciales de inicio de sesión son capaces de acceder a la Internet.
Diseño e implementación de un sistema de seguridad para el acceso de la red inalámbrica del Colegio Otto Arosemena Gómez"(Allauca, 2016)	Construir un sistema de seguridad que permita el mejoramiento de la red inalámbrica en el consumo de la banda ancha de internet en el	**Hardware:** router TP-LINK TL-MR3220. **Software:** Linux Debian 8, MysQL, pHp5, FrreRadius, Dalo Radius 0.9.	Este sistema permitió que el consumo de la banda ancha de internet mejore en un 80% de su capacidad; con esta mejora en el consumo de internet, se cuenta con	Se ejecutó el aplicativo administrador Daloradius para tener un control total de los usuarios que acceden a la red mediante la autenticación, se pudo restringir el tiempo de conectividad del

	Colegio Fiscal Otto Arosemena Gómez.		un ambiente de conexión segura y eficiente para el acceso de cada uno de los usuarios dentro de la red inalámbrica. Se mejoró el proceso de autenticación de usuarios en la red WI-FI en un 95%, puesto que el colegio no contaba con ninguna restricción y seguridad para los usuarios que accedían a la red.	usuario visitante y se permitió total acceso a los estudiantes y docentes del colegio mediante cada una de las máquinas con tarjeta de red inalámbrica que posee el colegio en su laboratorio de computación.
Administración y gestión de usuarios para acceso a la red inalámbrica de la facultad de Ingeniería en Ciencias Aplicadas basado en el protocolo 802.1x (Cárdenas y Bosmediano, 2017)	Diseño e implementación de un servidor que proporcione Autenticación, Autorización y Auditoria (AAA) en la red inalámbrica de la Facultad de ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, para el control de acceso y administración de recursos de red, empleando soluciones basadas en software libre.	**Hardware:** Mikrotik router 1100 AH, Swicth QPCOM 1240-r. **Software:** Debian 8 FreeRADIUS, OpenLDAP, SecureW2.	La implementación del servidor de Autentificador Radius en la Facultad de Ingeniería en Ciencias Aplicadas (FICA), logró como resultado una gestión centralizada de usuarios mediante un servidor de autentificación seguro. Con la integración del servicio de autentificación se aprovecha al máximo el rendimiento de los dispositivos inalámbricos, logrando autentificar y registrar a diferentes usuarios simultáneamente a través de 802.1x evitando que el servicio caiga por saturación de peticiones en el punto de acceso y otorgando el ingreso solo a usuarios permitidos.	El sistema implementado se encuentra enfocado para todos aquellos dispositivos con soporte del estándar 802.1x, esto debido a que en la actualidad la mayoría de marcas comerciales dan este tipo de soporte nativo, facilitando la integración de seguridad en las redes inalámbricas. Integrando el servidor RADIUS con el directorio LDAP se logró una administración centralizada del sistema AAA, sincronizando las cuentas de usuario de autenticación con los privilegios de acceso para el proceso autorización.
Diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS - LDAP en Linux para fortalecer el acceso de la red de la Clínica Millenium Chiclayo 2016" (Albujar, 2017)	Realizar el diseño de un sistema de seguridad basado en la integración de los servidores RADIUS – LDAP en Linux.	**Hardware:** Routers Cisco 881-K9,880va, 88; Switch Cisco 2960L; Access Point TP-LINK TL WT843N; Firewall Cisco ASA 5520. **Software:** VMWare Workstation 10, Ubuntu Server 14.04 TLS, FreeRadius,SLASP, Packet Tracer 7, JXplorer, SecureW2, Plug-in PGINA.	La integración de los servidores RADIUS – LDAP en la plataforma Linux permitió: Al identificar las vulnerabilidades en la red de la clínica, obtuvimos información necesaria para utilizar las herramientas adecuadas y así fortalecer la seguridad disminuyendo considerablemente las	La creación de usuarios y políticas de acceso a la red, generan el deber de autenticarse si desean consultar o utilizar recursos de la red interna o externa. Mejora el control y distribución de recursos a los usuarios dentro de la red.

			vulnerabilidades mediante los mecanismos presentados en el informe.	
Introducción a un sistema de gestión de accesos a una red Wi-Fi utilizando software libre (Mori, 2017)	Diseño e implementación de un sistema de acceso seguro a la red inalámbrica que contemple la administración de sus usuarios por medio de una plataforma de gestión Web basada en PHP.	**Software:** OpenLDAP, FreeRADIUS, MySQL.	La arquitectura propuesta solucionó el principal problema que se puede desarrollar en la implementación de una red inalámbrica 802.11 de manera segura.	Fue posible la integración de todas las herramientas de software libre utilizadas (FreeRADIUS, OpenLDAP, SAMBA, MySQL) con un dominio desarrollado con Microsoft Windows.
Implementación de un servidor de autenticación RADIUS en un ambiente de pruebas para la red inalámbrica de la UTB-SEDE LAURALES	Implementación de un servidor RADIUS con el fin de proveer servicios AAA en la red inalámbrica de la Universidad Pontificia Bolivariana -sede Laureles.	**Hardware:** PC procesador Intel Pentium IV; 3 Ghz. DD SATA 70 GB; 2 GB RAM; S.O. CentOS 5.5 Controladora Wireless Cisco 4400. **Software:** Free Radius 2.1.7; Active Directory; Windows Server 2003.	La implementación del servidor RADIUS al ambiente de prueba resulto exitosa, pues se obtuvo un escenario en donde se ofrecieron servicios AAA. Los datos sobre el tiempo requerido para acceder a los recursos de red permitieron establecer un promedio de demora en el proceso de conexión de 0,27 segundos. El servicio de contabilidad del servidor RADIUS entregó información valiosa para el seguimiento del uso de los recursos de red.	La implementación de un servidor RADIUS en conjunto con el protocolo WPA2-Enterprise permitió verificar la autenticidad de las identidades provistas, contra un repositorio se usuarios, con el fin de ofrecer el servicio de autenticidad. La política de seguridad de la red inalámbrica universitaria representa un reto para las tareas de gestión, debido a su naturaleza dependiente de la buena fe de los usuarios. Ante esta infraestructura, se realizó un diagnóstico para evidenciar las deficiencias en el esquema de seguridad vigente y proponer una solución especializada.

Fuente: El autor

Es importante mencionar que la presente revisión bibliográfica estructurada en 3 partes, sustentó desde los aportes teóricos y prácticos de las investigaciones de diferentes autores a la consecución de los objetivos, proporcionando al autor pautas a considerar en la realización de las actividades descritas en el desarrollo metodológico del presente trabajo.

CAPÍTULO III. DESARROLLO METODOLÓGICO

El desarrollo metodológico del presente trabajo comienza presentando el diseño de las encuestas y entrevistas realizadas para la recolección de información proporcionada por los usuarios (docentes, administrativos y estudiantes) del sector 8, seguido del muestreo utilizado para su aplicación, la población encuestada, método de observación y la metodología empleada para el desarrollo de los objetivos, dentro de cada uno de ellos se muestran resultados o hallazgos que permitieron definir las conclusiones y recomendaciones.

3.1. DISEÑO DE ENCUESTA Y ENTREVISTA

La elaboración de la entrevista y encuesta se sustenta en las fuentes de información que son parte de la revisión bibliográfica (tesis, artículos científicos y otros documentos), que sirvió como referencia para la inclusión de algunos temas dentro de su estructura. Adicionalmente, se procedió a buscar ejemplos que dentro de su contenido se plantearan temas de organización e infraestructura tecnológica, los mismos que respaldan la pertinencia de los instrumentos elaborados, estas fueron:

- Informe de resultados de la “1° encuesta de seguridad de la información en universidades ecuatorianas miembros de CEDIA, realizada a 29 universidades (CEDIA, 2014).
- Informe del estado de tecnologías de la información y la comunicación en las universidades ecuatorianas, realizada a 37 universidades (CEDIA, 2017).

A continuación, se presenta el diseño de la entrevista y encuestas.

Tabla 3. 1. Diseño de la Entrevista

Fuente: El autor

Estructura de la entrevista
Organización
✓ **Estructura organizativa.**
✓ **Comité de seguridad de la información.**
✓ **Normativa interna de aseguramiento de la información.**
✓ **Manual de funciones y responsabilidades del personal de la unidad.**
✓ **Acuerdo de confidencialidad.**
✓ **Presupuesto para la seguridad de la información institucional.**
Política de seguridad de la información
✓ **Existencia de la política de seguridad de la información.**
✓ **Aprobación de la política.**
✓ **Estándar o norma alineada a la política.**
✓ **Socialización de la política a nivel institucional.**
✓ **Existencia de la política de buen uso de internet.**
Procedimientos
✓ **Procedimientos para efectivizar la política de seguridad de la información.**
✓ **Concientización en temas de seguridad de la información en la institución.**
Redes
✓ **Mecanismos de control para las redes inalámbricas.**
✓ **Acceso de usuarios a las redes inalámbricas.**
✓ **Mecanismos de seguridad para asegurar la información.**
Autenticación
✓ **Sistema de autenticación.**
Autorización
✓ **Procesos para autorización a las redes inalámbricas a usuarios.**
Auditoría
✓ **Control o monitoreo de las actividades de los usuarios al ser uso de la red inalámbrica.**
Amenazas y vulnerabilidades
✓ **Herramientas de análisis de vulnerabilidades.**
✓ **Incidentes ocurridos en la seguridad de la información.**
Plano de distribución de la red
✓ **Distribución lógica y física de la red.**
Servicios y recursos
✓ **Servicios y recursos de usuarios.**
✓ **Roles y privilegios para acceso a sistemas.**

Tabla 3. 2. Diseño de la Encuesta

Estructura de la encuesta
Organización
✓ **Acuerdo de confidencialidad.**
Política de seguridad de la información
✓ **Existencia de la política de seguridad de la información.**
✓ **Socialización de la política a nivel institucional.**

✓ **Existencia de la política de buen uso de internet.**
Procedimientos
✓ **Procedimientos para efectivizar la política de seguridad de la información.**
✓ **Concientización en temas de seguridad de la información en la institución.**
Redes
✓ **Acceso de usuarios a las redes inalámbricas.**
Servicios y recursos
✓ **Servicios y recursos de usuarios.**
Seguridad de la información
✓ **Percepción de la seguridad de la información por parte de los usuarios.**

Fuente: El autor

3.2. MUESTREO

El muestreo utilizado para la aplicación de las encuestas fue el muestreo por conglomerados, según Ozten y Manterola (2017), en este tipo de muestreo, los sujetos a estudio, se encuentran incluidos en lugares físicos o geográficos (conglomerados); por ende, resulta imprescindible diferenciar entre sujetos a estudio (quiénes va a ser medidos) y unidad muestral (conglomerado a través del cual se logra acceder a los sujetos a estudio).

3.3. POBLACIÓN

La población encuestada fue la siguiente:

Tabla 3. 3. Población encuestada por área

Área	Usuarios	Cantidad
Edificio de Bibliotecas	Docentes	5
	Administrativos	24
	Estudiantes	175
Edificio de Carrera de Computación	Docentes	20
	Administrativos	6
	Estudiantes	92
Edificio de Posgrado	Docentes	5
	Administrativos	6
	Estudiantes	113
Total		446

Fuente: El auto

3.4. MÉTODO DE OBSERVACIÓN

El autor a través de este método pudo visualizar y registrar algunos hechos tal y como suceden, lo que aportó información directa del problema tal como el uso indiscriminado que se le da a los recursos de red, como también a la propagación de las claves de las redes inalámbricas al no contar con procedimientos formales para su divulgación, entre otros, lo que se puede corroborar con los resultados de la encuesta realizada a los usuarios.

La metodología utilizada para el desarrollo de los objetivos de la investigación fue:

3.5. METODOLOGÍA EDER

Se utilizó la metodología EDER (Estudio, Diseño, Ejecución y Revisión), misma que permitió el cumplimiento de los objetivos establecidos. Según Morales *et al.* (2018), EDER es una metodología aplicable a proyectos de infraestructura tecnológica, sencilla, fácil de comprender y aplicar, y que al mismo tiempo cumpla con todos los ámbitos que requieren los proyectos tecnológicos en su ejecución. En la metodología EDER se establecen 4 etapas, las mismas que actúan directamente en la ejecución técnica de todo trabajo de infraestructura tecnológica, las que se muestran a continuación.

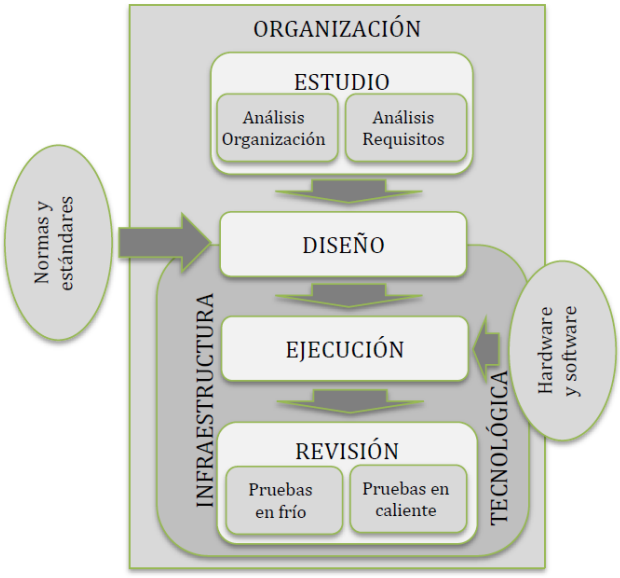


Figura 3. 1. Etapas y actividades de la metodología EDER

3.6. DESARROLLO DE LOS OBJETIVOS DE LA INVESTIGACIÓN

A continuación, se describen el desarrollo de los objetivos de la investigación:

3.6.1. ANÁLISIS DE LA SITUACIÓN ACTUAL SOBRE EL ACCESO Y SEGURIDAD DE LAS REDES INALÁMBRICAS DE LA ESPAM MFL

Para el desarrollo de este objetivo se entrevistó el día 14 de febrero de 2019 al Licenciado Geovanny García Montes, Coordinador de la Unidad de Tecnología de la ESPAM MFL (UTI), y al personal que está a cargo de las redes inalámbricas y Data Center: Ingeniero Patricio Zambrano, supervisor de redes, técnico de redes e Ingeniero César Moreira Administrador de Data Center y se encuestó a docentes, administrativos y estudiantes del Sector 8.

Este primer objetivo dio a conocer como está constituida organizativamente la UTI, (estructura orgánica, competencias y funciones del personal a cargo de las redes inalámbricas), aplicación de políticas, normativas, mecanismos, procedimientos y procesos establecidos para efectivizar la seguridad de la información, lo cual se contrasta con el grado de conocimiento de la existencia de las mismas por parte de los usuarios y se presentan los datos más relevantes obtenidos en las entrevista.

ORGANIZACIÓN INTERNA DE LA UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL

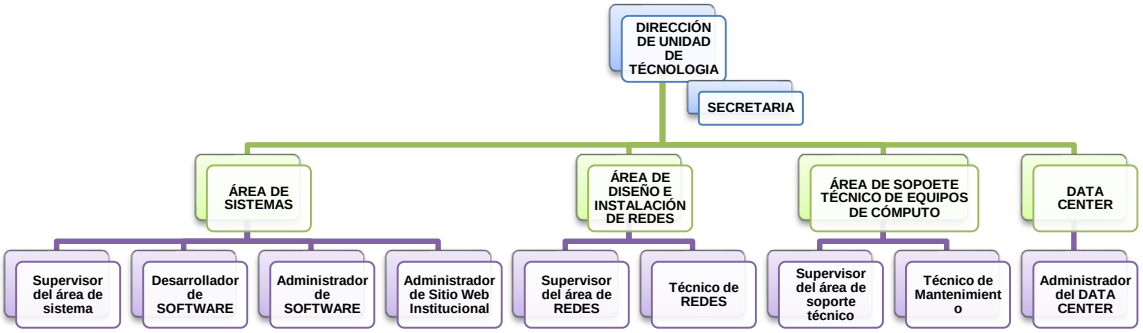


Figura 3. 2. Organigrama de la Unidad de Tecnología de la ESPAM MFL

Fuente: El autor

Los resultados de la aplicación de las entrevistas al personal de la UTI y de las encuestas realizadas a los usuarios fueron enmarcados dentro de las siguientes dimensiones y secciones:

Dimensión: Organización interna

Sección: Estructura orgánica

Dimensión: Políticas

Sección: Políticas de aseguramiento de la información

Sección: Políticas del buen uso del internet

Sección: Acceso a las redes inalámbricas

Dimensión: Normativa

Sección: Aseguramiento de la información institucional.

Dimensión: Mecanismos de seguridad

Sección: Autenticación

A continuación, se presenta lo anteriormente mencionado:

Tabla 3. 4. Dimensión organización interna.

Dimensión: ***Organización interna***			
Sección: ***Estructura orgánica***	**Funciones y responsabilidades**		
	Área de Diseño e Instalación		**Área de Data center**
	Supervisor de redes	**Técnico de redes**	**Administrador de data center**
• ¿La unidad de tecnología cuenta con una estructura organizativa? ***• ¿Existe un manual de funciones y responsabilidades del personal de la Unidad de tecnología de la ESPAM MFL?***	**Competencias genéricas del cargo**:		
	• El supervisor del área de redes tendrá a su responsabilidad coordinar las acciones de planificación, diseño e instalación de redes de datos a nivel institucional. • El supervisor del área de redes deberá coordinar actividades para el respectivo mantenimiento y soporte de las redes.	• El técnico de se encargará de realizar las instalaciones y brindar el soporte técnico requerido en el área de redes.	• El administrador del Data Center deberá establecer estrategias y procedimientos que garanticen la disponibilidad, integridad y seguridad de la información. • El administrador del Data Center será responsable de administrar todo lo relacionado con el acceso y manejo de servidores, dominios y otras plataformas tecnológicas que se utilicen en la institución, como correo electrónico institucional.
	Funciones inherentes al cargo se pueden observar:		
	• Realizar planes de contingencia y propuestas para el mejoramiento de redes y cableado estructurado. • Tener un control de registro de las direcciones IP que utilizan los usuarios en la red. • Realizar un registro de las actividades realizadas en la red.	• Realizar las configuraciones de los equipos. • Dar soporte técnico a las redes de la institución.	• Establecer políticas de seguridad, privacidad, integridad y respaldo de datos. • Implementar los mecanismos de seguridad de las cuentas, asegurando la confidencialidad de la información. • Investigar y asesorar en la consecución de nuevas tecnologías para mejorar la infraestructura tecnológica de la Institución.

Fuente: Manual de puestos y funcio**ne**s de la Unidad de Tecnología de la ESPAM MFL.

Tabla 3. 5. Dimensión políticas.

Dimensión: ***Políticas***			
Sección: ***Políticas de seguridad de la información***			
Pregunta	**Respuestas obtenidas en la entrevista**	**Análisis de las respuestas obtenidas en las encuestas**	
1.- ¿Existe una política de seguridad de la información institucional?	La política está aprobada por el HCP.	El 24% de los usuarios conocen de su existencia.	Mientras que el 76% de los usuarios no conocen de su existencia.
		El 15% de los usuarios conocen que se ha socializado la política.	Mientras que el 85% los usuarios no conocen sobre la socialización.
Sección: ***Políticas para el buen uso del internet***			
2.- ¿Existe una política del buen uso del internet?	La política está aprobada por el HCP.	El 34% de los usuarios conocen de su existencia.	Mientras que el 66% de los usuarios no conocen de su existencia.
	Contenido de la política	**Análisis de las respuestas obtenidas en las encuestas**	
	El servicio de internet solo será utilizado por personal administrativo, docentes y estudiantes para fines laborales, consultas e investigaciones, accediendo a sitios de carácter académico y científico.	El 74% de los usuarios utilizan el internet para acceder al sistema de gestión academia (SGA), el 44% al sistema de gestión de encuestas, el 61% a bibliotecas virtuales, el 55% al sitio web institucional y el 77% accede al correo electrónico.	
	Los usuarios no deben ingresar a páginas con contenido pornográfico, de entretenimiento u otros que no estén relacionados con las actividades laborales de la ESPAM MFL.	El 9% de los usuarios utilizan el internet para acceder a páginas con contenidos para adultos.	
	Los usuarios no deberán descargar videos, imágenes, música o programas gratuitos sin licencias que oferten en la web.	El 19% de los usuarios utilizan el internet para acceder a juegos en línea, el 15% a páginas de descarga de películas y el 64% para acceder a YouTube.	
	Los usuarios tienen prohibido el uso de chat o acceder a páginas de redes sociales como Facebook, LinkedIn, Instagram, Twitter, entre otro excepto personal autorizado por la máxima autoridad.	El 46% de los usuarios utiliza el internet para acceder a Facebook, el 23% a Instagram, el 13% a Twitter y el 22% para acceder a otras redes sociales.	

	La Unidad de Tecnología bloqueara páginas web de redes sociales, entretenimiento u otras, para evitar el consumo excesivo de ancho de banda del internet.	
	Los usuarios no deberán utilizar el internet para realizar llamadas internacionales o conferencias a través de programas online, como Skype, Hangouts, WhatsApp u otros.	El 8% de los usuarios utiliza el internet para acceder a sistema de mensajería instantánea como WhatsApp u otros.

Sección: ***Acceso a redes inalámbricas***		
Pregunta	**Respuestas obtenidas en la entrevista**	**Análisis de las respuestas obtenidas en las encuestas**
3.- ¿Qué mecanismos de control se implementan para el acceso a las redes inalámbricas?	Se utilizan claves WEP, WPA Y WPA2 en la actualidad.	El 28% de los usuarios acceden a una red inalámbrica utilizando una clave.
	Contenido de la política de acceso a redes inalámbricas	**Análisis de las respuestas obtenidas en las encuestas**
	El UTI proveerá del servicio de red inalámbrica a los docentes y a la comunidad estudiantil de la ESPAM MFL en el campus politécnico.	El 41% de los usuarios acceden a una red inalámbrica por medio de una computadora portátil, mientras que el 59% accede por medio de dispositivos como Smartphone, Tablet u otro.
	Los usuarios que cuenten con un dispositivo móvil, sea este un celular, Tablet o laptop, podrán acceder a la red inalámbrica, para realizar trabajos académicos como investigación y consultas.	

Tabla 3. 6. Dimensión normativas.

Dimensión: ***Normativas***			
Sección: ***Aseguramiento de la información institucional***			
Pregunta	**Respuestas obtenidas en la entrevista**	**Análisis de las respuestas obtenidas en las encuestas**	
4.- ¿Existe una normativa interna para el aseguramiento de la información institucional?	La normativa está aprobada por el HCP.	El 28% de los usuarios conocen que se ha concientizado sobre temas de seguridad de la información.	Mientras que el 72% de los usuarios no conocen que se haya concientizado sobre temas de seguridad de la información.
	No se establecen acuerdos de confidencialidad para el buen tratamiento de la información.	El 13% de los usuarios conocen que se celebra acuerdos de confidencialidad.	Mientras que el 87% de los usuarios no conocen que se celebren acuerdos de confidencialidad.
		El 9% de los usuarios perciben que no está nada segura la información dentro de la institución, mientras que el 45% es poco segura, el 41% segura y el 4% muy segura.	
	Contenido del reglamento de aseguramiento y gestión de información	**Respuesta obtenida en las entrevistas**	
	La UTI controlara el acceso a la red y servidores de la ESPAM MFL, de acuerdo a las necesidades del usuario.	No existen procesos definidos para atender solicitudes de autorización para el acceso a las redes inalámbricas a los usuarios.	
	Los usuarios tienen prohibido ejecutar alguna forma de monitoreo en la red, la cual intercepte datos que hayan sido destinados a otros usuarios.	No se utiliza un control o monitoreo de las actividades que los usuarios cuando acceden a la red inalámbrica, solo se puede ver el número de usuario conectados.	
	Los usuarios no deberán evadir la autenticación de usuario o cualquier seguridad de algún equipo, red o cuenta de usuario propiedad de la ESPAM MFL.		
	La UTI monitoreara la red inalámbrica mediante análisis de tráfico, detectando usos indebidos del servicio y así mantener en buen funcionamiento la red.		
	Los usuarios tienen prohibido utilizar cualquier equipo de cómputo propiedad de la ESPAM MFL conectado a la red de datos, para la distribución de cualquier tipo de software maligno o material pornográfico que valla en contra de la moral y las buenas costumbres.	No se utiliza ninguna herramienta de análisis de vulnerabilidades.	
	Contenido del reglamento de y gestión de Información	**Análisis de las respuestas obtenidas en las encuestas**	
	El personal administrativo y docente no deberá revelar la clave de su cuenta de usuario de red a terceras personas, esto incluye a cualquier miembro de su familia, compañero de trabajo o persona externa que se encuentre realizando actividades propias dentro de la institución.	El 57% le comparten la clave de acceso.	
	Los usuarios no deberán evadir la autenticación de usuario o cualquier seguridad de algún equipo, red o cuenta de usuario propiedad de la ESPAM MFL.	El 52% tienen acceso libre.	

Tabla 3.7. Dimensión mecanismos de seguridad.

Dimensión: *Mecanismos de seguridad*		
Sección: *Autenticación*		
Pregunta	**Respuestas obtenidas en la entrevista**	**Análisis de las respuestas obtenidas en las encuestas**
¿Existe utiliza un sistema de autenticación de doble factor?	No se utiliza un sistema de autenticación.	El 20% de los usuarios acceden a una red inalámbrica utilizando usuario y contraseña.
	Contenido del reglamento de aseguramiento y gestión de información	**Análisis de las respuestas obtenidas**
	La UTI para evitar que intrusos puedan acceder a la red inalámbrica ha creado el portal cautivo para la autenticación de acceso a los estudiantes y personal administrativo docentes.	El 20% de los usuarios aseguran que al momento de acceder a una red inalámbrica utilizan un usuario y contraseña, sin embargo, al contrastar la respuesta que se obtuvo en la entrevista con el personal de la UTI no existe en la universidad implementado ningún sistema de autenticación, por lo que este porcentaje no es real.
	Los usuarios tendrán acceso a la red de datos mediante la autenticación de usuario y contraseña provistos por la UTI.	
	La UTI proporcionara el usuario y clave de acceso al portal cautivo a las autoridades y directores de carreras de la ESPAM MFL y estos a su vez lo socialicen a los estudiantes y docentes.	
	Los usuarios deberán ingresar a la red inalámbrica a través del portal cautivo de la ESPAM MFL, ingresando el usuario y clave socializado con anterioridades.	
	Los usuarios no deberán proporcionar las credenciales (usuario y clave) del portal cautivo a personas ajena a la ESPAM MFL.	

Fuente: Reglamento y aseguramiento de la información de la ESPAM MFL/ resultados de entrevistas y encuestas realizadas a personal del área tecnológica y a usuarios.

Una vez obtenidos estos resultados se procedió a contrastarlos con lo establecido en normas que dentro de su marco conceptual hace referencia a lineamientos y directrices que se deben cumplir en la organización e infraestructura tecnológica de las entidades, organismos del sector público y personas jurídicas de derecho privado. Estas normas fueron:

- Normas del control interno de la contraloría general del estado 410 TECNOLOGÍAS DE LA INFORMACIÓN (Contraloría General del Estado, 2014).
- Norma ISO 27002(ISO 27002.es, 2015).

Tabla 3.8. Análisis general de la situación actual de la organización TI según norma de control interno de la contraloría general del estado.

Norma de control interno de la contraloría general del estado	Cumplimiento		
410-01. Organización informática	**Si**	**No**	**Parcialmente**
La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.	X		
Se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.	X		
410-02. Segregación de funciones			
Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.			X
La descripción documentada y aprobada de los puestos de trabajo que conforman la Unidad de Tecnología de Información, contemplará los deberes y responsabilidades, así como las habilidades y experiencias necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de			X

personal clave.			
410-16. Comité informático			
La definición clara de los objetivos que persigue la creación de un Comité de Informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.		X	
La conformación y funciones de su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.		X	
410-04. Políticas y procedimientos			
La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.	X		
La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.			X
Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales, además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.			X
410-10. Seguridad de tecnología de información			
Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.		X	
410-12. Administración de soporte de tecnología de información			
Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen			X

con los sistemas y servicios de tecnología de información de la entidad.			
Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.		X	

Fuente: El autor

Tabla 3.9. Análisis general de la situación actual de la organización TI según Norma ISO 27002.

Norma ISO 27002	**Cumplimiento**		
Control de acceso	**Si**	**No**	**Parcialmente**
1. Requerimientos de negocio para el control de accesos: Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización. **Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.**			X
1.1. Política de control de acceso: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.			X
2. Gestión de acceso de usuario: Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. **Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.**		X	
2.1. Registro de usuario: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información		X	
2.2. Gestión de privilegios: Se debería restringir y controlar la asignación y uso de los privilegios.	X		
2.3. Gestión de contraseñas de usuario: Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal.		X	
2.4. Revisión de los derechos de acceso de los usuarios: El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.		X	
3. Responsabilidades del usuario: Se deberá impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.		X	
3.1. Uso de contraseña: Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.			X
4. Control de acceso de red: Impedir el acceso no autorizado a los servicios en red.			X
Se deberían controlar los accesos a servicios internos y externos conectados en red:			

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:		
a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;		X
b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;	X	
c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.	X	
4.1. Política de uso de los servicios de red: Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	X	
4.2. Autenticación de usuario para conexiones externas: Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.	X	
4.3. Autenticación de nodos de la red: Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos.	X	
4.4. Control de conexión a las redes: En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.	X	
Gestión de comunicaciones y operaciones		
1. Gestión de redes: La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección. Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas.	X	
1.1. Controles de red: Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.		X
1.2. Seguridad en los servicios de red: Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.		X

Fuente: El autor

Una vez que se procesó la información, se pudo determinar lo siguiente:

Tabla 3.10. Resultados del análisis de la organización TI

Dimensión	Análisis de la organización
Estructura orgánica y organización interna	La Unidad de Tecnología cuenta con una estructura organizacional que consta de 4 áreas establecidas en las que se incluye el área de diseño e instalación de redes, su personal a cargo cuenta con funciones y responsabilidades definidas.
	Sin embargo, la institución no cuenta con un comité informático que se encargue de la toma de decisiones referente a la implementación de controles y herramientas para mejorar la seguridad de la información institucional.
Políticas y procedimientos	La Unidad de Tecnología cuenta con un Reglamento de aseguramiento y gestión de la información aprobado por el Honorable Consejo Politécnico (HCP) donde se han definido políticas y se han establecidos procedimientos para la seguridad de la información, controles internos entre otros elementos, a pesar de que están descritos y en el caso particular en el acceso y seguridad de las redes inalámbricas hay procedimientos que la unidad debe seguir y no las ha ejecutado y tampoco han sido difundidos a docentes, personal administrativos y estudiantes desconociendo su contenido, alcance y restricciones.
Implantación de mecanismos de seguridad	El mecanismo de acceso a las redes inalámbricas implementado actualmente son las claves de seguridad, al no ejecutarse procesos para atender solicitudes de autorización, no se puede controlar la propagación de las mismas.
	No se realiza un control o monitoreo de las actividades que los usuarios realizan cuando acceden a las redes inalámbricas, solo se puede observar el número de usuarios conectados.
	No existen restricciones en el uso de los recursos de red, los usuarios acceden a sitios que no son para fines académicos o administrativos.
	Dentro de su normativa interna, la UTI establece la implementación de un portal cautivo como mecanismo de control de acceso a las redes, pero hasta la actualidad no ha sido puesta en marcha.

Fuente: El autor

De manera general se pudo observar que la Unidad de tecnología de la ESPAM MFL no cumple totalmente con algunos de los procedimientos y proceso establecidos, ni la implementación de mecanismos propuestos dentro de su normativa interna para efectivizar la política de seguridad de la información, buen uso del internet y de control de acceso a las redes inalámbricas, así como también el cumplimiento parcial e incumplimiento de lineamientos descritos en la Norma de Control Interno de la Contraloría General del Estado y la Norma ISO 27002.

CARATERIZACIÓN DE REDES Y PUNTOS DE ACCESOS INALÁMBRICOS

El Sector 8 del Campus Politécnico de La ESPAM MFL comprende la plaza mayor y los edificios de Biblioteca, carrera de Computación, Posgrado y Hotel-Laboratorio El Higuerón, debido a que en este lugar funcionan muchas unidades administrativas y académicas, lo convierten en un punto de gran afluencia de usuarios (docentes, administrativos y estudiantes) que hacen uso de las redes inalámbricas disponibles.

A continuación, se muestra la topología de red con la que cuenta el Sector 8.

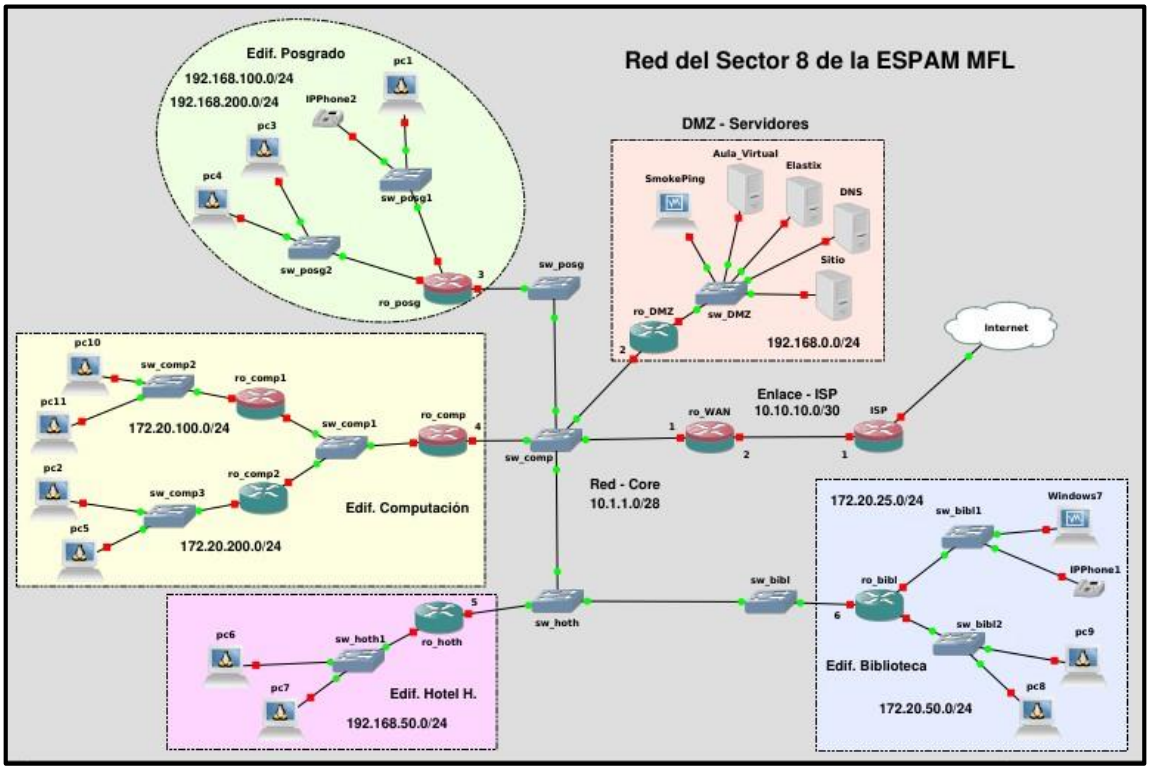


Figura 3.3. Diseño de la topología de red con la que cuenta el Sector 8 de la ESPAM MFL.

Para la caracterización de las redes inalámbricas del Sector 8 se utilizó el software Acrylic Wi-Fi Home de distribución gratuita, que permite realizar la monitorización de redes Wi-Fi para sistemas Windows, permitiendo la visualizar información Wi-Fi en tiempo real, también se puede obtener información sobre

el tipo de seguridad de la red, puntos de acceso, nivel de señal, análisis de distribución de redes inalámbricas y canales y el software Acrylic Wi-Fi Head Maps, que permite diseñar, analizar y detectar problemas Wi-Fi fácilmente y generar informes, funciona definiendo localizaciones (edificios, plantas, perímetro interno y perímetro externo) a las que se asocian planos o un área geográfica concreta, el sistema captura el tráfico Wi-Fi y almacena información detallada de los dispositivos, su nivel de señal, así como otros datos relevantes (Acrylic Wi-Fi Sofware, 2019).

DETECCIÓN DE REDES INALÁMBRICAS

Para la detección de las redes inalámbricas y puntos de acceso en el Sector 8 se tomaron tres para lo cual se tomaron tres puntos de georreferenciación: edificio de la Bibliotecas, edificio de Carrera de Computación y edifico de Posgrado como se puede visualizar en la siguiente imagen:

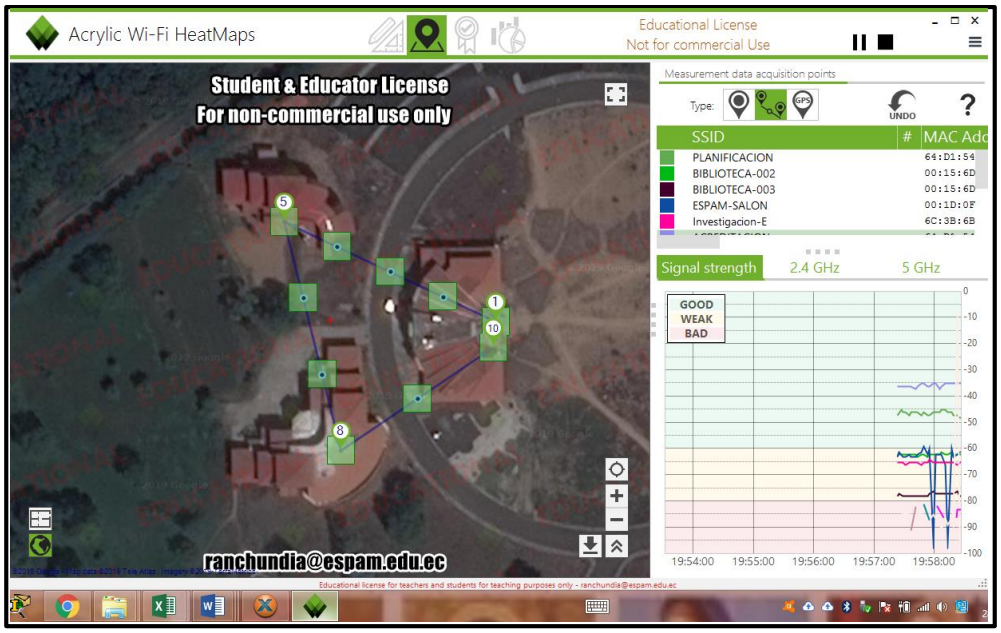


Figura 3.4 Puntos de georreferenciación en el área del Sector 8 de la ESPAM MFML.

RESULTADO DEL MONITOREO DE LAS REDES INALÁMBRICAS

La siguiente tabla contiene información relevante sobre las redes detectadas durante el monitoreo:

- **SSID:** Identificador de la red.
- **BSSID:** Identificador único del dispositivo
- **Canal:** Número de canal donde la red está funcionando.
- **Frecuencia:** Frecuencia en Mhz en la cual se encuentra el canal de la red.
- **RSSI Medio:** Media de la intensidad de señal detectada durante el estudio de cada dispositivo.
- **RSSI Máximo:** Máxima intensidad de señal detectada durante el estudio de cada dispositivo.
- **RSSI Mínimo:** Mínima intensidad de señal detectada durante el estudio de cada dispositivo.
- **Seguridad:** Tipos de autenticación y cifrado soportado por la red.
- **WPS:**
- Versión WPS que soporta la red.

En la siguiente tabla se pueden observar las redes Wi-Fi encontradas.

Tabla 3.11. Caracterización de las redes inalámbricas del Sector 8 de la ESPAM MFL.

SSID	BSSID	CANAL	FREC	RSSI MEDIO	RSSI MAX	RSSI MIN	SEGURIDAD	WPS
[Hidden]	02:9F:C2:3D:31:AF	1	2412	-82	-68	-95	WPA2 Personal-CCMP	
	02:9F:C2:3E:31:AF	36	5180	-79	-71	-88	WPA2 Personal-CCMP	
	8A:8A:20:81:1C:B9	6	2437	-72	-66	-95	WPA2 Personal-CCMP	
	8A:8A:20:82:1C:B9	149	5745	-81	-81	-81	WPA2 Personal-CCMP	
	C8:B3:73:59:71:02	6	2437	-92	-85	-95	Open	

	D4:6E:0E:43:27:EA	153	5765	-86	-85	-89	Open	
ACREDITACION	64:D1:54:E5:29:A1	1	2412	-63	-34	-95	WPA2 Personal-CCMP	1.0
ADMINISTRACION-A	CC:2D:E0:0F:3F:6B	6	2437	-71	-57	-95	WPA2 Personal-CCMP	1.0
ADMINISTRACION-B	CC:2D:E0:0F:3B:57	4	2427	-83	-69	-95	WPA2 Personal-CCMP	1.0
AGROINDUSTRA-II	CC:2D:E0:0F:3E:B1	2	2417	-74	-57	-95	WPA2 Personal-CCMP	1.0
AGROINDUSTRIA-I	CC:2D:E0:0F:3E:BD	2	2417	-75	-63	-95	WPA2 Personal-CCMP	1.0
AULA-7	64:D1:54:E5:3F:31	1	2412	-88	-88	-88	Open	
BIBLIOTECA-001	00:15:6D:10:6E:32	8	2447	-86	-86	-86	Open	
BIBLIOTECA-002	00:15:6D:10:6E:27	6	2437	-70	-61	-85	Open	
BIBLIOTECA-003	00:15:6D:10:6E:21	8	2447	-79	-77	-86	Open	
CAAI	C8:B3:73:59:7C:9C	1	2412	-81	-69	-95	WPA Personal-(TKIP|CCMP) WPA2 Personal-(TKIP|CCMP)	1.0
	C8:B3:73:59:7C:9D	157	5785	-81	-80	-82	WPA Personal-(TKIP|CCMP) WPA2 Personal-(TKIP|CCMP)	1.0
COOR-ACADEMICA	98:FC:11:B1:73:B5	11	2462	-85	-85	-86	WPA2 Personal-CCMP	1.0
DIRECT-44039B3D	46:D2:44:03:1B:3D	6	2437	-84	-77	-95	WPA2 Personal-CCMP	1.0
DIRECT-Oh-BRAVIA	DA:5D:E2:6F:13:3D	11	2462	-72	-63	-95	WPA2 Personal-CCMP	1.0
EMPRENDIMIENTO	C4:E9:84:D1:51:32	10	2457	-72	-62	-91	WPA2 Personal-(TKIP|CCMP)	
ESPAM-BIBLIOTECA1	00:27:22:46:80:D1	157	5785	-82	-77	-85	WPA2 Personal-(TKIP|CCMP)	

ESPAM-EP	C0:56:27:49:FC:23	6	2437	-85	-82	-89	WPA2 Personal-CCMP	1.0
ESPAM-SALON	00:1D:0F:CC:22:4E	11	2462	-81	-57	-95	WPA Personal-(TKIP|CCMP) WPA2 Personal-(TKIP|CCMP)	
ESTUDIANTES	64:D1:54:9C:EA:B3	2	2417	-61	-48	-90	Open	
	64:D1:54:9F:15:47	1	2412	-75	-48	-95	Open	
	64:D1:54:A0:2A:CD	6	2437	-81	-72	-95	Open	
	64:D1:54:A0:2B:6F	1	2412	-80	-68	-95	Open	
	64:D1:54:A2:C5:21	3	2422	-88	-80	-95	Open	
	78:8A:20:81:1C:B9	6	2437	-79	-68	-95	Open	
	78:8A:20:81:22:EE	6	2437	-88	-79	-95	Open	
	78:8A:20:81:80:6F	11	2462	-91	-76	-95	Open	
	78:8A:20:82:1C:B9	149	5745	-80	-80	-81	Open	
	78:8A:20:82:22:EE	36	5180	-89	-88	-91	Open	
	78:8A:20:82:80:6F	149	5745	-86	-84	-89	Open	
	98:FC:11:B1:74:1F	10	2457	-67	-58	-95	Open	1.0
	98:FC:11:B1:B4:C7	11	2462	-88	-76	-95	Open	1.0
	C8:B3:73:59:71:03	149	5745	-89	-88	-90	Open	
	F0:9F:C2:3D:31:AF	1	2412	-77	-62	-95	Open	
	F0:9F:C2:3E:31:AF	36	5180	-78	-71	-89	Open	
	FC:EC:DA:8A:F7:00	6	2437	-69	-53	-95	Open	
	FC:EC:DA:8B:F7:00	157	5785	-69	-69	-71	Open	
IDIOMAS	C4:6E:1F:DE:18:72	6	2437	-84	-82	-88	WPA2 Personal-CCMP	1.0
INVESTIGACION-E	6C:3B:6B:8C:FB:52	1	2412	-69	-64	-95	WPA Personal-CCMP WPA2 Personal-CCMP	

M-Ambiente2A	86:E9:84:D1:51:04	10	2457	-69	-59	-85	WPA2 Personal-CCMP	
NO-DISPONIBLE	0C:80:63:6B:5E:7A	9	2452	-92	-84	-95	WPA2 Personal-CCMP	1.0
OFICINA DIRECCION	14:CC:20:5E:60:96	6	2437	-75	-58	-95	WPA Personal-CCMP WPA2 Personal-CCMP	
	14:CC:20:5E:60:97	36	5180	-85	-83	-89	WPA Personal-CCMP WPA2 Personal-CCMP	1.0
PLANIFICACION	64:D1:54:9F:14:63	1	2412	-50	-45	-90	WPA2 Personal-CCMP	1.0
POSGRADO	C4:E9:84:D1:51:04	10	2457	-69	-60	-95	WPA2 Personal-(TKIP|CCMP)	
PROFESORES	7A:8A:20:81:1C:B9	6	2437	-69	-66	-73	Open	
	7A:8A:20:81:22:EE	6	2437	-91	-83	-95	Open	
	7A:8A:20:81:80:6F	11	2462	-89	-67	-95	Open	
	7A:8A:20:82:1C:B9	149	5745	-80	-79	-81	Open	
	7A:8A:20:82:80:6F	149	5745	-87	-85	-89	Open	
	F2:9F:C2:3D:31:AF	1	2412	-81	-61	-95	Open	
	F2:9F:C2:3E:31:AF	36	5180	-78	-70	-88	Open	
	FE:EC:DA:8A:F7:00	6	2437	-66	-54	-95	Open	
	FE:EC:DA:8B:F7:00	157	5785	-69	-69	-70	Open	
RECAF	C0:56:27:4A:02:86	11	2462	-82	-67	-95	WPA2 Personal-CCMP	
SALON-MFL	20:AA:4B:55:94:3D	6	2437	-84	-74	-95	WPA Personal-(TKIP|CCMP) WPA2 Personal-(TKIP|CCMP)	
SYSKONTROL	C4:E9:84:C1:5A:90	7	2442	-66	-60	-95	WPA2 Personal-CCMP	1.0

TT-HH	64:D1:54:34:BF:0E	10	2457	-79	-73	-93	WPA2 Personal-CCMP	1.0
TURISMO	CC:2D:E0:0F:3F:8F	3	2422	-80	-71	-95	WPA2 Personal-CCMP	1.0
UPS DESARROLLO	D4:6E:0E:43:27:EB	11	2462	-80	-56	-95	WPA2 Personal-CCMP	
USUARIO-PC_Network_1	B4:75:0E:89:6E:F4	1	2412	-93	-84	-95	WPA2 Personal-CCMP	1.0
YANDY-RESTAURANT	00:23:69:52:B8:CC	6	2437	-95	-95	-95	WPA Personal-TKIP WPA2 Personal-TKIP	
ZOOTECNIA	CC:2D:E0:0F:3B:15	8	2447	-81	-65	-95	WPA2 Personal-CCMP	1.0

Fuente: el autor

DETECCIÓN DE LOS PUNTOS DE ACCESO

También se realizó el monitoreo de los puntos de acceso que se encuentra en esta área, tal como se presenta en la siguiente imagen:

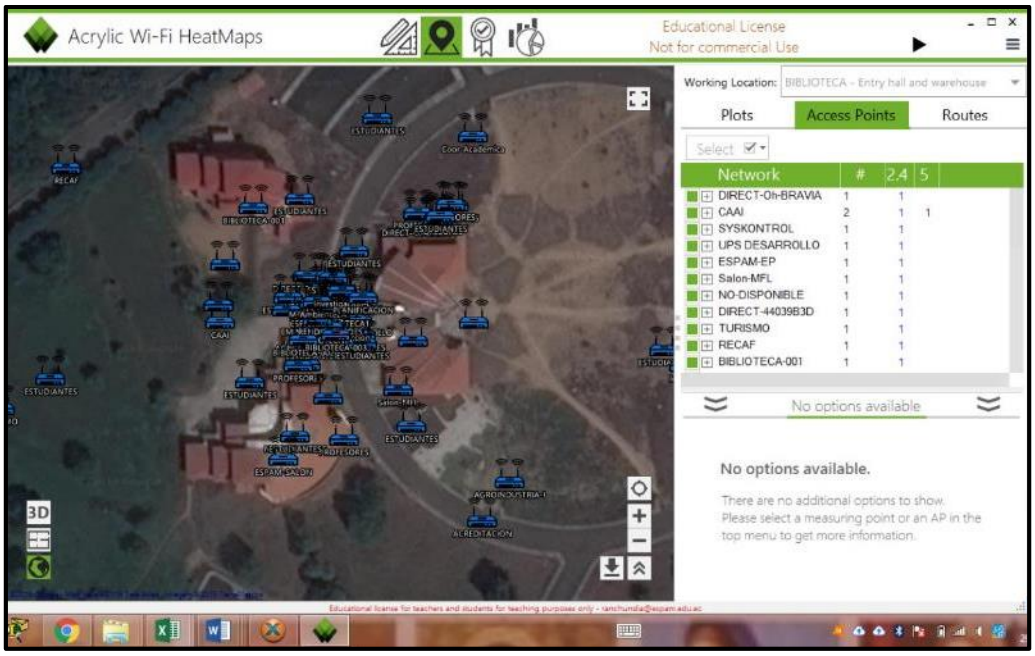


Figura 3.5. Puntos de accesos encontrados a las redes inalámbricas en el área del Sector 8 de la ESPAM MFL

Una vez realizado el monitoreo se puede visualizar las características de los puntos de acceso tal como se presentan en la siguiente imagen.

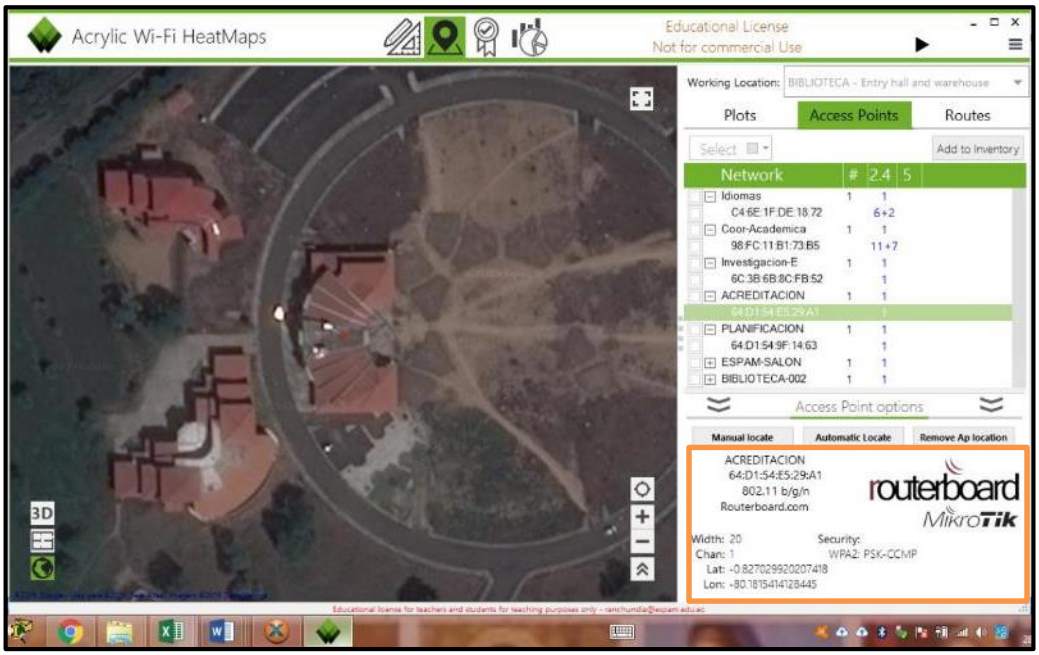


Figura 3.6. Características de puntos de accesos encontrados a las redes inalámbricas en el área del Sector 8 de la ESPAM MFL.

RESULTADO DEL MONITOREO DE LOS EQUIPOS INALÁMBRICOS DEL SECTOR 8 DE LA ESPAM MFL

A continuación, se muestra la información sobre los puntos de acceso detectados durante el monitoreo:

- **SSID:** Identificador de la red.
- **BSSID:** Identificador único del dispositivo
- **Fabricante:** Fabricante del dispositivo.
- **802.11:** Estándar soportado.
- **Canal:** Número de canal donde la red está funcionando.

En la siguiente tabla se puede observar los equipos inalámbricos encontrados.

Tabla 3.12. Caracterización de los equipos inalámbricos del Sector 8 de la ESPAM MFL.

	SSID	BSSID	FABRICANTE	802.11	CANAL
1	[Hidden]	02:9F:C2:3E:31:AF	Cisco-Linksys. LLC	a, n, ac	36
		C8:B3:73:59:71:02		b, g, n	6
		8A:8A:20:82:1C:B9		a, n, ac	149
		8A:8A:20:81:1C:B9		b, g, n	6
		02:9F:C2:3D:31:AF		b, g, n	1
		D4:6E:0E:43:27:EA	TP-LINK TECHNOLOGIES CO.LTD.	a, n, ac	153
2	ACREDITACION	64:D1:54:E5:29:A1	Routerboard.com	b, g, n	1
3	ADMINISTRACION-A	CC:2D:E0:0F:3F:6B	Routerboard.com	b, g	6
4	ADMINISTRACION-B	CC:2D:E0:0F:3B:57	Routerboard.com	b, g	4
5	AGROINDUSTRIA-I	CC:2D:E0:0F:3E:BD 2	Routerboard.com	b, g	2
6	AGROINDUSTRA-II	CC:2D:E0:0F:3E:B1	Routerboard.com	b, g	2
7	BIBLIOTECA-001	00:15:6D:10:6E:32	Ubiquiti Networks Inc.	b, g, n	8
8	BIBLIOTECA-002	00:15:6D:10:6E:27	Ubiquiti Networks Inc.	b, g, n	6
9	BIBLIOTECA-003	00:15:6D:10:6E:21	Ubiquiti Networks Inc.	b, g, n	8
10	CAAI	C8:B3:73:59:7C:9D	Cisco-Linksys. LLC	a, n	157
		C8:B3:73:59:7C:9C	Cisco-Linksys. LLC	b, g, n	1
11	COOR-ACADEMICA	98:FC:11:B1:73:B5	Cisco-Linksys. LLC	b, g, n	11
12	DIRECT-Oh-BRAVIA	DA:5D:E2:6F:13:3D	Hon Hai Precision Ind. Co.Ltd.	g, n	11
13	DIRECT-44039B3D	46:D2:44:03:1B:3D	Seiko Epson Corporation	g, n	6
14	EMPRENDIMIENTO	C4:E9:84:D1:51:32	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	10
15	ESPAM-BIBLIOTECA1	00:27:22:46:80:D1	Ubiquiti Networks Inc.	a, n	157
16	ESPAM-EP	C0:56:27:49:FC:23	Belkin International Inc.	b, g, n	6
17	ESPAM-SALON	00:1D:0F:CC:22:4E	TP-LINK TECHNOLOGIES CO.LTD.	b, g	11
18	ESTUDIANTES	64:D1:54:A0:2B:6F	Routerboard.com	b, g, n	1
		F0:9F:C2:3D:31:AF	Ubiquiti Networks Inc.	b, g, n	
		64:D1:54:9F:15:47	Routerboard.com	b, g	
		64:D1:54:9C:EA:B3	Routerboard.com	b, g	2
		64:D1:54:A2:C5:21	Routerboard.com	b, g	3
		64:D1:54:A0:2A:CD	Routerboard.com	b, g	6
		FC:EC:DA:8A:F7:00	Ubiquiti Networks Inc.	b, g, n	
		78:8A:20:81:22:EE	Ubiquiti Networks Inc.	b, g, n	
		78:8A:20:81:1C:B9	Ubiquiti Networks Inc.	b, g, n	

		98:FC:11:B1:74:1F	Cisco-Linksys. LLC	b, g, n	10
		98:FC:11:B1:B4:C7	Cisco-Linksys. LLC	b, g, n	11
		78:8A:20:81:80:6F	Ubiquiti Networks Inc.	b, g, n	
		F0:9F:C2:3E:31:AF	Ubiquiti Networks Inc.	a, n, ac	36
		78:8A:20:82:22:EE	Ubiquiti Networks Inc.	a, n, ac	
		78:8A:20:82:80:6F	Ubiquiti Networks Inc.	a, n, ac	149
		78:8A:20:82:1C:B9	Ubiquiti Networks Inc.	b, g, n	
		C8:B3:73:59:71:03	Cisco-Linksys. LLC	a, n	
		FC:EC:DA:8B:F7:00	Ubiquiti Networks Inc.	a, n, ac	157
19	**IDIOMAS**	C4:6E:1F:DE:18:72	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	6
20	**Investigacion-E**	6C:3B:6B:8C:FB:52	Routerboard.com	b, g	1
21	**M-AMBIENTEA2**	86:E9:84:D1:51:04		b, g, n	10
22	**NO-DISPONIBLE**	0C:80:63:6B:5E:7A	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	9
23	**OFICINA DIRECCION**	14:CC:20:5E:60:96	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	6
		14:CC:20:5E:60:97	TP-LINK TECHNOLOGIES CO.LTD.	a, n	36
24	**PLANIFICACION**	64:D1:54:9F:14:63	Routerboard.com	b, g	1
24	**POSGRADO**	C4:E9:84:D1:51:04	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	10
25	**PROFESORES**	7A:8A:20:81:1C:B9	Ubiquiti Networks Inc.	b, g, n	6
		7A:8A:20:81:22:EE	Ubiquiti Networks Inc.	b, g, n	6
		7A:8A:20:81:80:6F	Ubiquiti Networks Inc.	b, g, n	11
		7A:8A:20:82:1C:B9	Ubiquiti Networks Inc.	a, n, ac	149
		7A:8A:20:82:80:6F	Ubiquiti Networks Inc.	a, n, ac	149
		F2:9F:C2:3D:31:AF	Ubiquiti Networks Inc.	b, g, n	1
		F2:9F:C2:3E:31:AF	Ubiquiti Networks Inc.	a, n, ac	36
		FE:EC:DA:8A:F7:00	Ubiquiti Networks Inc.	b, g, n	6
		FE:EC:DA:8B:F7:00	Ubiquiti Networks Inc.	a, n, ac	157
26	**RECAF**	C0:56:27:4A:02:86	Belkin International Inc.	b, g, n	11
27	**SALON-MFL**	20:AA:4B:55:94:3D	Cisco-Linksys. LLC	b, g	6
28	**SYSKONTROL**	C4:E9:84:C1:5A:90	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	7
29	**TT-HH**	64:D1:54:34:BF:0E	Routerboard.com	b, g	10
30	**TURISMO**	CC:2D:E0:0F:3F:8F	Routerboard.com	b, g	3
31	**UPS DESARROLLO**	D4:6E:0E:43:27:EB	TP-LINK TECHNOLOGIES CO.LTD.	b, g, n	11
32	**USUARIO-PC_NETWORK_1**	B4:75:0E:89:6E:F4	Belkin International Inc.	b, g, n	1
33	**YANDY RESTAURANT**	00:23:69:52:B8:CC	Cisco-Linksys. LLC	b, g, n	6
34	**ZOOTECNIA**	CC:2D:E0:0F:3B:15	Routerboard.com	b, g	8

Fuente: el autor

COMPATIBILIDAD DE EQUIPOS INALÁMBRICOS DEL SECTOR 8 DE LA ESPAM MFL CON EL ESTÁNDAR IEEE 802.1X

Para implementar un servidor Radius es importante comprobar la compatibilidad de los equipos (access point y routers) que forman parte de una red inalámbrica con el estándar IEEE 802.1X, tal como se muestra en la siguiente tabla:

- **Producto:** equipo access point o router
- **Fabricante:** Fabricante del dispositivo.
- **Modelo:** Modelo de dispositivo inalámbrico.
- **802.1X:** Estándar de autenticación.

Tabla 3.13. Compatibilidad de los equipos inalámbricos del Sector 8 de la ESPAM MFL con el estándar IEEE 802.1X

Producto	Fabricante	Modelo	802.1X
	Routerboard.com	RB951Ui-2Dn	SI
	Routerboard.com	RB951Ui-2H2n	SI
	Cisco-Linksys. LLC	WAP300N	SI
	TP-LINK TECHNOLOGIES CO.LTD.	EAP 120	SI
	Ubiquiti Networks Inc.	Rocket M2	SI

Fuente: el autor.

Se analizó las características de los equipos inalámbricos que se encontraron durante el monitoreo y se pudo comprobar su compatibilidad con el estándar 802.1X, por lo que la implementación del servidor RADIUS en la infraestructura tecnológica del Sector 8 fue viable.

3.6.2. DISEÑAR LA ARQUITECTURA DEL SERVIDOR RADIUS

La implementación del servidor RADIUS se llevó a cabo en el área del edificio de Posgrado según el siguiente esquema:

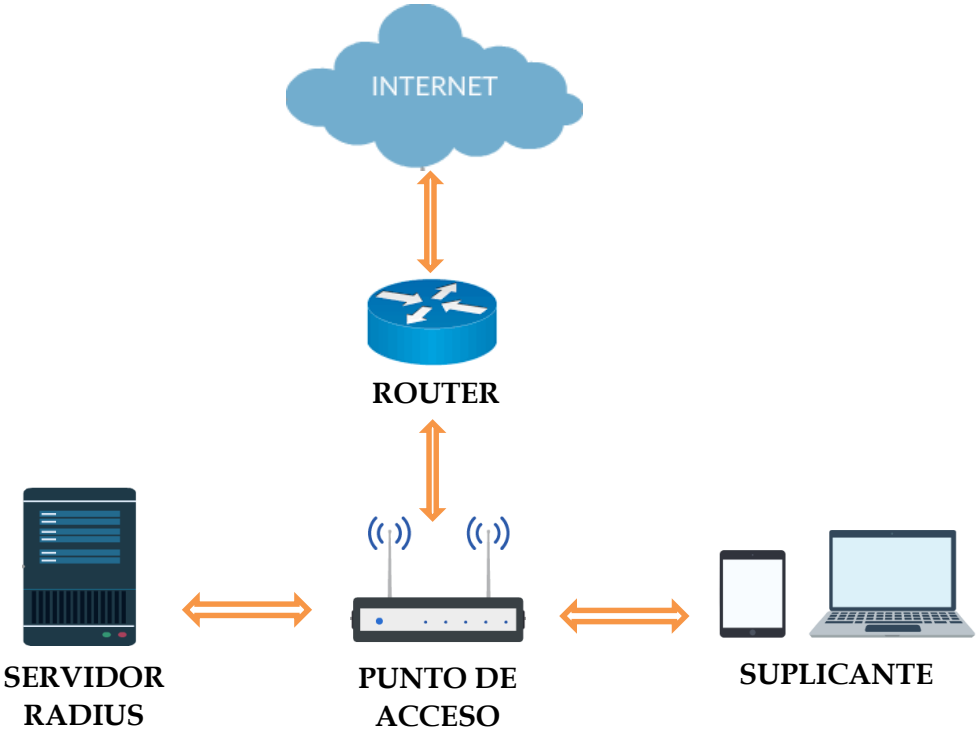


Figura 3.7. Esquema de implementación de servidor RADIUS en el área del Edificio de Posgrado.

ANÁLISIS DE LOS REQUISITOS PARA LA IMPLEMENTACIÓN DEL SERVIDOR RADIUS

Para la implementación del servidor RADIUS se utilizó el siguiente soporte tecnológico:

Tabla 3.14. Soporte tecnológico utilizado para la implementación del servidor RADIUS

HARDWARE:
Computadora PC Acer Aspire V5, SO Windows 8.1 Pro 64 bits , Memoria RAM 6,00 GB, Procesador Intel(R) Core i5 3317U 1.70 Ghz
Access points: TP-LINK TL-WR840N 300Mbps
SOFTWARE:
Oracle VM Virtual Box 6.0, CentOS 7, daloRADIUS 9.0-0, FreeRadius, PhP 7 MariaDB 10

Fuente: el autor

IMPLEMENTACIÓN DEL SERVIDOR RADIUS

Para la implementación del servidor RADIUS se hizo el análisis de requerimientos con base a la información que se presentó en la revisión bibliográfica del presente trabajo, luego se comenzó con la instalación de las aplicaciones software y configuración de los servicios requeridos para poner en funcionamiento el servidor de autenticación dentro de la infraestructura tecnológica del sector 8 y realizar las pruebas respectivas.

INSTALACIÓN DE SOFTWARE Y CONFIGURACIÓN DE LOS SERVICIOS REQUERIDOS PARA LA IMPLEMENTACIÓN DEL SERVIDOR RADIUS

Las aplicaciones software y los servicios que se instalaron fueron los siguientes:

SOFTWARE

- OracleVirtual Box
- CentOS 7

SERVICIOS

- Freeradius y módulos adicionales
- MariaDB 10
- PHP7
- daloRADIUS

A continuación se describen los pasos para la implementación del servidor RADIUS, donde se muestra la instalación de las aplicaciones software y configuración de los servicios requeridos.

INSTALACIÓN DE SOFTWARE

Paso: 1 Instalación de Oracle Virtual Box

Se instaló Oracle Virtual Box 6.6. para la creación de la máquina virtual que permitió dar soporte en la instalación del sistema operativo CentOS 7, Freeradius y otros servicios requeridos para la implementación del servidor RADIUS.

Paso 2: Creación de la máquina Virtual en Virtual Box

Clic en Nueva para crear una máquina virtual (vm), a continuación se debe dar un nombre en este caso se le denominó SERVIDORRADIUS, luego se selecciona la carpeta donde va a crear la mv y por último se selecciona el sistema operativo que se desea instalarse.

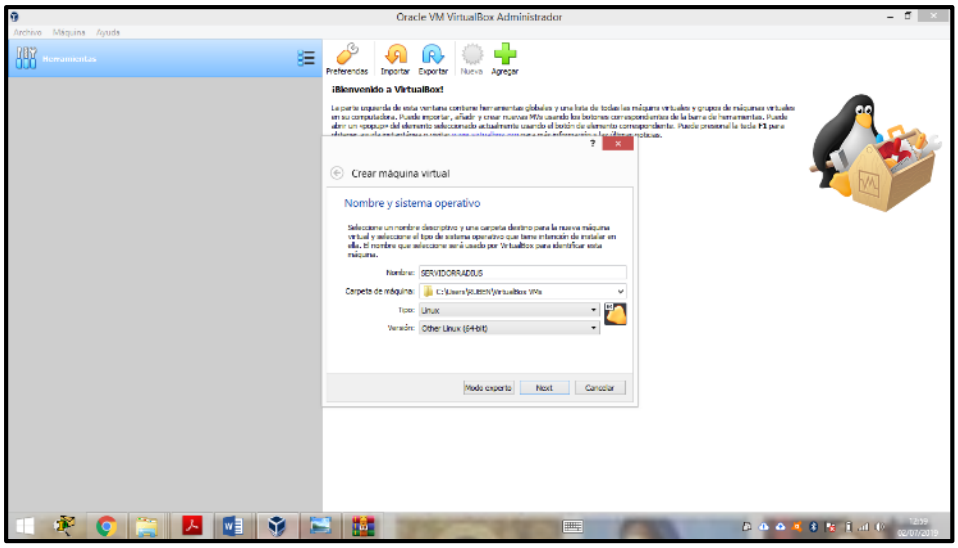


Figura 3.8. Creación de Máquina Virtual (VM)

2.2. Seleccionar la cantidad de memoria RAM para la máquina virtual, en este caso se le dio una cantidad de 2048 MB.

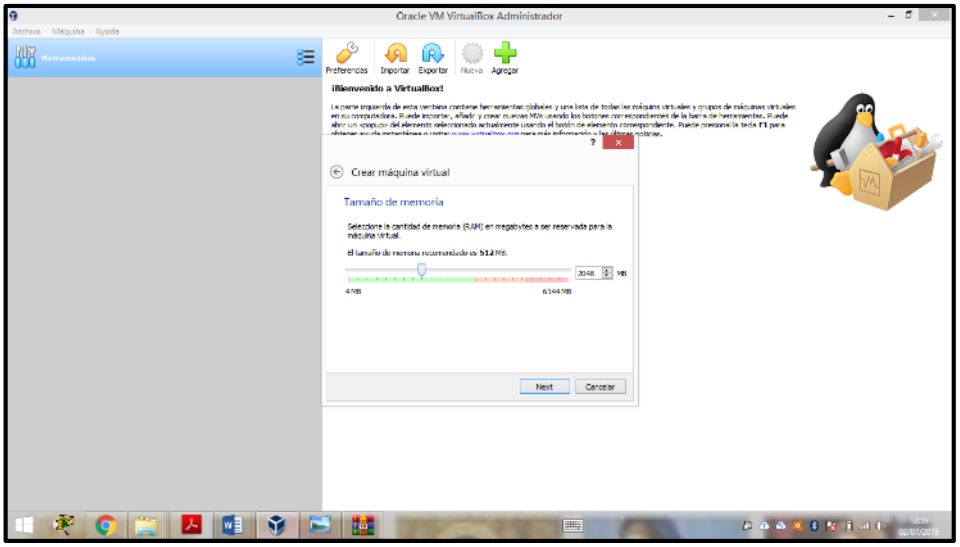


Figura 3.9. Asignación de tamaño de memoria RAM.

2.3. Crear un disco duro virtual para la máquina.

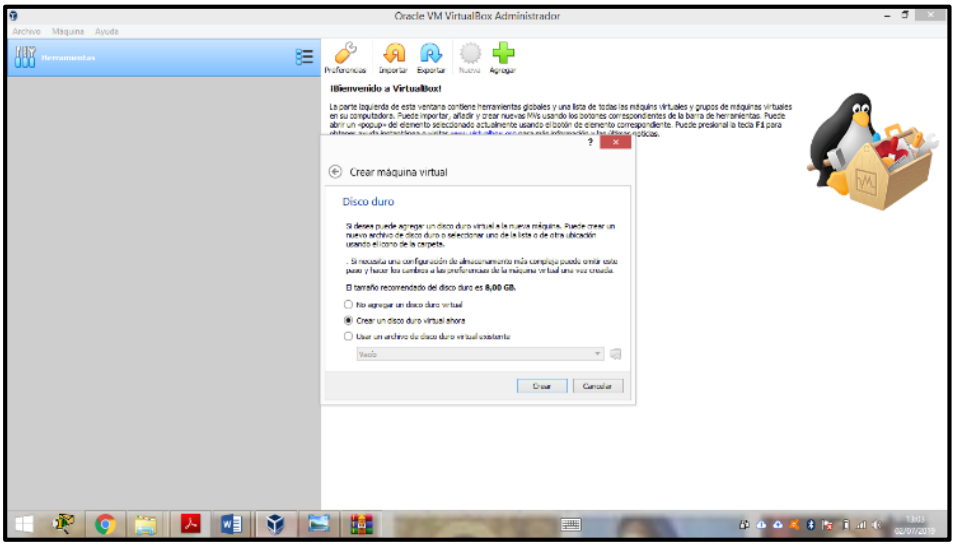


Figura 3.10. Creación de un disco duro virtual

2.4. Seleccionar el tipo de archivo que se desee usar para el nuevo disco duro virtual, en este caso se seleccionó VDI (VirtualBox Disk Image)

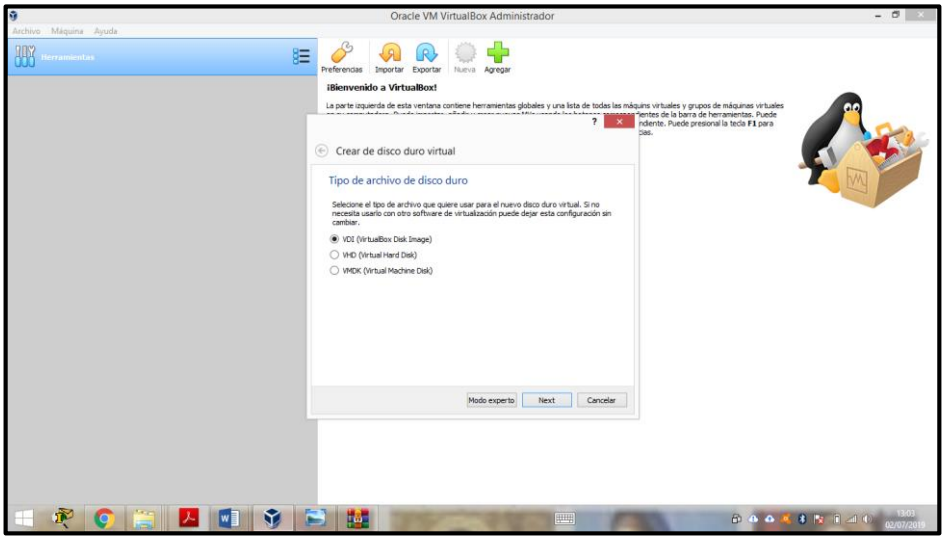


Figura 3.11. Selección del tipo de archivo para el nuevo disco duro virtual.

2.5. Seleccionar el tipo de tamaño de almacenamiento que tendrá el disco duro virtual, en este caso se seleccionó reservado dinámicamente.

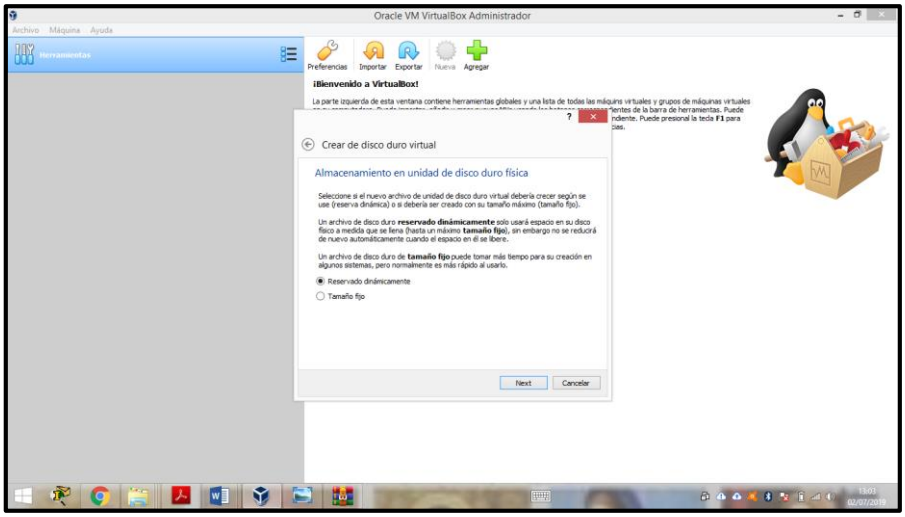


Figura 3.12. Selección de almacenamiento en unidad de disco duro físico.

2.6. Seleccionar la ubicación del archivo y el tamaño que se le desee asignar al disco duro virtual, en este caso se asignó 20.00 GB.

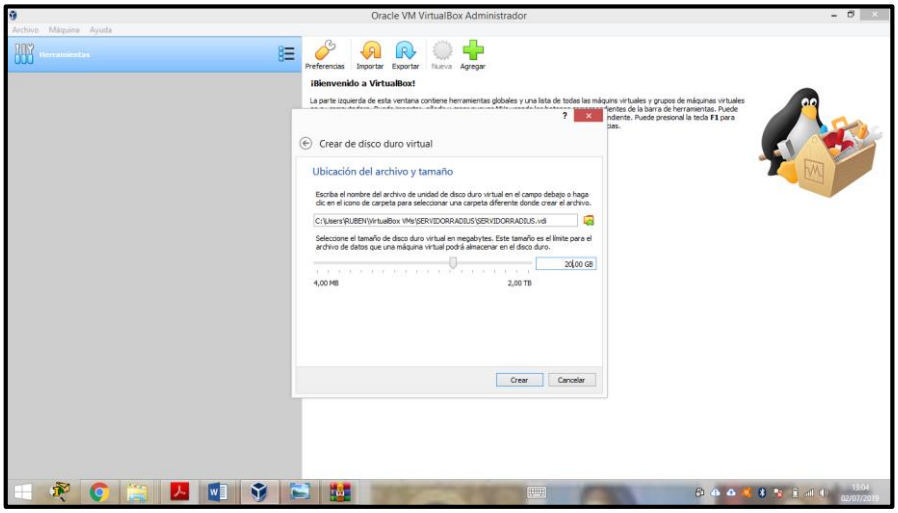


Figura 3.13. Selección de ubicación del archivo y tamaño de disco duro virtual.

2.7. La creación de la máquina virtual ha sido completada.

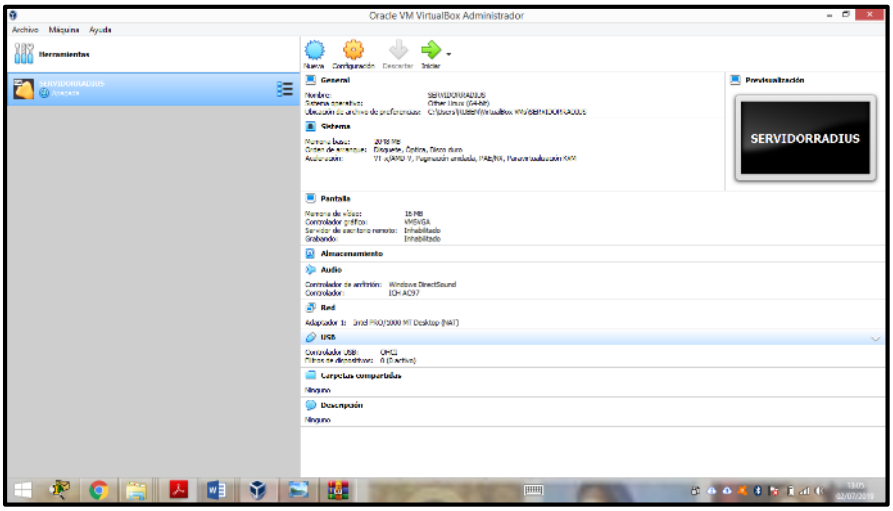


Figura 3.14. Características de la máquina virtual creada.

Paso 3. Instalación de Sistema Operativo CentOS 7

3.1. Se debe iniciar la máquina virtual creada

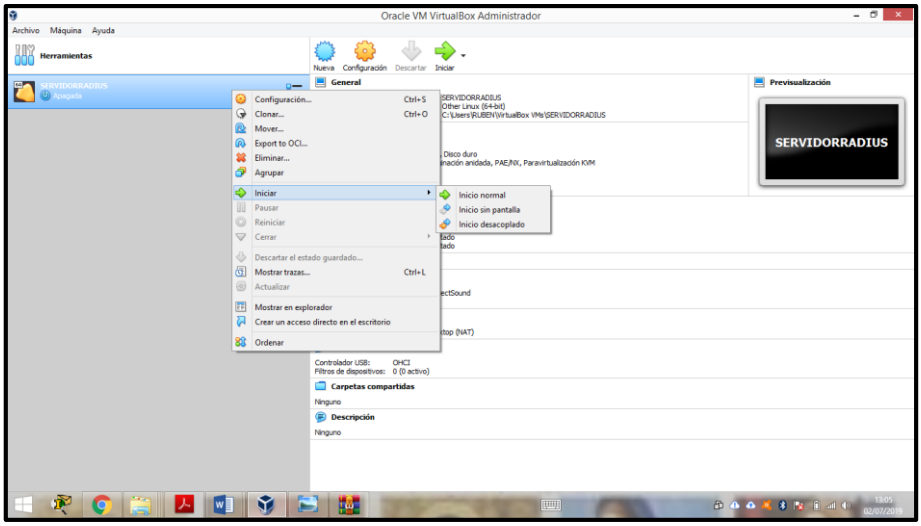


Figura 3.15. Iniciación de la máquina virtual

3.2. Se debe seleccionar un disco de inicio.

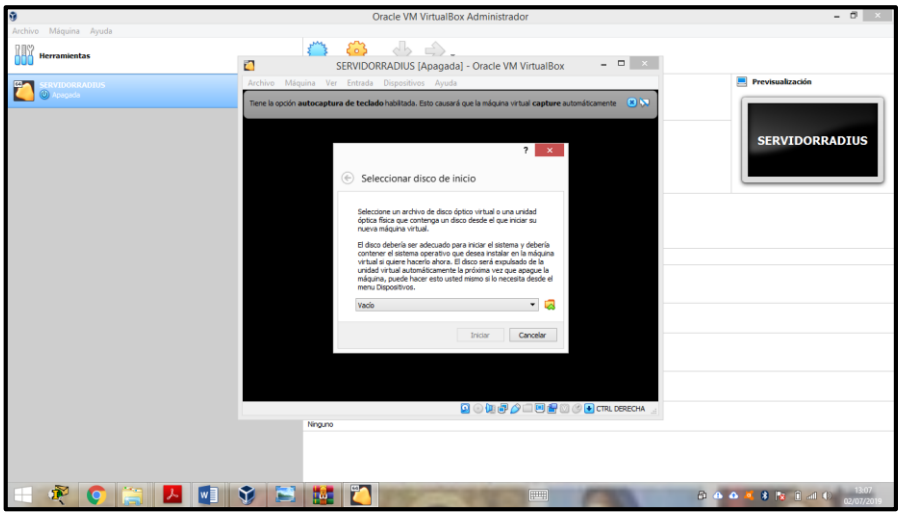


Figura 3.16. Selección de disco de inicio.

3.3. Abrir la ubicación para seleccionar un archivo de disco óptico virtual, en este caso se seleccionó una imagen ISO del sistema operativo CentOS 7.

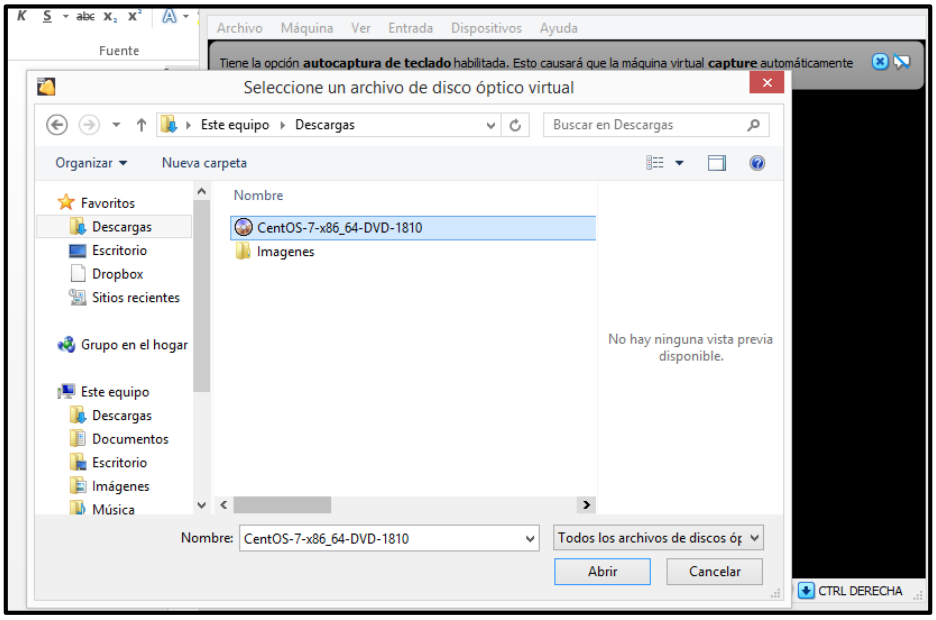


Figura 3.17. Selección de disco óptico virtual ISO CentOS 7.

3.4. Iniciación de disco óptico virtual para comenzar instalación de CentOs 7.

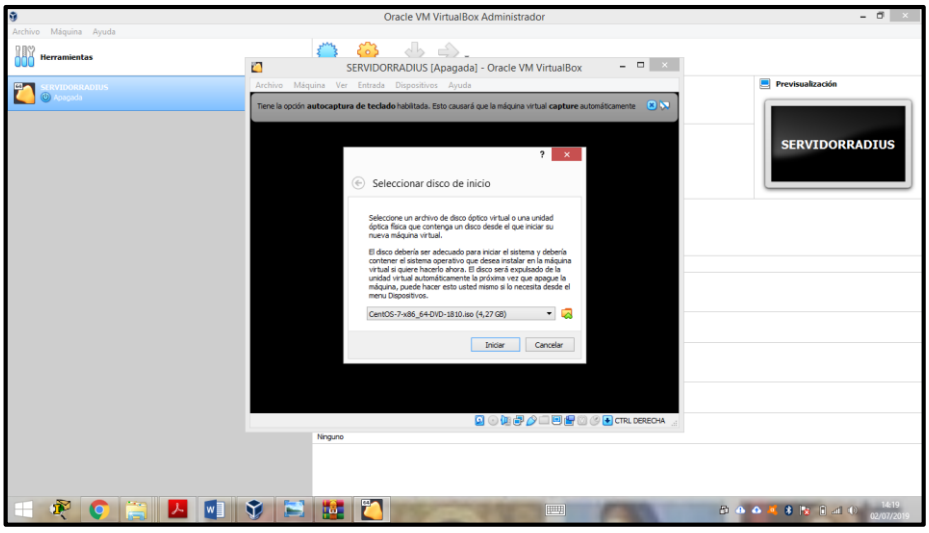


Figura 3.18. Iniciación de disco óptico para instalación de CentOS 7.

3.5. Página de inicio de instalación de CentOs 7.

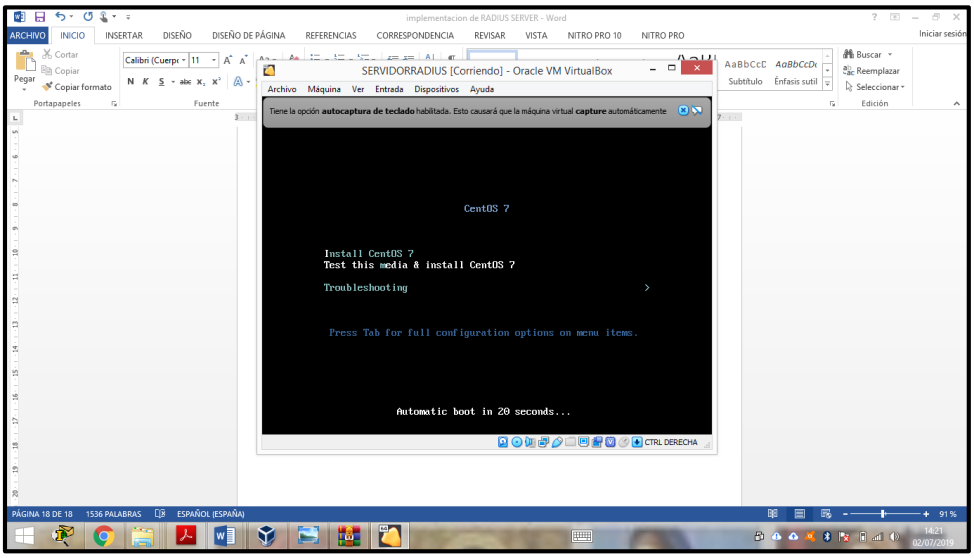


Figura 3.19. Página de inicio de instalación de CentOS 7.

3.6. Configurar el idioma a utilizar en el proceso de instalación de CentOs 7.

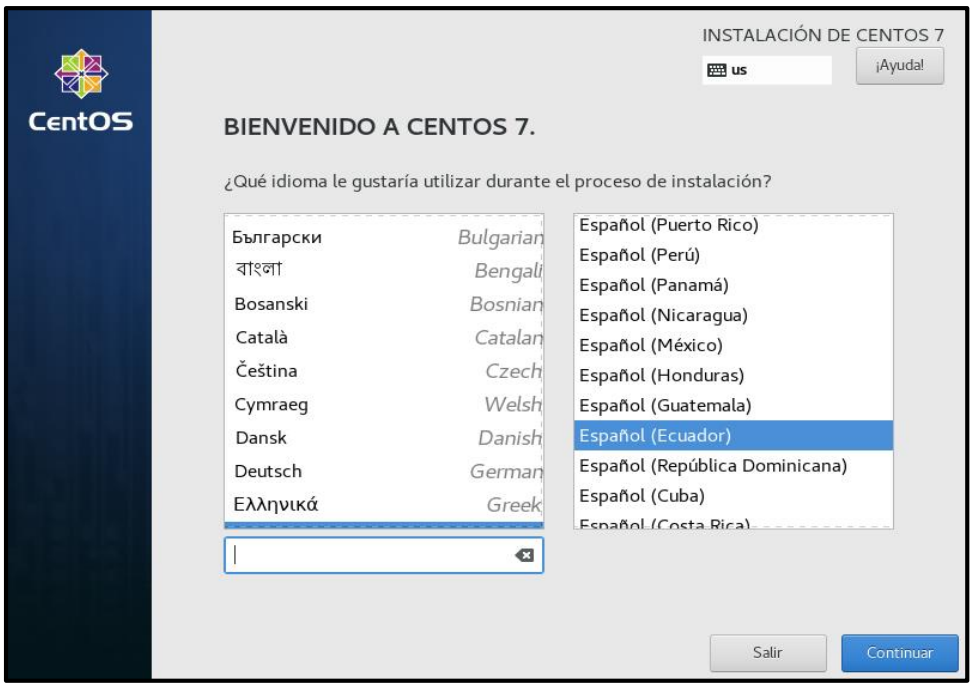


Figura 3.20. Configuración de idioma en instalación de CentOS 7.

3.7. Configurar la interfaz de red.

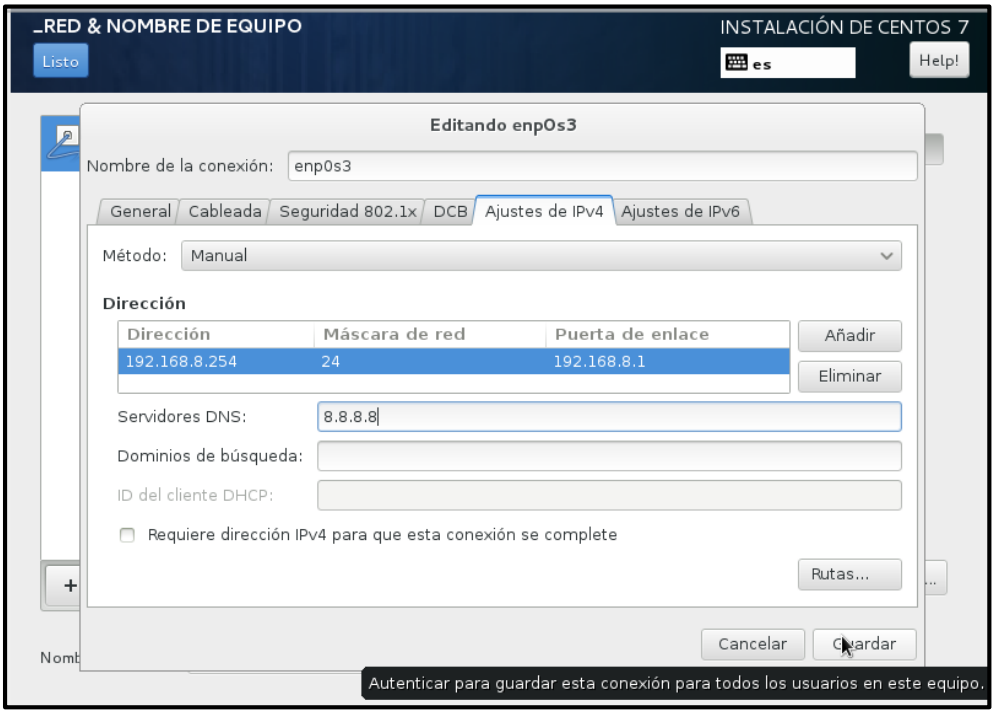


Figura 3.21. Configuración de interfaz de red.

3.8. Crear la contraseña root.

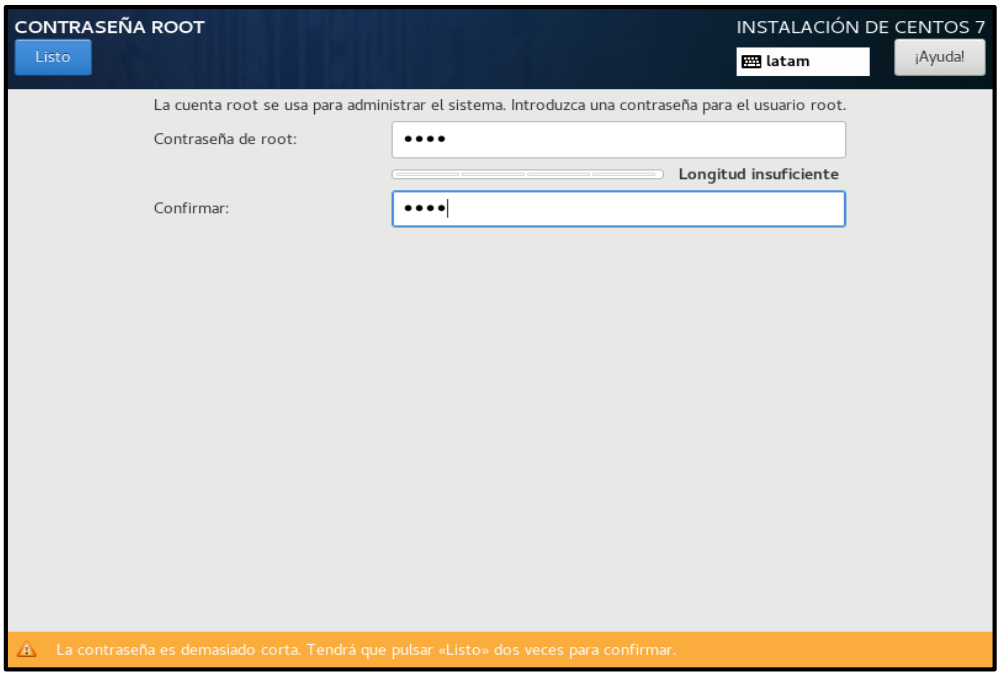


Figura 3.22. Creación de la contraseña root.

3.9. Finalización de la instalación de CentOS 7

Figura 3.23. Finalización de la Instalación de CentOS 7.

CONFIGURACIÓN DE SERVICIOS

Paso 4: Instalación de FreeRADIUS y módulos adicionales en Centos 7

- Freeradius
- Freeradius-utils
- Freeradius-mysql
- Freeradius-perl

4.1. Actualizar el índice de paquetes del sistema utilizando el comando: $ sudo yum –y update

4.1. Realizar una búsqueda de todos los paquetes utilizando el comando: **$ sudo yum search all freeradius**

4.2. Instalación de freeradius**, freeradius-utils, freeradius-mysqly freeradius-perl** utilizando el comando: **$ sudo yum –y install freeradius freeradius-utils freeradius-mysql freeradius-perl**

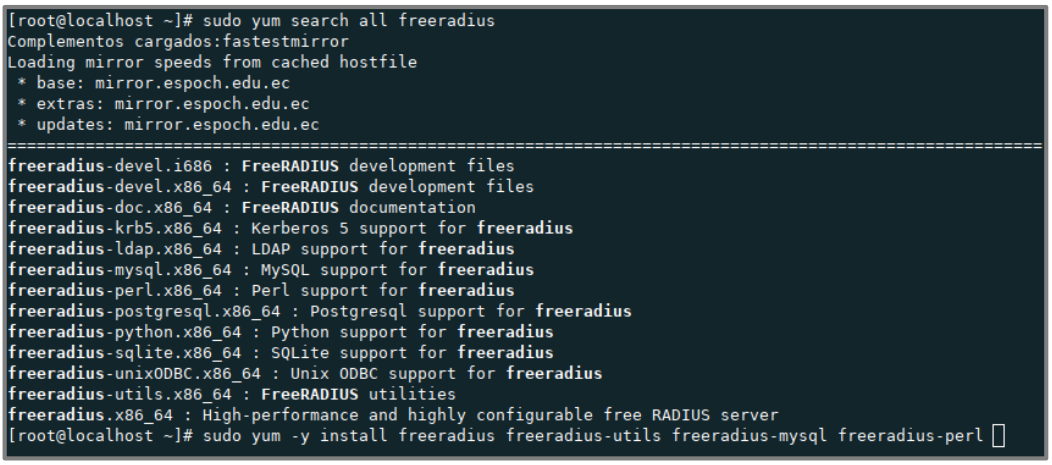


Figura 3.24. Actualización de paquetes del sistema e instalación de Freeradius

4.3. Iniciación y habilitación de **freeRADIUS** para que se ejecute y se inicie en el arranque, utilizando los comandos: **$ systemctl start radiusd.service y $ systemctl enable radiusd.service**

4.4. Comprobación del estado de **radius.service**, utilizando el comando: **$ systemctl status radiusd.service**

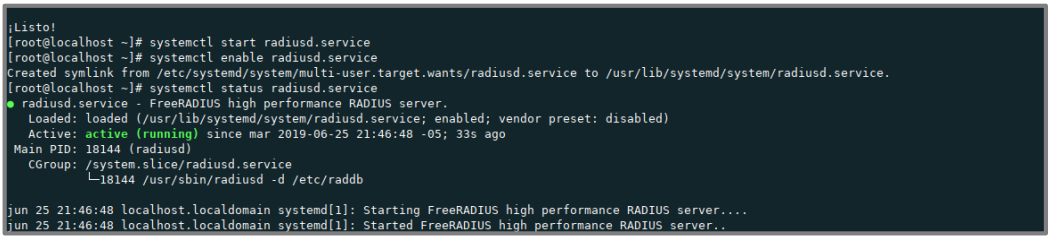


Figura 3.25. Iniciación y habilitación de FreeRADIUS.

Paso 5: Configurar CentOS 7 firewall para freeRADIUS

5.1. Configuración del **firewall** para permitir los paquetes **radius y httpd**, utilizando el comando: **$ cat /usr/lib/firewalld/services/radius.xml**. Se debe iniciar, habilitar **firewalld** y verificar su estado, utilizando los comandos: **$ systemctl enable firewalld**, **$ systemctl start firewalld** y $ **systemctl status firewalld**

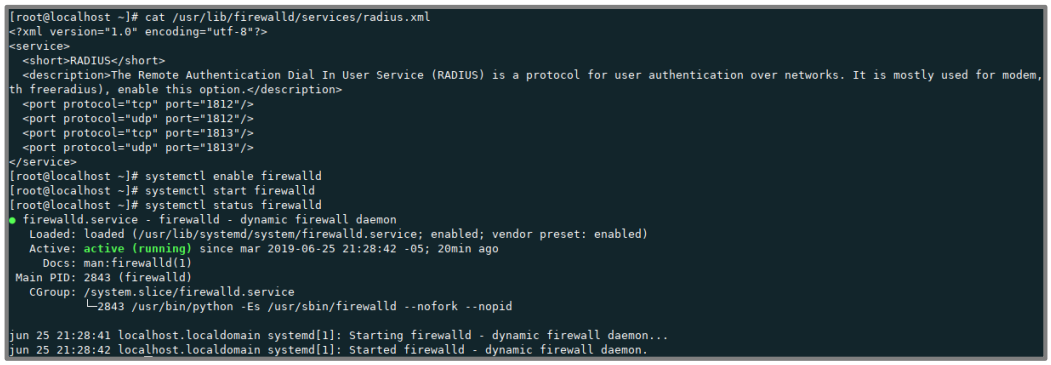


Figura 3.26. Configuración CentOS 7 firewall para FreeRADIUS.

5.2. Hay que asegurarse de que **firewalld** se está ejecutando, utilizando el comando: **$ firewall-cmd --state**.

5.3. Se deben crear reglas permanentes a la zona predeterminada para permitir **http, https y radius servicios**, se utiliza el comando: **$ firewall –cmd --add-service= {http, https, radius} –permanent**. Se debe recarga **firewalld** para que los cambios surtan efecto, utilizando el comando: **$ firewalld-cmd --reload** y por último se debe confirmar que los servicios se agregaron correctamente a la zona predeterminada con los comandos: **$firewall-cmd --get-default-zone** y **$ firewall-cmd --list-services --zone=public**

Figura 3.27. Creación de reglas.

Paso 6. Servidor de Prueba RADIUS

6.1. Hay que probar el servidor RADIUS en modo de depuración, para lo cual se debe ejecutar el servicio, lo primero que se debe hacer es eliminar el servicio de **radius**, utilizando el comando: **$ pkill radius**, luego hay que ejecutar el servidor RADIUS en modo depuración para verificar si todo funciona se ejecuta el comando: **$ radiusd –x**

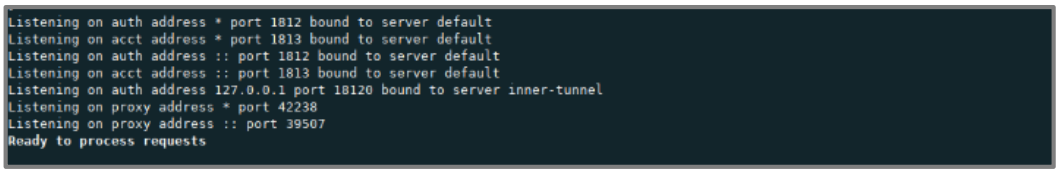


Figura 3.28. Prueba del servidor RADIUS en modo depuración.

La configuración básica de FreeRADIUS ha sido exitosa.

Paso 7. Instalación y configuración de MariaDB 10 en CentOS 7

7.1. Lo primero es agregar los repositorios oficiales de **MariaDB**, utilizando el siguiente comando: **$ nano /etc/yum.repos.d/MariaDB.repo** y se debe agregar el siguiente contenido, luego guardar y salir del archivo cuando se haya terminado.

[mariadb]

name = MariaDB

baseurl = http://yum.mariadb.org/10.1/centos/-amd64

gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB

gpgkeycheck=1

7.2. Se debe actualizar el índice del paquete, utilizando el comando **$ yum –y update**, e instalar MariaDB utilizando el comando: **$ yum install –y mariadb-server mariadb**

Figura 3.29. Instalación y configuración de MariaDB 10 en CentOS 7.

7.3. Iniciar MariaDB y ejecutar el arranque, utilizando los comandos: **$ systemctl start mariadb** y **$ systemctl enable mariadb** y comprobar que esté funcionando y habilitado, usando los siguientes comando: **$ systemctl status mariadb** y **$ systemctl is-enabled mariadb.service**

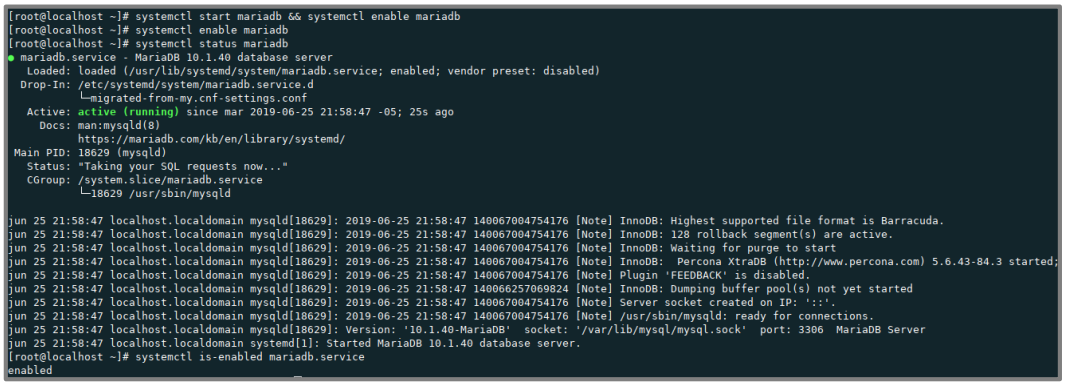


Figura 3.30. Iniciación de MariaDB 10 en CentOS 7.

Paso 8. Asegurando MariaDB/MySQL

8.1. Primero hay que utilizar el siguiente comando: **$ mysql_secure_installation**

Figura 3.31. Comprobación de la instalación de MariaDB 10.

8.2. Se debe establecer la contraseña de **root.**

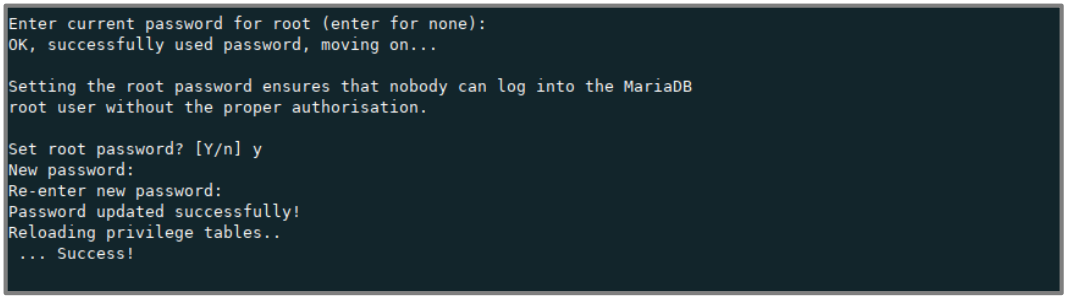


Figura 3.32. Configuración de la contraseña root.

8.3. Se debe eliminar/mantener algunos valores predeterminados, se debe seguir las siguientes instrucciones:

Figura 3.33. Configuración de valores predeterminados.

Paso 9. Instalación de PHP7 en CentOS 7

9.1. Se debe instalar el repositorio **EPEL**, utilizando los siguientes comandos: **$ sudo yum install epel-release yum-utils** y **$ sudo yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm**

```
[root@localhost ~]# sudo yum install epel-release yum-utils

[root@localhost ~]# sudo yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
Complementos cargados:fastestmirror
remi-release-7.rpm
Examinando /var/tmp/yum-root-CwNRVy/remi-release-7.rpm: remi-release-7.6-2.el7.remi.noarch
Marcando /var/tmp/yum-root-CwNRVy/remi-release-7.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete remi-release.noarch 0:7.6-2.el7.remi debe ser instalado
--> Resolución de dependencias finalizada
```

Figura 3.34. Instalación de PHP7 en CentOS 7.

9.2. Se debe habilitar el repositorio **PHP 7.3 Remi**, utilizando el comando**: $ sudo yum-config-manager --enable remi-php7.3**, luego ejecutar el siguiente comando para instalar **PHP 7.3** junto con algunos de los módulos PHP más comunes:

$ sudo yum install php php-common php-opcache php-mcrypt php-cli php-gd php-curl php-mysqlnd

```
Running transaction test
Transaction test succeeded
Running transaction
  Instalando    : remi-release-7.6-2.el7.remi.noarch
  Comprobando   : remi-release-7.6-2.el7.remi.noarch

Instalado:
  remi-release.noarch 0:7.6-2.el7.remi

¡Listo!
[root@localhost ~]# sudo yum-config-manager --enable remi-php73
Complementos cargados:fastestmirror

[root@localhost ~]# sudo yum install php php-common php-opcache php-mcrypt php-cli php-gd php-curl php-mysqlnd
```

Figura 3.35. Habilitación del repositorio PHP 7.3 Remi.

9.3. Verificación de la instalación de la versión de PHP, utilizando el comando **$ php –v**

Paso 10. Configuración de FreeRADIUS para usar MariaDB/MySQL

Para configurar **FreeRADIUS** para usar **Maria/MySQl**, se debe crear una base de datos con tablas que usará el servidor de FreeRADIUS para encontrar usuarios RADIUS y para almacenar datos contables.

10.1. Iniciar sesión en MariaDB o MySQL y crear y configurar una base de datos, en este caso se llamará radius, utilizando el siguiente comando: **$ mysql –u root –p**

10.2. Ingresar una contraseña cuando se solicite, una vez que se inicie sesión ejecutar los siguientes comandos para crear y configurar la base de datos:

MariaDB [(none)]> CREATE DATABASE radius;

MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword";

MariaDB [(none)]> FLUSH PRIVILEGES;

MariaDB [(none)]> quit;

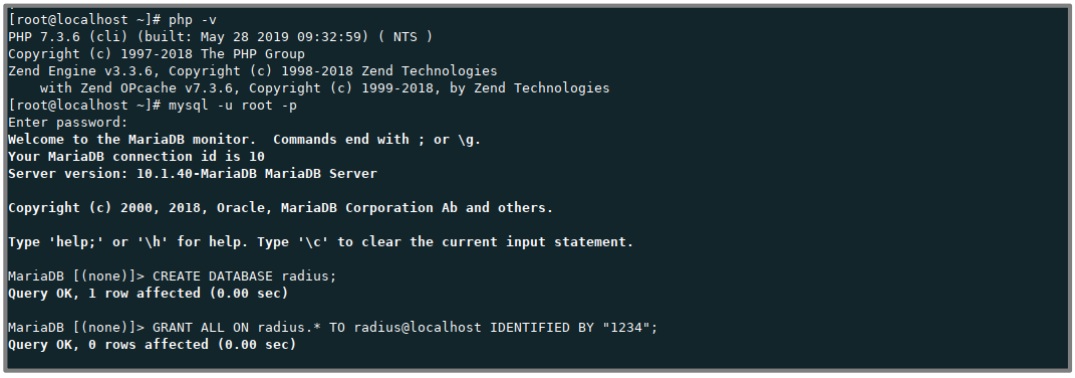


Figura 3.36. Configuración de FreeRADIUS para usar MariaDB.

10.3. A continuación se debe importar el **esquema de base de datos RADIUS** para completar la base de datos radius, utilizando el siguiente comando**: $ mysql –uroot –pyour_password radius < /etc/raddb/mods-config/sql/main/mysql/schema.sql**

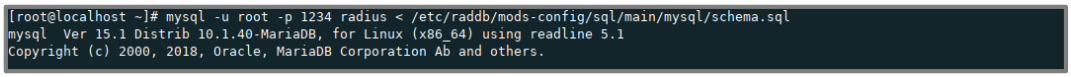


Figura 3.37. Importación del esquema de base de datos RADIUS.

10.4. Se debe crear un **enlace flexible para SQL en /etc/raddb/mods-enabled**, se utiliza el siguiente comando: **$ ln –s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/** y se debe configurar el servidor **freeRADIUS** para usar el servidor de base de datos, abriendo el archivo **/raddb/mods-available/sql** utilizando el comando **$ nano /etc/raddb/mods-available/sql**

Figura 3.38. Creación de enlace flexible para SQL.

Aparecerá una sección sql como la siguiente:

```
sql {
driver = "rlm_sql_mysql"
dialect = "mysql"
# Connection info:
server = "localhost"
port = 3306
login = "radius"
password = "radiuspassword"
# Database table configuration for everything except Oracle
radius_db = "radius"
}
```

Set to ‘yes’ to read radius clients from the database (‘nas’ table)

```
# Clients will ONLY be read on server startup.
read_clients = yes
# Table to keep radius client info
client_table = “nas
```

10.5. Se debe cambiar los siguientes parámetros:

Cambiar driver = ¨rlm_sql_null¨ a driver = ¨**rlm_sql_mysql**¨

Cambiar dialect = ¨sqlite¨ a dialect = ¨**mysql**¨

Descomentar **server, port, login** y **password** mediante la eliminación de #

Cambiar password = ¨**radpass**¨ a password = ¨**radiuspassword**¨

Descomentar la línea **read**_clients = yes , eliminando #

10.6. Se debe cambiar los derechos de grupo de /**etc/raddb/mods-enabled/sql** a radiusd utilizando el siguiente comando: **$ chgrp –h radiusd /etc/raddb/mods-enabled/sql**

10.7. Se debe ejecutar **FreeRADIUS** nuevamente en modo de depuración, ya que se ha realizado algunos cambios, si el servidor RADIUS se está ejecutando, primero hay que eliminar el demonio con el comando: **pkill radiusd** y ejecutar el servidor en modo de depuración con el comando **radiusd –x**

Paso 11. Instalación de daloRADIUS WebPanel en CentOS 7

11.1 Primero se debe instalar el servidor **httpd**, utilizando los comandos**: $ yum groupinstall ¨Development Tools¨ -y y $ yum –y install httpd httpd-devel**

Figura 3.39. Instalación de servidor httpd.

11.2. Iniciar y habilitar el servidor httpd, utilizando el comando: $ systemctl enable httpd y systemctl start httpd

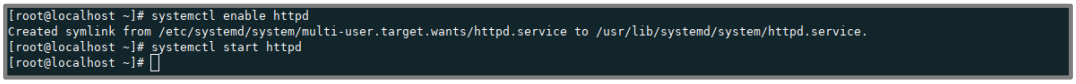


Figura 3.40. Iniciación y habilitación del servidor httpd.

11.3. Comprobar el estado del servidor **httpd** para asegurarse de que se está ejecutando, utilizando el comando: **$ systemctl status httpd**

11.4 Descarga de daloRADIUS

Descargar **daloRADIUS,** utilizando los comandos: **$ wget** **http://liquidtelecom.dl.sourceforge.net/project/daloradius/daloradius/daloradius0.9-9/daloradius-0.9.tar.gz**

$ tar zxvf daloradius-0.9-9.tar.gz

$ mv daloradius-0.9-9 daloradius

$ cd daloradius

Figura 3.41. Descarga de daloRADIUS.

11.5. Añadir el esquema SQL daloRADIUS

Se debe importar las tablas daloRADIUS MySQL, utilizando los siguientes comandos: **$ mysql –u root –p radius < contrib/db/fr2-mysql-daloradius-and-freeradius.sql** y **$ mysql –u root –p radius < contrib/db/mysql-daloradius.sql**

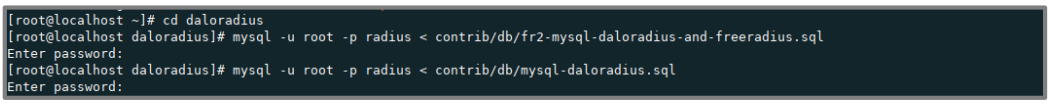


Figura 3.42. Añadir esquema SQL daloRADIUS.

11.6. Configuración de detalles de conexión de la base de datos daloRADIUS DB

Configurar los detalles de conexión de la base de datos daloRADIUS, utilizando los comandos: **$ cd ..** y **$ mv daloradius /var/www/html/**

Figura 3.43. Configuración de base de datos daloRADIUS.

11.7. Cambiar los permisos para la carpeta http daloRADIUS y establecer los permisos apropiados para el archivo de configuración, utilizando los comandos: **$ chown –R apache:apache /var/www/html/daloradius/ y $ chmod 664 /var/www/html/daloradius/library/daloradius.conf.php**

Figura 3.44. Configuración de permisos.

11.8. Modificar **daloradius.conf.php** para agregar la información SQL, se debe abrir el archivo:

$ nano /var/www/html/daloradius/library/daloradius.conf.php, una vez que se ha modificado, guardar y cerrar el archivo.

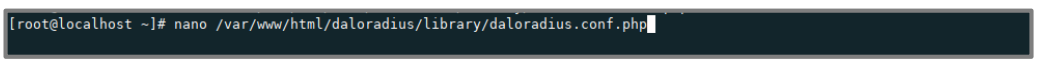


Figura 3.45. Modificación de archivo para agregar la información SQL.

11.9. Hay que asegurarse que todo funcione, utilizando los comandos **$ systemctl restart radiusd.service**, **$ systemctl restart mariadb. service** y **$ systemctl restart httpd** y ejecutar los comandos: **$ yum install php-pear** y **$pear install DB**

Figura 3.46. Comprobación de funcionamiento.

11.10 Otra vez se ejecuta los comandos: comandos **$ systemctl restart radiusd.serviceP**, **$ systemctl restart mariadb. service** y **$ systemctl restart httpd, adicionlamente** se ejecuta el comando **setenforce 0**; **nano /etc/sysconfig/selinux** y cambiar SELINUX=**disabled**

3.6.3. PONER EN FUNCIONAMIENTO EL SERVIDOR RADIUS EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ESPAM MFL.

Una vez que se ha instalaron las aplicaciones softwares y configuró los servicios requeridos, el siguiente paso fue poner en funcionamiento al servidor RADIUS, para lo cual se procedió a realizar lo siguiente:

12. Inicio de sesión en daloRADIUS

Una vez que sea instalado con éxito daloRADIUS, se accede visitando: **http:// 192.168.8.254/daloradius/index.php**, utilizando las credenciales predeterminadas: **Nombre de usuario** y **contraseña**

Figura 3.47. Inicio de sesión en daloRADIUS

12.1. Registro de equipos de autenticación de acceso en daloRADIUS

Se procedió a registrar las direcciones IP de los equipos autenticación de acceso, la clave secreta y se le asignó un nombre NAS.

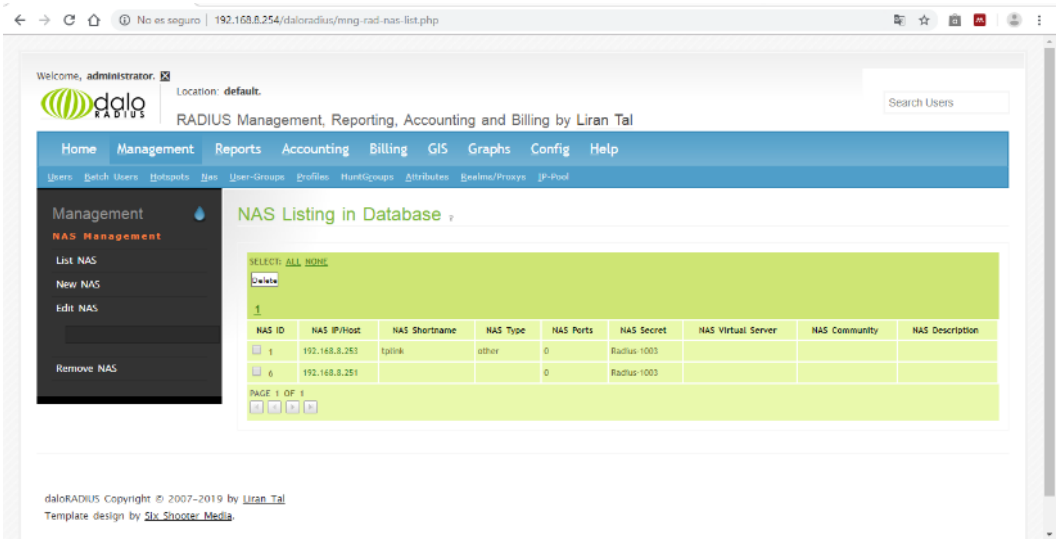


Figura 3.48. Registro de equipos de autenticación de acceso en daloRADIUS.

12.2. Creación de usuarios en DaloRADIUS.

Se procedió a crear los usuarios que estarán registrados en la base de datos, los cuales solo tendrán acceso a las redes inalámbricas. Se registró el nombre de usuario y la contraseña de autenticación.

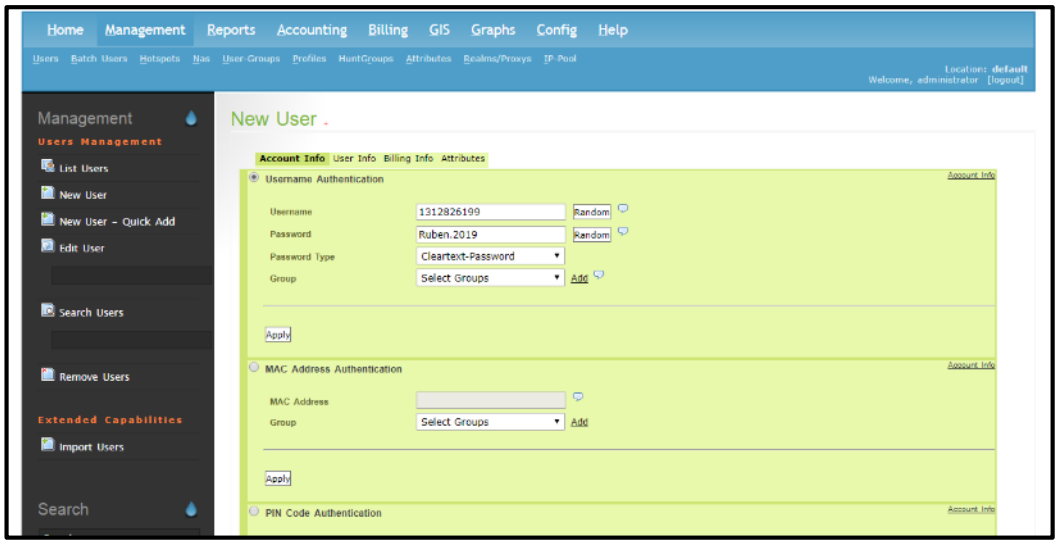


Figura 3.49. Creación de usuarios en daloRADIUS.

12.3. Listar usuarios creados en DaloRADIUS.

Una vez creados los usuarios se pudieron listar.

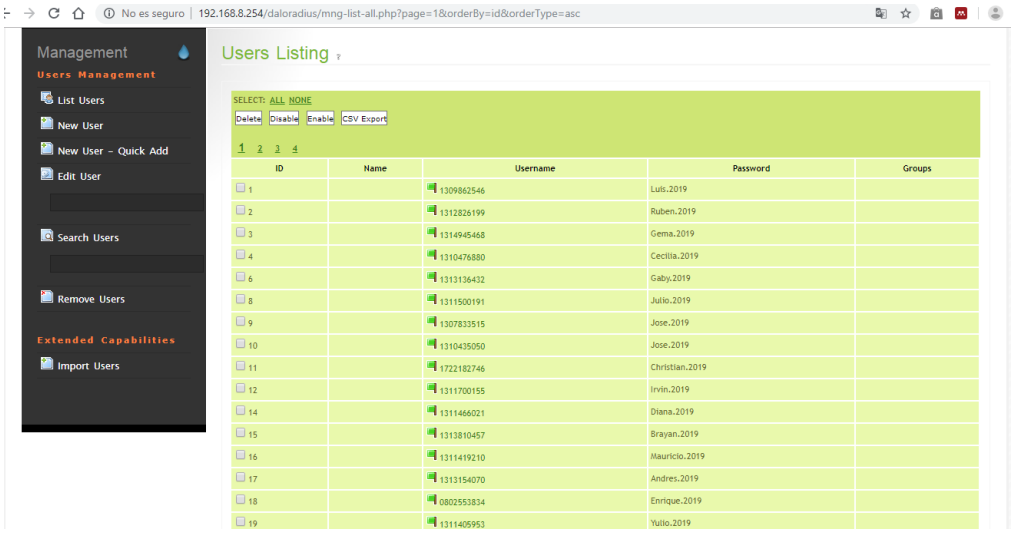


Figura 3.50 Listado de usuarios creados en daloRADIUS.

El siguiente paso es la configuración de los equipos inalambricos, como se muestra acontinuación:

13. Configuración del equipo inalámbrico

Se configuró el router inalámbrico asignándole un nombre a la red, en este caso ESTUDIANTES_POSGRADO.

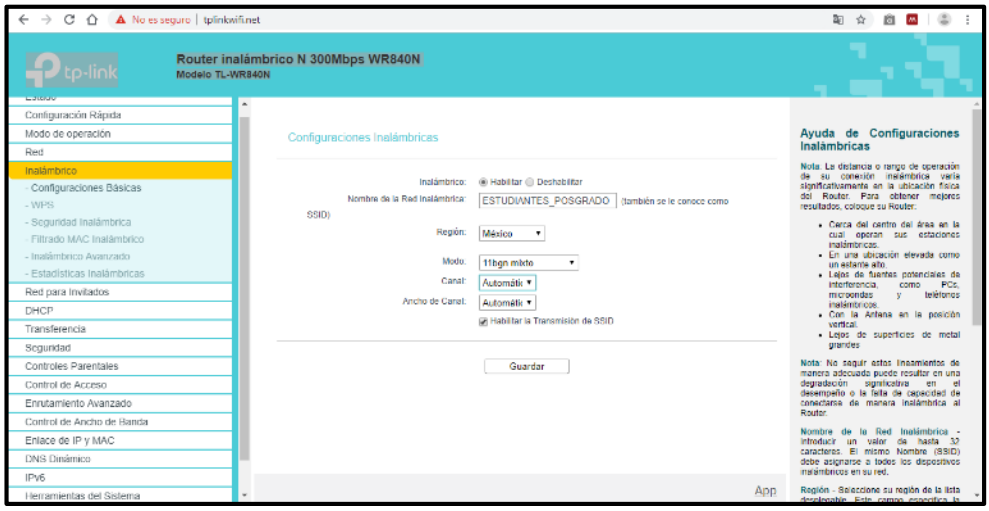


Figura 3.51. Configuración de red inalámbrica.

13.1. Se realizó la configuración de WAN, asignándole una IP estática: 192.168.8.251

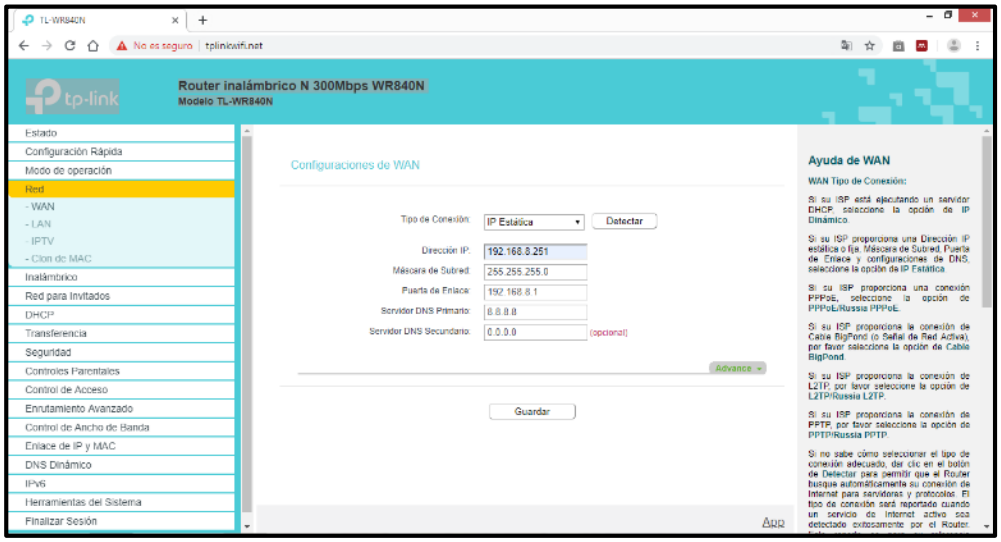


Figura 3.52. Configuración de WAN.

13.2. En la configuración de la seguridad inalámbrica se seleccionó WPA/WPA2-Empresarial, se ingresó la dirección IP que se le asignó al servidor RADIUS: en nuestro caso **192.168.8.254** y la contraseña: **Radius -1003** asignada durante la configuración en daloRADIUS.

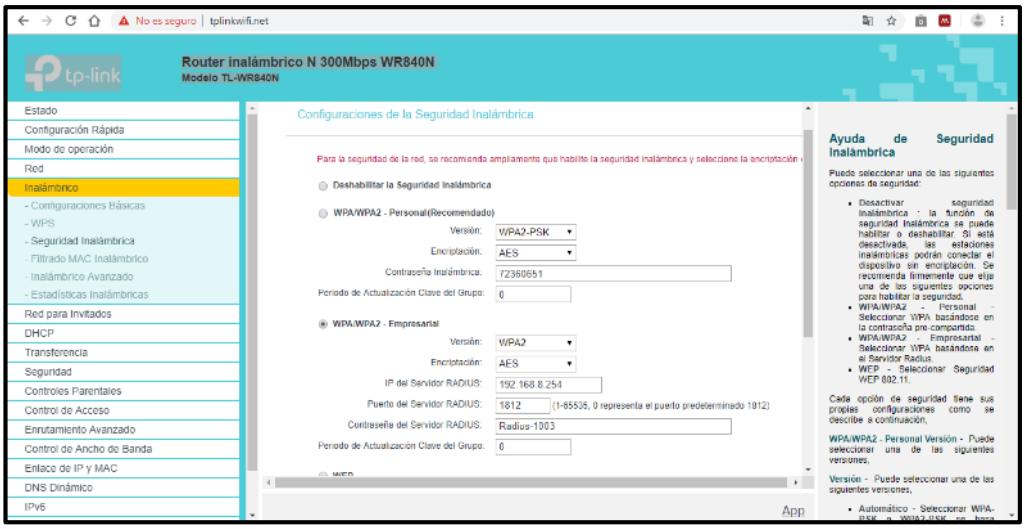


Figura 3.53. Configuración de seguridad inalámbrica.

13.3 Pruebas de Autenticación

Terminada la configuración de los equipos inalámbricos fue necesario realizar las pruebas de autenticación de los usuarios, como se puede visualizar en las siguientes imágenes, la primera consiste en una prueba de implementación realizada en un entorno no universitario y la segunda dentro del Edificio de Posgrados de la ESPAM MFL.

Prueba en ambiente no universitario

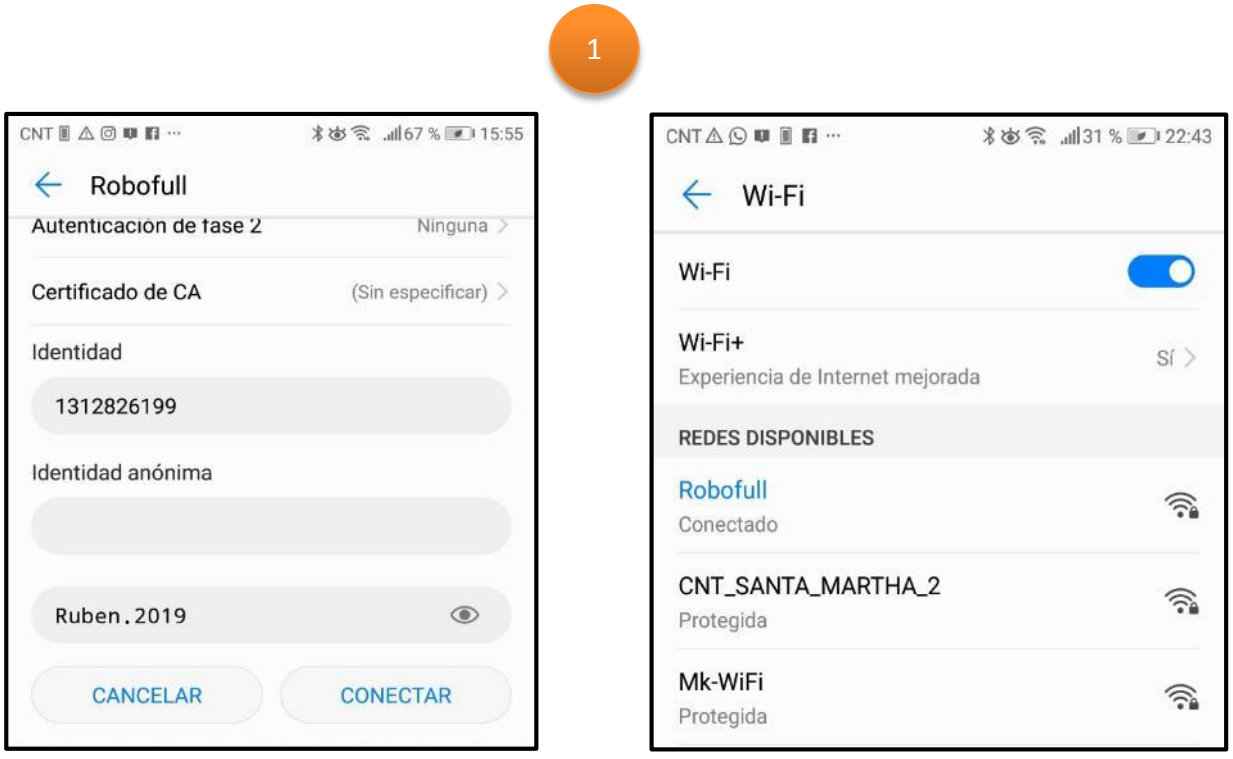


Figura 3.54. Prueba de autenticación en implementación de servidor RADIUS en un ambiente no universitario.

Prueba en ambiente universitario

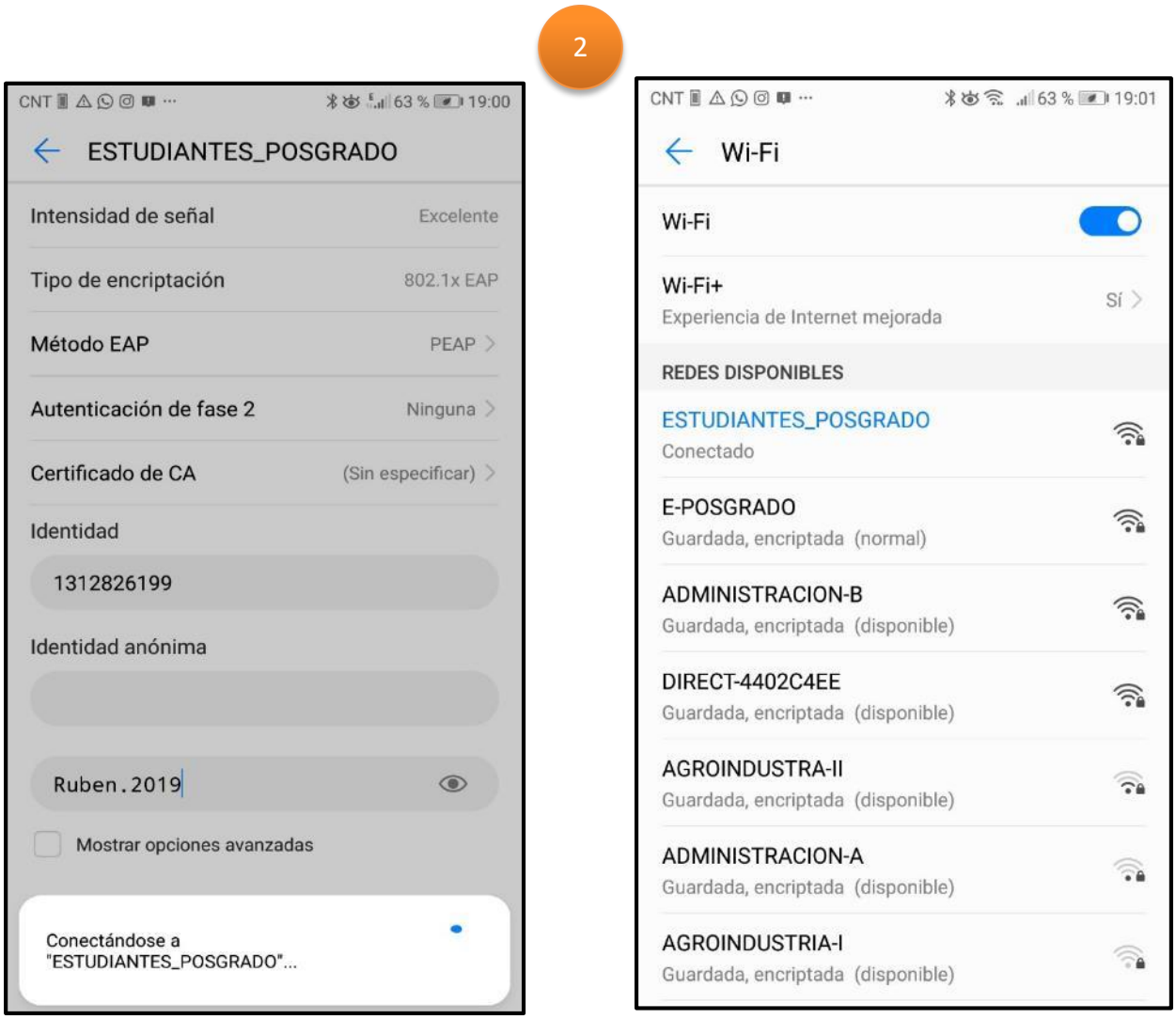


Figura 3.55. Prueba de autenticación en implementación de servidor RADIUS en Edificio de Posgrado.

Este fue el procedimiento a seguir para la implementación de un servidor RADIUS dentro de la red inalámbrica del sector 8 de la ESPAM MFL, realizado en el edifico de Posgrado.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Se presentan los siguientes resultados:

- En el análisis de la organización se pudo constatar de que la Unidad de tecnología la ESPAM MFL (UTI) consta con una estructura orgánica donde se incluye el área de diseño e instalación de redes, sin embargo, no cuenta con un comité informático que se encargue de tomar las decisiones referentes a la implementación de controles y herramientas para mejorar la seguridad de la información institucional.

- La UTI cuenta con normativa aprobada por el Honorable Consejo Politécnico, se han definido políticas y procedimientos para la seguridad de la información, controles internos entre otros, en el caso particular del acceso y seguridad de las redes inalámbricas hay procedimientos que la unidad debe seguir y no las ha ejecutado y tampoco han sido difundidos a los usuarios (docentes, administrativos y estudiantes) desconociendo su contenido, alcance y restricciones; según la encuesta realizada a los usuarios del área de Posgrado el 81% desconoce sobre la existencia de una política de seguridad de la información, el 94% sobre su socialización, el 71% sobre la política del buen uso del internet y un 88% sobre la concientización sobre temas de seguridad de información universitaria.

- Actualmente el mecanismo de acceso a las redes inalámbricas implementado actualmente son las claves de seguridad, al no ejecutarse procesos para atender solicitudes de autorización, no se puede controlar la propagación de las mismas, según los datos obtenidos el 63% asegura que le comparten la clave de seguridad para acceder a las redes inalámbricas.

- No se realiza un control o monitoreo de las actividades que los usuarios realizan cuando acceden a las redes inalámbricas, por lo que no existen restricciones en el uso de los recursos de red, los usuarios acceden a sitios que no son para fines académicos, sin embargo, solo el 32% de los encuestados afirma que accede a sitios no académicos.

- Dentro de su normativa interna, la UTI establece la implementación de un portal cautivo como mecanismo de control de acceso a las redes, pero hasta la actualidad no ha sido puesta en marcha.

- La caracterización de las redes inalámbricas realizada dio como resultado de que algunas redes no tiene ningún tipo de seguridad establecida (WPA/WPA2) o un mecanismo de autenticación para poder acceder a ellas; en el área de Posgrado a pesar de que no hay redes inalámbricas abiertas, el 85% de las redes tienen la misma clave de seguridad.

- El 50% de los usuarios en el área de posgrado afirman conectarse a una red inalámbrica por medio de Smarphones, Tablets u otro dispositivo.

- Se realizó una prueba de implementación del servidor RADIUS en un ambiente no universitario, la cual fue exitosa, y sirvió como guía para la implementación final.

4.2. DISCUSIÓN

Según lo observado en la actualidad dentro del Sector 8 de la ESPAM MFL se ha utilizado como mecanismo de control de acceso a las redes inalámbricas claves WPA Personal y WPA2-Personal con cifrado TKIP, estos tienen un nivel de seguridad aceptable y un rendimiento normal, en comparación con WPA2 Enterprise que permite la autenticación mediante el estándar IEES 802.1X con método de autenticación EAP (Protocolo de autenticación extensible), la misma que al utilizar un servidor de autenticación como RADIUS emplea para su comunicación una clave secreta la cual se valida por un punto de acceso (Router o access point) que actúa como intermediario entre el solicitante y el servidor AAA, lo que representa una mayor nivel de seguridad ya que permite la generación de claves individuales para que los usuarios se puedan autenticar al conectarse a una red inalámbrica, sin un usuario no se encuentra dentro de la base de datos del servidor no se podrá autenticar correctamente y hacer uso de los recursos de red.

La implementación del servidor RADIUS en el Sector 8 de la ESPAM MFL partió de un análisis de la organización sobre el cumplimiento de la política de seguridad de la información institucional, buen uso de internet y de los procedimientos y mecanismos establecidos para el acceso a las redes inalámbricas, al encontrarse una problemática social sobre el actual control de acceso a las redes y la utilización de los recursos disponibles, se procedió a la implementación de una solución que permita lograr un mayor nivel de seguridad y al mismo tiempo permita la autenticación de usuarios a través de una mejor gestión de credenciales como lo es un servidor RADIUS.

Dentro de la revisión bibliográfica que sustenta este trabajo se pueden encontrar otros similares relacionados con la implementación de un servidor AAA (RADIUS o TACAS+) tales como los desarrollados por Paredes (2013) y Valdivieso (2015) sin embargo no hacen un mayor énfasis en la importancia que tiene la implementación de un servidor de autenticación desde la aplicación de una política de control de acceso como lo hace la presente investigación, en donde

se demuestra que según los datos obtenidos en la entrevista y encuesta a los usuarios no existe un cumplimiento satisfactorio de los procedimientos y procesos definidos para restringir el acceso a las redes inalámbricas y a los recursos disponibles, como también se pudo observar también en la realidad actual del Sector 8 de la ESPAM MFL que aunque existen medidas de seguridad comúnmente utilizadas como WPA y WPA2, estas *no garantizan la confiabilidad que debería haber en una red inalámbrica y es necesario un método de seguridad de alto nivel como un servidor RADIUS*, tal como lo manifiestan Cuanilo y Gonzáles(2013).

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se concluye lo siguiente:

Por medio de los instrumentos utilizados para la recopilación de información, se llevó a cabo el análisis de la problemática existente con las redes inalámbricas del Sector 8 de la ESPAM MFL, con la cual se detectaron carencias en el control de acceso, la necesidad de un mayor nivel de seguridad mediante la implementación de un servidor de autenticación como es RADIUS.

La implementación de un mecanismo de seguridad en las redes inalámbricas trabaja adecuadamente cuando se encuentra enmarcada dentro de normas y políticas claramente establecidas y aplicadas y las mismas son socializadas con los usuarios de una organización, al no cumplir estas políticas puede representar vulnerabilidades a la red.

La utilización de servidores virtuales disminuye el costo de implementación, obteniendo un mayor aprovechamiento de los recursos disponibles.

Los equipos que conforman la infraestructura de red del Sector 8 están habilitados para poder soportar el estándar IEEE 802.1X, en la actualidad la mayoría de equipos de acceso de las diferentes fabricantes están diseñados para ser compatibles con este estándar, lo que facilita la integración de la seguridad en redes que no cuentan con un control de acceso a los usuarios.

Establecer un esquema de seguridad basado en autenticación de usuarios es de mucha utilidad ya que sirve para proteger la información que circula por la red. Con la implementación de un servidor AAA se controla a los usuarios que acceden a la red universitaria otorgando solo acceso a los usuarios permitidos.

5.2. RECOMENDACIONES

Se recomienda lo siguiente:

A la Unidad de Tecnología de la ESPAM MFL (UTI) cumplir con sus políticas, normativas y las demás establecidas en normas nacionales e internacionales o marcos de referencia para conseguir una mejor organización interna en materia de seguridad informática.

A la Unidad de Tecnología implementar mecanismos de control de acceso que permitan realizar una mejor gestión y administración de las redes inalámbricas y garantizar una mayor seguridad a las mismas, así como también lograr un buen aprovechamiento de los recursos de red disponibles a los usuarios.

Llevar a cabo la implementación del servidor RADIUS en el Campus Politécnico de la ESPAM MFL, partiendo desde un diagnóstico inicial para comprobar la compatibilidad de la infraestructura tecnológica con el estándar 802.1X en los demás sectores del Campus.

De implementarse el servidor RADIUS en el Campus Politécnico se debe establecer un mecanismo formal para llevar un mejor control de la administración de credenciales de autenticación, solicitando cada periodo académico la actualización de listas de usuarios a las unidades administrativas correspondientes.

BIBLIOGRAFÍA

Acrylic WiFi software. (2019). Analizador WiFi - Escaner WiFi - Cobertura WiFi. https://www.acrylicwifi.com/programas-software-herramientas-wifi/

Albujar Moreno, O. R. (2017). Diseño de un sistema de seguridad de red basado en la integración de los servidores RADIUS–LDAP en linux para fortalecer el acceso de la red de la Clínica Milenium Chiclayo 2016.

Allauca, L. (2016). “Diseño e implementación de un sistema de seguridad para el acceso de la red inalámbrica del Colegio Otto Arosemena Gómez”. (Tesis). Escuela Superior Politécnica del Litoral. Guayaquil

Arana, J. R., Villa, L., & Polanco, O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. Ingeniería y Competitividad, 15(1), 127-137.

Aryeh, F. L., Asante, M. and Danso, A. E. Y. (2016), “Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication”, Ghana Journal of Technology, Vol. 1, No. 1, pp. 40 - 45.

Calienes, R. I. G. (2015). Despliegue del Servicio eduroam en el Campus Universitario de la UNMSM.

Capcha, R. O. T., Quispe, H. G. M., & Quintana, C. M. (2017). Evaluación del desarrollo de políticas de seguridad de información. Ciencia & Desarrollo, (18).

Cárdenas torreblanca, m. V., & quispe ruelas, f. E. Propuesta de una red segura para la interconexión y cooperación de las comisarías y municipalidades de arequipa utilizando los protocolos vpn y olsr con servidor radius y monitoreo nagios.

Cárdenas, B., & Patricio, C. (2017). Administración y gestión de usuarios para acceso a la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas basado en el protocolo 802.1 x(Bachelor's thesis).

Casanova Gallegos, C. F. (2010). Control de acceso a una red inalámbrica privada con administración centralizada en 802.1 X.

CEDIA. (2014). Informe de resultados de la “1° encuesta de seguridad de la información en universidades ecuatorianas miembros de CEDIA. Recuperado de https://csirt.cedia.org.ec/wp-content/uploads/2014/05/Informe-de-Resultados-2014.pdf

CEDIA. (2017). Informe del estado de tecnologías de la información y la comunicación en las universidades ecuatorianas. Recuperado de https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/UETIC_2017.pdf

Centro Criptológico Nacional. (2017). Guía de Seguridad de las TIC CCN-STIC 816. Recuperado de https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html

Chaparro, R. A., y Fajardo, M. V. (2007). Análisis de desempeño y evaluación de requerimientos AAA en protocolos de seguridad sobre redes inalámbricas IEEE 802.11. Ciencia e Ingeniería Neogranadina, 16(2), 7. Recuperado de http://www.redalyc.org/articulo.oa?id=91116208

Contraloría General del Estado. (2014). Normas del control interno de la contraloría general del estado 410 TECNOLOGÍAS DE LA INFORMACIÓN. Recuperado de https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Cubillos Pinilla, D. E. (2013). Políticas de seguridad para redes inalámbricas (Bachelor's thesis, Universidad Piloto de Colombia).

Escalona, S. B. (2012). Protocolos de control de acceso RADIUS. Revista Telemática, 10(1).

Espinosa, F. S., García, J. V., & Llanos, D. B. (2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. Revista Ibérica de Sistemas e Tecnologias de Informação, (E15), 24-38.

Enaceanu, A., & Garais, G. (2010). Cost Effective RADIUS Authentication for Wireless Clients. Database Systems, 27.

Dussan, C. A. (2006). Políticas de seguridad informática. Entramado, 2(1). Recuperado de www.redalyc.org/pdf/2654/265420388008.pdf

González Paz, A. (2017). Mecanismos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos (Doctoral dissertation, Universidad Central" Marta Abreu" de Las Villas, Facultad de Ingeniería Eléctrica, Departamento de Electrónica y Telecomunicaciones).

Guanilo Gómez, P. R., & Gonzales Meléndez, P. J. (2013). Diseño de un modelo de autenticación Radius para reforzar los niveles de seguridad en el diseño de redes inalámbricas IEEE 802.11 x para la Cooperativa de Ahorro y Crédito Tumán.

Gutiérrez, M. S. (2012). Mecanismos De Seguridad En Redes Inalámbricas.

ISO 27002.es (2014). PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002 https://iso27002.wiki.zoho.com/ISO-27002.html

Martínez Candel, C. (2015). Acceso WiFi mediante servidor centralizado implementando puntos de acceso basados en Open-WRT

Martinez Cáceres, C. F., & Oñate Haro, O. M. (2017). Mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético (Bachelor's thesis, Riobamba, Universidad Nacional de Chimborazo).

Mauricio, M. (2010). Diseño e implementación de arquitectura de conectividad y seguridad AAA en UDNET (authentication, authorization and accounting).

Mendoza, C. M. H., Vidal, L. M. R., & Almanza, M. A. (2017). Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. Revista Iberoamericana de Producción Académica y Gestión Educativa, 4(7).

Monsalve, J. A., Aponte, F. A., y Chaparro, F. (2016). Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. Dyna, 82(189), 226-232. Recuperado de http://www.redalyc.org/pdf/496/49635366029.pdf

Morales, J. J., Cedeño, L. C., Párraga, J. A., y Molina, B. A. (2018). Propuesta Metodológica para Proyectos de Infraestructura Tecnológica en Trabajos de Titulación. Información tecnológica, 29(4), 249-258. Recuperado de

https://scielo.conicyt.cl/pdf/infotec/v29n4/0718-0764-infotec-29-04-00249.pdf

Morales, M. (2014). Seguridad en redes inalámbricas. Recuperado de https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas

Mori, J. A. L. (2017). Introducción a un sistema de gestión de accesos a una red Wi-Fi utilizando software libre. *Perspectiv@ s*, *13*(12), 20-22.

Ocampo Vélez, L. S., & Vivanco Encalada, H. P. (2016). Implementación Active Directory aplicando el estándar 802.1 x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja (Bachelor's thesis).

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. International Journal of Morphology, 35(1), 227-232

Paredes Samaniego, M. P. (2013). Implementación de un plan piloto de seguridad bajo el protocolo IEEE 802.1 x para el departamento de gestión tecnológica del ministerio de telecomunicaciones y sociedad de la información (Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería en Redes y Comunicación de Datos).

SB, V. K., Kumar, P., Shahi, B., Jha, D., & Monica, B. V. (2016). Role of Diameter Based Protocol in enhancing of new and Upcoming Technologies. Procedia Computer Science, 78, 415-422.

Sikarwar, A. P. S., & Saxena, P. An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS. International Journal of Computer Applications, 975, 8887.

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Primera edición. Recuperado de http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Vaca Aguirre, W. E. (2015). Control de accesos y administración de recursos de RED mediante un servidor AAA en el GAD Municipal de Urcuquí usando software libre (Bachelor's thesis).

Valdivieso Villamarín, Á. A. (2015). Diseño e implementación de un sistema de autenticación y políticas de seguridad mediante un servidor AAA, haciendo uso del estándar IEEE 802.1 xy los protocolos Radius y Tacacs+ para la red corporativa de la empresa proyectos integrales de Ecuador PIL SA (Bachelor's thesis).

Vallejo, T. (2010). Vulnerabilidades y niveles de seguridad de redes WI-FI. Recuperado de http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf

Zhang, J., Guo, Y., Chen, Y., & Ma, J. (2015, December). AAA Based on 802.1 x Authentication. In 2015 Joint International Mechanical, Electronic and Information Technology Conference (JIMET-15). Atlantis Press

ANEXOS

ANEXO 1

SOLICITUD DE PERMISO PARA LA FASE DE DESARROLLO DEL TRABAJO DE TITULACIÓN

Calceta, 29 de enero de 2019

Mg. Joffre Moreira Pico
COORDINADOR DE MAESTRÍA TI ESPAM MFL

De mis consideración.-

Reciba un cordial saludo de quién escribe, Ing. Rubén Loor Anchundia egresado de la I cohorte de la Maestría de Tecnologías de Información mención en Redes y Sistemas Distribuidos y a la vez deseándole éxitos en cada una de sus actividades encomendadas. Me permito escribirle para solicitarle de la forma más respetuosa posible se me conceda por su digno intermedio a quién corresponda tramitar el permiso para proceder a desarrollar mi trabajo de titulación: **ACCESO A REDES INALÁMBRICAS DE LA ESPAM MFL MEDIANTE UN SERVIDOR RADIUS,** el mismo que fue aprobado por la Junta Académica de Posgrado, tomando como objeto de estudio el sector 8 del Campus Politécnico el cual comprende las áreas de Edificio de Computación, Posgrado, Bibliotecas y Hotel Higuerón. Con la implementación del presente trabajo de titulación lo que se busca **es mejorar el desempeño de las redes inalámbricas de nuestra institución y a la vez establecer un control más eficiente del acceso a las mismas.** Así mismo, de ser concedido el permiso correspondiente, solicito se me facilite la información que sea útil y se me de las facilidades para poder desarrollar e implementar mi trabajo.

Pensando siempre en el mejoramiento continuo de nuestra querida institución he propuesto este trabajo de titulación.

Reiterándole mis sentimientos de consideración y estima, sin otro particular me despido.

Atentamente,

Rubén Loor Anchundia
Egresado de Maestría TI ESPAM MFL

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
COORDINACIÓN DE MAESTRÍA
RECIBIDO POR: Aida Cevallos
Fecha: 30-01-2019
Hora: 8:50

ANEXO 2

ACEPTACIÓN DE SOLICITUD DE PERMISO PARA LA FASE DE DESARROLLO DEL TRABAJO DE TITULACIÓN

REPÚBLICA DEL ECUADOR

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
Ley 99- 25 R.O. 181 -30-04-1999

UNIDAD I
TECNOL

COORDINACIÓN ACADÉMICA
MAESTRÍA TI
Para la firma correspondiente
13/02/19

Memorando Nro.: ESPAM MFL-CUT -2019- 039-M
Calceta, 08 de febrero de 2019

PARA: Dr.C. María Fernanda Garzón Félix
DIRECTORA DE POSGRADO Y FORMACIÓN CONTINUA

ASUNTO: En atención a Memorando N.º: ESPAM MFL-DPFC-2019-041-M

Reciba un coridal saludo, en atención a Memorando N.º: ESPAM MFL-DPFC-2019-041-M, me complace en informar que su requerimiento ha sido autorizado y coordinado con el Ing. Patricio Zambrano Ganchozo, Mg. y el Ing. Belisario Vera Vera, Mg. personal encargado de las Redes y Telecomunicaciones. Por tanto el maestrante Ing. Rubén Loor Anchundia podrá realizar el análisis respectivo, como parte de sus desarrollo de trabajo de titulación, cuyo objetivo es presentar una propuesta que permita mejorar el desempeño de las redes inalámbircas en las áreas (Edificio de Computación, Posgrado , Biblioteca y Hotel Higuerón).

Sin otro particular me suscribo de Usted.

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
COORDINACIÓN DE MAESTRÍA
En II - 1 Cohorte
RECIBIDO POR: Paula Gonzalez
Fecha: 14-02-2019
Hora: 14:51

Cordialmente,

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
COORDINACIÓN DE TECNOLOGÍA

Lic. Geovanny García Montes
COORDINADOR (E) DE LA UNIDAD TECNOLÓGICA DE LA ESPAM MFL

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA
FECHA: 13-02-2019
HORA: 15:53
RECIBIDO POR:

ANEXO: Memorando N.º: ESPAM MFL-DPFC-2019-041-M

GGM/jvg

ANEXO 3

SOLICITUD DE USUARIOS Y CONTRASEÑAS PARA CONFIGURACIÓN DE PUNTOS DE ACCESO

Calceta, 03 de julio de 2019

Lic. Geovanny García Montes
COORDINADOR DE UNIDADA DE TI ESPAM MFL

De mis consideraciones.-

Reciba un cordial saludo, deseándole éxitos en sus actividades y a la vez le solicito de la forma más respetuosa posible autorice a quién corresponda me facilite las credenciales: usuario y contraseña de los puntos de acceso inalámbricos del Edificio de posgrado, para poder realizar la configuración correspondiente para la implementación del servidor RADIUS en dicho lugar, ya que toda vez que me encuentro desarrollando la fase final del trabajo de titulación: **IMPLEMENTACIÓN DE SERVIDOR RADIUS EN EL SECTOR 8 DE LA ESPAM MFL,** necesito de dicho requerimiento, y a la vez se me conceda una dirección IP que esté dentro del rango de direcciones IP asignadas, para poder asignarle al servidor RADIUS, y de esta manera ponerlo en funcionamiento.

Por la atención prestada a la presente, le quedo muy agradecido.

Atentamente,

José Rubén Loor Anchundia
MAESTRANTE DE LA MAESTRÍA TI ESPAM MFL

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
RECIBIDO
FECHA: 03/07/2019 HORA 16:14
COORDINACIÓN DE TECNOLOGÍA

ANEXO 3-A

ENTREGA DE USUARIOS Y CONTRASEÑAS PARA CONFIGURACIÓN DE PUNTOS DE ACCESO

EQUIPOS DE REDES WI-FI UBICADOS EN EL EDIFICIO DE POSGRADO

RED WIFI	MARCA	IP	CLAVE	USUARIO
AGROINDUSTRA-II	Mikrotik	192.168.50.1	adminEspam*0.	Admin
AGROINDUSTRA-I	Mikrotik	192.168.50.2	adminEspam*0.	Admin
TURISMO	Mikrotik	192.168.50.3	adminEspam*0.	Admin
ADMINISTRACION-B	Mikrotik	192.168.50.4	adminEspam*0.	Admin
ZOOTECNIA	Mikrotik	192.168.50.5	adminEspam*0.	Admin
ADMINISTRACION-A	Mikrotik	192.168.50.6	adminEspam*0.	Admin
EMPRENDIMIENTO	TP-LINK	192.168.0.254	adminEspam*0.	root
POSGRADO	TP-LINK	192.168.0.253	adminEspam*0.	root

ANEXO 4

FORMATO DE ENTREVISTA AL PERSONAL DE UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL

ENTREVISTA AL PERSONAL DE UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL

ENTREVISTADO:

CARGO: Coordinador de Tecnología

FECHA DE ENTREVISTA:

ORGANIZACIÓN

¿La unidad de tecnología cuenta con una estructura organizativa?

_____

¿Existe un manual de funciones y responsabilidades del personal de la Unidad de tecnología de la ESPAM MFL?

_____

¿Quién o quienes al interior de la unidad de tecnología es/son el/los responsable/s de la administración de las redes inalámbricas de la institución?

_____

_____

¿Existe una normativa interna para el aseguramiento de la información institucional?

_____

_____

¿Se establecen acuerdos de confidencialidad para el buen tratamiento de la información?

_____

_____

¿Existe un comité de seguridad de la información que se encargue de la toma de decisiones referentes a la implementación de controles y herramientas para mejorar la seguridad de la información institucional?

_____

_____

¿Existe un presupuesto exclusivo para la seguridad de la información?

_____

_____

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

¿Existe una política de seguridad de información institucional?

_____

_____

¿A qué estándar o norma ISO se alinea la política de seguridad institucional?

_____

¿La política de seguridad de información está aprobada/implementada?

_____

_____

¿La política de seguridad de la información se ha socializado en la institución?

_____

_____

¿Existe una política del buen uso de internet?

_____

_____

PROCEDIMIENTOS

¿Qué procedimientos se implementan para efectivizar la política de seguridad de la información en la institución?

_____

_____

¿Se ha concientizado a la comunidad politécnica en temas de seguridad de la información?

_____

_____

ENTREVISTA AL PERSONAL DE UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL

ENTREVISTADO:

CARGO: Técnico de Redes

FECHA DE ENTREVISTA:

REDES

¿Qué mecanismos de control se implementan para el acceso a las redes inalámbricas?

_____

_____

¿Se limita el número de usuarios en el acceso a una red inalámbrica?

_____

¿Cuáles de los siguientes mecanismos de seguridad se utilizan para asegurar la información y sistemas?

Sistema de detención de intrusos ( )

Sistema de prevención de intrusos ( )

Firewall en software ( )

Firewall en hardware ( )

Cifrados de datos ( )

Firmas digitales/certificados digitales ( )

VPN ( )

Listas de control de acceso ( )

Antivirus ( )

AUTENTICACIÓN

¿Se utiliza un sistema de autenticación de doble factor?

Usuario + contraseña + código adicional

_____

_____

AUTORIZACIÓN

¿Existen procesos definidos para atender solicitudes de autorización para el acceso a las redes inalámbricas a los usuarios (administrativos, docentes y estudiantes)?

_____

_____

AUDITORÍA

¿Se realiza un control o monitoreo de las actividades que los estudiantes, administrativos o docentes realizan cuando acceden a las redes inalámbricas?

_____

_____

AMENAZAS Y VULNERABILIDADES

¿Se utiliza alguna herramienta de análisis de vulnerabilidades?

_____

¿Cuáles de los siguientes incidentes han ocurrido con respecto a la seguridad de la información?

Spam ( )

Robo de Información ( )

Fraude económico por medios informáticos ( )

Incumplimiento de la política de seguridad de la información ( )

Denegación de servicios ( )

Suplantación de Identidad ( )

Phishing ( )

Accesos no autorizados a sistemas o información ( )

Malware ( )

SERVICIOS Y RECURSOS

¿Se han definido roles y privilegios para el acceso a los sistemas?

_____

¿A qué servicios pueden tener acceso los usuarios mediante la conexión a las redes inalámbricas?

DOCENTES

_____

_____

ADMINISTRATIVOS

_____

_____

ESTUDIANTES

_____

_____

PLANO DE DISTRIBUCIÓN DE LA RED

¿La distribución lógica de la red se estructura con base a?

- Direccionamiento IP ( )
- Vlans ( )
- Elementos de seguridad ( )

¿La distribución física de la red se estructura con base a?

- Routers ( )
- Switches ( )
- Servidores ( )
- DVRS ( )
- RACKS ( )

ENTREVISTA AL PERSONAL DE UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL

ENTREVISTADO:

CARGO: Administrador de Data Center

FECHA DE ENTREVISTA:

ORGANIZACIÓN

¿A qué estándar o norma ISO se alinea la política de seguridad institucional?

CONTROL DE ACCESO A REDES INALAMBRICAS

¿Qué mecanismos de control se implementan para el acceso a las redes inalámbricas?

¿Cuáles de los siguientes mecanismos se utilizan para la seguridad de la red?

Sistema de detención de intrusos ( )

Sistema de prevención de intrusos ( )

Firewall en software ( )

Firewall en hardware ( )

Cifrados de datos ( )

Firmas digitales/certificados digitales ( )

VPN ( )

Listas de control de acceso ( )

Antivirus ( )

AMENAZAS Y VULNERABILIDADES

¿Se utiliza alguna herramienta de análisis de vulnerabilidades?

_____

¿Cuáles de los siguientes incidentes han ocurrido con respecto a la seguridad de la información?

Spam ( )

Robo de Información ( )

Fraude económico por medios informáticos ( )

Incumplimiento de la política de seguridad de la información ( )

Denegación de servicios ( )

Suplantación de Identidad ( )

Phishing ( )

Accesos no autorizados a sistemas o información ( )

Malware ( )

ANEXO 5

FORMATO DE LA ENCUESTA A USUARIOS

ENCUESTA

Reciba un cordial saludo, deseándole éxitos en sus actividades, a la vez me permito realizar la presente encuesta con el objetivo de determinar el nivel de conocimiento acerca de temas relacionados con la seguridad de la información universitaria, misma que servirá para el desarrollo de un trabajo académico, esperando tener información objetiva y real que permita implementar soluciones tecnológicas que ayuden al mejoramiento institucional.

De antemano le agradezco por su atención.

Fecha:

Lugar:

Encuestado:

Docente ( ) Personal Administrativo ( ) Estudiantes ( )

PREGUNTAS

1. ¿Conoce Usted si existe una política de seguridad de la información?

   Conoce ( ) No conoce ( )

2. ¿Conoce Usted si se ha socializado la política seguridad de la información?

   Conoce ( ) No conoce ( )

3. ¿Conoce Usted si existe una política de buen uso del internet?

   Conoce ( ) No conoce ( )

4. ¿Conoce Usted si se ha concientizado en temas de seguridad de la información universitaria?

   Conoce ( ) No conoce ( )

5. ¿Normalmente cuando usted accede a una red inalámbrica, se conecta por :

   Clave ( ) Usuario y contraseña ( ) Acceso libre ( )

6. Cuando usted intenta acceder a una red inalámbrica por clave, ¿pide autorización o le comparten la clave (contraseña) de acceso?

   Pide autorización ( ) Le comparten la clave ( )

7. Al momento de conectarse a una red inalámbrica aquí en la universidad utiliza **(puede seleccionar más de una):**

- Computador portátil (notebooks) ( )
- Smart phone (teléfono móvil) ( )
- Tablets ( )
- Otro especifique _____

8. ¿A cuáles de los siguientes servicios usted tiene acceso mediante la conexión a una red inalámbrica?

- Sistemas de gestión académica ( )
- Sistemas de encuestas ( )
- Bibliotecas virtuales ( )
- Sitio web institucional ( )
- Correo electrónico ( )
- Juegos en línea ( )
- Páginas web de descargas de películas ( )
- Redes sociales
  - Facebook ( )
  - Instagram ( )
  - Twitter ( )
  - Otro ( )
- Youtube ( )
- Páginas con contenido para adultos ( )
- Otro ( ) especifique: _____

9. ¿Conoce Usted si se implementan acuerdos de confidencialidad para el tratamiento de la información?

Conoce ( ) No conoce ( )

10. ¿Qué tan segura cree usted que esté la información dentro de la institución?

Nada segura ( )

Poco segura ( )

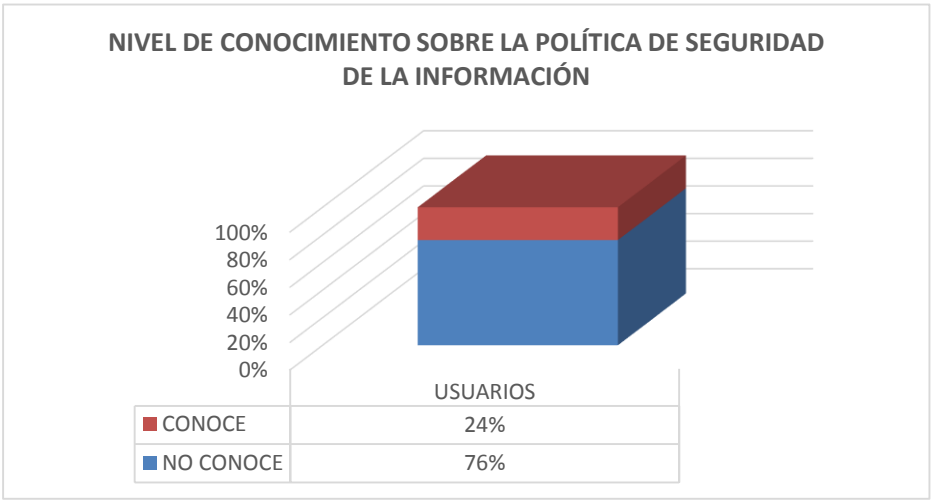
Segura ( )

Muy segura ( )

ANEXO 6

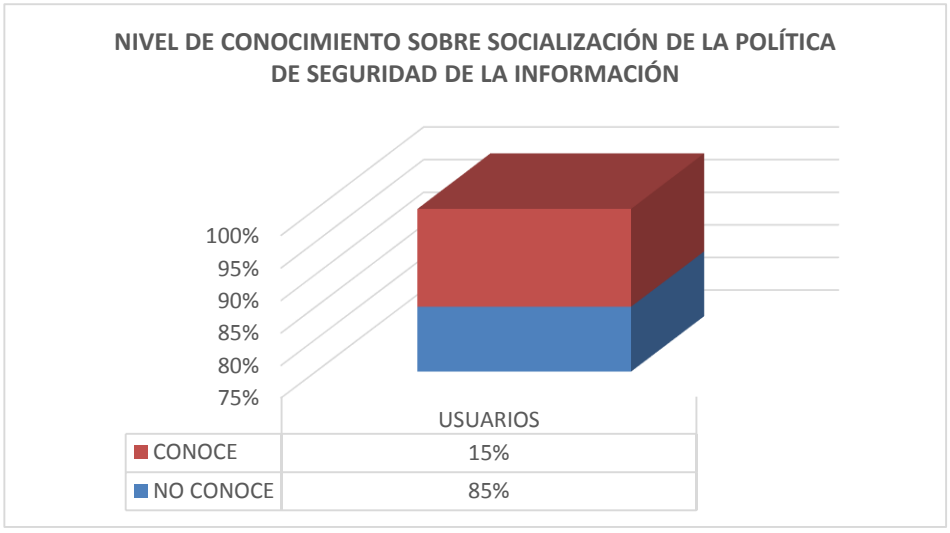
RESULTADOS GENERALES DE LAS ENCUESTA REALIZADA A USUARIOS

Gráfico 5. 1. Nivel de conocimiento sobre la política de seguridad de la información.



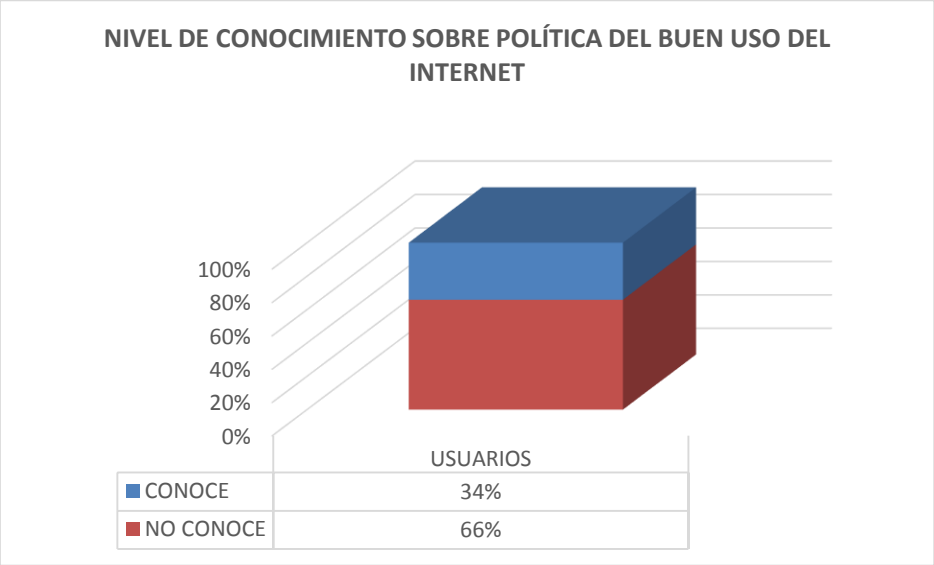
Fuente: La encuesta

Gráfico 5. 2. Nivel de conocimiento sobre socialización de la política de seguridad de la información.



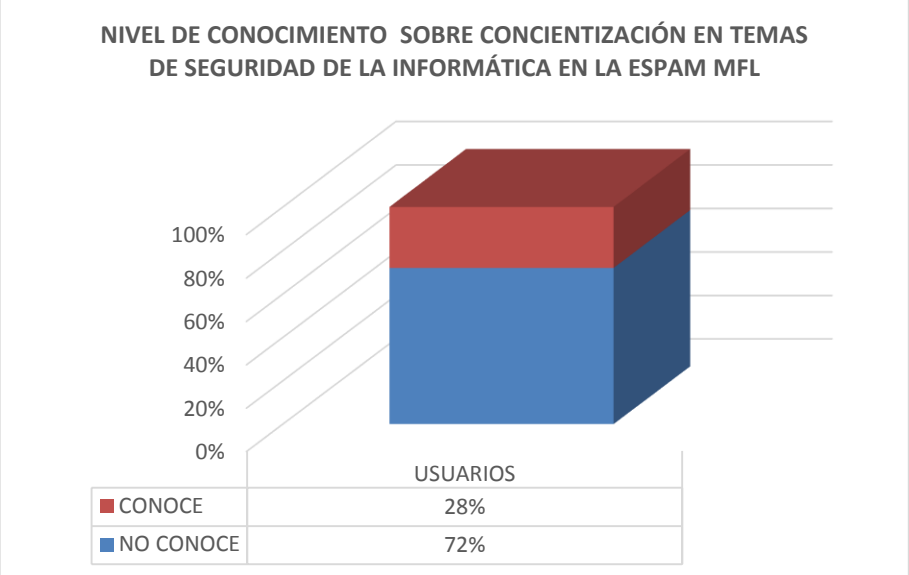
Fuente: La encuesta

Gráfico 5. 3. Nivel de conocimiento sobre política del buen uso del internet.



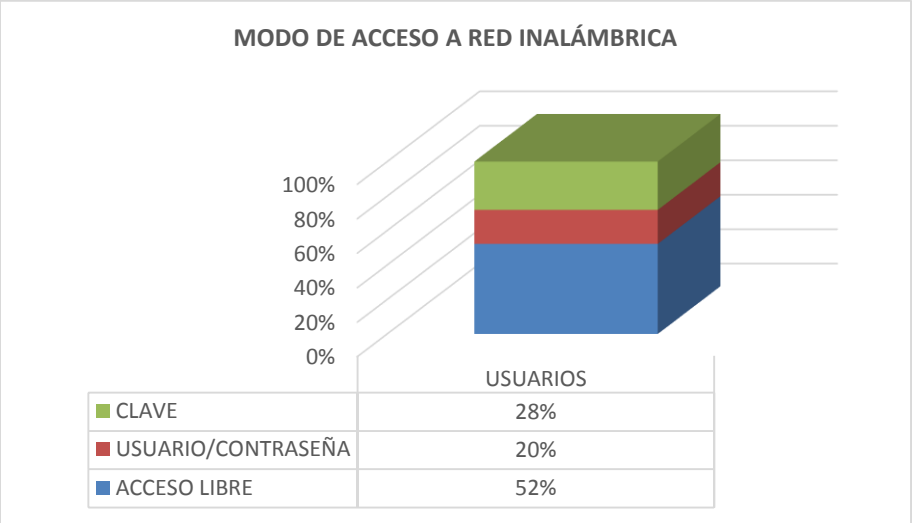
Fuente: La encuesta

Gráfico 5. 4. Nivel de conocimiento sobre concientización en temas de seguridad de la información en la ESPAM MFL.



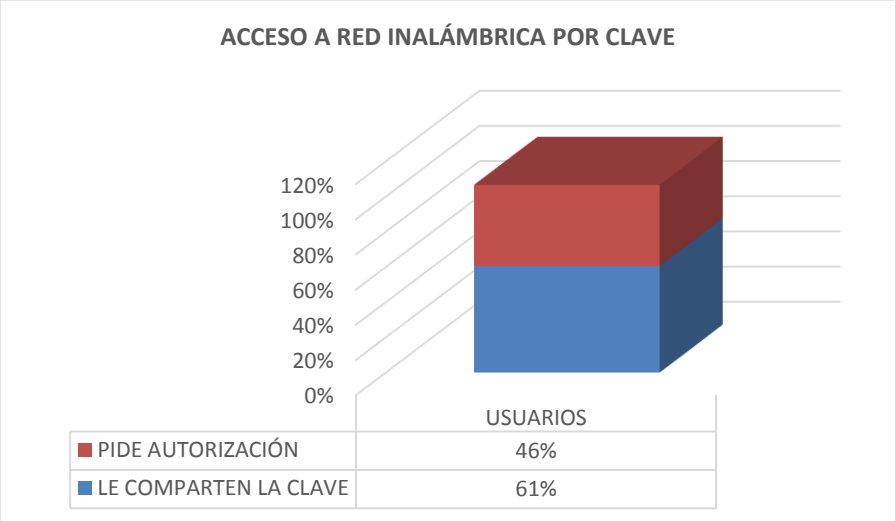
Fuente: La encuesta

Gráfico 5. 5. Modo de acceso a red inalámbrica.



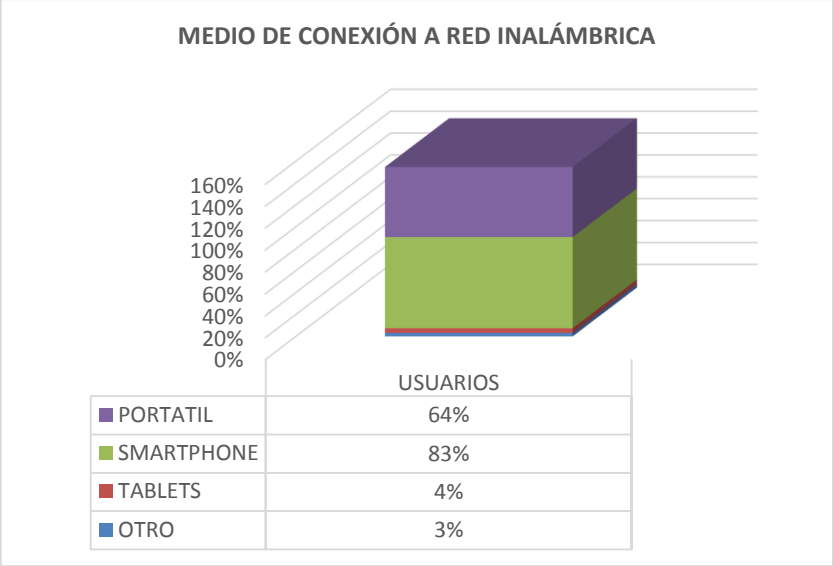
Fuente: La encuesta

Gráfico 5. 6. Acceso a red inalámbrica por clave.



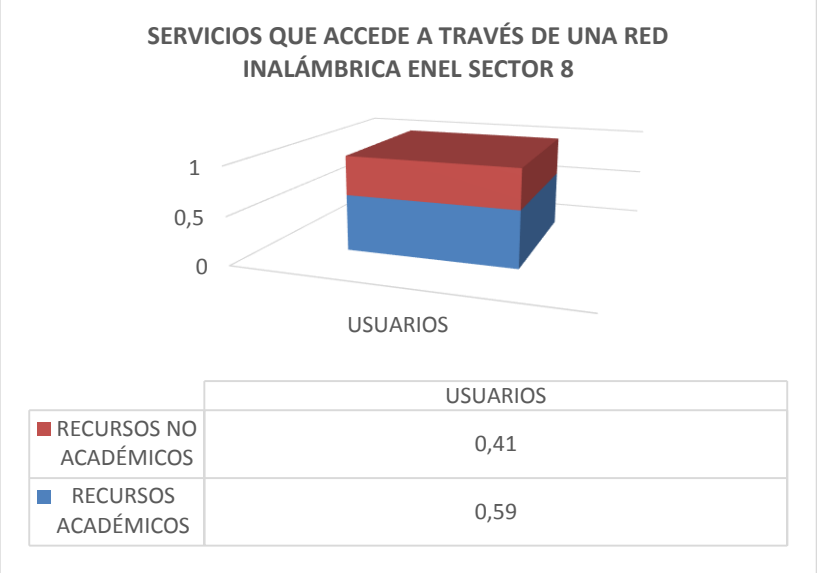
Fuente: La encuesta

Gráfico 5. 7. Medio de conexión a red inalámbrica.



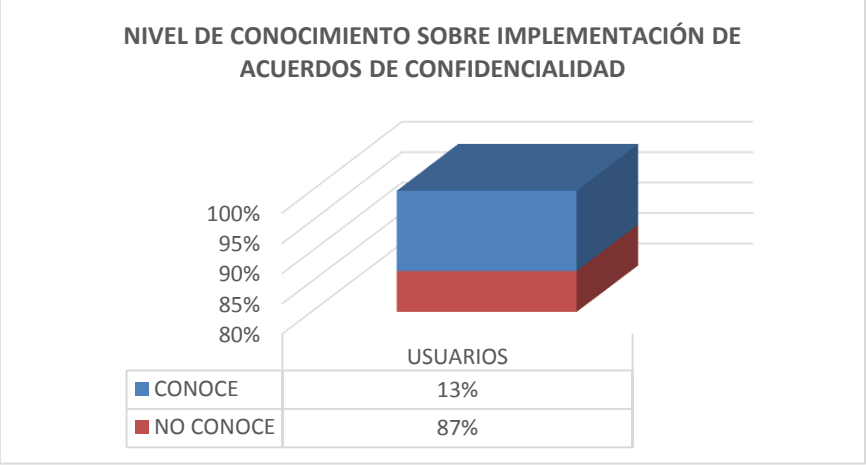
Fuente: La encuesta

Gráfico 5. 8. Servicios que accede a través de una red inalámbrica en el Sector 8.



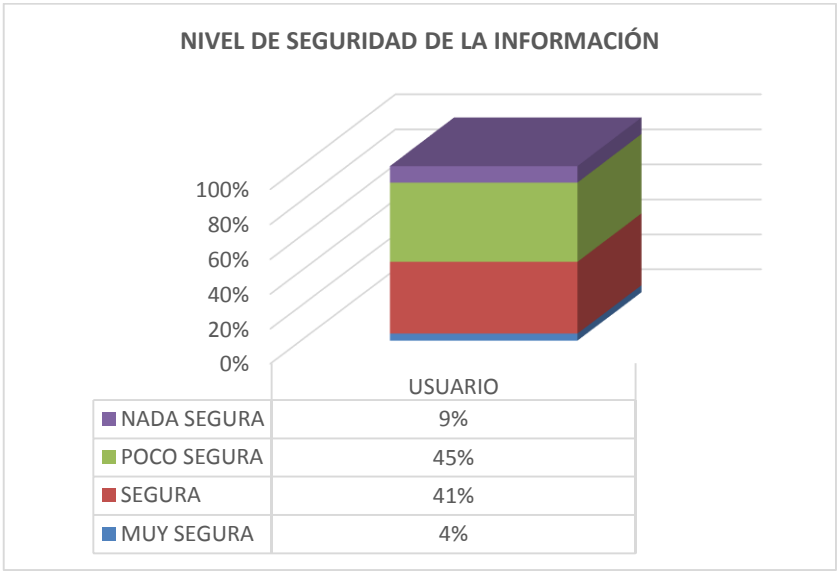
Fuente: La encuesta

Gráfico 5. 9. Nivel de conocimiento sobre implementación de acuerdos de confidencialidad.



Fuente: La encuesta

Gráfico 5. 10. Percepción del nivel de seguridad de la información institucional.



Fuente: La encuesta