UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020

Trabajo de titulación previa la obtención del
Título de Ingeniero en Informática

AUTORES: Piarpuezán López Jefferson Alexander
Riascos Ortiz Dany Alexander

TUTOR: Ing. Del Hierro Mosquera Milton Gabriel, MSc

Tulcán, 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Piarpuezán López Jefferson Alexander con el número de cédula 0401720065 ha elaborado el trabajo de titulación: Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

f.....	**f.....**
Ing. Del Hierro Mosquera Milton Gabriel, MSc	Ing. Hidalgo Guijarro Jairo Vladimir, MSc
TUTOR	**LECTOR**

Tulcán, abril de 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Riascos Ortiz Dany Alexander con el número de cédula 0401819164 han elaborado el trabajo de titulación: Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

f.....	**f.....**
Ing. Del Hierro Mosquera Milton Gabriel, MSc	Ing. Hidalgo Guijarro Jairo Vladimir, MSc
TUTOR	**LECTOR**

Tulcán, abril de 2021

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de **Ingeniería** en la Carrera de Ingeniería en Informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Nosotros, Piarpuezán López Jefferson Alexander con cédula de identidad número 0401720065 y Riascos Ortiz Dany Alexander con cédula de identidad número 0401819164 declaramos: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de nuestra absoluta responsabilidad.

f.....
Piarpuezán López Jefferson Alexander
AUTOR

f.....
Riascos Ortiz Dany Alexander
AUTOR

Tulcán, abril de 2021

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Nosotros, Piarpuezán López Jefferson Alexander y Riascos Ortiz Dany Alexander declaramos ser autores de los criterios emitidos en el trabajo de investigación: "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020" y eximimos expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....
Piarpuezán López Jefferson Alexander
AUTOR

f.....
Riascos Ortiz Dany Alexander
AUTOR

Tulcán, abril de 2021

AGRADECIMIENTO

Agradezco a Dios por haberme dado la salud y vida para poder culminar mis estudios y seguir cumpliendo mis metas propuestas. De la misma manera agradezco a mis padres Sonia Piedad López y Manuel Efraín Piarpuezán Pantoja, que con su esfuerzo y trabajo constante han logrado que sea una persona de bien para la sociedad, ayudándome a cumplir una de mis metas y es la de ser profesional. A mis hermanas y familiares que han complementado la base de mi formación como persona, apoyándome desinteresadamente en los momentos en los que más he necesitado su ayuda para poder cumplir mi objetivo personal. A la Universidad Politécnica Estatal del Carchi, la institución que me dio la oportunidad de cumplir una de mis metas, la de llegar a ser un profesional de mi país, además de ser como mi segundo hogar en donde he adquirido gran conocimiento y valores que me servirán en el ámbito profesional.

Finalmente, agradezco a mi compañero Dany Alexander Riascos Ortiz por compartir y darme la oportunidad de trabajar en el presente trabajo de investigación.

Piarpuezán López Jefferson Alexander

AGRADECIMIENTO

Agradezco en primer lugar a Dios por permitirme seguir compitiendo el día a día con mis seres queridos, por concederme la dicha de luchar por mis sueños, otorgándome el don de la paciencia, tolerancia y sabiduría. De igual manera agradezco a mi familia, quienes me apoyaron en mi desarrollo profesional, brindándome consejos, palabras de aliento y sobre todo su amor incondicional. Agradezco a mi madre, esa mujer luchadora que con sus consejos supo llegar a mí para orientarme por el camino correcto. Agradezco a la noble casona universitaria, la misma que me permitió formar parte de una de sus carreras, esta es Ingeniería en Informática, a los docentes quienes con su ilustre conocimiento supieron encaminarnos en nuestro desarrollo profesional, siendo participes en muchos de nuestros logros académicos.

Finalmente, agradezco a todas las personas que depositaron su confianza en mí, aquellas personas quienes que me brindaron su amistad en todo el trascurso de mi vida universitaria, de igual manera agradezco aquellos amigos que estuvieron en mis días más amargos, motivándome para no declinar de mi objetivo, Gracias a todos.

Riascos Ortiz Dany Alexander

DEDICATORIA

El presente trabajo de investigación denota el trabajo constante que he venido realizando durante el tiempo que este conllevó. En primer lugar, se lo dedico a Dios por haberme dado la fortaleza y sabiduría para superar las grandes adversidades en las que he estado inmerso. A mis padres Sonia Piedad López y Manuel Efraín Piarpuezán Pantoja que de todo corazón han sido un pilar fundamental en mi vida, con sus sabias palabras y consejos han forjado la clase de persona que soy hoy en día; todos mis logros se los debo a ellos, entre los que se incluye este. A mis hermanas Erika, María, Mayra y Viviana que han confiado en mí incondicionalmente, impulsándome con palabras de aliento para no decaer a lo largo de mi travesía universitaria. A mis amigos, cuñados, sobrinos y familiares en general que se han preocupado desinteresadamente por mi bienestar, brindándome su apoyo constante con consejos y palabras de aliento en los momentos difíciles.

Piarpuezán López Jefferson Alexander

DEDICATORIA

En honor al arduo trabajo, esfuerzo y dedicación en mi preparación académica universitaria, dedico mi logro principalmente a Dios quien me brindo salud, sabiduría y permitió hacer posible el sueño más anhelado de cualquier chico, ser un profesional. A mi hijo Dariel Riascos Becerra, que desde su llegada a mi vida me brindo motivos para superarme y soñar en un mejor futuro para los dos, enseñándome a creer en el verdadero amor, alegrando mis días, cambiando mis preocupaciones por sonrisas. A mi madre Yajaira Ortiz Llumiquinga, quien me dio la vida y supo brindarme su amor incondicional, guiándome en la vida por el camino correcto, le agradezco por sus innumerables palabras de alientos, consejos y sacrificios que realizo por mirarme como un profesional. Gracias por confiar en mí. A mi hermano Johan Mallama Ortiz, mi compañero en la vida, mi amigo quien con sus palabras me enseñó a valorar cada día de mi vida, siendo un apoyo y fortaleza en aquellos momentos difíciles, compartiendo conmigo risas, consejos y penumbras a ti gracias, gracias, hermano por todo. Agradecer a mi familia, a mis tíos Johana Ortiz, Marco Ayala, Diana Almeida, Carlos Ortiz, quienes fueron participes en mi logro al brindarme su ayuda en el momento más oportuno de mi vida. A mis abuelitos Pastora Llumiquinga y Ramiro Ortiz quienes con sus consejos y vivencias supieron enseñarme el valor de la honestidad, rectitud y tolerancia.

Riascos Ortiz Dany Alexander

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación para la obtención del título en ingeniería en Informática denominado, Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020, tuvo como finalidad determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN, Wireless Local Área Network), enfocándose en la infraestructura tecnológica de la misma, logrando así identificar los principales factores que afectan el rendimiento de la red y disminuyen la accesibilidad al contenido de la web a los estudiantes de la institución. La población total es de 3450 alumnos, de la cual se tomó una muestra de 252 involucrados. Para ello se planteó elegir una solución informática, llegando a determinar la implementación de un portal cautivo el mismo que ayudó a disminuir los fallos en la red.

El estudio se desarrolló con un enfoque de tipo mixto, los tipos de investigación utilizados fueron el descriptivo, de campo e investigación-acción, los cuales permitieron indagar sobre el problema y brindar una solución, ayudado del método analítico e inductivo. Para la recolección de información se utilizó dos técnicas, una entrevista dirigida a los Profesionales de TIC´s (Tecnologías de Información y Comunicación) de la Institución, permitiendo puntualizar información sobre la red WiFi (Wireless Fidelity), acompañada de una encuesta con el propósito de conocer el grado de satisfacción de los usuarios hacia el servicio que ofrecía la red de la Universidad. Como idea a defender, se mantuvo que la elevada latencia en la red de datos inalámbrica disminuye la accesibilidad al contenido web a los estudiantes de la UPEC. Finalmente, con la investigación se logró concluir que la utilización de un portal cautivo aporta a disminuir latencia, controlando el acceso de usuarios no autorizados, bloqueo de páginas y monitorear en el consumo de ancho de banda en la red de datos inalámbrica.

Palabras Claves: Latencia, Navegación, Portal Cautivo, Red De Datos, Contenido WEB.

ABSTRACT

The research work named "Captive Portal created for Universidad Politécnica Estatal del Carchi in the term 2019-2020" was developed not only to obtain the degree in Computer Science Engineering, but to determine latency generating agents in the wireless data network (WLAN, Wireless Local Area Network). Moreover, it focused on its technological infrastructure, thus identifying the main factors that affect network performance and reduce accessibility to web content. The total population is 3450 students, from which a sample of 252 took part on it. On the other hand, this research was developed with the purpose of mitigating the latency in the data network that generates problems to navigate when using portable devices. The issue mentioned before reduces the accessibility to the content on the web. Consequently, students do not perform well in different academic activities, such as researches, surf academic pages, delivery of assignments, online tests, among others. To do this, it was proposed to choose a computer solution, determining the implementation of a captive portal which would help reduce failures in the network. In addition, this study was used a mixed approach. There were applied the descriptive, field and action research, which allowed to investigate the problem and provide a solution. All of this was supported by the analytical and inductive method. For the collection of information, two techniques were used: an interview directed to the ICT staff (Information and Communication Technologies) that helped to specify information about the wireless network accompanied by a survey which focused on knowing the degree of user satisfaction regarding the service offered by the University's wireless data network (WLAN). As an idea to defend, it was maintained that the high latency in the wireless data network reduces the accessibility to the web content of portable devices of UPEC students. With the research, it was possible to conclude that the use of a captive portal helps to reduce latency, control the access of unauthorized users, block pages and monitor the consumption of bandwidth in the wireless data network that affected students' navigation and accessibility to content on the web.

Keywords: Latency, Navigation, Captive Portal, Data Network, WEB Content.

INTRODUCCIÓN

La Universidad Politécnica Estatal del Carchi posee una red inalámbrica libre, la misma que permite a los estudiantes tener acceso sin restricción alguna, pero impide la navegación debido a la elevada latencia y consumo desmesurado del ancho de banda, generando así inconformidad a los usuarios los cuales desean contar con el servicio para realizar actividades académicas. Por tal motivo se ha planteado utilizar herramientas tecnológicas basadas en software libre, tales como portales cautivos, estas aplicaciones se encargan de controlar y gestionar el acceso de usuarios, ancho de banda y monitorear el tráfico que se genera en la red inalámbrica. Para llevar a cabo el proyecto se instaló Pfsense, que fue elegido después de realizar una comparativa entre siete portales cautivos, logrando identificar que este se acopla a los requerimientos y necesidades que la institución posee. Se instaló módulos a nivel open source como NtopNg y SquidGuard que permiten bloquear contenido inapropiado, además de ayudar a gestionar la red WiFi de una mejor manera en tiempo real. Finalmente se configuró servidores DHCP, DNS, Proxy y Radius, el último se conectó al Active Directory de la institución donde reposan usuarios y contraseñas de los miembros de la comunidad universitaria, logrando de esa manera controlar el acceso de usuarios no autorizados a la red.

Para una mejor comprensión se la ha dividido en siete capítulos, cuyos contenidos contemplados son los siguientes:

Capítulo I: Problema. En este capítulo se define la problemática y tema de investigación juntamente con el objetivo general y específicos, además del planteamiento del problema, formulación del problema y las variables a estudiar.

Capítulo II: Fundamentación Teórico. En el presente capítulo se define las bases teóricas y científicas que sustentan la investigación, también se presenta los antecedentes que sirven de guía para la investigación actual.

Capítulo III: Metodología. En este capítulo se redacta las generalidades de la fase de la metodología, describiendo así el enfoque metodológico, los tipos de investigación, métodos de investigación, idea a defender, definición y operacionalización de variables, además de indicar instrumentos de recolección de datos, análisis estadísticos sobre la población y muestra.

Capítulo IV: Resultados y Discusiones. En este capítulo se redacta los resultados alcanzados con cada objetivo, así también la discusión que se extrajo de los antecedentes investigativos con respecto al presente trabajo de titulación.

Capítulo V: Conclusiones y Recomendaciones. En este capítulo se detalla e indica las conclusiones y recomendaciones a las que se ha llegado con la investigación, estableciendo una por cada objetivo propuesto.

Capítulo VI: Referencias Bibliográficas. En este capítulo se detallan las referencias bibliográficas utilizadas para la recopilación de información del presente trabajo de titulación.

Capítulo VII: Anexos. En este capítulo se evidencia la encuesta, entrevista, manual de configuración, además de figuras que avalan el trabajo realizado.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El internet se ha convertido en una herramienta fundamental en el diario vivir de las personas, cabe resaltar que el WiFi (Wireless Fidelity*)* es el principal método de conexión en la actualidad. Así, el rendimiento de latencia en una red de datos se ha convertido en un elemento indispensable en cuanto a la experiencia del usuario. En estudios realizados en el continente asiático, específicamente en la Universidad de Tsinghua – China, se generó un primer estudio sistemático sobre la latencia y sus factores, se recopiló información de 47 Access Points en el campus de la Universidad durante dos meses. Lo primero que se observó fue que la red WiFi se ha convertido en el principal método de acceso a Internet, el 55% del tráfico informático que se generaba sucedía en la red inalámbrica. En segundo lugar, los usuarios esperaban un tiempo de respuesta rápida, si el tiempo de carga del contenido web era superior a 3 segundos el 40% de los usuarios abandonaban las páginas. Un aproximado del 47% de los usuarios esperaba que su contenido web se cargue en un tiempo estimado de 2 segundos. En tercer lugar, la mayoría de las páginas de internet se basan en el protocolo HTTP que es sensible a la latencia de la red, el cual mostró que cada 10 milisegundos de aumento de latencia en el ancho de banda; provocaba un aumento de 1000 milisegundos en el tiempo de carga de la página web. En cuarto lugar, un factor influyente es la presencia de interferencia de red, cuando se da el caso puede provocar una latencia prolongada de paquetes en la red WiFi. Un cálculo basado entre los datos de los puntos 2 y 3 muestra que esta debe estar por debajo de un umbral estricto de 20∼30ms para satisfacer la expectativa del usuario (Pei et al., 2016). Por lo tanto, se puede corroborar que la latencia llega a ser un factor que repercute en las conexiones inalámbricas, las cuales pueden ser afectadas negativamente al aumentar el tiempo de respuesta entre la petición de cliente / servidor.

En el Ecuador la empresa nPerf efectuó un estudio en el 2018 con 229.517 usuarios que realizaron pruebas de conexión a los cuatro proveedores del servicio de Internet fijo más importantes en Ecuador, Punto Net, Netlife, Claro y CNT. El objetivo del Speed Test era medir la capacidad máxima de la conexión de datos en términos de velocidad.

Para conseguir dicho objetivo se establecieron conexiones simultáneas, el propósito fue saturar el ancho de banda, de ese modo las mediciones reflejarían la capacidad máxima de la conexión en las redes de datos y la velocidad con la que se logra dicha conexión.

Es así como se consideró que la velocidad y la latencia pueden ser afectadas por la calidad de la red que el usuario posee en su domicilio o lugar de trabajo (nPerf, 2018). Algo semejante ocurre con el estudio centrado en la Universidad de Guayaquil que abarcó la temática de un prototipo para videoconferencia, el mismo que permitió la difusión del contenido de manera eficaz, logrando que la comunicación generada entre los interesados sea nítida, sin interrupciones y en tiempo real. Pazmiño y Uquillas (2019) al realizar la investigación identificaron que la latencia es un factor el cual está presente en todas las redes inalámbricas, comprobando que la difusión de video consume más ancho de banda, efectuaron pruebas mediante consumo de tráfico con el servidor BigBlueButton BBB o sistema de conferencia web y pudieron detectar que entre menos usuarios realicen conexiones simultáneas disminuye el grado de latencia. Así, realizaron las pruebas entre el servidor de videoconferencia y el Moodle con un número de 2, 4 y 6 usuarios, transmitieron primero video, después audio, chat, edición de presentaciones y los demás servicios que provee el BBB. Al difundir el video se aprecia que se alcanzó un valor de 37,38µs para 2 clientes, 39,97µs para 4 clientes y 43,90µs para 6 clientes. Con las pruebas de audio se generó un valor de 3,23µs para 2 clientes, 5,66µs para 4 clientes y 7,70µs para 6 clientes. Al realizar pruebas de chat y edición de presentaciones se alcanzó 0,044µs para 2 clientes, 0,055µs para 4 clientes y 0,068µs para 6 clientes. Con los datos obtenidos se concluyó que el servicio de video generó mayor latencia en la red que los demás servicios.

Abordando el ámbito local, el tema de investigación se desarrolla en la Universidad Politécnica Estatal del Carchi de la ciudad de Tulcán, esta es una institución pública y acreditada. En la actualidad la Universidad brinda el servicio de internet por medio de la red inalámbrica identificada con el SSID: WUPEC.EVENTOS que es utilizada en diferentes actividades académicas, dicha red no posee ningún tipo de autenticación ni control de acceso, al no contar con una herramienta que regule el uso del servicio los usuarios realizan actividades ajenas a lo académico como: descargas de archivos, visita a páginas de entretenimiento, juegos en línea, videos online, etc. Esto ocasiona así un mayor consumo de recursos en cuanto al ancho de banda, provocando un aumento de tráfico en la red de datos inalámbrica que influye negativamente en las actividades académicas para la cual fue destinada, llegando a producir perdidas momentáneas del servicio por el aumento de latencia, causando una mala experiencia al usuario.

El internet en la educación es una poderosa herramienta la cual ayuda a la difusión del conocimiento, de hecho, es una de las mayores fuentes de información disponibles, reduciendo

considerablemente el tiempo y esfuerzo empleado en la búsqueda del saber y la información, de ahí la importancia de contar con una red inalámbrica totalmente funcional y accesible para los estudiantes.

1.2. FORMULACIÓN DEL PROBLEMA

La elevada latencia en la red de datos inalámbrica genera indisponibilidad en la navegación de dispositivos portátiles, disminuyendo la accesibilidad a los sitios web a los estudiantes de la UPEC, año 2021

1.3. JUSTIFICACIÓN

El presente trabajo de investigación alude a la accesibilidad al contenido web para fines académicos de la comunidad estudiantil de la UPEC, en virtud de que, en el acuerdo ministerial 70-14 expedido en el año 2014, habla del uso de tecnología dentro de la educación, ayudando a potencializar la misma y aún más dentro de la educación de tercer nivel. Asimismo, se ha mirado la necesidad de los estudiantes al no poder navegar en internet dentro de la Universidad.

Dentro de la UPEC, los estudiantes realizan distintas actividades de carácter académico tales como: consulta de notas, visita a páginas académicas, entrega de tareas, pruebas online, entre otras; lo que conlleva el uso de conexión inalámbrica, utilizando dispositivos móviles como laptops, celulares y tablets. Por consiguiente, el acceso al contenido web es necesario dentro de la institución.

Mediante la disminución de latencia en la red de datos inalámbrica se pretende mejorar la navegación a internet, perfeccionando la accesibilidad a plataformas virtuales e información digital a los estudiantes, brindando un servicio de calidad y mejorando la experiencia de usuario en la Universidad. Por consiguiente, la presente investigación tiene como propósito determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN), basándose en la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la accesibilidad al contenido en la web de los estudiantes de la Universidad Politécnica Estatal del Carchi, de esta manera se pretende mejorar la navegación a internet haciendo uso de herramientas tecnológicas basadas en software libre.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN), basándose en la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la accesibilidad al contenido en la web a los estudiantes de la Universidad Politécnica Estatal del Carchi.

1.4.2. Objetivos Específicos

- Fundamentar teóricamente las variables de estudio mediante la recopilación bibliográfica, identificando los factores determinantes de riesgo que afectan la disponibilidad de la red.
- Analizar la red de datos inalámbrica (WLAN), examinando la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la navegación a los estudiantes de la UPEC.
- Elegir una solución informática mediante la comparativa de portales cautivos, ayudando a la disminución de latencia, mejorando la accesibilidad al contenido web en la institución.
- Implementar un portal cautivo mediante la utilización de herramientas tecnológicas de software libre, mitigando la latencia en la red de datos y mejorando su navegación.

1.4.3. Preguntas de Investigación

¿La fundamentación teórica ayuda a determinar los factores principales de riesgo que afectan a la red inalámbrica de datos?

¿El análisis de la latencia en la red de datos inalámbrica aporta a identificar puntos críticos que provocan errores de conexión y perjudica la accesibilidad al contenido web?

¿Hasta qué punto las herramientas informáticas a utilizar ayudarán en el monitoreo de la red?

¿Cuáles son las ventajas y desventajas de implementar un portal cautivo para mejorar la red de datos de la Universidad?

¿Cuáles son los instrumentos que aportan al desarrollo del portal cautivo?

¿Cuáles son los parámetros necesarios para implementar un portal cautivo?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

En el presente proceso de investigación se toman en cuenta los siguientes antecedentes:

En el trabajo de investigación realizado por Chalen Asunción Gilson y Plúas Gorotiza Manuel Isidro en el 2017 denominado *PROPUESTA TECNOLÒGICA DE UN PORTAL CAUTIVO, BAJO PILA IPV6 Y TRANSMISIÒN DE DATOS MEDIANTE Li-Fi* el cual se basa en la problemática que muchos han atravesado, en ocasiones no se puede acceder a la web, ya sea por no contar con datos de internet o simplemente por no conectarse de manera exitosa a la red inalámbrica, y si la conexión logra ser exitosa esta impide navegar en internet y acceder al contenido web por la lentitud de la red. El objetivo trazado para la mitigación del problema y cumplimiento de sus actividades fue proponer un centro de información digital con acceso a internet mediante un portal cautivo a través de una red inalámbrica WLAN, usando la tecnología Li-fi, situada en la Facultad de Ciencias Administrativas en la carrera de I.S.A.C de la Universidad de Guayaquil, difundiendo además información general de los eventos que se realizaron en la institución educativa superior. Dentro del capítulo metodológico, los tipos de investigación utilizados fueron dos: de campo porque se necesita recolectar datos que sean de ayuda en la propuesta tecnológica realizada directamente a los administradores de la red en I.S.A.C y los usuarios y la investigación aplicada la cual permitiría brindar una solución a los usuarios mediante la problemática planteada.

Las conclusiones a las que llegaron los autores con su trabajo de titulación resumen lo siguiente: las entrevistas que se le realizaron al encargado de administrar la red ayudó a determinar que se podía realizar el diseño e implementación de una herramienta tecnológica como lo es el portal cautivo, se realizó estudios tanto en el hardware como en software para levantar los requerimientos necesarios para el diseño del portal cautivo y finalmente el software seleccionado permitía ingresar al usuario únicamente a contenido educativo, según los autores de este trabajo las redes sociales no aportan de manera significativa al estudio.

En segundo lugar, en el trabajo de titulación realizado por Linda Inés Andrade Cayambe en el año 2019, denominado *Diseño y simulación de portal cautivo, que permita: autenticación, aplicación de herramientas, políticas de seguridad, QoS y sonda de red para el filtrado de contenido mediante equipo UTM en la CISC-CINT*, el cual contempla problemas de conexión, control de acceso y lo referente a la seguridad contra ataques informáticos. Este a su vez busca

prevenir inconvenientes de lentitud de la red o pérdida de conexión que afecta la accesibilidad al contenido educativo. Los estudiantes constantemente realizan actividades como proyectos, tareas, prácticas en equipos inalámbricos. El objetivo propuesto en este trabajo fue el diseñar una red inalámbrica administrable para supervisar y gestionar el acceso de los recursos de la CISC-CINT mediante el uso de una herramienta tecnológica open source, garantizando una conexión estable y segura a los usuarios que ingresan a la red. El tipo de investigación utilizado en este trabajo de titulación es la descriptiva porque esta se centra en conocer aspectos de trascendencia a partir del problema y ayudado de los usuarios que son los principales involucrados.

La conclusión a la que se llegó al utilizar una herramienta tecnológica de código abierto es que se solventa de manera eficaz las necesidades de la institución para administrar la red Wireless, mejora la funcionalidad y rendimiento de la red con medidas de seguridad y métodos de autenticación.

Por último, en el trabajo de titulación realizado por Juan Alejo Peirano en el año 2015, denominado *Ampliación y optimización de mediciones de latencia para la región de América Latina y el Caribe*, la cual buscaba que a través de la medición de latencias y estudio de la interconexión se genere información que permita a las empresas y organizaciones de la región de LACNIC realizar negocios, los mismos que ayuden al desarrollo y la interconexión a nivel local y regional. La medición de latencia en la región se la realizaba basándose en algoritmos que consultan de manera pseudoaleatoria en servidores de base en Internet, utilizando como origen aplicaciones (en general WEB) en el propio equipo de quién realiza la medición. En particular, consultas a servidores de mediciones de velocidad de conexión (siendo uno de los más utilizados el Speedtest de Ookla). El objetivo planteado para el cumplimiento de dicho trabajo de titulación fue el realizar y almacenar mediciones de latencia en la región de Latinoamérica y el Caribe. Para cumplir con este objetivo, utilizaron la herramienta “Simon” que posee diferentes tipos de medidores especialmente diseñados para medir latencias.

Como conclusión se tiene que la contribución realizada ha otorgado un beneficio al proyecto, en la ampliación y optimización de mediciones de latencia y a su vez se han fomentado actividades para continuar desarrollando en el futuro.

2.2. MARCO TEÓRICO

Existen varias definiciones sobre herramientas tecnológicas, latencia en la red de datos y accesos al contenido web, razón por la cual, se procede a definirlas como parte de las variables que componen la investigación sobre herramientas tecnológicas para el mejoramiento de la navegación inalámbrica.

2.2.1. Fundamentación Legal

Para el desarrollo de la presente investigación de finalización de carrera se ha tomado como sustento legal a los artículos establecidos en la constitución de la república del Ecuador del año 2008, los mismos que respaldan el derecho a innovar en el campo educativo mediante la ciencia y tecnología.

Art. 80.- El Estado fomentará la ciencia y la tecnología, especialmente en todos los niveles educativos, dirigidas a mejorar la productividad, la competitividad, el manejo sustentable de los recursos naturales, y a satisfacer las necesidades básicas de la población. Garantizará la libertad de las actividades científicas y tecnológicas y la protección legal de sus resultados, así como el conocimiento ancestral colectivo. La investigación científica y tecnológica se llevará a cabo en las universidades, escuelas politécnicas, institutos superiores técnicos y tecnológicos y centros de investigación científica, en coordinación con los sectores productivos cuando sea pertinente, y con el organismo público que establezca la ley, la que regulará también el estatuto del investigador científico.

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación (...).

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.
2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica (...).

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

- **Resolución N.- 1014 Utilización de Software Libre**

En el estado ecuatoriano en la constitución de la república del 2018 da a conocer una serie de leyes y reglamentos en los cuales podemos sustentar la presente investigación tal es el caso de la resolución 1014 que dice así, El Estado fomentará la ciencia y la tecnología, especialmente en todos los niveles educativos, dirigidas a mejorar la productividad, la competitividad, el manejo sustentable de los recursos naturales, y a satisfacer las necesidades básicas de la población. Garantizará la libertad de las actividades científicas y tecnológicas y la protección legal de sus resultados, así como el conocimiento ancestral colectivo. La investigación científica y tecnológica se llevará a cabo en las universidades, escuelas politécnicas, institutos superiores técnicos y tecnológicos y centros de investigación científica, en coordinación con los sectores productivos cuando sea pertinente, y con el organismo público que establezca la ley, la que regulará también el estatuto del investigador científico. (Resolución N.- 1014, 2008).

Decreta:

Artículo 1.- Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

Artículo 2.- Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a. Utilización del programa con cualquier propósito de uso común.
b. Distribución de copias sin restricción alguna.
c. Estudio y modificación del programa (Requisito: código fuente disponible).
d. Publicación del programa mejorado (Requisito: código fuente disponible).

Artículo 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

Artículo 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este decreto se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa de patrimonio nacional.

Mediante los artículos previamente mencionados el estado ecuatoriano ampara el desarrollo de investigaciones en instituciones del Estado, universidades, escuelas politécnicas, institutos de investigación públicos y particulares, con la finalidad de fomentar el crecimiento tecnológico del país.

2.2.2. Tecnologías inalámbricas

En los últimos tiempos se ha visto un desarrollo acelerado en las tecnologías inalámbricas, las cuales han avanzado de manera sustancial en el desarrollo digital, el auge de las tecnologías inalámbricas poco a poco va tomando mayor fuerza en el siglo XXI. Así, las conexiones inalámbricas hacen posible la comunicación de múltiples dispositivos inteligentes, facilitando de esta manera que los equipos se conecten de una manera remota y sin presentar inconvenientes, en la instalación de las redes WLAN, no es necesario cometer cambios significativos en cuanto a infraestructura. Esta evolución aportada a la creación de múltiples nuevos tipos de redes, escenarios y ámbitos destinados a la tecnología Wireless (Cano, 2016). Paralelamente, estos avances se vieron impulsados por una notable evolución de las tecnologías de hardware, las mismas que permitieron que dispositivos se doten de diferentes formas de conexiones inalámbricas, esta conexión inalámbrica permite tener mayor versatilidad.

2.2.2.1. Definición de red informática

Se define a una red informática al conjunto de dispositivos que están conectados entre sí a través de un medio de comunicación, sea este físico, inalámbrico u otros; esta red informática depende de la infraestructura dinámica para la interacción de la red. Casillas y Gallardo (2016) aseguran que:

> Una red es un conjunto de dispositivos interconectados entre sí a través de un medio, intercambian información y comparten recursos. Básicamente es un proceso que tiene dos funciones específicas para los dispositivos conectados, emisor y receptor que se van

> asumiendo y alternando en distintos instantes de tiempo. La estructura y el modo de funcionamiento de las redes informáticas están definidos en varios estándares el más extendido es el modelo TCP/IP, basado en el modelo de referencia o teórico OSI. TCP/IP es un conjunto de instrucciones o reglas conocidas con el nombre de protocolo, lo que permite que ordenadores remotos con procesadores y sistemas operativos diferentes se entiendan y en definitiva que Internet funcione como lo hace en la actualidad. Internet utiliza varios protocolos, pero los que están en la base de todos los demás son el Transport Control Protocol (TCP) y el llamado Internet Protocol (IP), o en definitiva TCP/IP para abreviar. Se trata de una serie de reglas para mover de un ordenador a otro los datos electrónicos descompuestos en paquetes, asegurándose de que todos los paquetes llegan y son ensamblados correctamente en su destino. Todos los ordenadores en Internet utilizan el protocolo TCP/IP y gracias a ello se consigue eliminar la barrera de la heterogeneidad de los ordenadores y resolver los problemas de direccionamiento. (p.10)

Las redes informáticas para realizar una correcta comunicación utilizan medios y dispositivos, los mismos que hacen posible la transferencia de información entre las entidades involucradas.

2.2.2.2. Tipos de redes (LAN, WAN y MAN)

La red de datos atiende a un gran número de factores como: tamaño, distancia que abarca y su arquitectura física, los cuales facilitan su clasificación. Así, como principal solución que se les ocurrió al Institute of Electrical and Electronics Engineers (IEEE) fue la creación de estándares en su afán de generalizar la comunicación. el primer estándar fue LAN el cual proporcionaba un conjunto de pautas para la creación de hardware y software, estas pautas permiten la interacción de equipos provenientes de diferentes empresas con el pasar del tiempo las LAN no eran suficientes debido al crecimiento de las empresas, lo que necesitaba ahora era una forma en la cual la información se pudiera transferir rápidamente y de manera eficiente dentro de una misma empresa pero en diferentes lugares del país la solución más óptima fue la creación de Redes de Área Metropolitana (MAN) y Redes de Área Extensa (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, facilitando a las empresas la comunicación entre ellas a pesar de estar separadas por grandes distancias (Mendoza & Andrade, 2016). Es por ello por lo que cada establecimiento o institución adecua su red de datos de acuerdo con los factores con los que cuenta.

2.2.2.3. Redes inalámbricas

Se las define a las redes inalámbricas como la interconexión de dispositivos, los mismos que tienen la capacidad de compartir información entre ellos, pero con la diferencia de que no utilizan ningún medio físico de transmisión. Adriano y Estrada (2015) indican que estas redes permiten a la conexión ser mucho más versátil permitiendo mayor movilidad, no pretenden sustituir a las redes cableadas más bien intentan estar a la par en cuanto a funcionalidad. Con el desarrollo de nuevas tecnologías construir una infraestructura inalámbrica puede ser una buena inversión, al asumir precio y costos sumamente bajos a comparación de sus similares las redes tradicionales de cable, a todo esto, levantar redes inalámbricas genera un ahorro no solo de dinero también ayuda a mejorar la experiencia del usuario final. La comunidad que utiliza estas tecnologías posee un acceso a la información más sencilla y rápida sin olvidar que lo puedo hacer teniendo movilidad en distancias cortas teóricamente hasta 100 m.

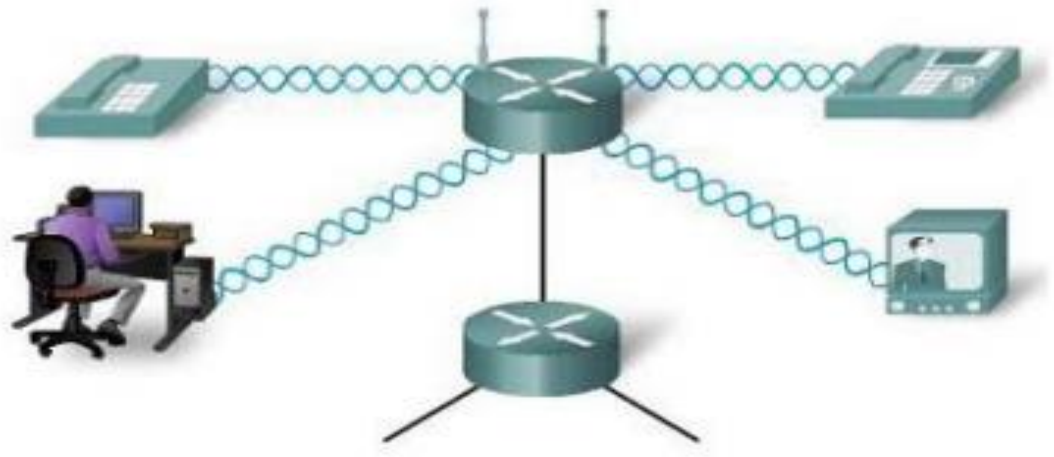


***Figura* 1.** Interconexión inalámbrica entre dispositivos
Fuente: Estrada. (2015*)*

2.2.2.4. Aplicaciones de las redes inalámbricas

En la actualidad las redes inalámbricas tienen un propósito muy fundamental el cual es proporcionar acceso a internet, multimedia vía web. Dentro de las tecnologías que existen hoy en día sobre redes inalámbricas. Obando, (2018) menciona las siguientes:

a) Bluetooth: Se define como una tecnología de transmisión inalámbrica que emplea ondas de radio de corto alcance (hasta 100m²), que tienen la capacidad de traspasar determinados materiales como es el caso de muros de hormigón. Obando (2018) afirma: “Esta tecnología requiere del uso de antenas, las cuales pueden ser externas o internas al dispositivo. La

transmisión mediante Bluetooth ha sido estandarizada de manera 12 independiente y cuenta con una velocidad de transmisión de hasta 1 Mbps" (p.28). En los últimos años se ha hecho popular el uso de dispositivos de bajo consumo sobre BLE (Bluetooth Low Energy) permitiendo la creación de Tags inteligentes con baterías internas de larga duración.

b) Microondas: Es una tecnología inalámbrica que tiene su aplicabilidad en comunicaciones a gran escala, las cuales se caracterizan por ser muy costosas y de poco uso doméstico. "Como parte de esta tecnología se pueden mencionar la de tipo satelital y la terrestre, siendo necesario el uso de antenas para ambos casos, ya sea para la emisión como la recepción de la transmisión".

c) Wi-Fi: También conocida como WLAN (Wireless Local Área Network) o redes de área local inalámbricas. Como su nombre lo indica, se trata de una tecnología de transmisión inalámbrica, la cual se realiza mediante el uso de ondas de radio para distancias cortas que pueden alcanzar una distancia teórica de hasta 100 m. Como se había mencionado anteriormente, esta tecnología está estandarizada por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE), organización internacional que define las reglas de operación de ciertas tecnologías. Para la operatividad de esta tecnología es necesario el uso de antenas integradas en las tarjetas, donde los obstáculos no resultan ser una limitante de transmisión entre el emisor y el receptor. (p.29)

Hay que considerar que estas conexiones dependen en gran mayoría para su correcta emisión de la intensidad de señal de radio que se envié, de igual manera se debe asumir factores como el ruido de fondo, tasa de datos y el número de clientes que se conecten a la red.

2.2.2.5. Definición de red WLAN

Las denominadas Redes Inalámbricas De Área Local o también conocidas por su sigla en inglés como WLAN forman parte de un sistema de comunicación inalámbrico el cual se asemeja a las redes LAN, diferenciadas por el medio con el que transmiten la información. Las redes WLAN están diseñadas para brindar acceso inalámbrico en una cobertura de 1 hasta 100 metros. López (2017) afirma:

Una red inalámbrica de área local o WLAN (Wireless Local Área Network), es un sistema de comunicación inalámbrica flexible que tiene similar cobertura que una red LAN. Se utiliza como alternativa a las redes cableadas o como una extensión de estas. Usa tecnologías

de radiofrecuencia que permite mayor movilidad a los usuarios sobre todo por la tendencia al uso de equipos Smart como celulares y tables. Estas redes van adquiriendo importancia en muchos campos pues permiten transmitir información desde diversos dispositivos a una terminal central. Actualmente su uso está muy extendido en la industria, la educación y el gobierno. (p.11)

Una red WLAN es utilizada frecuentemente como una alternativa de las LAN, permitiendo la conectividad a internet sin necesidad de la utilización de cables logrando de esta manera darle al usuario una mayor movilidad en una determinada área de trabajo.

2.2.2.6. Definición de WiFi (Wireless Fidelity)

La red WI-FI tiene como denominación Wireless Local Área Network o su vez redes de área local inalámbrica, esta tecnología tiene como finalidad la transmisión de datos mediante ondas de radio a distancias cortas y con buena calidad de emisión. Vélez (2016) afirma:

> Una red Wi-Fi está diseñada bajo una estructura de red, permiten una conexión inalámbrica entre varios dispositivos, funcionan en base a ciertos protocolos previamente establecidos como la IEEE 802.11, creado para acceder a redes locales inalámbricas y a conexiones a varios dispositivos. Las redes inalámbricas Wi-Fi por sí mismas son móviles, eliminan la necesidad del uso de cableado, permitiendo su fácil accesibilidad, pero sobre todo a incrementado la productividad y eficiencia en empresas, lugares públicos, privados, hogares, áreas metropolitanas y sobre todo en el ámbito educativo como escuelas, colegios y universidades. (p.12-13)

Ahora bien, además de tener protocolos que permiten la conexión también los dispositivos deben contar con un hardware que permite dicha conexión en este caso son las antenas integradas las mismas que vienen ensambladas desde la fabricación de los dispositivos.

2.2.2.7. Ventajas de un Red WLAN

Las redes WLAN poseen ciertos beneficios en relación con las redes cableadas motivo por el cual a continuación se mencionará algunas de ellas. Salazar, (2016) menciona:

> Aumento de la eficiencia: La comunicación a través de una WLAN se produce de manera más ágil beneficiando a los usuarios de la red. Por ejemplo, un vendedor en una tienda de vestir puede brindar información exacta y precisa a su cliente sobre precios y descuentos de

> alguna prenda de vestir sin necesidad de andar preguntando a los propietarios generando así mayor eficiencia en sus ventas. Mejor cobertura y movilidad: Conectarse av. una red WLAN otorga la libertad de moverse y cambiar de ubicación sin perder la conexión. Recordando que dicha conexión no tiene la necesidad de ningún cable que lo ligue a un lugar en específico. Flexibilidad: Los usuarios de redes inalámbricas pueden tener una conexión sin necesidad de estar ligados a estaciones de trabajo, logrando así seguir siendo productivos. Ahorro de costes: Las redes inalámbricas en la actualidad con el desarrollo de la tecnología lograron evolucionar rápidamente. Permitiendo así, ser más baratas y fáciles de instalar, especialmente en lugares como casas o edificios en donde los propietarios del lugar no permiten dicha instalación ya que dañarían la estructura del inmueble. Considerando además la ausencia de cables hace bajar el costo en su instalación. Adaptabilidad: Se logra con una mayor rapidez y facilidad al conectar dispositivos en la red, y una mayor flexibilidad al intentar realizar modificaciones en la ubicación de los dispositivos que generan la conectividad. (p.36)

Las ventajas en cuando a las redes WLAN son muy amplias mostrando eficiencia, movilidad, además de ser más baratas en su implementación en relación de las LAN, cableadas.

2.2.2.8. Desventajas de una red WLAN

La utilización de las redes WLAN en el ámbito empresarial y educativo son ventajosas al aportar movilidad y una conexión eficiente para los usuarios, pero como en todo, se tiene el otro lado de la moneda posee algunas desventajas las mismas que se indicaran a continuación. Al respecto Salazar, (2016) explica:

> Seguridad: Las redes WLAN al trasmitir la información lo realizan mediante ondas de radio las mismas que se encuentran en el aire, por lo que resultan ser más susceptibles y vulnerables al ataque y robo de información por parte de usuarios mal intencionados. Problemas de instalación: Con las redes WLAN al realizar la instalación se debe considerar ciertos parámetros y especificación debido al medio por el que se trasmite la información, puesto que al encontrarse con edificios en el medio afectaría y disminuiría la señal de dichas redes. De igual hay que considerar el clima dado que si se presentan descargas electromagnéticas afectan en su rendimiento llegando hasta el punto de que se puede perder la comunicación inalámbrica por completo. Cobertura: La señal de estas redes es de 1 a 100 metros aproximadamente, pero debido a construcciones con base en materiales de acero

> puede que resulte dificultoso la recepción de la señal llegando a crear problemas de cobertura lo que conlleva a la existencia de los llamados puntos negros en donde no hay cobertura. Se debe considerar para la creación en cuanto a la infraestructura de estas redes, Utilizar estándares internacionales para de esa manera no verse tan afectado con la aparición de los puntos negros. Velocidad de transmisión: Respecto a la trasmisión inalámbrica de las redes WLAN se consideró la definición del autor Jordi Salazar en la que indica lo siguiente. "La transmisión inalámbrica puede ser más lenta y menos eficiente que las redes cableadas. (p.36)

Las redes WLAN son actualmente utilizadas en la mayoría de las instituciones, al presentar mayor versatilidad, pero como se pudo apreciar hay parámetros en los que se debe poner énfasis como por ejemplo la seguridad y la distribución de los equipos Access Point.

2.2.2.9. Ondas electromagnéticas

Las ondas electromagnéticas poseen elementos eléctricos y magnéticos, siendo también además capaces de no necesitar un medio material para propagarse. Sánchez, et al (2018) afirma:

> Son aquellas ondas que no necesitan un medio material para propagarse, entre otras esta la luz visible, ondas de radio, ondas de televisión, telefonía móvil, se propagan por el aire a una velocidad rápida per no infinita, motivo por el cual podemos observar la luz que irradia estrellas a bastantes años luz de distancia de la tierra y enterarnos por telefonía móvil de sucesos que ocurren a grandes distancias casi de manera inmediata. Las ondas electromagnéticas se propagan mediante la excitación de campos eléctricos y magnéticos (campos electromagnéticos) estos campos son la base de medios de telecomunicación no guiados, que es la base de la tecnología WiFi o telefonía móvil, sin embargo, cada tecnología está dividida en el espectro electromagnético dependiendo de la frecuencia de funcionamiento. (p.43)

Así mismo las ondas electromagnéticas son consideradas actualmente como puntal fundamental de las telecomunicaciones y el desempeño de la actualidad.

2.2.3. Estándares de comunicación

2.2.3.1. Estándar IEEE 802.11

El mundo de las redes inalámbricas es muy extenso, y al contar con varias características se ha buscado estandarizar, es así que miembros del Instituto de Ingenieros Eléctricos y Electrónicos crearon una norma llamada IEEE 802.11. Así, el protocolo IEEE 802.11 es un estándar internacional que tiene como finalidad normalizar características que posee una red inalámbrica. Con la ayuda de este estándar se puede instaurar los niveles bajos que el modelo OSI posee para conexiones inalámbricas, las mismas que son realizadas por medio de ondas electromagnéticas (Villagómez, 2018). En la actualidad el estándar IEEE 802.11 ha generado estándares denominados físicos que ayudan en la optimización del ancho de banda o para detallar componentes de forma óptima.

Tabla 1. Estándar IIEE 802.11

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54Mbps.
802.11b	Estándar WLAN para la banda de 2.4GHz, soporta 11Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2,4GHz. Dirigido a proporcionar velocidades de hasta 54Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir las vulnerabilidades actuales en la seguridad para protocolos de autenticación y de codificación.
802.11n	Estándar WLAN dirigido a proporcionar un rendimiento mucho más alto, ofrece compatibilidad para los dispositivos en una red con versiones anteriores de WiFi. Trabaja con velocidades altas.

Fuente: Villagómez, 2018

2.2.3.2. Estándar IEEE 802.11a

El estándar IEEE 802.11 con el pasar de los años ha venido evolucionando con diferentes versiones, la primera de ellas es IEEE.802. 11a. (Salazar, 2016) menciona:

> El estándar IEEE 802.11a puede operar a una velocidad de hasta 54 Mbps y utiliza la banda de frecuencia de 5 GHz. En lugar de DSSS, este estándar utiliza OFDM, lo que permite que los datos sean transmitidos por subportadoras en paralelo, proporcionando una mayor resistencia a las interferencias y una mayor velocidad de transmisión. Esta tecnología, con mayor velocidad, permite a la red inalámbrica un mejor comportamiento en aplicaciones de vídeo y conferencia. Al no utilizar las mismas frecuencias que otros dispositivos (como teléfonos inalámbricos que funcionan en la banda de frecuencia de 2,4 GHz), OFDM y IEEE 802.11a proporcionan una mayor velocidad de transferencia y una señal más limpia, con muchas menos interferencias. La velocidad de bits de 54 Mbps es alcanzable bajo condiciones ideales. Si no se cumplen las condiciones ideales, se utilizan las velocidades más lentas de 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps y 6 Mbps. (p.26)

Este estándar no es compatible con versiones posteriores a esta, como lo son las 802.11b, 802.11g y 802.11n.

2.2.3.3. Estándar IEEE 802.11b

Este es el segundo avance que pertenece al estándar principal IEEE 802.11, este ofrece que los dispositivos en donde se implementa este estándar brinden mayor alcance y el poder traspasar estructuras edilicias. Salazar, (2016) explica:

> La principal mejora de IEEE 802.11 por IEEE 802.11b es la estandarización de la capa física para soportar velocidades de transmisión más altas. El estándar IEEE 802.11b admite dos velocidades adicionales, 5.5 Mbps y 11 Mbps, utilizando la banda de frecuencia de 2,4 GHz. Se utiliza el esquema de transmisión DSSS con el fin de proporcionar velocidades de transmisión más altas. La velocidad de 11 Mbps es alcanzable bajo condiciones ideales. Si no se cumplen las condiciones ideales, se utilizan las velocidades más lentas de 5,5 Mbps, 2 Mbps y 1 Mbps. Es importante señalar que 802.11b utiliza la misma banda de frecuencia que utilizan los hornos de microondas, teléfonos inalámbricos, monitores de bebés, cámaras de vídeo inalámbricas y los dispositivos Bluetooth. (p.27)

Este estándar no es compatible con la visión anterior IEEE 802.11a, pero aun en algunas instituciones optan por la utilización de este estándar.

2.2.3.4. Estándar IEEE 802.11g

El estándar IEEE 802.11g es una extensión de la versión anterior IEEE 802.11b que entre sus primiciales avances ofrece una velocidad de trasmisión de datos. Salazar (2016) menciona:

> El estándar IEEE 802.11g puede operar a una velocidad de hasta 54 Mbps, pero utiliza la banda de frecuencia de 2,4 GHz y OFDM. 802.11g también es compatible con 802.11b, y puede operar a las velocidades de bits 802.11by utilizar DSSS. Adaptadores de red inalámbrica 802.11g pueden conectarse a un punto de acceso inalámbrico 802.11b, y adaptadores de red inalámbrica 802.11b pueden conectarse a un punto de acceso inalámbrico 802.11g. Por lo tanto, 802.11g proporciona una ruta de migración para redes 802.11b a una tecnología estándar compatible en frecuencia, pero con una velocidad de transmisión más alta. Los adaptadores existentes de red inalámbrica 802.11b no se pueden actualizar a 802.11g mediante una actualización del firmware del adaptador, deben ser reemplazados. A diferencia de la migración de 802.11b a 802.11a (en la que todos los adaptadores de red, tanto en los clientes inalámbricos como en los puntos de acceso inalámbricos deben ser reemplazados al mismo tiempo), la migración de 802.11b a 802.11g se puede hacer de forma incremental. Al igual que 802.11a, 802.11g utiliza 54 Mbps en condiciones ideales y las velocidades más lentas de 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps y 6 Mbps en condiciones menos ideales. (p.27)

Este estándar tiene una particularidad, brinda una compatibilidad con su versión antecesora IEEE 802.11b.

2.2.3.5. Estándar IEEE 802.11n

El estándar IEEE 802.11n es un estándar evolucionado del original IEEE 802.11 que ofrece velocidades de transmisión superiores a las antes mencionadas. Así lo corrobora Salazar, (2016):

> El estándar IEEE 802.11n tiene como objetivo mejorar la distancia (hasta 250 m) y la velocidad de transmisión de las dos normas anteriores, 802.11a y 802.11g, con un aumento significativo de la velocidad máxima de datos en bruto de 54 Mbps a 600 Mbps en condiciones ideales añadiendo la tecnología de múltiple entrada múltiple salida y canales de

> 40 MHz, de mayor ancho de banda. Esta tecnología, denominada MIMO (Múltiple Input Múltiple Output), utiliza múltiples señales inalámbricas y antenas en el transmisor y el receptor. El estándar puede funcionar en las bandas de frecuencia de 2,4 GHz o 5 GHz. (p.27)

Este estándar tiene una particularidad y es que es compatible con todos los estándares IEEE 802.11 anteriores a esta.

2.2.4. Protocolo de enlace de datos

2.2.4.1. PPP (Protocolo punto a punto)

El Protocolo punto a punto es un método el cual permite transportar datagramas multiprotocolo mediante enlaces punto a punto, proporcionando encapsulamiento sobre enlaces sincrónicos y asincrónicos con 8 bits de datos. Ariganello (2019) afirma:

> PPP se diseñó como un protocolo abierto para trabajar con varios protocolos de capa de red, como IP, IPX y AppleTalk.
>
> Se puede considerar a PPP la versión no propietaria de HDLC, aunque el protocolo subyacente es considerablemente diferente. PPP funciona tanto con encapsulación sí-ncrona como así-ncrona porque el protocolo usa un identificador para denotar el inicio o el final de una trama. Dicho indicador se utiliza en las encapsulaciones así-ncronas para señalar el inicio o el final de una trama y se usa como una encapsulación sí-ncrona orientada a bit. Dentro de la trama PPP el Bit de entramado es el encargado de señalar el comienzo y el fin de la trama PPP (identificado como 01111110). El campo de direccionamiento de la trama PPP es un Broadcast debido a que PPP no identifica estaciones individuales.
>
> PPP se basa en el protocolo de control de enlaces LCP (Link Control Protocol), que establece, configura y pone a prueba las conexiones de enlace de datos que utiliza PPP. El protocolo de control de red NCP (Network Control Protocol) es un conjunto de protocolos (uno por cada capa de red compatible con PPP) que establece y configura diferentes capas de red para que funcionen a través de PPP. Para IP, IPX y AppleTalk, las designaciones NCP son IPCP, IPXCP y ATALKCP, respectivamente. (p.1)

El protocolo PPP puede funcionar con cualquier interfaz DTE/DCE además de operar con enlaces FULL-Dúplex dedicados permitiendo transmitir y recibir datos entre ambos dispositivos al mismo tiempo.

2.2.4.2. PAP

El PAP es un protocolo de autenticación simple, este solo se utiliza al iniciar el enlace de comunicación. Castro y Eras (2017) aseguran:

> PAP un protocolo de autenticación para autenticar un usuario hacia un servidor de acceso remoto. PAP es un sub-protocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), aprobando a un usuario que permite acceder a ciertos recursos. PAP transfiere passwords en ASCII sin ningún cifrado, por lo que es considerado inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte. (p.38)

Una vez que se ha completado la fase de conexión inicial pasa a establecer el enlace PPP, mediante el nodo envía varias peticiones seguidas al router para autentificar el usuario y contraseña logrando así la autentificación. Como se mencionó anteriormente no las contraseñas que se envían no son seguras porque estas están en modo abierto y sin ninguna protección lo que hace posible el robo de información.

2.2.4.3. CHAP

El protocolo CHAP se lo conoce como un método de autenticación más seguro que su predecesor PAP. Castro Eras (2017) explica:

> CHAP es un procedimiento de autenticación usado por servidores accesibles vía PPP. CHAP comprueba periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto acontece cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa por medio de la contraseña. (2017, p.38)

Este protocolo es empleado durante el inicio del enlace y posteriormente se encargará de verificar periódicamente la entidad de los dispositivos que se van a utilizar como routers remoto. A diferencia del PAP, este utiliza el método MD5 para encriptar la contraseña y una vez que se logró establecer el enlace los routers agrega un mensaje de desafío, el cual se genera para verificar que ambos coincidan aceptando la autentificación de lo contrario dicha conexión se cerrará inmediatamente.

2.2.4.4. MS-CHAP v2

MS-CHAP v2 fue desarrollado por Microsoft en el año 2013, como un método de validación. Así, el Protocolo de autenticación por desafío mutuo se empleó en VPNS y está basado en el protocolo de túnel punto a punto (PPTP). Microsoft indica a las organizaciones que utilizan MS-CHAP v2 sin encapsulamiento, están trabajando con una configuración insegura. (Microsoft ,2021). En páginas oficiales de Microsoft sugiere utilizar MS-CHAP v2/PPTP implementen un protocolo de autenticación como el PEAP, permitiendo de esta manera encapsular el tráfico que se genere en TLS evitando así inconvenientes que se pueden generar.

2.2.5. Protocolos de seguridad SSL, SSH y HTTPS

Adicionalmente en las redes WLAN se puede aplicar otros protocolos de seguridad tales como SSL, SSH y HTTPS.

> El protocolo SSH es un protocolo criptográfico diseñado para proveer comunicaciones seguras en internet. El cual se basa en el uso de certificados digitales y se ha convertido en el estándar de facto para transacciones Web seguras. HTTPS es la versión segura de HTTP que utiliza un cifrado basado en SSL para crear un canal más apropiado para el tráfico de información sensible que el protocolo HTTP. SSL y HTTPS permiten asegurar la comunicación mediante el acceso web entre cliente y servidor, protegiendo el proceso de autenticación con certificados que posibilita que con herramientas como el firebug que es un plugin para Firefox, con el cual se pueden observar los datos transferidos entre clientes y servidores web, no puedan obtenerse el usuario y la contraseña durante la conexión. En el caso del protocolo Secure Shell (SSH), sirve para acceder a máquinas remotas usando técnicas de cifrado a través de un canal SSH para que un atacante no pueda descubrir el usuario y la contraseña, ni lo que se escribe durante la conexión a los servidores. (González, Beltrán y Fuentes, 2016, p.133)

Con la ayuda de los protocolos de seguridad anteriormente mencionados se logra una comunicación confiable entre los usuarios, servidores y ordenadores que utilizan estos mecanismos, protegiendo así la integridad y confidencialidad de los datos personales del usuario. Cabe mencionar que estos protocolos no son los únicos, pero sí los más utilizados para este proyecto.

2.2.5.1. Estándares de seguridad para redes WLAN

Los estándares que actúan en la seguridad de Redes WLAN son diversos, entre los que se pueden mencionar con mayor relevancia son:

- WEP (Privacidad equivalente al cableado).
- WPA (Acceso protegido WiFi).
- WPA2(IEEE 802.11i y acceso protegido Wi-Fi2).

Considerando los estándares expuestos anteriormente cabe mencionar que existen 2 aspectos fundamentales como lo es la autenticación y el cifrado. La autenticación se define como un proceso con el que se verifica y asegura la identidad de las partes que interactúan en la transacción, logrando así evitar que un intruso asuma una identidad falsa, comprometiendo la integridad y la privacidad de la información. EL cifrado por su parte se encarga del tratamiento de todo el conjunto de datos que contiene un paquete con la finalidad de impedir que entidades ajenas logren mirar su contenido es por ello, que el cifrado posee un algoritmo que le permite transformar el mensaje modificando su estructura lingüística, con la finalidad de que sea incomprensible para todos aquellos que no tengan la clave del cifrado (González, Beltrán y Fuentes, 2016, p.131-133).

- **Definición de WEP**

Se lo define al estándar Web como sistema de cifrado, este apareció en el año de 1999 con el propósito de solucionar problemas que se suscitaban en redes inalámbricas abiertas. Portilla, Latorre, Pozo y Gonzáles (2016) mencionan:

> WEP o Wired Equivalente Privacy es el algoritmo opcional de seguridad para ofrecer protección a las redes inalámbricas incluido en la primera versión del IEEE 802.11. El estándar 802.11 ofrece mecanismos de seguridad mediante procesos de autenticación y de cifrado. En el modo Ad Hoc la autenticación puede realizarse mediante un sistema abierto o mediante un sistema de clave compartida. Un punto de acceso que reciba una petición podrá conceder autorización a cualquier estación o sólo a aquellas que estén permitidas. Como bien hemos visto en un sistema de clave compartida tan sólo aquellas estaciones que posean una llave cifrada serán autenticadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire. El estándar define el uso de RC4 con claves semillas (seeds) de 64 y/o 128 bits, de los cuales 24 bits corresponden al

vector de inicialización (IV – Inicialización Vector) y el resto, 40 o 104 bits, a la clave secreta compartida entre emisor y receptor. (p.3)

De esta manera se diría que el estándar WEB es un sistema de cifrado el que permite brindar seguridad a una red WLAN (red de área local inalámbrica) proporcionando un nivel de seguridad y privacidad complejo con la identificación de un usuario y contraseña.

- **Definición WPA**

El estándar WPA realizó apareció con la finalidad de subsanar los problemas que su predecesor WEP dejaba, mejorando así el cifrado de datos y ofreciendo un nuevo protocolo de cifrado. Tafur y Chávez (2018) afirman:

> La WPA (Wi-Fi Protected Access, Acceso protegido Wi-Fi) utiliza un nuevo protocolo de seguridad llamado TKIP (Temporal Key Intergrity Protocol), que es el mismo que se utiliza en el estándar IEEE 802.11i. Este sistema también utiliza claves simétricas con el algoritmo RC4, pero para añadir protección adicional, TKIP genera claves temporales que son cambiadas de forma dinámica. Corrige fallos de seguridad y añade algunas mejoras más respecto a WEP, por ejemplo, usa un vector de iniciación de 48 bits en lugar de los 24 utilizados en WEP. El WPA contempla los siguientes algoritmos de autenticación: WPA-Enterprise: donde la autenticación se realiza por medio de un servidor de autenticación (tipo RADIUS), normalmente esta solución se implementa en escenarios corporativos. WPA-PSK (WPA Pre-Shared Key): Se realiza por medio de una clave precompartida, este tipo de solución tiene menos restricciones y es usada en ambientes caseros. La contraseña comúnmente solicitada es de tipo alfanumérica de entre 8 a 63 caracteres teniendo un valor de 256 bits. (p.15)

Con la utilización del estándar WPA se logró de una manera disminuir las vulnerabilidades que el protocolo WEP poseía, sin embargo, al realizar pruebas resultó que aún estos dos eran bastante funerales ante ataques.

Tabla 2. Características WEP-WPA

Función	WEP	WPA
Encriptación	Débil	Soluciona debilidades
Claves	40 bits	128 bits
Claves	Estáticas	Dinámicas
Claves	Distribución manual	Automática
Autenticación	Débil	Fuerte, según 802.1x y EAP

Fuente: Tafur y Chávez. (2018)

- **Definición WPA 2**

En el año 2004 se conoció un estándar que sería el sucesor del WAP este era el IEEE 802.11i también conocido como WPA2. Tafur y Chávez (2018) indican que fue creado por la organización WIFI-ALLIANCE y tenía como meta mejorar la seguridad de su predecesor con la finalidad de disminuir los ataques que se generaban por medio de archivos diccionarios. Uno de los cambios que se observó fue la utilización de AES (Advanced Encryption Standard, Estándar de encriptación avanzado) en vez de usar RC4, aunque la utilización de este estándar implicaba cambio de hardware, pero incluye todas las características de WPA.

2.2.5.2. Protocolos de autenticación

Los protocolos de autenticación están diseñados concretamente para la transferencia de datos entre dos dispositivos o entidades, para la investigación presente se ha tomado en consideración los siguientes los siguientes:

- EAP
- PEAP
- LEAP
- RADIUS

- **Protocolo EAP**

EAP es un protocolo que se utiliza generalmente para transmitir información entre un usuario (cliente) y un servidor de autenticación, dicho protocolo tiene característica que busca incrementar la seguridad de las redes WLAN. Marín, Zapata y Gómez, (2007) manifiestan:

> EAP proporciona una manera flexible de autenticación usando los llamados métodos de autenticación EAP (que generalmente proporcionan material criptográfico como resultado de una autenticación correcta) (...). El Protocolo Extensible de Autenticación EAP ha sido

> diseñado para permitir diferentes clases de mecanismos de autenticación, a través de los llamados métodos EAP. Dichos métodos se ejecutan entre un cliente EAP (el usuario móvil) y un servidor EAP (normalmente ubicado junto al servidor AAA) a través de un verificador EAP (EAP autenticar), el cual simplemente reenvía los paquetes EAP entre el cliente EAP y el servidor EAP con la intención de completar el proceso de autenticación. Para esto, por un lado, entre el cliente EAP y el verificador EAP, se usa un protocolo de transporte EAP (EAP lower-layer) para llevar los paquetes EAP entre ambas entidades. Por otro lado, un protocolo AAA como RADIUS o Diameter se utiliza para el mismo propósito entre el verificador EAP y el servidor EAP. (p.487)

La finalidad del protocolo EAP es incrementar la seguridad de una red limitando el acceso de los usuarios mediante el uso de credenciales las mismas que serán verificadas en un servidor de autenticación, dicho protocolo puede ser utilizado tanto en redes WLAN como en redes cableadas.

- **Tipos de autenticación EAP**

a) EAP-TLS

Las redes inalámbricas al estar accesible a todo aquel que posea un dispositivo que recepta este tipo de señal se vuelve vulnerable, a lo que dentro de las redes inalámbricas se brindan autenticaciones de todo tipo, es así el caso de la autenticación de seguridad del nivel de transporte. Choez, Benites y Espinal (2016) afirman:

> EAP-TLS está basado en el uso de certificados digitales para la autenticación tanto del cliente como el servidor de autenticación. Esta implementación requiere del despliegue de una arquitectura PKI, en donde al menos debe existir un servidor de certificación para la emisión y manejo de los certificados, y un servidor de autenticación como un servidor RADIUS. (p.4)

Este tipo de autenticación hace uso de certificados que emplean contraseñas, además de permitir la gestión de claves WEP dinámicas.

b) EAP-TTLS

La atención de EAP-TTLS es una variante del protocolo EAP añadiendo en el nivel de transporte la seguridad TLS. Dicho protocolo permite realizar una mutua autenticación entre el

usuario y el servidor que lo autentica, obteniendo un mayor cifrado y de esa manera generar claves más seguras. Bosmediano y Cusme (2017) aseguran:

> EAP-TTLS es el método EAP (Extensible Autenticación Protocolo) que encapsula una sesión TLS (Seguridad de la capa de transporte), el cual consiste en establecer la conexión segura mediante la creación de un canal cifrado entre el cliente y el servidor para el envío de las credenciales de acceso durante el proceso de autenticación. Durante la fase de datos, el cliente se autentica al servidor (o cliente y el servidor se autentican mutuamente) utilizando un mecanismo arbitrario de encapsulado dentro del túnel seguro (PAP, CHAP, MS-CHAP o MS-CHAP-V2). Es indescriptible la instalación de un certificado digital en el servidor de autenticación RAIDUS, permitiendo de esta forma reducir la complejidad del sistema, evitando la difusión de certificados a todos los dispositivos. (p.32)

A pesar de que EAP-TTLS no es tan seguro las conexiones inalámbricas cuenta con este certificado siendo útiles en algunos casos al configurar una WLAN.

Figura 2. Funcionamiento de autenticación EAP-TTLS
Fuente: Bosmediano y Cusme (2017)

c) EAP-MD5

Este tipo de autenticación es la primera implementada a lo largo del tiempo, fundamentalmente duplica la protección que ofrece con las passwords CHAP dentro de una red WiFi. “EAP-MD5 representa un tipo de soporte entre los dispositivos 802.1x. Debido a las vulnerabilidades conocidas de los sistemas de seguridad, un sistema que depende del dispositivo no es recomendable en empresas muy concienciadas en la seguridad.” (Blas, 2017, p.29). Con el tiempo este tipo de autenticación puede llegar a crecer, llegando a vendedores de software y poder llegar a posicionarse en el mercado dentro del mundo de seguridades inalámbricas por el potencial que esta brinda.

d) EAP-AKA

La autenticación EAP-AKA es un componente utilizado en las autenticaciones UTMS y acuerdo de claves. Ferigra, (2017) explica:

> Las características de EAP-AKA es permitir al Servidor AAA proveer acceso a los servicios del dominio PS del EPC a través de una red de acceso WLAN a los usuarios no 3GPP que utilizan USIMs, mejorando la seguridad de la red y previniendo ataques de redes no autorizadas, los equipos involucrados en el proceso de autenticación serían el UE, AC/BRAS, TGW, servidor AAA 3GPP y HSS. El AC/BRAS funciona como un cliente Radius, el TGW funciona como un proxy Radius para retransmitir los paquetes Radius de autenticación entre el AC y el Servidor AAA, el servidor AAA es el encargado de autenticar a los usuarios obteniendo la información de autenticación del suscriptor desde el HSS. Al utilizar este tipo de autenticación las llaves de inscripción de cada usuario son aprovisionadas en las USIM y en el HSS para ser requeridas en el proceso de autenticación. (p.83)

En breves rasgos este tipo de autenticación es un componente utilizado para autenticar y distribuir claves de sesión, haciendo uso del USIM (Módulo de Identificación del Abonado) del UMTS (Sistema Universal de Telecomunicaciones Móviles).

e) PEAP

Es un protocolo de autenticación, que viene a ser un bosquejo del protocolo del Grupo de Trabajo de Ingeniería en Internet (IETF) ayudado por Microsoft, Cisco y RSA Security. Bosmediano (2017) asevera:

> Propuesta por Cisco y Microsoft que al igual que EAP-TTLS lo que se pretende es eliminar los requisitos que necesita TLS. Es ideal para aquellos fabricantes que aún no disponen una certificación digital para cada dispositivo de su red, el cual autentifica a los usuarios en una base de datos realizando la autenticación de usuarios contra un servidor Windows (Active Directory, Windows NT), RADIUS o incluso contra los puntos de acceso de Cisco, la única falencia es que se limita a 50 usuarios. (p.32)

Este tipo de autenticación tiene su diseño para beneficiarse de la seguridad que se ofrece a nivel de transporte del lado del servidor, además de conceder varios métodos de autenticación.

f) LEAP

Este protocolo de autenticación es extensible, incluyendo funcionalidades de autenticación desafío-respuesta, además de conceder la asignación de claves dinámicas.

> El protocolo de autenticación extensible ligero (LEAP), desarrollado por Cisco, se basa en el marco de autenticación 802.1X, pero aborda varias debilidades mediante el uso de WEP dinámico y administración sofisticada de claves. LEAP también agrega autenticación de dirección MAC. (Prieto, 2018, p.26)

Entonces este tipo de autenticación cifra las comunicaciones de datos ayudado de claves WEP creadas de forma dinámica, con ello también admitiendo la autenticación mutua.

g) RADIUS

El protocolo RADIUS es un servidor que utiliza un esquema cliente-servidor, haciendo que mediante el uso de credenciales pueda autenticar el ingreso o denegación a determinado recurso. Así, un servidor Radius es un protocolo para permitir y autorizar el acceso a determinado recurso, por lo general hace uso del Puerto 1812 para permitir sus conexiones. Sus principales características son: el cliente que se encarga de transportar la información del usuario a los servidores Radius y posteriormente tomar una decisión y devolver una respuesta, la red de seguridad que es un secreto compartido que se encarga de autenticar la conexión entre el cliente y el servidor Radius para evitar que personas que están husmeando en la red puedan acceder a contraseñas de los usuarios, mecanismo de autenticación flexible que es la parte en donde se Brinda el tipo de autenticación en la que se Puede ayudar como por ejemplo (PPP, PAP, CHAP) y finalmente el protocolo extensible que tiene como finalidad destinar objetos sobre registros en Internet (Albújar, 2017). Además, este protocolo permite una administración de la red para poder controlarla en todo momento, así mismo la facilidad de poder facturar en función de megas utilizadas, lo que es una ventaja en lo que a la implementación de portales cautivos se refiere.

2.2.6. Definición de red de datos

El término Red de datos forma parte indispensable para la presente investigación porque es indispensable para el desarrollo de esta, el concepto que se tomado en cuenta es el de los autores Díaz y Contreras (2009) en el que afirman:

> Una red de datos es una agrupación de computadoras, impresoras, routers, switches y dispositivos que se pueden comunicar entre sí a través de un medio de transmisión. La interconexión tiene como finalidad transmitir y compartir información, recursos, espacio en disco, etc. (p.28)

El desarrollo de las redes de datos posibilita su conexión mutua y, finalmente, la existencia de Internet. Con la creación de las redes de datos se desarrollaron un número elevado de aplicaciones las cuales eran diseñadas para microcomputadoras, las cuales para el inicio de la globalización los microcomputadores no estaban conectados entre sí, a diferencia de los terminales mainframe o computadora central esto lo usaban compañías que procesan gran cantidad de información con la finalidad de compartir datos entre varios computadores de una manera más eficaz y que consuma menos tiempo en transmisión. Asenjo, (2009) menciona:

> A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron 23 como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se volvió cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos. (p.22)

Una de las primeras soluciones fue la creación de los estándares de red de área local (LAN Local Área Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas.

2.2.6.1. Dispositivos de red

Los dispositivos y medios que componen la red son tan importantes como la información que se pretende enviar, debido a que si posee equipos que estén obsoletos puede tener inconvenientes al momento de transferir datos. De igual manera sucede con el medio por el que pretende compartir la información debe adaptarse a las tecnologías actuales para de esa manera no tener inconvenientes en propagar sus datos. Casillas y Gallardo (2016) definen:

> A los dispositivos de una red como entidades que están conectados entre sí y estos se clasifican en dos tipos. Aquellos que se encargan de gestionar el acceso y la comunicación como los módems, router, switch, bridge, access point entre otros y aquellos dispositivos que se conectan para utilizar el servicio como lo son celulares, tablets, computadores, impresoras, etc. Pues bien, pero estos dispositivos deben tener una manera de poder comunicarse y así lograr intercambiar información, esta manera de comunicarse se le define como medio de transmisión de datos. Estos medios pueden clasificarse por dos tipos de conexión inalámbrica y cableada. (p.18)

La conexión mayormente utilizada es la cableada, esta se trasmite mediante tecnologías como lo son los cables coaxiales, fibra óptica y el par trenzado (UTP/STP). Ahora bien, para los equipos inalámbricos la conexión se la realiza con la ayuda ondas de radio las mimas que se encuentran en el ambiente.

- **Definición Hub**

Dentro de las redes inalámbricas el tener equipos que brinden diferentes funcionalidades es algo imprescindible que hace que la red sea más robusta y brinde una calidad óptima, una de ellas es la ampliación de la red, uno de los tantos equipos que permite realizar esta acción es el Hub.

> Conocido como concentrador, pertenece a la capa física del modelo OSI y tiene como función conectar las PC´s sin ser administradas, la desventaja de su uso es que puede haber colisiones a la hora de comunicar varias computadoras a la vez y la topología no administrable. (Riveros, 2019, P.25)

En la actualidad hay más equipos que permiten realizar el trabajo del Hub Como son los switchs y los conmutadores, lo que hace que este equipo se lo utilice menos.

- **Switch o conmutador**

Dentro de una red informática se necesita conectar varios elementos para que trabajen dentro de una red, un switch logra realizar esta acción al trabajar en la capa de enlace de datos dentro del modelo OSI.

> Es semejante al Hub, pero trabaja de manera diferente ya que recibe la información por paquetes y lo envía a un punto de destino específico evitando el tráfico en red y fluyendo la información, se encuentra en el segundo nivel de OSI. (Amaya, 2018, p.27)

Este dispositivo al utilizarse en la conexión de equipos en red forma una red de área local, además de interconectar también dispositivos cableados.

- **Router**

Dentro de redes informáticas la administración del tráfico de información que transita por una red de computadoras es de suma importancia, dicha acción es posible gracias a routers o encaminadores. López, (2018) explica:

> Encaminador o router, el dispositivo de interconexión con mayor grado de relevancia en las redes informáticas. Este dispositivo es capaz de interconectar redes ubicadas en el mismo nivel o en niveles diferentes. Ejemplo: puede conectar redes que se encuentren en la misma capa de red del modelo OSI o conectar redes que se encuentren en la capa de enlace de datos con la capa de red. Así, el router se desenvuelve en la capa de red del modelo OSI (capa 3). (p.16)

En la actualidad los routers dan mayores funcionalidades como por ejemplo virtualización, colaboración multimedia y ahorro de costos en las operaciones.

- **Wireless LAN Controller**

WLC o (Wireless LAN Controller) un equipo de alto rendimiento que se emplea en combinación con un protocolo (LWAPP). Así, este equipo se utiliza para gestionar ligeros puntos de acceso en grandes cantidades por el administrador de red o centro de operaciones de red. Wireless LAN Controller forma parte del plano de datos en el modelo Wireless de Cisco. El Controlador WLAN maneja automáticamente la configuración de 6 hasta 500 puntos de acceso inalámbrico desde cualquier lugar, en función del modelo (Mena y Jara, 2013, p.52). El WLC se diseñó para trabajar con tecnologías actuales como son la 802.11n que permite ofrecer un mayor rendimiento y escalabilidad en una empresa. Logrando así brindar una mayor seguridad Rf, junto a la capacidad de ayudar a gestionar de manera simultánea de 250 AP y alrededor de 7000 clientes inalámbricos.

- **Switch Troncal (Core)**

Se define como Switch Core a un dispositivo de alta disponibilidad que permite la comunicación de datos utilizando diversas técnicas de conmutación logrando conseguir velocidades de hasta 10 Gbps. Entre sus características más destacadas se tiene: balanceo de

carga, procesadores redundantes, tiple bus de datos, alta densidad en puertos Fast o Gigabit Ethernet. Además, este dispositivo permite la configuración con PoE para la alimentación de dispositivos como lo son los AP y Teléfonos IP (Gonzáles, 2012). Este equipo es indispensable para medianas y grandes empresas al proporcionarles la posibilidad de centralizar toda la red.

- **Firewall**

Se le denomina firewall en el ámbito informático a un dispositivo de seguridad el cual permite realizar un monitoreo de todo el tráfico que se genere en una red. Este dispositivo cumple con varias funciones entre ellas bloquear el acceso a redes que no estén autorizadas, permitiendo limitar, cifrar y principalmente proteger todo el tráfico que circula en la red gracias a las reglas o políticas de seguridad que se le ha establecido (Guerra, 2019). El firewall mayormente se encarga de restringir el acceso a usuarios que no estén autorizados, bloqueando peticiones que se realizan desde una red pública y que intentan ingresar a una red LAN privada.

2.2.6.2. Medio de trasmisión de datos

- **Cable UTP**

En redes y telecomunicación existen ciertos servicios que están listos para ser brindados, los cuales deben tener un medio de trasporte adecuado para que este mismo servicio funcione con eficacia, un medio de trasporte físico es el cable UTP. Así, estos penden netamente del par de hilos trenzados lo que conlleva a que produzcan como resultado un efecto de anulación con la finalidad de que se limite la degradación de la señal, además de brindar un auto blindaje de los hilos de par trenzado. La TIA/EIA se encarga de brindar los estándares para el cableado UTP, pero la TIA/EIA-568 se encarga de promover los estándares comerciales para cableado en donde se requiera instalaciones LAN. Las características que se definen son tipos de cables a utilizar, la longitud, conectores, entre otros (Linares, 2017). La IEEE se encarga de calificar el cable por categorías dependiendo de la capacidad a la hora de transportar datos.

- **Cable de Fibra Óptica**

Las nuevas tecnologías de redes y telecomunicaciones han tenido grandes avances desde sus inicios. Así también el medio de transporte de datos también ha sufrido estos cambios para beneficio del hombre, puesto que anteriormente se utilizaban cables coaxiales, pero con los

avances tecnológicos realizados se ha comenzado a utilizar cables de fibra óptica que ofrece mayor velocidad al transportar paquetes. Jijón y Rojas (2017) afirman:

> La fibra óptica es un medio de transmisión utilizado generalmente en redes de datos y telecomunicaciones. Es uno de los medios de transmisión más utilizados en la actualidad, más avanzados ya que son inmunes a las interferencias electromagnéticas. El material con el que está hecho la fibra es de un hilo bien fino que puede ser de vidrio o materiales plásticos por donde pasan los haces de luz que representan los datos a transmitir (…). La fibra óptica es una guía de ondas dieléctrica construida a base de $SiO2$ por lo que no emite ni se ve afectada por las radiaciones electromagnéticas, diminuta con diámetros en el orden de los micrones, ligera en peso, que opera a determinadas frecuencias, capaz de transmitir a largas distancias con grandes anchos de banda y prácticamente con menores costos. Las fibras ópticas son filamentos generalmente en forma cilíndrica, que consiste en dos partes principales: un núcleo (Core) de vidrio en el orden de los 10 μm y un recubrimiento (Cladding) normalmente de 250 μm de diámetro de vidrio o plástico. (p.7)

La fibra óptica es una tecnología que se ha convertido en un medio casi indispensable por lo que muchas personas se cambian a esta, por la rapidez y calidad de conexión que esta ofrece.

2.2.6.3. Definición de nodos

Los nodos dentro de informática son puntos de conexión que se unen en un mismo lugar. Así, dentro de una red informática los nodos son componentes que forman parte de esta, además de estar conectados también interactúan entre ellos, compartiendo información, recursos y servicios; estas interacciones pueden generar fenómenos dinámicos de gran interés (Aldana, 2006). Si nuestra red es internet entonces los nodos que la formarán serán cada uno de los servidores.

2.2.7. Latencia en red de datos inalámbrica

La latencia dentro de redes es un factor que ha llegado a tomar relevancia dentro de conexiones inalámbricas. Así, la latencia muestra el tiempo de respuesta entre una petición y la respuesta, generando que los datos se pierdan de forma temporal. Los diferentes factores que inciden para que la latencia se eleve puede ir desde la estructura hasta la capacidad del internet (Mantilla, 2019). Cuando la latencia tiende a elevarse el tiempo de carga de las páginas también lo hace, incidiendo en la navegación en internet.

2.2.7.1. Factores generadores de latencia

La presencia de latencia en redes WLAN es comúnmente normal debido a que está presente en todas las redes inalámbricas, al utilizar una conexión mediante ondas electromagnéticas hay factores que generan mayor presencia de latencia. Panwar (2020) indica que entre estos factores se encuentra la señal de cobertura, infraestructura tecnológica, capacidad de propagación del equipo, ancho de banda, entre otros. Siendo el ancho de banda y la señal de cobertura los elementos más importantes puesto que entre menor ancho de banda posea una red inalámbrica la capacidad para enviar y recibir los paquetes de datos se verá reducida, y entre mayor sea la distancia que existe desde el equipo que propaga la señal su tiempo de respuesta se verá aumentado.

2.2.7.2. Latencia óptima

Para la medición de latencia se utiliza el ping, la unidad en la que se expresa la latencia es en milisegundo. Jiménez (2021) indica que para poder realizar labores cotidianas sin inconveniente alguno el valor debe estar por debajo de los 40ms aun que lograr obtener esta estimación puede ser casi imposible debido a varios factores. Si el valor entra en un rango de 40 a 100 ms ya se lo considera como un retardo llegando a generar fallos como ruido en el canal de audio, imágenes borrosas, perdidas momentáneas de internet.

2.2.7.3. Latencia Per-Frame en WiFi

Tal latencia es el tiempo que tarda en seleccionar una trama de datos para posteriormente ser enviada a través de la tarjeta NIC (Tarjeta interfaz de red) WiFi. Hay que tener en cuenta que el tiempo de espera en la tarjeta NIC no se incluye en el retraso al enviar paquetes. Pei et al. (2017) afirman:

> La latencia Per-Frame proviene principalmente de dos tipos de colas: la cola del host y la cola distribuida, que es causada por el mecanismo CSMA / CA cuando varios nodos compiten por el canal. Si bien la cola del host se puede omitir fácilmente mediante la programación de prioridad en el host final, la cola distribuida no lo es. Anteriormente, IEEE 802.11e intenta proporcionar prioridades en esta cola distribuida ajustando los parámetros de la capa MAC, pero no escala cuando hay un número creciente de flujos sensibles al retardo. (p.4)

La latencia no solo depende de factores externos como lo es la red o los equipos que propagan la señal WiFi, sino también los equipos que el usuario posee para realizar dicha conexión.

2.2.7.4. Definición de ancho de banda

El ancho de banda es la capacidad que posee una red al transferir datos en un tiempo concreto. Castillo (2019) indica que el ancho de banda llega a ser básicamente la cantidad de datos que se puede enviar y recibir en el ámbito de una comunicación y está definida por una unidad de tiempo que son los segundos. Se puede medir el ancho de banda en bit/s o sus múltiplos (Kbit/s, Mbit/s). Hay que tener en cuenta que entre mayor ancho de banda se posea puede transferir datos con mayor velocidad y disminuir el tiempo en el que se transfieren las tramas de paquetes.

2.2.7.5. Ancho de banda en redes WiFi

Como se mencionó anteriormente el ancho de banda es la capacidad datos que se pueden trasferir entre dos puntos, no obstante, el ancho de banda en redes WI-Fi está definido por el tipo de estándar IEEE 802.11 con el que fue diseñado la red WLAN. El estándar mencionado previamente posee versiones que han ido evolucionando en cuanto al ancho de banda utilizable, el estándar más utilizado es el IEEE 802.11b el cual aplica una tasa de transmisión de 11 Mbit/s utilizando una banda de 2.4 GHz (Tobar, Gaitán y Urrego, 2016). Pues bien, con el transcurrir del tiempo el estándar 802.11g está posicionándose como uno de los preferido debido a que dicho estándar puede trasferir hasta 54Mbps entre el equipo cliente y el dispositivo AP.

2.2.8. Contenido web

El contenido web encontrado en internet ha sido una herramienta fundamental en la vida diaria de las personas en los últimos tiempos debido a la información que este brinda. Así, el contenido web es un conjunto de documentos que por medio de hipertextos juntan en él información como imágenes, texto, videos y archivos de todo tipo para juntarlos en un solo documento. Este contenido web viene a formar parte de todo el contenido que existe en internet. Los diferentes tipos de contenido que han ido emergiendo con el tiempo hasta la actualidad son los siguientes: la web 1.0 en la cual solo se podía realizar consultas para acceder a contenido sin poder tener interacción bidireccional, la web 2.0 abarca contenido en el que se puede compartir información mediante interacción, la web 3.0 permite acceder al contenido mediante palabras claves y la web 4.0 que es relativamente nueva porque empezó en el 2016 en la que el contenido web se lo puede obtener mediante afirmaciones o peticiones (Latorre, 2018). Entonces el

contenido web disponible en internet viene a ser extenso y fundamental para las acciones que se realizan en esta era digital en la que se vive actualmente.

2.2.8.1. Definición de sitio web

Un sitio web en el mundo actual se ha convertido en una tecnología fundamental, llegando a convertirse en una revolución tanto en lo académico como en el hogar. Así, un sitio web es un espacio virtual en internet, el mismo que abarca diferente información a partir de una programación previa, este se hace esencial por la diversa información que contiene como imágenes, documentos, audio, videos, entre otros archivos. Para el acceso a estos sitios se debe conocer la dirección IP publica o nombre (Sansano, 2017). Con esto los sitios web han tomado gran protagonismo en los últimos tiempos, llegando a ser parte del diario vivir.

2.2.9. Definición de herramientas tecnológicas

La tecnología ha dado pasos agigantados a través de la historia y hoy en día se ha convertido en instrumento fundamental para varias actividades. Pereira, Camacho, y de la Rosa (2018) afirman:

> La eficacia de las nuevas tecnologías está dada en la influencia de ésta en elementos básicos que le son inherentes a las personas, como el habla, el recuerdo o el aprendizaje, es por ellos que las herramientas tecnológicas modifican en muchos sentidos la forma en la que es posible desarrollar diversas actividades en la sociedad moderna.

Estas nuevas tecnologías en el mundo moderno están inmersas en diferentes actividades y áreas.

2.2.9.1. Definición de portal cautivo

Las redes inalámbricas en la actualidad se han convertido en una herramienta casi indispensable ya sea por lo fácil que es acceder a estas, además de que en la mayoría de los casos las personas ya cuentan con dispositivos de conexión WiFi. Por otra parte, es fundamental también conocer los lugares donde se expanden estas ondas inalámbricas, una de las formas más habituales es en los hogares o instituciones en donde la conexión se la realiza ingresando una contraseña o en algunos casos más específicos otro tipo de credenciales y la otra forma son en lugares de negocios como por ejemplo restaurantes, hoteles, centros comerciales y hasta en parques en donde se lo realiza mediante portales cautivos. Chérigo (2017) menciona:

> Un portal cautivo (o captivo) es un programa o máquina de una red pública y/o privada que vigila el tráfico HTTP1 y obliga a los usuarios a pasar por una página Web especial, en el cual deben ingresar un nombre de usuario (username) y una contraseña (password) asignadas, para así poder navegar por internet de forma normal. (p.25)

Es así, los portales cautivos son herramientas valiosas para el control de redes inalámbricas que ofrecen acceso a usuarios a una determinada red, mediante la realización de una acción.

- **Funcionalidad de un portal cautivo**

La funcionalidad de un portal cautivo es muy fácil, el funcionamiento es el siguiente: el usuario se conecta a la red e inmediatamente se visualizar la página del portal cautivo, el cual va a contener un Login de ingreso en donde se colocar las credenciales respectivas, estos serán validadas por medio de un servidor Radius o Windows Server 2012, posteriormente si el acceso es exitoso el portal cautivo le asignara una IP mediante DHCP para que pueda navegar (Guerra, 2014, p.113).

- **Ventajas de portal cautivo**

Los portales cautivos ofrecen varias ventajas por lo que se han convertido en una herramienta fundamental para establecimientos que ofrecen servicio de internet. Guerra (2014) asegura que los portales cautivos están disponibles para redes LAN y WLAN, se puede autenticar el acceso mediante usuarios ya establecidos en servidores externos o locales, la configuración no es compleja. Con la ayuda de esta herramienta se puede visualizar estadísticas de cada usuario conectado en la red, se puede asignar políticas por cada usuario o por todos los usuarios, no se compromete todo el sistema y lo mejor de todo es que a mayoría de portales cautivos son de software libre.

- **Desventajas de portal cautivo**

Si bien se ha mirado el beneficio de un portal cautivo ahora se tiene el otro lado de la moneda. Guerra (2014) afirma que las desventajas de la utilización de estos equipos pueden variar dependiendo del equipo o software que se utiliza por ejemplo las vulnerabilidades más observadas son: Vulnerabilidad ante spoofing (suplantación de identidad) de direcciones MAC e IP, el equipo cliente debe poseer un navegador para poder autenticarse, cifrado menos seguro (puede combinarse WEP/WPA). Presenta retrasos de conexión dependiendo del S.O. Las

desventajas mencionadas son las más comunes que se pueden presentar estas varían dependiendo el software o hardware que utilizan para la implementación del portal cautivo.

- **Portal Cautivo por Hardware**

Dentro de redes informáticas el controlar el tráfico y los usuarios dentro de la misma se ha convertido en un trabajo de suma importancia, una de las formas de realizarlo es con portales cautivos, los mismos que pueden ser implementados por hardware o software. Así, los portales cautivos por hardware son herramientas que cumplen la misma funcionalidad de un portal cautivo por software, los cuales no necesita de un computador porque el dispositivo ya contiene la configuración para ser utilizada. Entre los diferentes portales por hardware se tiene: Endian HotSpot, 4ipnet HSG300 Wireless HotSpot Gateway, Pfsense, entre otros (Casillas y Gallardo, 2016). Cabe recalcar que la utilización de los portales cautivos va a depender de la parte económica disponible, los portales cautivos por hardware son un poco más costosos con referencia a los portales cautivos por software.

- **Portal Cautivo por Software**

Los portales cautivos por software no son más que programas, los mismos que van a ser instalados en un equipo físico dependiendo de las características y requerimientos que el software necesite, estos pueden ser tanto privativos como open source , a continuación, se indica los portales en la tabla 3.

Tabla 3. Portales cautivos por software

N°	Portal Cautivo
1.	OpenWRT
2.	WifiDog
3.	CoocaChilli
4.	AirMarshal
5.	Pfsense
6.	ZeroShell
7.	ChilliSpot

Hay que mencionar que estos programas la mayoría están basados en Linux motivo por el cual son utilizados comúnmente como una herramienta de control y seguridad de redes WLAN.

a) AntamediaHotSpot

Hoy en día la administración de puntos de acceso a internet inalámbrico se ha convertido en algo muy necesario en establecimientos como restaurantes, hoteles, centros comerciales e incluso parques. Anta media HotSpot ofrece una administración fácil y completa de lo que se requiere para administrar una red WiFi.

> Anta media HotSpot Software es el software de gestión de puntos de acceso WiFi para invitados con más funciones de la industria. Le ayuda a controlar y facturar a sus clientes por el acceso a Internet, involucrarlos con anuncios cautivadores, recopilar datos de huéspedes y encuestas, enviar correos electrónicos promocionales automáticos.
>
> Cree una conexión WiFi -gratuita para invitados utilizando el inicio de sesión social, palabras clave compartidas, verificación por SMS o correo electrónico, u ofrezca un acceso WiFi de pago más rápido con una tarjeta de crédito o pagos de PayPal, boletos preimpresos, integración de Hotel PMS con habitación / nombre y mantenga el 100% de ganancias. (ANTAMEDIA, 2021)

El software Anta media HotSpot es esencial cuando se desea una administración del punto de acceso WiFi con cualquier PC, además de brindar una licencia de por vida y soporte gratuito con respaldo de profesionales expertos en la industria.

b) Chillispot

Una herramienta reconocida para el manejo y control de redes inalámbricas es ChilliSpot, que al ser una herramienta dedicada a portal cautivo la hace ser más simple y fácil de utilizar.

> ChilliSpot es un portal cautivo de código abierto o controlador de punto de acceso LAN inalámbrico. Se utiliza para autenticar a los usuarios de una LAN inalámbrica. Admite el inicio de sesión basado en web, que es el estándar actual para los HotSpots públicos. La autenticación, autorización y contabilidad (AAA) está a cargo de su servidor Radius favorito. Las descargas binarias están disponibles para Redhat, Febora, Debian, Mandrake y OpenWRT. ChilliSpot es un ebuild en Gentoo y se compila bajo FreeBSD. El código fuente bajo GPL está disponible para otras plataformas. Para crear su propio HotSpot, necesita los siguientes elementos: conexión a Internet, punto de acceso de LAN inalámbrica, software ChilliSpot para tu PC, servidor de radio, y servidor web. (ChilliSpot, 2021)

Actualmente ChilliSpot no cuenta con versiones actuales, su ultimo versión data del año 2006. Es por ello por lo que no cuenta con una comunidad que brinde soporte en el caso de necesitarlo.

c) WifiDog

Un software con una gran trayectoria para el manejo de host spots es WifiDog que al ser un portal cautivo completo y fácil de configurar ha contribuido en el trabajo de los operadores de redes abiertas en instituciones que estas lo requieran.

> El proyecto WifiDog fue iniciado por Ile sans fil y actualmente está en producción. Las soluciones de portal cautivo existentes eran casi imposibles de integrar (NoCat, que se basa en perl, GnuPG, OpenSSL), o solo estaban diseñadas para mostrar descargos de responsabilidad sin ningún control de acceso (NoCatSplash y otros). WifiDog está diseñado para tener control de acceso centralizado opcional, contabilidad de ancho de banda completo, latido de nodo y contenido local específico para cada punto de acceso. No depende de una ventana de JavaScript, por lo que funciona con cualquier plataforma con navegador web, incluidos PDA y teléfonos móviles. Está desarrollado en C para facilitar su inclusión en sistemas integrados (ha sido diseñado para el Linksys WRT54G, pero se ejecuta en cualquier plataforma Linux reciente). Una instalación típica solo toma 30 kb en i386, y una instalación completamente funcional podría realizarse en menos de 10 kb si fuera necesario.
>
> La suite del portal es principalmente un servidor de autenticación codificado en PHP usando una base de datos PostgreSQL. Por otro lado, la puerta de enlace WifiDog se conecta al servidor de autenticación para obtener directivas basadas en la información enviada por los usuarios en uno de los puntos de acceso. Todas las cosas administrativas / locales están en el servidor de autenticación y la puerta de enlace solo está jugando con las reglas de firewall de la puerta de enlace para permitir o denegar el acceso de los usuarios.
>
> También cabe destacar las amplias funciones de gestión de LBC (contenido basado en la ubicación) disponibles. Hay algunas funciones de LBS (servicio basado en la ubicación) disponibles y continúan siendo un área de desarrollo. (WifiDog, 2021)

Actualmente esta herramienta de portal cautivo sigue brindando sus servicios, brindando soporte y contando con una comunidad brindando aportes.

d) Zero Shell

Una herramienta con múltiples funcionalidades, pero a su vez fácil de configurar es ZeroShell, esta es muy reconocida en lo que a gestión de redes se refiere, por lo que hoy en día muchos lugares que ofrecen hotspot la usan por las diferentes funciones que esta otorga.

> Zeroshell es una distribución basada en Linux dedicada a la implementación de dispositivos de enrutador y firewall completamente administrables a través de una interfaz web. Zeroshell está disponible para plataformas x86 / x86-64 y dispositivos basados en ARM como Raspberry Pi. Algunas características avanzadas de Zeroshell son: Equilibrio de carga y conmutación por error de varias conexiones a Internet, VPN de sitio a sitio y VPN de host a sitio, acceso al portal cautivo para Internet Hotspot, reglas de firewall que utilizan la inspección profunda de paquetes (filtros de capa 7 y nDPI), calidad de los servicios y modelado del tráfico mediante la inspección profunda de paquetes, proxy web transparente con antivirus y listas negras de URL, autenticación y contabilidad RADIUS, gestión de puentes y VLAN, punto de acceso inalámbrico con soporte para múltiples SSID, conexiones móviles, seguimiento y registro de las conexiones de red. (Zeroshell, 2021)

Esta herramienta cuenta con una actualización y una extensa comunidad activa hasta la fecha que la hace estar en auge entre diferentes softwares de portales cautivos.

e) MonOwall

La herramienta m0n0wall brinda diferentes funciones para poder configurar un HotSpot, además de no ser un sistema que pide muchos requisitos.

> m0n0wall es un proyecto destinado a crear un paquete completo de software de firewall integrado que, cuando se usa junto con una PC integrada, proporciona todas las características importantes de las cajas de firewall comerciales (incluida la facilidad de uso) a una fracción del precio (software gratuito).
>
> m0n0wall se basa en una versión básica de FreeBSD, junto con un servidor web, PHP y algunas otras utilidades. Toda la configuración del sistema se almacena en un solo archivo de texto XML para mantener la transparencia.

> m0n0wall es probablemente el primer sistema UNIX que tiene su configuración de arranque realizada con PHP, en lugar de los scripts de shell habituales, y que tiene toda la configuración del sistema almacenada en formato XML. (m0n0wall, 2021)

Actualmente esta herramienta no brinda actualizaciones y el soporte en su comunidad data del año 2015, siendo esto no tal fiable utilizarla en este momento si se presentan errores no se tendrá una comunidad que ayude a brindar soluciones.

f) OPNsense

OPNsense es una herramienta de código abierto con diferentes funcionalidades en las que destacan configuraciones de firewall y portal cautivo.

> OPNsense es una plataforma de enrutamiento y firewall de código abierto, fácil de usar y fácil de construir, basada en HardenedBSD. OPNsense incluye la mayoría de las funciones disponibles en costosos firewalls comerciales y más en muchos casos. OPNsense comenzó como una bifurcación de pfSense® y m0n0wall en 2014, con su primer lanzamiento oficial en enero de 2015. El proyecto ha evolucionado muy rápidamente y aún conserva aspectos familiares de m0n0wall y pfSense. Un fuerte enfoque en la seguridad y la calidad del código impulsa el desarrollo del proyecto.
>
> OPNsense ofrece actualizaciones de seguridad semanales con pequeños incrementos para reaccionar ante nuevas amenazas emergentes en un momento de moda.
>
> Un ciclo de lanzamiento fijo de 2 lanzamientos principales cada año ofrece a las empresas la oportunidad de planificar actualizaciones con anticipación. Para cada lanzamiento importante, se establece una hoja de ruta para guiar el desarrollo y establecer objetivos claros. (OPNsense, 2021)

Esta herramienta a pesar de sus buenas funcionalidades ya no cuenta con soporte al día y tampoco actualizaciones.

g) Pfsense

Pfsense es una herramienta que es de código abierto, brindando funcionalidades para el manejo de redes, contando también con una interfaz fácil de configurar.

> El proyecto Pfsense es una distribución de firewall de red gratuita, basada en el sistema operativo FreeBSD con un kernel personalizado e incluye paquetes de software gratuitos de terceros para una funcionalidad adicional. El software Pfsense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más de los cortafuegos comerciales comunes, sin ninguna de las limitaciones artificiales. Ha reemplazado con éxito todos los firewalls comerciales de renombre que pueda imaginar en numerosas instalaciones en todo el mundo, incluidas Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro y más.
>
> El software Pfsense incluye una interfaz web para la configuración de todos los componentes incluidos. No es necesario tener conocimientos de UNIX, no es necesario utilizar la línea de comandos para nada y no es necesario editar manualmente ningún conjunto de reglas. Los usuarios familiarizados con los firewalls comerciales se familiarizan con la interfaz web rápidamente, aunque puede haber una curva de aprendizaje para los usuarios que no están familiarizados con los firewalls comerciales. (Pfsense, 2021)

Actualmente esta herramienta cuenta con actualizaciones disponibles hasta la fecha, además de tener una comunidad activa que brinda soluciones de inmediato.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Dentro de la presente investigación de grado se propone la utilización de un método de investigación de enfoque mixto, el cual para el estudio de la variable independiente denominada latencia en la red de datos se utilizó el enfoque cuantitativo discreto, este permitirá conocer valores enteros en la investigación. Así, el enfoque cuantitativo muestra la necesidad de realizar mediciones y estimar magnitudes de los fenómenos de estudio (Hernández, 2017). Este enfoque va a permitir recolectar datos numéricos tales como número de dispositivos conectados, número de conexiones establecidas, porcentaje de ancho de banda, porcentaje fallos en la conexión a internet entre otros factores que influyen y están presentes en la red de datos de la Universidad Politécnica Estatal del Carchi.

Por otra parte, el enfoque cualitativo ordinal se aplicará a la variable dependiente denominada accesibilidad al contenido en la web. Así, el enfoque cualitativo es un procedimiento en el cual no se requiere la recolección de datos no predispuestos completamente, esta se basa en recolectar puntos de vista de los participantes en la investigación, recalcando también que la medición no es numérica (Hernández, 2017). El enfoque cualitativo para utilizar es de tipo ordinal el mismo que permitirá mediante una encuesta conocer el grado de satisfacción con el servicio que brinda la Universidad, conocer datos como porcentajes de tareas enviadas mediante el uso de internet, número de páginas web visitadas.

3.1.2. Tipo de Investigación

Tomando en cuenta que el estudio tiene un enfoque mixto se ha seleccionado los siguientes tipos de investigación a utilizar.

- Investigación de campo

Con ayuda de la investigación de campo se recolectará datos directamente del lugar de los hechos siendo la Universidad Politécnica Estatal del Carchi el centro de estudio, aquí se aplicará una entrevista dirigida al personal de TIC’s, la cual arrojará información sobre la red inalámbrica y las falencias que esta posee. La información que se recolecta es de gran trascendencia para la propuesta tecnológica que se pretende realizar. Se ha iniciado el estudio

con la investigación de campo al respecto Palella y Martins (2010), afirman: “La investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables (...).” (p.88). Por esta razón se debe identificar primero los problemas que se están generando en la casona Universitaria.

- Investigación-Acción

En el estudio presente se utilizará la investigación-acción, esta permite brindar varias soluciones a las problemáticas que se presentan en el diario vivir. Teniendo en cuenta que la Investigación -Acción. “No solo involucra al investigador, sino también a todos los integrantes de este, los cuales, a partir de la detección de la situación problemática, aportarán sus ideas y posibles soluciones desde la elaboración de proyectos o planes de acción” (Sequera ,2014, p.223-229). Considerando la definición anterior se pretende identificar los problemas que afectan a la red inalámbrica de la Universidad logrando de esa manera elegir una herramienta informática basada en software libre que ayude a mitigar las falencias como: conexiones fallidas, errores al descargar archivos, retardo en la carga de páginas web, pruebas online suspendidas, entre otras.

- Investigación descriptiva

Esta investigación ayudará a verificar el estado actual de la red de datos inalámbrica de la UPEC además de identificar equipos que se encuentran obsoletos, los mismos que afectan la accesibilidad al contenido web. Este tipo de investigación brindo la oportunidad de conocer diferentes puntos de vista los mismos que son fundamentales dentro del estudio, Así, la investigación descriptiva permite conocer aspectos que son de suma importancia como características específicas de un cierto objeto, persona o grupo (Sánchez, Reyes, y Mejía, 2018). A partir de los involucrados como son los estudiantes y la red de datos de la Universidad, partiendo del problema el cual es la indisponibilidad a la navegación por parte de dispositivos inalámbricos.

3.2. IDEA A DEFENDER

La elevada latencia en la red de datos inalámbrica disminuye la accesibilidad al contenido web a los estudiantes de la UPEC.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

3.3.1. Definición de variables

Para la definición de las variables de investigación en el presente estudio se ha tomado en cuenta dos variables:

- **Variable Independiente (Cuantitativa-Discreta)**

En la investigación actual se establece como variable independiente "latencia en la red de datos", a esta se la define como la suma de retrasos momentáneos que están presentes en la trasmisión y propagación de paquetes de datos en una red, Jackson (2019) afirma:

> La latencia de la red se refiere al tiempo y/o retraso que está implicado en la transmisión de datos a través de una red. En otras palabras, el tiempo que tarda un paquete de datos para ir de un punto a otro. Hoy día esto es normalmente medido en milisegundos, sin embargo, podía ser segundos dependiendo de la red. Mientras más cercana se aproxima a cero.

El estudio de esta variable tiene como finalidad analizar posibles fallas que se generan en la red y tratar de mitigarlas, se ha considerado la definición de Jackson al ser la más acertada para la investigación.

- **Variable Dependiente (Cualitativa - Ordinal)**

Para la investigación se tiene en cuenta como variable dependiente "accesibilidad al contenido web", la cual se la define de la siguiente manera.

Por una parte, se tiene la palabra accesibilidad. Accesible se refiere "De fácil acceso o trato." (Real Academia Española, s.f., definición 2).

La definición de contenido web se define de la siguiente manera. Así, el contenido web se lo viene a tomar como un conjunto de información como imágenes, texto, videos y archivos que por medio de hipertextos se juntan en un solo documento (Latorre, 2018). Es así como el contenido web es fundamental para obtener información que se desee en internet.

Por lo tanto, para la presente investigación y con los conceptos revisados anteriormente de la variable accesibilidad al contenido web se puede definirla como, la facilidad que una persona

tiene para manipular o acceder a la información que se encuentra en internet; ya sea esta en documentos, audios, imágenes, etc.

3.3.2. Operacionalización de variables

Tabla 4. Operacionalización de variables

Variable	Dimensión	Indicadores	Técnica	Instrumento
V.I. latencia en la red de datos inalámbricos (cuantitativa - discreta)	Red de datos	Porcentaje de fallos en la conexión a internet.	Encuesta	Cuestionario
	Dispositivos de interconexión	Numero de dispositivos totales en la infraestructura	Entrevista	
	Conexiones simultáneas	Número de dispositivos inalámbricos conectados simultáneamente a la red	Entrevista	
	Ancho de banda	Cantidad de megas distribuidas en la red	Entrevista	
	Paquetes transmitidos	Cantidad de paquetes transmitidos		
	Medios físicos de transmisión de datos	Estado de la infraestructura de la red		
VD. Accesibilidad al contenido en la web (cualitativa-ordinal)	Calidad de servicio	Grado de satisfacción de la red inalámbrica	Encuesta	Cuestionario
		Escala de utilización de la red	Encuesta	
		Eficiencia en las conexiones a la red	Encuesta	
		Tipos de dispositivos que se utiliza en la red inalámbrica	Encuesta	
	Ancho de banda	Megas utilizados en la red de datos inalámbrica	Encuesta	
		Distribuidos megas en cada red inalámbrica	Entrevista	
		Cobertura de la red	Entrevista	

3.4. MÉTODOS UTILIZADOS

- **Método Analítico**

Para la investigación se ha considerado el método analítico. Así, este método se justifica en el conocimiento general de la totalidad de un suceso o realidad con la finalidad de observar las causas y efectos que este posee, para llegar a conocer y explicar las peculiaridades de cada una de las partes y la relación que existe entre ellas (Cervera, 2014). Se utilizó este método, el mismo que ayudará a definir un todo, en la investigación será la red de datos inalámbrica de la Universidad Politécnica Estatal del Carchi con una de sus partes la latencia, el método antes mencionado aportó a identificar las causas y efectos que generan la latencia en la red inalámbrica de la Universidad.

- **Método Inductivo**

El método inductivo es un método científico que permite alcanzar conclusiones generales partiendo de antecedentes e hipótesis. Calduch (2014) afirma. "Consiste en conocer las características generales o comunes a una diversidad de realidades, tal y como se obtienen a partir del empleo del método comparativo, para articularlas mediante relaciones de causalidad y formular así proposiciones de validez general" (p. 33). En este sentido, este método elabora generalizaciones amplias con el apoyo de observaciones específicas. Este a su vez cumple pasos a realizar, iniciando por la observación de los hechos para posteriormente registrarlos, analizarlos y contrastarlos. Con lo anterior se clasifica la información, se establecen patrones y se genera una explicación o teoría.

3.5. ANÁLISIS ESTADÍSTICO

- **Población y Muestra**

La población seleccionada para la actual investigación es real finito, esta es la comunidad estudiantil de la UPEC la misma que consta de un número de 3450 estudiantes legalmente matriculados y distribuidos en diferentes carreras. La muestra con la que se trabajó fue de 252 alumnos, la cual se determinó mediante la siguiente formula.

$$n = \frac{z^2 \sigma^2 N}{e^2(N-1) + z^2 \sigma^2}$$

Donde:

- **n** es el tamaño de la muestra, es decir número de unidades a determinar.
- **N** es la población en la cual se define a los estudiantes universitarios de la UPEC.
- **σ** es la varianza de la población, este es un valor constante que equivale a 0.5, cuyo valor elevado al cuadrado es 0.25.
- **Z** es el valor determinado mediante el nivel de confianza, valor constante que se lo toma en relación de 90, equivale a 1.65
- **e** es el límite de error de la muestra que generalmente varía de acuerdo con el nivel de confianza en este caso 0.05%.

$$n = \frac{z^2 \sigma^2 N}{e^2(N-1) + z^2\sigma^2}$$

$$n = \frac{(1.65)^2 * (0.5)^2 * (3450)}{(0.05)^2 * (3450-1) + (1.65)^2 * (0.5)^2}$$

$$n = \frac{(2346)}{(9.30)}$$

$$n = 252$$

- **Técnicas de investigación**
  - Entrevista

Dentro de la presente investigación se tomando en cuenta la variable independiente denominada "latencia en la red de datos inalámbrica", para la recolección de información se realizó la entrevista al personal encargado de Redes y Telecomunicaciones del Centro de TIC's, el tipo de entrevista a utilizar es abierto. Así, la entrevista se la define como un intercambio de información entre las personas entrevistadas y el entrevistador. La entrevista puede clasificarse en estructuradas, semiestructuradas y abiertas. La primera es realizada cuando el entrevistador recolecta datos mediante el seguimiento de una guía sin que se desvincule de esta, la segunda se basa en el seguimiento de una guía, pero si se tiene la necesidad de aumentar preguntas se la realizará para obtener más información y finalmente la entrevista abierta se basa en que el entrevistador se ayuda de una guía en la cual tiene toda la flexibilidad del caso para realizar preguntas que le ayuden a recolectar los datos (Hernández, 2017). Por ello, se consideró a la

entrevista de tipo abierto como un método de recolección de información la cual permite levantar requerimientos necesarios para cumplir con el objetivo trazado.

- Encuesta

En la presente investigación se ha tomado como técnica de recolección de información la encuesta. Reyes (2015) define a la encuesta como una técnica la cual ayuda a la recolección de datos mediante el uso de un cuestionario y esta se aplica a una muestra de individuos siguiendo una serie de reglas científicas que hacen que esa muestra sea un conjunto representativo de la población general de la que procede. Con la ayuda de la encuesta se puede conocer opiniones y puntos de vista de ciudadanos. Para el actual estudio dicho instrumento fue diseñado en escala ordinal y con preguntas de tipo cerrado, la variable que se tomó para este caso es la dependiente, accesibilidad al contenido en la web, el instrumento fue dirigido a la comunidad estudiantil de la UPEC con la finalidad de que los usuarios aporten en la investigación, eligiendo una de las opciones que se les presentó en un listado, mediante el resultado de esta encuesta se proporciona información precisa referente al enfoque de estudio y de esta manera obtener un resultado cuantificable y de carácter uniforme.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

En la presente investigación se han planteado cinco objetivos de los cuales uno es general y los cuatro restantes son específicos, estos objetivos aportaron para analizar la latencia de la red de datos inalámbrica de la Universidad Politécnica Estatal del Carchi, ayudando a disminuir retrasos en el envío y recepción de paquetes de datos que influyen negativamente en la accesibilidad al contenido web a los estudiantes de la institución.

Se pudo conocer sobre los fallos que presentaba la red, gracias a una entrevista dirigida a los miembros del personal de TIC's, los mismos que son los encargados del monitoreo de la red, paralelamente con la ayuda de una encuesta aplicada a estudiantes de la Universidad se pudo conocer el grado de satisfacción que brinda la red inalámbrica.

El objetivo general es determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN), basándose en la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la accesibilidad al contenido en la web a los estudiantes de la Universidad Politécnica Estatal del Carchi.

Para el cumplimiento de este objetivo general se recopiló información en medios digitales y físicos los mismo que aportaron a determinar agentes que generan latencia. Estos agentes se los detalla en la tabla 5.

Tabla 5. Agentes generadores de latencia

N°	Factores determinantes	Agente
1	Tecnología de conexión a Internet	Medios de transmisión de datos, ondas electromagnéticas.
2	Equipos de red	Equipos obsoletos o desactualizados
3	Distribución de equipos en la red	Alcance y cobertura idónea en la red inalámbrica.
4	Protocolos de navegación	Protocolo HTTP.
5	Capacidad de la red	Límite máximo equipos soportados en la red inalámbrica.

6	Actividades en la red	Visita a páginas web, juegos online, descargas, etc.
7	Ancho de banda	Cantidad de megas contratadas para la Universidad.

Se determinó que los agentes generadores de latencia pueden estar presentes de diferente manera en las redes inalámbricas, por ejemplo: el medio en el cual se transmite los datos, al hablar de conexiones WiFi, se refiriere a la conexión mediante ondas electromagnéticas que se ven afectadas por la infraestructura de la institución y hasta el equipo que las emite. Otro factor influyente son los equipos de red, estos repercuten en la generación de latencia en caso de encontrarse obsoletos o desactualizados, tendiendo a comprometer su funcionalidad.

De igual manera, otro inconveniente que se presentó es la distribución de Access Points sin ninguna norma o estándar que garantice la distancia en la que deben ser implementados, esto genera puntos negros donde no llega la señal de internet.

Las páginas con el protocolo de navegación HTTP son más sensibles a latencia, puesto que no cuenta con un encapsulamiento que asegure la correcta transmisión de los datos.

Se ha identificado que entre menos equipos estén conectados en una red inalámbrica la latencia disminuye, al existir un menor consumo de ancho de banda. Además, la visita a páginas de entretenimiento como redes sociales, deportes, películas online, entre otras afectan en el rendimiento de la red, esto se debe al contenido multimedia que almacenan dichos sitios web, llegando a consumir mayor ancho de banda, saturando la red en la que se despliega toda la información. Por lo tanto, el ancho de banda debe estar acorde al número de equipos a los que se pretende brindar el servicio.

Primer objetivo específico: Fundamentar teóricamente las variables de estudio mediante la recopilación bibliográfica identificando los factores determinantes de riesgo que afectan la disponibilidad de la red.

Para dar cumplimiento al primer objetivo específico se ha recopilado información de medios digitales y físicos, acerca de latencia en redes de datos inalámbricas además de identificar factores que disminuyen la navegación y que afecten a la accesibilidad al contenido web.

Segundo Objetivo específico: Analizar la red de datos inalámbrica (WLAN), examinando la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la navegación a los estudiantes de la UPEC.

Para el cumplimiento de este objetivo se ha solicitado al departamento de TIC's se facilite la documentación concerniente a la infraestructura de la red de datos inalámbrica, en donde se pudo generar un bosquejo de esta, con los datos obtenidos se determinó que la universidad posee 139 equipos de red inalámbrica (ver tabla 6), posteriormente se identificó cuál de estos afectan en el rendimiento de la red y disminuyan la navegación. Ver tabla 6.

Tabla 6. Equipos de red inalámbrica

Equipo	Descripción	Cantidad
Firewall	Router Cisco ASA 5520 Series Adaptative Security Appliance	1
Router Mikrotik	Router Mikrotik RB951Ui-2HnD	1
Switch de Core	Cisco Catalyst 4506-E Switch	1
Controladora	Cisco 5500 Series Wireless Controller	1
Switch 2960	Switch Cisco Catalyst series 2960-X	47
AP	AIR-CAP2702E-A-K9 AIR-LAP1262N-A-K9 AIR-CAP2702E-A-K9 AIR-CAP2702E-A-K9 AIR-CAP2702E-H-K9 AIR-CAP2702E-A-K9 AIR-CAP2702E-E-K9 AIR-LAP1131AG-A-K9 AIR-CAP2702E-A-K9 AIR-LAP1041N-A-K9 AIR-LAP1262N-A-K9	88
Total		139

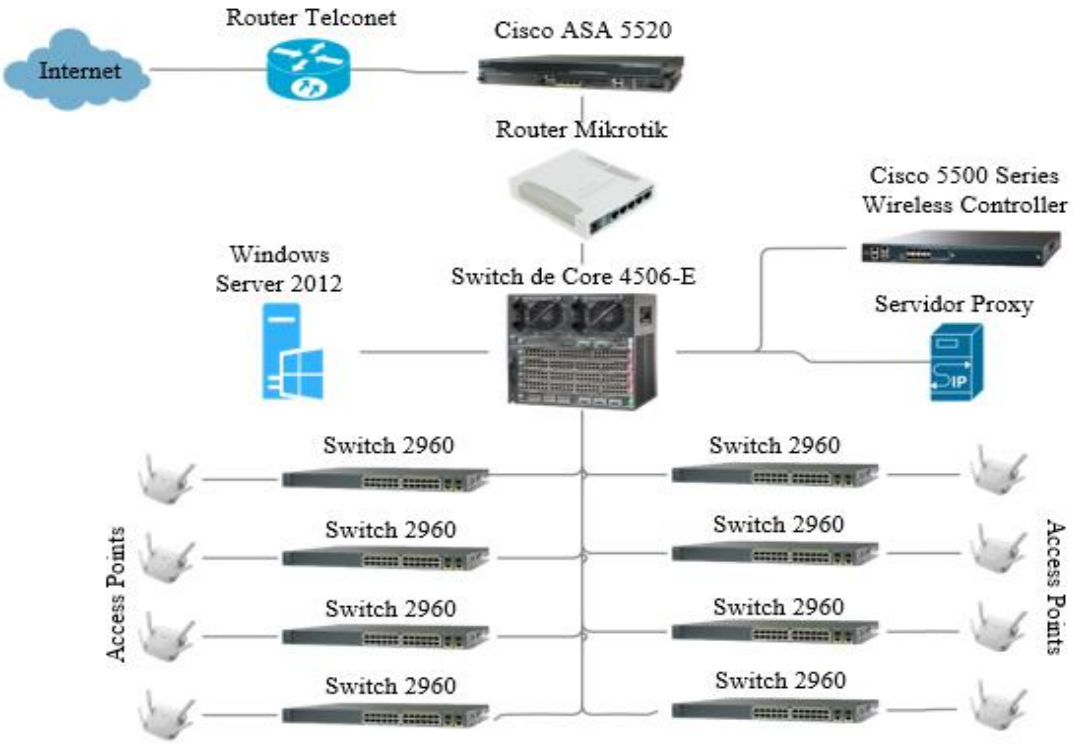


Figura 3. Topología de la red inalámbrica UPEC marzo 2021, elaborada por los autores

Se llegó a establecer que la infraestructura inalámbrica está compuesta por los siguientes equipos: Router Cisco ASA 5520, Router Mikrotik RB951Ui-2HnD, Switch de Core 4506-E, Cisco 5500 Series Wireless Controller, Switch Cisco Catalyst 2960-Plus 24TC-S y Wireless Access Points. En donde se determinó que el Router Cisco ASA 5520 es el más susceptible a presentar fallos, puesto que el ultimo soporte a este equipo se dio el 30 de septiembre del 2018. Este dispositivo en la actualidad está obsoleto y ha llegado al fin de su vida útil, al no contar con soporte del fabricante. El equipo es propenso a presentar fallas de funcionamiento como vulnerabilidades, en donde se vea comprometida la confidencialidad, integridad y disponibilidad de información de la Universidad. Así, en la investigación de Anderson Aza denominada "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3", afirma que la Universidad ha reportado problemas de seguridad pues se ha registrado ataques como la denegación de servicios enfocados principalmente a la página web y portafolio estudiantil de la institución (Aza, 2019). Se determinó que el firewall es propenso a ataques lo que compromete la navegación y accesibilidad al contenido web.

El segundo equipo susceptible a errores es la Wireless LAN Controller Cisco 5508 al dejar de recibir actualizaciones siendo propensa a fallos como la ejecución de código arbitrario,

denegación de servicio y acceso no autorizado. Motivo por el cual Cisco sugiere migrar a un dispositivo actual.

Además de realizar el análisis de la red de datos inalámbrica se complementó con dos instrumentos de recolección de datos. El primero, una entrevista no estructurada dirigida al personal de TIC's, la cual permitió realizar preguntas a partir de una base con la finalidad de ahondar en temas que sean de trascendencia en la investigación, las preguntas que permiten cumplir con este objetivo se las visualiza en la siguiente tabla.

Tabla 7. Preguntas de entrevista objetivo 2

Pregunta	Respuesta
1. ¿El ancho de banda asignado a las diferentes dependencias es uniforme dentro de los edificios de la Universidad?	La red universitaria se encuentra segmentada en VLANs, y a cada una se ha asignado un determinado ancho de banda de acuerdo con las necesidades e importancia del tráfico de información al cruzar por la red. Es diferente la información que genera la VLAN destinada para la parte administrativa que la VLAN destinada para el área financiera.
2. ¿El ancho de banda que tiene la Universidad es el adecuado para el número de usuarios que posee la institución?	Si es el adecuado, pero es necesario la adquisición e implementación de un equipo llamado balanceador de carga, el cual permite que el ancho de banda no utilizado por cada VLAN sea asignado a la VLAN que lo requiera.
3. ¿La cobertura de la red inalámbrica abarca todo el campus universitario?	La institución posee sectores en los cuales los dispositivos que propagan la red no se encuentran presentes tal es caso del coliseo, la plaza roja, áreas verdes entre otros. Para eliminar este inconveniente se tendría que adquirir antenas bidireccionales, pero al ser costosas la institución no puede realizar esta compra.
4. ¿Conoce usted alrededor de cuántos usuarios se conectan simultáneamente a la red inalámbrica de la Universidad?	Dentro de la red WiFi se tiene aproximadamente 1500 dispositivos conectados, este valor no determina cuantos usuarios, debido a que un usuario puede conectarse con varios dispositivos: celular, tablets o laptops a la misma red.
5. ¿Se tiene un número aproximado de usuarios los cuales pueden conectarse simultáneamente a la red y no afecte su rendimiento?	2000 sería el número aproximado de dispositivos conectados a la red para que no afecte en el rendimiento y consumo de ancho de banda del

	internet, pero dentro de la intranet podríamos superar fácilmente los 5000 usuarios sin tener inconvenientes.
8. ¿Ha considerado la restricción de páginas de redes sociales y páginas de videos?	Más que las páginas de redes sociales y videos, es necesario realizar el bloqueo de páginas de contenido inapropiado (Pornográficas, gestores de descargas, streaming de películas y series, entre otras). Mientras que las páginas de redes sociales (Facebook, WhatsApp, Twitter) y de videos (YouTube) se debe controlar el ancho de banda que consumen porque son usados para fines académicos.

De acuerdo con la entrevista realizada a los administradores de la red inalámbrica de la institución, se puede determinar que:

El servicio de internet inalámbrico no es el mismo para las diferentes redes existentes en la Universidad, puesto que la asignación de ancho de banda dependerá de las necesidades que se requiera. El ancho de banda con el cual dispone la Universidad es el adecuado, pero no se cuenta con un balanceador de cargar que permita asignar el ancho de banda de la WLAN que menos utiliza hacia la WLAN que más lo requiera. El número de dispositivos conectados a la red inalámbrica es aproximadamente 1500 dispositivos, cabe considerar que no se puede afirmar que sean los 1500 estudiantes los que se conectan, puesto que un estudiante puede hacer uso de diferentes dispositivos. El número de dispositivos que se pueden conectar simultáneamente a la red para no tener problemas con el servicio es de 2000 usuarios, esto deja ver que si los estudiantes se conectan con más de un dispositivo puede llegar a generar latencia en la red. Se ha considerado el bloqueo de páginas de contenido inapropiado que por una parte son irrelevantes para una institución en donde se va a recibir conocimientos y por otra parte estas mismas páginas son más propensas a generar latencia.

Como segundo instrumento de recolección de información se elaboró una encuesta orientada a un grupo de estudiantes conformado por 252 personas valor definido anteriormente en la muestra, de la encuesta total que se aplicó se ha seleccionado diez ítems, los mismos que aportan al cumplimiento de este objetivo.

Los datos recolectados de los ítems seleccionados se muestran a continuación indicando el respectivo análisis de cada una de ellas.

Tabla 8. Preguntas de encuesta objetivo 2

Pregunta	Opción	Porcentaje
1. ¿Con qué frecuencia usted hace uso del servicio de internet dentro de la Universidad?	Siempre	46,83%
2. ¿Con qué frecuencia usted se conecta a la red inalámbrica WiFi que provee la Universidad? (Si su respuesta es nunca puede dar por terminada la encuesta)	Siempre	37,30%
3. ¿Al estar conectado a la red inalámbrica WiFi cuantos dispositivos utiliza simultáneamente para su navegación?	2 dispositivos	57,94%
4. ¿Al conectarse al internet inalámbrico de la Universidad cuál de los siguientes dispositivos a utilizado? (La respuesta puede ser más de uno)	Celular	86,11%
5. ¿Qué uso le da usted al internet inalámbrico dentro del campus universitario? (La respuesta puede ser más de uno)	Educativo	55,56%
6. ¿Cuándo usted se conecta al WiFi, de la Universidad desde cualquier lugar de las instalaciones su conexión y el tiempo que dura la misma es totalmente satisfactoria?	Rara vez	51,19%
7. ¿Con qué frecuencia usted presenta problemas para conectarse a la red inalámbrica WiFi de la Universidad?	Casi siempre	60,32%
8. ¿Con que frecuencia ha sufrido problemas de conexión, los mismos que han influido negativamente en actividades académicas como pruebas online, consulta de información, entre otras?	Casi siempre	43,65%
9. ¿Cuál es el rango de tiempo que usted invierte en el servicio de internet inalámbrico WiFi de la universidad?	Más de 45 minutos	42,06%
10. ¿Cuán satisfactoria fue la velocidad con la que navegó al utilizar el servicio de internet inalámbrico de la Universidad?	Regular	53,57%

Los resultados indican que el 46,83% de los estudiantes utilizan siempre el servicio de internet dentro de la Universidad, lo que deja en evidencia que un gran porcentaje de los encuestados hacen uso de la red inalámbrica que brinda la Universidad siendo esto un 37,30% que hace uso constante de la red WiFi, de los cuales el 57,94% se conecta en dos dispositivos de manera simultánea generando un doble consumo de ancho de banda y una navegación lenta que impide acceder al contenido web académico para la cual está destinada la red inalámbrica, los dispositivos que frecuentan los estudiantes para el uso de este servicio son celulares con un 86,11% y laptops con un 72,22% lo que confirma que estos dos dispositivos se usan de manera simultánea siendo esto atípico puesto que para el ámbito académico no se necesita más de un

dispositivo, la pregunta numero 5 da a conocer que el 55,56% de los estudiantes utilizan el WiFi de la institución para lo académico y el 49,60% para el entretenimiento siendo esto un factor generador de latencia considerando que estas páginas tienen un consumo de ancho de banda mayor a las páginas de origen académico. Para terminar de afirmar lo anterior se dice que el 42,06% de los estudiantes utiliza el internet por más de 45 minutos siendo algo no tan normal debido a que el uso de internet en las clases no conlleva tanto tiempo, dando a entender que se le da otro uso diferente al académico.

El 51,19% de los estudiantes afirman que rara vez tiene una conexión satisfactoria cuando se encuentran haciendo uso de la red WiFi de la Universidad, esto tiene diferentes causas como la estructura de la Universidad porque al tratarse de una consistencia robusta reduce el alcance de las ondas electromagnéticas emitidas por el WiFi, además de la distribución de los Access Points que en la institución fueron colocados mediante la practica site survey que tiene el riesgo de dejar lugares sin cobertura de la red.

El 60,32% de los estudiantes casi siempre ha presenta problemas para conectarse a la red inalámbrica, lo que impide que puedan acceder a contenido académico en internet, siendo esto un problema de mayor magnitud dando entender que el 43,65% de los estudiantes casi siempre presentan estos inconvenientes, impidiendo realizar actividades fundamentales para lo cual fue creada la red.

El grado de satisfacción de la velocidad del internet inalámbrico según los estudiantes de la Universidad es regular en un 53,57% debido a los problemas detallados anteriormente que impiden acceder al contenido web en internet, pero además trae un análisis más profundo debido a que el origen de los inconvenientes lo generan los mismos estudiantes con sus acciones las mismas que puede llegar a producir fallos en la red inalámbrica, provocando un déficit en la calidad del servicio.

Tercer Objetivo Específico: Elegir una solución informática mediante la comparativa de portales cautivos ayudando a la disminución de latencia, mejorando la accesibilidad al contenido web en la institución.

Para la ejecución del tercer objetivo específico se recopiló información en medios digitales y físicos con la finalidad de indagar e identificar portales cautivos de software libre que se adapten a las necesidades y requerimientos de la institución.

Se ha desarrollado la comparativa con la ayuda de dos tablas, la primera mencionará los criterios de selección y la segunda tabla requerimientos del software. Una vez culminada esta fase se procede a realizar la sumatoria de cada criterio para determinar el valor total y conocer el portal cautivo que cumpla con los requisitos que la institución necesita, dando paso al siguiente objetivo específico. La evaluación para esta tabla está basada en una escala del 1 al 5, donde 1 es el valor más bajo y 5 el más alto.

Tabla 9. Criterios de selección de portal cautivo

Portal cautivo	**Antamedia HotSpot**	**Chillispot**	**Wifidog**	**ZeroShell**	**MonOwall**	**OPNsense**	**Pfsense**
Documentación	2	3	2	3	4	5	5
Comunidad	3	1	1	3	3	4	5
Simplicidad y modularidad del software	3	2	2	3	3	4	5
Distribución Software libre	5	5	5	5	5	5	5
Facilidad de instalación	5	3	3	3	3	3	3
Seguridad	5	3	3	5	5	5	5
Total	23	17	16	22	23	26	28

Tabla 10. Características de portales cautivos analizados

Portal cautivo	**Antamedia HotSpot**	**Chillispot**	**Wifidog**	**Zeroshell**	**MonOwall**	**OPN sense**	**Pfsense**
Plataforma	Windows 7,8,10	Linux Debian	Linux	Linux	Freebsd	Freebsd	Freebsd
Última actualización	2019	2006	2009	2016	2015	2019	2020
Interfaz web de administrador	✓	✓	✓	✓	✓	✓	✓
Editor de interfaz de usuario	✓		✓	✓	✓	✓	✓
Soporte actualizado	✓					✓	✓
Panel configurable	✓			✓	✓	✓	✓
NAT	✓	✓	✓	✓	✓	✓	✓
Comunidad activa						✓	✓

Portal Cautivo	✓	✓	✓	✓	✓	✓	✓
Servidor DNS	✓		✓	✓	✓	✓	✓
Servidor DHCP	✓	✓	✓	✓	✓	✓	✓
Servidor PROXY	✓		✓	✓	✓	✓	✓
Servidor LDAP				✓	✓	✓	✓
Servidor RADIUS	✓	✓		✓	✓	✓	✓
Compatibilidad Ip v4/Ip v6	✓				✓	✓	✓
Monitoreo de la red	✓		✓		✓	✓	✓
Escalabilidad	✓			✓	✓	✓	✓
Protocolo Https	✓	✓			✓	✓	✓
VLAN					✓	✓	✓
VPN				✓	✓	✓	✓
Sistema IPS/IDS							✓
Total	14	6	8	12	16	18	19

Después de realizar la comparación de criterios y características de cada portal cautivo se constató que Pfsense obtuvo la mayor puntación, con un total de 28 puntos respecto a los criterios de selección, en la segunda tabla se alcanzó un total de 19 puntos con respecto a los requerimientos de software que la red de la institución demanda. No obstante, se pudo visualizar la alternativa que más se acerca es OPNsense teniendo características similares, vale aclarar que uno de los principales motivos por los cuales se ha seleccionado a este software es por su extensa documentación acompañada de una comunidad de soporte netamente activa generando un plus de valía ante posibles fallos que se generen en la implementación, cabe mencionar que Pfsense cuenta con extensos componentes que pueden permitir a dicho Firewall tener una escalabilidad logrando así adaptarse a nuevos cambios en la red, claro eso si se realiza las respectivas configuraciones que amerite el sistema.

Se tomó Pfsense como portal cautivo debido a que se ajustaba a los requerimientos de la institución, además de acoplarse a las necesidades del presente proyecto. La principal ventaja de esta herramienta es que viene preconfigurada, lo cual reflejó un ahorro de tiempo significativo, a la vez de presentar módulos ya instalados como lo son el servidor DHCP, DNS, PROXY, NTP, PPPoE, VPN, AAA, entre otros. Adicionalmente el portal cautivo estaba

acompañado de características como una interfaz web para el administrador, permitiendo gestionar de manera más sencilla, eficaz e intuitiva.

Otra ventaja del Firewall es poseer servicios y módulos que se utilizan para mejorar su rendimiento como son el Squid proxy y SquidGuard, los mismos que permiten al administrador filtrar contenido y bloquear páginas web que no sean de relevancia académica, junto a estas se instala ClamAV, un antivirus el mismo que permite bloquear páginas web maliciosas. Otro servicio esencial del proyecto es el servidor RADIUS, con la ayuda de este se realizó la conexión con el Active Directory que la Universidad posee, donde se almacenan las credenciales y contraseñas de los usuarios que pertenecen a la institución, además de contar con certificados SSL/TLS propios de freeradius. Algo esencial de este software es que permite realizar backup de todas las configuraciones realizadas, además de respaldar los módulos instalados. Pfsense posee una consola Shell que acepta comandos generalmente utilizados en Linux.

PHP es el principal lenguaje de programación que utiliza este software, logrando así facilitar el entendimiento del código fuente para cualquier persona que este familiarizada con desarrollo back-end.

Finalmente, la instalación de Pfsense no se torna compleja al poseer manuales que indican paso a paso cómo realizarlo, en caso de presentarse algún inconveniente se puede obtener respuesta ingresando a los foros de la comunidad NetGate, el foro de Pfsense cuenta con soporte internacional en 14 idiomas siendo el de ingles el más concurridos por los usuarios al presentar el mayor número de post publicados.

Cuarto Objetivo Específico: Implementar un portal cautivo mediante la utilización de herramientas tecnológicas de software libre, mitigando la latencia en la red de datos y mejorando su navegación.

Se logró cumplir con este objetivo analizando el portal cautivo que mejor se adapte a la institución e infraestructura, además de utilizar los dispositivos de red con los que cuenta la Universidad actualmente. A continuación, la tabla 11 detalla la aceptación que tendría el implementar la herramienta tecnológica en la institución.

Los ítems de la encuesta se los muestra a continuación, indicando el respectivo análisis de cada uno de ellos.

Tabla 11. Preguntas de encuesta objetivo 4

Pregunta	Opción	Porcentaje
11. ¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico?	Regular	51,19%
12. ¿Estaría de acuerdo con la implementación de una herramienta tecnológica que permita mejorar la accesibilidad al contenido web dentro de la red inalámbrica de la Universidad?	Totalmente de acuerdo	68,25%

Los resultados de la encuesta indican que el 51,19% de los estudiantes consideran regular el servicio de internet inalámbrico de la Universidad, dejando notar que este posee fallas en la conexión, generando descontento a los estudiantes, los mismos que están totalmente de acuerdo en un 68,25% para que se implemente una herramienta informática que permita mejorar la accesibilidad al contenido web dentro de la red inalámbrica de la institución.

Además, para complementar este objetivo se realizó preguntas al encargado de TIC's, las mismas que se muestran en la siguiente tabla.

Tabla 12. Preguntas de entrevista objetivo 4

Pregunta	Respuesta
6. ¿La institución posee algún software o hardware que controle el número de dispositivos que un usuario puede tener conectado simultáneamente a la red inalámbrica?	Dentro de la red institucional no poseemos ningún equipo que permita controlar el número de dispositivos a conectarse por cada usuario.
7. ¿La Universidad está regulando las páginas web a las cuales los usuarios tienen acceso?	En este momento no tenemos un equipo que permita realizar el control y bloqueo del acceso a los sitios web, es decir dentro de la red universitaria se puede acceder a páginas web referentes a cualquier información.
9. ¿Se han generado sugerencias sobre el mejoramiento a la red?	Claro que sí, se han sugerido muchos cambios los cuales poco a poco se han ido implementando para el mejoramiento de la red en todo sentido, velocidad, seguridad, distribución, segmentación. Pero al ser una institución pública que usa recursos del estado, tenemos grandes inconvenientes en la adquisición de este equipamiento por falta de recursos económicos.
10. ¿Qué opina usted de implementar un software open source que ayude en la administración de la red?	Me parece que la implementación de este software es indispensable porque permitirá tener una mejor administración y control en los segmentos de red, permitiendo bloquear contenidos y páginas web que no son de uso académico.

De acuerdo con la entrevista realizada a los administradores de la red inalámbrica de la institución, se puede determinar que:

La institución no cuenta una herramienta que controle el número de dispositivos conectados por cada usuario, generando que los usuarios se conecten con más de un dispositivo y con ello consuman el doble de ancho de banda por cada uno. La red de la Universidad en general no bloquea ninguna página, lo que causa que estudiantes accedan a páginas referentes a cualquier información como streams o descargas. El servicio de red inalámbrica ha sido blanco de sugerencias en sentidos como velocidad, seguridad, distribución, segmentación, etc. La implementación de un portal cautivo es considerado importante para la Universidad, puesto que, permite mejor la administración y control en los segmentos de red, permitiendo bloquear contenidos y páginas web que no son de uso académico.

- **Cumplimiento de indicadores**

A continuación, se detalla cada uno de los indicadores identificados en la operacionalización de variables, describiendo los resultados y la ubicación de estos en el presente trabajo de investigación, ver tabla 13.

Tabla 13. Cumplimiento de indicadores

Indicadores	**Descripción del indicador**	**Resultados**	**Ubicación**
Porcentaje de fallos en la conexión a internet.	Indica las conexiones que no se lograron concretar en la red	43.65%	Anexo 6 Figura 63
Número de equipos totales en la infraestructura	Indica los equipos que la infraestructura posee	139 equipos	Tabla 4
Número de dispositivos inalámbricos conectados simultáneamente a la red	Dispositivo que lograron acceder correctamente al portal cautivo	2 equipos	Figura 50
Cantidad de megas distribuidas en la red	Indica el valor asignado a la red	600 Mbps	Anexo 8 Figura 72
Cantidad de paquetes transmitidos	Indica la cantidad de paquetes que entraron y	Paquetes de entrada: 4140648 Paquetes de salida:	Figura 45

	salieron de la red inalámbrica	3790526	
Estado de la infraestructura de la red	Estado actual de la red y equipos que esta posee.	2 equipos Obsoletos	Resultados: Objetico especifico dos
Grado de satisfacción de la red inalámbrica	Satisfacción hacia el servicio que brindaba la institución en la red inalámbrica.	53.57 %	Anexo 6 - Pregunta 10
Escala de utilización de la red inalámbrica	Muestra uso constante del internet inalámbrico de la Universidad	37,30 %	Anexo 6 – Pregunta 2
Eficiencia en las conexiones a la red inalámbrica	Indica los problemas constantes de conexión de la red inalámbrica	43,65%	Anexo 6- Pregunta 8
Tipos de dispositivos que se utiliza en la red inalámbrica	Indica los dispositivos inalámbricos utilizados con mayor frecuencia en la red WiFi.	Celulares 51,42 % Laptop 43,13 %	Anexo 6 – Pregunta 4
Megas utilizadas en la red de datos inalámbrica	Indica el valor asignado a la red inalámbrica	300 Mbps	Anexo 8 Figura 72
Distribución de megas en cada red inalámbrica	Indica el valor asignado en Mbps en cada red.		Anexo 8 - Figura 72
Cobertura de la red	Hace referencia a los puntos negros en la red inalámbrica.	Coliseo Piletas centrales Plaza Roja	Entrevista

4.1.1 Metodología Informática

La metodología PPDIOO de Cisco es fundamentar para el cumplimiento de ciclos en donde los principales beneficios son disminuir el costo de administración de la red, dándole además mejoras en la agilidad a la red. Así, una planificación que contenga una estructura es fundamental dentro de una empresa o institución que trabaja en base a lograr objetivos, la

metodología PPDIOO ayuda a cumplir esto en base a sus seis fases: Preparar (Prepare), en esta fase se determina los requerimientos que desea el establecimiento para posteriormente poder proponer una estrategia tecnológica de alto nivel. Planificar (Plan), en esta fase se identifica los requerimientos, pero en este caso de la red; teniendo en cuenta las necesidades y realizando análisis controlados como Ingeniería de Tráfico focalizado en el ambiente operacional. Diseñar (Design), esta fase del diseño de la red consta de los requerimientos obtenidos de las fases anteriores, el diseño debe estar orientado en brindar disponibilidad, confiabilidad, seguridad, escalabilidad y desempeño a la red. Implementar (Implement), en esta fase se da la instalación y configuración de los equipos para implementar el diseño. Operar (Operate), en esta fase se brindará operaciones diarias a la red porque al ponerse en marcha el diseño se puede tener anomalías o errores, algunas fases operaciones que se realizan son las siguientes: monitoreo y manejo remoto de los dispositivos y componentes de la red, mantenimiento de las políticas de enrutamiento y seguridad, manejo sistematizado de actualizaciones, identificar y corregir fallas de red. Optimizar (Optimize), en esta fase se debe realizar una administración proactiva; para de esta manera resolver errores que afecten el funcionamiento de la red (3ciencias, 2015). Esta metodología de proyecto es útil tanto para el diseñador como para el dueño del establecimiento, brinda asesoramiento y orden para lograr un proyecto.

4.1.2. Elaboración del sistema

Para el presente estudio se ha determinado la utilización de la metodología de proyecto PPDIOO, se contempló las cuatro primeras fases: preparar, planificar, diseñar e implementar. Debido a que se ha mirado oportuno el diseño, simulación e implementación de un prototipo basado en los requerimientos de la red. Esta metodología tiene como finalidad satisfacer las necesidades de la institución con ayuda de un portal cautivo que mitigue la latencia y mejore la accesibilidad al contenido web de la comunidad universitaria, adicionando a esto un mejor control en cuanto a parámetros de administración y seguridad se refiere. A continuación, se describe las fases de rediseño y simulación de la administración de la red inalámbrica.

Tabla 14. Metodología de proyecto PPDIOO

Fase	Objetivo	Función	Metodología
Análisis de la red inalámbrica actual	Analizar la infraestructura de la red de datos inalámbrica. Análisis de software	Determinar falencias en la red de datos inalámbrica Pruebas de ancho de banda actual software por implementar	Investigación-Acción/ Descriptiva

Propuesta de diseño	Plantear un diseño que mejore el servicio de la red de datos inalámbrica	Obtener el diseño de la red de datos inalámbrica anterior Diseño que mejore el servicio de la red de datos inalámbrica	Descriptivo
Implementación de proyecto	Instalación, configuración de las herramientas de software libre	Instalación y Configuración de Módulos.	Investigación-Acción/ Campo
Pruebas y mejoras	Realizar la verificación y ajustes pertinentes para mejorar el rendimiento de la red de datos inalámbrica	Ingreso a la red de datos inalámbrica Administrar ingreso de usuarios Bloquear páginas innecesarias	Investigación-Acción /Campo
Documentación	Manual de configuración herramientas tecnológicas	Desarrollar un manual técnico basado en las configuraciones planteadas	Descriptivo

Fase 1.- Análisis de la red inalámbrica actual

Falencias en la red de datos inalámbrica

Se realizó el análisis de la red inalámbrica actual, aquí se identificó los equipos con los cuales la institución contaba, determinando que el Cisco ASA 5520 Series Adaptative Security debe ser innovado, al estar actualmente obsoleto pasando a un estado de vida útil finalizada. Este equipo no recibe soporte por parte su fabricante, por otra parte, se determinó que no posee el servicio de seguridad web, ni el servicio de control y visibilidad de aplicaciones. Motivo por el cual hay un libre acceso a página de todo tipo siendo este otro factor que afectaría al rendimiento de la red.

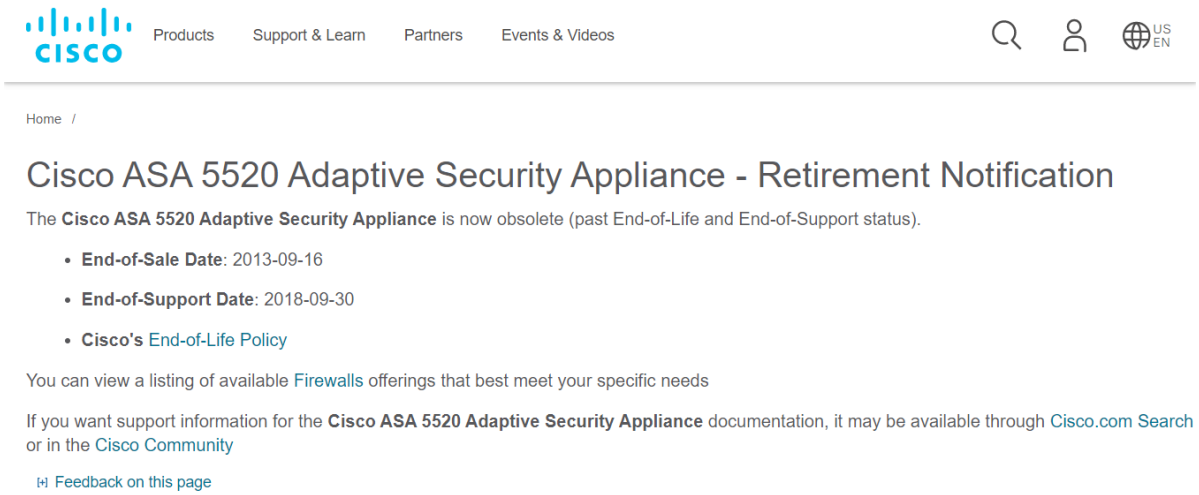


Figura 4. Estado actual del equipo Cisco ASA 5520

Fuente*:* https://www.cisco.com/c/es_mx/support/security/asa-5520-adaptive-security-appliance/model.html

A continuación, se detallará en la tabla 15 las características que el equipo Cisco ASA 5520 no posee con relación a su similar el Cisco ASA 5525-X

Tabla 15. Comparativa Cisco ASA 5520 vs Cisco ASA 5525-X

Característica	**Dispositivo de seguridad adaptable Cisco ASA 5520**	**Dispositivo de seguridad adaptable Cisco ASA 5525-X**
Cortafuegos de próxima generación	No	Sí
Servicio de control y visibilidad de aplicaciones	No	Sí
Servicio de seguridad web	No	Sí
Servicio IPS	Sí (requiere un módulo de hardware separado)	Sí (no requiere un módulo de hardware separado)
Módulo de tarjeta de seguridad de contenido	Sí	Funcionalidad similar disponible a través de Cloud Web Security (anteriormente conocido como ScanSafe)
Rendimiento del cortafuegos (máx.)	450 Mbps	2 Gbps
Rendimiento IPS (máx.)	450 Mbps	600 Mbps
Rendimiento de VPN (máx.)	225 Mbps	300 Mbps
Conexiones (máx.)	280.000	500000
Conexiones por segundo	12000	20000
E/S integradas	4 GE Cobre + 1 FE	8 GE Cobre
E/S de expansión	GE Cu de 4 puertos o GE SFP de 4 puertos	Ge Copper de 6 puertos o GE SFP de 6 puertos
UPC	Núcleo simple	Varios núcleos
Memoria	2 GB	8 GB
Hardware de acelerador IPS	No. Todas las firmas se ejecutan en la CPU del módulo de seguridad IPS	Acelerador de hardware incorporado para firmas predeterminadas y personalizadas

Soporte de hardware para certificados de 2048 bits	No	Sí

***Fuente*:** Recuperado de: http://ciscofirewalls.weebly.com/asa-5550-vs-asa-5555-x-asa-5520-vs-asa-5525-x-asa-5510-vs-asa-5515-x.html

Otro equipo que requiere prestar atención en la infraestructura inalámbrica es la Wireless LAN Controller Cisco 5508, equipo que se encuentra fuera del mercado dejando de recibir actualizaciones y cuyo soporte se tiene previsto hasta el 31 de julio del 2023. El equipo 5508 tiene la capacidad de centralizar hasta 500 Access Points, sin embargo, Cisco sugiere actualizar el equipo anterior por la Cisco WLC 5520, la misma que posee un mejor rendimiento en cuanto al servicio y funcionalidades para la red, se mostrará en la figura 5 y tabla 16 lo mencionado anteriormente.

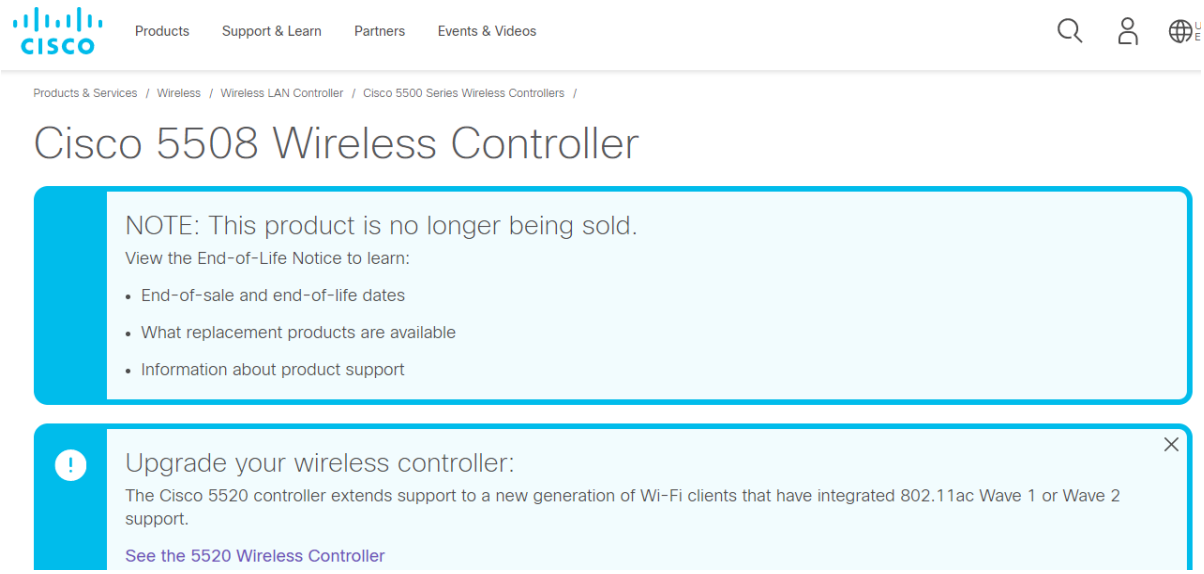


***Figura* 5.** Estado actual del equipo Cisco 5508 Wireless Controller
Fuente: https://www.cisco.com/c/en/us/products/wireless/5508-wireless-controller/index.html

- **Cisco Wireless Controller 5508 vs 5520**

Tabla 16. Cisco Wireless Controller 5508 vs 5520

Parámetro	WLC 5508	WLC 5520
Access Points soportados	500	1500
Clientes soportados	7000	20000
Etiquetas RF soportadas	5000	25000
Rendimiento	8 Gbps	20 Gbps
Grupos de Access Point	500	1500
Grupos de FlexConnect	100	1500
Máximo de Access Point por grupo	25	100
VLAN’s soportadas	512	4094
Interfaces 10G	No soportado	Soportado
De no 10 G interfaces	0	2
Poder máximo de consumo	125 W	190 W
Autenticación de usuario por segundo	235 usuarios	764 usuarios

Fuente: Recuperado de: https://ipwithease.com/cisco-wlc-5508-vs-5520/

- **Pruebas de ancho de banda actual**

Se realizó pruebas para conocer el ancho de banda aproximado que la red de datos inalámbrica poseía mediante la herramienta online SPEEDTEST, donde se determinó que la red actualmente posee 8.30 Mbps de descarga y 15.90 Mbps de carga generando un ping de 8ms, hay que considerar que el valor puede variar puesto que la institución posee el equipo Router Mikrotik RB951Ui-2HnD, el mismo que se encarga de segmentar el ancho de banda dependiendo de las necesidades que cada subred requiera, ver figura 6.

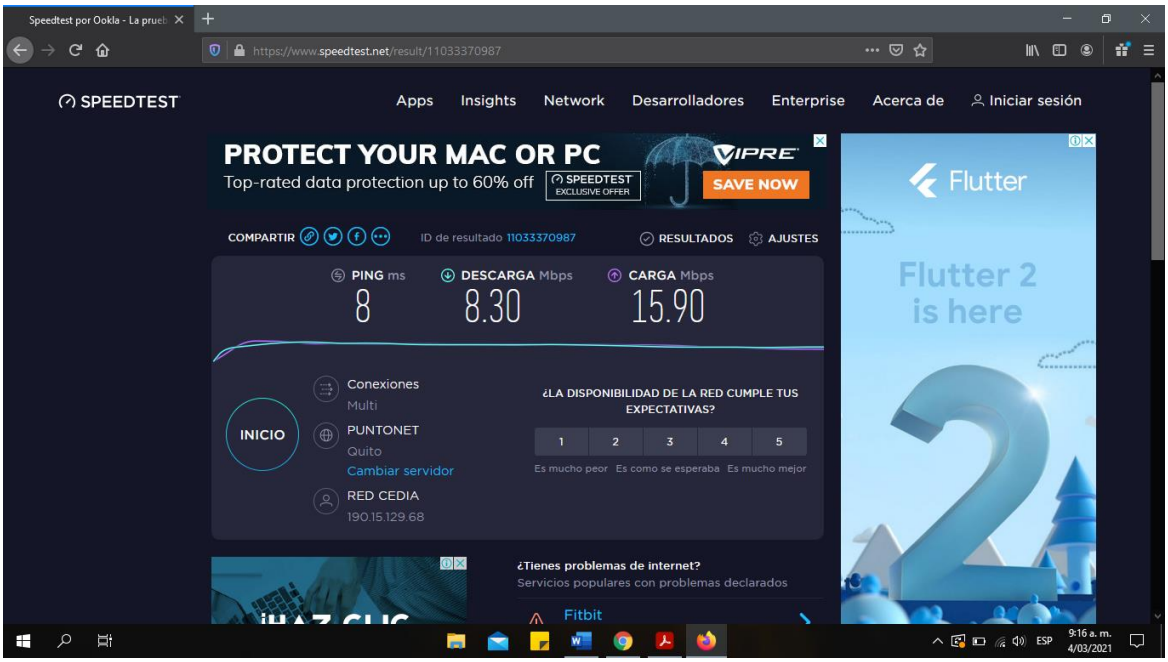


Figura 6. Pruebas de ancho de banda actual en la UPEC, marzo 2021

Realizando este estudio se planteó generar una mayor prioridad de ancho de banda al servicio relacionado con actividades académicas, logrando disminuir paquetes innecesarios obteniendo como resultado un acceso a internet sin inconvenientes.

- **Análisis de software**

  - **Software por implementar**

Para el desarrollo de esta fase se ha tomado como referencia los datos obtenidos en las tablas 9 y 10, donde se realizó una comparativa de software llegando a determinar que la herramienta Pfsense es la más idónea al obtener la puntación más alta. Pfsense pasará a ser implementado al cumplir con los criterios y características que la institución demandaba.

Figura 7. Firewall Pfsense

Pfsense al ser de software libre no genera ningún costo de ahí la factibilidad de la implementación, cuenta con una extensa documentación acompañada de una comunidad netamente activa en la que generan debates sobre la herramienta, ayudando a dar soluciones ante errores en su instalación, la comunidad NetGate es la que brinda soporte internacional en catorce idiomas siendo el inglés el más concurrido por los usuarios.

El software de Pfsense puede ser instalado en ordenadores que para algunos usuarios son obsoletos, no necesita grandes recursos se puede instalar en máquinas que cumplan con estas características: 256 Mb de RAM, 500mhz de CPU, 1 Gb de almacenamiento y dos tarjetas de red. Estos valores pueden variar dependiendo de la empresa o institución donde se pretenda implementar, la instalación es muy similar a las herramientas de FreeBSD. La principal ventaja de este software son las extensas funcionalidades y módulos predefinidos como lo son:

Tabla 17. Funcionalidades de Pfsense

N°	Funcionalidades de Pfsense
1.	Interfaz web para el administrador
2.	Monitoreo de la red mediante gráficos y logs
3.	Servidor DHCP
4.	Servidor DNS
5.	Servidor PROXY
6.	Servidor NTP
7.	Servidor PPPoE
8.	VPN
9.	VLAN
10.	Portal cautivo
11.	Firewall

Esta herramienta cuenta con un gestor de paquetes, el mismo que da la opción de ampliar las funcionalidades, existen alrededor de 70 módulos que están disponibles entre ellos se encuentran Squid, SquidGuard, Suricata, ClamAV, entre otros más.

- **Fase 2.- Propuesta de diseño**

    - **Diseño de la red inalámbrica de datos anterior**

Para el desarrollo de esta fase se ha tomado como punto de partida analizar la infraestructura de la red de datos inalámbrica que la institución posee actualmente. Los equipos que conforman la infraestructura se los puede visualizar en el siguiente diagrama.

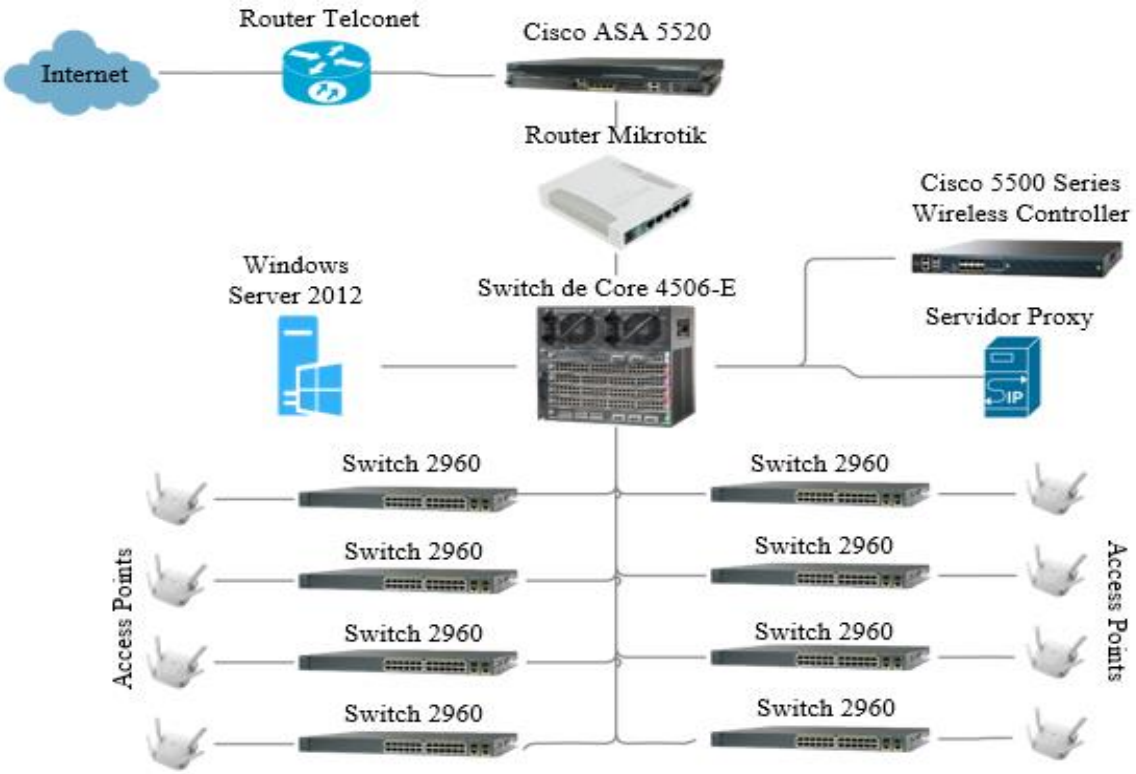


***Figura* 8.** Topología de la red inalámbrica UPEC marzo 2021, elaborada por los autores

La red inalámbrica cuenta con dispositivos que van desde Firewall hasta Access Points, se pretende realizar cambios en su infraestructura agregando la herramienta tecnológica Pfsense que se encargue de generar un portal cautivo, el mismo que ayudará a disminuir factores generadores de latencia.

    - **Diseño que mejore el servicio de la red de datos inalámbrica**

Con la implementación de Pfsense se mitigo la latencia en la red de datos, mejorando la navegación y la accesibilidad al contenido web que la comunidad universitaria requiere. A continuación, se mostrará en la figura 9 el nuevo diseño que la infraestructura de la Universidad Politécnica Estatal del Carchi tendrá.

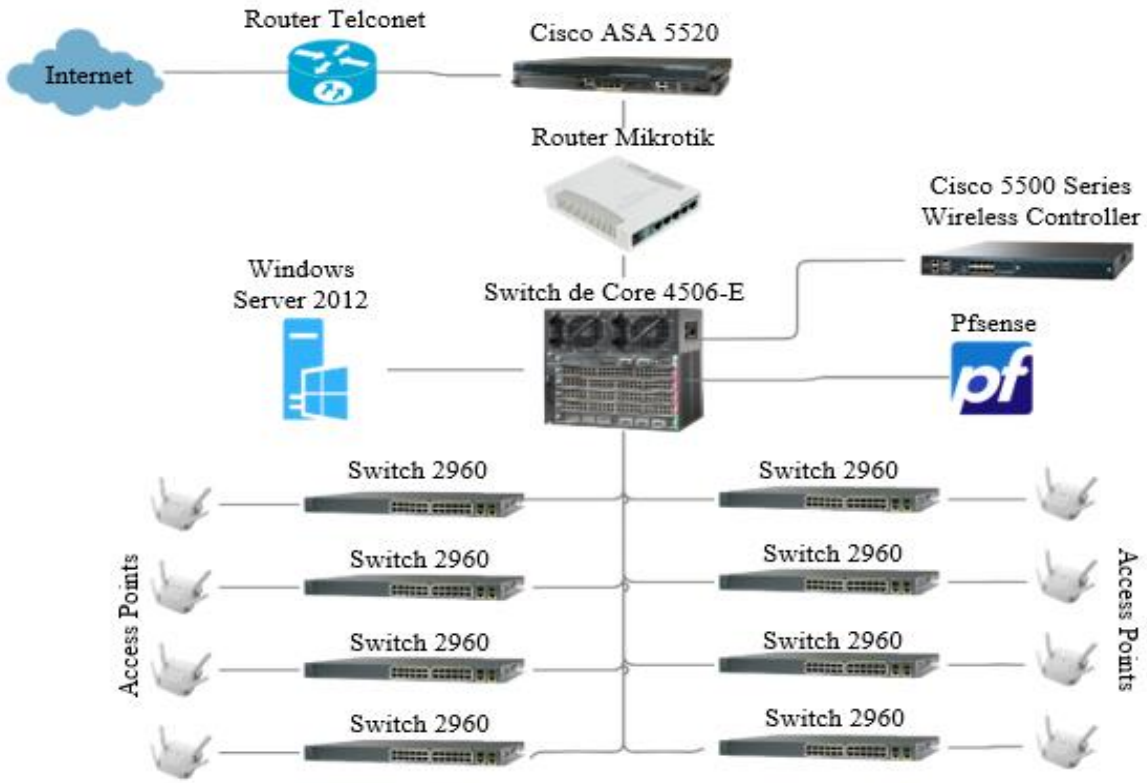


Figura 9. Topología red inalámbrica de la UPEC con Pfsense, elaborada por los autores

Para la implementación se necesitó generar cambios en cuanto a infraestructura, sustituyendo el servidor proxy de la infraestructura antigua, la herramienta Pfsense 2.4.5 Realese no alterará el correcto funcionamiento de esta, puesto que el software asumirá varios roles adicionales en la red inalámbrica de la institución para ello se configuró módulos y servicios que son necesarios. Se determinó que la instalación de esta herramienta agregará un plus a la institución al permitir vigilar de manera constante la red.

- **Fase 3: Implementación del proyecto**

Para la implementación del software Pfsense se ha visto necesario reutilizar los equipos que la institución poseía en bodega, con la finalidad de no incurrir en gastos adicionales tomando en cuenta las recomendaciones que la comunidad NetGate sugiere para su implementación. Las características se muestran en la tabla 18.

Tabla 18. Requerimientos de Pfsense

Equipo	Característica	Cantidad
Disco Duro	500 Gb	1
Memoria RAM	4 Gb	2
Procesador	Intel(R) Core (TM) i7-8700 CPU @ 3.20GHz	1

Placa Base	GYGABYTE Z370 HD3	1
Monitor	Senseye LED 24 pulgadas	1
Teclado	Genius GK-07	1
Tarjetas de Red	Placa base ENEGA-1320	2

Previo a la implementación del software en el equipo físico, se necesitó crear una VLAN destinada únicamente para Pfsense, esta VLAN se configuró en el Switch de Core Cisco ASA 5520. Hay que mencionar que tras esta configuración se encuentran algunos procedimientos adicionales realizados por el personal de TIC´s.

Una vez configurado la VLAN, se procederá a configurar el SSID en el Wireless Controller, para ello inicialmente se creará una nueva interfaz asignándole un nombre y el ID VLAN, dicha interfaz adoptará la configuración mostrada en la figura 10.

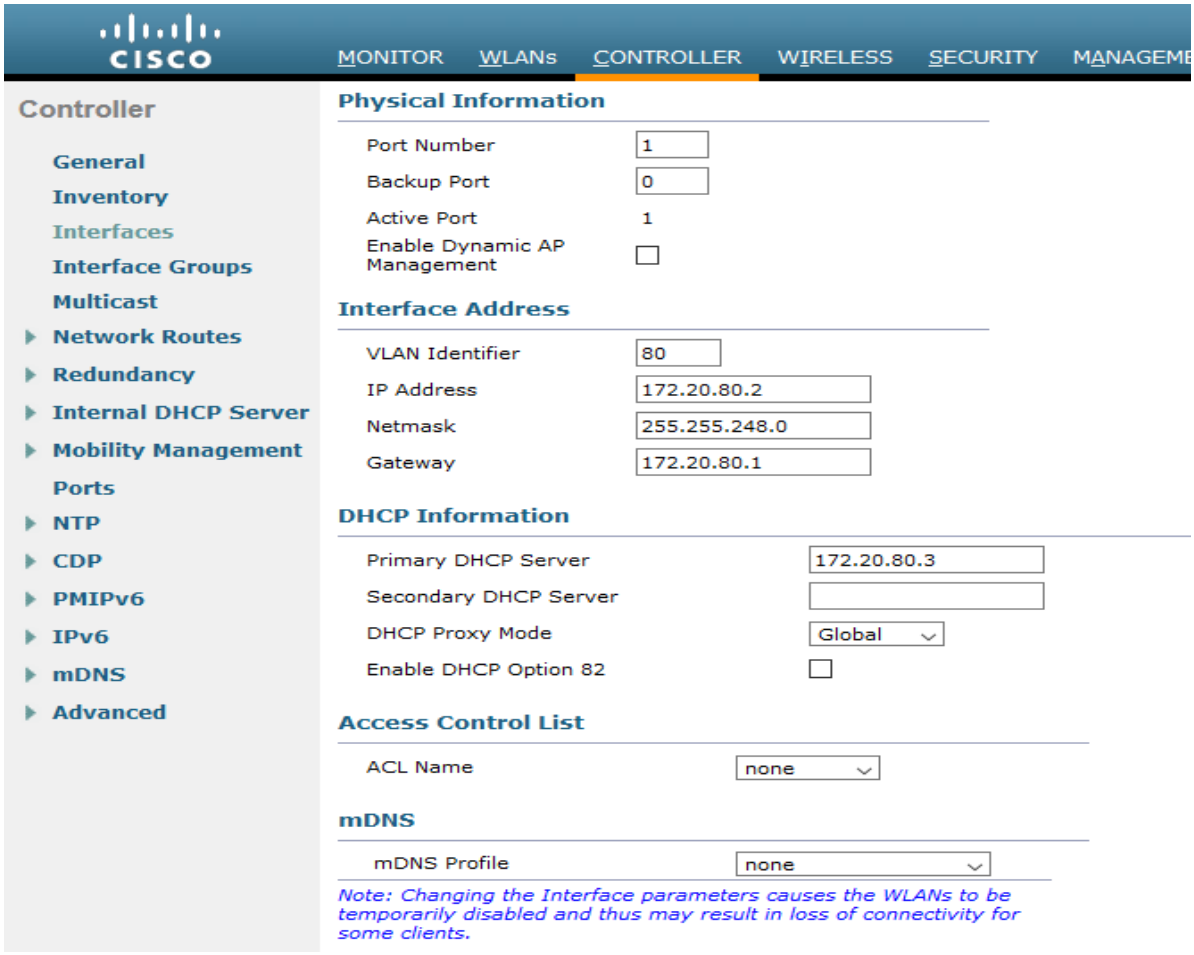


Figura 10. Configuración del SSID en la Wireless Lan Controller de la UPEC

El siguiente paso a realizar es configurar una nueva WLAN, se lo consigue en la ruta WLANS / new, a continuación, en la ventana WLAN/ General se escogerá la interfaz que se configuró previamente.

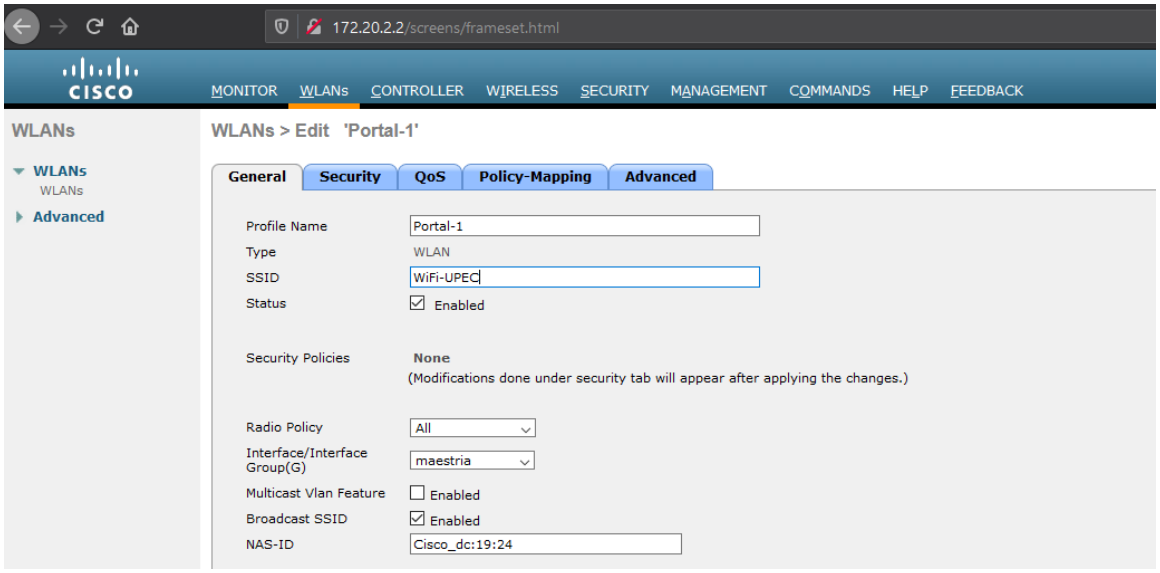


Figura 11. Configuración de nueva WLAN en la Wireless Lan Controller de la UPEC

Se verificará la WLAN creada.

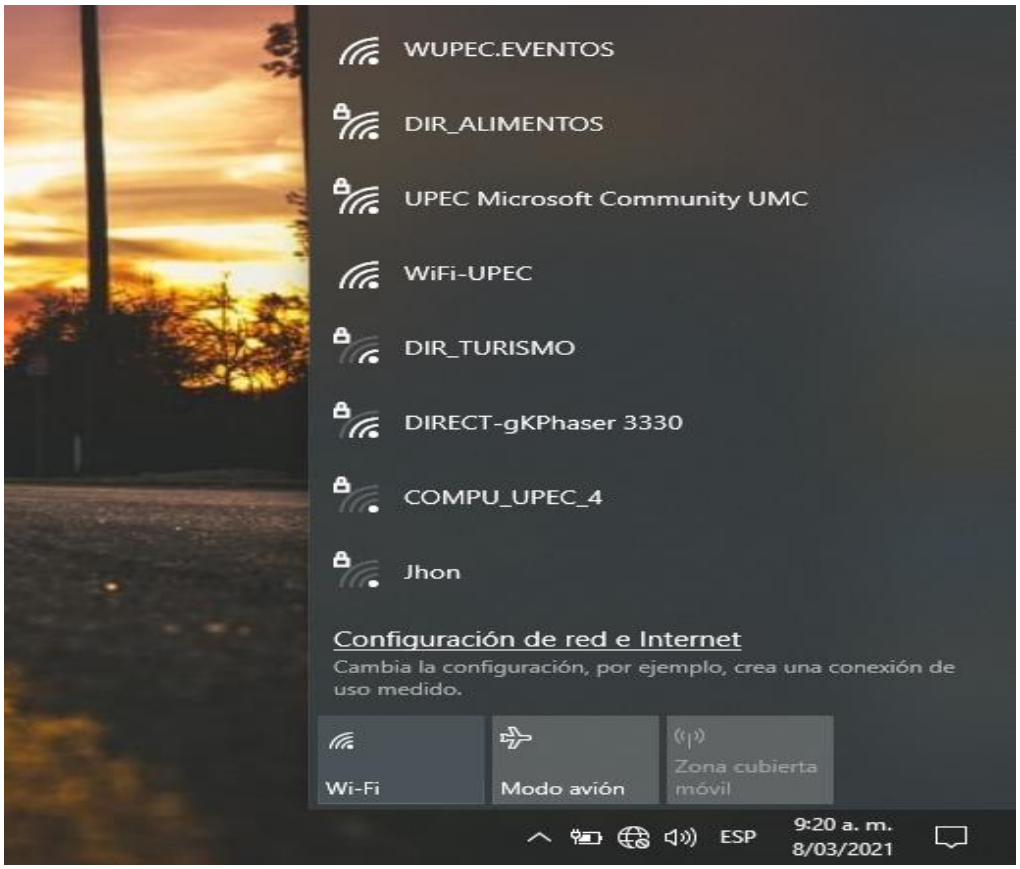


Figura 12. Verificación de WLAN creada

Una vez creada y configurada correctamente la WLAN se procederá a la instalación de Pfsense, la misma que posteriormente se enlazará con estos dos equipos teniendo la finalidad de mostrar el portal cautivo en la red inalámbrica de la institución.

- **Implementación Pfsense**

Para iniciar con la instalación de Pfsense se debe copiar la imagen ISO en un CD o USB booteable, luego se configura el arranque del equipo para que inicie desde la unidad creada. Una vez reconocida la USB de instalación se mostrará la siguiente pestaña.

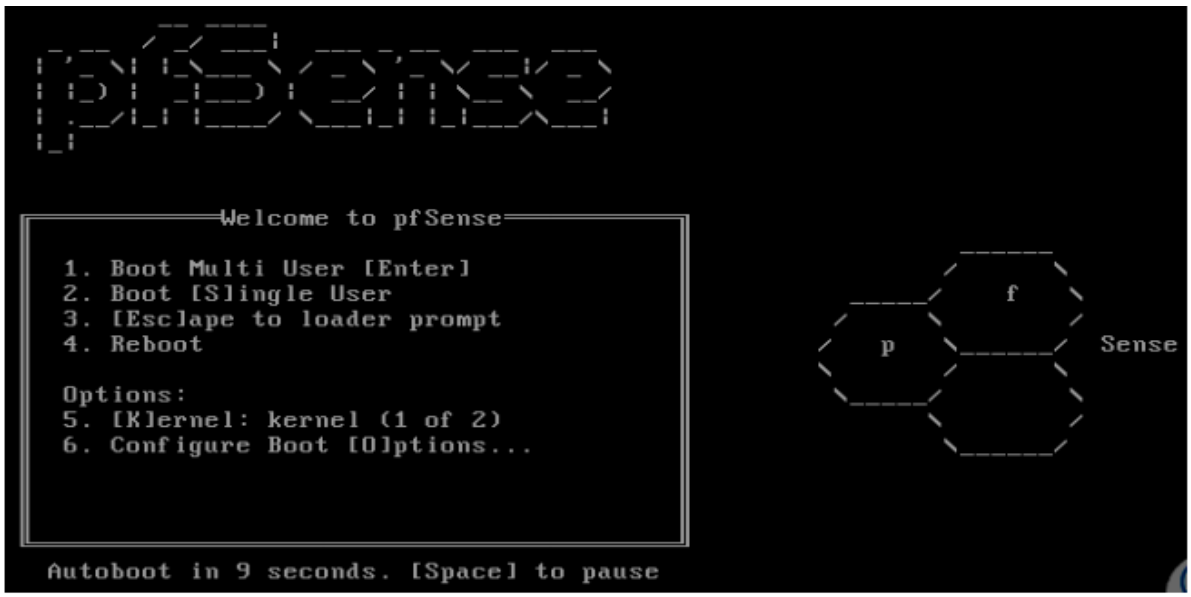


Figura 13. Arranque de instalación de Pfsense

Para iniciar el proceso de escritura en el disco se elige la opción 1. Terminada esta instalación se visualizará la siguiente pestaña confirmando la correcta instalación del firewall.

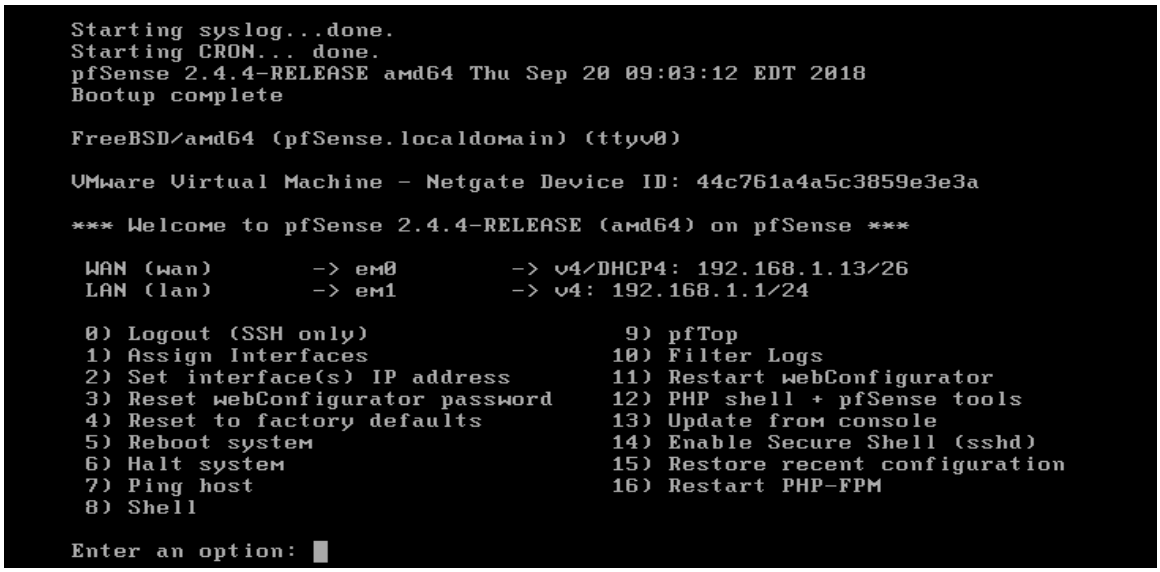


Figura 14. Menú de configuración Pfsense

Al conectar el Firewall a internet adquiere automáticamente una dirección IP mediante DHCP, por seguridad se recomienda colocar una IP estática.

Ingresando la IP de la red LAN en un browser, redirige a la interfaz web de configuración. Para ingresar al panel se coloca las credenciales por defecto que Pfsense asigna.

User: admin y Password: Pfsense

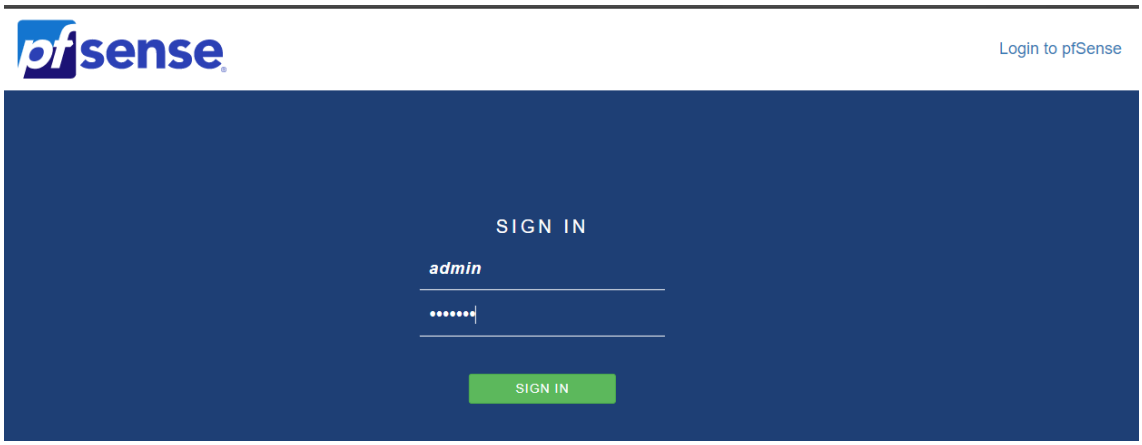


Figura 15. Login de ingreso a interfaz gráfica de Pfsense

Al ingresar correctamente las credenciales se visualizará esta pantalla (figura 16), siendo el punto de partida para realizar las configuraciones necesarias. Una vez dentro, el software indica en el lado izquierdo las características del equipo junto a la interfaz que reconoció, además de mostrar el estado actual del servicio de internet en su panel Gateway.

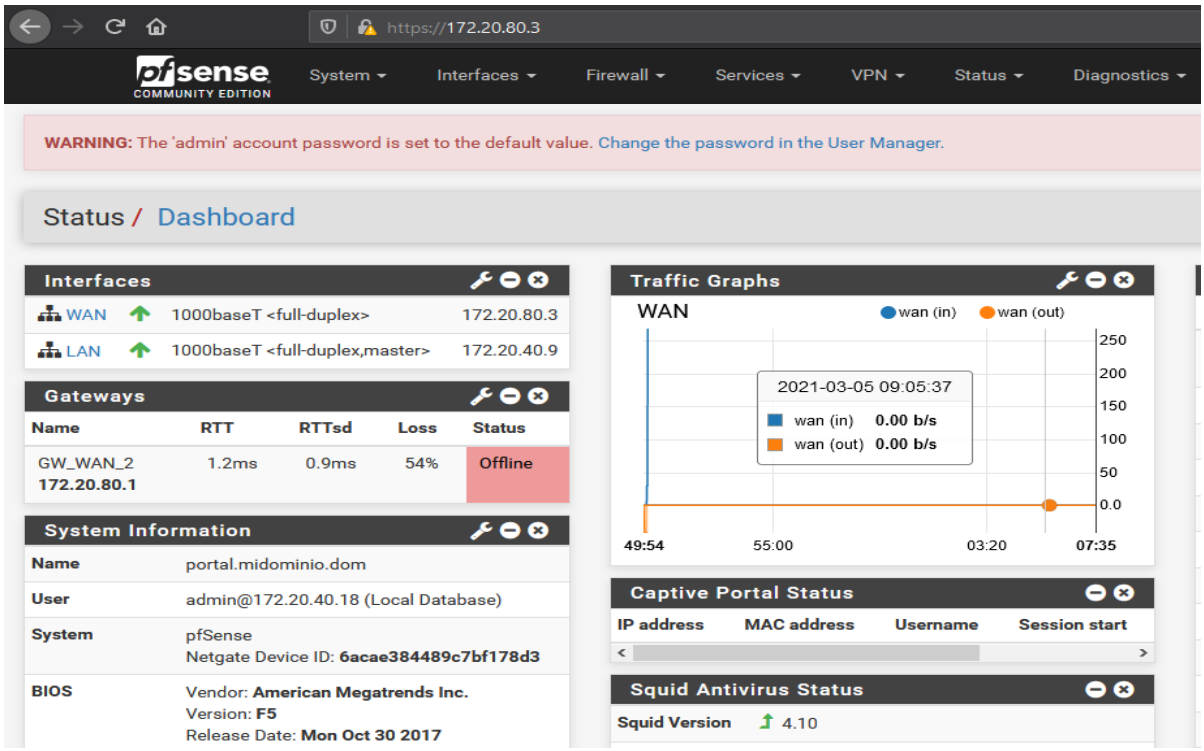


Figura 16. Dashboard de Pfsense

En las configuraciones de interfaz se elegirá el tipo de configuración IPv4, asignándole una máscara de subred /21.

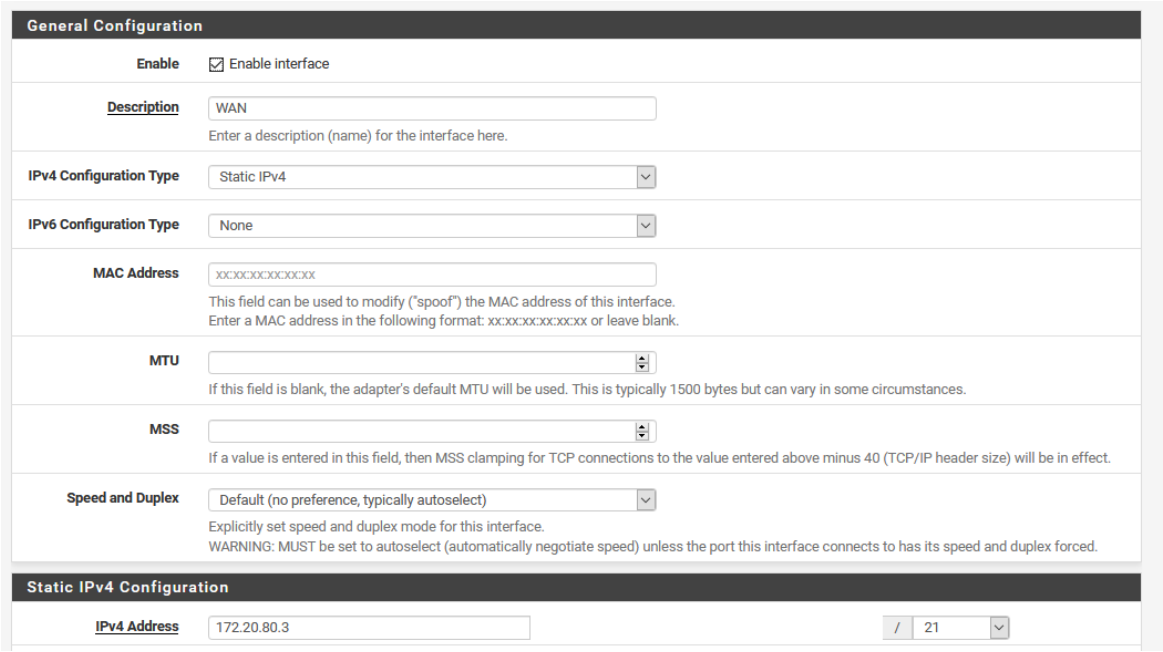


Figura 17. Configuración de interfaz WAN en Pfsense

Se establece una IP estática en la WAN con la finalidad de no tener inconvenientes a futuro, con internet en nuestro firewall se configura la interfaz que propaga el DHCP, este servicio es sumamente importante puesto que será utilizado por el portal cautivo.

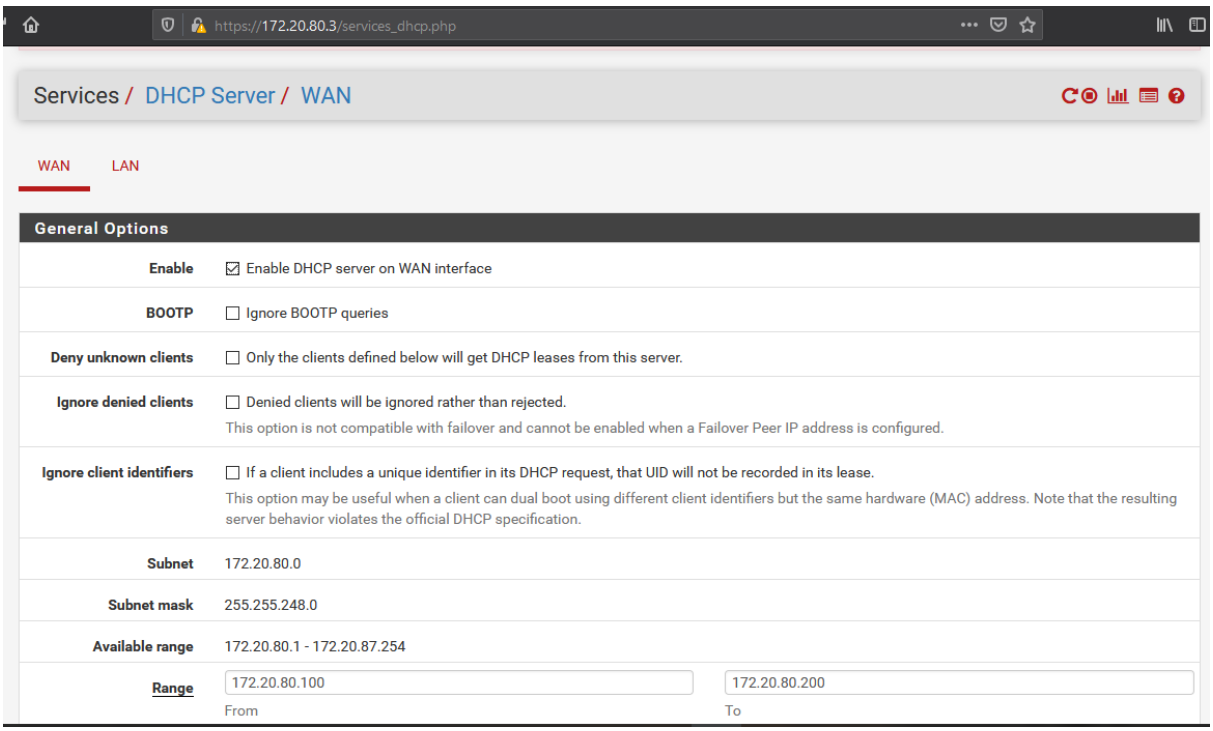


Figura 18. Configuración DHCP en Pfsense

- **Instalación Módulos**

A continuación, se detallará las herramientas y módulos que permitirán administrar la red de datos WiFi con la herramienta Pfsense, también se puede agregar funcionalidades extras dependiendo de las necesidades que tenga el administrador debido a que Pfsense posee setenta módulos adicionales.

- **NtopNg**

Una herramienta que se utilizó para permitir dar seguimiento a los dispositivos conectados a la red fue NtopNg, esta herramienta permite presentar varias vistas detallando direcciones IP, direcciones MAC, hosts, flujos de la interfaz en donde se montó la herramienta, también da la opción de monitorear e informar en tiempo real el rendimiento, latencia, estadísticas TCP, estadística RRT (tiempo de ida y vuelta) y paquetes que se trasmitieron en bytes. En las siguientes figuras se visualiza lo mencionado anteriormente.

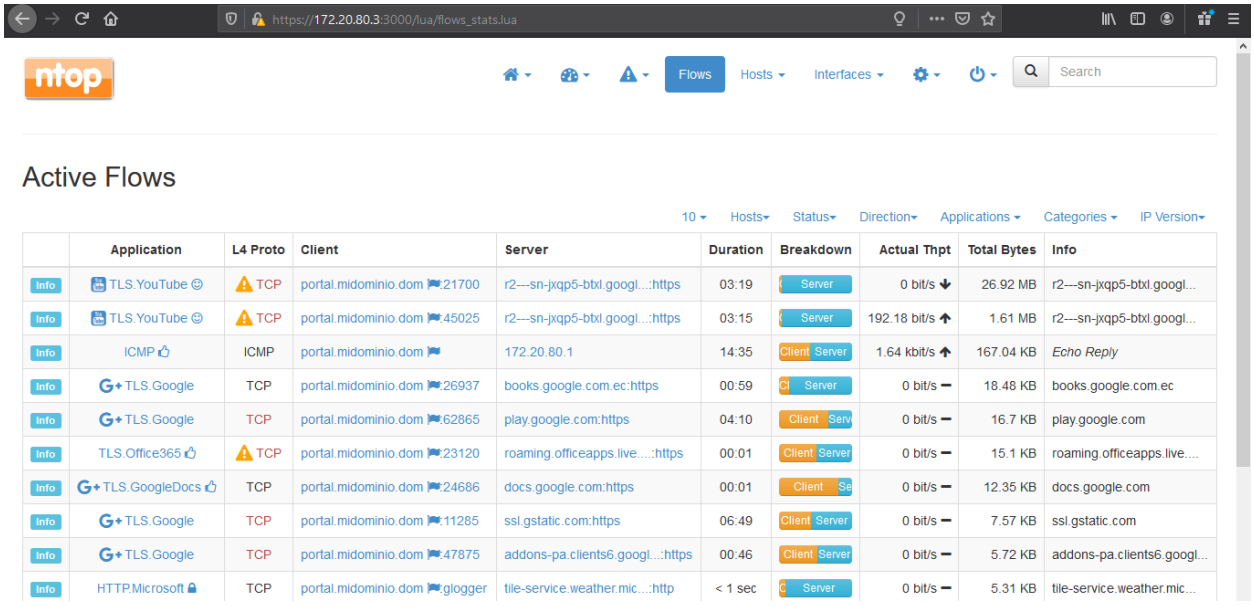


Figura 19. Visualización de aplicaciones y protocolos con la herramienta NtopNg

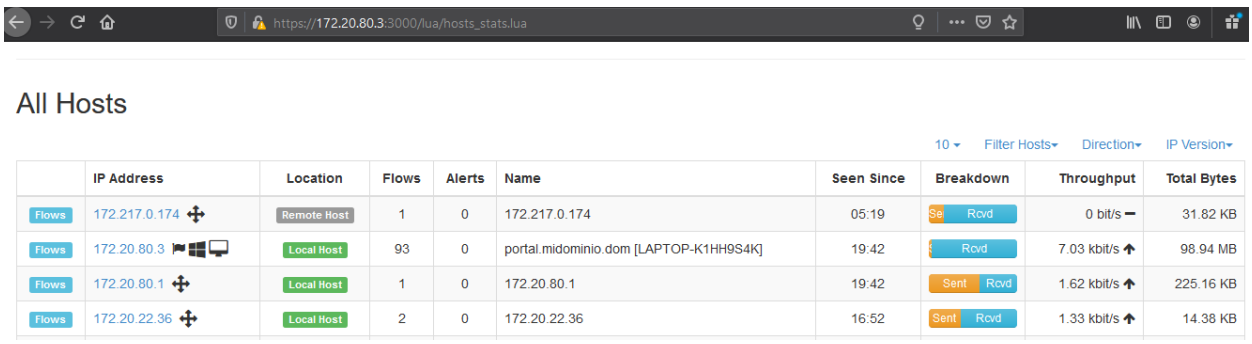


Figura 20. Visualización de host locales con la herramienta NtopNg

En el último gráfico se puede visualizar como la herramienta trabaja en conjunto, indicando: IP del dispositivo, nombre, tiempo de conexión, rendimiento y total de bytes usados. Ante esta situación el administrador puede dar seguimiento aquellos dispositivos que generen el consumo excesivo de recursos en la red.

- **FreeRadius**

Este paquete forma parte de una suite de Radius, se encuentra disponible en los módulos de Pfsense. Será implementado en la verificación y autentificación de usuarios, hay que aclarar que, se hará uso del Radius instalado en el Active Directory de la institución para recuperar las credenciales de acceso a la red, el FreeRadius instalado en el software únicamente servirá para realizar la conexión.

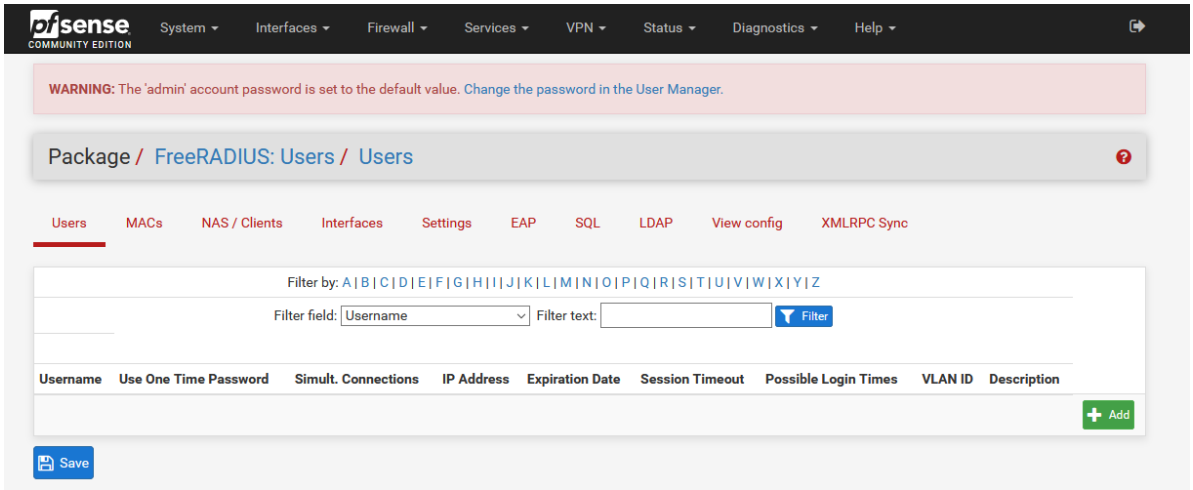


Figura 21. Instalación del paquete FreeRadius – Pfsense

Se debe configurar las interfaces para especificar puertos escucha 1812-1813-1816, mediante estos el servidor Radius podrá establecer la conexión.

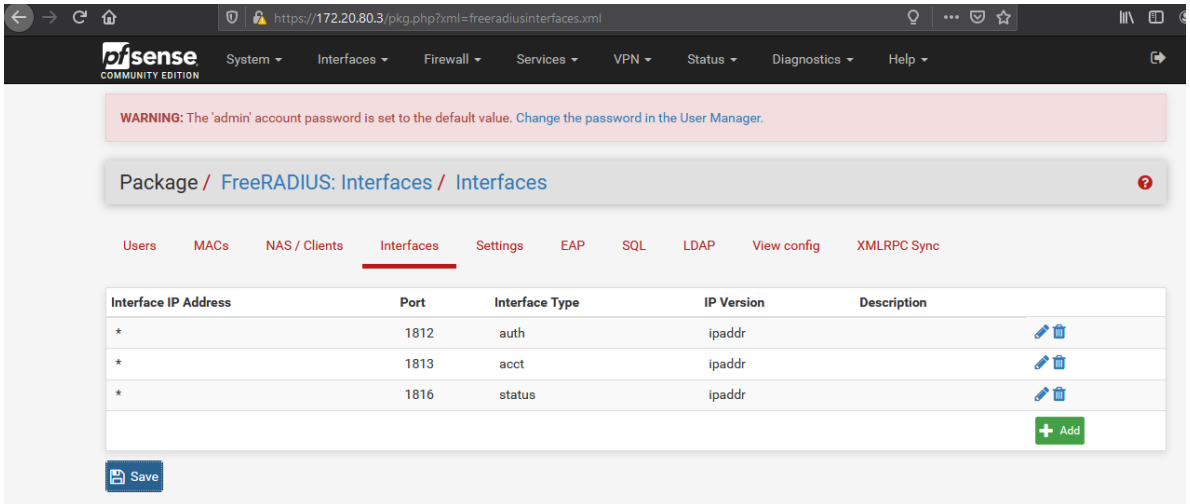


Figura 22. Configuración de puertos escucha en el servidor FreeRadius - Pfsense

Se debe configurar un cliente NAS, esto permitirá realizar la comunicación con el Radius del Active Directory instalado en Windows Server 2012

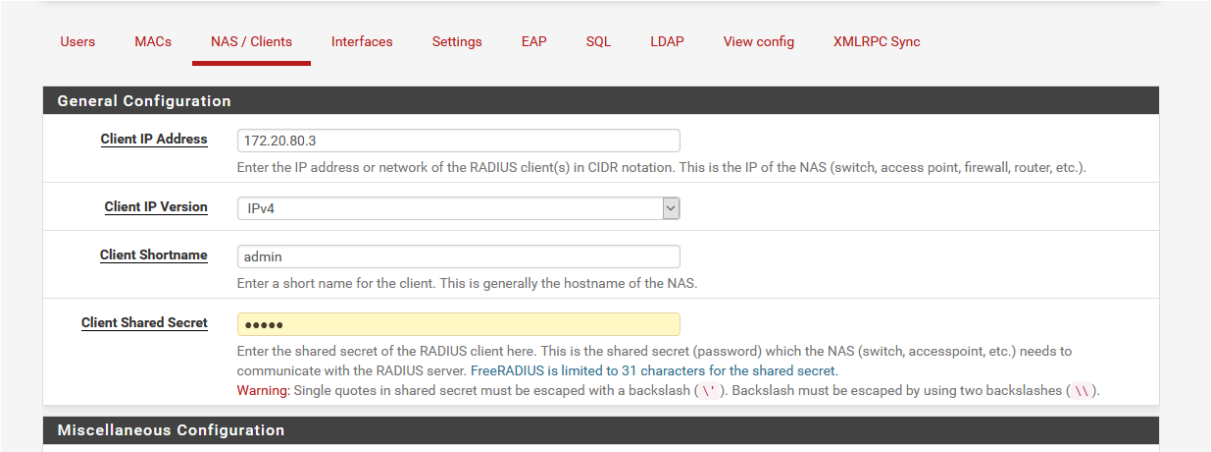


Figura 23. Configuración del cliente NAS en el servidor FreeRadius - Pfsense

- **Radius en Active Directory**

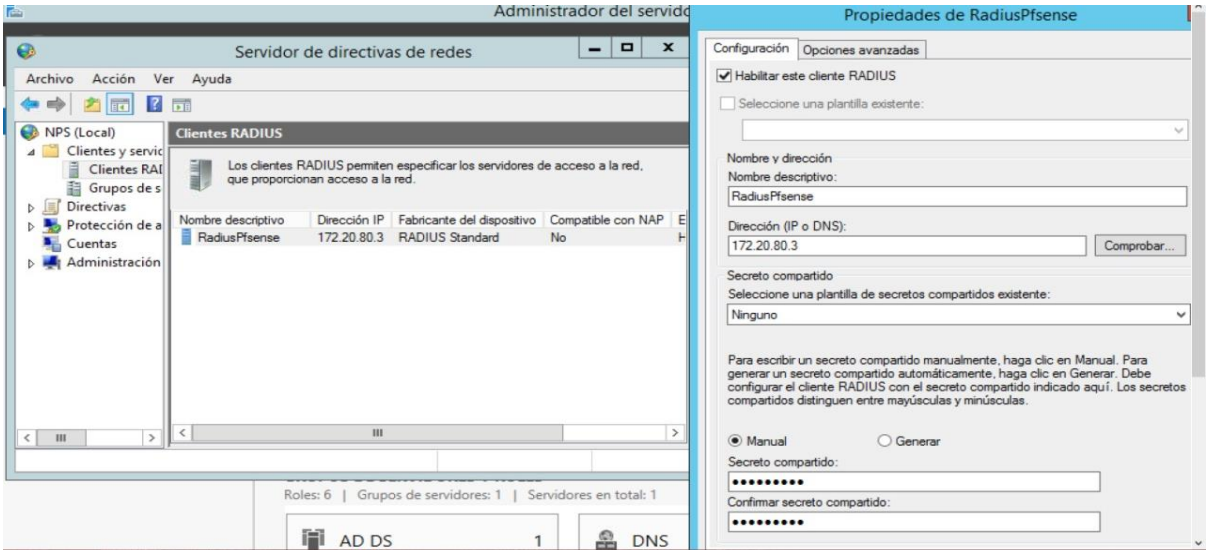


Figura 24. Conexión de Pfsense con el servidor Radius de la UPEC

- **Conexión Active Directory – Pfsense**

Para establecer la conexión entre al Active Directory y el servidor Radius de Pfsense, hay que dirigirse a la ruta System/ User Manager/ Authentication Servers, se crea una nueva conexión donde se específica el nombre, tipo y protocolo de seguridad Radius. En el apartado Radius Server/Settings se facilita la IP y el secreto compartido del Radius configurado en el Active Directory.

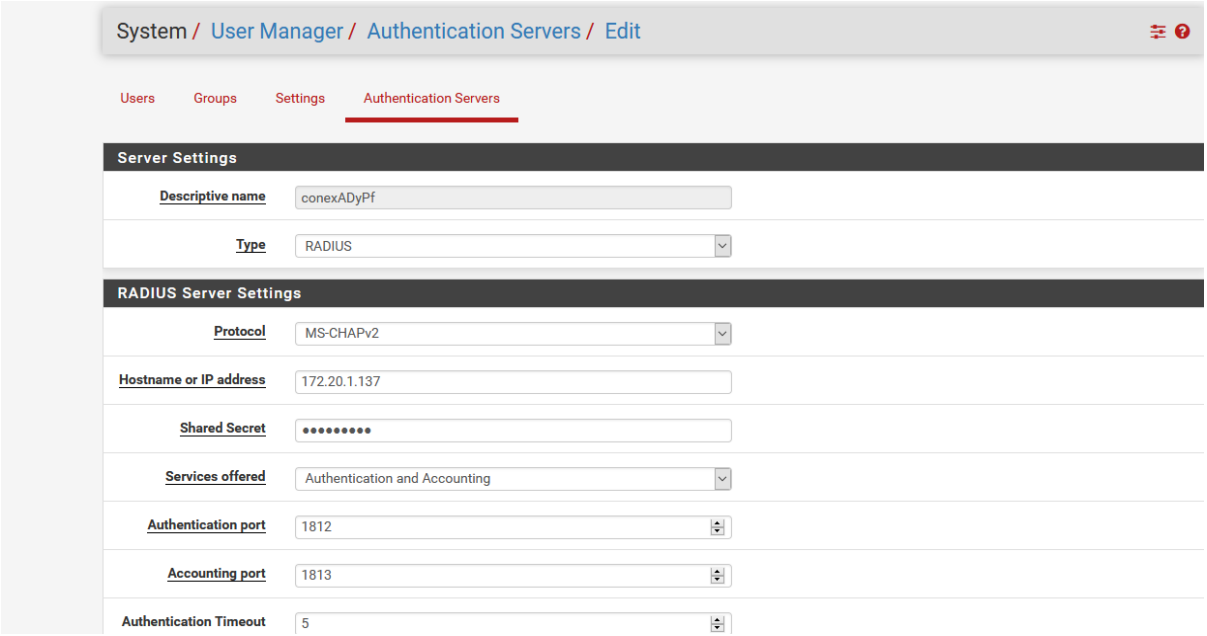


Figura 25. Configuración del servidor de autenticación Radius

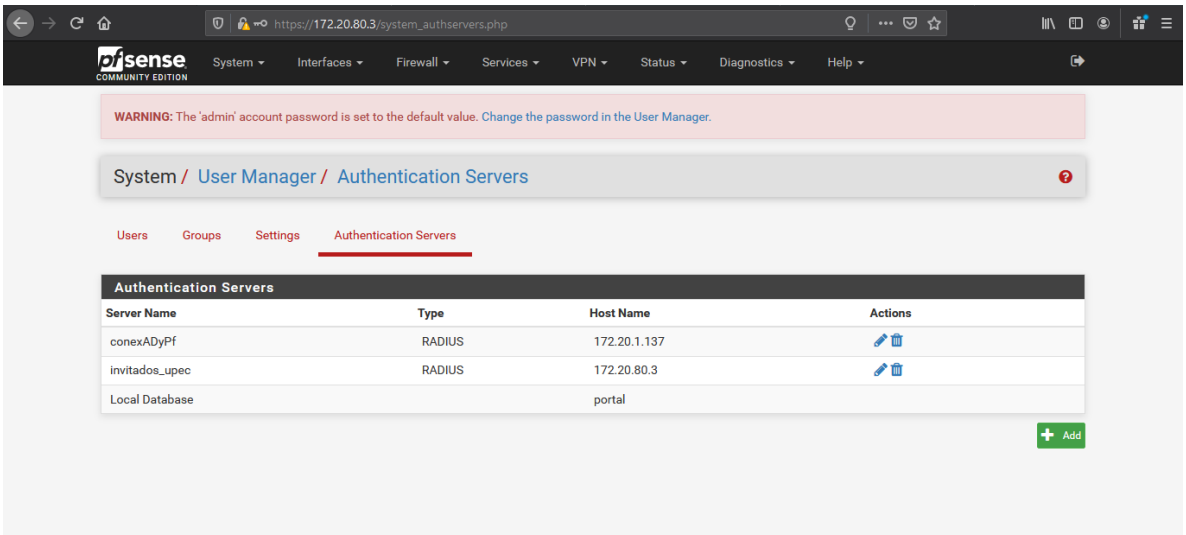


Figura 26. Conexión establecida servidor de autenticación Radius - Active directory

- **Squid Proxy Server**

Forma parte de la paquetería de Pfsense, este es un servidor proxy utilizado para mejorar el rendimiento de las conexiones a internet mediante el filtrado HTTP y HTTPS.

- **Proxy transparente (Squid y SquidGuard)**

Instalado el paquete se procede con las configuraciones, en donde se elige la interfaz WAN, para restringir el acceso a páginas web innecesarias.

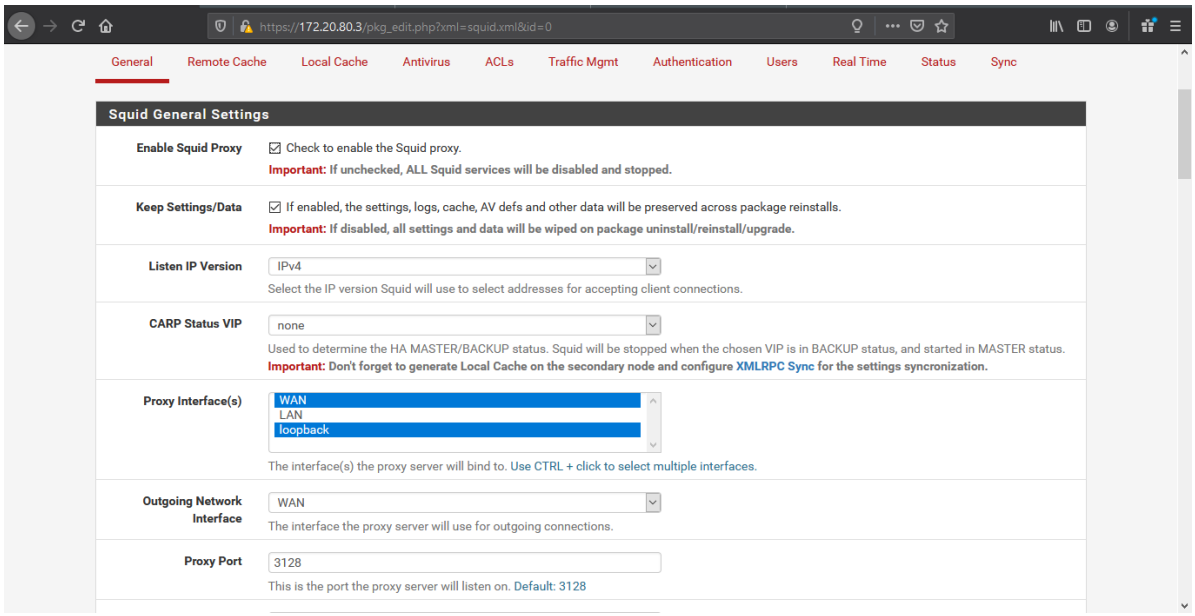


Figura 27. Squid Proxy Server - Pfsense

Se configura el Proxy de modo transparente, de esta manera permitirá interceptar y desviar las conexiones hacia el proxy sin la necesidad de configurar en cada cliente, la ventaja de esto es que el usuario no conocerá de su existencia. Se elegirá Bypass Proxy para que las direcciones privadas (RFC 1918) pasen directamente a través del Firewall.

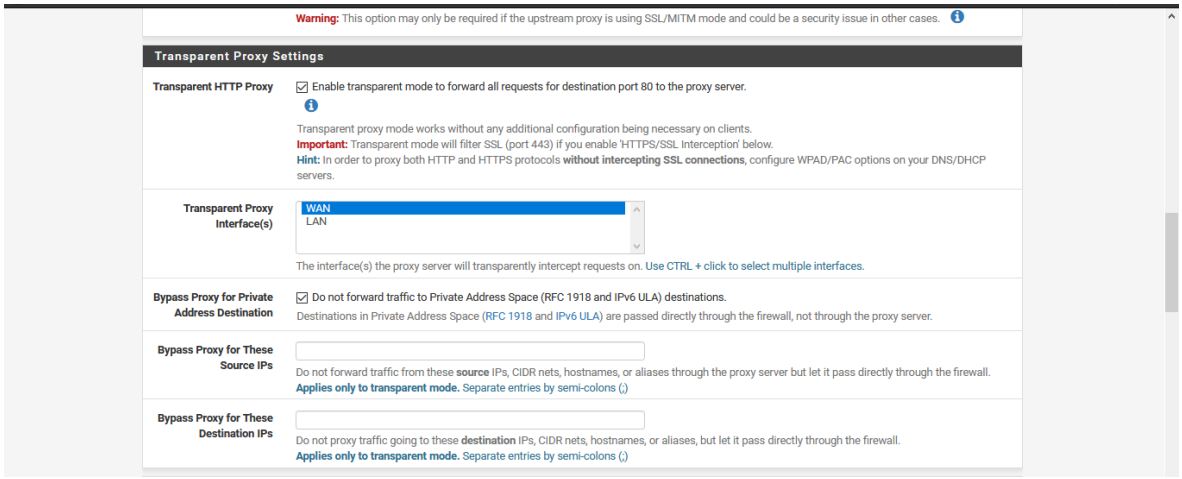


Figura 28. Configuración de Squid Proxy Server en Pfsense

Una recomendación adicional para el proxy es habilitar la casilla HTTPS/SSL, esta opción permite interceptar los certificados y brindar una navegación segura a los usuarios.

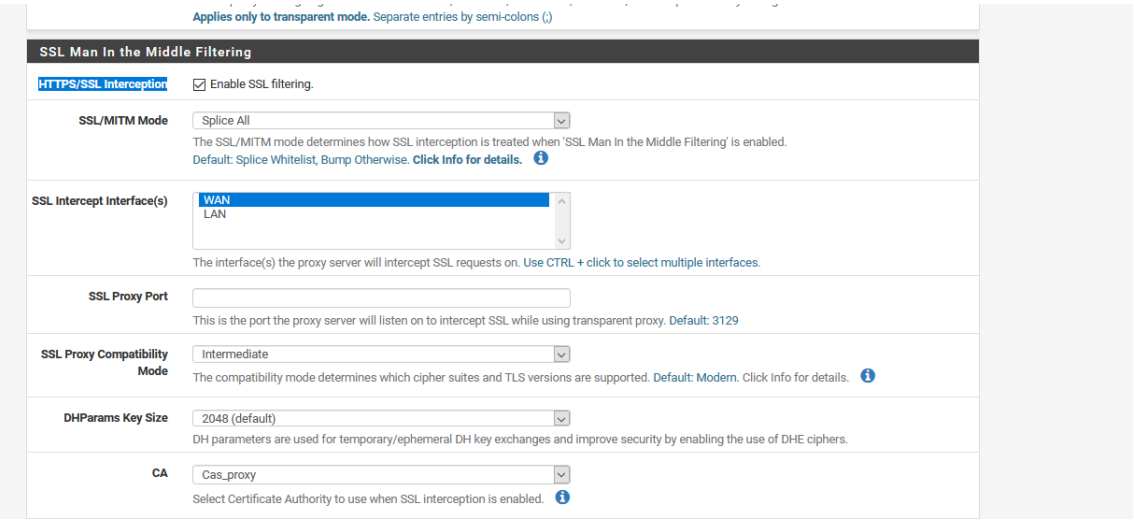


Figura 29. Habilitar casilla HTTPS/SSL en Squid Proxy

- **Proxy filter SquidGuard**

Es una herramienta que se deriva de Squid para filtrar el contenido web mediante la utilización de una de lista de acceso que se puede adquirir en páginas web gratuitas como Shallalist.

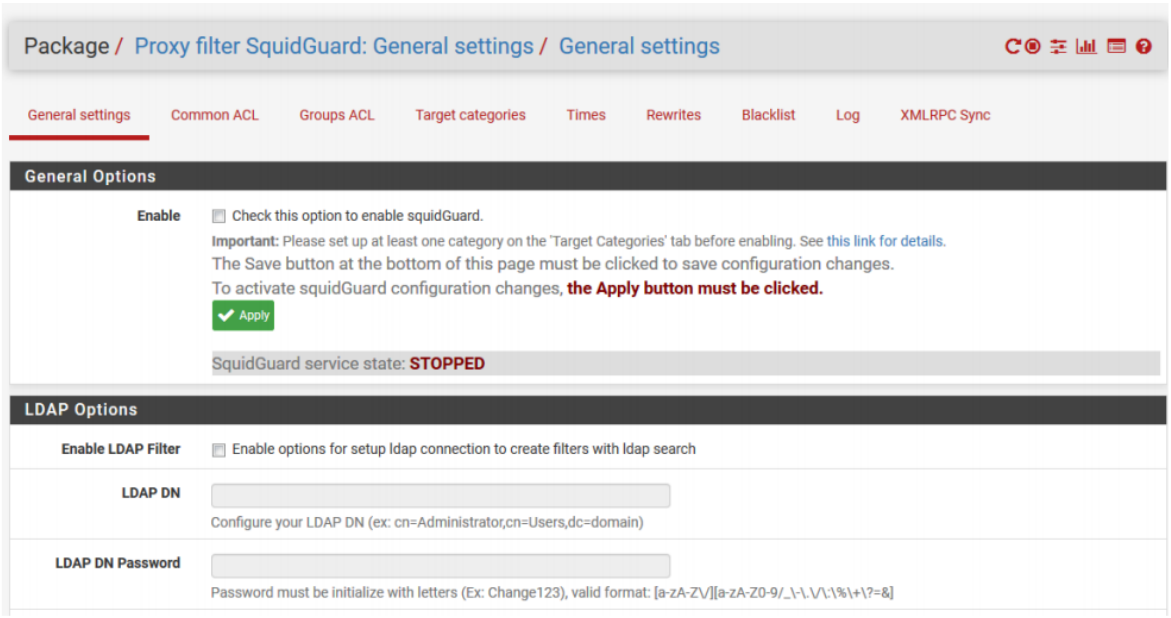


Figura 30. Configuración Proxy filter SquidGuard

Se mostrará a continuación la BlackList que se descargó de Shallalist, esta permitirá bloquear las páginas web innecesarias.

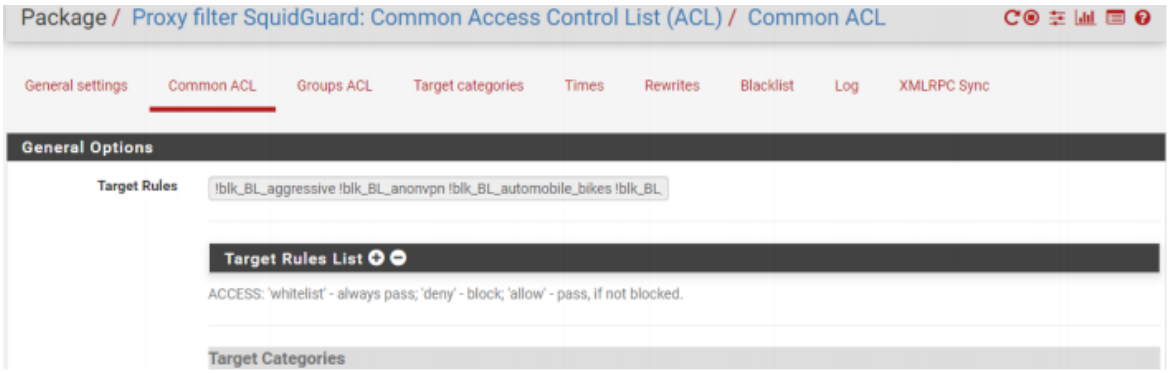


Figura 31. BlackList descargado de Shallalist

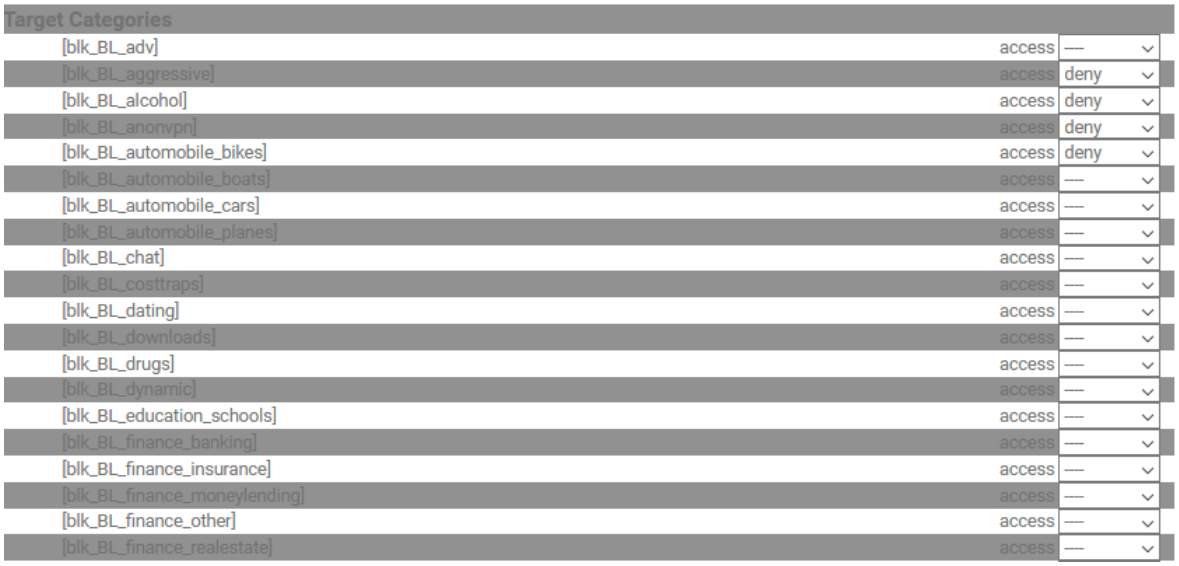


Figura 32. Configuración de bloqueo de páginas web innecesarias 1

Figura 33. Configuración de bloqueo de páginas web innecesarias 2

Figura 34. Configuración de bloqueo de páginas web innecesarias 3

- **Configuración portal cautivo**

Se considera al portal cautivo como una red informática, la misma que se encarga de gestionar y controlar el acceso a usuarios, redireccionándolos a una página predefinida donde debe colocar usuario y contraseña para tener acceso a internet. Cabe mencionar, que este sistema se aplica comúnmente en redes WiFi, pero también se lo puede implementar en una red LAN.

Para configurar esta herramienta es necesario ingresar al apartado Service/ Captive portal, para ello se aumenta una nueva zona y se realizará las configuraciones necesarias.

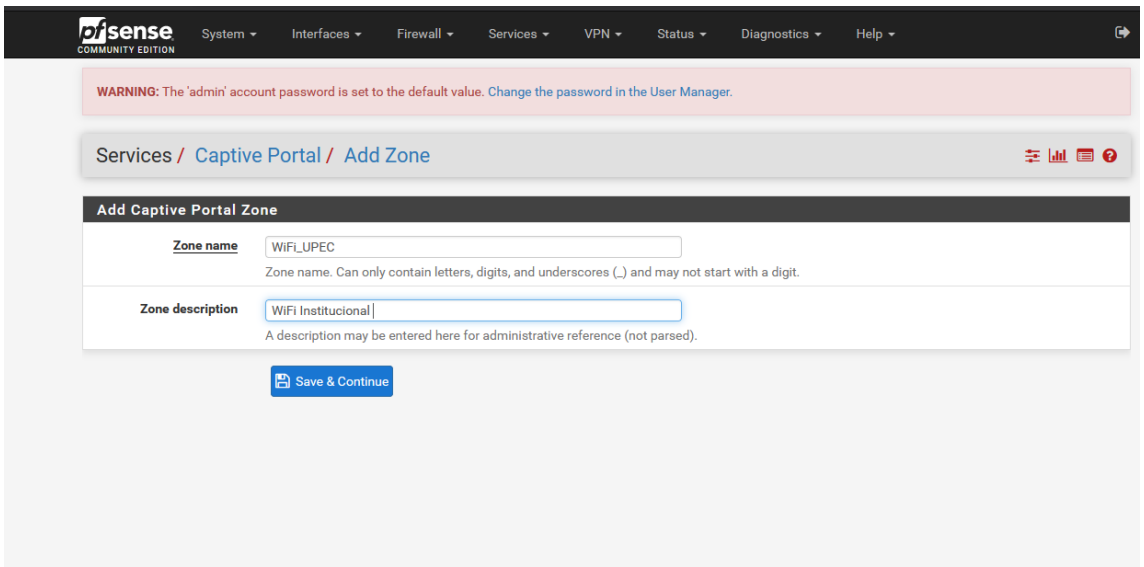


Figura 35. Agregando portal cautivo a Pfsense

Se elige la interfaz de red donde será implementado el portal cautivo, considerando los requisitos que se obtuvieron mediante los instrumentos de recolección de datos, logrando así adaptar el portal cautivo a las necesidades de la institución. Las respectivas configuraciones serán visualizadas a continuación en las figuras 36-38.

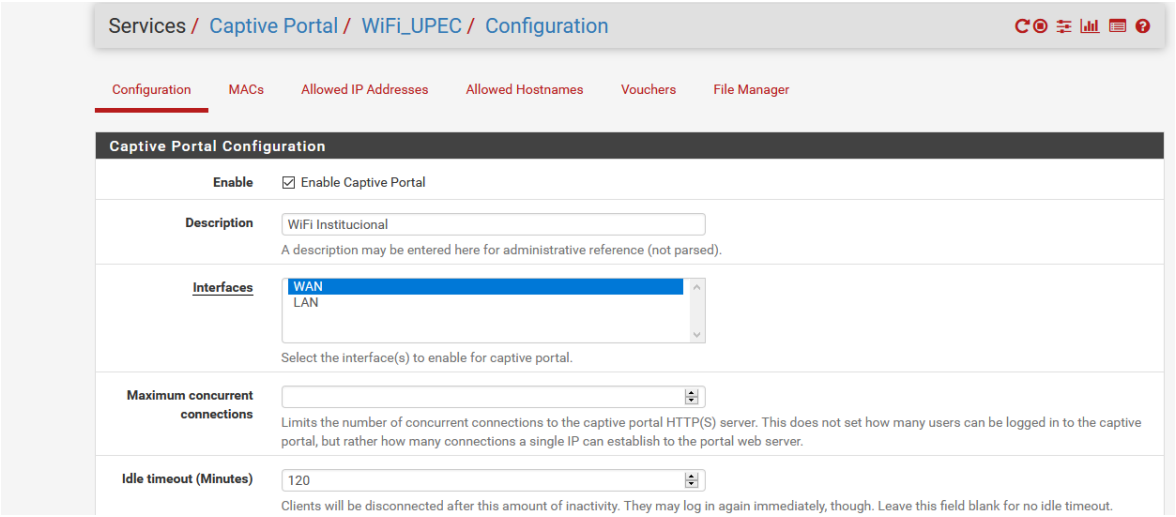


Figura 36. Selección de interfaz de red para portal cautivo

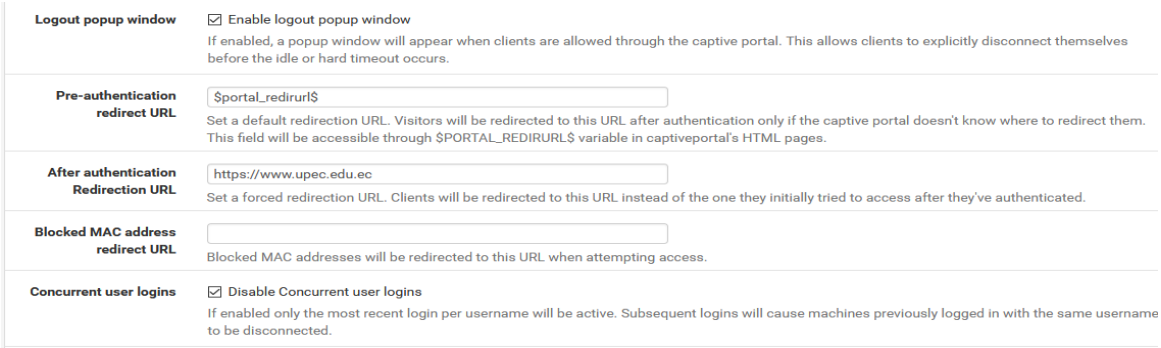


Figura 37. Redirección de página web después de autenticación en el portal cautivo

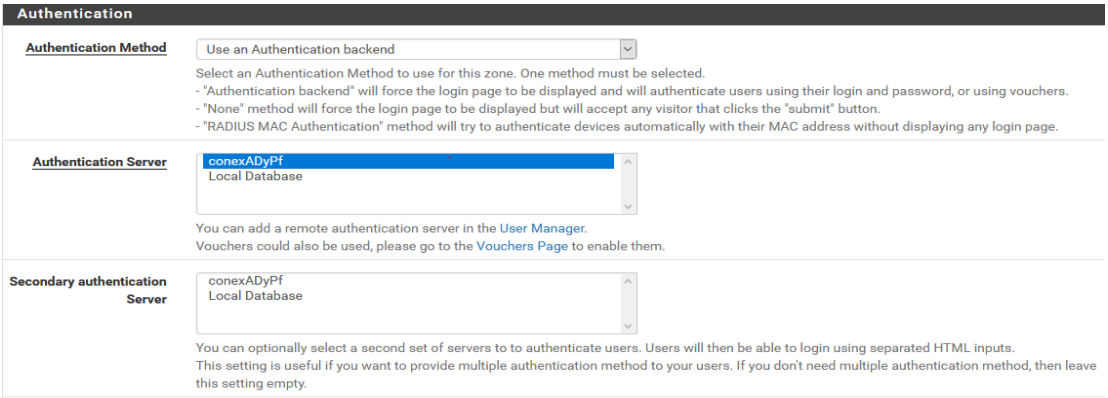


Figura 38. Selección de servidor de autenticación Radius

Pfsense tiene una opción para personalizar el portal cautivo, habilitando “Use custom captive portal page”, para este caso se ha generado una página HTML que se acople a la imagen de la

Universidad, respetando ciertos parámetros como los colores institucionales. Se tendrá un método de autentificación mediante usuario y contraseña, los mismo que reposan en el portafolio académico.

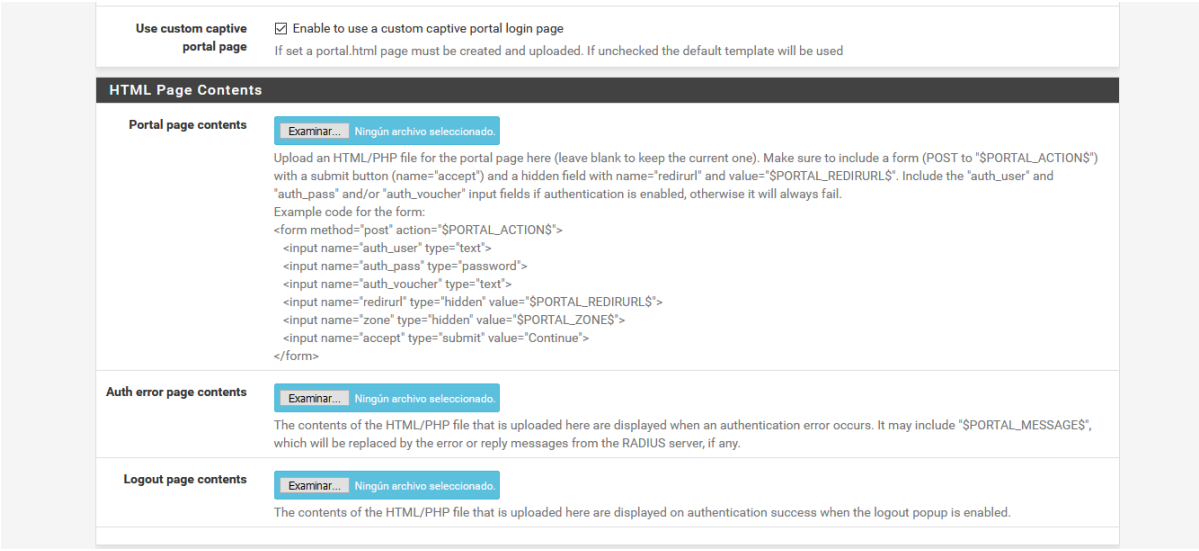


Figura 39. Configuración para personalizar portal cautivo de Pfsense

Concluida la fase de implementación, se agregará en el panel Pfsense widgets para conocer en tiempo real el estado de los servicios instalados. Ver Figuras 43,44,45 y 46.

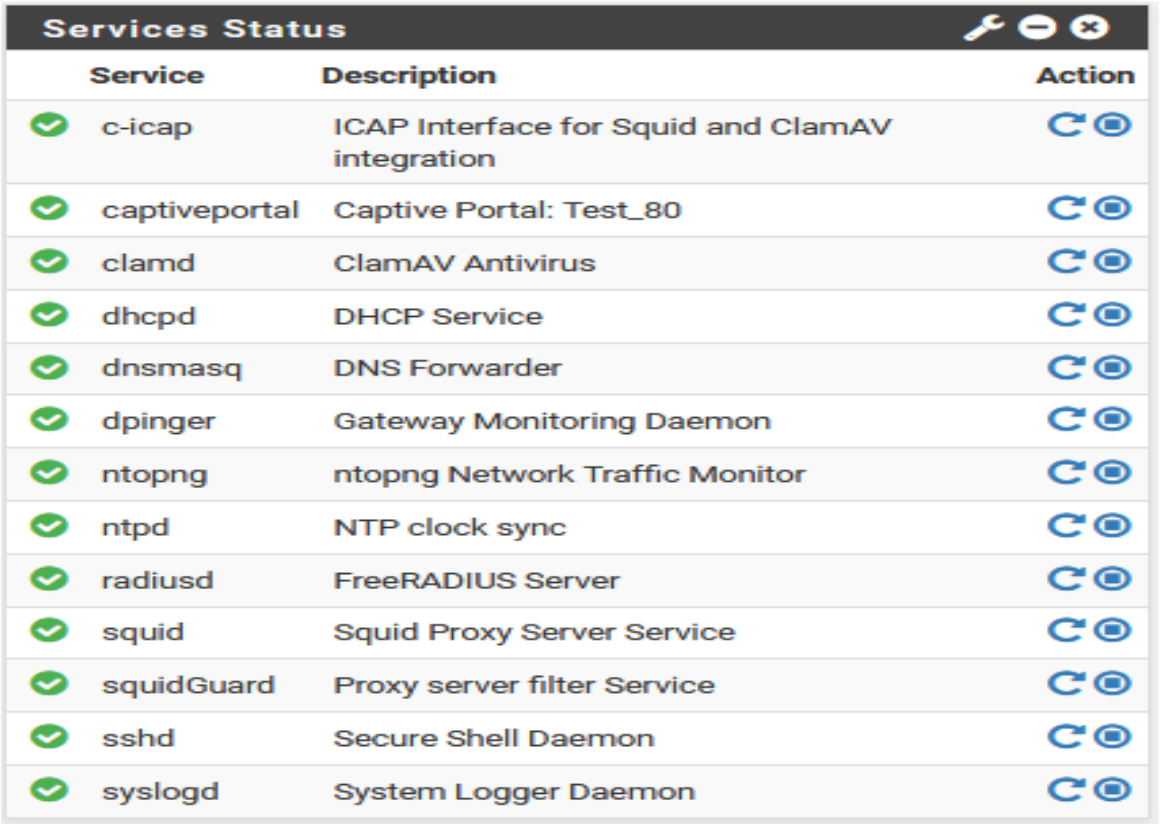


Figura 40. Servicios instalados en Pfsense

Figura 41. Estado del portal cautivo

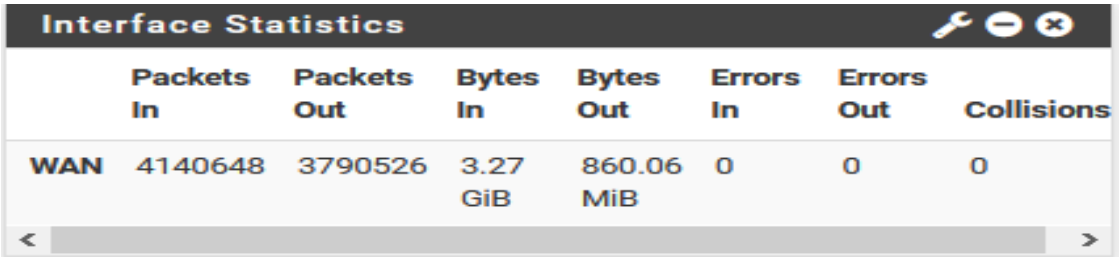


Figura 42. Estadísticas de interfaz de la red WAN

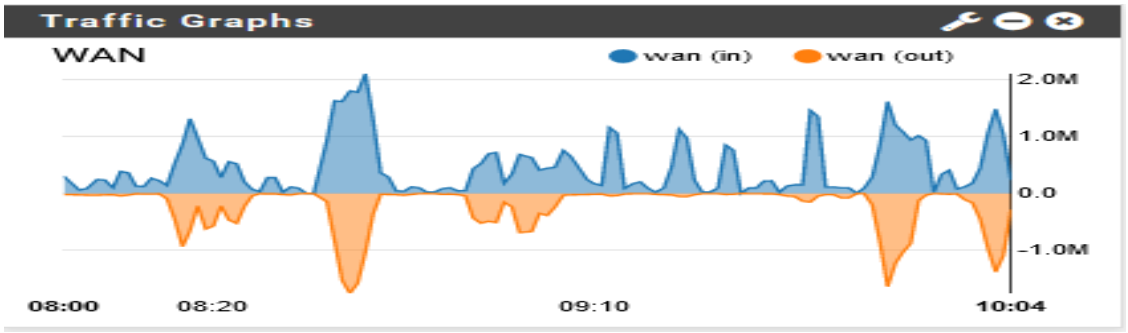


Figura 43. Grafica del tráfico en la red WAN

- **Reglas de Firewall**

Con la implementación casi terminada se debe configurar reglas en el firewall las mismas que permitan un mejor control.

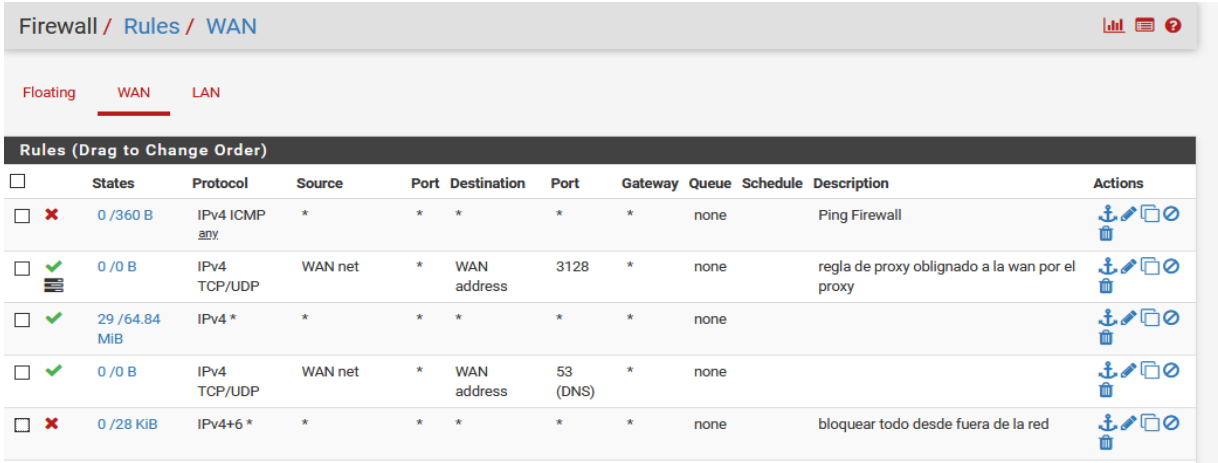


Figura 44. Configuración de reglas de Firewall en Pfsense

Regla 1: Impide realizar ping al servidor.

Reglas 2: Todo tráfico con protocolo TCP/UDP que tenga como destino la red WAN pasará por el servidor Proxy mediante el puerto 3128.

Regla 3: Permite la entrada y salida de datos en la red WAN, pasando previamente por el puerto 3128.

Regla 4: Permite tráfico con protocolo TCP/UDP mediante el puerto 53 (DNS).

Regla 5: Bloquea todo lo no contemplado en las reglas anteriores.

- **Fase 4.- Pruebas y mejoras**

Esta fase consiste en testear cada una de las herramientas instaladas anteriormente. Para ello se procedió a realizar pruebas con la intención de corregir o mejorar la red inalámbrica. Una vez finalizada toda la fase de configuración se ingresó a la red WiFi, para visualizar el funcionamiento del portal cautivo.

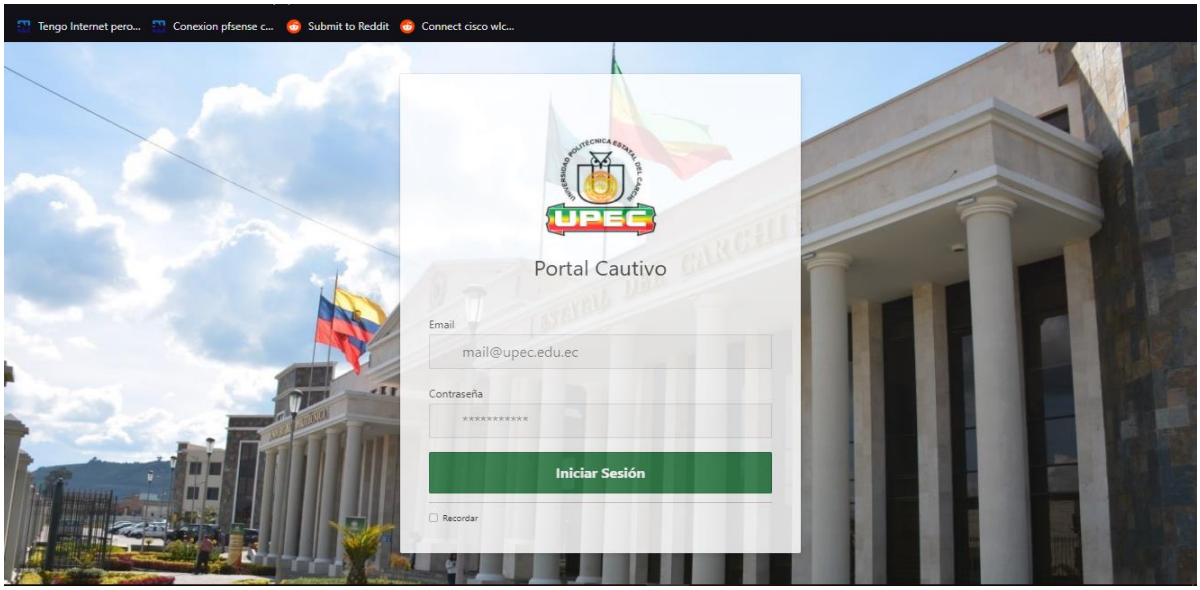


Figura 45. Login del portal cautivo de la UPEC

Para hacer uso del servicio se inicia sesión con las credenciales que la institución ha generado, los usuarios que se conecten a la red deben tener en cuenta que se estableció un tiempo de inactividad el cual será 120 minutos, adicionalmente se configuró el "Concurren Login" que limita a 1 dispositivo por usuario. Ver Figura 46.

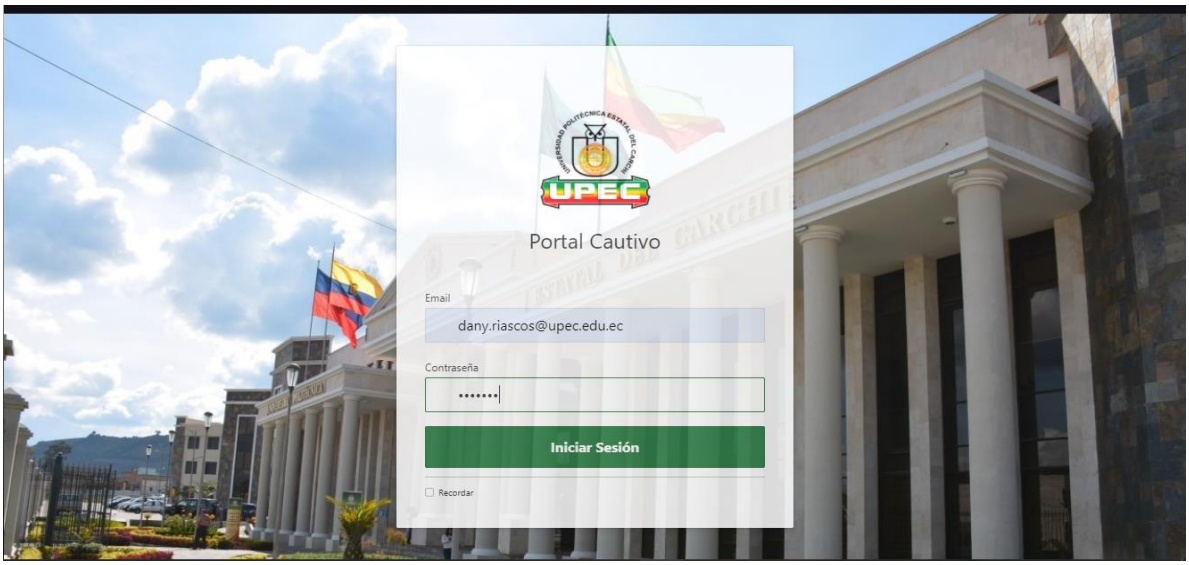


Figura 46. Ingreso de credenciales en Login de portal cautivo UPEC

Se verificó en el estado del Portal Cautivo aquellos usuarios que han iniciado sesión en la red WiFi mediante el uso de sus credenciales.

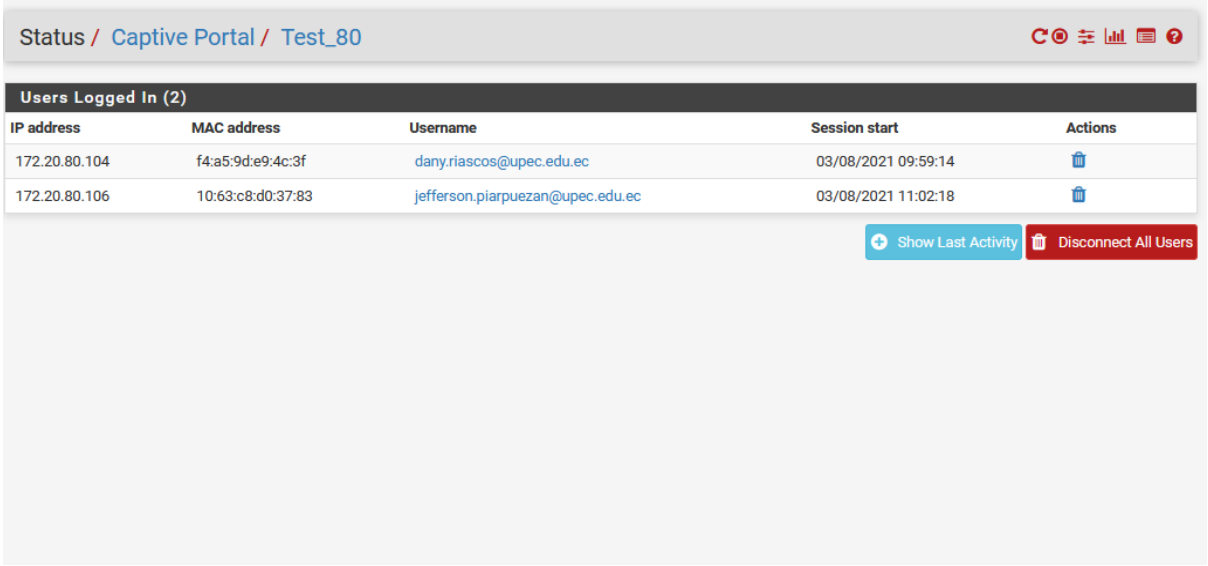


Figura 47. Registro de usuarios conectados al portal cautivo de la UPEC

Se procedió a verificar el correcto funcionamiento del servidor PROXY, ingresando a las páginas bloqueadas con la ayuda de la BlackList configurada previamente en el SquidGuard.

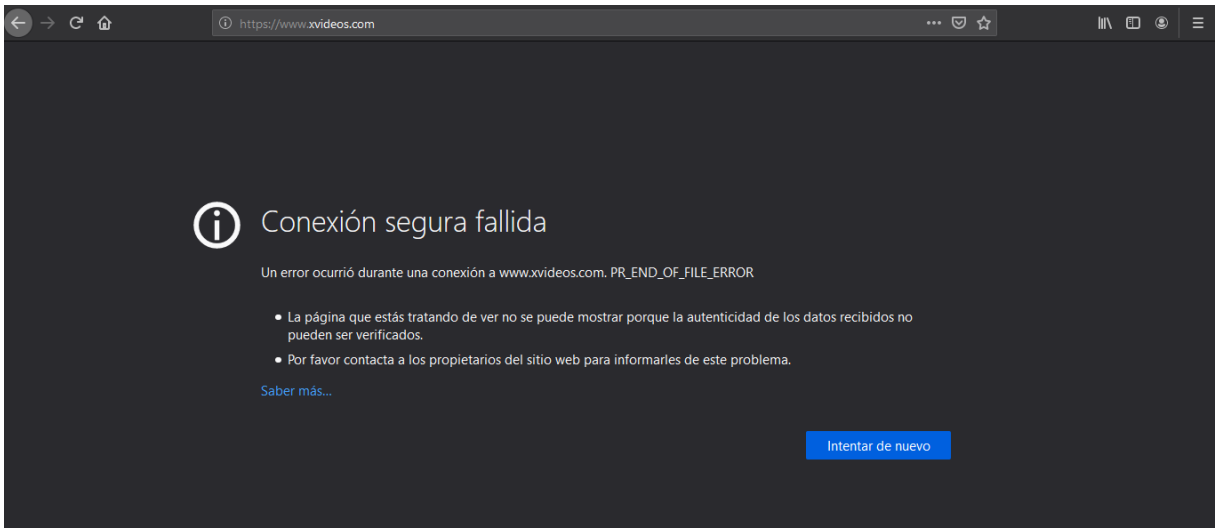


Figura 48. Bloqueo contenido para adultos

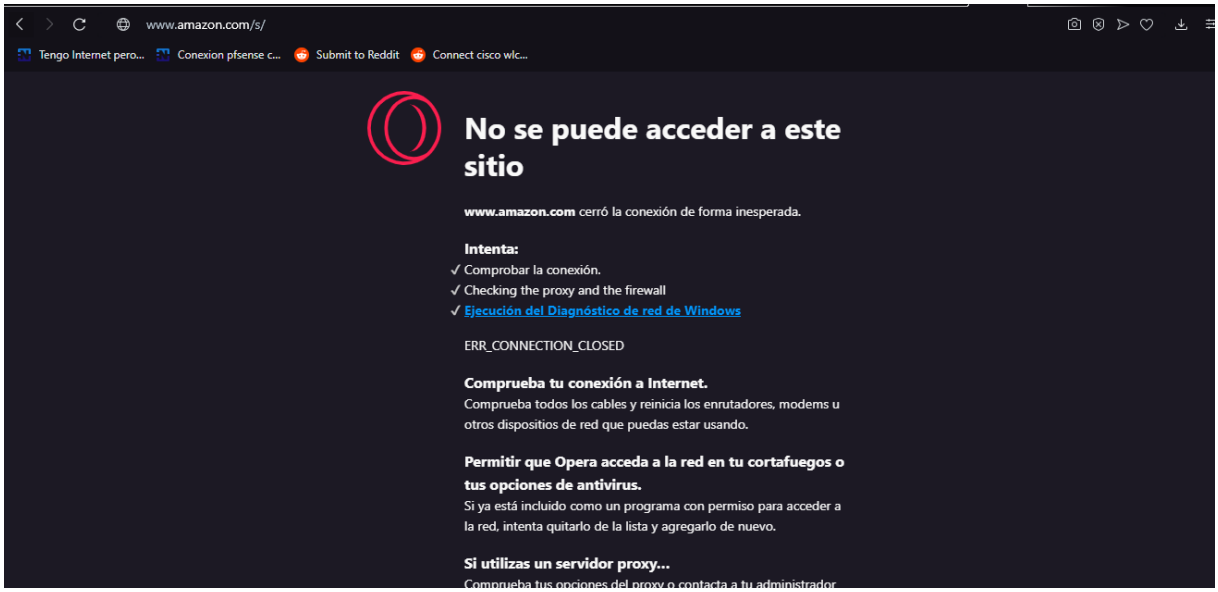


Figura 49. Bloqueo Compras Online

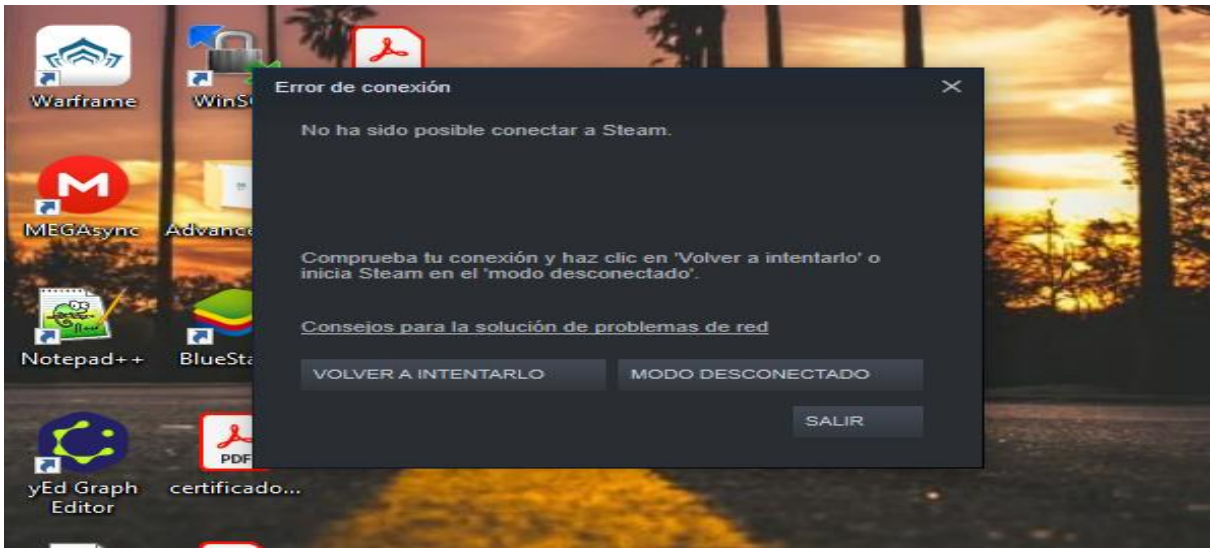


Figura 50. Bloque juegos online 1

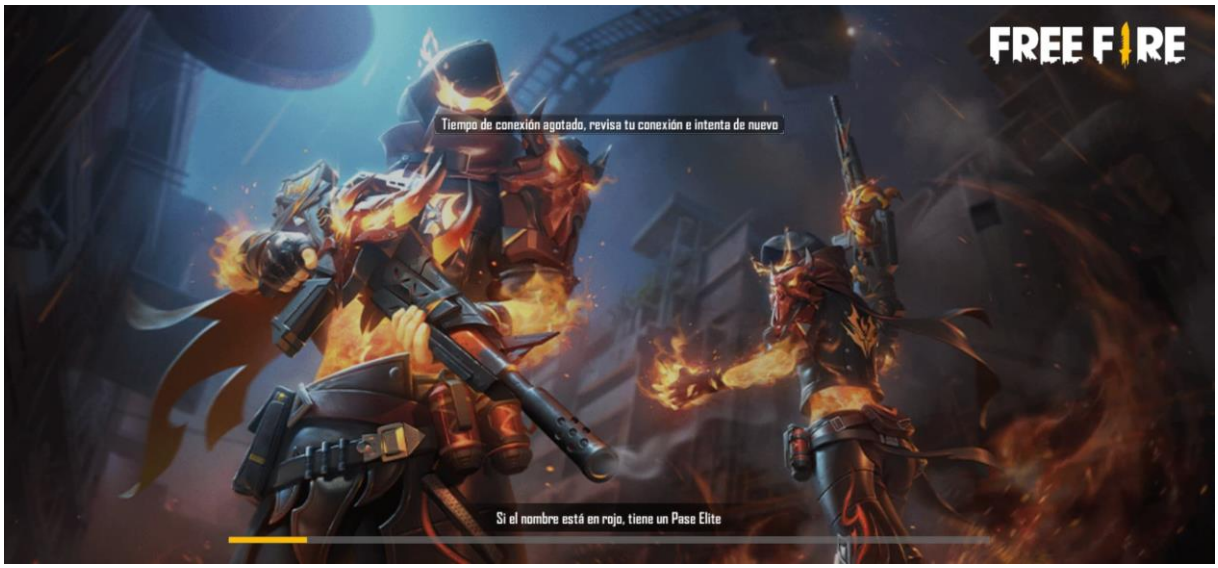


Figura 51. Bloque juegos online 2

A continuación, se indicará mediante el panel de administrador el registro de los dispositivos que se conectaron simultáneamente a la red WiFi a través del portal cautivo. Ver figura 52.

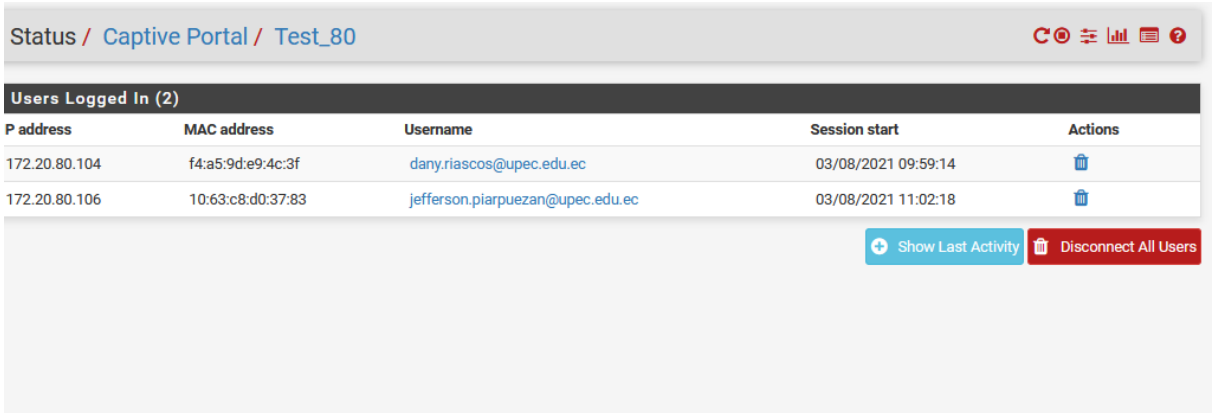


Figura 52. Registro de equipos conectados en el portal cautivo de la UPEC

- **Cumplimiento de requerimientos y funcionalidad del portal cautivo**

Una vez culminada la implementación del portal cautivo en la Universidad, se procedió a verificar el cumplimiento de los requisitos y funcionalidades que los miembros de TIC's puntualizaron previamente. Dichas características podrán ser visualizadas en la tabla 19.

Tabla 19. Cumplimiento de requerimientos y funcionalidad del portal cautivo

N°	Característica	Cumple	No cumple
1	Uso de software libre	✓	
2	Diseño de página web personalizada para la Universidad	✓	

3	Bloque páginas de Web	✓
4	Ingreso de usuarios por credenciales	✓
5	Limitar equipos por usuario	✓
6	Limitar ancho de banda	✓
7	Conexión con Active Directory	✓
8	Conexión con WLC	✓
9	Servidor DHCP	✓
10	Servidor DNS	✓
11	Servidor Proxy	✓
12	Servidor Radius	✓
13	Control y monitoreo de la red	✓
14	Portal cautivo	✓
15	Antivirus	✓

- **Comparativa de mejoras entre WUPEC_EVENTOS (WLAN antigua) y WiFi-UPEC (WLAN actual)**

La implementación de un portal cautivo en la red WiFi-UPEC trajo consigo ventajas a nivel de control y administración con respecto a la red inalámbrica WUPEC_EVENTOS, beneficiando a usuarios y administradores de la red, se detalla en la tabla 20 las funcionalidades que las diferencia.

Tabla 20. Comparativa red actual vs red antigua

WUPEC_EVENTOS (WLAN antigua)	**WiFi -UPEC (WLAN actual)**	**Resultado**
Conexión sin restricción de dispositivos por usuario	Conexión limitada a un dispositivo por usuario	Según la encuesta realizada a los estudiantes de la Universidad se determinó que el 57,49% utiliza dos dispositivos en la red inalámbrica. Con la implementación del portal cautivo se redujo este valor en un 100% puesto que se limita a un dispositivo por usuario.

El usuario no posee límite de ancho de banda	Límite de ancho de banda por usuario	Asignación uniforme de ancho de banda para cada usuario, permitiendo controlar el consumo desmesurado del servicio
La conexión es abierta por ende el ingreso a la red es para personas internas y externas a la Universidad	La conexión de los usuarios es mediante credenciales que se encuentran albergadas en el Active Directory de la institución. Cabe resaltar que estas credenciales las posee toda la comunidad universitaria	Garantiza el acceso a la conexión inalámbrica por parte de la comunidad universitaria, denegando el acceso de personas externas a la red
Acceso libre a cualquier página web	Bloqueo de páginas web innecesarias	Mediante el bloqueo de páginas de entretenimiento (Streams, películas, juegos en línea, pornografía, entre otros) se reduce el consumo de ancho de banda de la red inalámbrica, además de perimir que el uso sea enfocado al contenido académico
No posee ningún control ni monitoreo de la red inalámbrica	Control y monitoreo de la red inalámbrica	Permite a los encargados de TIC's llevar una administración y control detallado de la red inalámbrica
Total, de latencia 20.8 ms	Total, de latencia 18 ms	La Universidad presentaba una latencia inicial de 20.8 ms, con la implementación de un portal cautivo se redujo a 18 ms.

- **Análisis del resultado**

    - **Límite de conexiones de dispositivos por usuario**

Según la encuesta realizada a los estudiantes de la Universidad se determinó que el 57,49% utiliza dos dispositivos en la red inalámbrica. Con la implementación del portal cautivo se redujo este valor en un 100% puesto que se limita a un dispositivo por usuario.

- **Control de acceso de usuarios a la red**

Con la red anterior existía el acceso de personas ajenas a la institución, las misma que realizaban varias actividades como visita a redes sociales, descargas de archivos, videos, Streams, juegos online, entre otros. Ahora bien, con la red actual se garantiza el uso de internet inalámbrico a las personas que pertenecen a la institución.

- **Bloqueo de páginas web innecesarias**

Mediante el bloqueo a páginas de entretenimiento tales como Streams, películas, juegos en línea, pornografía, entre otro, se determinó que el consumo de ancho de banda puede mejorar un aproximado del 10 % puesto que, un usuario promedio consume 7.70 Mb por minuto al visualizar un video de YouTube con calidad de 480p, mientras que Facebook y Twitter consumen 1 Mb por minuto visualizando videos, fotos y gif. Por otro lado, al intentar jugar en línea el consumo de ancho de banda es superior con respecto a las otras aplicaciones, uno de los juegos más populares en la actualidad es Free Fire que consume 12.00 Mb en 20 minutos, mientras que Dota 2, League of Legends, Fortnite consumen de 70 a 100 Mb por hora.

- **Control de la red inalámbrica**

Los encargados de TIC´s al trabajar con la red WUPEC-EVENTES no contaban con herramientas para monitorear el rendimiento ni generación de reportes, impidiendo de alguna manera conocer el estado actualmente de esta. Con la implementación del portal cautivo en la red WiFi-UPEC se podrá monitorear el consumo de ancho de banda por cada usuario, cantidad de paquetes den entrada y salida, usuarios conectados, además de conocer las aplicaciones que están siendo utilizadas, todo esto en tiempo real gracias a la herramienta NtopNg. El porcentaje de mejora que se obtuvo es de un 60% con respecto al control de la red.

- **Latencia Total**

La red WUPEC-EVENTOS en un inicio no poseía parámetros de seguridad ni control de acceso, por ello la presencia de latencia era mayor, el estado inicial fue de 20,8 ms generando perdidas momentáneas del servicio a internet, además de disminuir la accesibilidad al contenido en la web a los estudiantes de la UPEC. Ahora bien, con la implementación del portal cautivo en la red WiFi-UPEC se ha disminuido el anterior valor a 18 ms, logrando así reducir en un 13,46 % la generación de latencia, esto se logró gracias al bloqueo de páginas innecesarias conjúntateme con un control de usuarios. Cabe mencionar que estos valores son un aproximado

en cuanto a la latencia real que posee la institución puesto que estos resultados se los obtuvo con un total de 100 personas las mismas que participaron en un evento de la institución.

4.2. DISCUSIÓN

El estudio actual tuvo como propósito determinar agentes generadores de latencia en la red de datos inalámbrica (WLAN), basándose en la infraestructura tecnológica de la misma, identificando los principales factores que disminuyen la accesibilidad al contenido en la web a los estudiantes de la Universidad Politécnica Estatal del Carchi.

En la presente investigación se tiene cinco objetivos, de los cuales uno es el objetivo general y cuatro son específicos, los tipos de investigación utilizados fueron de campo para recolectar datos directamente del lugar de estudio, la investigación descriptiva para conocer características específicas de un cierto grupo de personas u objeto, la investigación-acción que estudia una problemática en un grupo personas en específico el mismo que requiere ser solucionada. Se utilizó esta metodología para solucionar el problema que impide la accesibilidad al contenido en la web a la comunidad universitaria, el enfoque utilizado fue de tipo mixto, contó con dos variables una de ellas de tipo cuantitativa discreta la misma que va a permitir recolectar datos numéricos tales como número dispositivos conectados, número de conexiones establecidas y cifra de consumo en bytes por usuario, por otra parte la variable cualitativa ordinal va a permitir conocer factores como grados de satisfacción con el servicio que brinda la Universidad, conocer datos tales como porcentajes de tareas no enviadas mediante el uso de internet inalámbrico, preferencia de páginas web visitadas. Para la recolección de esta información se utilizó dos instrumentos de investigación el primero fue la entrevista de tipo no estructurada dirigida al personal de TIC’s de la Universidad, el segundo instrumento fue la encuesta con preguntas de tipo cerrada aplicada a una muestra de 252 estudiantes de una población total de 3450, validada por el MSc. Jhony Enríquez (director de TIC’s), Ing. Javier Torres (Encargado del área de Redes y Telecomunicaciones) y MSc. Milton del Hierro (Tutor). Se utilizó los métodos analítico e inductivo, el analítico ayudó a definir un todo que en este caso es la red de datos inalámbrica de la UPEC y el inductivo que permitió alcanzar conclusiones generales partiendo de los antecedentes e idea a defender que se planteó.

Este proyecto está enfocado a los estudiantes de la Universidad Politécnica Estatal del Carchi, pero también puede aplicarse a hoteles, restaurantes, parques, escuelas, colegios, entre otros lugares que tengan la necesidad de controlar su red inalámbrica.

Para el desarrollo del portal cautivo que se implementó en la Universidad se utilizó software libre, concretamente la herramienta Pfsense la misma que posee características y funcionalidades acordes con la necesidad de la Universidad como son las de poder conectarse a un servidor externo en este caso Active Directory que alberga usuarios y contraseñas de estudiantes, además de tener que mostrar el portal en una red especifica que es manejada por la Wireless Lan Controller.

De esta forma se tuvo en cuenta el proyecto de titulación de Chalen y Plúas en el año 2017 en la Universidad de Guayaquil en el cual se propone la implementación de una red inalámbrica con la tecnología de transmisión de datos Li-Fi la misma que incremente la velocidad de trasmitir datos en la institución, mediante un protocolo de Ip v6. Además de configurar un portal cautivo en Zeroshell para controlar políticas y accesibilidad a la red. Este proyecto se asemeja al estudio actual en la implementación de un portal cautivo utilizando software libre para controlar la red, ayudado de un servidor Radius que permita la autenticación de usuarios, buscando prevenir inconvenientes de lentitud de la red o perdida de conexiones que afecte la accesibilidad al contenido en los estudiantes y difiere en el uso de la red inalámbrica que para el presente estudio cuenta con la tecnología WiFi. Asimismo está el trabajo de titulación realizado por Linda Inés Andrade Cayambe en el año 2019, el cual tuvo la finalidad de diseñar una propuesta con ambiente controlado de herramientas administrativas y portal cautivo para controlar usuarios, además de administrar la red por medio de políticas de seguridad en la carrera de Networking y Sistemas de la Universidad de Guayaquil, que al igual que el presente estudio hace uso de la herramienta de software libre Pfsense, con la diferencia de que utilizó hardware y en este estudio software. Finalmente, se tiene el trabajo de titulación realizado por Juan Alejo Peirano en el año 2015 en la que se realizó una medición de latencia en la región, ayudado de algoritmos que trabajaban mediante una consulta pseudoaleatoria, logrando una ampliación y optimización de esta, esta medición de latencia es diferente a la del presente estudio la cual se lo realizó mediante la examinación de la infraestructura tecnológica de la Universidad.

Como punto final se aceptó la idea a defender, siendo esta es de tipo causal debido a que la variable independiente denominada latencia en la red de datos inalámbrica genera un efecto en la variable dependiente denominada accesibilidad al contenido web, a continuación, se detalla en la tabla 21.

Tabla 21. Aceptación de Idea a defender

Idea a defender	Aceptación / Negación	Razones
La elevada latencia en la red de datos inalámbrica disminuye la accesibilidad al contenido web a los estudiantes de la UPEC.	Aceptación	Con los resultados obtenidos mediante la recolección de datos, ayudados de investigaciones de campo se determinó que la Universidad Politécnica Estatal del Carchi necesita implementar una herramienta informática que ayude a controlar aspectos como número de dispositivos conectados simultáneamente por estudiantes, bloqueo de sitios web, entre otras con la finalidad de disminuir latencia y optimizar la accesibilidad al contenido web. La implementación de un portal cautivo contribuye en el control de acceso de usuarios a la red inalámbrica de la Universidad. Mediante la implementación de un portal cautivo los usuarios en la red inalámbrica podrán acceder de manera óptima al contenido académico.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se determinó que la latencia se genera por diferentes factores como lo son el uso de contenido HTTP que es un contenido sensible a fallos, equipos obsoletos o desactualizados, infraestructura que impide el paso de las ondas electromagnéticas, distribución de Access Points de forma rudimentaria y la ausencia de herramientas que controlen el consumo de ancho de banda.
- Mediante la recopilación bibliográfica digital y escrita se logró adjuntar información importante de estudios, investigaciones y datos referentes a la latencia y accesibilidad a contenidos web en redes inalámbricas, la finalidad de la recopilación de esta información fue tener bases y fundamentos en los que se sustenta el marco teórico además de ayudar a la conceptualización de los términos utilizados.
- Se analizó la red de datos inalámbrica mediante el diagrama físico de la infraestructura, identificando que el equipo Ciso ASA 5520 terminó su vida útil en el año 2018 y actualmente está obsoleto, generando problemas de integridad, disponibilidad y confidencialidad de la información en la institución. Por otra parte, la Wireless Lan Controller Cisco 5508 se encuentra desactualizada siendo propensa a fallos como la ejecución de código arbitrario, denegación de servicio y acceso no autorizado. Además de que los Access Points están configurados mediante la técnica site survey.
- Se eligió una solución informática que ayude a mitigar la latencia en la red de datos inalámbrica, para ello se generó una comparativa de portales cautivos en la cual se evaluó las funcionalidades, requerimientos y criterios de cada software, seleccionando a la herramienta de software libre Pfsense como la más óptima, la misma que se acoplaba a las necesidades tanto de la institución como de la infraestructura, además de ser una herramienta intuitiva y de fácil manejo para el administrador de la red.
- Se implementó el portal cautivo el cual permite controlar el acceso de usuarios mediante una previa autenticación, conjuntamente se instaló herramientas con las que cuenta el Firewall como el SquidGuard y NtopNg, la primera se encarga de bloquear el acceso a páginas web innecesarias, mientras que NtopNg permite realizar el monitoreo de la red inalámbrica en tiempo real, indicando el consumo de ancho de banda por equipo, la aplicación, el protocolo y el total de bytes utilizados.

- La latencia es un factor influyente dentro de las redes inalámbricas, siendo provocada por varios factores como el exceso de usuarios, consumo de ancho de banda, la infraestructura, distribución de equipos, entre otros factores. Con la implementación de un portal cautivo se mitigó la latencia en un 13,46 %, mejorando en un porcentaje considerable el acceso al contenido web de los estudiantes de la Universidad. Cabe mencionar que este porcentaje es un valor aproximado, puesto que no se cuento con valores exactos por motivos ajenos a la institución.

5.2. RECOMENDACIONES

- Es importante considerar que la institución posee equipos que actualmente se encuentran obsoletos y desactualizados, ante esta situación se recomienda a los encargados del área de Redes y Telecomunicaciones realizar un estudio de factibilidad para migrar a equipos actuales con el objetivo de poseer soporte y una infraestructura actualizada, impidiendo a personas mal intencionadas atentar contra la integridad, confidencialidad y disponibilidad de la información.
- Es necesario realizar una investigación posterior para complementar el presente estudio, debido a que Pfsense es una herramienta escalable en cuanto a servicios y funcionalidades para el control y manejo de la red, esta posee alrededor de 70 módulos los mismos que pueden ir adaptándose de acuerdo con las necesidades que la institución requiera posteriormente.
- Se recomienda a los encargados de Redes y Telecomunicaciones al agregar e implementar nuevos equipos Access Point en la infraestructura de la red, tener en cuenta estándares o protocolos que permitan la correcta distribución, evitando generar zonas sin cobertura que afecten a la experiencia del usuario al navegar en la red inalámbrica.
- Es necesario tomar en cuenta que el Estado ecuatoriano obliga la utilización de software libre en instituciones públicas, como lo menciona en los artículos 142, 145 y 151 del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación con la finalidad de optimizar el gasto estatal fortaleciendo el desarrollo local y facilitar la inclusión digital.
- Se recomienda realizar mejoras en la página personalizada del portal cautivo basándose en la norma NTE INEN-ISO/IEC 40500 concerniente a la accesibilidad web para personas con discapacidad visual. Además de agregar una segunda autenticación para invitados que la Universidad albergue en eventos o congresos por medio de váuchers que limite el tiempo de conexión, ancho de banda, entre otros.
- Basado en la presente investigación se recomienda realizar pruebas de latencia que permitan conocer un valor más preciso al mostrado en el estudio, contando con diferentes pruebas a grupos de estudiantes y en horarios variados donde la latencia puede fluctuar dependiendo del tráfico que se genera.

VI. REFERENCIAS BIBLIOGRÁFICAS

3ciencias. (2015). Glosas de innovación aplicadas a la pyme. *3C Tecnología, investigación y pensamiento crítico, 4*(1), 2254 - 4143

Adriano, W. y Estrada, C. (2015). Estudio comparativo de portales cautivos basados en Software libre para autentificar y controlar una red inalámbrica de la escuela Gabriel García Moreno (Bachelor's thesis, Riobamba: Universidad Nacional de Chimborazo, 2015).

Albujar, O. (2017). DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED BASADO EN LA INTEGRACIÓN DE LOS SERVIDORES RADIUS - LDAP EN LINUX PARA FORTALECER EL ACCESO DE LA RED DE LA CLÍNICA MILLENIUM CHICLAYO 2016 (Trabajo de titulación). Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

Aldana, M. (2006). Redes complejas. Recuperado a partir de http://www. fis. unam. mx/~ max/English/notasredes. pdf.

Amaya, E. (2018). Introducción a las redes, necesidad de una red, tipo y equipos de redes, topología de una red, diseño de redes, instalación y administración de redes LAN. (Monografía de Licenciatura). Universidad Nacional de Educación Enrique Guzmán y Valle, Lima, Perú.

Andrade, L. (2019). Diseño y simulación de portal cautivo, que permita: autenticación, aplicación de herramientas, políticas de seguridad, QoS y sonda de red para el filtrado de contenido mediante equipo UTM en la CISC-CINT (Tesis de titulación). UNIVERSIDAD DE GUAYAQUIL, Ecuador.

Ariganello, E. (2019). Protocolo punto a punto. [Blog]. Recuperado de: https://aprenderedes.com/2019/10/protocolo-punto-a-punto/.

Avellaneda, D. y Chahua, J. (2018). Modelo de una red inalámbrica en la mejora de la calidad de servicio de atención al usuario dentro de la gerencia regional de infraestructura del Gobierno Regional de Junín. Universidad Nacional de Huancavelica, Perú.

Ballesteros, J. y Chaparro, F. (2016). Seguridad en redes inalámbricas de acceso local bajo parámetros de uso de herramientas libres.

Benites, J. A., Choez, D. A., y Espinal, A. G. (2016). Auditoría de Seguridad en Redes Inalámbricas, Soluciones y Recomendaciones

Bermejo, J. (2014) SQL Server: ¿Para qué sirve y cuál es la versión que necesito? recuperado de:https://www.itsitio.com/ar/sql-server-para-que-sirve-y-cual-es-la-version-que-necesito/

Bermúdez Castro, E. (2016). Análisis de Uso y Ventajas de Linset para Auditorias de Redes Inalámbricas con Encriptación WPA y WPA2 (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Teleasoicaciones).

Bernal, G. (2019). ¿Qué es CSS?. Recuperado de: https://www.hostinger.es/tutoriales/que-es-css/

Blas, J. (2017). SEGURIDAD Y CONTROL DEL ACCESO A LAS REDES INALÁMBRICAS EN LA UNSM-T MEDIANTE SERVIDORES DE AUTENTIFICACIÓN RADIUS CON EL USO DE CERTIFICADOS DIGITALES (Tesis de grado). Universitario Universidad Nacional De San Martín, Tarapoto, Perú.

Bosmediano, 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).

Cano, J. (2016). Evaluación de tecnologías inalámbricas de área personal. (Tesis doctoral). Universidad de Málaga, España.

Casillas y Gallardo. (2013). Análisis, Diseño y propuesta de implementación de un portal cautivo para la red inalámbrica de la Universidad Politécnica Salesiana sede Quito campus Sur. (Tesis de pregrado). Universidad Politécnica Salesiana sede Quito. Ecuador.

Casillas y Gallardo. (2016). Implementación y configuración de un servidor cautivo utilizando herramientas de software libre (Linux) para mejorar el acceso a la red inalámbrica en

el laboratorio de redes de la carrera de ingeniería en informática y sistemas computacionales de la universidad técnica de Cotopaxi durante el periodo 2015. (Tesis de pregrado). Universidad Técnica de Cotopaxi, Ecuador.

Castro, C. y Eras, G. (2017). ANÁLISIS DE FACTIBILIDAD PARA LA CONFIGURACION DEL PROTOCOLO DIAMETER EN LOS SERVIDORES DE TELEFONIA IP ELASTIX PARA EL CIFRADO DE PAQUETES DE VOZ Y AUTENTICACIÓN CASO DE ESTUDIO: EMPRESAS QUE TENGAN INTEGRADA LA CENTRAL DE TELEFONIA IP ELASTIX. (Proyecto de Titulación). Universidad de Guayaquil. Guayaquil, Guayaquil, Ecuador.

Cervera, R. (2014). Métodos y técnicas de investigación internacional. Recuperado de: https://www. ucm. es/data/cont/docs/247-2013-09-26-metodosytecnicas_rafaelcalduch2013_2014. pdf.

Chalen y Plúas. (2017). Propuesta tecnológica de un portal cautivo, bajo pila ipv6 y transmisión de datos mediante li-fi. (Tesis de pregrado). Universidad de Guayaquil. Ecuador.

Chalen, G., & Plúas, M. (2017). PROPUESTA TECNOLÒGICA DE UN PORTAL CAUTIVO, BAJO PILA IPV6 Y TRANSMISIÒN DE DATOS MEDIANTE Li-Fi (Tesis de titulación). UNIVERSIDAD DE GUAYAQUIL, Ecuador.

Chérigo, R. (2017). PORTAL CAUTIVO PARA REDES PRIVADAS (Trabajo de titulación). Universidad Metropolitana de Educación, Ciencia y Tecnología, Panamá, Panamá.

Cruz, M. & Velásquez, R. (2015). Construcción de una página web con PHP y LATEX para el aprendizaje de las matemáticas. BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA, México.

De León, A. (2019). Servidor de Correo: ¿Qué es? ¿Para qué sirve?. [Blog post]. Recuperado de: https://blog.infranetworking.com/servidor-de-correo/#:~:text=Un%20servidor%20de%20correo%20es,recepci%C3%B3n%20y%20reenv%C3%ADo%20de%20correos.

Delgado y Díaz, (2018). Rediseño de la red inalámbrica de la Unidad Educativa Mundial para la ampliación de cobertura utilizando hotspot con control de acceso. Recuperado de:

http://repositorio.ug.edu.ec/bitstream/redug/32990/1/B-CINT-PTG-N.323%20Delgado%20Carre%C3%B1o%20Kiara%20Mily%20.%20Diaz%20Solis%20Steven%20David.pdf.

Egan, K., & Judson, G. (2018). Educación imaginativa: Herramientas cognitivas para el aula (Vol. 214). Narcea Ediciones.

Espinoza, G. (2019). Así es el uso de Internet en Ecuador. Recuperado de: https://www.expreso.ec/ciencia-y-tecnologia/internet-ecuador-479.html.

Ferigra, C. (2017). Propuesta de diseño de una red de datos móviles con la solución WiFi Offload complementaria a las redes UMTS y LTE, que permita brindar servicio de internet a usuarios móviles a través de un acceso WiFi (Trabajo de titulación). Universidad Católica de Santiago de Guayaquil, Guayaquil, Ecuador.

Fidias, G. (2014). El proyecto de investigación. Caracas, Venezuela: Episteme.

González Paz, A., Beltrán Casanova, D., y Fuentes Gari, E, (2016). Propuesta de protocolos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos. Scielo,8(4), 128-135. Recuperado de: https://search.scielo.org/?lang=es&count=15&from=0&output=site&sort=&format=summary&fb=&page=1&q=PROPUESTA+DE+PROTOCOLOS+DE+SEGURIDAD+PARA+LA+RED+INAL%C3%81MBRICA+LOCAL+DE+LA+UNIVERSIDAD+DE+CIENFUEGOS

Guarino, L. (2017). Servidor Web IIS en Windows Server 2016. Recuperado de https://luigiasir.files.wordpress.com/2017/11/servidorwebiis_luigi.pdf

Guerra, V. (2019). Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil. (Tesis de pregrado). Universidad Catolica de Santiago de Guayaquil, Ecuador.

Hamano, T. (2016). Por qué escoger Visual Studio como IDE. Recuperado de:https://stories.devacademy.la/por-qu%C3%A9-escoger-visual-studio-como-ide-3be274236279

Hincapié, S. (2014). Métodos, Tipos y enfoques de investigación. Recuperado de: http://sanjahingu.blogspot.com/2014/01/metodos-tipos-y-enfoques-de.html

Intelectual e industria. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica,3(1), 47-50.

Jijon, M. y Rojas, S. (2017). ANÁLISIS DE FACTORES QUE INFLUYEN EN LA TRANSMISIÓN DEL CABLE DE FIBRA ÓPTICA (Trabajo de Titulación). Escuela Superior Politécnica Del Litoral, Guayaquil, Ecuador.

Latorre, M. (2018). Historia de la web, 1.0, 2.0, 3.0 y 4.0. Universidad Marcelino Champagnat. Perú.

Latorre, M. (2018). Historia de las webs, 1.0, 2.0, 3.0 y 4.0. Universidad Marcelino Champagnat. Perú.

Linares, K. (2017). Cableado UTP - CCNA V6.0 [Mensaje en un blog]. Recuperado de https://kevin-linares.blogspot.com/2017/05/acceso-a-la-red-Medios-de-red-Cableado-UTP.html

López, J. (2017). DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN WI-FI CENTRALIZADO, EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, MEDIANTE ROUTEROS, PARA MEJORAR LA CALIDAD DE SERVICIO. (Tesis de pregrado). Universidad Técnica del Norte, Ecuador.

López. R. (2018). ENRUTAMIENTO Y CONFIGURACIÓN DE REDES. Bogotá, Colombia: Fundación Universitaria del Área Andina.

Lozada, J. (2014). Investigación Aplicada: Definición, Propiedad Intelectual e Industria. Dialnet, 3. (1), 47-50. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6163749

Mantilla, F. (2019). MEDICIÓN DE LATENCIAS DE INTERNET CON SERVIDORES INTERNACIONALES DE CLIENTES DE LA CORPORACIÓN NACIONAL DE LAS TELECOMUNICACIONES (CNT) EN LA CENTRAL ZONAL 5. (tesis de grado). Universidad Católica de Santiago de Guayaquil, Ecuador

Manuel, V. (2017). Itinerancia para la gestión en el acceso inalámbrico de la Universidad Regional Autónoma de Los Andes (Master's thesis).

Marín, R., Zapata, S., & Gómez, A. F. (2007). Protocolo seguro para autenticación rápida en redes inalámbricas basadas en EAP. IEEE LATIN AMERICA TRANSACTIONS, 5(6).

Martín, S. y Lafuente, V. (2017). Referencias bibliográficas: indicadores para su evaluación en trabajos científicos. Investigación bibliotecológica, 31(71), 151-180.

Martínez, F. (2017). Redes Inalámbricas. Recuperado de http://redes-segun-su-cobertura-geografica.blogspot.com/2017/03/redes-inalambricas.html

Maseda, J. (2020). Dispositivos que interactúan en una red inalámbrica. Recuperado de: https://www.kionetworks.com/blog/data-center/dispositivos-de-interconexion-de redes#: ~:text=Un%20dispositivo%20de%20interconexi%C3%B3n%20de, repetidores%20y%20puertas%20de%20enlace.

Maseda, J. (2020). Networking II: Dispositivos de red y tipos de tráfico. Recuperado de: https://itadmins.es/networking-ii-dispositivos-de-red-y-tipos-de-trafico/

Medina, Q. y Layonel, J. (2016). Sistema informático que permita la administración contable de los activos fijos que posee la PUCESE (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).

Mena, D. y Jara, J. (2013). Análisis, diseño y propuesta de implementación de un portal cautivo para la red inalámbrica de la Universidad Politécnica Salesiana Sede Quito Campus Sur. Universidad Politécnica Salesiana Sede Quito, Ecuador.

Mendoza, J. L. y Andrade, L.W. (2016*). Los dispositivos interconectados en el accesode información*. Dominio de las Ciencias, 2(3), 307-322.

Mesa, V. S. A. (2016). IMPLEMENTACIÓN DE UNA RED WLAN QUE PERMITA EL ACCESO A LA INTERNET, A LAS PCS DE TODAS LAS AULAS DE LA ESCUELA FISCAL MIXTA “JOSÉ MARÍA VARGAS” UBICADA EN EL BARRIO DE SANTO DOMINGO DE CONOCOTO. 103. Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/14300/1/CD-6764.pdf

Narváez Pupiales, S. (2015). Estudio de QoS basado en el estándar IEEE 802.11 alternativas de seguridad para las redes locales inalámbricas aplicado en la Wlan de la Universidad Politécnica Estatal del Carchi (Master's thesis, PUCE).

Obando, D (2018). Implantación de un testbed para una red inalámbrica utilizando sdn (open flow). (Tesis de grado). Universidad de las Fuerzas Armadas. Ecuador.

Pei, C., Zhao, Y., Chen, G., Tang, R., Meng, Y., Ma, M., … Pei, D. (2016). WiFi can be the weakest link of round-trip network latency in the wild. IEEE INFOCOM 2016. The 35th Annual IEEE International Conference on Computer Communications, 1-9. doi: 10.1109/INFOCOM.2016.7524396

Pereira, L. G., Camacho, A. P. H., & de la Rosa, Y. A. (2018). Las herramientas tecnológicas TIC s como elemento alternativo para el desarrollo del componente físico. Retos: nuevas tendencias en educación física, deporte y recreación, (34), 222-229.

Pilligua, H. (2013). INTERFACES GRÁFICAS PARA DESARROLLO DE APLICACIONES JAVA EN BLACKBERRY, COMPLEJIDAD DEL DESARROLLO Y PROPUESTA DE AMBIENTE DE DESARROLLO GRÁFICO. UNIVERSIDAD DE GUAYAQUIL, Ecuador.

Portilla, G., Latorre, C., Pozo, P., González, A., y de Computadores, R. (2017). Proyecto: Seguridad en Redes Wifi. Repositorio digital.

Prieto, J. (2018). Análisis comparativo del rendimiento de estándares inalámbricos utilizando Opnet Modeler (Componente práctico del examen complexivo). Universidad Católica de Santiago de Guayaquil, Guayaquil, Ecuador.

Quezada, L. (2015). INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES DHCP, DIRECTORIO VIRTUAL, SQUID PROXY, SAMBA Y SERVIDOR DE CORREO ZIMBRA BAJA LA PLATAFORMA DE SOFTWARE LIBRE UBUNTU Y TELEFONÍA IP, PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL NABÓN. (Trabajo de Titulación). UNIVERSIDAD TECNOLÓGICA ISRAEL, Quito, Ecuador.

REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.3 en línea]. <https://dle.rae.es/accesible?m=form> [25 de agosto de 2020].

Reyes, M. (2015). La encuesta. Recuperado de: https://files.sld.cu/bmn/files/2015/01/la-encuesta.pdf.

Riveros, J. (2019). Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín (Tesis para optar el Título Profesional de Ingeniero de Sistemas). Universidad Nacional del Centro del Perú, Huancayo, Perú.

ROJAS, J. y RUÍZ A. (2019). Diseño de una guía de aseguramiento en informática para servidores en entornos Windows con base en la norma ISO 27000 sgsi en las empresas conciving ingenieros s.a.s y arq s.a, sedes Bogotá (Tesis de grado). UNIVERSIDAD COOPERATIVA DE COLOMBIA. Bogotá, Colombia.

Salazar, J. (2016). Redes inalámbricas. Recuperado de: https://upcommons.upc.edu/handle/2117/100918

Sánchez, M., Avendaño, H., Sierra, M., Lara, J., Collazos, C., Montaño, D., Alfonso, B., y Rodríguez, J. (2018). Tecnologías de la Nueva Generación para el Fortalecimiento Empresarial. Bogotá, Colombia: Editorial Universidad Manuela Beltrán.

Sansano, H. (2017). Pruebas sobre sitios web (Trabajo Fin de Grado). Universidad de Alicante, España.

Santa, P. y Feliberto, M. (2010). Metodología de la investigación cualitativa. Caracas, Venezuela: Fedupel.

Schonwald, N, Dempsey, S., & Sullivan, B. (2018). U.S. Patent Application No. 15/959,947.

Segura, M. D. y Pecino, R. M. (2015). Ciberacoso mediante teléfono móvil e Internet en las relaciones de noviazgo entre jóvenes. Comunicar: Revista científica iberoamericana de comunicación y educación, (44), 159-167.

Sequera, M. (2014). Investigación acción: un método de investigación educativa para la sociedad actual. Revista Arjé,10(18), 223-229.

Tafur, C. y Chávez, J. (2018). ANÁLISIS DE PROTOCOLOS DE PROTECCIÓN DE REDES INALÁMBRICAS WI-FI PARA LA DETECCIÓN DE VULNERABILIDADES

FRENTE A POSIBLES ATAQUES QUE ATENTEN CONTRA LA SEGURIDAD DE LA INFORMACIÓN. (Tesis de grado). Universidad Señor de Sipán, Lima, Perú.

Tecnologiagt. (2015). Switch de Core. Guatemala. Recuperado de: https://www.tecnologiagt.com/switch-core

Terán, M. (2015). Dashboard de Ventas y Módulo de Reporteo Web para la Empresa Pinto S.A ubicada en la Ciudad de Quito. UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES, Ecuador.

Tobar, D., Gaitán, H., y Urrego, B., (2016). Calidad del servicio QoS en redes inalámbricas WIFI para la transmisión IPTV y tráfico multimedia. Encuentro Sennova del Oriente Antioqueño, 87-99.

Villagómez, C. (2018). Introducción a wifi (802.11 o WiFi). Recuperado de https://es.ccm.net/contents/789-introduccion-a-wifi-802-11-o-wifi

VII. ANEXOS

Anexo 1: Certificado o Acta del perfil de Investigación

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: Piarpuezán López Jefferson Alexander **CÉDULA DE IDENTIDAD:** 0401720065
NIVEL/PARALELO: 0 **PERIODO ACADÉMICO:** Nov 2020-Mar 2021

TEMA DE INVESTIGACIÓN: Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. Lascano Rivera Samuel Benjamin
LECTOR: MSC. Guano Cardenas Carlitos Alberto
ASESOR: MSC. Del Hierro Mosquera Milton Gabriel

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: martes, 16 de marzo de 2021
HORA: 10H00
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 5,10
2) Trabajo escrito 2,47
Nota final de PRE DEFENSA **7,57**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el martes, 16 de marzo de 2021

Firmado electrónicamente por:
SAMUEL BENJAMIN LASCANO RIVERA

MSC. Lascano Rivera Samuel Benjamin
PRESIDENTE

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.03.16 18:18:35 -05'00'
MSC. Del Hierro Mosquera Milton Gabriel
TUTOR

Firmado digitalmente por CARLITOS ALBERTO GUANO CARDENAS
MSC. Guano Cardenas Carlitos Alberto
LECTOR

Adj.: Observaciones y recomendaciones

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: Riascos Ortiz Dany Alexander **CÉDULA DE IDENTIDAD:** 0401819164
NIVEL/PARALELO: 0 **PERIODO ACADÉMICO:** Nov 2020-Mar 2021

TEMA DE INVESTIGACIÓN: Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. Lascano Rivera Samuel Benjamin
LECTOR: MSC. Guano Cardenas Carlitos Alberto
ASESOR: MSC. Del Hierro Mosquera Milton Gabriel

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: martes, 16 de marzo de 2021
HORA: 10H00
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 5,20
2) Trabajo escrito 2,47
Nota final de PRE DEFENSA **7,67**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el martes, 16 de marzo de 2021

Firmado electrónicamente por:
SAMUEL BENJAMIN LASCANO RIVERA

MSC. Lascano Rivera Samuel Benjamin
PRESIDENTE

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.03.16 18:17:09 -05'00'
MSC. Del Hierro Mosquera Milton Gabriel
TUTOR

Firmado digitalmente por CARLITOS ALBERTO GUANO CARDENAS
MSC. Guano Cardenas Carlitos Alberto
LECTOR

Adj.: Observaciones y recomendaciones

Anexo 2: Certificado de Abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Piarpuezán López Jefferson Alexander y Riascos Ortiz Dany Alexander
DATE: 22 de marzo de 2021

TOPIC: "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020"
REMARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐

TOTAL/AVERAGE
9 - 10: EXCELLENT
7 - 8,9: GOOD
5 - 6,9: AVERAGE
0 - 4,9: LIMITED

TOTAL 9

1

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Piarpuezán López Jefferson Alexander y Riascos Ortiz Dany Alexander
Fecha de recepción del abstract: 22 de marzo de 2021
Fecha de entrega del informe: 22 de marzo de 2021

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

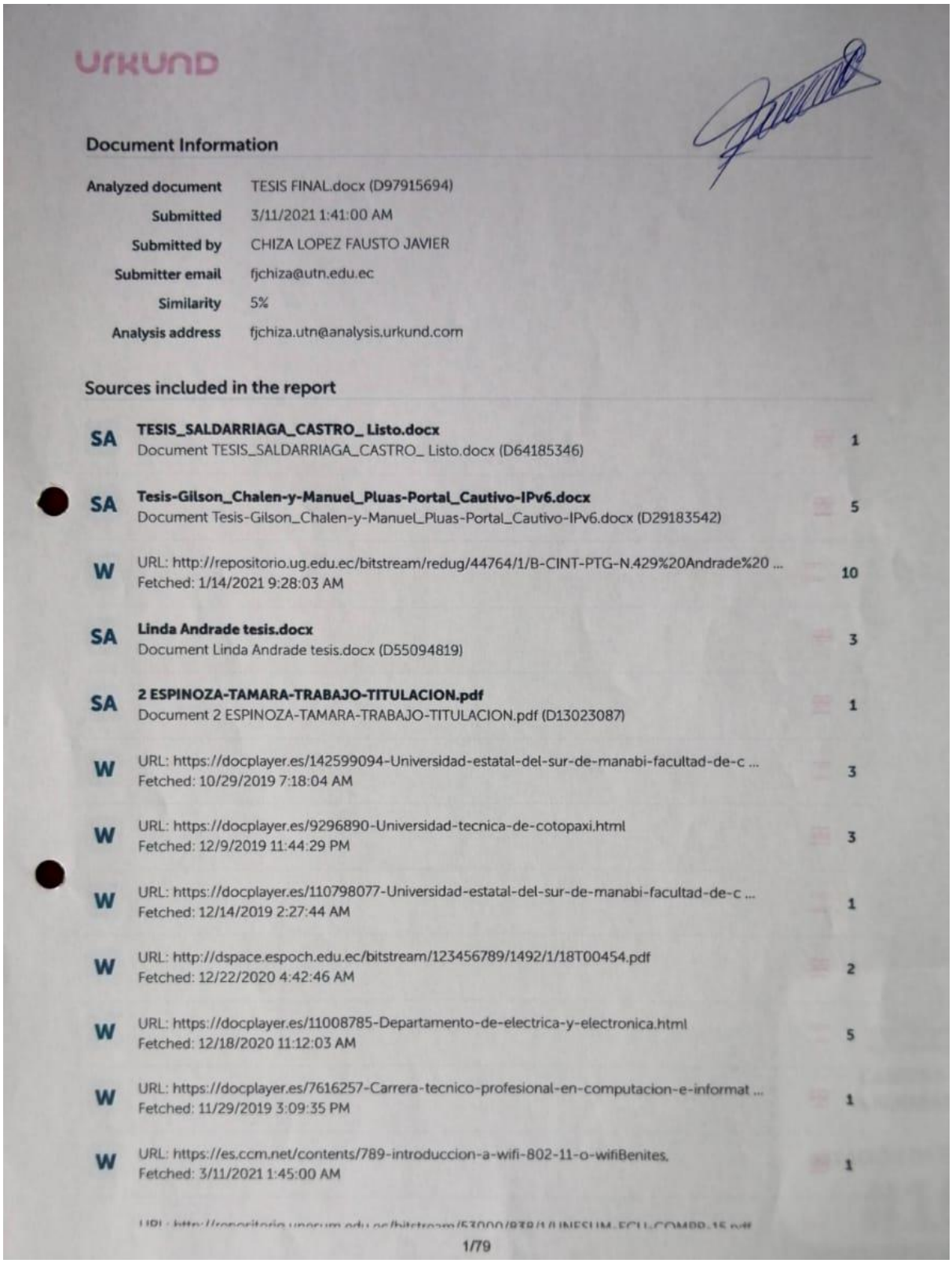
Observaciones:
Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

Firmado electrónicamente por:
EDISON BOANERGES
PENAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3: Informe de Originalidad



URKUND

Document Information

Analyzed document	TESIS FINAL.docx (D97915694)
Submitted	3/11/2021 1:41:00 AM
Submitted by	CHIZA LOPEZ FAUSTO JAVIER
Submitter email	fjchiza@utn.edu.ec
Similarity	5%
Analysis address	fjchiza.utn@analysis.urkund.com

Sources included in the report

SA	**TESIS_SALDARRIAGA_CASTRO_ Listo.docx** Document TESIS_SALDARRIAGA_CASTRO_ Listo.docx (D64185346)	1
SA	**Tesis-Gilson_Chalen-y-Manuel_Pluas-Portal_Cautivo-IPv6.docx** Document Tesis-Gilson_Chalen-y-Manuel_Pluas-Portal_Cautivo-IPv6.docx (D29183542)	5
W	URL: http://repositorio.ug.edu.ec/bitstream/redug/44764/1/B-CINT-PTG-N.429%20Andrade%20 ... Fetched: 1/14/2021 9:28:03 AM	10
SA	**Linda Andrade tesis.docx** Document Linda Andrade tesis.docx (D55094819)	3
SA	**2 ESPINOZA-TAMARA-TRABAJO-TITULACION.pdf** Document 2 ESPINOZA-TAMARA-TRABAJO-TITULACION.pdf (D13023087)	1
W	URL: https://docplayer.es/142599094-Universidad-estatal-del-sur-de-manabi-facultad-de-c ... Fetched: 10/29/2019 7:18:04 AM	3
W	URL: https://docplayer.es/9296890-Universidad-tecnica-de-cotopaxi.html Fetched: 12/9/2019 11:44:29 PM	3
W	URL: https://docplayer.es/110798077-Universidad-estatal-del-sur-de-manabi-facultad-de-c ... Fetched: 12/14/2019 2:27:44 AM	1
W	URL: http://dspace.espoch.edu.ec/bitstream/123456789/1492/1/18T00454.pdf Fetched: 12/22/2020 4:42:46 AM	2
W	URL: https://docplayer.es/11008785-Departamento-de-electrica-y-electronica.html Fetched: 12/18/2020 11:12:03 AM	5
W	URL: https://docplayer.es/7616257-Carrera-tecnico-profesional-en-computacion-e-informat ... Fetched: 11/29/2019 3:09:35 PM	1
W	URL: https://es.ccm.net/contents/789-introduccion-a-wifi-802-11-o-wifiBenites. Fetched: 3/11/2021 1:45:00 AM	1

URL: http://repositorio.unorum.edu.pe/bitstream/53000/838/1/UNFSUM-FCLL-COMPP-15.pdf

1/79

Anexo 4: Oficio y recibido para la obtención de información en TIC's

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No.2006-36. Publicada en el Segundo Suplemento del el Registro oficial No. 244 del 5 de abril del 2006

Fecha: *Tulcán, 17 de diciembre del 2019*

Señor(a):
MSc.Jhony Enríquez Herrera
DIRECTORA DEL CENTRO DE TIC'S

Presente.

De mi consideración

Yo, *Jefferson Alexander Piarpuezan López* CC *0401720065*.

Estudiante de la Facultad de *Industrias Agropecuarias y Ciencias Ambientales* Carrera de *Ingeniería en Informática* Semestre: *Noveno* Paralelo *A*

Jornada *Matutina* a usted comedidamente solicito: *se autorice a quien corresponda determinar la factibilidad del desarrollo del plan de investigación denominado "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020*.

Por la favorable atención que se digne dar al presente, anticipo mi agradecimiento

Atentamente,

Observaciones: Se ha determinado factible el trabajo de Investigación

Resolución: Se Autoriza la ejecución del mismo

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No.2006-36. Publicada en el Segundo Suplemento del el Registro oficial No. 244 del 5 de abril del 2006

Fecha: *Tulcán, 17 de diciembre del 2019*

Señor(a):

MSc.Jhony Enríquez Herrera

DIRECTORA DEL CENTRO DE TIC'S

Presente.

De mi consideración

Yo, *Dany Alexander Riascos Ortiz* CC *0401819164*

Estudiante de la Facultad de *Industrias Agropecuarias y Ciencias Ambientales* Carrera de *Ingeniería en Informática* *Semestre* *Noveno* Paralelo *A*

Jornada *Matutina* a usted comedidamente solicito: *se autorice a quien corresponda determinar la factibilidad del desarrollo del plan de investigación denominado "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020*.

Por la favorable atención que se digne dar al presente, anticipo mi agradecimiento

Atentamente,

Observaciones: *Se ha determinado factible el trabajo de investigación*

Resolución: *Se Autoriza la ejecución del mismo*

Anexo 5: Encuesta realizada a los estudiantes de comunidad universitaria

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

ENCUESTA SOBRE SATISFACCIÓN DE LA RED INALÁMBRICA.

Objetivo: La presente encuesta se genera previo a la obtención del título en ingeniería en informática, la misma que tiene como objetivo conocer la situación actual del servicio que se brinda mediante la red datos inalámbrica de la UPEC.

Por favor, Señale la respuesta que usted crea conveniente.

1. ¿Con qué frecuencia usted hace uso del servicio de internet dentro de la Universidad?

   ☐ Siempre ☐ Casi Siempre ☐ Rara vez ☐ Nunca

2. ¿Con qué frecuencia usted se conecta a la red inalámbrica WiFi que provee la Universidad? (Si su respuesta es nunca puede dar por terminada la encuesta)

   ☐ Siempre ☐ Casi Siempre ☐ Rara vez ☐ Nunca

3. ¿Al estar conectado a la red inalámbrica WiFi cuantos dispositivos utiliza simultáneamente para su navegación?

   ☐ 1 ☐ 2 ☐ 3 ☐ 4

4. ¿Al conectarse al internet inalámbrico de la Universidad cuál de los siguientes dispositivos a utilizado? (La respuesta puede ser más de uno)

   ☐ Celular ☐ Tablet ☐ Laptop ☐ Otros

5. ¿Qué uso le da usted al internet inalámbrico dentro del campus universitario? (La respuesta puede ser más de uno)

   ☐ Educativos ☐ Entretenimiento ☐ Descargas ☐ Otros

6. ¿Cuándo usted se conecta al WiFi, de la Universidad desde cualquier lugar de las instalaciones su conexión y el tiempo que dura la misma es totalmente satisfactoria?

   ☐ Siempre ☐ Casi Siempre ☐ Rara vez ☐ Nunca

7. ¿Con qué frecuencia usted presenta problemas para conectarse a la red inalámbrica WiFi de la Universidad?

   ☐ Siempre ☐ Casi Siempre ☐ Rara vez ☐ Nunca

8. ¿Con que frecuencia ha sufrido problemas de conexión, los mismos que han influido negativamente en actividades académicas como pruebas online, consulta de información, entre otras?

   ☐ Siempre ☐ Casi Siempre ☐ Rara vez ☐ Nunca

9. ¿Cuál es el rango de tiempo que usted invierte en el servicio de internet inalámbrico WiFi de la Universidad?

   ☐ 1 - 15min ☐ 16–30min ☐ 31-45min ☐ +de45 min

10. ¿Cuán satisfactoria fue la velocidad con la que navegó al utilizar el servicio de internet inalámbrico de la Universidad?

    ☐ Excelente ☐ Bueno ☐ Regular ☐ Malo

11. ¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico?

    ☐ Excelente ☐ Bueno ☐ Regular ☐ Malo

12. ¿Estaría de acuerdo con la implementación de una herramienta tecnológica que permita mejorar la accesibilidad al contenido web dentro de la red inalámbrica de la Universidad?

    ☐ Totalmente de acuerdo ☐ De acuerdo

    ☐ Indeciso ☐ En desacuerdo

Anexo 6: Análisis de datos de encuesta

1. ¿Con qué frecuencia usted hace uso del servicio de internet dentro de la Universidad?

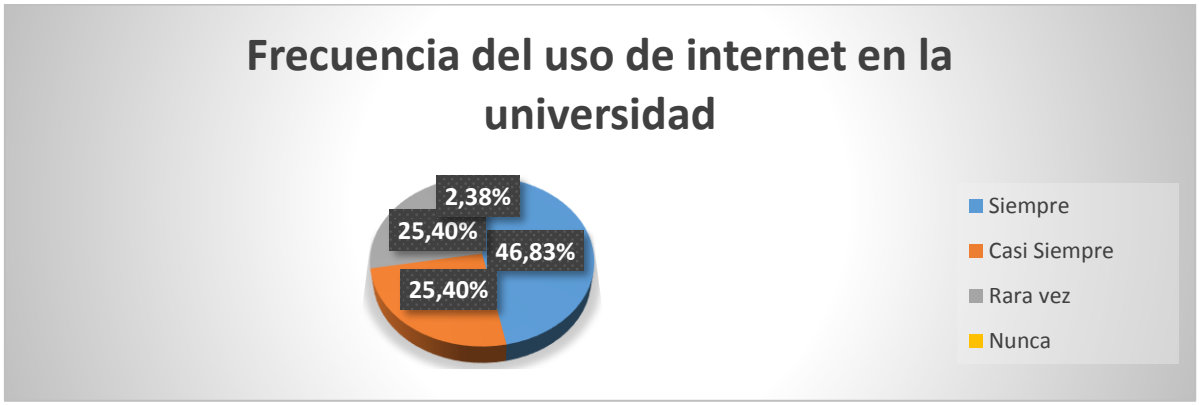


Figura 53. Pregunta 1

El grafico representa que un 46,83% de los estudiantes de la Universidad utiliza siempre el internet dentro de la Universidad, siendo no necesariamente el facilitado por la institución, el 25,40% de los encuestados afirman que lo utilizan casi siempre, el 25,40% lo utiliza rara vez y finalmente el 2,38% sobrante no utiliza el internet en la institución, lo que representa que más de la mitad de los estudiantes utilizan el WiFi que facilita la Universidad para tener acceso a internet.

2. ¿Con qué frecuencia usted se conecta a la red inalámbrica WiFi que provee la Universidad? (Si su respuesta es nunca puede dar por terminada la encuesta)

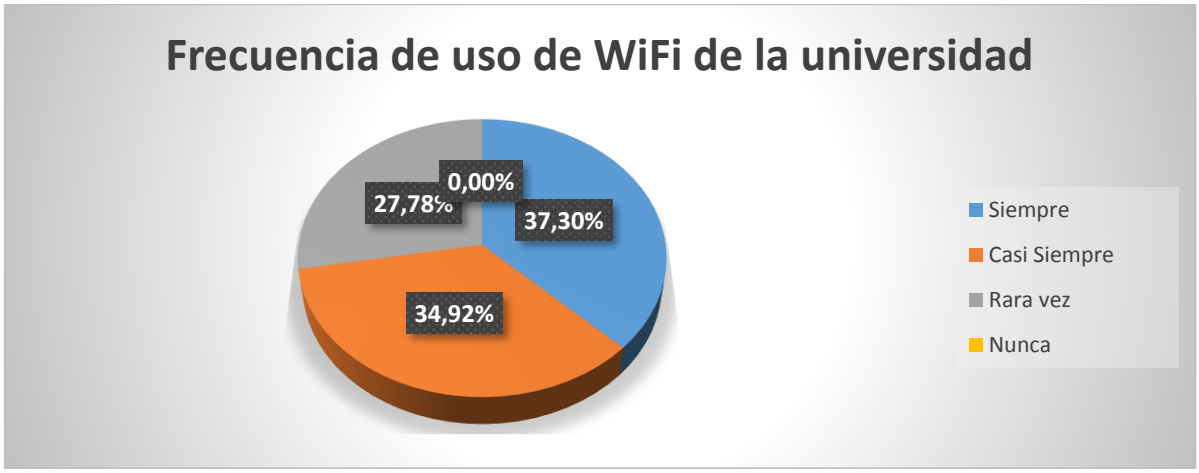


Figura 54. Pregunta 2

El gráfico representa que el 37,30% de los estudiantes encuestados hace uso constante del internet inalámbrico de la Universidad, el 34,92% se conecta casi siempre y el 27,78% rara vez,

lo que muestra que los estudiantes utilizan el internet inalámbrico de la Universidad, para acceder al contenido en la red.

3. ¿Al estar conectado a la red inalámbrica WiFi cuantos dispositivos utiliza simultáneamente para su navegación?

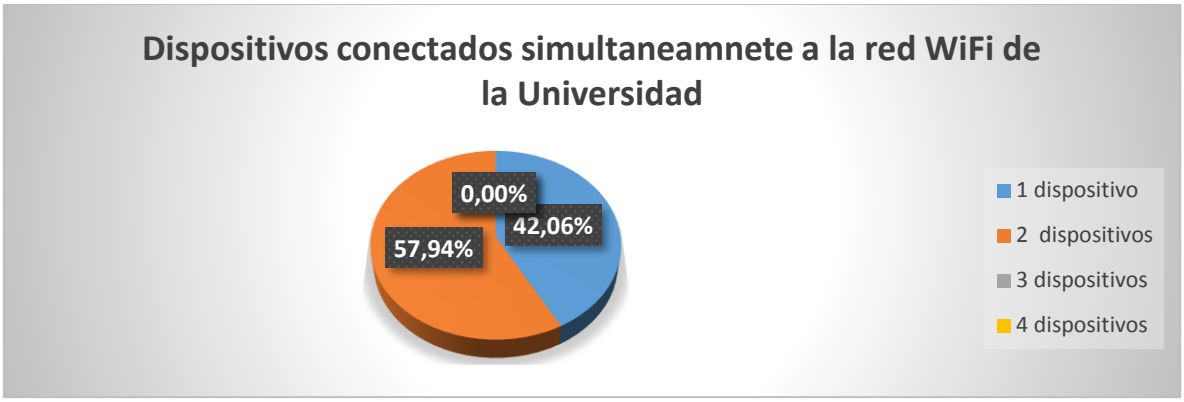


Figura 55. Pregunta 3

La representación gráfica muestra que el 57,94% de los estudiantes encuestados utiliza dos dispositivos para el acceso a internet inalámbrico y el 42,06% utiliza solo uno, lo que conlleva a que la red genere latencia y presente dificultades para acceder al contenido web en internet.

4. ¿Al conectarse al internet inalámbrico de la Universidad cuál de los siguientes dispositivos a utilizado? (La respuesta puede ser más de uno)

Figura 56. Pregunta 4

El gráfico representa que el 51,42% de los estudiantes encuestados utiliza el celular para acceder al WiFi de la Universidad, el 43,13% utiliza laptops y el 5,45% utiliza tabletas. Logrando identificar que los porcentajes de la utilización de celulares y tables son parejos, quedando en evidencia que se los utiliza de forma simultánea, siendo atípico para lo académico

no se necesita más de un dispositivo y esto refleja que el otro equipo se utiliza para otras acciones que no tienen que ver con los estudios.

5. ¿Qué uso le da usted al internet inalámbrico dentro del campus universitario? (La respuesta puede ser más de uno)

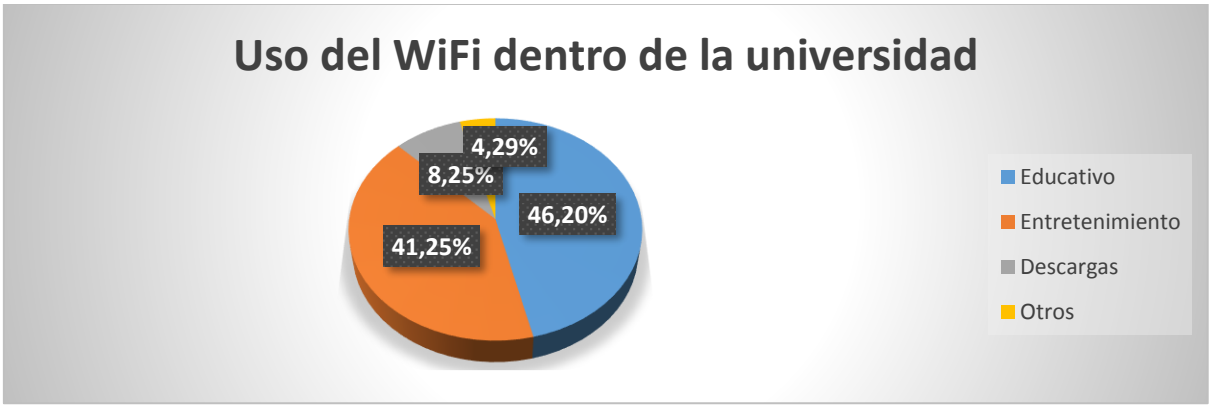


Figura 57. Pregunta 5

El gráfico representa que el 46,20% de los estudiantes encuestados utiliza el internet inalámbrico de la Universidad para fines académicos, el 41,25% lo utiliza para entretenimiento, el 8,25% lo utiliza para descargas y el 4,29% restante lo utiliza para otros fines. Lo que representan estos datos es que el internet inalámbrico en un porcentaje no tan alejado de la mitad es utilizado para entretenimiento, conllevando a generar latencia de estas páginas consumen mayor ancho de banda que las painas que son destinadas para lo académico.

6. ¿Cuándo usted se conecta al WiFi, de la Universidad desde cualquier lugar de las instalaciones su conexión y el tiempo que dura la misma es totalmente satisfactoria?

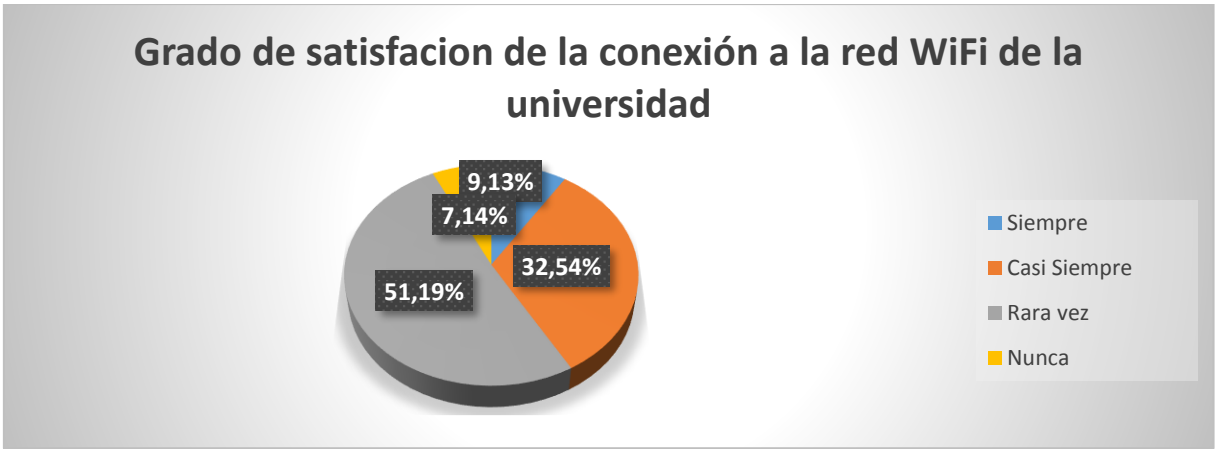


Figura 58. Pregunta 6

El análisis del gráfico indica que el 9,13% de los encuestados tiene siempre una conexión exitosa y satisfactoria, el 32,54% afirma que eso sucede casi siempre, el 51,19% dice que es rara vez y el 7,14% nunca tuvo una experiencia satisfactoria con la red inalámbrica. Esto deja visualizar que la inconformidad es evidente con el servicio, siendo esto por factores como la infraestructura de la Universidad y la distribución de Access Points en la institución.

7. ¿Con qué frecuencia usted presenta problemas para conectarse a la red inalámbrica WiFi de la Universidad?

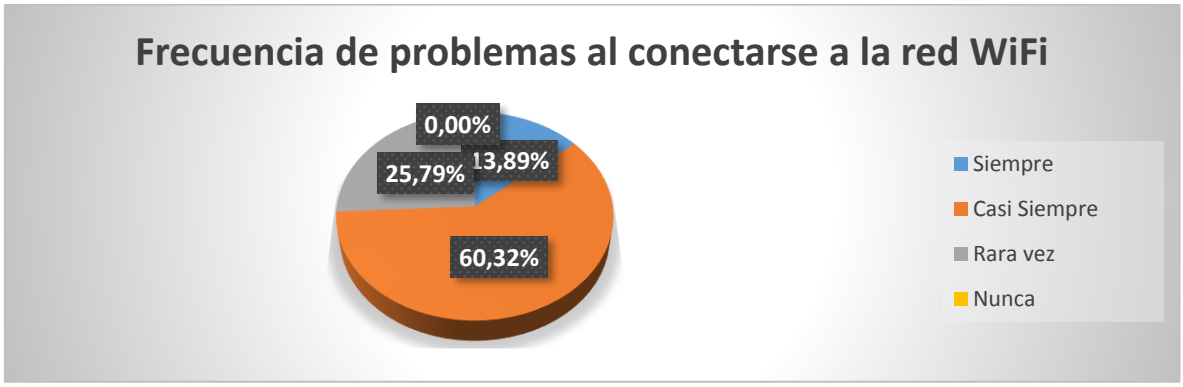


Figura 59. Pregunta 7

El análisis del grafico indica que el 60,32% de los encuestados casi siempre presenta problemas para conectarse al internet inalámbrico de la Universidad, el 25,79% lo presenta rara vez y el 13,89% siempre. Entonces se observa que los porcentajes de problemas para conectarse al WiFi de la Universidad son elevados lo que impide que estos accedan al contenido académico.

8. ¿Con que frecuencia ha sufrido problemas de conexión, los mismos que han influido negativamente en actividades académicas como pruebas online, consulta de información, entre otras?

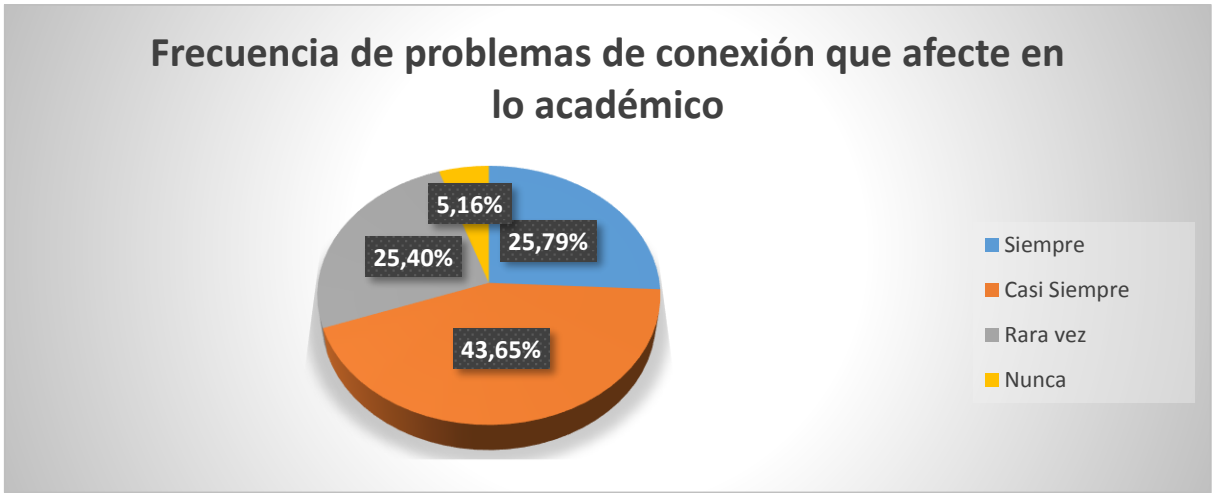


Figura 60. Pregunta 8

El gráfico muestra que el 25,79% de los encuestados presenta problemas constantes de conexión de la red inalámbrica que afecta en el ámbito académico, el 43,65% afirma que esto sucede casi siempre, el 25,40% por su parte muestra que sucede rara vez y el 5,16% restante indica que no afecta en lo académico. Así se logra identificar que son más los estudiantes que se ven afectados en lo académico por el servicio de internet inalámbrico que se brinda, siendo esto un efecto negativo que afecte en el récord académico de los estudiantes.

9. ¿Cuál es el rango de tiempo que usted invierte en el servicio de internet inalámbrico WiFi de la Universidad?

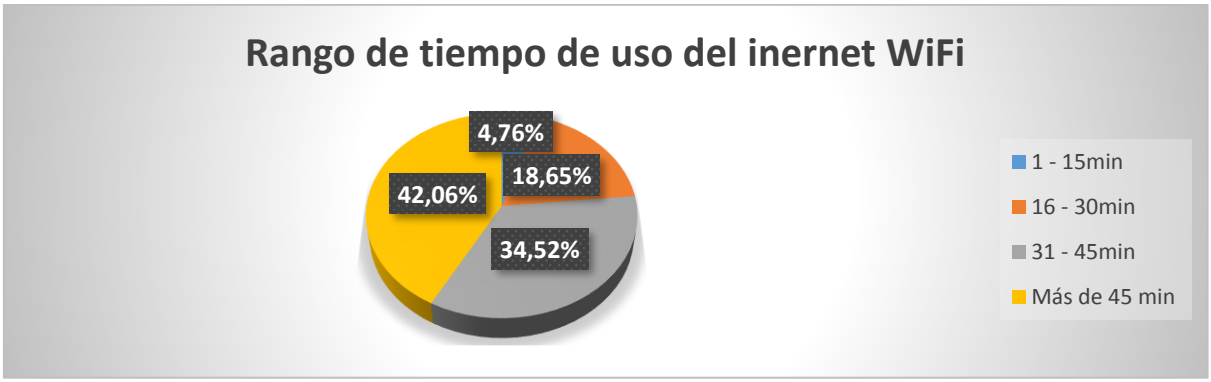


Figura 61. Pregunta 8

El análisis del gráfico indica que los estudiantes en un 42,06% utilizan el internet inalámbrico de la Universidad por más de 45 minutos lo que es algo ilógico puesto que para las actividades académicas no conlleva este tiempo, reflejando que se lo utiliza para acciones aparte de lo académico.

10. ¿Cuán satisfactoria fue la velocidad con la que navegó al utilizar el servicio de internet inalámbrico de la Universidad? (tomar como referencia la pregunta 5)

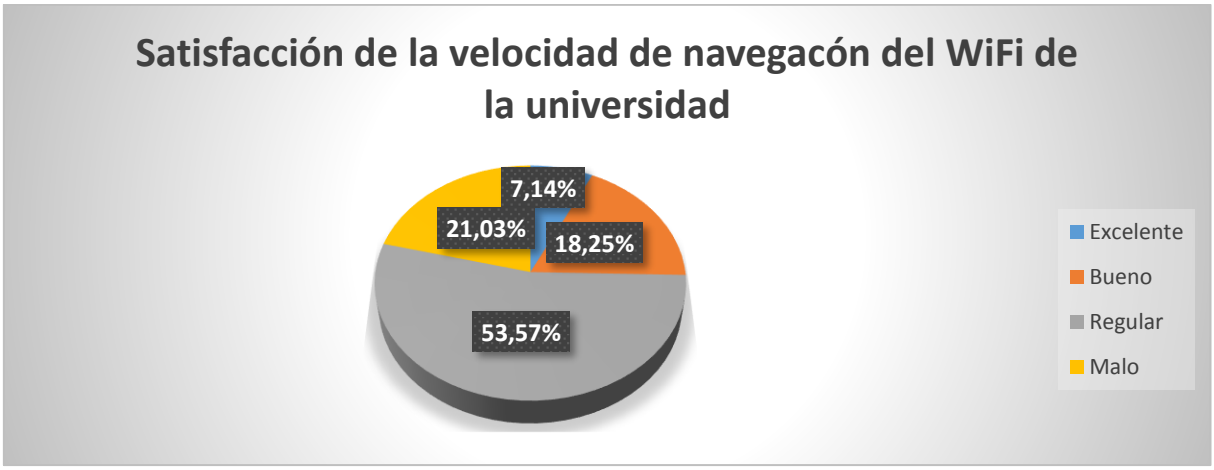


Figura 62. Pregunta 10

El gráfico muestra la satisfacción con la que se navegó dentro de la red inalámbrica de la Universidad, siendo para un 53,57% regular según los estudiantes, con lo que se evidencia un descontento por parte de los estudiantes con la red inalámbrica.

11. ¿Cuál es su grado de satisfacción que le daría al servicio de internet inalámbrico?

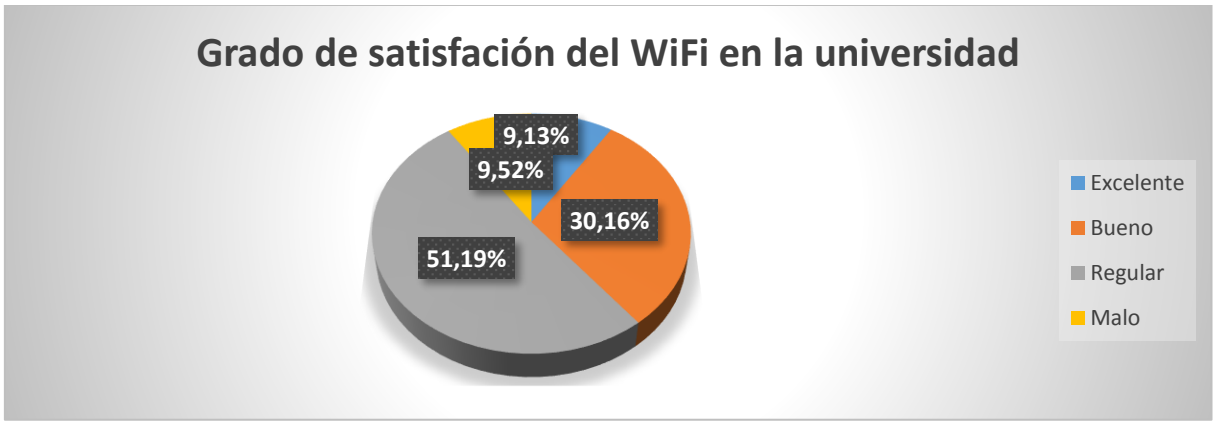


Figura 63. Pregunta 11

El análisis del grafico muestra el grado de satisfacción en general que se le da a la red inalámbrica de la Universidad, siendo considerada excelente por el 9,13%, buena por un 20,165, regular por el 51,19% y mala por el 9,52% restante. Siendo así que la satisfacción de la red inalámbrica para los estudiantes no es considerada óptima para acceder al contenido web.

12. ¿Estaría de acuerdo con la implementación de una herramienta tecnológica que permita mejorar la accesibilidad al contenido web dentro de la red inalámbrica de la Universidad?

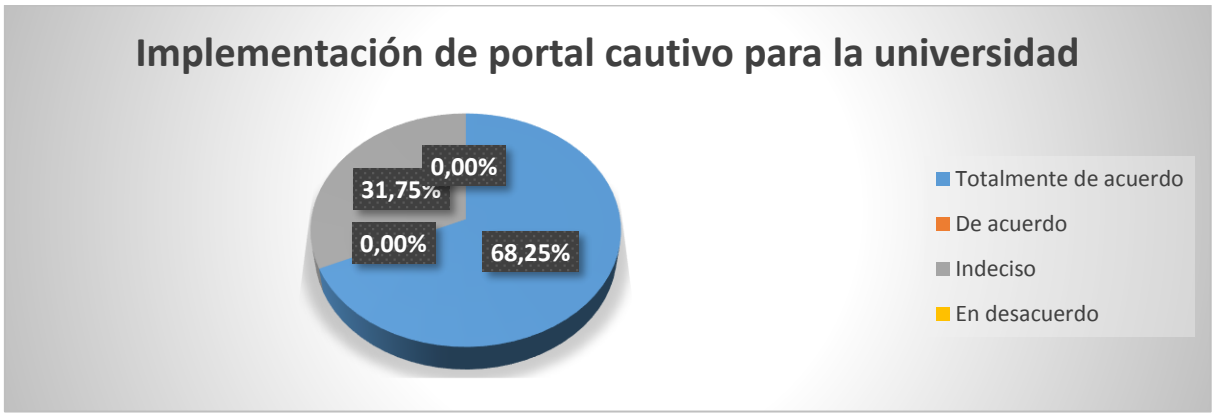


Figura 64. Pregunta 12

El análisis del gráfico muestra que un 68,25% de los estudiantes encuestados está totalmente de acuerdo en que se implemente una herramienta informática en la red inalámbrica de la Universidad para que mejorar la accesibilidad al contenido web.

Anexo 7: Registro fotográfico del área y equipos de trabajo

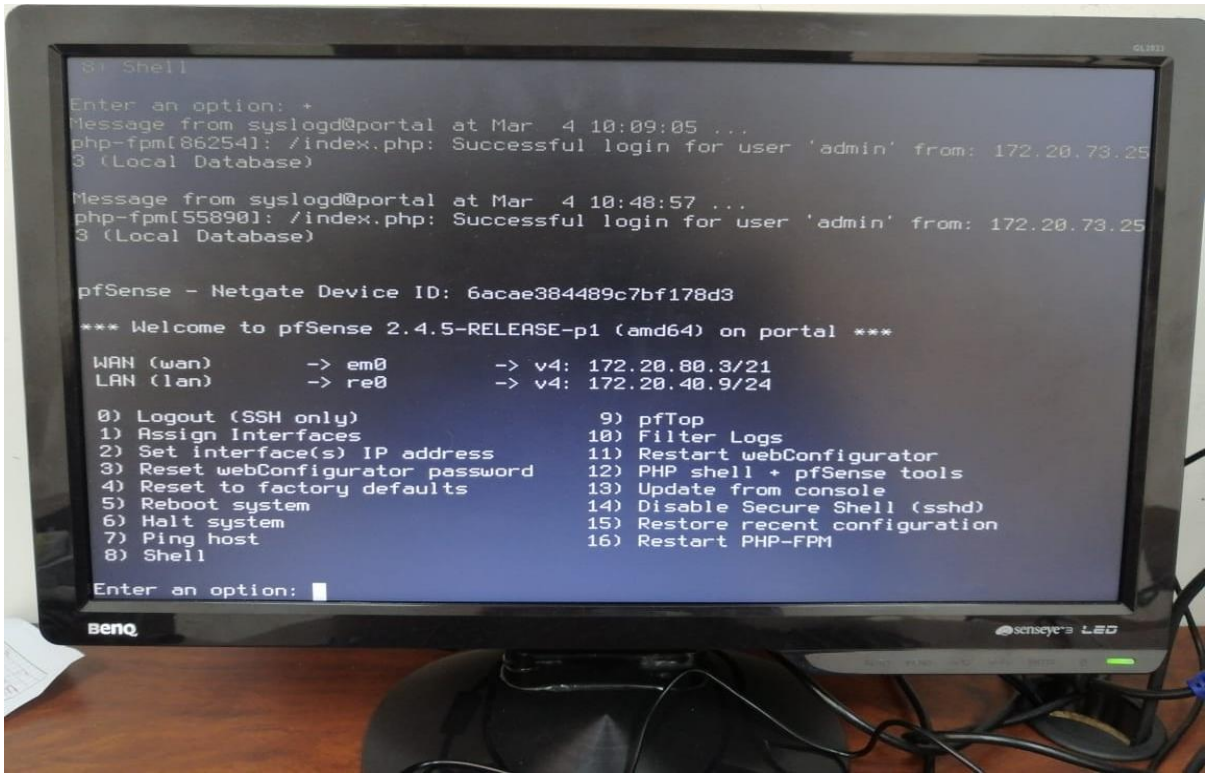


Figura 65. Estado funcional Pfsense

Figura 66. Equipo físico del Portal Cautivo

Figura 67. Área de trabajo 1

Figura 68. Área de Trabajo 2

Anexo 8: Diálogo de entrevista

Entrevistador: ¿EL ancho de banda asignado a las diferentes dependencias es uniforme dentro de los edificios de la Universidad?

Entrevistado: La red universitaria se encuentra segmentada en VLANs, y a cada una se ha asignado un determinado ancho de banda de acuerdo con las necesidades e importancia del tráfico de información a cruzar por la red. Es diferente la información que genera la VLAN destinada para la parte administrativa que la VLAN destinada para el área financiera.

Entrevistador: ¿El ancho de banda que tiene la Universidad es el adecuado para el número de usuarios que posee la institución?

Entrevistado: Primero hay que mencionar que la institución posee un ancho de banda de 600 Mbps de los cuales para la red inalámbrica se le asignado 300Mbs. En cuanto al ancho de banda para los usuario**s** si es el adecuado, pero es necesario la adquisición e implementación de un equipo llamado Balanceador de Carga, el cual permite que el ancho de banda no utilizado por cada VLAN sea asignado a la VLAN que lo requiera.

Name	Target	Upload Max Limit	Download Max Limit
VLAN[redacted]SEVIDORES	[redacted]	20M	30M
VLAN[redacted]TELEFONIA		5M	5M
VLAN[redacted]CAMARAS		20M	20M
VLAN[redacted]CENTRO_TICS		20M	20M
VLAN[redacted]_AUTORIDADES		20M	20M
VLAN[redacted]_FINANCIERO		10M	10M
VLAN[redacted]_ADMINISTRATIVOS		30M	30M
VLAN[redacted]_SALAS_DOCENTES		50M	50M
VLAN[redacted]_DEP_COMUNICACIONES		20M	20M
VLAN[redacted]_DOCENTES_AULAS		100M	100M
VLAN[redacted]_LAB_SERV_INFORMATICA		10M	10M
VLAN[redacted]_CARRERA_INFORMATICA		100M	100M
VLAN[redacted]_LAB_PCS_INFORMATICA		50M	50M
VLAN[redacted]_LAB_INGLES		50M	50M
VLAN[redacted]_LABORATORIOS		20M	20M
VLAN[redacted]_EVENTOS_Y_EDUROAM		300M	300M
VLAN[redacted]_MAESTRIAS		30M	30M
VLAN[redacted]_LAB_EXTRAS		30M	30M
VLAN[redacted]_LAB_INGLES		100M	100M
VLAN[redacted]_LAB_BIBLIOTECA		30M	30M
VLAN[redacted]_LAB_INFORMATICA_1		50M	50M
VLAN[redacted]_LAB_INFORMATICA_2		50M	50M
VLAN[redacted]_LAB_INFORMATICA_3		50M	50M
VLAN[redacted]_LAB_INFORMATICA_4		50M	50M
VLAN[redacted]_LAB_INFORMATICA_5		50M	50M
VLAN[redacted]_LAB_INFORMATICA_6		50M	50M
VLAN[redacted]_LAB_INFORMATICA_7		50M	50M
VLAN[redacted]_LAB_INFORMATICA_8		50M	50M
VLAN[redacted]_LAB_INFORMATICA_9		50M	50M
VLAN[redacted]_LAB_INFORMATICA_10		50M	50M
VLAN[redacted]_LAB_INFORMATICA_11		50M	50M
VLAN[redacted]_LAB_INFORMATICA_12		50M	50M
VLAN[redacted]_LAB_INFORMATICA_13		50M	50M

Figura 69. Distribución de megas en la red

Entrevistador: ¿Conoce usted alrededor de cuántos usuarios se conectan simultáneamente a la red de Inalámbrica de la Universidad?

Entrevistado: Dentro de la red WiFi se tienen aproximadamente 1500 dispositivos conectados, este valor no determina cuantos usuarios debido a que hay la posibilidad de que un usuario pueda conectarse con varios dispositivos: Celular, Tablets, Laptops.

Entrevistador: ¿La institución posee algún software o hardware que controle el número de dispositivos que un usuario puede tener conectado simultáneamente a la red inalámbrica?

Entrevistado: Dentro de la red institucional no poseemos ningún equipo que permita controlar el número de dispositivos a conectarse por cada usuario.

Entrevistador: ¿La cobertura de la red inalámbrica abarca todo el campus universitario?

Entrevistado: La institución posee sectores en los cuales los dispositivos que propagan la red no se encuentran presentes tal es caso del coliseo, la plaza roja, áreas verdes entre otros. Para eliminar este inconveniente se tendría que adquirir antenas bidireccionales, pero al ser costosas la institución no puedo realizar esta compra.

Entrevistado: Dentro de la red institucional no poseemos ningún equipo que nos permita controlar el número de dispositivos a conectarse por cada usuario.

Entrevistador: ¿Se tiene número aproximado de usuarios los cuales puedan conectar simultáneamente a la red y no afectan su rendimiento?

Entrevistado: 2000 serían el número aproximado de dispositivos conectados a la red para que no afecte en el rendimiento y consumo de ancho de banda del internet, pero dentro de la Intranet podríamos superar fácilmente los 5000 usuarios sin tener inconvenientes.

Entrevistador: ¿La Universidad está regulando las páginas web a las cuales los usuarios tienen acceso?

Entrevistado: En este momento no tenemos un equipo que nos permita realizar el control y bloqueo del acceso a los sitios WEB, es decir dentro de la red universitaria se puede acceder a páginas web referentes a cualquier información.

Entrevistador: ¿Ha considerado la restricción de páginas de redes sociales y páginas de videos?

Entrevistado: Más que las páginas de redes sociales y videos, es necesario realizar el bloqueo de páginas de contenido inapropiado (Pornográficas, gestores de descargas, streaming de películas y series, entre otras). Mientras que las páginas de redes sociales (Facebook, WhatsApp, Twitter) y de videos (YouTube) controlar el Ancho de Banda que consumen y son usados para fines académicos.

Entrevistador: ¿Se han generado sugerencias sobre el mejoramiento a la red?

Entrevistado: Claro que sí, se han sugerido muchos cambios los cuales poco a poco se han ido implementando para el mejoramiento de la red en todo sentido, velocidad, seguridad, distribución, segmentación. Pero al ser una institución pública que usa recursos del estado, tenemos grandes inconvenientes en la adquisición de este equipamiento por falta de recursos económicos.

Entrevistador: ¿Qué opina usted de implementar un software open source que ayude en la administración de la red?

Entrevistado: Me parece que la implementación de este software es indispensable porque nos permitirá tener una mejor administración y control en los segmentos de red, permitiéndonos bloquear contenidos y páginas web que no son de uso académico.

Figura 70. Entrevista a personal de TIC's

Anexo 9. Aplicación de encuestas

Figura 71. Aplicación de encuesta 1

Figura 72. Aplicación de encuesta 2

Figura 73. Aplicación de encuesta 3

Figura 74. Aplicación de encuesta 4

Figura 75. Aplicación de encuesta 5

Anexo 10. Pruebas de latencia

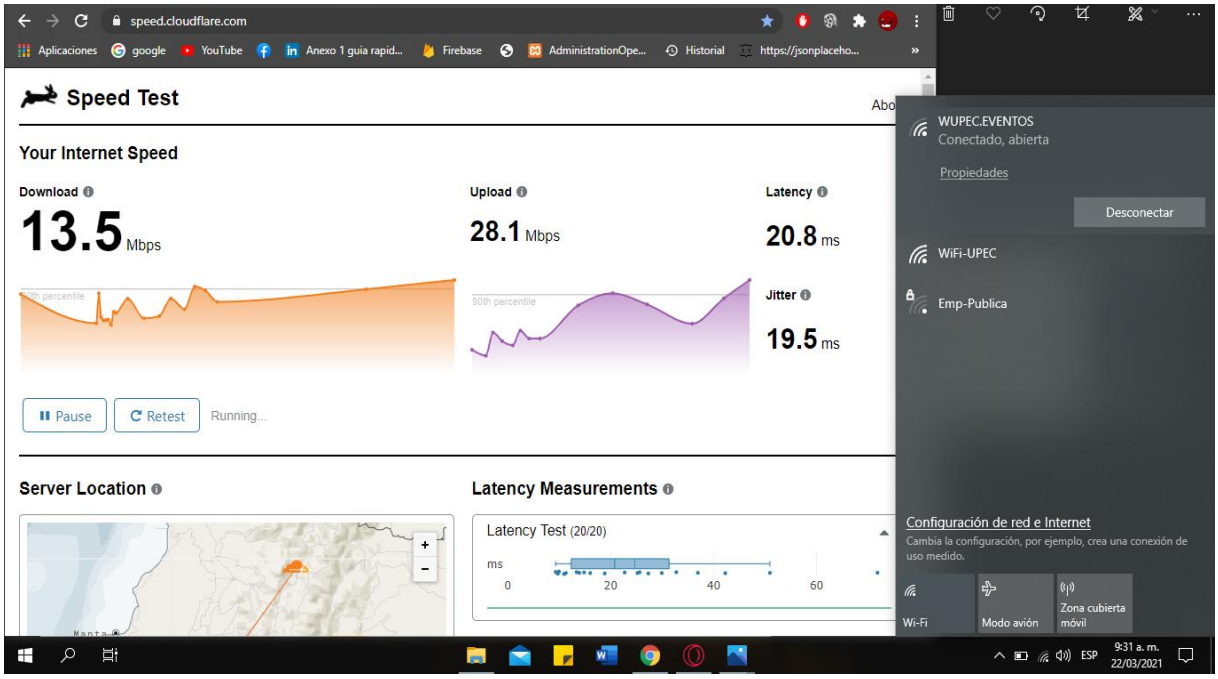


Figura 76. Latencia de la red inalámbrica WUPEC.EVENTOS, marzo 2021

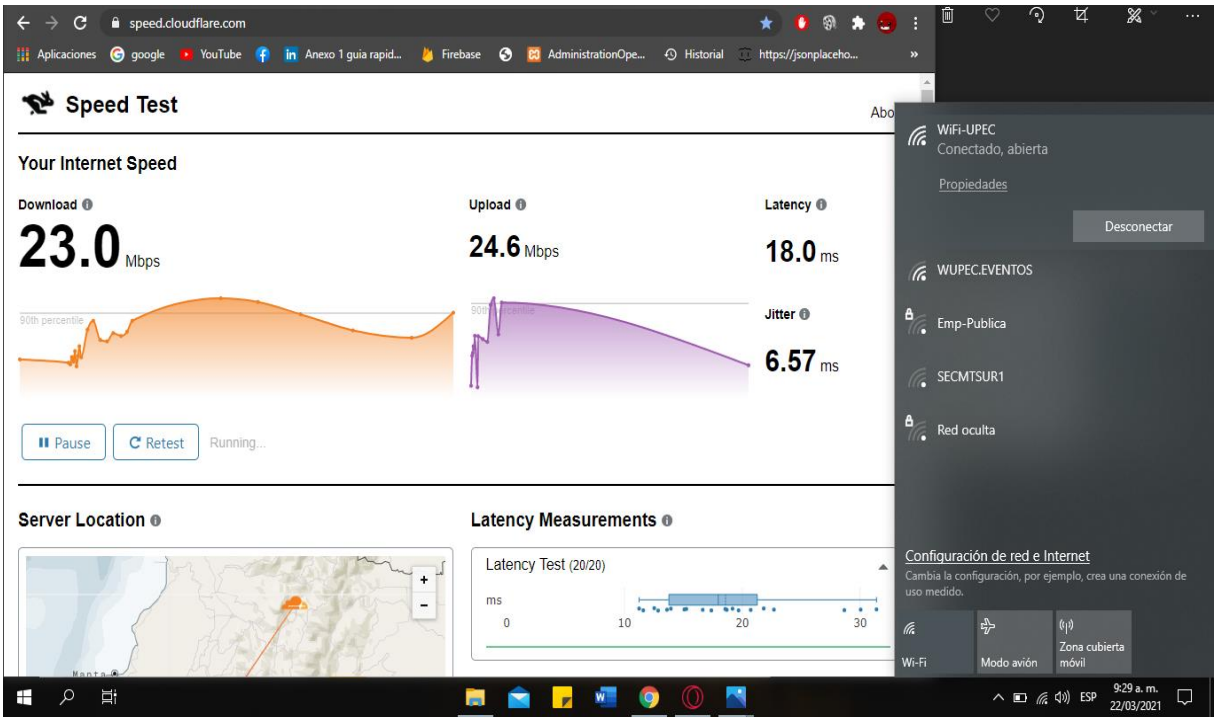


Figura 77. Latencia de la red inalámbrica WiFi-UPEC, marzo 2021

Anexo 11 Acta de finalización del proyecto

ACTA DE FIN DE PROYECTO

La Universidad Politécnica Estatal del Carchi, por medio de la Unidad de Redes y Telecomunicaciones, en su afán de implementar proyectos de tecnología que brinden mejoras sustanciales a los usuarios de la red de datos, ha visto la necesidad de configurar un portal cautivo para el acceso de la comunidad universitaria a la red WiFi.

En base a los requerimientos y características de la red, se sugirió que la implementación cuente con los siguientes parámetros:

- Uso de software libre
- Diseño de página web del portal cautivo para la Universidad
- Bloqueo a páginas Web con contenido inapropiado
- Ingreso de usuarios por credenciales
- Limitar equipos por usuario
- Conexión con Active Directory
- Conexión con Wireless Lan Controller
- Servidores DHCP, DNS, Proxy
- Control y monitoreo de la red inalámbrica
- Portal cautivo

Gracias al apoyo de los estudiantes de la carrera de Ingeniería en Informática de la Universidad, se ha podido plasmar este portal cautivo el cual permite:

- Bloquear el acceso a páginas web con contenido inapropiado, dentro de la red WiFi Universitaria.
- Permitir el acceso de un solo dispositivo electrónico a la red WiFi, por parte de los diferentes usuarios de la misma por medio de credenciales.
- Monitorear el rendimiento de la red WiFi

Este trabajo se lo realizó bajo el tema de titulación: "Portal Cautivo para la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020", realizado por los estudiantes

Educamos para transformar el mundo

Riascos Ortiz Dany Alexander con C.C.: 040181916-4 y Piarpuezán López Jefferson Alexander con C.C.: 040172006-5

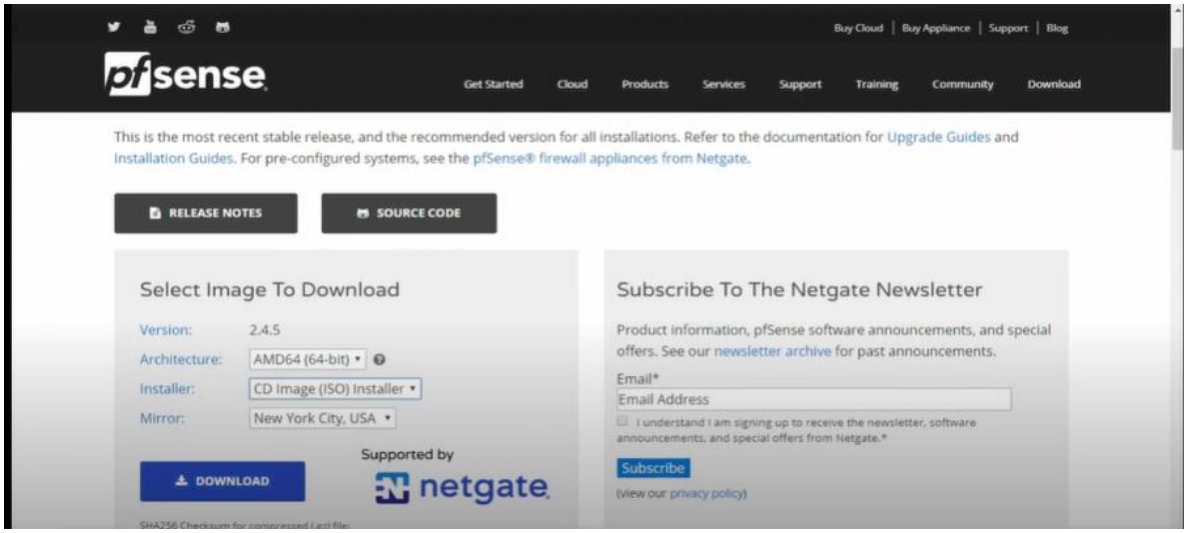
Para los fines pertinentes, me suscribo.

Ing. Andrés Zabala Villarreal MSc.
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexo 12. Manual de Configuración

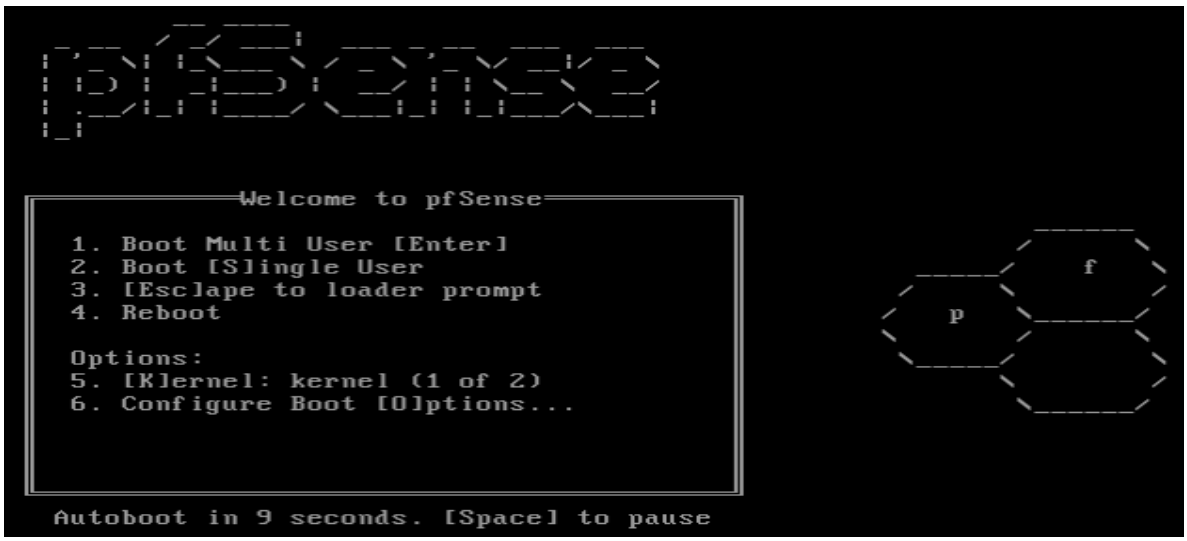
Instalación Pfsense

Para hacer posible la instalación del Firewall se debe bootear una USB con el S.O. de Pfsense descargado de la página oficial.



Sitio oficial de Pfsense

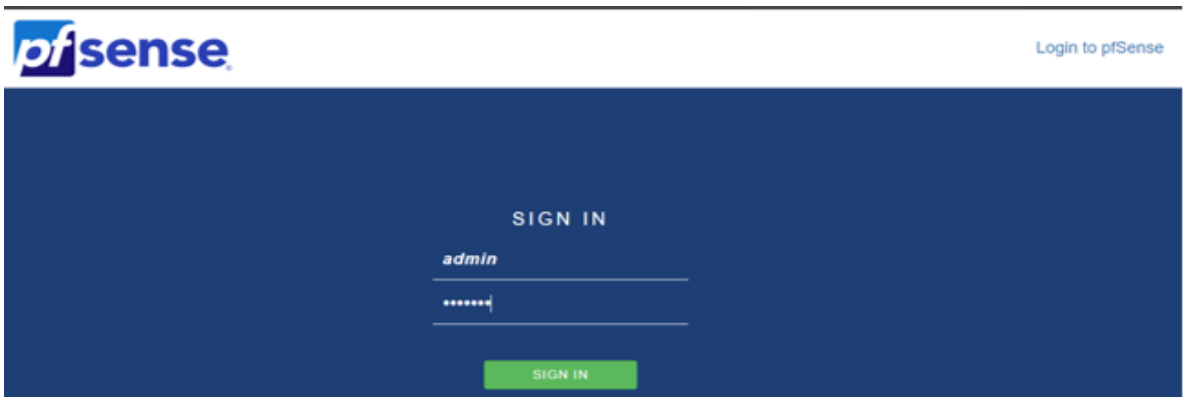
Con a la unidad booteada se iniciará la instalación, se mostrará la primera interfaz para comenzar a instalar, se elige la opción 1 y enseguida el firewall procederá a escribir los archivos en el disco de la máquina que va a contener el Pfsense.



Interfaz de instalación de Pfsense

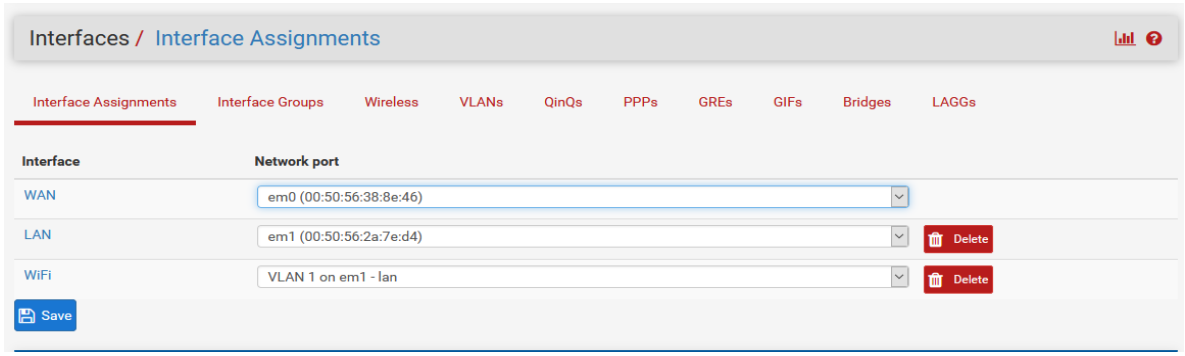
Terminada la instalación Pfsense poseerá una IP que se le fue asignada mediante DHCP, se debe ingresar la Dirección IP en un navegador con la finalidad de acceder al panel de

configuración, posteriormente se procede a ingresar el usuario y contraseña que por defecto son admin y Pfsense respectivamente.



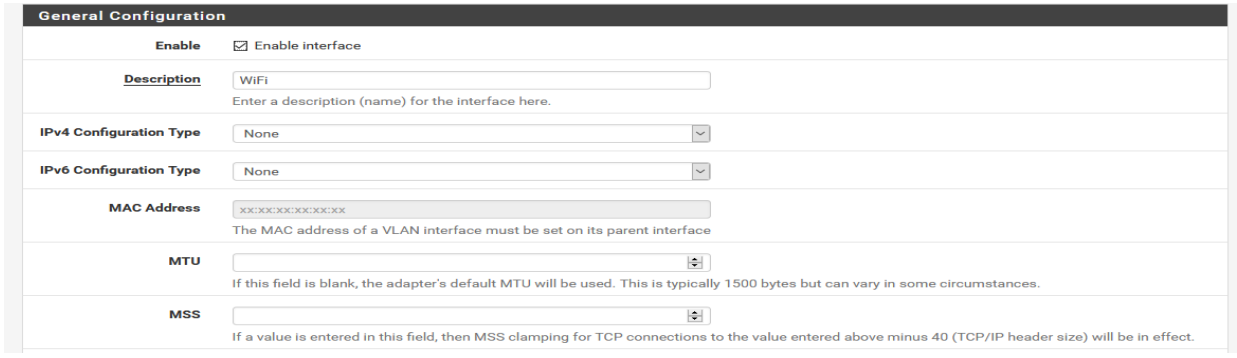
Acceso al panel de configuración de Pfsense

Ahora bien, al ingresar en el panel configuración hay que generar una nueva interfaz esta será llamará WiFi. Se encargará de brindar DHCP a los usuarios que estén bajo esta red.



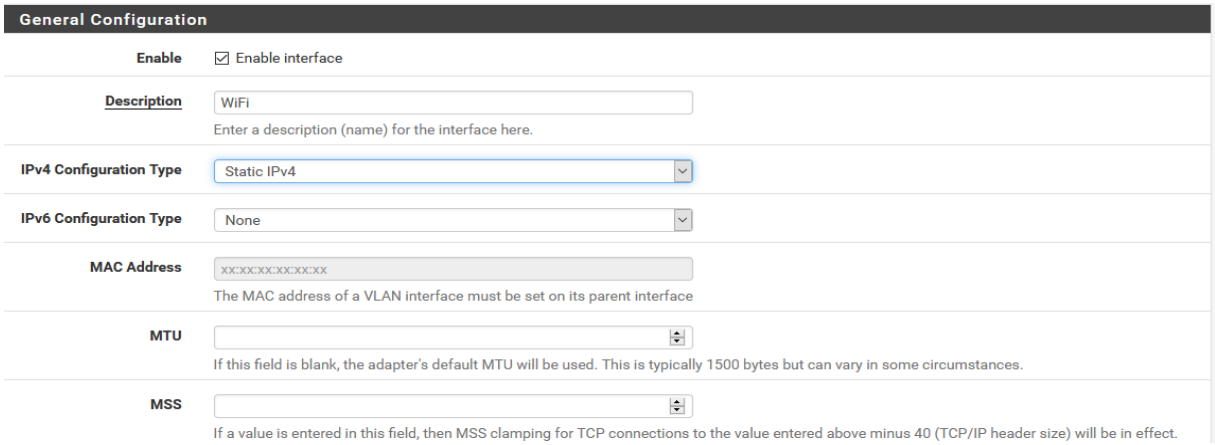
Asignación de interfaces en Pfsense

Se habilitará la interfaz creada.



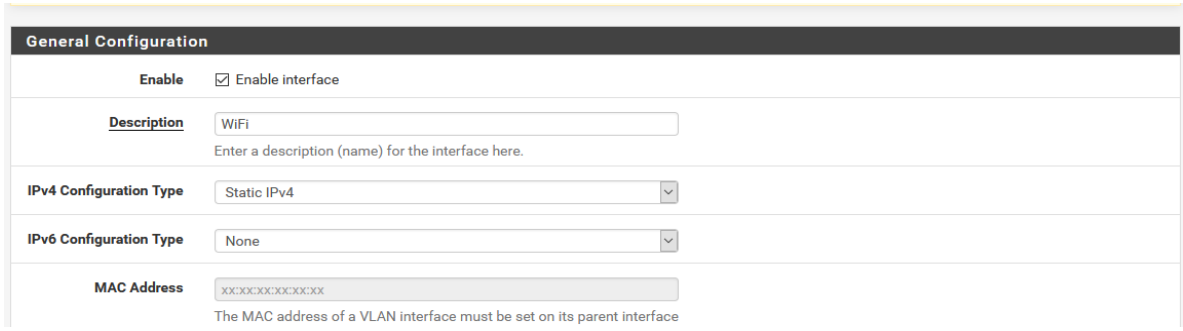
Asignación de interfaz WiFi

Se elige la configuración Static IPv4, con la finalidad de asignar una IP fija, además de asignarle la máscara de red.



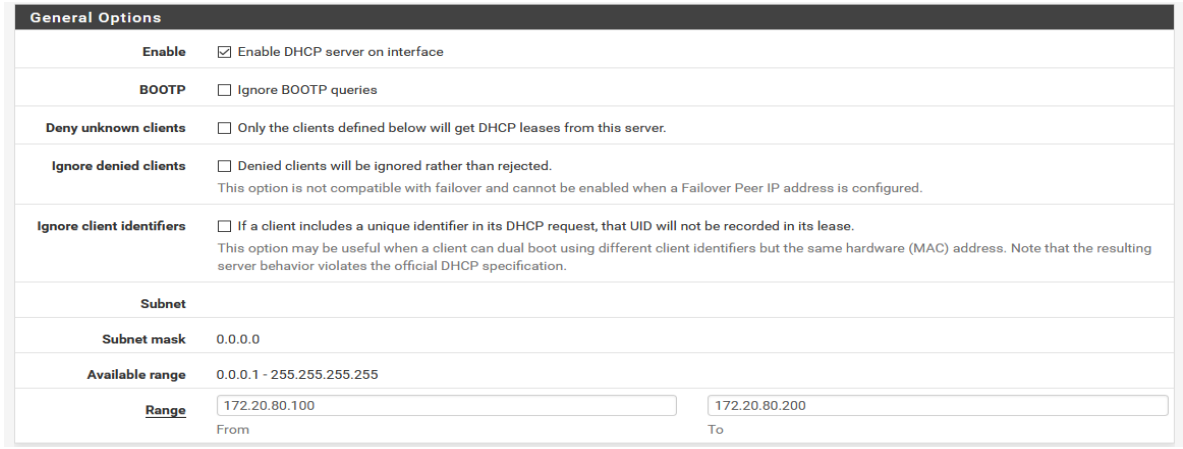
Configuración interfaz WiFi

Al guardar las configuraciones se indicará la siguiente pestaña.



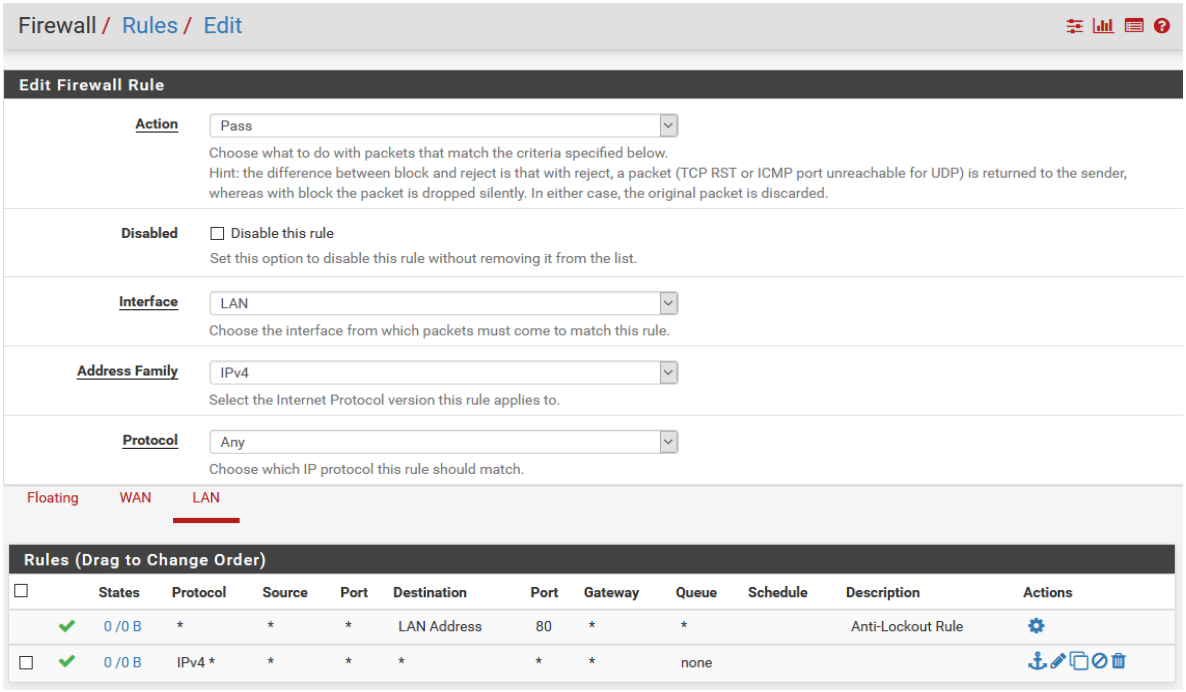
Configuración interfaz WiFi

Hay que dirigirse a la pestaña Servicios / DHCP Server para configurar el DHCP en la interfaz WiFi, hay que asignar el rango de IPS que vamos a utilizar. No hay que olvidar activar el servicio.



Configuración del servidor DHCP en la interfaz WiFi

Para concluir con la configuración de la interfaz, se crea una regla que permita el libre acceso a internet, posteriormente con la ayuda de otras reglas, hay que limitar la entrada y salida de paquetes dependiendo de los servicios que se instale en el firewall.

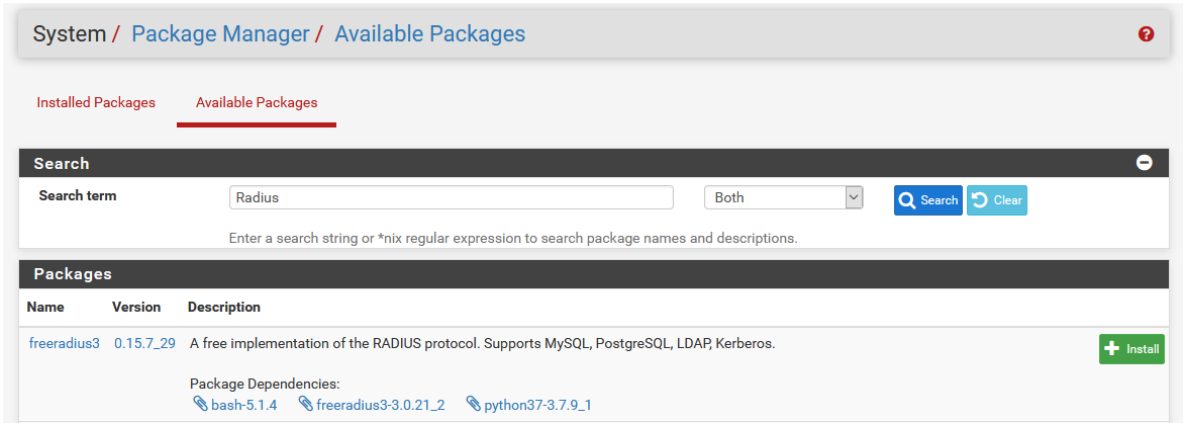


Creación de reglas de Firewall

Instalación FreeRadius

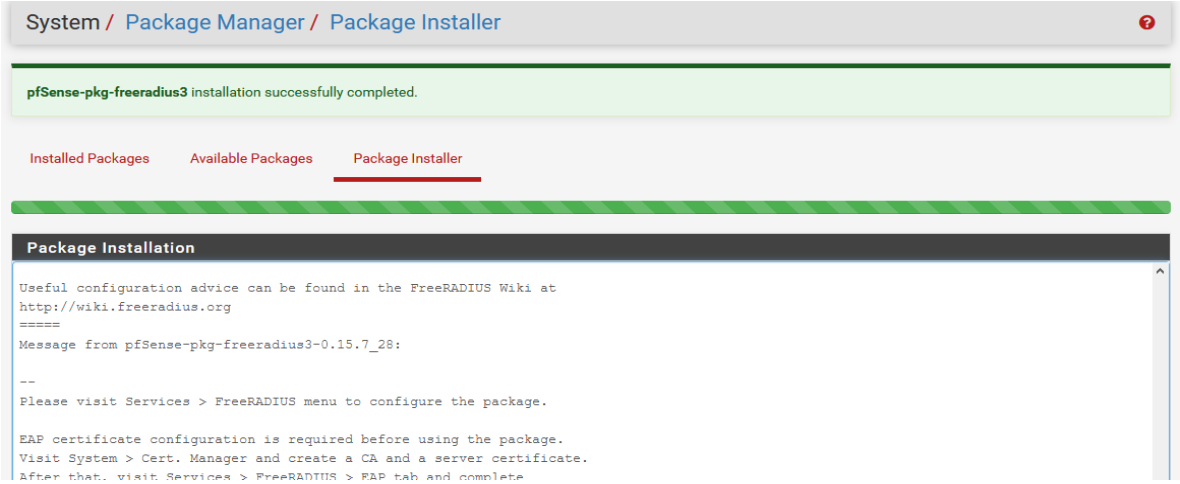
El servidor FreeRadius se encuentra en los más de 70 paquetes que tiene Pfsense, será implementado para la verificación las credenciales de los usuarios.

Para instalar el servidor se dirigirá al apartado System/Package Manager/ Avaliale Packages.



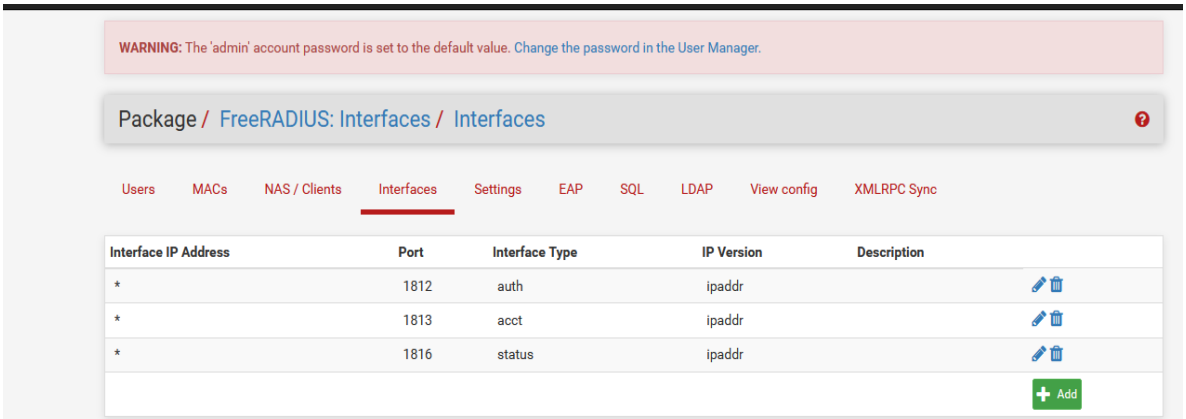
Instalación de paquete FreeRadius

Al presionar clic en el botón instalar empezará a descargar los paquetes, terminada la instalación se encontrará el servidor en la pestaña de services/FreeRadius.



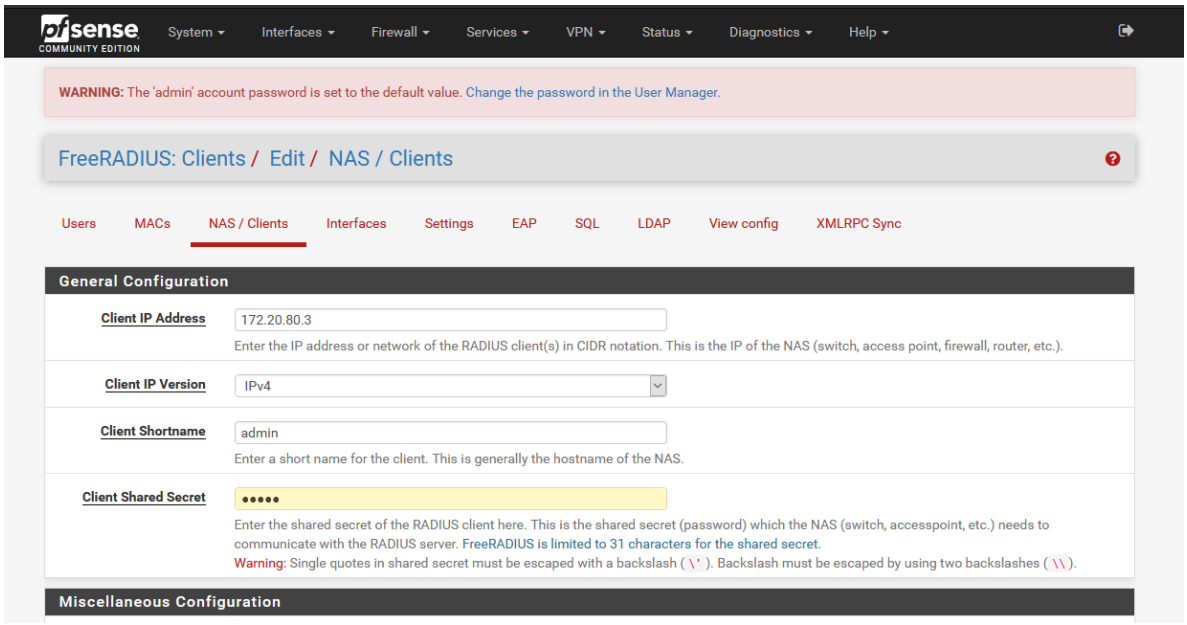
Instalación de paquete FreeRadius

Se debe configurar la Interfaz para especificar los puertos escucha 1812-1813-1816, mediante estos puertos el servidor Radius podrá establecer la conexión.



Configuración de puertos para servidor Radius

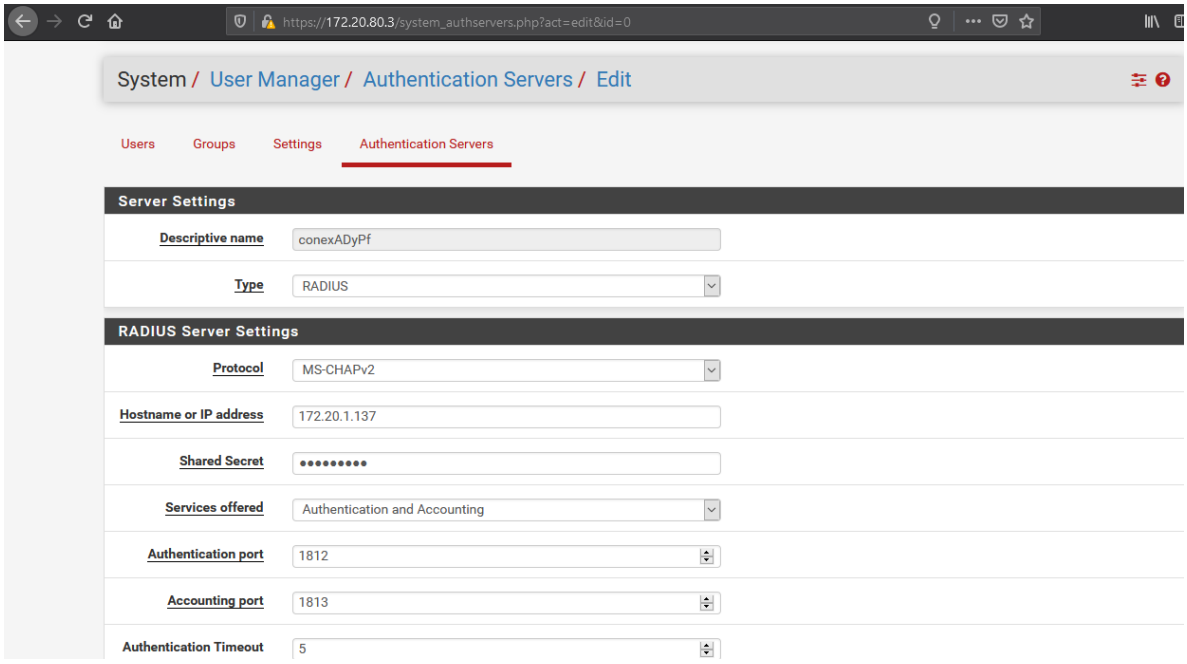
Se procede a crear un cliente NAS/Cliente que permita la comunicación con el servidor Radius del Active Directory.



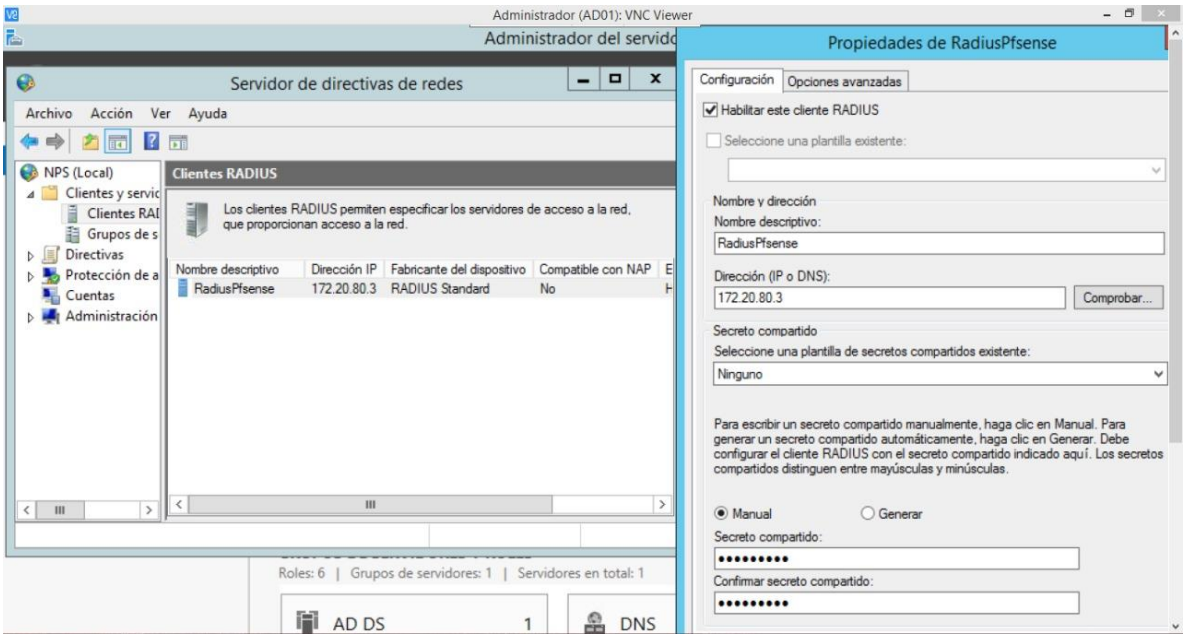
Configuración cliente NAS

Conexión Active Directory – Pfsense

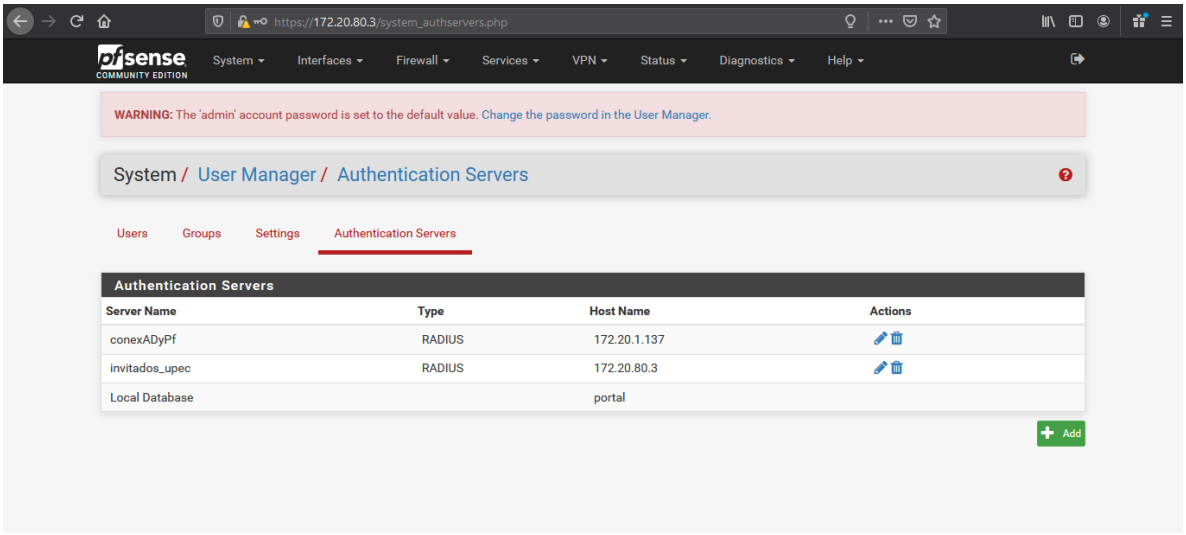
En el servidor Radius de Pfsense se establece la conexión, indicándole las credenciales del Active Directory para permitir la validación de los valores asignados. Mientras que el Radius del Active Directory deberá apuntar hacia la IP de Pfsense indicándole de igual manera sus credenciales.



Conexión Pfsense-Active Directory



Conexión Active Directory-Pfsense



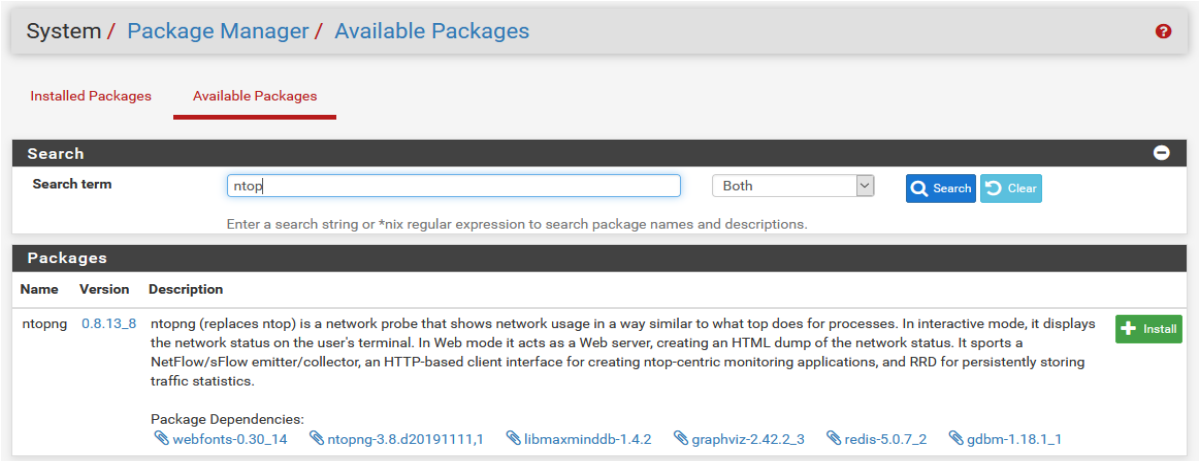
Conexión generada entre Pfsense y Active Directory

Instalación de paquetes

NtopNg

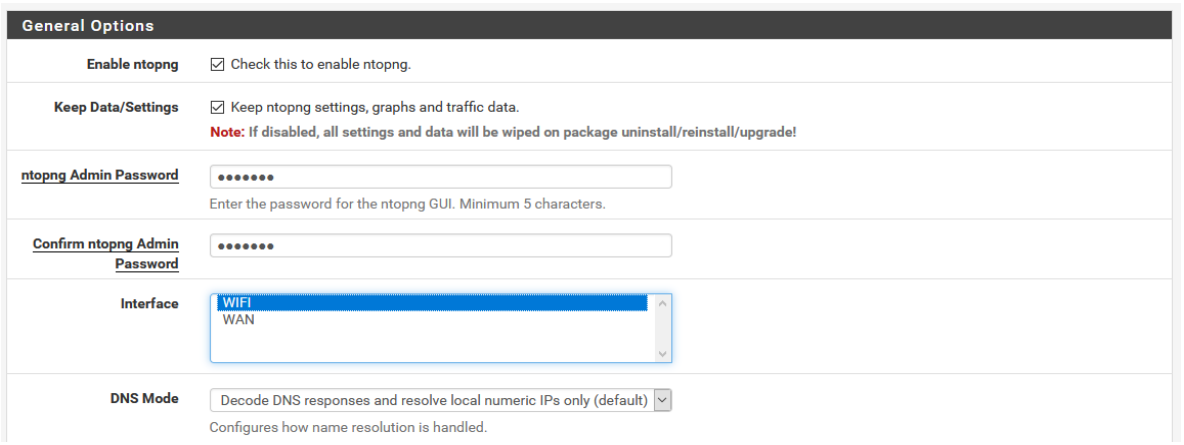
Una herramienta que se utilizó para permitir dar seguimiento a los dispositivos que se conectan a la red fue NtopNg. Esta herramienta puede ser incluida en Pfsense, permitiendo presentar varias vistas detallando direcciones IP, direcciones MAC, hosts, flujos, de la interfaz en donde se montó esta herramienta.

Para su instalación se tendrá que descargar desde System/ PackageManager/ Package Installer.

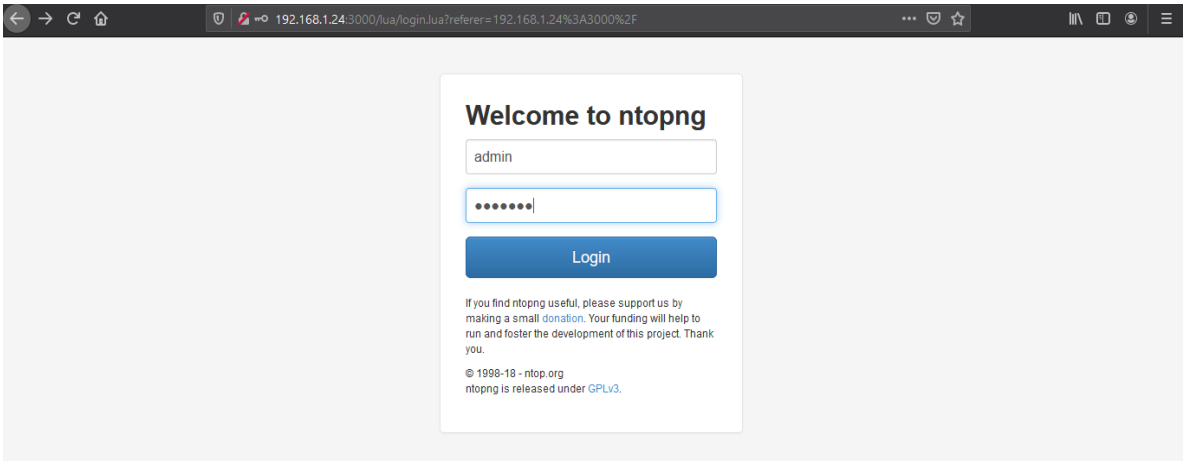


Instalación de NtopNg

Instalada esta herramienta se la puede encontrar en Diagnostics: NtopNg/ Settings NtopNg / Settings, dándole clic en NtopNg se puede ingresar al panel de configuración con las credenciales admin y Pfsense.

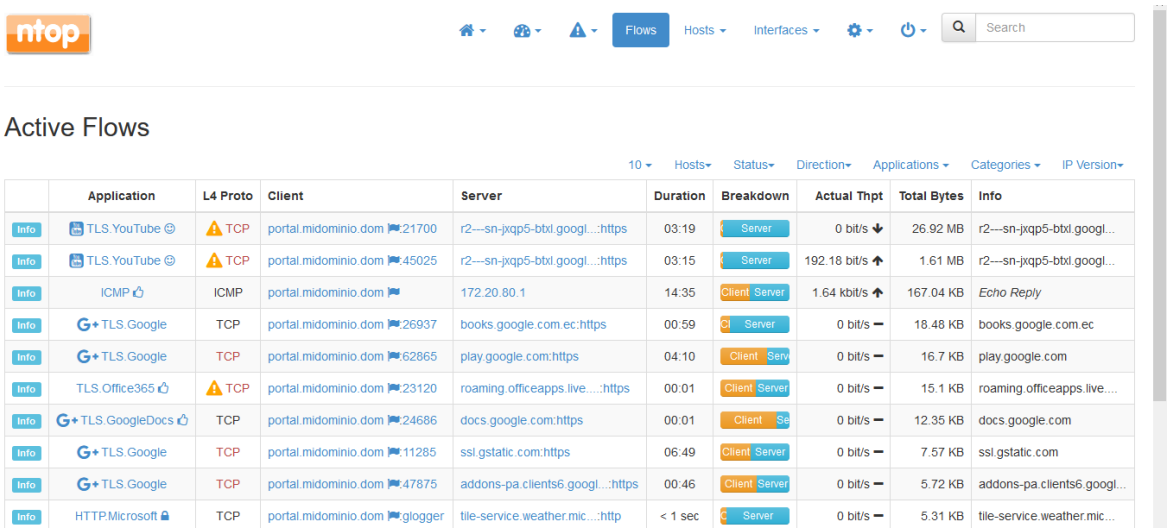


Asignación de NtopNg a interfaz WiFi



Panel de acceso a NtopNg

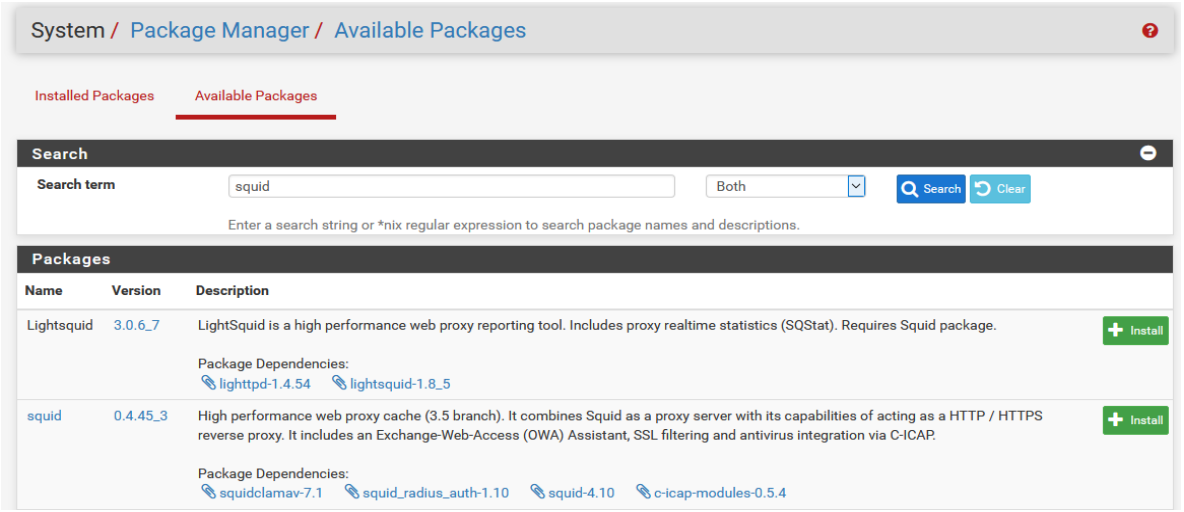
Al ingresar correctamente se puede observar el funcionamiento de la herramienta, como se mencionó anteriormente NtopNg permite monitorear la red.

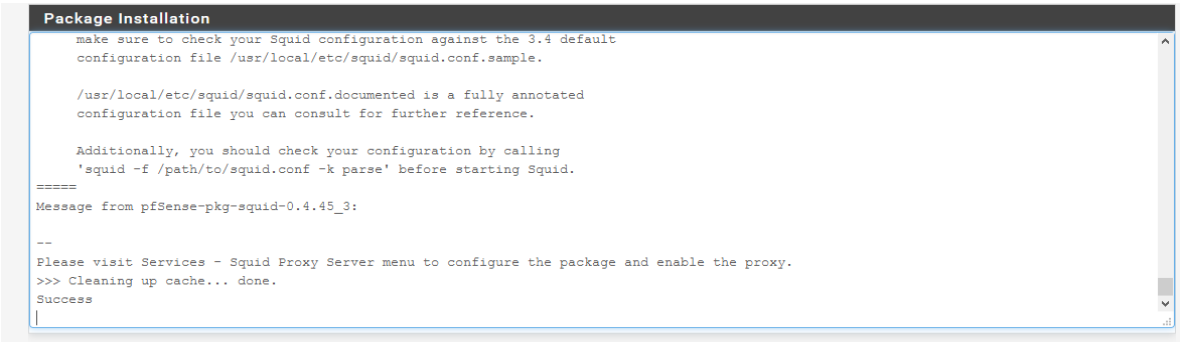


Panel de NtopNg

Squid Proxy Server

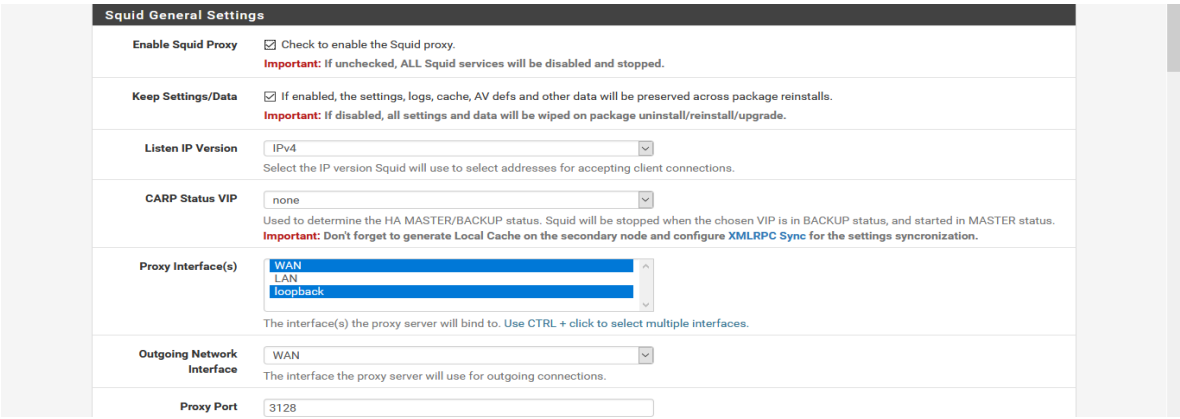
El uso del servidor Squid, mejorará el rendimiento de las conexiones tanto HTTP y HTTPS, además de aportar con la herramienta SquidGuard que permite el bloqueo de páginas web innecesarias. De igual manera como se realizó con el servidor Radius, esta herramienta se la encuentra en la ruta System/ PackageManager/ Package Installer.





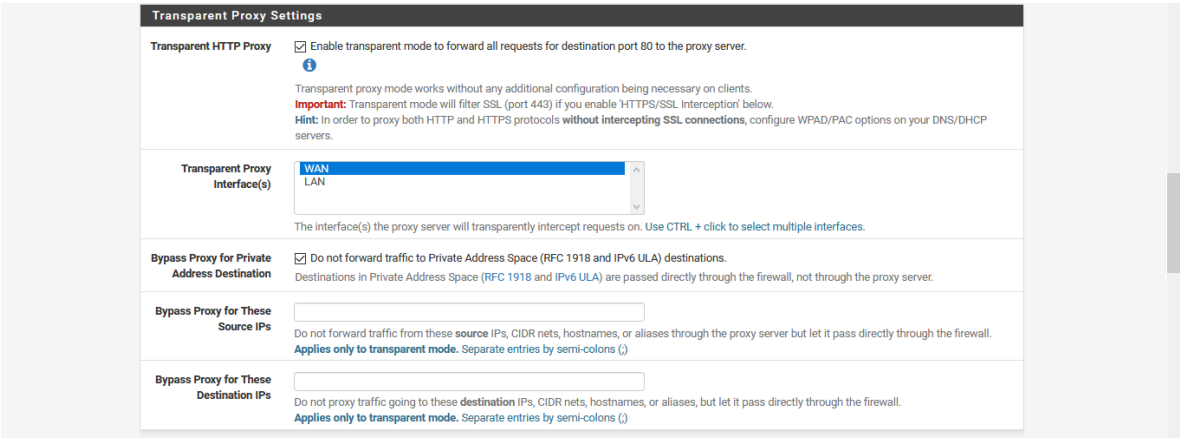
Instalación de Squid

Terminado la instalación habrá que realizar configuraciones seleccionando la interfaz WiFi, el servidor proxy trabaja por el puerto 3128 con la ayuda de una regla se redireccionará todo el tráfico hacia ese puerto.



Configuración de Squid

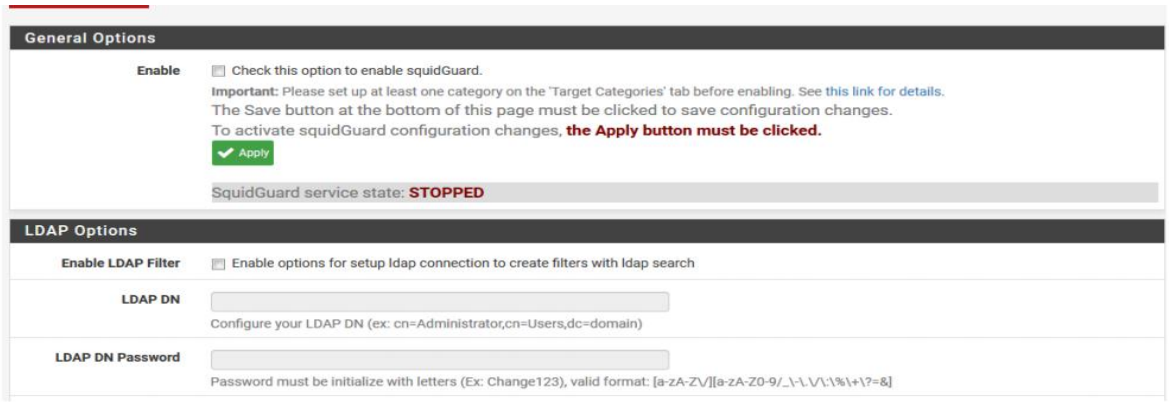
Se configura el Proxy de modo transparente, de esta manera permitirá interceptar y desviar las conexiones hacia el proxy sin la necesidad de configurar en cada cliente.



Configuración de modo transparente (Squid)

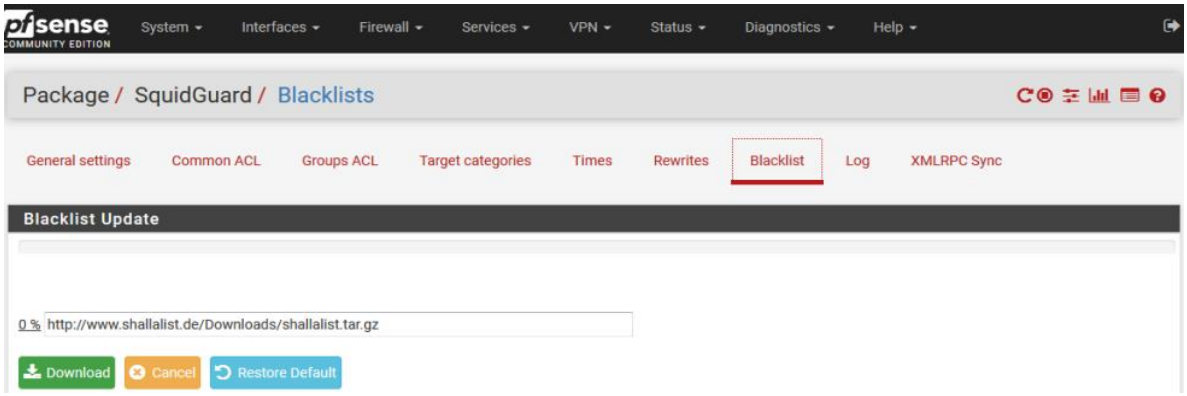
Proxy filter SquidGuard

Es una herramienta que se deriva de Squid permite filtrar el contenido web mediante la utilización de una de listas de acceso.



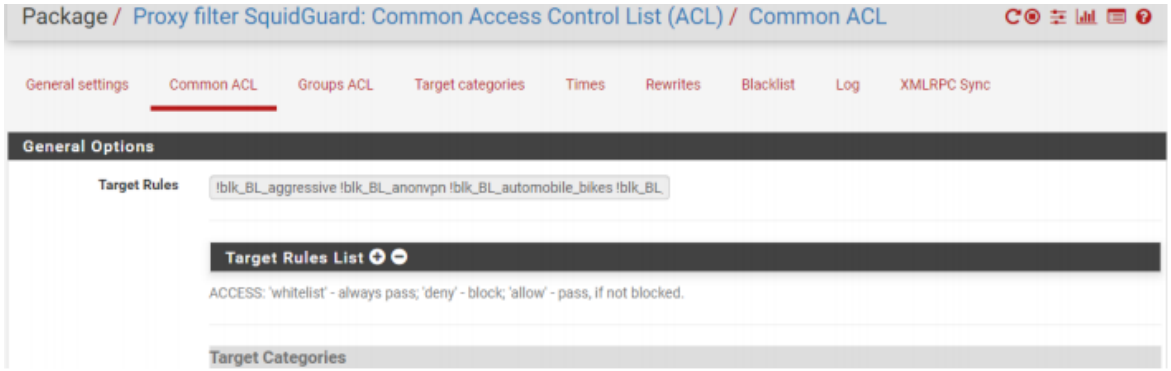
Configuración de SquidGuard

Esta BlackList se la puede descargó de páginas web como Shallalist, dicha lista permitirá bloquear las páginas web innecesarias. Para no tener inconvenientes en la descargar de la lista desde Shallalist vamos hasta el apartado SquidGuard/ Blaklist indicando la siguiente URL: https://www.shallalist.de/Downloads/shallalist.tar.gz, clic en Down load y empezar con la descarga como se muestra en la siguiente figura.

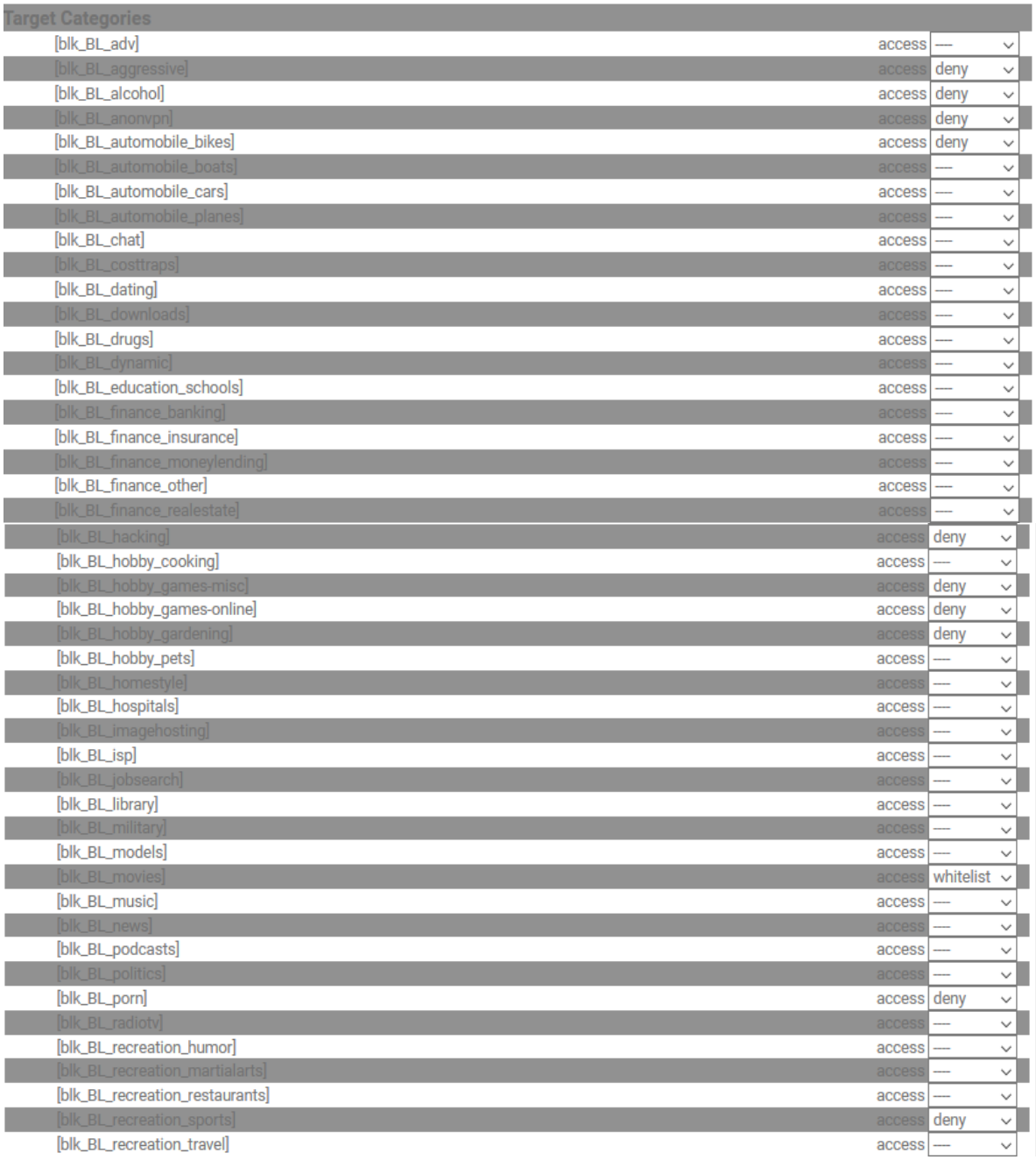


Configuración de blacklist

Se muestra a continuación el listado que se logró descargar desde el URL de Shallalist, esto se encuentra en Common ACL, con el uso de este elemento se puede elegir que páginas web serán permitidas o bloqueadas.



Acceso a ACL blacklist

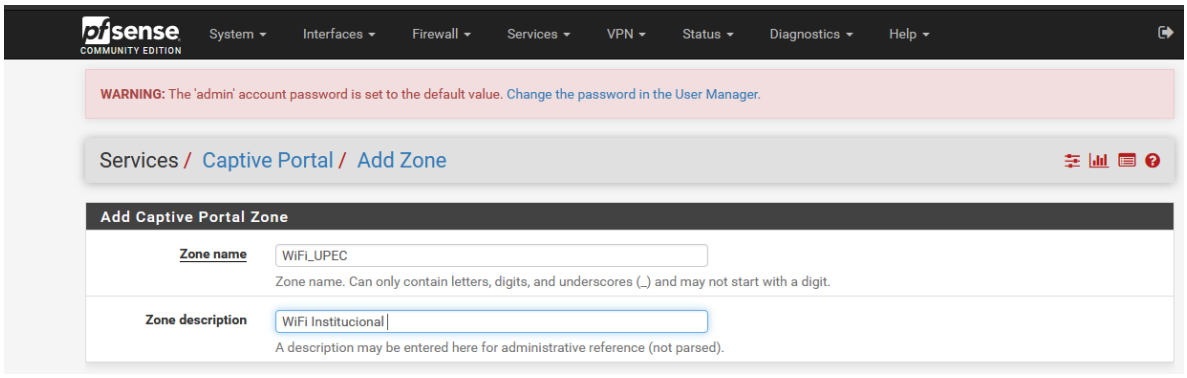


Lista de ACL blacklist

Finalmente, para aplicar los cambios se presiona un clic en la opción guardar.

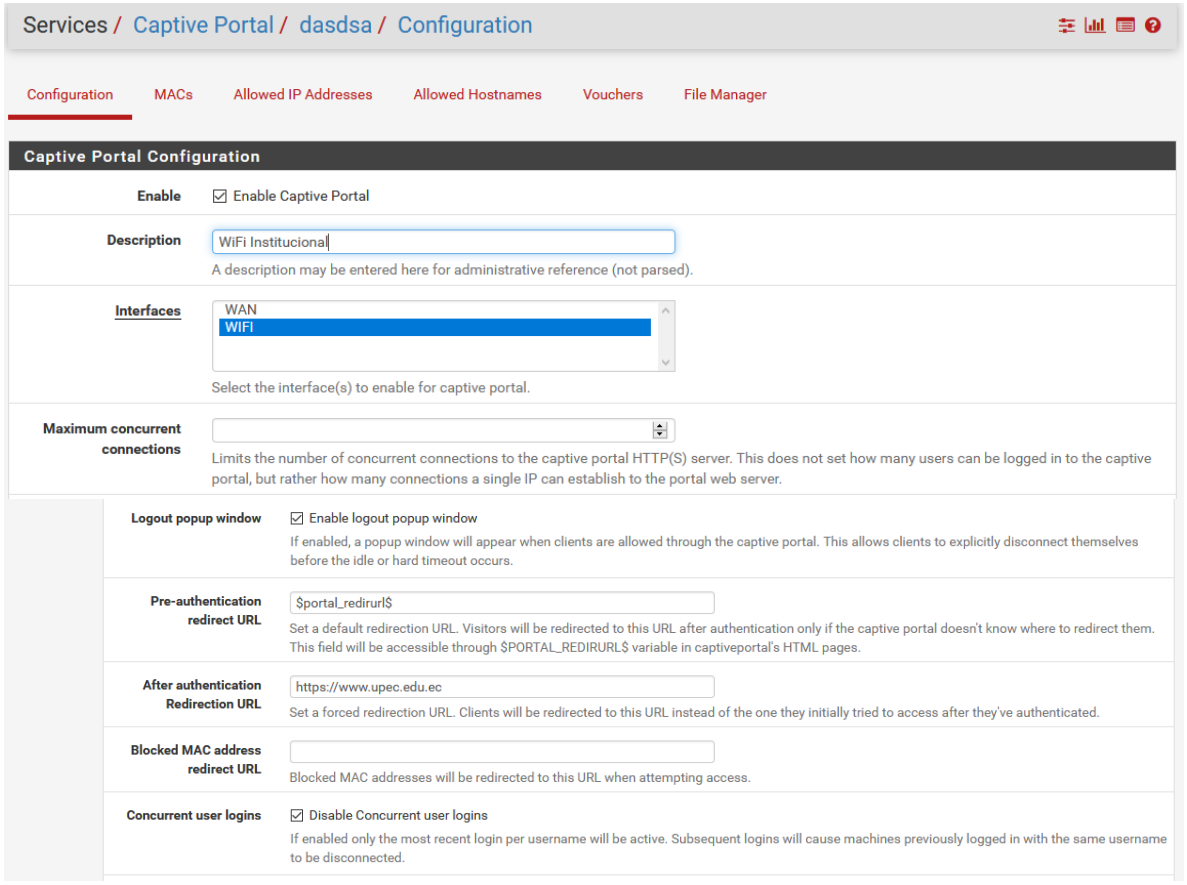
Portal Cautivo

Se considera al portal cautivo como una red informática la misma que se encarga de gestionar y controlar el acceso a usuarios redireccionándolos a una página predefinida en donde deben colocar usuario y contraseña para poder tener acceso a internet. Para configurar esta herramienta habrá que ir al apartado Service/ Captive portal, se agrega una nueva zona, aquí hay que especificar las configuraciones necesarias.



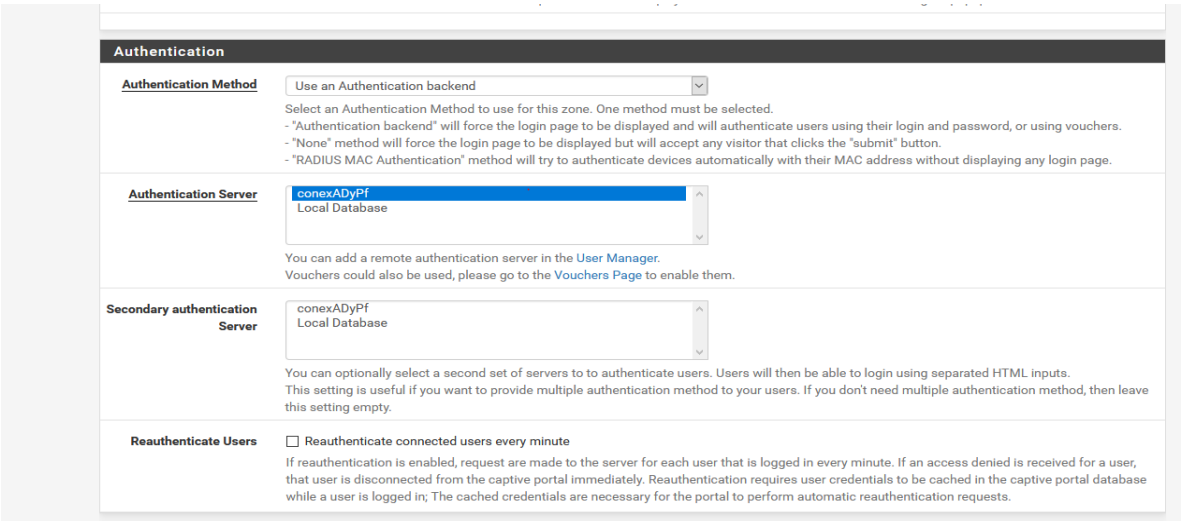
Creación de zona para portal cautivo

Se elige la interfaz de red donde se llegará a implementar el portal cautivo.



Configuración de portal cautivo

Además del modo de autentificación, para el estudio la conexión será mediante el Radius que se configuro anteriormente.



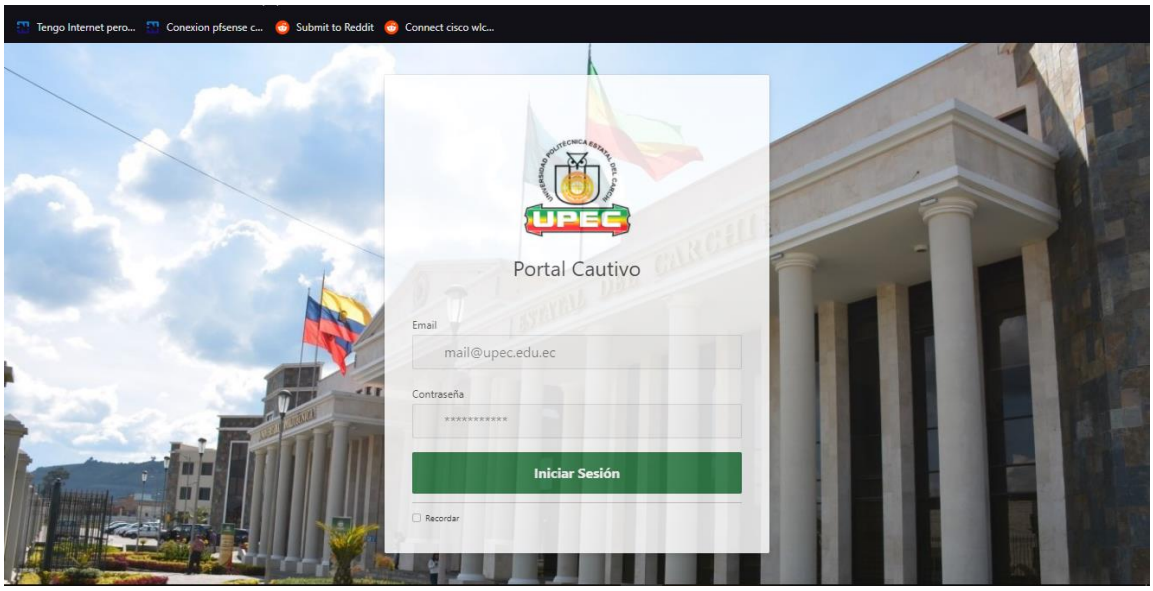
Autenticación mediante Radius

Pfsense tiene una opción para personalizar el portal cautivo habilitando la opción Use custom captive portal page, para este caso se ha generado una página HTML que se acople la imagen de la Universidad.

Personalización de página HTML Pfsense

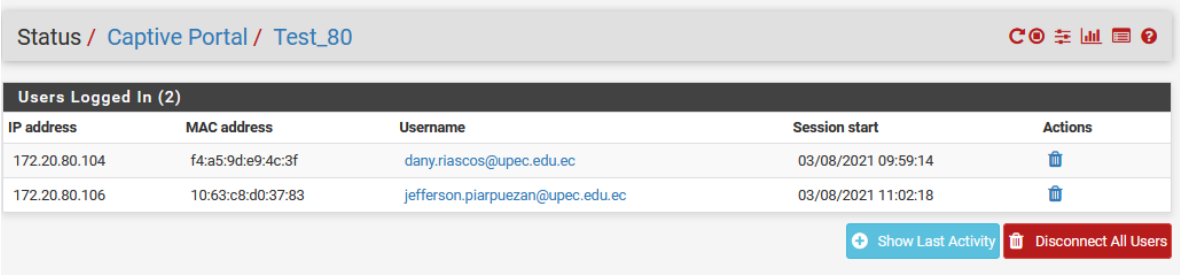
Para configurar esta herramienta se debe dirigir al apartado Service/ Captive portal, se agrega una nueva zona, aquí se especifica las configuraciones necesarias.

A continuación, se indicará la página web que se ha configurado.



Página inicial del portal cautivo

Al ingresar correctamente el usuario y contraseña, se redireccionará automáticamente la página institucional, ahora bien, para verificar la conexión que se realizó se debe dirigir al apartado status/ Portal cautivo ahí se muestra los usuarios activos.



Usuarios conectados al portal cautivo