UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

“Propuesta de rediseño y simulación de la infraestructura de red de la Unidad Educativa La Libertad basado en vlans y políticas de seguridad de acceso.”

AUTOR:

ASCENCIO CAICHE ANTHONY BRYAN

PROFESOR TUTOR:

ING. IVÁN CORONEL SUÁREZ, MSIA.

LA LIBERTAD – ECUADOR

2022

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Ascencio Caiche Anthony Bryan

APROBACIÓN DEL TUTOR

En mi calidad de Tutor/Tutora del trabajo de titulación denominado: "Título del Proyecto", elaborado por la estudiante Apellidos y Nombres del Autor, de la carrera de Informática/Electrónica y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La libertad, Julio del 2022

Ing. Iván Coronel Suárez, MSIA.

AGRADECIMIENTO

Agradezco a mis padres, que me han motivado y han estado siempre pendiente de que logre mis metas.

A la Universidad por haberme permitido formar parte de su comunidad y brindarme la oportunidad de formarme profesionalmente.

A mis profesores que supieron compartir sus conocimientos y fueron un pilar fundamental para que logre esta meta.

A mi docente guía quien formo parte de este proyecto, por haber aclarado mis dudas en cada fase del proyecto y por haber compartido parte de su tiempo para que logre culminar este estudio.

Ascencio Caiche Anthony

DEDICATORIA

Dedico este trabajo a mi madre, que a lo largo de mi carrera estuvo siempre apoyándome, por brindarme siempre su apoyo y por siempre haberse esforzado para brindarme todo lo que he necesitado, las noches de desvelo y los días cansados llenos de trabajos y tareas no son nada en comparación a lo que tú has hecho por y para mí a lo largo de mi vida.

“Soy lo que soy por y gracias a ti, y todo lo que logre en mi vida, te lo dedico a ti”

Ascencio Caiche Anthony

TRIBUNAL DE GRADO

Ing. Jaime Orozco, Mgt.

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Iván Coronel Suárez, MSIA

PROFESOR TUTOR

Lsi. Daniel Quirumbay, MSIA

PROFESOR DE ÁREA

Ing. Marjorie Coronel, Mgt

DOCENTE GUÍA

RESUMEN

El objetico de esta propuesta tecnología es realizar los debidos estudios para evidenciar la situación actual de la red de telecomunicaciones de la Unidad Educativa La Libertad de la provincia de Santa Elena, cantón La Libertad, con este primer estudio se evidenciaron las necesidades de la institución y a su vez se detallan las falencias que tiene la red.

El estudio está constituido por tres capítulos principales, dentro de los cuales se analiza tanto la parte teórica la implementación y pruebas de funcionamiento, se tomaron en cuenta los debidos estándares y metodologías tanto de investigación y de desarrollo, las cuales están detalladas dentro del segundo capítulo del proyecto.

Dentro del primer capítulo del proyecto se detallarán todas las metas de este, fue necesario establecer los objetivos tanto principales como específicos, partiendo desde las necesidades de la unidad educativa, se delimito la zona sobre la cual se trabajar y se justica la investigación y desarrollo.

En el segundo capítulo se especifican las metodologías que se utilizaras y se introduce la parte teórica sobre la cual se basará el proyecto se investigaron todas las herramientas que se necesitaron para la simulación y futura implementación, para este punto fue necesario investigar proyectos del área para tener mejores bases, se tomaron en cuenta proyectos a nivel local, nacional e internacional.

Dentro del tercer capítulo se lleva a cabo la propuesta, se estudian las herramientas a utilizar para escoger las que mejor cumplan con las necesidades de la institución, se realizan los posibles diseños de la propuesta y las debidas configuraciones, las cuales se dividen en tres partes, en la primera se llevó a cabo el diseño propuesto mediante el uso de la herramienta Packet Tracer, lo que ayudo a simular una red LAN y configurar los equipos, seguido a esto se realizó la configuración de un laboratorio en una red propia, en la cual se implementaron los servicios de firewall y proxy para la seguridad de la red y por último se creó un manual de políticas de seguridad para la Unidad Educativa, en el cual se contemplan tanto la seguridad lógica como física de la red, una vez finalizadas las configuraciones se realizaron las debidas pruebas para evidenciar el funcionamiento.

Palabras clave: Telecomunicaciones, redes LAN, firewall, seguridad lógica, simulación.

ABSTRACT

The objective of this technological proposal is to carry out the necessary studies to demonstrate the current situation of the telecommunications network of the "Unidad Educativa La Libertad" in the province of Santa Elena, canton La Libertad, with this first study the needs of the institution were evidenced and at the same time the shortcomings of the network are detailed.

The study is made up of three main chapters, within which both the theoretical part and the implementation and functional tests are analyzed, taking into account the due standards and methodologies of both research and development, which are detailed in the second chapter of the project.

In the first chapter of the project, all the goals of the project will be detailed, it was necessary to establish the main and specific objectives, starting from the needs of the educational unit, delimiting the area in which to work and justifying the research and development.

In the second chapter the methodologies to be used are specified and the theoretical part on which the project will be based is introduced, all the tools needed for the simulation and future implementation were investigated, for this point it was necessary to investigate projects in the area to have better bases, projects at local, national and international level were taken into account.

In the third chapter the proposal is carried out, the tools to be used are studied to choose the ones that best meet the needs of the institution, the possible designs of the proposal and the proper configurations are made, which are divided into three parts, in the first one the proposed design was carried out using the Packet Tracert tool, which helped to simulate a LAN network and configure the equipment, followed by the configuration of a laboratory in its own network, in which firewall and proxy services were implemented for network security and finally a security policy manual was created for the Educational Unit, in which both the logical and physical security of the network are contemplated, once the configurations were completed, the proper tests were carried out to demonstrate the operation.

Keywords: Telecommunications, LAN networks, firewall, logical security, simulation.

TABLA DE CONTENIDO

ÍNDICE FIGURAS

ÍNDICE TABLAS

ÍNDICE ANEXOS

INTRODUCCIÓN

El objetivo de este proyecto es realizar un estudio que permita crear un nuevo diseño para la red LAN de la Unidad Educativa La Libertad, la cual es una Unidad Educativa perteneciente a la Provincia de Santa Elena ubicaba específicamente en el cantón La Libertad, a pesar de ser una de las instituciones educativas más conocidas dentro de la provincia y con una gran trayectoria, se nota la insuficiencia en el servicio de internet que posee y a su vez en la administración de red que maneja.

Las instituciones educativas son uno de los puntos en donde contar con un sistema de internet optimo es necesario, actualmente y con la aparición de la pandemia por COVID-19 se notó la gran importancia de esta herramienta para sobrellevar los efectos negativos que trajo consigo esta pandemia y posterior uso masivo de los medios de telecomunicaciones, pero a pesar de esto a muchas de las instituciones educativas no se le presta la debida importancia del caso, siendo una de estas la unidad educativa sobre la cual se pretende realizar el proyecto.

El presente estudio tiene la finalidad de impulsar una instalación adecuada de la red de telecomunicaciones para la Unidad Educativa, con el fin de que el personal que labora dentro de la institución y los estudiantes tengan una forma óptima de acceder al internet y a su vez amplíen sus herramientas y métodos de educción.

Se implementarán los debidos estudios de factibilidad, para evaluar el nivel de eficiencia de las herramientas y métodos de seguridad que se implementara, esto ayudara a tener un conocimiento en cuanto a costos de implementación y a su vez conocer las características de cada uno de los equipos y la forma en la que ayudan a la mejora para la institución.

Además, se tomaron en cuenta las metas, requerimientos y objetivos de la Unidad Educativa, para generar un correcto diseño que satisfaga cada uno de estos aspectos, el uso de herramientas de simulación y creación de laboratorios virtuales fue necesario debido a que la institución no cuenta con los equipos de red adecuados que soporten las configuraciones necesarias para crear el rediseño.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

Actualmente es evidente que las redes y el Internet tienen un notable impacto en todos los niveles de educación, las actividades que se realizan en línea son parte de la vida de muchos jóvenes de modo que se considera al Internet como un requisito básico de la vida moderna [1]. Existen varios factores que impiden que se desarrolle de mejor manera la educación en base al Internet, entre los cuales destacan la falta de acceso, infraestructura inadecuada y falta de inclusión [2]. En base a esto se puede decir que uno de los principales puntos donde se debe tener una buena administración y acceso a redes son las Unidades Educativas, en las cuales a diario miles de estudiantes y docentes se ven en la necesidad de hacer uso de herramientas tecnologías para su desarrollo educacional, muchos de los cuales se ven afectados por la mala calidad de la red provista por la institución o por la poca importancia que se les da a estas redes por ser de pequeño o mediano tamaño.

La unidad educativa La Libertad está situada en la provincia de Santa Elena, cantón de La Libertad en la parroquia de La Libertad, es un centro educativo de educación regular y sostenimiento fiscal, con jurisdicción hispana. La modalidad es presencial de jornada matutina y vespertina, el nivel educativo es de EGB (Educación General Básica) y Bachillerato. Fue fundada el 11 de abril de 1986, en la actualidad posee un total de 69 docentes y 1668 estudiantes. [3]

La unidad educativa se encuentra situada en un área de 16.497 m2 , en base a observación se constató que actualmente cuenta con seis pabellones de aulas, cinco se encuentran constituidos por tres aulas y uno de ellos por cinco aulas, cuenta con un pabellón para laboratorios de computación, donde se encuentran dos aulas con equipos, además de un edificio administrativo en las cuales está ubicada una biblioteca con equipos de computación, oficina de secretaria, rectorado y vicerrectorado, la unidad también cuenta con un pabellón donde se encuentran laboratorios de física, química y biología.

Con el plan de regreso a clases progresivo, la institución se ha visto en la necesidad de reintegrar a los docentes de forma presencial, los cuales tienen sus aulas designadas, desde

las cuales realizan sus acompañamientos educativos, estos se realizan de forma virtual por aplicaciones de videoconferencia como Zoom y Microsoft Teems, además de que cada docente debe atender a docenas de padres y alumnos que a diario se acercan a las instalaciones de la Unidad Educativa.

En los próximos periodos lectivos se tiene previsto que al menos la mitad de los estudiantes regresen a las aulas, con el nuevo modelo de educación a los estudiantes se les permitirá el ingreso con dispositivos móviles, sean estos Smartphone's o Tablets, los cuales serán necesarios para acceder a las herramientas tecnologías que se utilizaran para el desarrollo de la clase.

En un primer análisis se detectó fallos en la red de la Unidad Educativa, existen puntos en ciertos pabellones donde el acceso a Internet mediante una red WiFi resulta imposible, de igual forma, la infraestructura no se encuentra segmentada de forma correcta para tener un óptimo desempeño, la configuración actual no cuenta con políticas de acceso mediante wifi, basándonos en este primer análisis, se notó que la infraestructura y topología actual de la red, no cumple con las condiciones necesarias para un próximo reingreso de los estudiantes.

En España en la Universidad Politécnica de Valencia en la escuela Técnica Superior de informática se llevó a cabo el proyecto de diseño, desarrollo e implementación de una red de área local en una empresa con el fin de determinar cuáles son las vulnerabilidades principales y los riesgos más propensos a los cuales están expuestos con la red actual, se buscó implementar una arquitectura solvente tomando en cuenta la infraestructura, el área y el presupuesto de la empresa. [4]

Para lograr la instalación de un directorio activo y la administración de tráfico y la seguridad lógica por medio de la creación de reglas, perfiles y listas de control de acceso se realizó En Perú en la Universidad Nacional Centro de Perú en la carrera de ingeniería en sistemas, la implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la red en la Oficina Departamental en Estadísticas e Informática de Junín. [5]

En Ecuador en la Universidad Politécnica Salesiana con Sede en Guayaquil se realizó una reestructuración de red LAN basada en las normas de cableado estructurado y en la

aplicación de políticas de seguridad para el control de acceso mediante un servicio proxy sobre la plataforma Linux en una Unidad Educativa. [6]

Basándonos en un primer análisis y luego de realizar las debidas investigaciones se propone realizar una reestructuración de la red actual, basado en normas y estándares tanto de segmentación y aplicación de políticas de seguridad, esto debido a que la red actual no cumple con las condiciones necesarias para un acceso masivo de dispositivos, el cual se llevaría a cabo por el inminente regreso de los estudiantes y docentes a las instalaciones de la Unidad Educativa.

1.2 DESCRIPCIÓN DEL PROYECTO

En base a la necesidad de la Unidad Educativa La Libertad de contar con una óptima red para el acceso al servicio de Internet tanto de los maestros como de los estudiantes y de igual forma por la falta de seguridad que presenta la infraestructura, se propone realizar un estudio de la situación actual y aplicación de segmentación de red que permita tener un acceso más controlado y seguro, seguido de la elaboración y aplicación de políticas de seguridad para el control de acceso a los puntos mediante wifi o equipos cableados.

El presente proyecto se basará en la metodología Top-Down Network Design propuesta por CISCO, la cual cuenta de las siguientes fases:

Fase de recolección de datos de infraestructura

Esta primera fase se basará en la recolección de información de la infraestructura actual, la cual incluye la topología de la red, esto permitirá identificar las falencias del diseño, de igual forma se analizarán los equipos y tecnología existentes, esta información incluirá datos como: medios para transmisión, usuarios de la Unidad Educativa, usuarios por cada pabellón y laboratorios, medios físicos y quipos utilizados, además será necesario conocer las velocidades de transmisión, área de cobertura, se constatar los servicios que hacen uso de la red como datos, video conferencia, Internet, video vigilancia y servicios de impresión, esto permitirá tomar acciones para poder mejorar el rendimiento del servicio en cada uno de los puntos de la Unidad Educativa.

Fase de análisis de requerimientos

En este punto se acoplarán los requerimientos de los usuarios para definir un nuevo diseño de la red, los principales fueron:

1. Cantidad de usuarios que harán uso de la red.
2. Identificar cantidad de puestos y puntos de red.
3. Segmentación necesaria para cada área del edificio administrativo y laboratorios.
4. Volumen de tráfico.
5. Autenticación para uso de servicio wifi.
6. Uso de aplicaciones de video conferencia.
7. Seguridad de red.
8. Apoyo de soporte y mantenimiento.

Fase de diseño lógico

En esta fase será necesario plantear una topología de red que satisfaga los requerimientos de la Unidad educativa, lo que implica, direccionamiento de capas de red, protocolos, intercambio y enrutamiento, dentro de esta fase también se incluye el planteamiento de seguridad y administración de red.

Fase de diseño físico

Dentro de esta fase se determinará las tecnologías que se utilizarán, los protocolos, especificaciones técnicas de los equipos y productos para llevar a cabo la red diseñada en la fase de diseño lógico.

Prueba y documentación del diseño

Dentro de la simulación se tendrán en cuenta todos los posibles escenarios que se puedan presentar realizando pruebas para cada uno de ellos, además de analizar las políticas de seguridad que se implementarán, se debe realizar la documentación del nuevo diseño, características principales y características técnicas de cada uno de los equipos y estándares utilizados.

Tecnologías a utilizar

Segmentación

VLANs

Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados

al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. [7]

Las LANs virtuales (VLANs) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre si como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, para la colaboración en sistemas informáticos de redes. [8]

Servicios

Servicio Proxy

Un servidor proxy es una tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet); Generalmente se trata de un dispositivo u ordenador intermedio que nos permite conectarnos a Internet de manera indirecta, es un intermediario entre la red a la que nos conectamos e Internet, para registrar el contenido antes: HTML, CSS e imágenes, es muy utilizado para acelerar el contenido de un sitio al navegar, los datos de una web quedan almacenados en la primera visita y si hay una segunda no necesita revisarlos todos de nuevo, así el acceso es mucho más rápido. [9]

Firewall

Un firewall es un sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet, estos pueden ser de tipo hardware o software, o una combinación de ambos, protegen tu computadora, o una serie de computadoras en una red, de los sitios web llenos de malware o de los puertos de red abiertos vulnerables. [10]

Herramientas

Pfsense

El software PfSense es una distribución personalizada gratuita y de código abierto de FreeBSD diseñada específicamente para su uso como firewall y enrutador que se

administra completamente a través de la interfaz web, además de ser una plataforma de enrutamiento y cortafuegos potente y flexible, incluye una larga lista de características relacionadas y un sistema de paquetes que permite una mayor capacidad de expansión sin agregar vulnerabilidades de seguridad potenciales y excesivas a la distribución base. [11]

Proxmox

Proxmox Virtual Environment es una solución de código abierto para la virtualización empresarial, su objetivo es ayudarte a optimizar el uso de los recursos ya existentes, minimizar el costo por hardware y el tiempo empleado, se basa en Debian GNU/Linux y utiliza un Kernel de Linux personalizado, es por eso por lo que las imágenes de disco (archivos ISO) en la instalación incluyen un sistema Debian completo. Además, permite su instalación sobre uno ya existente. [12]

Squid

Squid es un proxy de almacenamiento en caché para la Web que admite HTTP, HTTPS, FTP y más. Reduce el ancho de banda y mejora los tiempos de respuesta al almacenar en caché y reutilizar las páginas web solicitadas con frecuencia. Squid tiene amplios controles de acceso y es un excelente acelerador de servidores. [13]

Proporciona servicios de proxy y caché para el Protocolo de transporte de hipertexto (HTTP), el Protocolo de transferencia de archivos (FTP) y otros protocolos de red populares, Squid puede implementar el almacenamiento en caché y el proxy de las solicitudes de capa de conexión segura (SSL) y el almacenamiento en caché de las búsquedas del servidor de nombres de dominio (DNS), y realizar un almacenamiento en caché transparente, Squid también admite una amplia variedad de protocolos de almacenamiento en caché, como Internet Cache Protocol (ICP), Hyper Text Caching Protocol (HTCP), Cache Array Routing Protocol (CARP) y Web Cache Coordination Protocol (WCCP). [14]

SquidGuard

Es un sistema de filtrado combinado de redireccionamiento web y plugin del controlador de acceso para Squid, utiliza listas negras “Blacklist” como base de datos para denegar o

permitir el acceso a sitios web, su mayor utilidad es la prevención de dominios o URLs que contengan información no deseada o nada productiva en horarios laborales. [15]

Listas de control de acceso – ACL

Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos. [16]

Equipos

Router

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web, los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino; El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión. [17]

Switch Administrativo

Los switches son piezas de construcción clave para cualquier red, conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus, un switch permite a los dispositivos conectados compartir información y comunicarse entre sí, ofrecen seguridad y flexibilidad dado a que pueden ser configurados de acuerdo a las necesidades de la red, permitiendo tener un mejor control de la red y mejorar la calidad del servicio. [18]

Cableado estructurado

El cableado estructurado se define como el conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o recinto, se encargan de transportar señales desde unos dispositivos (emisores) a otros (receptores) con el objetivo de crear la red de área local del mismo; Esta estructura contiene una combinación de cables trenzados

(UTP/STP/FTP) , fibras ópticas (FO) y/o cables coaxiales que deben cumplir ciertos estándares universales para que puedan ser fácilmente entendidos. [19]

La simulación de segmentación y aplicación de políticas de seguridad en la Unidad Educativa La Libertad contribuye a la línea de investigación de Telecomunicaciones (TLC) y su sub línea de investigación Telemática, debido a que el proyecto consiste en análisis de infraestructura y aplicación de políticas de seguridad para acceso a la red. [20]

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Realizar modelos basados segmentación y políticas de seguridad mediante el uso de Vlans y servicios proxy para el acceso y control de la red LAN de la Unidad Educativa la Libertad.

1.3.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la situación actual de la red de la unidad para presentar la propuesta del nuevo diseño de red basado en redes virtuales.
- Establecer políticas de seguridad para el control de acceso de los estudiantes y mantener una correcta administración de la red.
- Ejecutar pruebas en un laboratorio virtual para verificar la efectividad del servicio proxy basado en las herramientas pfsense y squid.

1.4 JUSTIFICACIÓN

Para mantener una buena administración de redes es necesario la adopción de tecnologías escalables y flexibles que se adapten cambios. [21] la implementación de un correcto diseño de red permite facilitar la administración, a través de diferentes tecnologías, esto para que los usuarios sean capaces de comunicarse entre sí y acceder a los datos y servicios. [22]

Según la Agenda Educativa Digital del ecuador, actualmente, gracias al acuerdo entre MinEduc (Ministerio de Educación) y CNT EP (Corporación Nacional de Telecomunicaciones), 4765 unidades ya cuentan con conectividad y cubren a 2720000 de estudiantes, esto abarca el 89% de los estudiantes del sistema Publio. [23]

Con el presente proyecto se identificará las falencias con las que cuenta la red institucional, partiendo con la aplicación de una correcta segmentación que permitirá controlar de forma más inteligente el tráfico de red, dividiendo a la red en grupos de trabajos se logra como consecuencia directa, la incrementación del ancho de banda de dicho grupo de trabajo, además de que se vuelve una red más segura, permitiendo así agrupar datos sensibles y separarlos del resto de la red, disminuyendo los posibles ataque o violaciones a la información.

Una correcta segmentación permite que la red se vuelva escalable y que se le puede asignar nuevos grupos de trabajo, su mantenimiento en caso de fallas se vuelve más rápido y práctico, esto debido a que se vuelve más fácil de hallar la posible causa del problema o en caso de algún ataque de igual forma se puede aislar al atacante en un solo segmento de la red dejando a los demás grupos protegidos, si a esto le sumamos la aplicación de las políticas de seguridad tanto para acceso y navegación, el riesgo de ataques disminuye.

Con las políticas de seguridad, se puede controlar a los usuarios que se quieren conectar a la red, permite el bloqueo de sitios considerados maliciosos, ayuda a aumentar la seguridad mediante el filtrado de sitios, además de permitir la creación de listas negras para bloquear usuarios o sitios no deseados.

Con el fin de precautelar la seguridad de los usuarios, el estudio permitirá hacer un análisis y tomar las medidas para corregir todas las falencias y posibles riesgos. Los principales beneficiarios del proyecto de forma directa serán los estudiantes y docentes que hagan uso de la red, además de todos los departamentos existentes dentro de la institución, el estudio permitirá dar cabida a nuevas mejoras en la red para en un futuro implementarlas en todas las áreas de la Unidad.

El presente proyecto está alineado con los objetivos del Plan de Creación de Oportunidades específicamente en el siguiente eje.

Eje Social

Objetivo 5.- Proteger a las familias, garantizar sus derechos y servicios erradicar la pobreza y promover la inclusión social. [24]

Política 5.5.- Mejorar la conectividad digital y acceso a nuevas tecnologías de la población. [24]

Lineamientos Territoriales

Pol. 5.4

A4.- Fortalecer la conectividad y acceso a las TIC como vía para mejorar el acceso a otros servicios. [24]

1.5 ALCANCE DEL PROYECTO

El presente proyecto presentará una propuesta de rediseño de red basado en segmentación mediante Vlans y políticas de seguridad permitirá mantener un mejor control de la red al igual que una mejor administración de los equipos que se encuentran ubicados dentro de la red de la Unidad Educativa La Libertad.

El presente proyecto abarcará las siguientes fases:

- Fase de recolección de datos de infraestructura
  - En esta fase se recolectarán todos los datos de la infraestructura de la red, tomando en cuenta topología, tecnologías y equipos utilizados, técnicas y protocolos de seguridad**.**
- Fase de análisis de requerimientos
  - En esta fase se analizarán tanto las metas y objetivos de la institución, de igual forma los requerimientos extraídos mediante las técnicas de recolección de información para poder proceder con los diseños lógicos y físicos**.**
- Fase de diseño lógico
  - En esta fase se detalla y configura todas las tecnologías con las que se llevará a cabo la implementación del proyecto, lo cual implica metodologías, técnicas y protocolos.
- Fase de diseño físico
  - En esta fase se realizará una comparación entre los componentes físicos que conformarán la red para escoger el que mejor cumpla con lo establecido en la fase de diseño lógico.
- Simulación, optimización y documentación del diseño

- Luego de culminar con las fases de configuraciones se realiza una prueba piloto para constatar la efectividad del proceso.

La propuesta de segmentación de red nos permitirá tener un mayor control sobre el tráfico de red, además de funcionar como una primera barrera en caso de ataques, nos permite aislar el ataque en un punto especifico y de igual manera mantenerlo controlado sin que se vean afectados los otros puntos de red.

Además, mediante la aplicación de políticas de seguridad se podrá tener un control sobre cada uno de los equipos conectados, mediante filtrados los equipos podrán tener acceso a la red, pero solo a los sitios permitidos y seguros, cabe mencionar que el trabajo no se encuentra dirigido a la creación de software para control de acceso ni de amenazas, todo lo implementado en el proyecto será bajo estándares y herramientas existentes, para tener un rendimiento óptimo de todos los recursos de red.

CAPÍTULO II

2. MARCO TEORICO Y METODOLOGIA DEL PROYECTO

2.1 MARCO CONCEPTUAL

2.1.1 RED DE TELECOMUNICACIÓN

Las redes surgen como respuesta a la necesidad de compartir datos de forma rápida. En su nivel más elemental, una red de equipos consiste en dos equipos conectados entre sí a través de un canal guiado, este puede ser cableado de tipo twister pair, coaxial o fibra óptica, esto permite compartir datos entre ellos, todos los tipos de redes sin importar su nivel de complejidad se basan en este modelo simple de transmisión. [25]

Cuando nos comunicamos, estamos compartiendo información, esta compartición puede ser local o remota, entre los individuos, las comunicaciones locales se producen habitualmente cara a cara, mientras que las comunicaciones remotas tienen lugar a través

de la distancia, el término telecomunicaciones, que incluye telefonía, telegrafía y televisión, significa comunicación a distancia (tele significa lejos en griego). [26]

2.1.2 Redes LAN

Las redes LAN son consideradas eficientes recursos tecnológicos que permiten el intercambio de información entre equipos de cómputo interconectados entre sí: son un conjunto de dispositivos interconectados que ocupa un lugar físico, como una oficina de una empresa o una habitación en el hogar; estas pueden ser grandes o pequeñas, y puede ir desde la conexión de un usuario a la red doméstica hasta miles que estén conectados a la red de una empresa, institución, organismo o corporación. [27]

Las redes de área local (Local Area Network) son un conjunto de dispositivos electrónicos conectados entre sí que comparten una línea de comunicación común o un enlace inalámbrico con un servidor, la conexión LAN abarca dispositivos y periféricos conectados a un servidor dentro de un área relativamente pequeña, como una oficina, sucursal o edificio. [28]

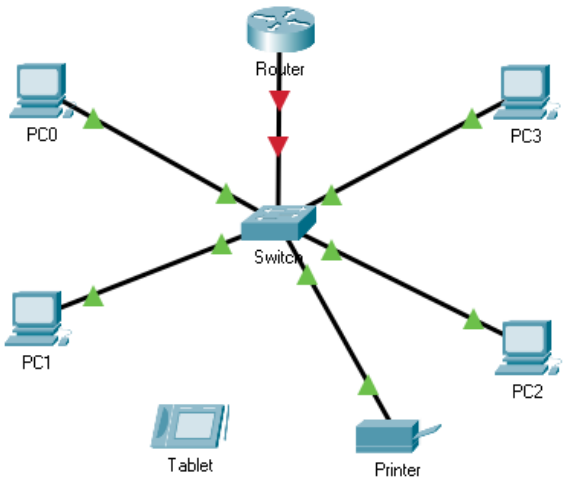


Figura 1 Diagrama de red LAN

2.1.3 IPv 4

IPv4 (Internet Protocol versión 4) es el formato de dirección estándar que permite que todas las máquinas en Internet se comuniquen entre sí. IPv4 se escribe como una cadena

de dígitos de 32 bits y una dirección IPv4 se compone de cuatro números entre 0 y 255, separados por puntos**,** es un protocolo sin conexión, lo cual significa que los datos se pueden enviar sin que las partes inviertan tiempo en establecer una conexión directa, y solo requiere pequeñas cantidades de memoria. [29]

2.1.4 Segmentación de redes

La segmentación de red es una técnica de seguridad que divide una red en distintas subredes más pequeñas, que permiten a los equipos de red compartimentar las subredes y otorgar controles y servicios de seguridad únicos a cada subred; El proceso de segmentación de red implica dividir una red física en diferentes subredes lógicas, una vez la red se ha subdividido en unidades más pequeñas y manejables, se aplican controles a los segmentos individuales compartimentados**.** [30]

2.1.5 VLAN

Una red de área local virtual (VLAN) es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo, puede crear redes VLAN para redes de área local que utilicen tecnología de nodo, al asignar los grupos de usuarios en redes VLAN, puede mejorar la administración de red y la seguridad de toda la red local; También puede asignar interfaces del mismo sistema a redes VLAN diferentes**.** [31]

La segmentación por Vlans permite: Crear una división lógica entre los grupos de trabajo, dividir grupos de trabajo en dominios de emisión administrables, designar diferentes directivas de seguridad para los grupos de trabajo, incrementar el desempeño de la red, incrementa el número de dominios y permite tener una mejor eficiencia del personal de TI. [32]

2.1.5.1 Enlaces Troncales de VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red, Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet. Las VLAN no serían muy útiles sin los enlaces troncales de VLAN, los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la

misma VLAN, pero conectados a distintos switches se puedan comunicar sin la intervención de un router. [33]

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red, Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet. [34]

2.1.7 Enrutamiento dinámico

El enrutamiento dinámico se basa en la utilización o empleo de protocolos de enrutamiento con el fin de automatizar el intercambio y la actualización de las tablas de enrutamiento de cada uno de los routers, estos protocolos comparten las tablas de enrutamiento de forma automática con los routers cercanos, lo que hace que su utilización sea recomendada para redes grandes. [35]

2.1.8 Enrutamiento Estático

Un protocolo de enrutamiento es un software complejo que se ejecuta de manera simultánea en un conjunto de routers, con el objetivo de completar y actualizar su tabla de enrutamiento con los mejores caminos para intercambiar información con otras redes, estos permiten, además: Mantener la información de enrutamiento actualizada de manera fiable. [36]

El enrutamiento estático lo proporciona el mismo administrador de red, aplica de forma manual todas las direcciones ip de cada dispositivo, basándose en una tabla de enrutamiento, por lo tanto, mantiene un control total sobre la red lo que permite tener una administración más personalizada. [37]

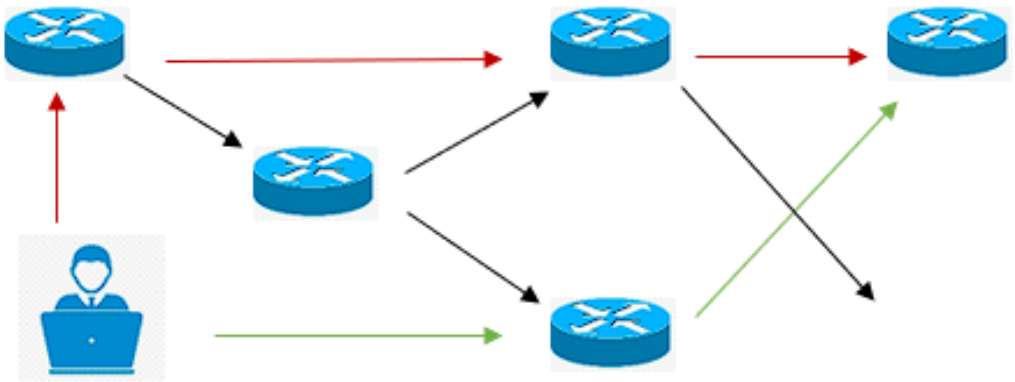


Figura 2 Protocolo de enrutamiento Estático (fuente autor)

2.1.9 Protocolo de enrutamiento 802.1Q

Creado en el año 2005, 802.1Q es, conocido también como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita segmentar una red física en varias redes lógicas, sin problemas de interferencia entre ellas, 802.1Q en realidad no encapsula la trama original, sino que añade 4 bytes al encabezado Ethernet original, todos los dispositivos de red que soportan VLAN siguen el estándar IEEE 802.1Q que especifica el funcionamiento y administración de LAN virtuales, en revisiones posteriores del estándar se decidió incluir IEEE 802.1D en IEEE 802.1Q. [38]

2.1.10 Servicio Proxy

Un servidor proxy (cuya traducción literal es "representante") es una interfaz de comunicación en una red que actúa como mediadora entre dos sistemas informáticos, la tarea básica de un servidor proxy es hacerse cargo, como delegado, de las peticiones de los clientes en un servidor y de transmitirlas con la dirección IP adecuada al ordenador de destino, en este tipo de comunicación no existe una conexión directa entre el remitente y el destinatario, en ocasiones, ni el sistema al que se le hacen las peticiones ni el ordenador de destino saben que hay un proxy de por medio. [39]

2.1.11 Squid

Squid es un proxy de almacenamiento en caché para la Web que admite HTTP, HTTPS, FTP y más, reduce el ancho de banda y mejora los tiempos de respuesta al almacenar en caché y reutilizar las páginas web solicitadas con frecuencia, Squid tiene amplios controles de acceso y es un excelente acelerador de servidores. Se ejecuta en la mayoría de los sistemas operativos disponibles, incluido Windows, y tiene licencia GNU GPL. [40]

Squid es usado como proxy-caché por miles de administradores web. Wikipedia, sin ir más lejos, utilizó durante años varios servidores proxy Squid para entregar los contenidos, con el objetivo de descongestionar la base de datos y el servidor web, asimismo, el hecho de soportar el protocolo HTTPS lo hace idóneo para establecer conexiones SSL seguras. [41]

2.1.12 Squidguard

SquidGuard es una herramienta que impulsa a mejorar las funciones de Squid, entre algunas de estas: ayuda a limitar el acceso web permitido para algunos usuarios a una

lista de servidores web y/o URL aceptados/conocidos solamente, mientras niega el acceso a otros servidores web y/o URL de la lista negra, bloquea el acceso a sitios por medio de dirección IP que coincidan con una lista de expresiones regulares o palabras para algunos usuarios, exige el uso de nombres de dominio/prohibir el uso de direcciones IP en las URL, redirige las URL bloqueadas a páginas de información o de error. [42]

2.1.13 Firewall

Los cortafuegos se utilizan para proteger las redes esenciales de los ataques externos para guiar el acceso a la red según las reglas de acceso del cortafuegos. El sistema de firewall juega un aspecto importante que protege del analista de reglas y del ataque maligno que brinda seguridad a todos los usuarios de Internet. [43]

Un cortafuegos o firewall es un servicio que permite filtrar información, a través del monitoreo constante del contenido entrante en la red, donde de acuerdo con las políticas establecidas por la compañía se decide si se bloquea o permite el tráfico. Para el sistema desarrollado el firewall será un filtro que protegerá a la red local del tráfico externo no deseado. [44]

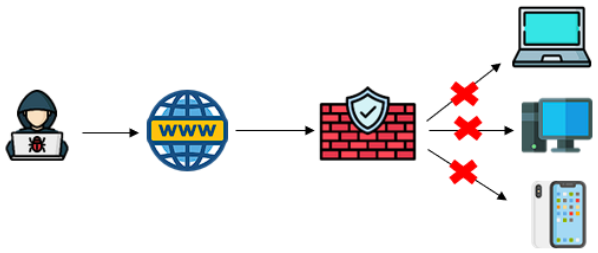


Figura 3 Firewall (fuente autor)

2.1.14 Pfsense

PfSense destaca entre las varias soluciones TI de cortafuegos o firewall disponibles en el mundo del software libre de código abierto ya que ofrece seguridad de nivel empresarial junto con características encontradas solamente en un software comercial, la seguridad es una de las partes más importantes de cualquier red de computadoras para asegurar la integridad de los sistemas, el software de protección actúa como una pared entre las redes internas y externas, detiene a los intrusos que pueden ser virus, troyanos o hackers, además monitorea el tráfico entrante y saliente para bloquear cualquier clase de ataque ya sea cracking, snooping, DDOs, etc. [45]

2.1.15 ACL

Una ACL dicho de manera más técnica es una lista de control de acceso, donde podremos observar que el router controlará el acceso de los paquetes y decidirá según la información que hemos añadido a nuestra ACL si descartar o reenviar los paquetes, algunas de las tareas que llevan a cabo las ACLs son: limitar el tráfico de red para aumentar el rendimiento, proporcionar control de flujo de tráfico, filtrar tráfico según el tipo de tráfico, proporcionar a nivel básico de seguridad para acceso a la red, pueden además filtrar a los host para permitirles o denegarles el acceso a los servicios de red. [46]

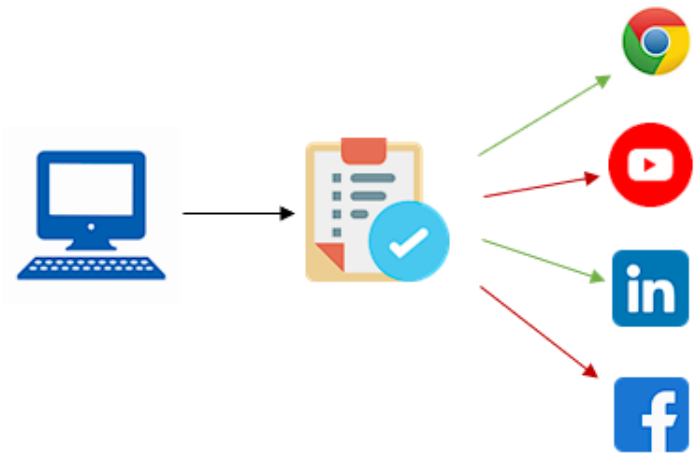


Figura 4. ACL sitios web (fuente autor)

2.1.16 HTTP

Hypertext Transfer Protocol (HTTP) (o Protocolo de Transferencia de Hipertexto en español) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web, aunque puede ser utilizado para otros propósitos también. Sigue el clásico modelo cliente-servidor, en el que un cliente establece una conexión, realizando una petición a un servidor y espera una respuesta de este. [47]

HTTP usa TCP aportando fiabilidad en la entrega de mensajes además de control de flujo y de congestión. Un detalle importante a tener en cuenta es que HTTP está diseñado para el envío esporádico de información, por lo que la creación de la conexión TCP cada vez

que se inicia una comunicación, da como resultado un gran aumento del ancho de banda consumido frente a otros protocolos**.** [48]

2.1.17 TCP

También conocido como TCP/IP (Internet Protocol) o Internet Protocol Suite, el TCP es un protocolo muy utilizado que rige la forma en que los ordenadores se comunican entre sí cuando intercambian datos. Sin embargo, La omnipresencia de TCP no significa que sea el único protocolo de transferencia de datos que existe. [49]

El protocolo TCP está orientado a brindar una conexión fiable y segura, de modo que cuenta con las siguientes características, es orientado a conexión ya que obliga una conexión previa entre maquinas antes de transmitir algún dato, debe ser fiable, la información que se envía desde el emisor llega de forma correcta al destino**.** [50]

2.2. MARCO TEÓRICO

2.2.1 Información, el principal activo dentro de toda organización.

Actualmente, la seguridad informática es un tema que debería ser de conocimiento para toda persona que haga uso de las redes de internet, esto para que su información no quede comprometida ante las posibles debilidades de la red o ataques que se puedan dar hacia esta, dentro del trabajo de investigación "POLITICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH " se mencionan algunas características con las que debe contar la información entre las cuales se destacan la integridad, Confidencialidad, Disponibilidad e Irrefutabilidad, dentro de este mismo trabajo se muestra la relación que tiene la información con la informática y a su vez la seguridad dentro de una empresa. [51]

Para salvaguardar los datos de una empresa se recomienda la instalación de protocolos de seguridad, estos garantizan la seguridad y la integridad de los datos cuando se encuentran viajando de un punto a otro, dentro de los principales se encuentran: Protocolo TCP/IP, Protocolo HTTP, FTP y DNS, estos son los protocolos de protección de red más conocidos y más usados. [52]

2.2.2 VLANS dentro de una institución

El uso de VLANS ayuda a mejorar de forma eficaz la administración de la red, además de controlar patrones de tráfico y mejorar tiempos de respuesta y capacidad de dispositivos conectados a la red, son algunos de los factores que se mejoraron al implementar una correcta segmentación por VLANS como lo indica el trabajo de Titulación "DISEÑO E IMPLEMENTACIÓN DE VLANS PARA MEJORAR LA EFICIENCIA DE TRANSMISIÓN DE DATOS EN LA MUNICIPALIDAD PROVINCIA DE HUANCAYO". [53]

Una correcta implementación de una red basada en vlans puede ser la solución a problemas de conexión y administración dentro de la misma, en el proyecto "INSTALACIÓN Y CONFIGURACIÓN DE UN SWITCH CON VLANS PARA LA MEJORA DE RENDIMIENTO DE ANCHO DE BANDA DE LA RED" se nos muestra como una aplicación exitosa logro mejorar la conexión para uso de aplicaciones de video conferencia y de forma general mejoro los servicios que se brindan dentro de la empresa Skyguardian. [54]

2.2.3 Proxy para mejorar conexión y seguridad de red.

El servicio proxy tiene entre uno de sus objetivos el dar acceso a la red mediante una dirección ip. Para que esto funciones, un ordenador debe desempeñar el rol de servidor, este contendría dicha dirección ip, el servicio proxy tiene el control total de las conexiones que se realicen dentro de la red, de un cliente hacia un servidor de destino, esto permite que exista un acceso más rápido a las páginas web, ya que el servicio mantiene almacenado el cache de las páginas más solicitadas, y se vuelve más corto el periodo de carga. [55]

Dentro del proyecto "PROPUESTA DE INTERCEPTOR PROXY COMO MODELO DE ACCESO SEGURO A UN ENTORNO WEB, PARA EL CONSORCIO INFRAESTRUCTURA EDUCATIVA 2016" vemos como con la implementación de un servicio proxy se concluye que es fundamental dentro de cualquier empresa que se esfuerce en mantener la seguridad tanto de sus sistemas como de su información, la seguridad de los datos o ciberseguridad, se enfoca en la protección de la infraestructura principalmente en la información que está contenida en los diferentes dispositivos de la red. [56]

2.3. METODOLOGÍA DEL PROYECTO

2.3.1 METODOLOGÍA DE INVESTIGACIÓN

Para conocer el estado actual de red de la unidad educativa a un nivel superficial, se realizó una entrevista dirigía a la rectora de la unidad y al docente de informática encargado de los laboratorios, además se utilizó técnicas de observación basadas en la metodología de diagnóstico [57]. La variable que se deberá demostrar es: Optimización del nivel de cumplimiento lógico de la red LAN en el área del edificio administrativo y laboratorios.

Se consideró el uso de una metodología exploratoria, esta es un tipo de investigación que se utiliza para estudiar un problema que no se encuentra definido de forma clara, es utilizada para investigaciones del comportamiento del problema [58]. para llevar a cabo esta metodología es necesario seguir una serie de pasos y fases para tener resultados apropiados, además de aplicar diferentes métodos de recolección de información como encuestas, entrevistas e investigaciones de otros proyectos que le anteceden al que se encuentra en desarrollo.

2.3.2 TÉCNICAS DE RECOLECCIÓN DE INFORMAICIÓN

Para la recolección de información se emplearon dos técnicas, una basada en entrevistas dirigidas al personal que labora en las instalaciones de la Unidad Educativa además del uso de técnicas de observación para verificar el estado físico de la red, esto para recolectar toda la información posible de los equipos físicos de la red institucional, esto ayudo a crear un nuevo diseño en donde los equipos se encuentren ubicados de forma estratégica para mejorar la cobertura de la red.

Entrevistas

Una de las técnicas utilizadas para la recolección de la información fue el uso de entrevistas dirigidas al personal de la Unidad, en este caso se realizaron dos entrevistas, una hacia la rectora de la unidad (Anexo 1) y otra dirigida al docente encargado del área de computación y de los dos laboratorios que se encuentra en la institución (Anexo 2).

Con estas entrevistas que se realizaron se pudo conocer algunos de los principales problemas con los que cuenta la red, para tener un mejor análisis se estudiaron cada uno

de los puntos de las entrevistas, en base a esto se propuso la posible solución a cada uno de los problemas que se exponen.

Entrevista dirigida a la rectora de la institución y al docente encargado de laboratorios.

En las entrevistas que se realizaron al personal de la institución se pudo extraer información importante a tener en cuenta para el desarrollo de la propuesta de rediseño, uno de los puntos principales que se pudo notar es que la red en todo el tiempo que lleva funcionando no ha crecido ni ha tenido la debida administración, ambos entrevistados indican que la red tiene fallos en el diseño, de modo que existen puntos donde no se puede acceder a ella, dentro de la administración con la que se cuenta no se sigue ningún protocolo que garantice mantener una conexión estable, además, las medidas de seguridad no son las apropiadas, se cuenta con medidas de seguridad básicas.

Otro de los puntos a tener en cuenta es la cantidad de estaciones de trabajo y de usuarios que hacen uso de la red, lo principal es mantener una conexión estable en el área administrativa y el área de los laboratorios, siendo estos los puntos más indispensables en el desarrollo de las actividades académicas en el día a día.

Ambos entrevistados llegaron a la conclusión de que es necesario un rediseño de la red y aparte la implementación de mecanismos de seguridad, esto para tener un mejor control de la red y a su vez mejorar la conectividad, evitando así el acceso masivo de dispositivos ajenos a la institución y el ingreso a páginas web que demandan demasiado uso del ancho de banda de la red.

Observación

Se aplico la técnica de observación para analizar de forma directa la institución con la que se va a trabajar, esta técnica se basó en la recolección de datos e información sobre cada una de las áreas que se pretender intervenir, para lograr esta técnica fue necesario planear una visita técnica a la institución con el fin de observar de forma directa el área, características y funciones con las que cumple la red, la información recolectada se fue redactando en una ficha (Anexo 3) en donde se especificaron los aspectos físicos de la red.

Algunos de los puntos clave que se lograron observar fue la presencia de una mala gestión de los dispositivos de red, los mismos que no se encuentran ubicados en la infraestructura adecuada, el cuarto de redes con el que se cuenta no tiene una correcta administración de cableado, este mismo se encuentra expuesto ya que las canaletas en por las que pasa el cableado ya se encuentran deterioradas.

Otro de los factores que podrían estar causando inconvenientes es que en algunos sectores el cableado de red se encuentra ubicado en las mismas canaletas por donde pasa el cableado eléctrico, esto se debe evitar para disminuir posibles interferencias que se puedan causar entre ambos tipos de cableado (Anexo 14).

Se cuenta con un número elevado de dispositivos que tiene acceso mediante cableado, pero no se cuenta con antenas o repetidores que faciliten el acceso mediante wifi en los diferentes puntos de la institución.

2.3.3. METODOLOGIA DE DESARROLLO DEL PROYECTO

En este apartado se expondrá toda la información relevante para llevar a cabo el rediseño de una red LAN, el proyecto se basó en la metodología TOP-DOWN establecida por CISCO, dicha metodología está basada principalmente en el ciclo de vida de redes PPDIOO de modo que para el desarrollo será necesario tener en cuenta conceptos de ambos puntos.

Ciclo de vida CISCO para redes (PPDIOO)

La metodología PPDIOO posee su origen bajo los lineamientos propuestos en el ciclo de vida PPDIOO que usa Cisco para administración de red, el seguimiento de este ciclo de vida propuesto ayuda a cumplir objetivos trazados como son la disminución del costo total de administración de la red y aumento de disponibilidad de la red a su vez mejora en agilidad para implementación de cambios en la estructura de la red. [59]

A continuación, se presenta la ilustración que detalla el proceso de esta metodología

Figura 5. Ciclo de vida PPDIOO (fuente autor)

Fases del ciclo de vida PPDIOO

Preparar

En esta fue necesario identificar los requerimientos de la red, de igual manera se realizó un análisis para verificar todo lo que afecta a la infraestructura de comunicaciones de la Unidad Educativa.

Planear

Se elaboro un plan para analizar las fallas y funcionalidades de todos los componentes de la red.

Diseñar

Se realizo un diseño tomando en cuenta los requerimientos técnicos sobre la infraestructura, servicios y aplicaciones, además de que se hace uso de diagramas y listas de los equipos utilizados.

Implementar

Esta fase siempre estará ligada a las tres que le anteceden, en esta etapa se incluyó la descripción, guías y cronogramas de las actividades que se realizaron durante todo el proyecto.

Operar

Esta fase siempre estará ligada al seguimiento y mantenimiento del proyecto, con una constante administración y corrección de errores.

Optimizar

Para que el ciclo de vida se complete, es necesario tener un constante monitoreo y mitigación de errores que puedan afectar en un futuro a la infraestructura.

Metodología de Diseño de redes Cisco (Top-Down Network Desing)

La metodología Top-Down propuesta por Cisco Press & Priscilla Oppenheimer se basa en las necesidades de análisis de requerimientos y diseño arquitectónico de las redes de comunicación, que debe realizarse antes de la selección de determinados componentes específicos para construir la red física. Un proceso Top-Down describe las múltiples fases por las que una red atraviesa utilizando el llamado ciclo de vida de redes PDIOO (planificación- diseño- implementación-operación- optimización) [60]

Esta metodología cuenta de las siguientes cinco fases que se detallan a continuación:

Fase de recolección de datos de infraestructura

Se realizo la recolección de información que contenga las características de la red, aspectos lógicos y físicos, lo que incluye el diseño actual y los componentes físicos con los que se cuenta.

Fase de análisis de los requerimientos

Dentro de esta fase fue necesario enfocarse en las metas propuestas por la Unidad Educativa, partiendo de esto, se analizaron los requerimientos, objetivos y limitación con las que se cuenta, se utilizó como fuente de consulta al personal que labora dentro de la institución, en cuento a la red se analizó y describió tanto a nivel físico como lógico, esto para tener un panorama claro del área en el que se va a intervenir.

Fase de diseño lógico

En esta fase se diseñó la topología propuesta para la red, dentro de este apartado se mostraron los tipos de enrutamiento que se implementaron, además de que se establecieron los protocolos de comunicación y los mecanismos de seguridad para la gestión y mantenimiento de la red.

Fase de diseño físico

Esta fase se centró en la selección de equipos y tecnologías que se implementaron, esto se realizó teniendo en cuenta el análisis y diseño de las fases anteriores, se buscó los

equipos que más se ajusten a las necesidades de la institución, se realizó un estudio en el cual se compararon las características de las marcas más conocidas en el mercado.

Prueba y documentación del diseño

En esta fase se realizaron las pruebas de conexión mediante una simulación, lo que permitió identificar posibles errores de configuración que posteriormente fueron solucionados, con esta simulación se pudo realizar un monitoreo de rendimiento y seguridad, con los datos que se extrajeron de esta fase se realizó se procedió a realizar la documentación respectiva, donde se detallan todas las características del nuevo diseño y de las medidas de seguridad que se implementaron.

CAPÍTULO III

3. PROPUESTA

3.1 Componentes de la Propuesta

3.1.1 Fase 1: Recolección de datos de infraestructura.

Esta fase se basó en la recolección de datos de la red, se implementaron técnicas de recolección como entrevistas, las cuales están dirigidas a la rectora de la unidad educativa y al docente encargado de los laboratorios de computación y de la red de la institución, además de realizar la debida observación de cada uno de los puntos y de la infraestructura con la que cuentan tanto el edificio administrativo como el laboratorio de computación.

Característica	Detalle
Redes	• Red General (UELL LA LIBERTAD)
Edificio administrativo	• Oficina de rectorado • Oficina de vicerrectorado • Oficina de secretaria • Oficina de orientación • Cuarto de redes
Pabellones de aulas	• 5 pabellones de 3 aulas • 1 pabellón de 5 aulas

Pabellones de laboratorios	• 1 pabellón con dos laboratorios de cómputo y biblioteca • 1 pabellón con 3 laboratorios de otras ciencias

Tabla 1: datos extraídos de entrevista (fuente autor)

3.1.1.1 Situación del edificio administrativo.

Edificio administrativo			
Descripción	Planta	Estaciones de trabajo	Medio
Oficina de rectorado	Alta	1	Cableado - Wifi
Oficina de vicerrectorado	Alta	1	Cableado - Wifi
Cuarto de redes	Alta	1	Cableado - Wifi
Oficina de secretaria	Alta	2	Cableado - Wifi
Oficina de orientación	Baja	1	Cableado - Wifi
Laboratorio 1	Baja	14	Cableado - Wifi
Total de equipos		**20**	

Tabla 2: Situación del edificio administrativo (fuente autor)

3.1.1.2 Situación del pabellón de laboratorios

Pabellón de laboratorios		
Descripción	Estaciones de trabajo	Medio
Laboratorio 2	13	Cableado - Wifi
Biblioteca	7	Cableado - Wifi
Total de equipos	**20**	

Tabla 3: situación de pabellón de laboratorios (fuente autor)

3.1.1.3 Situación de la red

Red		
Descripción	Subredes	Seguridad
Red General (UELL LA LIBERTAD)	UELLA	WPA – WPA2

Tabla 4: situación de la red (fuente autor)

3.1.1.4 Servicios de red

La red aparte de ser utilizada para proveer el servicio a internet también cuenta con algunos servicios extras, que se muestran a continuación:

Servicios	
Servicio	Descripción
Video vigilancia	Cámaras de video ubicadas en el pabellón de laboratorios de cómputo y edificio administrativo, este servicio se encuentra deshabilitado.
Impresoras IP	Equipos de impresión ubicados en el edificio administrativo
Video conferencia	Uso de aplicaciones como Zoom y Microsoft teems para realizar clases virtuales
Conexión cableada	Servicio dirigido a las estaciones de trabajo de las oficinas y laboratorios.
Wifi	Conexión inalámbrica en toda el área de la unidad

Tabla 5: Servicios de red (fuente autor)

3.1.1.5 Topología actual

La red de la unidad educativa cuenta con una topología de red basada en el formato Árbol, esta topología esta desarrollada de forma básica, el punto central se encuentra en el cuarto de redes, de la cual parten cada uno de los diferentes puntos de acceso hacia las oficinas y los laboratorios de computación.

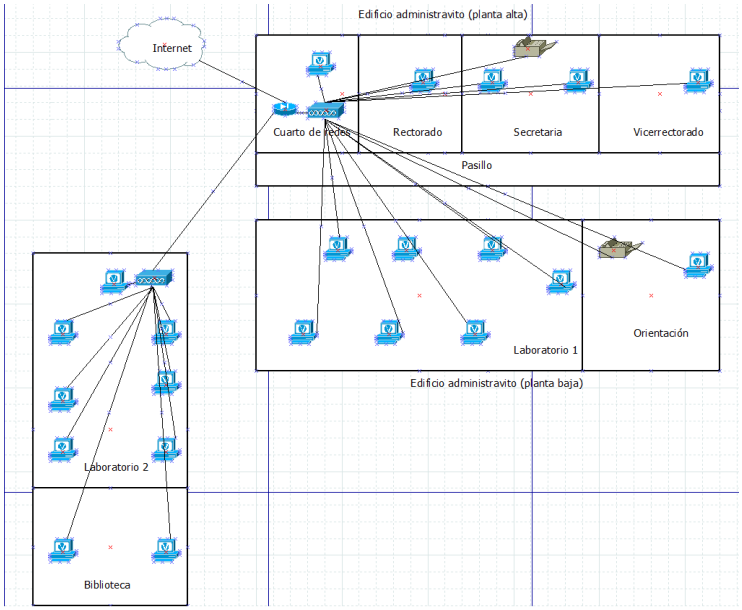


Figura 6 Topología actual de red (fuente autor)

3.1.1.6 Tecnologías de seguridad

Las redes de la unidad cuentan con la protección básica WPA y WPA 2, estos funcionan de forma eficiente, pero están dirigidos más para redes de hogares, de modo que es necesario la implementación de políticas de seguridad.

3.1.1.7 Descripción de equipos

Equipos de red	
Equipo	Descripción
Repetidor Tp Link	• Frecuencia 2.4 GHz • Seguridad WPS WPA2 • WIFI 802.11n
Repetidor Ubiquiti Networks	• Frecuencia 2.4 GHz • Seguridad WPA2 • WIFI 802.11n
2 Nexxt Switch 24 Port 10/100 Mbps Fast Ethertet Switch	• Cantidad de puerto: 24 • Montable en bastidor y rack

	• Protocolo de interconexión: IEEE 802.3
Router Huawei EchoLife EG8145V5	• Tecnología GPON • Frecuencia 2.4 G y 5 G • Banda de doble frecuencia 802.11 IEEE 802.11 b / g / n (2.4G) IEEE 802.11 a / n / ac (5G)

Tabla 6: Equipos de red (fuente autor)

Equipos de computo	
Equipo	Descripción
12 equipos	• Sistema operativo Windows 10 • Procesador Core i3 • Memoria RAM 4 gb • Almacenamiento 500gb • Conectividad Cableada
5 equipos	• Sistema operativo Windows 10 • Procesador Intel celeron • Memoria RAM 4 gb • Almacenamiento 1tb • Conectividad Cableada
8 equipos	• Sistema operativo Windows 10 • Procesador Core i5 • Memoria RAM 4 gb • Almacenamiento 1tb • Conectividad Cableada
15 equipos	• Sistema operativo Windows 7 • Procesador Intel celeron • Memoria RAM 4 gb • Almacenamiento 500gb • Conectividad Cableada

Equipos wifi	• Teléfonos inteligentes • Tablets • Portátiles

Tabla 7: Equipos de cómputo (fuente autor)

3.1.2 Fase 2: Análisis de requerimientos

Para realizar un correcto análisis de los requerimientos de la red, es necesario tomar en cuenta los siguientes puntos: analizar las metas y restricciones de la unidad o negocio, características de la infraestructura actual de la red, topología lógica y física**,** características del tráfico de red y rendimiento actual, además de esto es necesario tomar datos directos de los usuarios**.**

Código	Especificación de requerimientos
RQ-1	El análisis se debe implementar tomando en cuenta cada una de las áreas dentro de la institución.
RQ-2	Se deberán realizar estudios para evaluar el presupuesto que tomaría la implementación del proyecto, especificando equipos y características de estos.
RQ-3	El diseño que se proponga deberá especificar cada uno de los puntos de acceso por área.
RQ-4	Para la implementación del servicio proxy será necesario un equipo con Windows 10, procesador Intel Core I5, 500GB de almacenamiento y 8 Gb de ram.
RQ-5	Las políticas de seguridad se basarán tanto en el medio lógico y físico de la red.
RQ-6	Se realizará la simulación en un laboratorio virtual, en el cual se implementará la red LAN con todas las características de la red de la Institución.
RQ-7	Para la simulación se utilizará pfsense como herramienta principal.

RQ-8	Se establecerán las tablas de direccionamiento basadas en la cantidad de dispositivos con los que cuenta la unidad educativa.
RQ-9	Cada punto de acceso tendrá un límite de usuarios que se pueden conectar de manera simultánea.
RQ-10	El acceso de dispositivos se regirá al horario que se establezca en las ACL
RQ-11	El ordenador que funcione como servidor proxy deberá mantenerse activo durante 2 horas durante la simulación para generar el análisis en tiempo real.
RQ-12	Durante la simulación, los equipos conectados a la red deberán mantener conexión con los diferentes servicios que hagan uso de internet, para evaluar el comportamiento de la red.
RQ-13	Se redactarán las características de los equipos que se utilizarían.
RQ-14	Se documentará el diseño de la red, especificando cada uno de sus puntos de acceso, áreas en las que se encuentran y cobertura que brindarían.
RQ-15	El documento final debe presentar un plan de mejora u optimización.

Tabla 8: Requerimientos (fuente autor)

3.1.3 Fase 3: Diseño Lógico

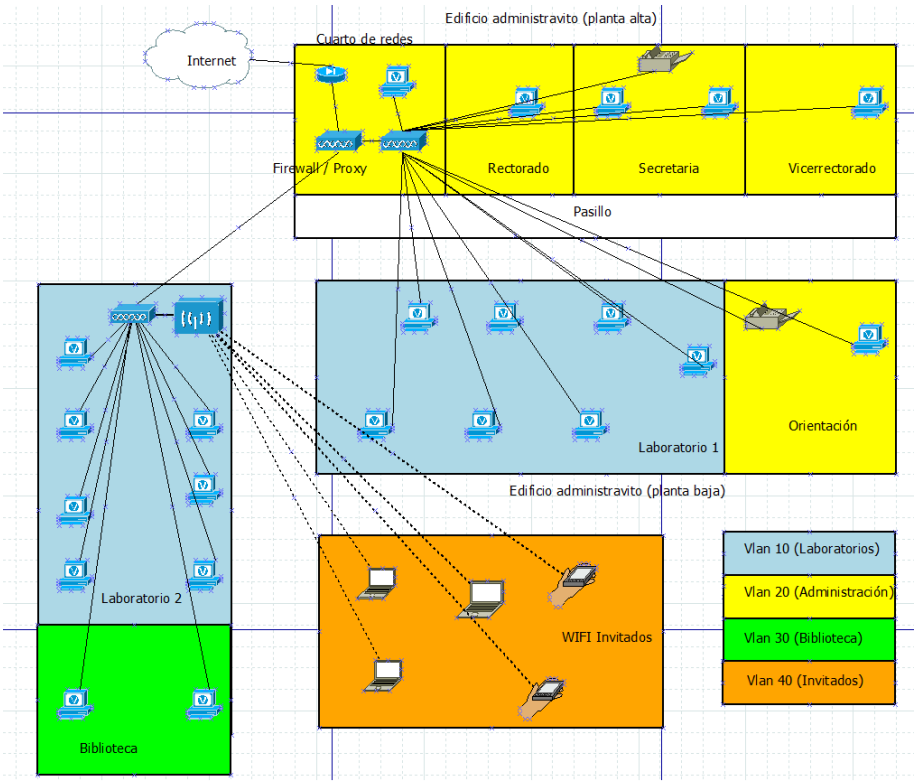


Figura 7 Propuesta de topología (fuente autor)

3.1.3.1. Detalles de la topología

La topología de la red utilizada está en formato árbol y está conformada de la siguiente manera.

- Router principal
- Switch de firewall Pfsense
- Switch Troncal
- Switch administración PT-A
  - ❖ Vlan 20
  - ❖ 5 pc cableadas
  - ❖ 1 impresora
- Switch administración PT-B
  - ❖ Vlan 10 y Vlan 20
  - ❖ 15 pc cableadas
  - ❖ 1 uso docente (laboratorio)
  - ❖ 13 uso estudiantes (laboratorio)
  - ❖ 1 uso administrativo
- Switch LAB
  - ❖ Vlan 30 y Vlan 40
  - ❖ 20 pc cableadas
  - ❖ 12 uso estudiantes (laboratorio)
  - ❖ 1 uso docente (laboratorio)
  - ❖ 6 uso biblioteca
  - ❖ 1 administrativo (biblioteca)
  - ❖ Router Inalámbrico (invitados Wifi)

3.1.3.2. Políticas de seguridad

Otro método de seguridad para salvaguardar la integridad lógica y física de los equipos pertenecientes a la red y de la información que se aloja dentro de la misma, es la creación de políticas de seguridad, para esto se generó un manual para la Unidad Educativa La Libertad, este manual cuenta con las principales directrices que deberán ser cumplidas por parte del personal académico, administrativo, estudiantil e invitados que lleguen a la

institución, cabe recalcar que dichas políticas están dirigidas para asegurar tanto el medio lógico como físico de la red, la documentación correspondiente al manual se encuentra redactada en el (Anexo 4) "MANUAL DE POLÍTICAS DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA LA LIBERTAD", el cual está basado en el Manual de Políticas de Seguridad Informática de la Universidad Estatal Península de Santa Elena. [61]

3.1.3.3. Tablas de enrutamiento

Para la creación de la red se utilizará el protocolo de enrutamiento estático. Las rutas estáticas son definidas por un administrador que quiera establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino, se establece un control preciso del enrutamiento según los parámetros del administrador. [62]

Para esto se utilizan las tablas de direccionamiento y de asignación de puertos, las cuales están elaboradas de acuerdo con la decisión del administrador y de acuerdo con la configuración que se realizara en la estructura de la red.

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway predeterminado
R1	Fa0/0.1	192.168.110.1	255.255.255.0	N/A
	Fa0/0.2	192.168.120.1	255.255.255.0	N/A
	Fa0/0.3	192.168.130.1	255.255.255.0	N/A
	Fa0/0.4	192.168.140.1	255.255.255.0	N/A
STroncal	--	--	--	--
SW PT-A	VLAN 20	N/A	N/A	N/A
SW PT-B	VLAN 10 - 20	N/A	N/A	N/A
SW LAB	VLAN 10-30 - 40	N/A	N/A	N/A
WR 1	VLAN 40	192.168.140.252	255.255.255.0	192.168.140.1
Impresora 1	VLAN 20	192.168.120.15	255.255.255.0	192.168.120.1
PC1	VLAN 10	192.168.110.2	255.255.255.0	192.168.110.1
PC2	VLAN 10	192.168.110.3	255.255.255.0	192.168.110.1

PC3	VLAN 10	192.168.110.4	255.255.255.0	192.168.110.1
PC4	VLAN 10	192.168.110.5	255.255.255.0	192.168.110.1
PC5	VLAN 10	192.168.110.6	255.255.255.0	192.168.110.1
…	VLAN 10	…	…	…
PC28	VLAN 10	192.168.110.28	255.255.255.0	192.168.110.1
PC29	VLAN 20	192.168.120.2	255.255.255.0	192.168.120.1
PC30	VLAN 20	192.168.120.3	255.255.255.0	192.168.120.1
---	VLAN 20	---	255.255.255.0	192.168.120.1
PC33	VLAN 20	192.168.120.6	255.255.255.0	192.168.120.1
PC34	VLAN 30	192.168.130.2	255.255.255.0	192.168.130.1
---	VLAN 30	---	255.255.255.0	192.168.130.1
PC40	VLAN 30	192.168.130.8	255.255.255.0	192.168.130.1
Equipo invitado	VLAN 40	192.168.140.2	255.255.255.0	192.168.140.1
Equipo invitado	---	---	---	---
Equipo invitado	VLAN 40	192.168.140.150	255.255.255.0	192.168.140.1

Tabla 9. Tabla de direccionamiento de red (fuete autor)

3.1.3.4. Asignación de puertos

Dispositivo	Puertos	Asignación	Red
Switch troncal	Fa0/1 - 0/4	Enlaces troncales 802.1q	--
SW PT-A	Fa0/1 – 0/10	Vlan20 - Administración	192.168.120.0/24
	Fa0/24	Enlace Troncal	--
SW PT-B	Fa0/1 – 0/16	Vlan10 - Laboratorios	192.168.110.0/24
SW LAB	Fa0/1	Vlan40 – Invitados	192.168.140.0/24
	Fa0/2 – 0/14	Vlan10 - Laboratorios	192.168.110.0/24
	Fa0/15 – 0/22	Vlan30 - Biblioteca	192.168.130.0/24
	Fa0/24	Enlace Troncal	--

Tabla 10: Tabla de asignación de puerto (fuete autor)

3.1.3.5 Configuración de red (Simulación)

Para realizar la simulación de la configuración de la red se siguió el estándar IEEE 802.1Q, es el estándar IEEE para etiquetar tramas en un enlace troncal y admite hasta 4096 VLAN. En 802.1Q**,** el dispositivo de enlace troncal inserta una etiqueta de 4 bytes en la trama original y vuelve a calcular la secuencia de verificación de trama (FCS) antes de que el dispositivo envíe la trama por el enlace troncal. [63]

Se utilizo la herramienta Packet Tracer en su versión 8.1.1.0022 para realizar la simulación de la topología de la red**,** al igual que para realizar las configuraciones correspondientes de los equipos para llevar a cabo la segmentación por vlans, dichas configuraciones pueden ser observadas en el (Anexo 5)**.**

3.1.3.6 Creación de laboratorio virtual

Para la creación del laboratorio virtual se empleó la herramienta Proxmox la cual permitió crear la máquina virtual de Pfsense dentro del equipo anfitrión, la configuración de esta herramienta se la puede observar en el (Anexo 6), seguido a la configuración de Proxmox se realizó la instalación de Pfsense (Anexo 7)**.**

Asignación de ip dentro de consola de pfsense

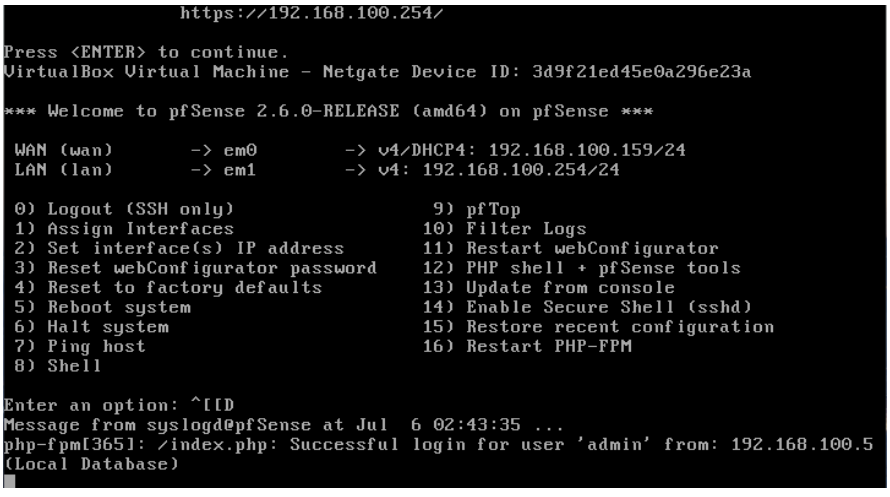


Figura 8: Direcciones Ip establecidas por defecto (fuente autor)

Para asignar una dirección ip a una de las interfaces de red, se selecciona la opción 2 (Set interfaces IP address) y se escoge la interfaz para luego asignar las direcciones ip.

En este caso la dirección ip de la red Wan se la asigna mediante dhcp y la ip de la red Lan se la asigna de forma estática.

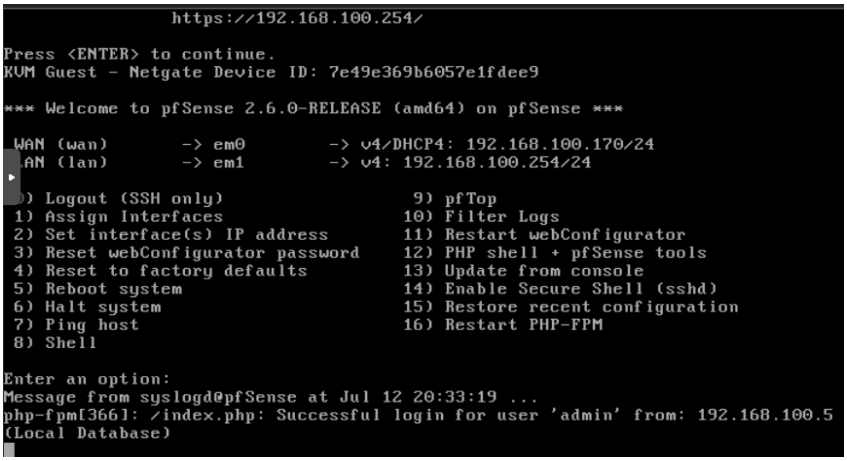


Figura 9: Direcciones Ip establecidas de forma estática (fuente autor)

Para acceder al dashboard de pfsense nos dirigimos al navegador de la maquina e ingresamos con la dirección ip que se le asigno a la red LAN. Lo primero que mostrará será la configuración básica, en la que se agregará un usuario y contraseña, se asignará una zona horaria, se establecerá la dirección ip y se deberá habilitar el protocolo DHCP de forma temporal, esta configuración se la detalla en el (Anexo 8).

Configuración de Vlans

Una de las características que tiene pfsense es que permite la configuración y administración de vlans desde su entorno gráfico, para empezar con la configuración de estas primero será necesario dirigirse al apartado de Interfaces/VLANS para crear las vlans necesarias

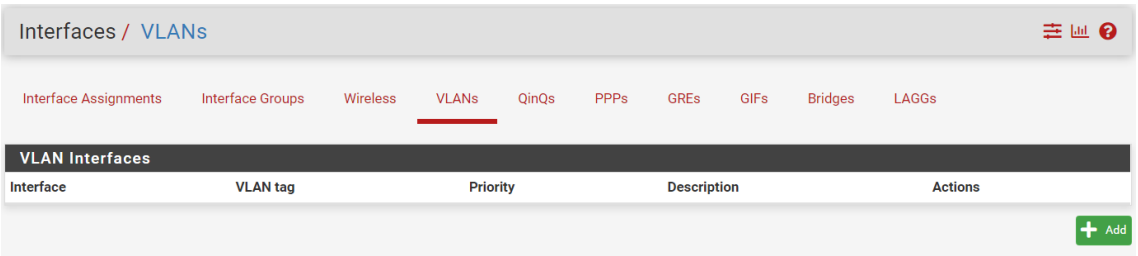


Figura 10: Ventana de Vlans (fuente autor)

Dentro de este apartado se asigna la interfaz de la que partirá la VLAN, en este caso la interfaz em1 perteneciente a la red LAN, seguido a eso se le asigna la etiqueta y la descripción

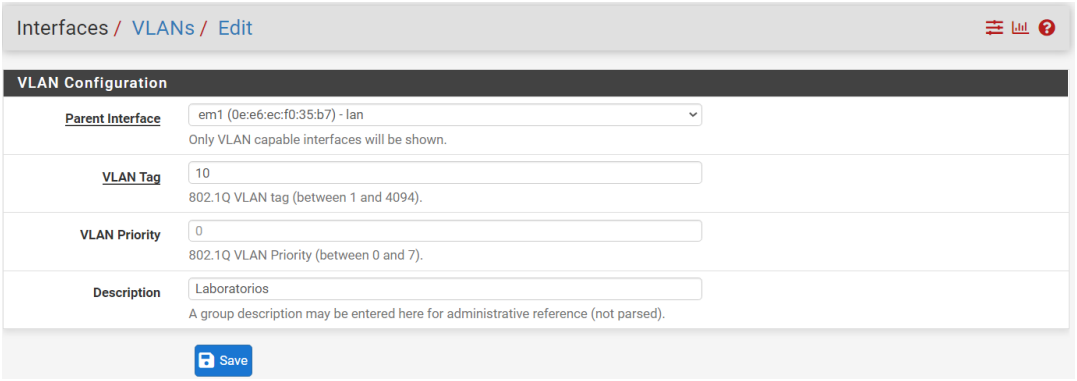


Figura 11: Etiqueta de Vlan (fuente autor)

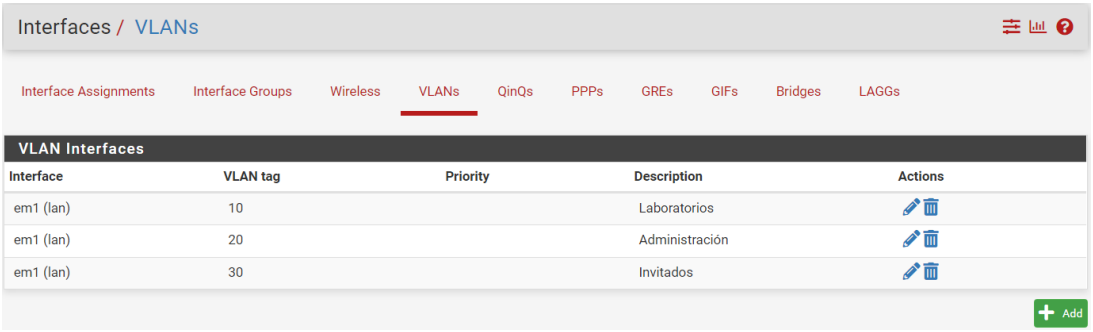


Figura 12: Vlans creadas (fuente autor)

Una vez creada las VLANS se selecciona la opción Interface Assignment, dentro de esta se listarán las vlans creadas y los puertos que están disponibles para que sean asignados.

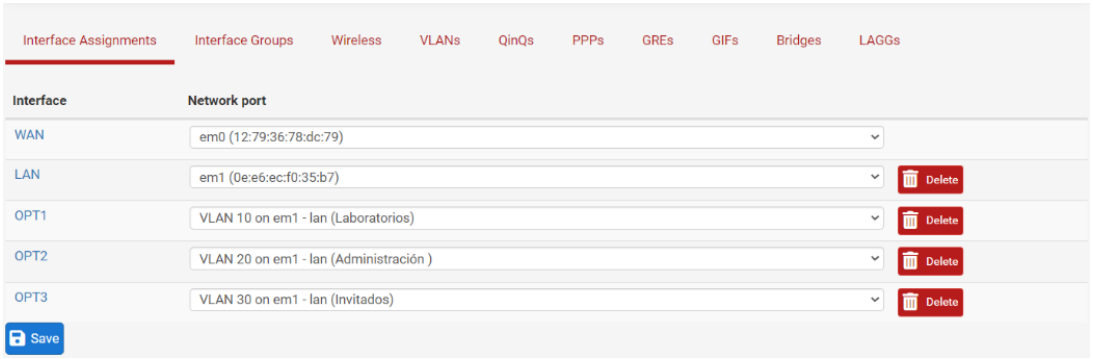


Figura 13: asignación de puertos a vlans (fuente autor)

Luego de haber creado las vlans necesarias, se procese a levantar cada una de estas, dentro de las opciones de configuración se las renombra de acuerdo con el orden que se crearon o la ubicación en la topología

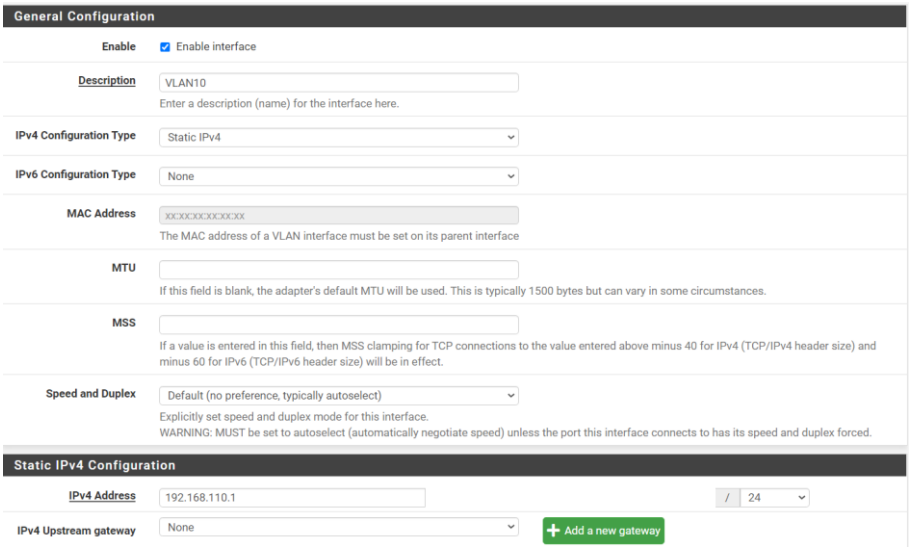


Figura 14: Activación de Vlan (fuente autor)

Una vez creadas y levantadas las vlans se podrán observar en la ventana principal del dashboard, en el cual nos reflejara el estado, la etiqueta y la dirección de cada una de las redes que tenemos disponibles.

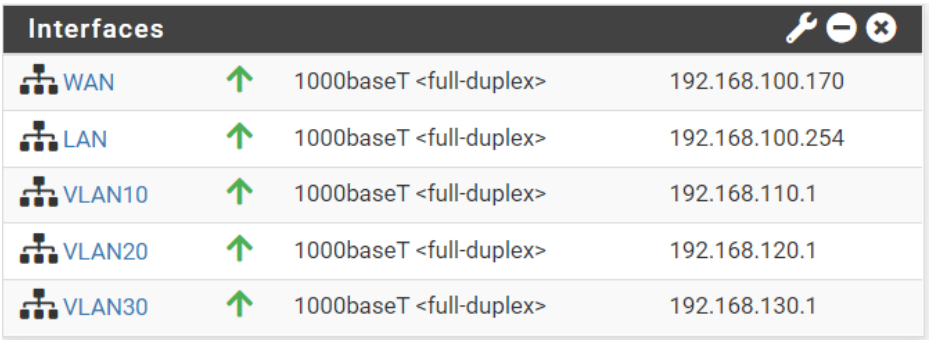


Figura 15: Redes activas en entorno grafico (fuente autor)

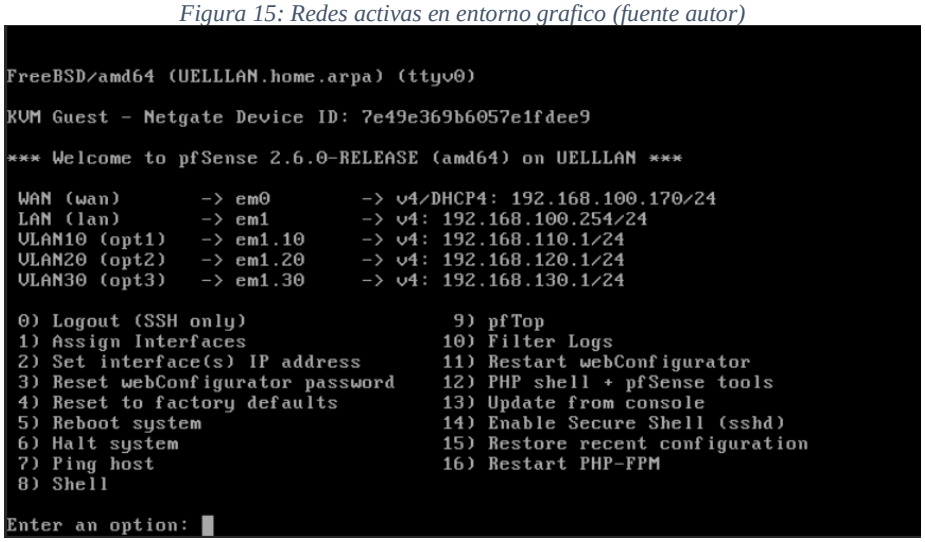


Figura 16: Redes activas en consola Pfsense (fuente autor)

Asignación de IP a dispositivos de la red

Configuración DHCP server

Para asignar direcciones IP de forma estática es necesario configurar el servicio DHCP, en el cual asignaremos un rango de dirección IP que se determinaran mediante el servicio dejando libres el resto de las direcciones para proceder con la asignación estática

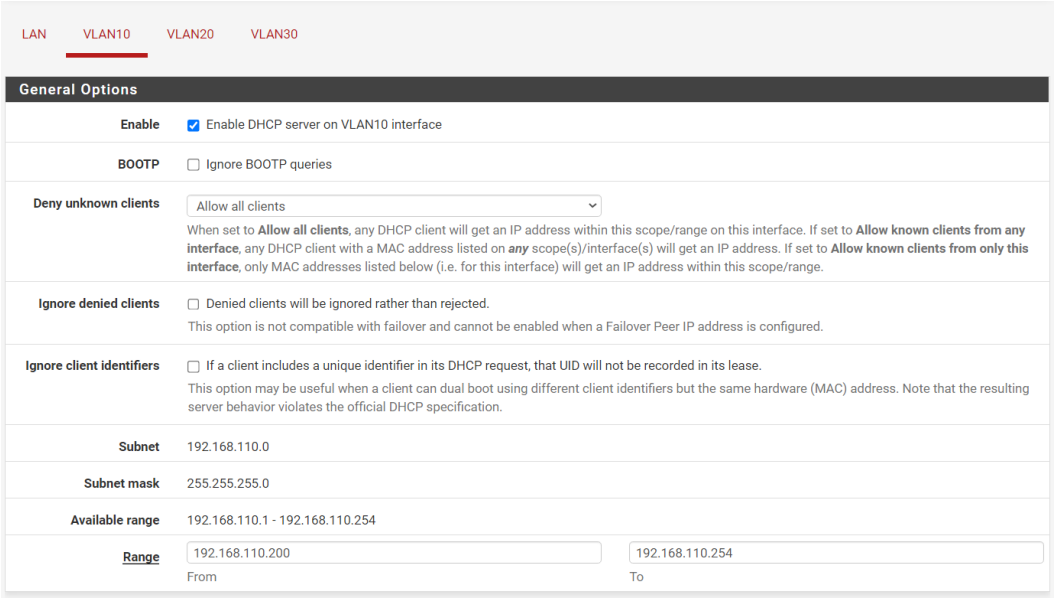


Figura 17: Habilitación de protocolo DHCP (fuente autor)

Dirigirse a la tabla (DHCP Static Mappings for this Interface) para agregar las direcciones de forma estática. Para proceder con la asignación de las direcciones IP, es necesario conocer la dirección MAC del dispositivo, luego de haber ingresado la dirección MAC llenamos los campos principales para asignar la dirección IP y hostname

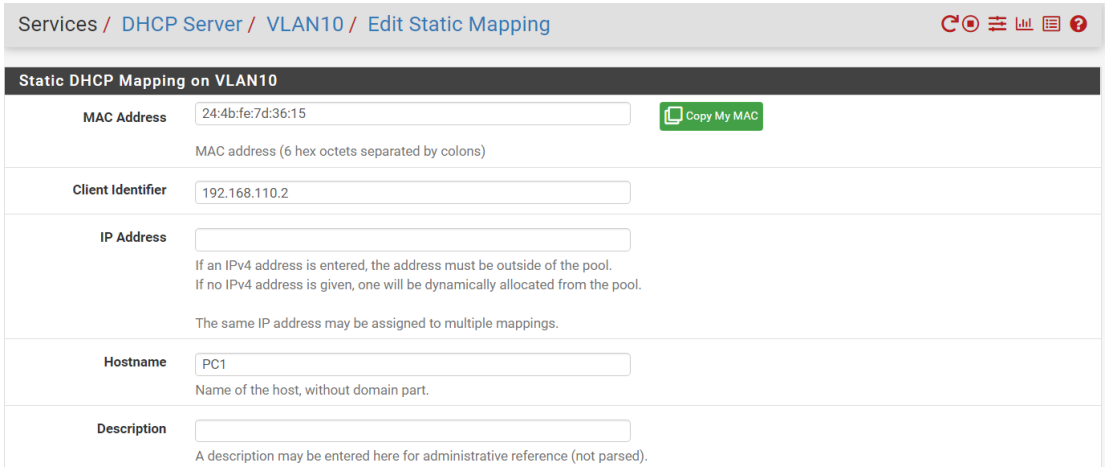


Figura 18: asignación de dirección IP de PC 1 perteneciente a Vlan 10 (fuente autor)

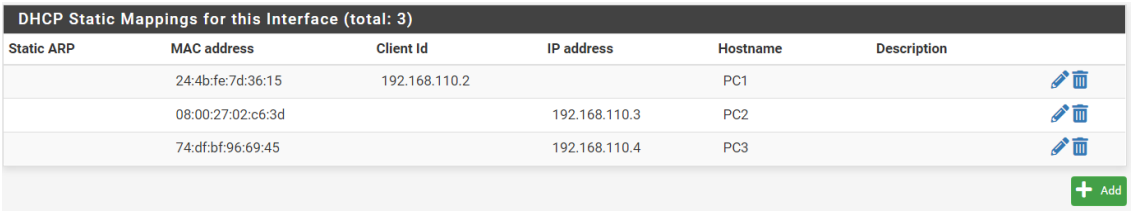


Figura 19: Direcciones IP establecidas para los equipos de la Vlan 10 (fuente autor)

La configuración debe repetirse para el resto de la VLANS creadas, tomando en cuenta las direcciones IP que ya se establecieron en las tablas de direccionamiento.

Habilitar servicio proxy

Luego de haber realizado la descarga del servicio Proxy Squid dentro del entorno de pfsense (Anexo 9) se procede con la activación y configuración.

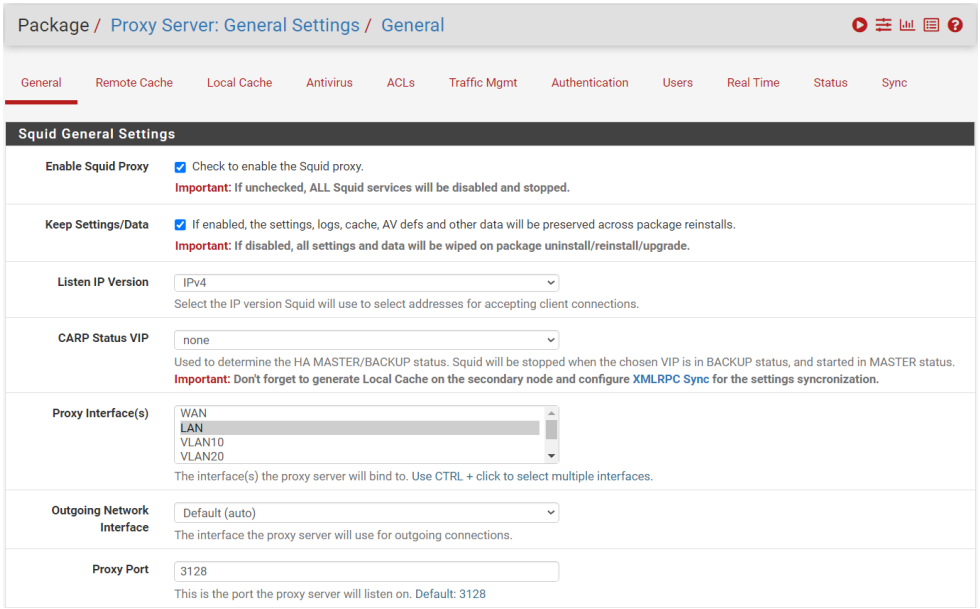


Figura 20: Habilitación de servicio proxy (fuente autor)

Configuración Squidguard

Se utilizó Squidguard como complemento del proxy Squid, esta herramienta permite la creación y agrupación de ACL definidas por categorías de contenido, lo que facilita el manejo de la seguridad de la red para el ingreso a sitios deseados o no.

Se empieza con la descarga del complemento, para esto es necesario ingresar a la opción de Available Packatges y buscar la herramienta SquidGuard.

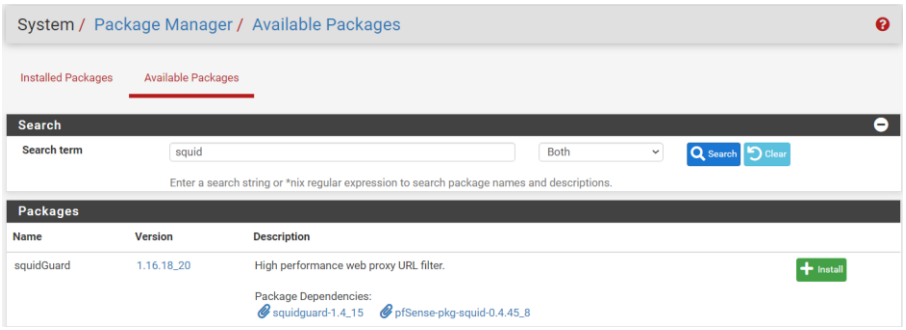


Figura 21: Descarga SquidGuard (fuente autor)

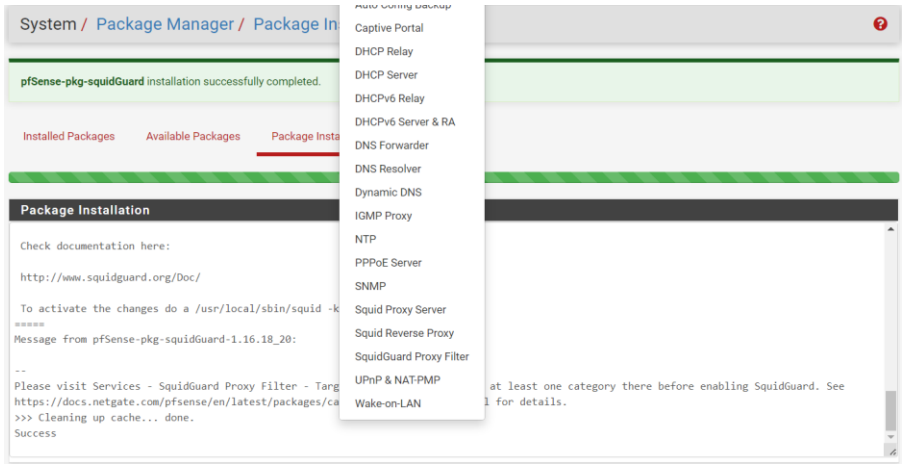


Figura 22: Instalación completada de SquidGuard (fuente autor)

Para empezar con la configuración hay que dirigirse al servicio de SquidGuard, dentro de este activamos la casilla “Enable” para levantar el servicio, además es necesario activar las casillas correspondientes al Logging options.

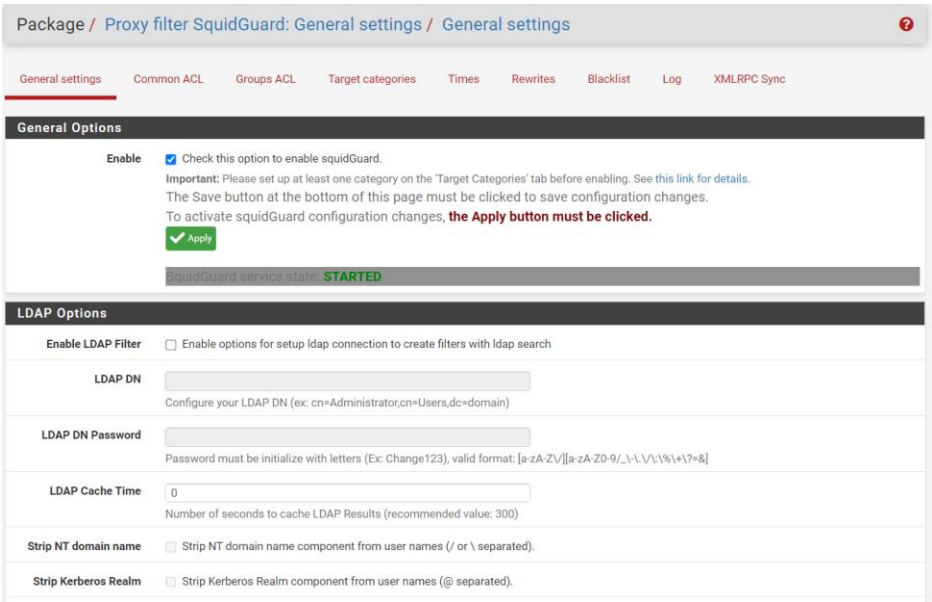


Figura 23: Activación de SquidGuard (fuente autor)

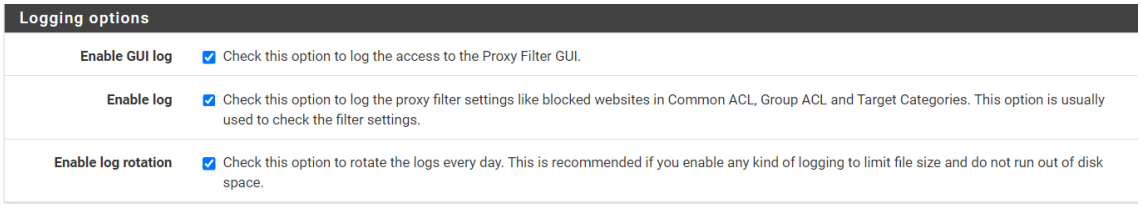


Figura 24: Activación de opcions logging (fuente autor)

Existen varias opciones de listas negras prediseñadas con las categorías de las páginas ya establecidas, se puede acceder a ellas ingresando el link del que se obtiene la lista en la opción Blacklist URL.

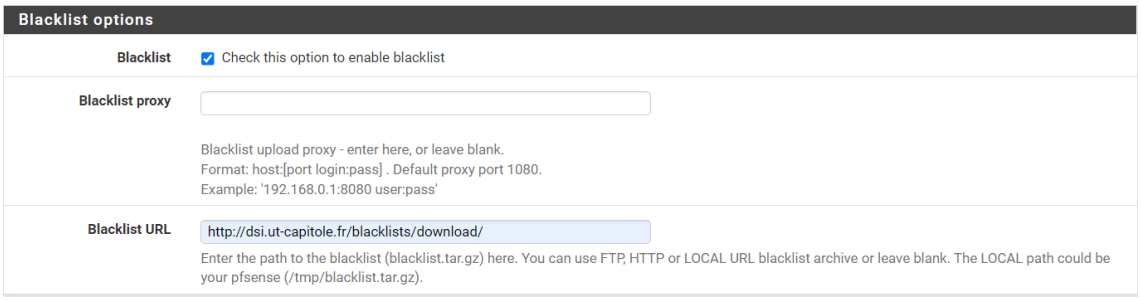


Figura 25: Ingreso de link de acceso a blacklist (fuente autor)

Para acceder a las categorías de la lista negra, hay que dirigirse al apartado Blacklist, dentro de este ingresamos el link de descarga del .gz

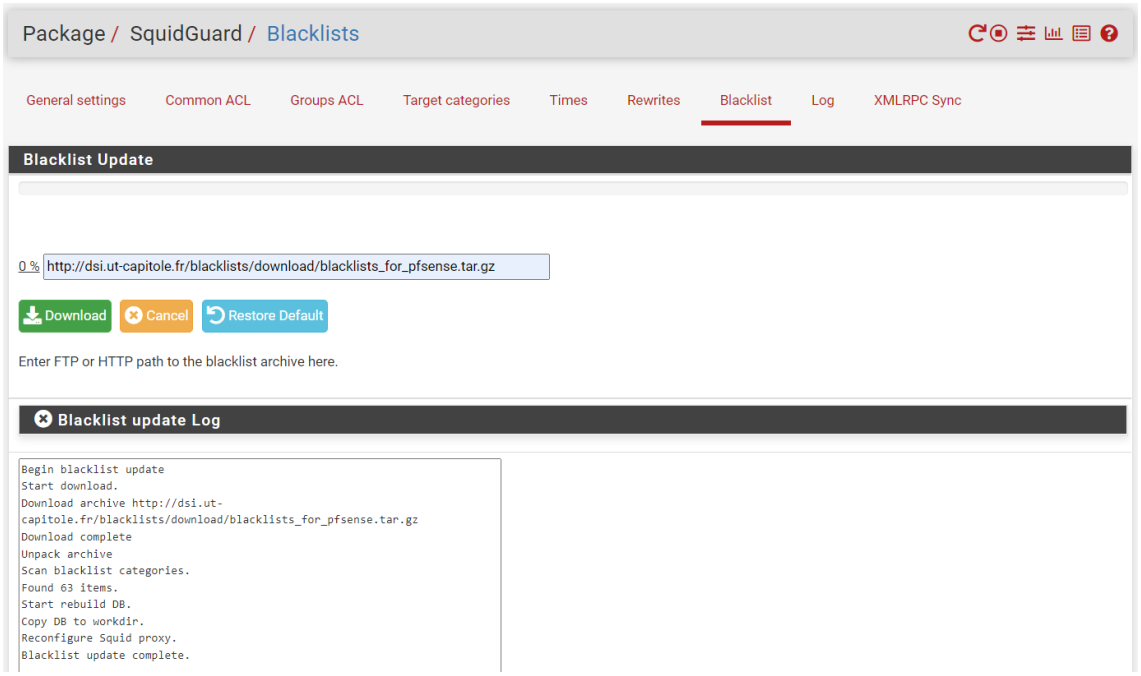


Figura 26: Descarga de ACL's (fuente autor)

Ahora deberá dirigirse al Common ACL donde se mostrará la lista que se descargo

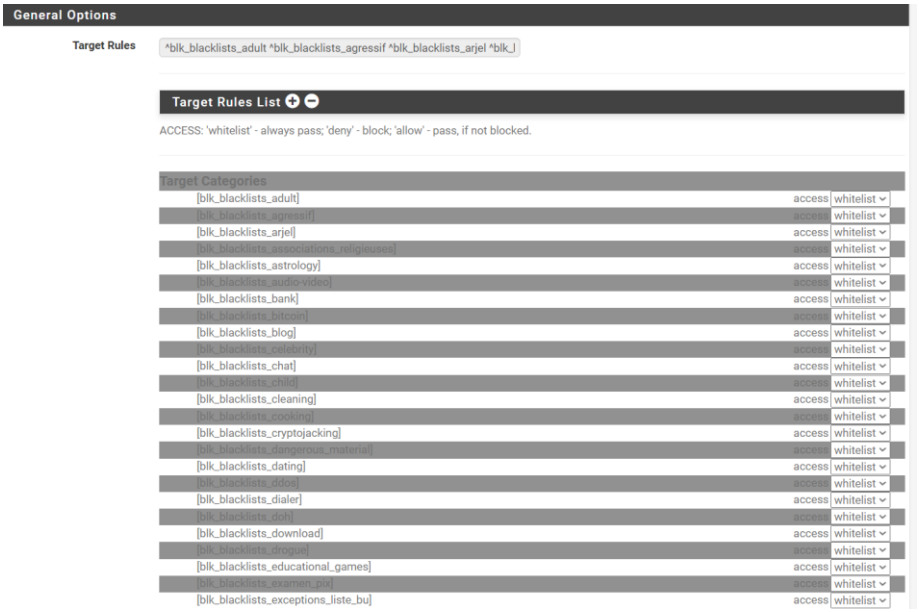


Figura 27: Categorías de ACL's (fuente autor)

Para especificar que categoría tiene acceso o no, se deberá cambiar las opciones de Whitelist o deny, para el laboratorio se bloquearan todas las categorías que estén apartadas del ámbito estudiantil, principalmente las categorías de videos, música, películas, sitios para adultos y redes sociales.

Luego de realizar las configuraciones se deberá ingresar a las configuraciones generales del SquidGuard y levantar el servicio, aparecerá un indicador en color verde o rojo que indicará el estado en activo o detenido según corresponda.

Una vez que el servicio este levantado se presenta la palabra STARTED en color verde.

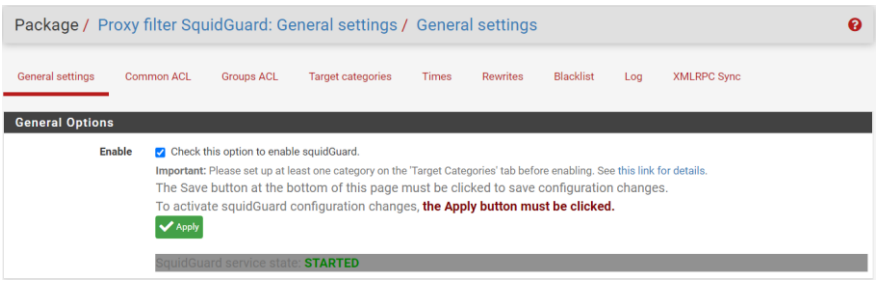


Figura 28: Estado de servicio Proxy (fuente autor)

Configuración individual de ACL´s

Existen dos tipos de configuración para las ACL, la primera se mostró en el proceso anterior, ahora se configurarán las listas de forma individual, para eso hay que ingresar al

apartado de ACL’s dentro de la configuración de Squid y llenar el cuadro de Balcklist con las url de los sitios que se quieren bloquear.

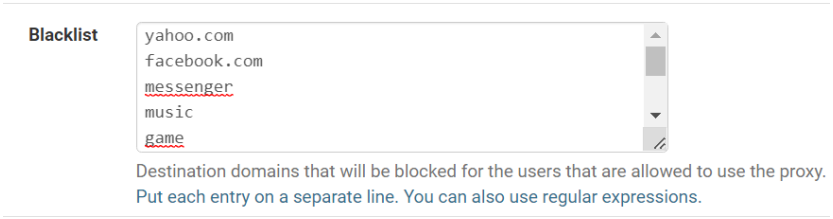


Figura 29: ACL sitios bloqueados (fuente autor)

Configuración acceso por IP

Para mantener un mejor control en la red, en el caso de los laboratorios se restringirá el acceso al servicio de internet, de modo que solo los dispositivos que pertenezcan a cada laboratorio tendrán acceso, esto se lo realiza configurando las reglas y alias que contengan las direcciones IP de los dispositivos permitidos, para esto primero se realiza la activación del Proxy en cada uno de los equipos (Anexo 10).

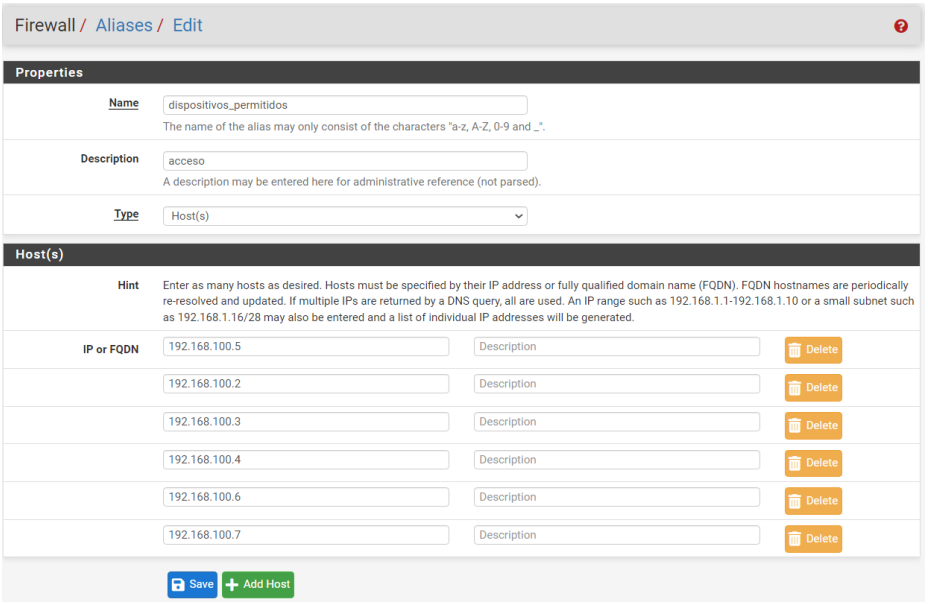


Figura 30: Configuración de nuevo alias (fuente autor)

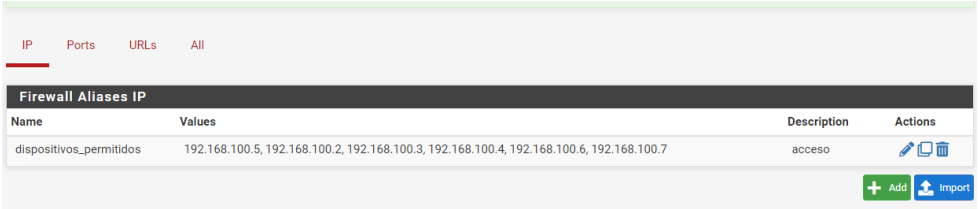


Figura 31: Tabla de alias existentes (fuente autor)

Luego de crear el alias con las respectivas IP de los equipos que tendrán acceso a internet, se procede a configurar las reglas de conexión, para esto se deshabilitaran las dos reglas que vienen por defecto que son las que permiten el acceso a internet.

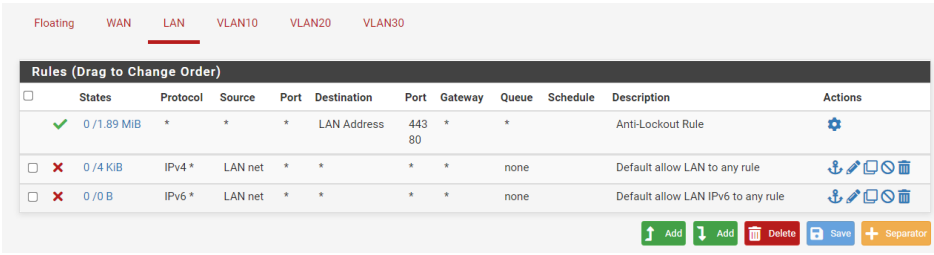


Figura 32: Deshabilitación de reglas por defecto (fuente autor)

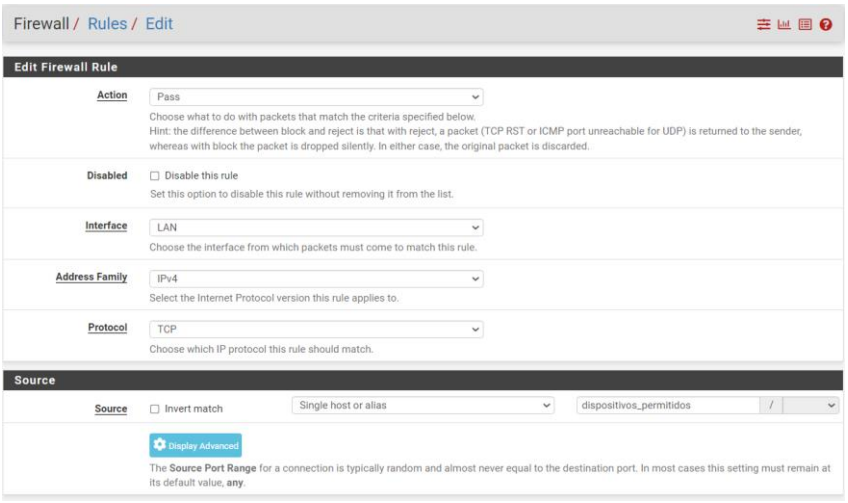


Figura 33: Creación de nueva regla (fuente autor)

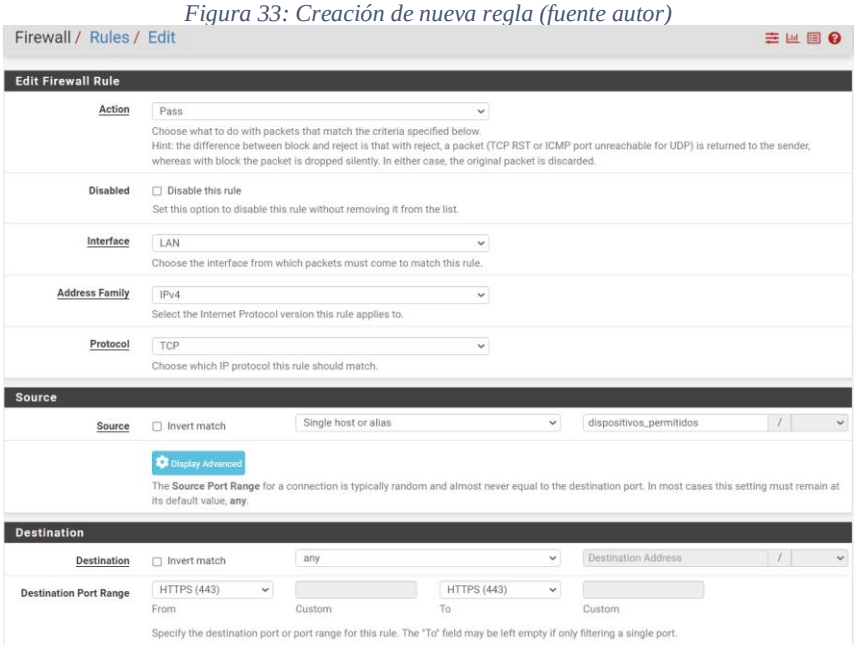


Figura 34: Configuración de regla con alias (fuente autor)

La misma regla fue copiada y se cambió el protocolo para tener acceso a ambos, http y https.

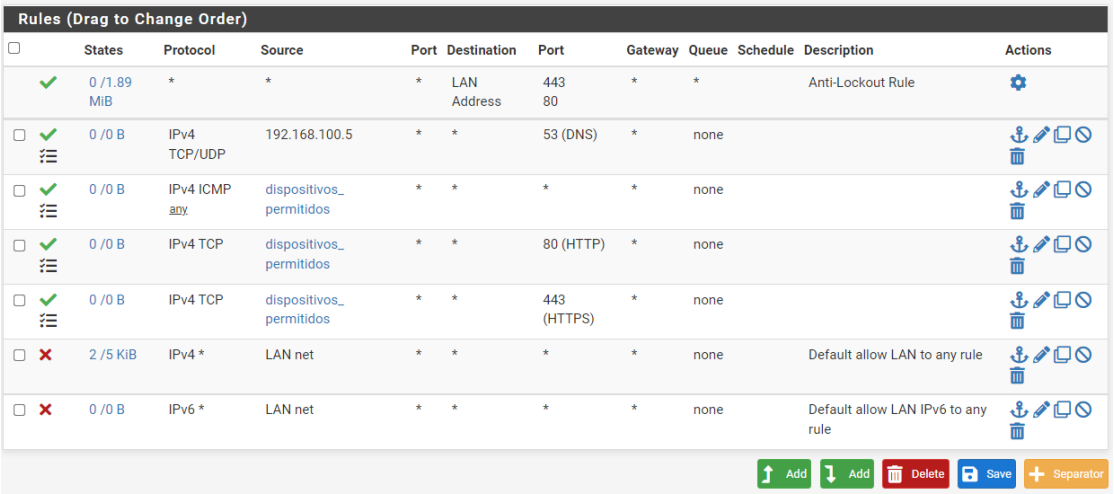


Figura 35: Listado final de reglas creadas (fuente autor)

Configuración de regla para bloqueo de acceso a panel de administración

Uno de los puntos que se debe de tener en cuenta al empezar la configuración, es que en un principio, todo dispositivo movil que se enceuntre ubicado dentro de la red tendra acceso a la administración del firewall, esto se lo evita creando una regla en la que designamos un solo equipo para el acceso al dashboard de Pfsense.

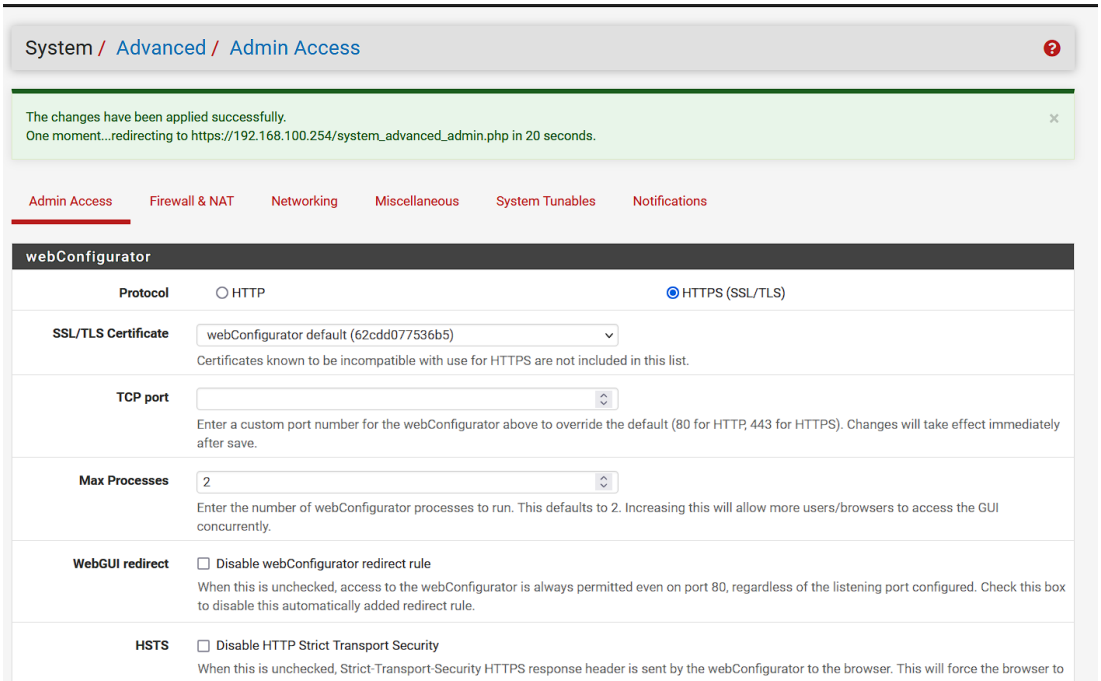


Figura 36: Regla de acceso administrador (fuente autor)

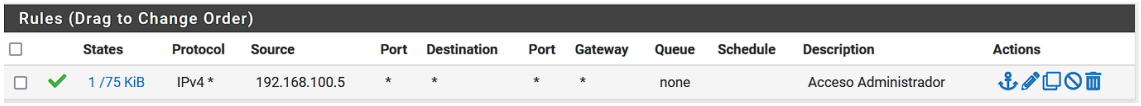


Figura 37: Regla activa (fuente autor)

Se creo una regla que permita acceder desde dos diferentes dispositivos al panel de administración del firewall, en este caso se trata del pc del administrador y de un dispositivo móvil.

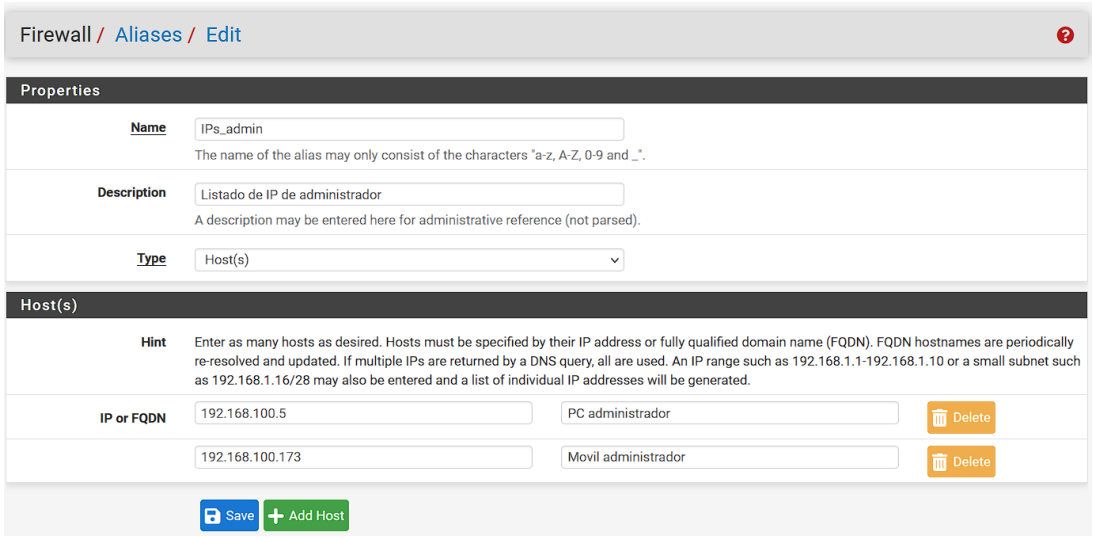


Figura 38: Creación de Alias de IPs_admin (fuente autor)

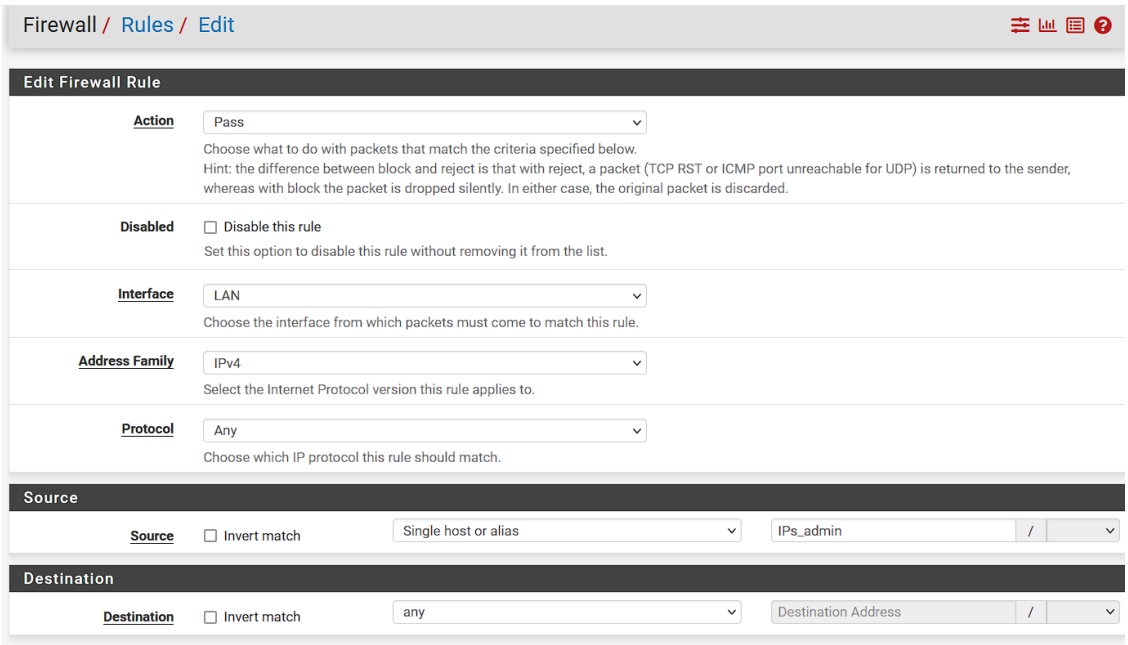


Figura 39: Regla Alias administrador (fuente autor)

Configuración de restricciones por grupos

La restricción por grupos permite asignar un rango de direcciones IP que tendrán ciertas restricciones al momento de navegar, esto es una opción para considerar para la administración de los equipos de los laboratorios de la Unidad Educativa, lo primero que se realiza en este caso es establecer el horario en el cual se generaran las restricciones, al tratarse de una unidad educativa que cuenta con dos horarios de claves, matutino y vespertino, se tomó en cuenta ambos horarios.

Primero se accede a la configuración de SquidGuard y seleccionar la opción Times, luego de seleccionar la opción para añadir el nuevo horario, se desplegará la ventana con los campos de configuración, al tratarse de un mismo horario para todos los días, solo se establecieron dos valores, uno para el horario matutino y otro para el vespertino, en caso de querer un horario diferente para cada día, se deberá seleccionar el día en el que se establecerá seguido de la configuración de la hora.

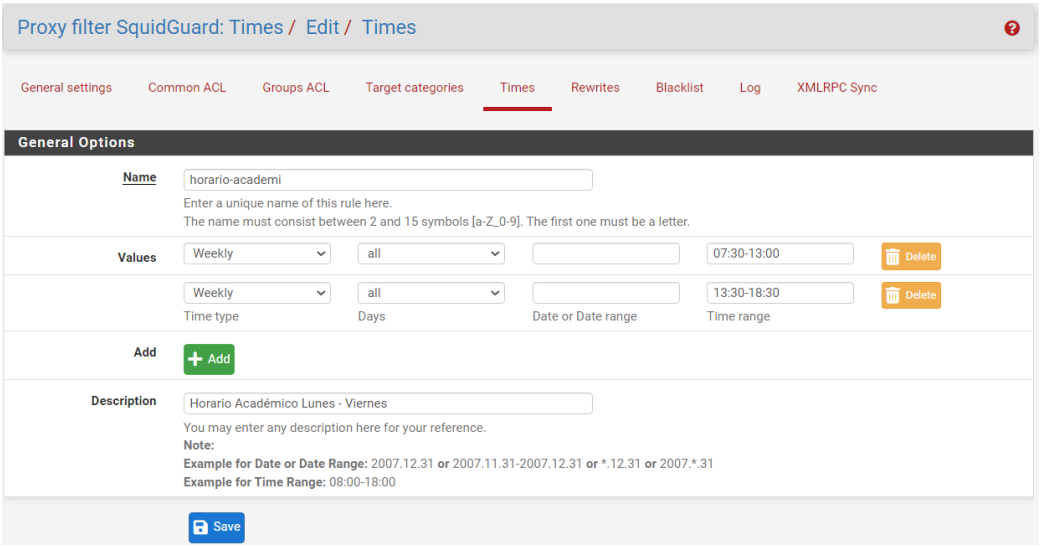


Figura 40: Creación de nuevo horario (fuente autor)

Creación de categorías

La creación de categorías permite agrupar contenidos que no se encuentren en las bases de listas negras que se pueden encontrar y están a disposición para su descarga, se debe de tener en cuenta que dichas bases de datos suelen tener contenido de páginas de otros países, de modo que crear una nueva categoría con nuevas listas permite que la base crezca, para la creación de categorías se tiene tres formas de ingresar los sitios que se

desean bloquear, por dominio, dirección URL o por caracteres, en este caso se ve más conveniente la primera y tercera opción.

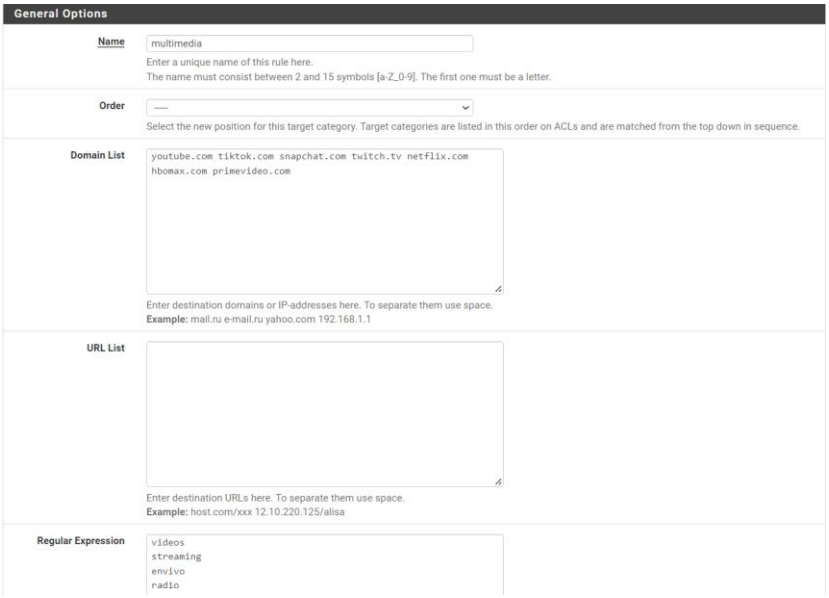


Figura 41: Configuración de categoría Multimedia (fuente autor)

Configuración de grupos

Luego de haber realizado la configuración de horarios y la creación de grupos, se puede utilizar ambos aspectos para completar la configuración de restricciones, para eso se deberá dirigir a Groups ACL y crear un nuevo grupo, dentro de esta configuración se asigna el nombre del grupo y las direcciones IP que estarán dentro.

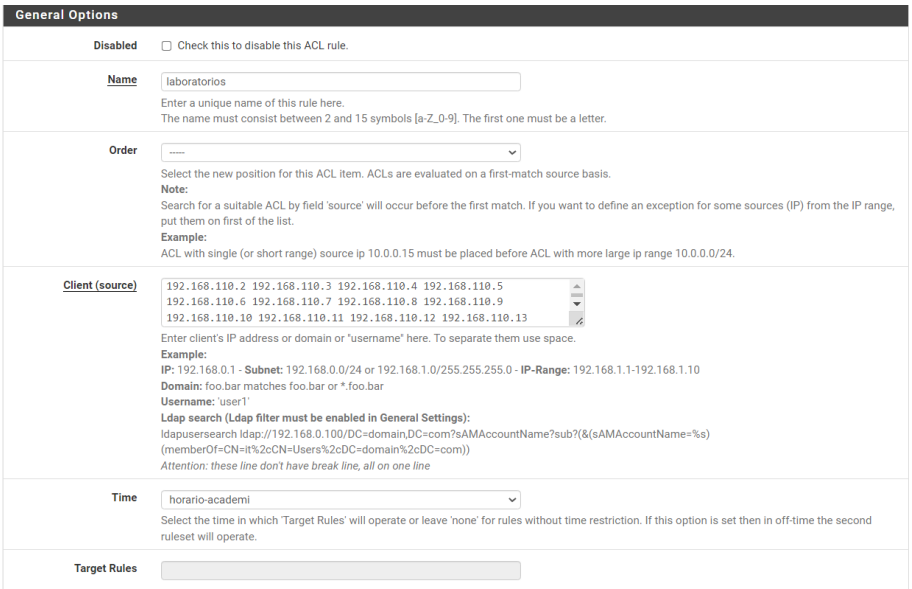


Figura 42: Configuración de grupo de IP laboratorios (fuente autor)

Se añade el horario que se estableció en las configuraciones anteriores junto con la lista "Multimedia", además de las demás categorías que ya se encuentran en la base de datos.

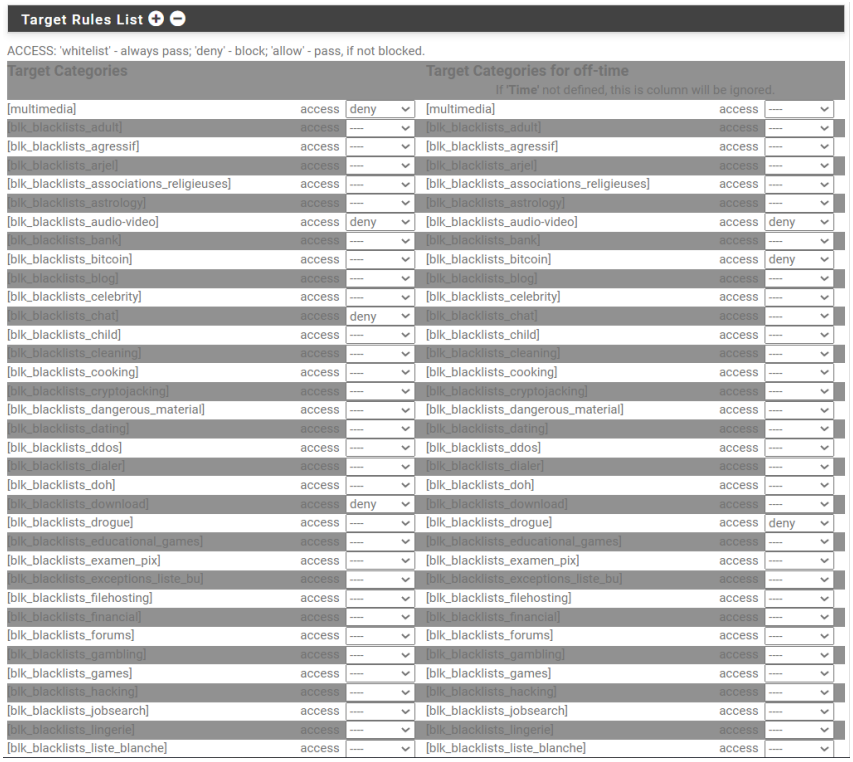


Figura 43: Listado de categorías (fuente autor)

Configuración de herramienta de reportes

Luego de haber configurado el servicio proxy y las listas de control de acceso, se pasa a la configuración de la herramienta que ayudara a generar el reporte de los dispositivos que se conecten a la red, para eso se utilizó el complemento Ligthsquid, al igual que con squidGuard primero es necesario descargar el paquete.

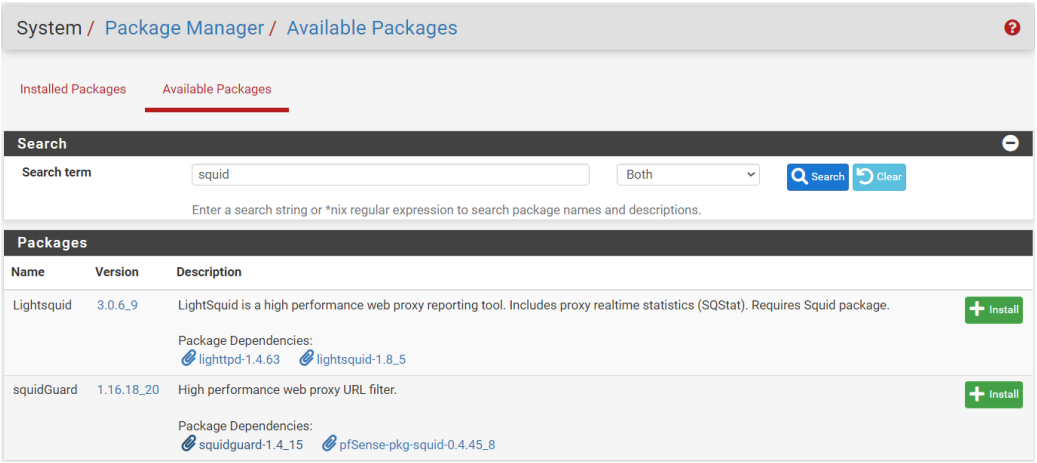


Figura 44: Descarga de paquete Ligthsquid (fuente autor)

Una vez terminada la instalación, la herramienta aparecerá en el apartado de status

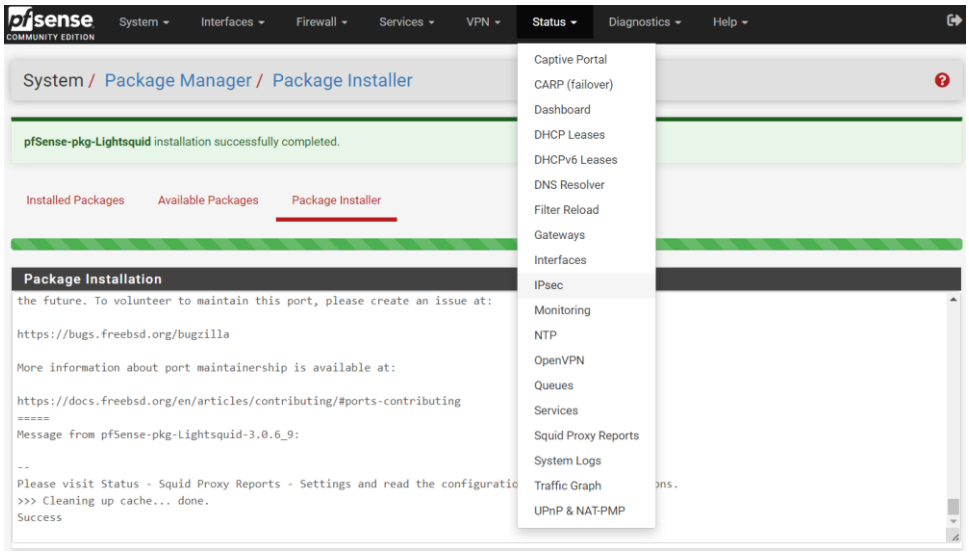


Figura 45: Instalación concluida de Ligthsquid (fuente autor)

Seguido a eso, se configuran los parámetros básicos para el reporte, cambiar la contraseña de usuario que se asigna por defecto y el tiempo de refresco del reporte.

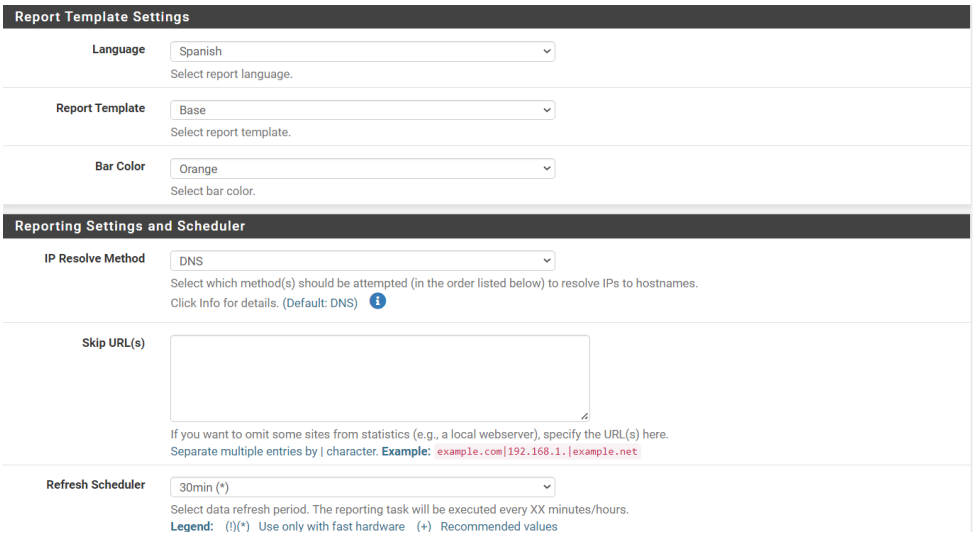


Figura 46: Configuración Ligthsquid (fuente autor)

3.1.4. Fase 4: Diseño Físico

Durante la fase de diseño físico, se proponen las tecnologías y productos (marcas y referencias de equipos) que concuerden con el registro de diseño lógico [64]. Para el desarrollo de esta fase se recomienda realizar comparaciones entre los diferentes equipos que se pueden utilizar para llevar a cabo la implementación. Para realizar una correcta selección de los equipos, se realizó un análisis de todas las características técnicas que

brinda cada uno de ellos, para el análisis, se creó una tabla con las 3 principales marcas del mercado.

Routers

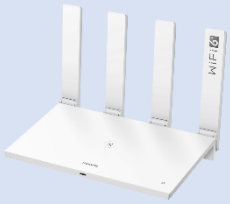
Equipo	Huawei	Asus	Tp-link
Imagen			
Modelo	Huawei AX3	RT-AX86U	TP-Link Archer C60
Cantidad de puertos	4	10	4
Velocidad	3000 Mbps	867Mbps	450Mbps
Señal	2.4GHz – 5GHz	2.4GHz – 5GHz	2.4GHz – 5GHz
Interfaz	10/100/1000Mbps	10/100/1000Mbps	10/100 Mbps
Seguridad	WPA3-Personal, WPA2-Personal	WPA3-Personal, WPA2-Personal, WPA-Personal, WPA-Enterprise, WPA2-Enterprise, WPS	WEP WPA WPA2 WPA/WPA2-Enterprise (802.1x)
IPv4	si	si	Si
IPv6	si	si	Si
Protocolos	IEEE802.11a, IEEE802.11n, IEEE802.11ac, IEEE802.11g, IEEE802.3, IEEE802.3U	802.11b, 802.11a, 802.11n, 802.11ac, 802.11ax	802.11ac, 802.11n
Valor 2022	90$	270$	70$

Tabla 11: características de equipos "Routers"

Switches

Equipo	Cisco	HP	Tp-link
Imagen			
Modelo	Catalyst Ws-c3560cg 24 Adm L3	Aruba 2930F PoE 24 Puertos Gigabit	Switch T3700G-28TQ
Cantidad de puertos	24	24	24
Velocidad	16Gbps	56 Gbps	48 gbps
Interfaces	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
IPv4	Si	Si	si
IPv6	Si	Si	no
Vlan	Si	Si	si
Enrutamiento	Rip-1, Rip2, OSPF, EIGRP	Rip-1, Rip2, OSPF	enrutamiento estático RIP v1, v2 OSPF v2 ECMP PIM-SM / PIM-DM / IGMP DHCP
Protocolos	IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.1q/p	IEEE802.3, IEEE802.3ab, IEEE802.3at, IEEE802.3u	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ae, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p
Valor 2022	748$	2300$	2200$

Tabla 12: Características de equipos "Switch"

Access point

Equipo	Cisco	Huawei	Tp-link
Imagen			
Modelo	Cisco Business 240AC	AP4050DN-S	TP-LINK EAP225
Frecuencia	2.4 GHz – 5 GHz	2.4 GHz – 5 GHz	2.4 GHz – 5 GHz
Capacidad de Transmisión	1733 Mbps	1267 Mbps	300 Mbps
RAM	255 MB	256 MB	256 MB
Interfaz	Rj45 – USB 2.0	Rj45	Rj45
Estándar	802.11ac	802.11ac	802.11a, 802.11b
Seguridad	WPA2 WPA3	WEP, WPA/WPA2–PSK, WPA/WPA2–PPSK, WPA/WPA2	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b
Número de usuarios	200	500	60
Área de cobertura	350m	300m	200m
Valor 2022	150$	350$	100$

Tabla 13: Características de equipos "Access Point"

En base a las características técnicas de cada uno de los equipos, se evalúa la mejor opción realizando una comparación tomando en cuenta las características, disponibilidad y costos, luego de realizar la correspondiente evaluación, se crea un indicador con un rango de 1 a 5 que servirá como forma de puntuación para los equipos siendo 5 el porcentaje más alto.

Calificación	Porcentaje
1	20%
2	40%
3	60%
4	80%
5	100%

Tabla 14: Indicador de evaluación

3.1.4.1. Comparación de equipos “Router”

Equipo	Huawei	Asus	Tp-link
Modelo	Huawei AX3	RT-AX86U	TP-Link Archer C60
Disponibilidad	5	4	5
Costo	5	4	5
Soporte	5	5	4
Especificaciones	4	5	3
Total	4.75%	4.50%	4.25%

Tabla 15: Calificación Equipos “Router”

En base a las comparaciones realizadas y de acuerdo con los indicadores de evaluación, para el caso del router, la marca que brinda mejores características y prestaciones es Huawei, contando con una disponibilidad inmediata en el país y con un soporte confiable desde la misma página oficial de Huawei.

3.1.4.2. Comparación de equipos “Switch”

Equipo	Cisco	HP	Tp-link
Modelo	Catalyst Ws-c3560cg 24Adm L3	Aruba 2930F PoE 24 Puertos Gigabit	Switch T3700G-28TQ
Disponibilidad	4	4	4
Costo	5	4	4
Soporte	3	5	5
Especificaciones	3	4	5
Total	3.75%	4.25%	4.5%

Tabla 16: Calificación Equipos “Switch”

Para el caso de los switches la marca Tp-link es la que presenta mejores características, el único punto negativo que se puede encontrar es que el stock dentro del país es limitado, pero cuenta con un gran stock en tiendas internacionales y se mantiene con un soporte inmediato desde las páginas y los canales de contactos oficiales de la marca.

3.1.4.3. Comparación de Access point

Equipo	Cisco	Huawei	Tp-link
Modelo	Cisco Business 240AC	AP4050DN-S	TP-LINK EAP225
Disponibilidad	5	4	3
Costo	5	4	4
Soporte	4	4	4
Especificaciones	5	4	5
Total	4.75%	4%	4%

Tabla 17: Calificación de equipos "Access Point"

Dentro de las opciones que se encontró en el mercado, entre las 3 principales marcas de Access point la que mejores características presenta en cuanto a soporte, estándares y cobertura fue el modelo perteneciente a la marca cisco, teniendo una disponibilidad inmediata dentro del país y un precio accesible.

3.1.5. Fase 5: Pruebas

Las pruebas que se detallan a continuación se realizaron en un laboratorio propio en una red doméstica.

Pruebas de acceso administrador Pc

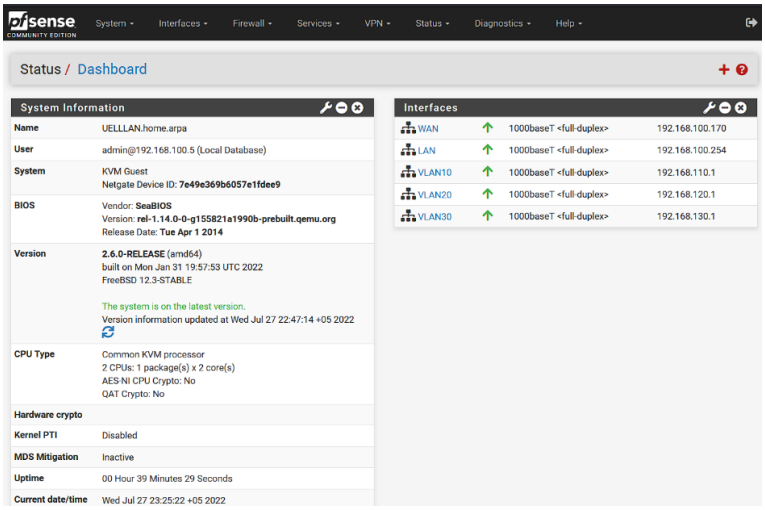


Figura 47: Acceso desde pc administrador (fuente autor)

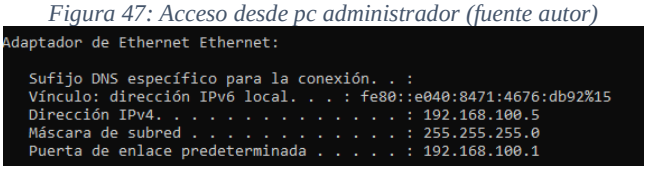


Figura 48: IP seleccionada para acceso (fuente autor)

Acceso Móvil con IP permitida dentro del rango de la regla configurada

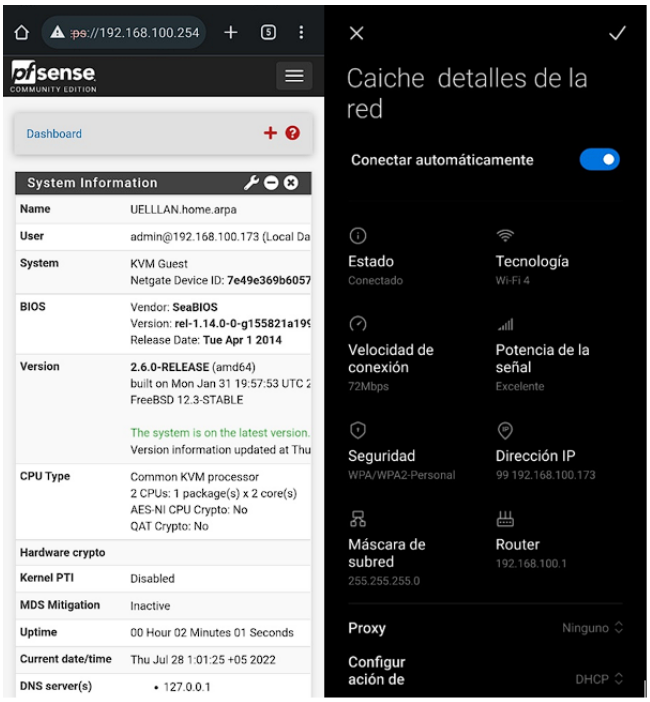


Figura 49: Acceso desde dispositivo móvil con IP permitida (fuente autor)

Pruebas de denegación de conexión a panel de administración a dispositivos no permitidos

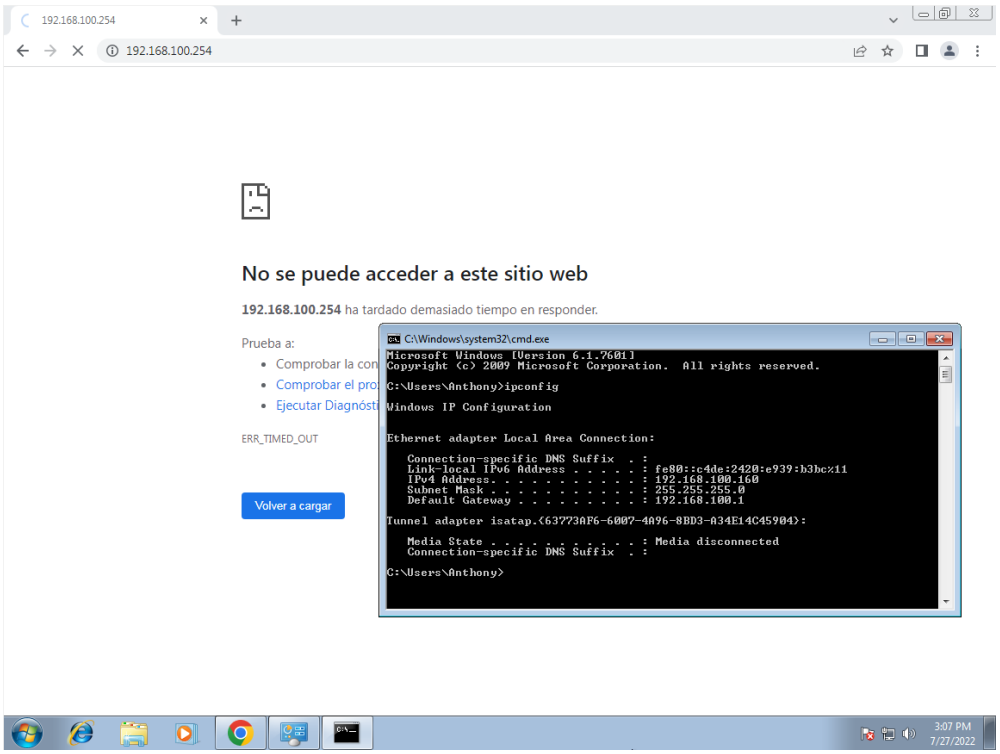


Figura 50: Acceso denegado a panel de administración a dispositivo no permitido (fuente autor)

Pruebas de navegación de dispositivos permitidos con direcciones IP asignadas en las reglas del Firewall

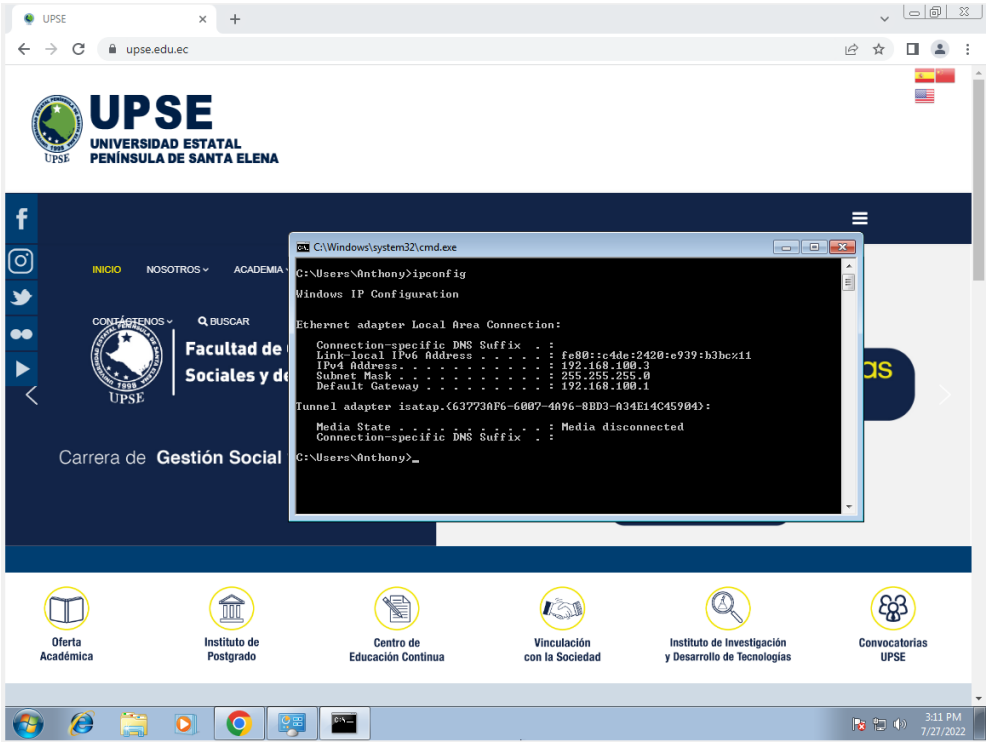


Figura 51: Prueba de navegación de dispositivo permitido 1 (fuente autor)

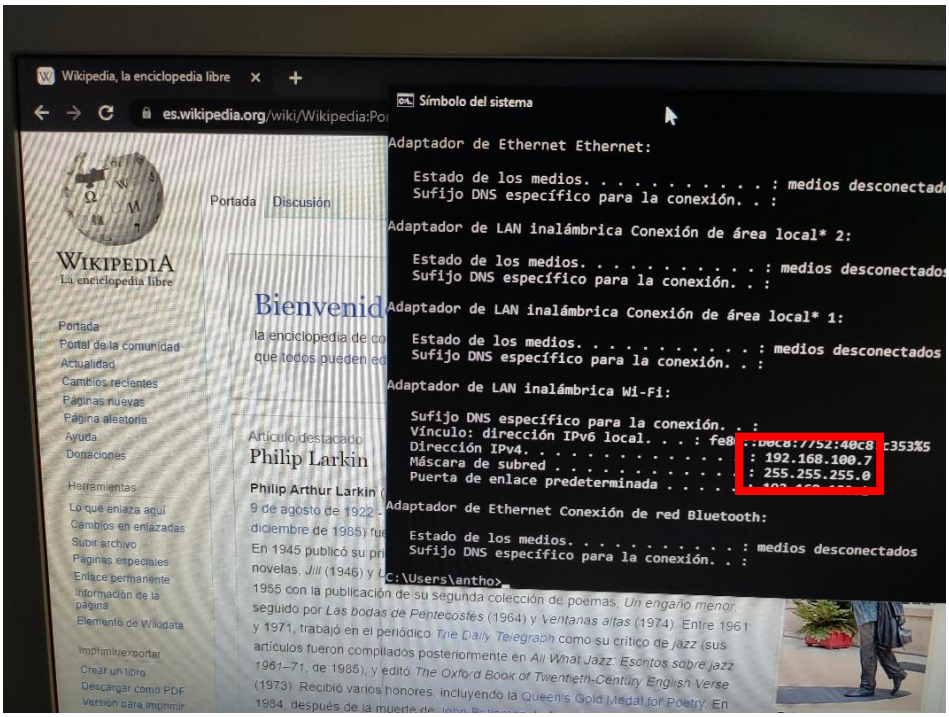


Figura 52: Prueba de navegación de dispositivo permitido 2 (fuente autor)

Pruebas de navegación de dispositivos no permitidos con IP distintos al rango establecido en las reglas del firewall.

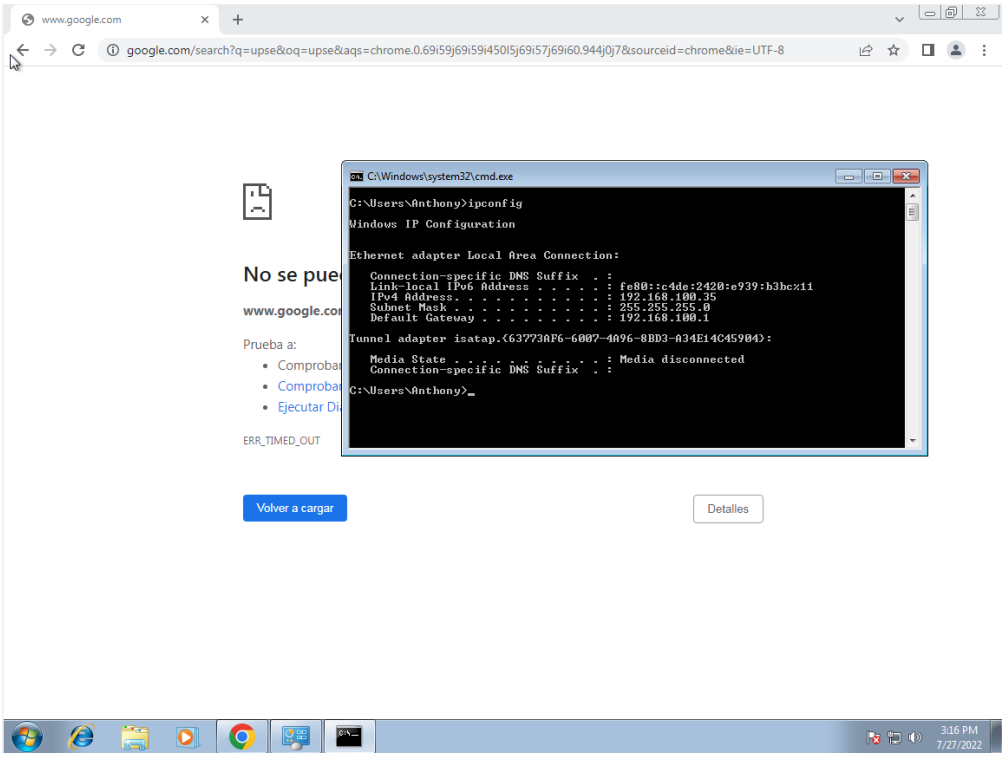


Figura 53: Prueba de navegación de dispositivo no permitido 1 (fuente autor)

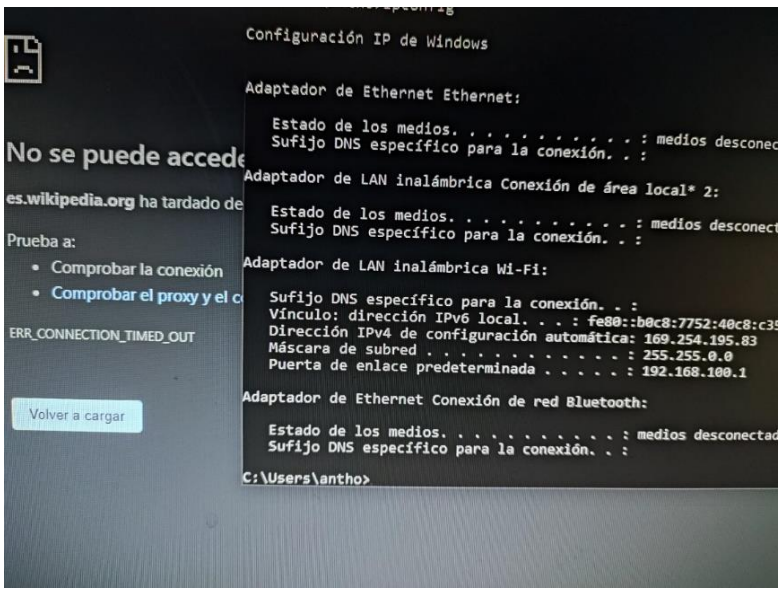


Figura 54: Prueba de navegación de dispositivo no permitido 2 (fuente autor)

Pruebas de bloqueo de sitios por servicio Proxy

Figura 55: Bloqueo de sitio "Facebook.com" dispositivo 1 (fuente autor)

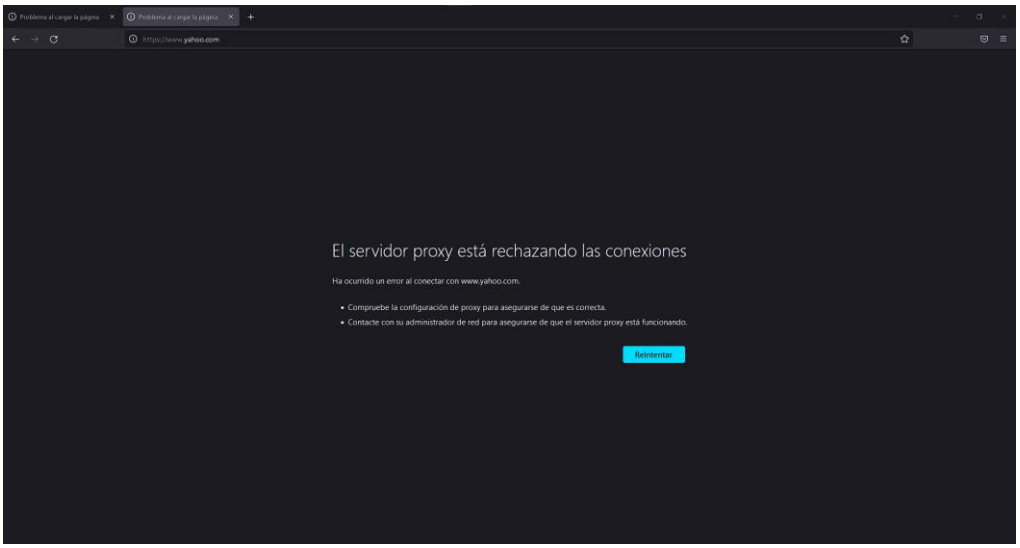


Figura 56: Bloqueo de sitio yahoo.com dispositivo 1 (fuente autor)

Figura 57: Bloqueo de sitio dispositivo 2 (fuente autor)

Figura 58: Bloqueo de sitio dispositivo 2 (fuente autor)

Pruebas de restricción por horarios

Las pruebas de restricción por horario se establecieron en base al horario académico que se configuro dentro del servicio Proxy el cual activa las configuraciones dentro del horario de 13:30 a 18:30.

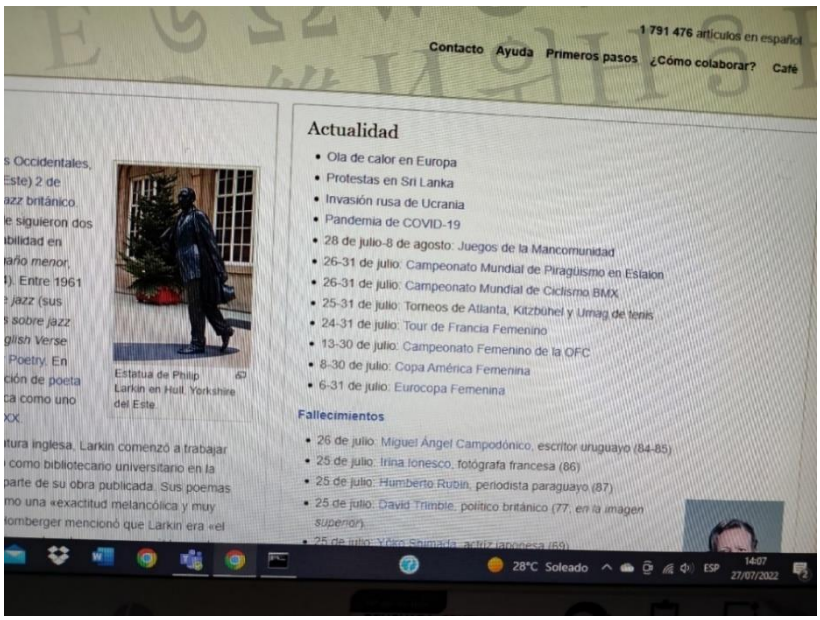


Figura 59: Prueba de conexión a página permitida dentro del horario (fuente autor)

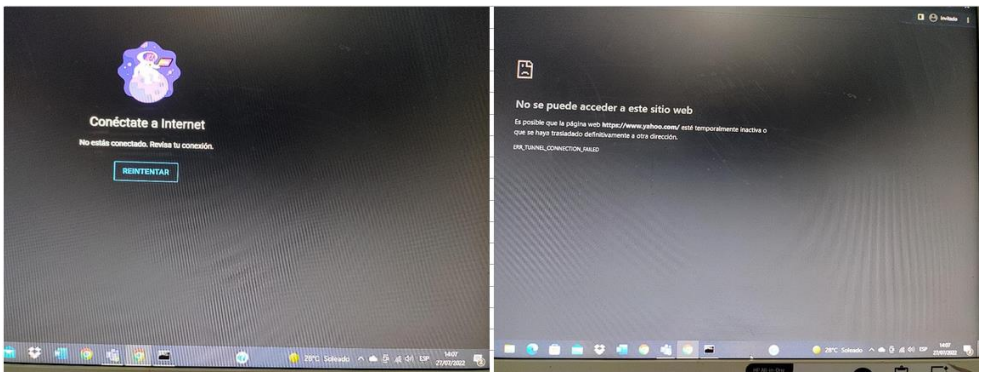


Figura 60: Prueba de conexión a páginas no permitidas dentro del horario (fuente autor)

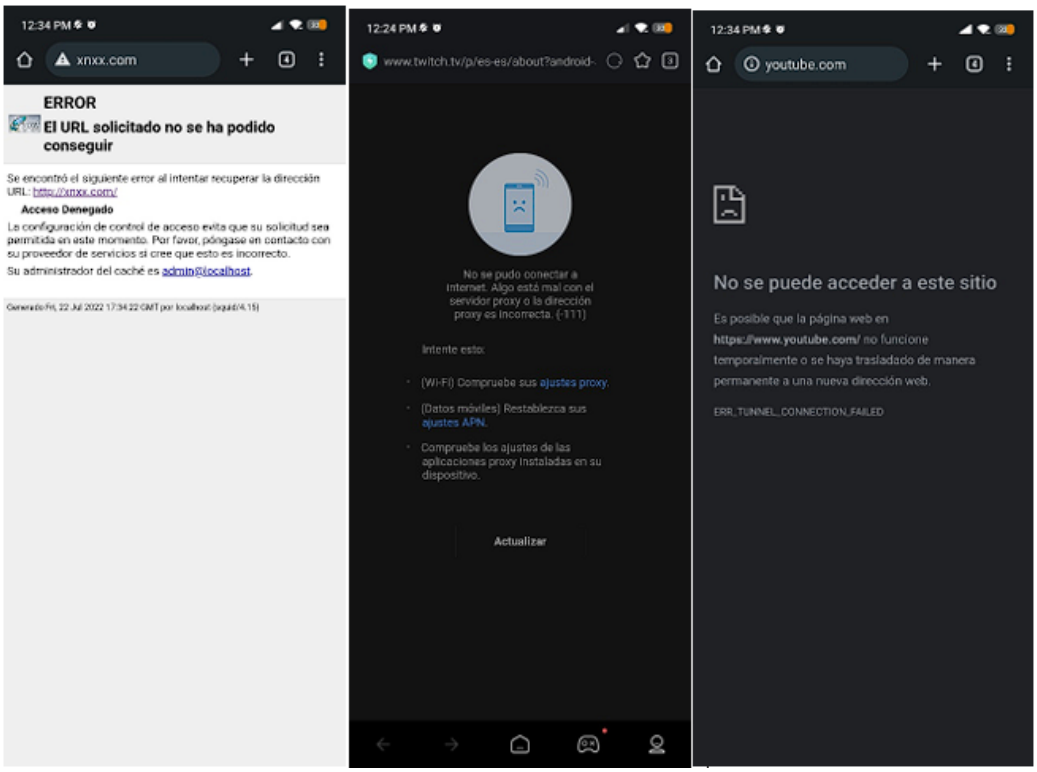


Figura 61: Prueba de conexión a paginas no permitidas en dispositivos móviles (fuente autor)

Reporte de tráfico generado

Para la primera prueba se estableció que se actualicen los logs cada 10 minutos, pasados los primero 10 minutos se podrá revisar el reporte de cada uno de los dispositivos que tuvieron conexión a la red, para acceder al menú de repostes se selecciona “Open lightsquid” dentro de la configuración de Squid Proxy Reports.

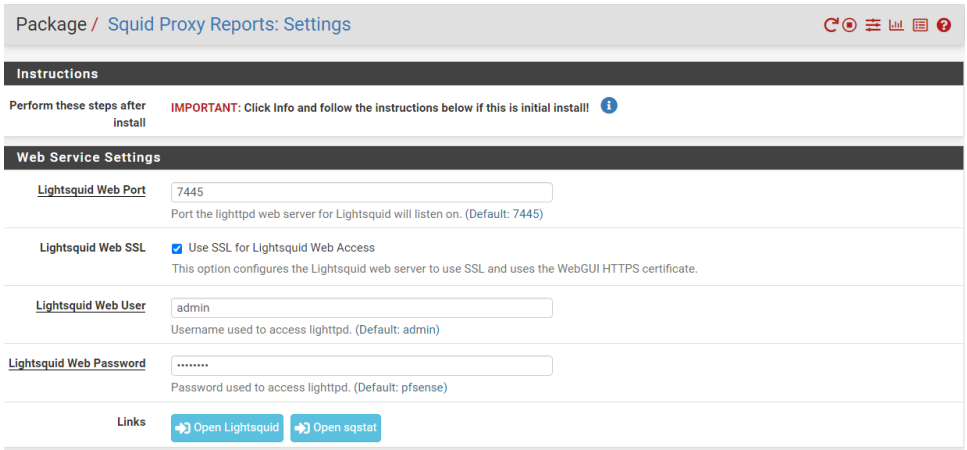


Figura 62: Usuario y contraseña para apartado de reportes de Squid (fuente autor)

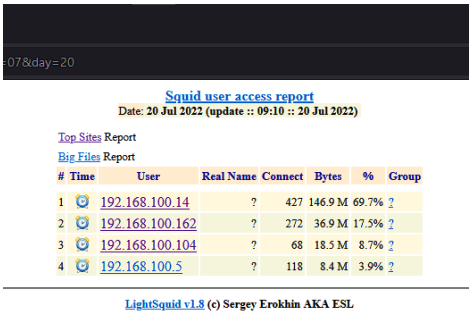


Figura 63: Direcciones IP de equipos conectados a la red con el servicio proxy activo (fuente autor)

Dentro del menú se observan las direcciones IP de los equipos que se encuentran conectados a la red y tienen configurado el servicio proxy, para ver el tráfico se selecciona el equipo en específico.

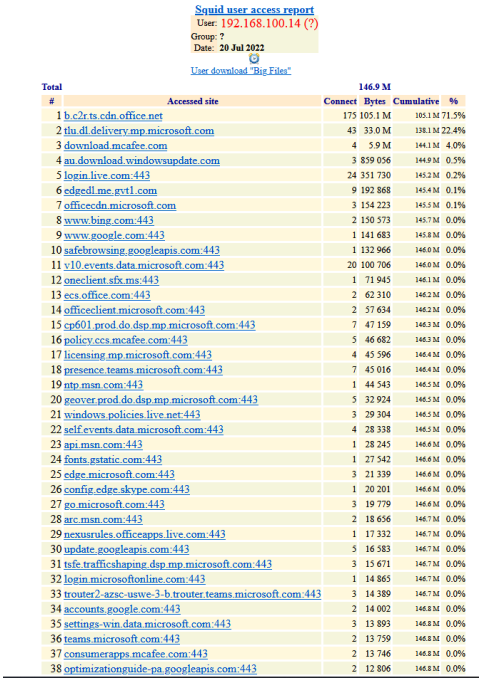


Figura 64: Paginas y dominios a los que se accede desde un dispositivo en específico (fuente autor)

3.1.6. Estudio de factibilidad

Por medio del estudio de factibilidad se busca manejar de la mejor forma la toma de decisiones al momento de llevar a cabo el desarrollo de la propuesta esto mediante la toma de información y la recolección de datos relevantes teniendo en cuenta que la propuesta actual servirá para una futura implementación.

Se deberán tomar en cuenta varios factores que podrían determinar o no el éxito del proyecto, el objetivo de este análisis es evaluar esos puntos dividiéndolos en tres estudios principales que abarcaran las necesidades, metas y lo que se espera al terminar la propuesta, estos estudios corresponden a los tres pilares fundamentales de la factibilidad, los cuales son:

- Factibilidad Operativa
- Factibilidad Técnica
- Factibilidad Económica

3.1.6.1. Factibilidad Operativa

En la primera fase del estudio de factibilidad se analizará la situación actual de la Unidad Educativa y a su vez se tomarán en cuenta las mejoras y ventajas que se lograrían con la implementación de la propuesta, además se tomara en cuenta las personas a las que se beneficiara con la propuesta.

Situación Actual:

Actualmente dentro de la Unidad Educativa La Libertad se llevan a cabo con normalidad las actividades académicas, pero dentro de las oficinas y laboratorios de cómputo existen un gran inconveniente con el acceso y la navegación en internet, algunos de los problemas que se lograron evidenciar son:

- Perdida de conexión
- Mala administración de dispositivos
- Mala ubicación de equipos
- Equipos de red administrables inexistentes
- Falta de seguridad para ingreso y navegación
- Acceso físico sin control a áreas restringidas

Figura 65: Ubicación de equipos de red

Se mencionan las principales falencias que se lograron encontrar, mencionando tanto el medio físico y lógico de la red, estos puntos mencionados hacen que las actividades que tengan que ver con la red institucional se dificulten.

Implementación

Para la implementación además de tomar en cuenta los puntos que se mencionaron en el análisis de la situación actual, también se debe analizar las necesidades de los usuarios que serán beneficiados con la implementación, teniendo en cuenta que la red en la que se pretende trabajar es una red institucional perteneciente a una Unidad Educativa, los principales beneficiarios serán tanto docentes como estudiantes, además de todo el personal que labore dentro de las instalaciones.

Dentro de la unidad existe personal designado para el área de TI para ellos se detallarán algunos puntos importantes que deberá tener en cuenta en caso de que se desarrolle una implementación futura.

- Se deberán instalar todas las herramientas que se mencionan en el estudio, siguiendo los pasos que se detallan.
- Se recomienda ampliar los conocimientos en manejo de redes.
- Los componentes que se tomaron en cuanta para el desarrollo de la red deberán ser estudiados nuevamente dependiendo el tiempo que se tarde en llevar a cabo la implementación, por factores de soporte y actualizaciones.

- Estudiar los conceptos de direccionamientos, ip, máscaras de red.
- Para el cableado se debe tomar en cuenta el tipo de cableado que se está implementando por canaleta, para evitar posible interferencia entre cableado de red y eléctrico.
- En caso de presentar dificultades para la instalación e implementación de las herramientas, se recomienda solicitar apoyo de personal más capacitado o en su defecto, del desarrollador de la propuesta.

Seguridad

La seguridad es uno de los principales puntos a tener en cuenta, luego de haberse realizado el debido rediseño de la infraestructura, es necesario mantener una seguridad que permita que el servicio funciones de la mejor forma. Los factores que se deberán tener en cuenta para esto son:

- El personal deberá actualizar sus conocimientos en cuento a métodos y técnicas de seguridad.
- Se deberá respetar el manual de políticas de seguridad de la Unidad Educativa La Libertad.
- Los docentes estarán encargados de transmitir los puntos del manual de políticas de seguridad a los estudiantes.
- En cuanto a los métodos de seguridad que se implementarán en la red, deberán mantener siempre un control para evitar posibles intentos de vulneraciones.
- El servicio proxy deberá mantenerse siempre que se encuentren en horario académico, esto permitirá limitar el tráfico que se produce en la red, mejorando así la conexión para las actividades primordiales.
- Revisar de forma periódica los informes entregados por la herramienta Squid para registrar posibles paginas filtradas que deberían ser bloqueadas, de esta forma se ira alimentando la base de las listas negras del servicio proxy.

Luego de haberse dado las debidas indicaciones y recomendaciones para la implementación, se mencionan algunas de las ventajas y mejoras que aporta la propuesta a la Unidad Educativa.

- Mejora de conectividad.
- Aumento de seguridad dentro de la red.

- Actualización de equipos.
- Reducir tiempos de espera al momento de navegar por internet.
- Aumentar la seguridad física, evitando así posibles factores que puedan dañar la integridad de los equipos de red.

3.1.6.2. Factibilidad Técnica

Mediante este estudio se analizan las tecnologías que podría utilizarse para llevar a cabo una implementación. Se deberán tener en cuenta todos los recursos que se necesitarán, desde equipos de comunicación, cableado y localización

Localización

La localización es un factor clave que determinara el éxito o no del proyecto, es necesario conocer el área sobre la cual se trabajará, para tener en cuenta las características de los equipos en cuanto a cobertura, de igual forma para conocer la cantidad de cableado que podría llegar a utilizarse, este último siendo un aproximado.

Dentro de la Unidad Educativa se trabajará sobre los dos edificios principales en los que se aloja casi en su totalidad la red cableada, el área total de la Unidad Educativa es de 18431m2.

Figura 66: Área total de la Unidad Educativa La Libertad (fuente: Google maps)

Dentro de esta área total se trabajará solo dentro de los edificios principales el edificio administrativo cuenta de dos plantas con un área de 172m2 y el pabellón de laboratorios que cuenta con un área de cerca de 145m2.

Figura 67: Edificio administrativo

Figura 68: Pabellón de laboratorios

Figura 69: Laboratorio 1 de computo

Figura 70: Laboratorio 2 de computo

Equipos de comunicación

Para llevar a cabo la implementación del proyecto es necesario determinar que tecnologías, herramientas y equipos se utilizaran, para esto durante este estudio se analizaran todos los posibles elementos que se utilizarían para el desarrollo, teniendo en cuenta que las características que brinden deben ser funcionales para abarcar todas las necesidades o requerimientos que se plantearon en la fase de desarrollo "Análisis de requerimientos".

Para revisar las características de cada uno de los equipos, al igual que las comparaciones se puede observar la (tabla 11 y tabla 12) dentro de la fase de diseño físico de la metodología de desarrollo del proyecto.

Requerimientos de recursos

Dentro de este punto es importante definir tanto herramientas de hardware como software que serán necesarias para llevar a cabo él trabajó, en el punto anterior y en la fase de diseño físico de la red ya se establecieron los elementos de comunicación que se necesitan para la implementación, en este apartado se abarcaran algunos otros equipos que se deben de tener en cuenta, en la siguiente tabla se detallan las características principales y cantidades de insumos necesarios.

Insumo	Características	Cantidad
Router Huawei AX3	3000 Mbps 2.4GHz – 5GHz 10/100/1000Mbps WPA3-Personal, WPA2-Personal	1
Switch T3700G-28TQ	24 puertos 48 gbps 10/100/1000 Mbps IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.1p	3
Cisco Business 240AC	Frecuencia 2.4 GHz – 5 GHz Velocidad de transmisión 1733 Mbps Memoria Ram 255 MB Puertos Rj45 – USB 2.0 Estándar 802.11ac Seguridad WPA2 WPA3	1
PC	Intel core i7 – Ryzen 7 De 8 a 16 Gb de RAM 1 TB HDD / 500 GB SSD	1
Caja de Cableado	FTP Categoría 6	3
Caja de conectores RJ-45	Categoría 6	3
Ponchadora		2
Multitoma para rack	125v – 8 puertos	3
Patch Panel	24 puertos Cat 6	3
Gabinete Rack	Soporte a pared con ventilación	3

Tabla 18: Insumos y características

3.1.6.3. Factibilidad Económica

Se realizo un análisis de los costos de implementación determinando un valor total de realización, teniendo en cuenta cada característica de este y a su vez cada área, partiendo de los equipos principales de red, cableado estructurado hasta la mano de obra. El estudio fue realizado para ser entregado a la Unidad Educativa La Libertad para que tengan la base para una futura implementación estableciendo así más veneficios para el personal docente y estudiantes de la Unidad.

Costos de Inversión					
Equipos de red					
Ítem	Descripción	Unidad	Cantidad	P. unitario	P. total
1	Router Huawei AX3	Unidad	1	90.00	90.00
2	Switch T3700G-28TQ	Unidad	3	2200.00	6600.00
3	Cisco Business 240AC	Unidad	1	150.00	150.00
4	PC	Unidad	1	750.00	750.00
Total					7590.00

Tabla 19: Costo equipos de red

Cableado					
Ítem	Descripción	Unidad	Cantidad	P. unitario	P.total
1	Caja de Cableado RJ-45 cat 6	Unidad	3	180.00	540.00
2	Caja de conectores RJ-45 cat 6	Unidad	3	25.00	75.00
3	Ponchadora	Unidad	2	5.00	10.00
4	Multitoma para rack	Unidad	3	32.00	96.00
5	Patch Panel	Unidad	3	25.00	75.00
6	Gabinete Rack	Unidad	3	150.00	450.00
7	Canaletas PVC 40x25mm caja 10un	Unidad	5	90.00	270.00
8	Tornillos	Unidad	100	0.05	5.00
Total					1425.00

Tabla 20: Costos cableado

Mano de obra				
Ítem	Descripción	Cantidad	P. unitario	P. total
1	Puntos de red	50	10.00	500.00
2	Configuración de dispositivos	45	15.00	675.00
Total				1175.00

Tabla 21: Costos mano de obra

Costo total	
Descripción	P. total
Costo equipos de red	7590.00
Costo Cableado	1425.00
Costo mano de obra	1175.00
Total	10190.00

Tabla 22: Costo total de inversión

Luego de haberse realizado las tablas con todos los valores de implementación se debe tener en cuenta que los elementos mencionados se escogieron teniendo en cuenta no solo las necesidades actuales de la Unidad Educativa, si no también viendo a futuro con posibilidades de una expansión o implementación de nuevos departamentos a la red.

CONCLUSIONES

Lego de haber realizado todas las etapas del proyecto y de haber evidenciado los veneficios que este traería a la institución, se puede concluir que.

- En la primera etapa, en la fase de recolección de información y datos de infraestructura, se logró evidenciar la situación actual de la Unidad Educativa La Libertad, evidenciando así las principales falencias que tiene la red institucional.

- Una correcta administración de la red permite mejorar el servicio y la seguridad de la red institucional, brindando así una mejor experiencia al usuario.

- Otro de las desventajas que se evidenciaron fue la poca seguridad que se maneja en cuanto a la red, de modo que se concluye que la implementación de las políticas de seguridad es uno de los factores más importantes para tener en cuenta.

- El diseño de red que se propone cumple con todas las necesidades de seguridad, estabilidad y escalabilidad permitiendo actualizaciones o expansiones futuras.

- Se determino que una de las principales características con las que deben contar los dispositivos de red es que cumplan con el estándar IEEE 802.1q el cual permite realizar una segmentación por vlans.

- Con el análisis de factibilidad económica se pudo evidenciar que la inversión requerida para llevar a cabo el proyecto es elevada, pero si se toman en cuenta los factores y las necesidades que tiene y podría tener la institución a futuro, es un gasto justificado y con un correcto mantenimiento y administración, tanto los equipos como las configuraciones podrían servir para varios años lectivos.

RECOMENDACIONES

- Una de las principales recomendaciones que se puede dar es que, en caso de no implementar el rediseño de la red, de momento se haga uso del manual de Políticas de Seguridad que se creó para la institución, esto ayudara a mantener la integridad de los equipos con los que actualmente cuenta la Unidad Educativa.

- Para el servicio Firewall no es necesario realizar todo el rediseño de la red, como se evidencio en las pruebas, se puede implementar el servicio desde un ordenador para un área específica de la red, en este caso podría realizarse en el segundo laboratorio de cómputo de la institución.

- En caso de implementar el servicio de pfsense en el segundo laboratorio de cómputo, se recomienda que para tener un buen servicio de parte de este se utilice un computador con las características que se especificaron en la sección de análisis de requerimientos.

- Para el diseño de la red se utilizó solo un punto de acceso WiFi, en caso de ser necesario se puede implementar más de uno en los diferentes puntos de la institución, lo que se recomienda es que existan al menos dos puntos de red extras.

- Para el personal encargado del área de TI, se recomienda ampliar los conocimientos en redes y cableado estructurado para mejorar la administración y gestión actual de los equipos existentes.

ANEXOS

Anexo 1: Entrevista dirigida a la rectora de la Unidad Educativa La Libertad

Entrevista dirigida a la rectora de la unidad Educativa la Libertad	
Objetivo: Conocer datos actuales de condiciones de red desde el punto de vista del usuario	
1.	¿Cuánto tiempo tiene desde que fue diseñada la red? La red ya se encontraba implementada al momento de que la rectora tome su cargo, se estima que la red tiene alrededor de 8 años aproximadamente, dentro de los cuales se han implementado pequeños cambios a medida que ha pasado el tiempo.
2.	¿Cuántas personas se conectan actualmente a la red? Durante el tiempo de modalidad virtual los docentes tenían turnos rotatorios en los que se acercaban a impartir sus clases desde las instalaciones, existen alrededor de 60 docentes en la institución que se dividen en los horarios matutinos y vespertinos, diariamente asisten cerca de 10 docentes a impartir clases de forma virtual, dicho número no es el mismo todos los días, ya que varían dependiendo el horario de cada docente, entre docentes y personal administrativo y demás personas que forman parte de la institución se estima que cerca de 25 personas se conecten a la red actualmente.
3.	¿Sera necesaria la red para el futuro regreso a clases? Sera necesario debido a que se tiene previsto un retorno a clases progresivo, lo que nos da a entender que muchos docentes seguirán haciendo uso de la red para impartir sus clases, además con el programa que se está implementando por parte de la alcaldía, que consta de proporcionar tablets a los estudiantes de bachillerato, se espera que puedan hacer uso de estas como una herramienta para su aprendizaje.
4.	¿Cuántas personas se tiene previsto que hagan uso de la red con el regreso a clases? Con el regreso a clases progresivo, se tiene previsto que en una primera etapa ingresen los estudiantes de los años superiores, estos son alrededor de 500

	estudiantes, aparte del personal docente y administrativo, en esta primera etapa se cree que un promedio de 150 personas hagan uso de la red y en las etapas siguientes con el ingreso total de los estudiantes se espera que al menos 200 usuarios hagan uso de la red.
5.	¿Conoce cuantos puntos de acceso existen? Dentro de la institución los principales puntos de red se encuentran en el área administrativa y el área de laboratorios, estos serán 3 puntos de acceso a la red que se dividen para toda la institución, en el área admirativa se encuentran un total de 5 oficinas.
6.	¿La conexión actual es eficiente? No es eficiente en su totalidad, existen sectores de la unidad en donde acceder por medio de Wifi es imposible, la red presenta varios problemas a lo largo del día, lo que hace que durante periodos de tiempo se pierda la conexión.
7.	¿Piensa que la administración actual es correcta? No se cuenta con una buena administración, hay un solo punto en donde llega el servicio de red de forma cableada y desde este se reparte a los demás puntos, pero no se cuenta con los equipos necesarios como para tener una correcta administración ni seguridad.
8.	¿Cree que sean necesario cambios en el diseño? Si, los cambios son necesarios, la idea es que se pueda implementar un cambio y que permita que la conexión se pueda establecer en casi la mayoría de los puntos existentes en la unidad y que esta conexión se mantenga estable en el edificio administrativo y el pabellón de laboratorios, que es donde más se utiliza el servicio.
9.	¿Para que utilizan la red los docentes? Actualmente los docentes utilizan el servicio de internet para impartir sus clases de forma virtual, al igual que para asistir a video conferencias que son realizadas como reuniones de profesores para topar puntos académicos.
10.	¿Cree que un nuevo diseño para administración y aplicación de políticas mejorara la eficiencia de la red?

	Con que se pueda tener una buena administración y gestión de la red sería un gran cambio en la eficiencia que el servicio nos brinda, además la implementación de políticas de seguridad añade un extra a la mejora del servicio.

Anexo 2: Entrevista dirigida al docente encargado de los laboratorios de cómputo y red

Entrevista dirigida al docente encargado de los laboratorios de cómputo y red	
Objetivo: Conocer datos actuales de condiciones de red desde el punto de vista del usuario	
1.	¿Conoce el estado actual de la red? Si, como docente encargado del área tecnológica conozco el estado en el que se encuentra la red, no se cuenta con una correcta arquitectura ni con los protocolos adecuados.
2.	¿Cree que el diseño con el que se cuenta cumple las necesidades de la unidad educativa? El diseño actual no cumple las necesidades que se tiene, existen puntos en los que no se puede acceder a la red y puntos en los que se ha querido implementar nuevas estaciones cableadas y por el mal diseño es imposible crear la extensión hasta el punto de que se requiere, la unidad cuenta con un total de 5 pabellones de 3 aulas y un pabellón de 5 aulas además del edificio administrativo y área de laboratorios, y existen pabellones a los que no llega el servicio.
3.	¿Se han implementado técnicas de seguridad en la red? Los únicos métodos de seguridad con los que se cuenta son las contraseñas de acceso a la red, pero es un método básico, aparte de eso, no se cuenta con más métodos de seguridad.
4.	¿Mantiene un monitoreo constante del estado de la red? La estructura y el diseño actual no permite mantener un monitoreo de la red, no se encuentra instalada una herramienta que facilite esta tarea, si en algún momento se pierde la conexión lo único que se hace es esperar a que el servicio se restablezca.

5.	¿Conoce cuantos puntos de acceso existen? Dentro de la institución existen puntos de acceso en el área administrativa y en el área de los laboratorios, desde estos puntos se reparte la señal para toda la unidad, en el área administrativa hay un punto de red y en los laboratorios hay dos puntos.
6.	¿La conexión actual es eficiente? No se cuenta con una buena conexión, existen periodos de tiempo en los que hay conexión a Internet, pero los dispositivos tardan en abrir o cargar los aplicativos que requieran una conexión estable.
7.	¿Piensa que la administración actual es correcta? No se cuenta con una buena administración, la gestión de cables y puntos de red no es adecuada.
8.	¿Cree que sean necesario cambios en el diseño? Si, para tener una mejora notable es necesario rediseñar por completo la red, además de implementar mecanismos de monitoreo y seguridad para precautelar la información de los usuarios que se conectan a la red.
9.	¿Qué cree usted que hace falta para que la red cumpla su propósito dentro de la institución? Una reestructuración total
10.	¿Qué aspecto es el que dificulta que la red funcione de forma óptima? No se cuenta con los equipos necesarios como para mantener una mejor gestión de la red, el presupuesto es uno de los factores que afecta de manera considerable en esto, no se puede adquirir los equipos óptimos.

Anexo 3: Registro descriptivo de la información

Registro descriptivo de la información
Fecha: 09/12/2021 Proceso: Recolección de información mediante método de observación Tipo de Observación: Natural Lugar: Unidad Educativa La Libertad
Objetivo
Extraer información de la red institucional mediante la técnica de observación.

<table>
<tr><td colspan="2">Hechos observados</td></tr>
<tr><td colspan="2">Routers y Switchs no se encuentran ubicados de forma correcta dentro de un rack o armario.
La estructura en donde se encuentran los equipos no brinda la seguridad contra caídas.
Equipos de red básicos.
Los equipos con los que se cuenta no son administrables.
Mala gestión de cables en laboratorios de cómputo y cuarto de redes.
Las conexiones de red se encuentran en las mismas canaletas de las conexiones eléctricas.
No se cuenta con repetidores o antenas ubicadas en las áreas alejadas al área administrativa y área de laboratorios.
La seguridad física de los equipos se está limitada al no encontrarse en un área adecuada.
Interferencia entre canal de la red con redes externas.
El cableado implementado no se encuentra en la categoría necesaria.
Los estudiantes y personal académico no autorizado tienen fácil acceso al área donde se encuentran instalados los equipos de red.
Sobrecarga de dispositivos para un punto de red.</td></tr>
<tr><td>Análisis</td><td>Se pudieron identificar problemas que afectan de forma notable el comportamiento del servicio, partiendo de una mala administración y la existencia nula de métodos de seguridad tanto físicos como lógicos para el acceso.</td></tr>
<tr><td>Responsable</td><td>Ascencio Caiche Anthony Bryan</td></tr>
</table>

Anexo 4: MANUAL DE POLÍTICAS DE SEGURIDAD INFORMATICA DE LA UNIDAD EDUCATIVA LA LIBERTAD

CAPITULO I

AMBITO, OBJETOS Y AFINES

Art 1. Ámbito. - Las presentes políticas abarcaran todos los servicios informáticos que ofrezca la UELL y es de aplicación obligatoria para todos los departamentos internos.

Art 2. Objeto. – El presente manual tiene como objeto asegurar el acceso de cada uno de los miembros de la unidad educativa a los servicios informáticos que esta brinda.

Art 3. Fines. – Son fines del presente documento:

1. Evitar incidentes de seguridad que puedan afectar la integridad de los servicios o la información.
2. Mantener un control activo de las medidas de seguridad y evaluar la efectividad de estas.
3. Garantizar un entorno seguro para el desarrollo de las actividades académicas.

CAPITULO II

CONTENIDO DEL MANUAL DE POLÍTICAS

Propósito

El presente manual tiene el propósito de mostrar a toda la comunidad educativa las políticas y normas a cumplir para mantener la seguridad y la integridad de los activos de TI que se encuentran dentro de la institución, además de asegurar el correcto desarrollo de actividades educativas.

Introducción

El manual de políticas de seguridad de TI de la Unidad Educativa La Libertad, representa una herramienta fundamental para el buen desarrollo de las actividades académicas, además del buen funcionamiento de los servicios que brinda la unidad, garantizando así la eficiencia y optimización de recursos y de sistemas internos

Se define a las TI como las herramientas y metodologías claves para generar, manipular, distribuir y emitir la información que se encuentra estrechamente relacionada con los

sistemas de información y con los elementos y equipos de Hardware que forman parte de una unidad, empresa o compañía.

Una de las bases principales para que se realice un correcto funcionamiento de funciones, además de generar confiabilidad de información y procesos es la definición de políticas y estándares de seguridad. Dentro de este documento se detallan las principales políticas para el usuario, las cuales se encuentran definidas en políticas generales para todo el personal académico y políticas específicas para las áreas de mayor control.

Puntos a considerar:

- Seguridad Personal.
- Seguridad Física.
- Controles de Acceso.
- Controles de Navegación.

Objetivo

Crear y definir políticas generales y específicas que ayuden con el cumplimiento óptimo de las actividades académicas, además de asegurar la integridad física y lógica de los dispositivos de cómputo y de red que formen parte de la red educativa.

Alcance

El presente manual está diseñado para que se cumplan las políticas a nivel general dentro de la institución, dirigido tanto para el personal administrativo, docentes y estudiantes que conforman la Unidad Educativa La Libertad.

Sanciones por incumplimiento

En caso de detectarse el incumplimiento del presente manual generara las respectivas sanciones dependiendo el nivel de gravedad y del usuario que haya generado la falta.

Beneficios

La implementación de una correcta política de seguridad brindara la seguridad necesaria para mantener la integridad de los activos que se encuentren dentro de la Unidad Educativa La Libertad.

POLÍTICA GENERAL

Todo usuario perteneciente a la institución que haga uso de bienes o servicios informáticos se compromete a regirse bajo los principios de uso adecuado de los recursos informáticos de la Unidad Educativa La Libertad y de igual forma seguir de forma rigurosa el Manual de Políticas y Estándares de Seguridad de La Información.

Obligaciones del Usuario

- Es responsabilidad del usuario cumplir con las normas y estándares que se indiquen en el presente manual.

Entrenamiento

- Todo colaborador que ingrese por primera vez a la laborar en las instalaciones de la Unidad Educativa La Libertad tendrá la obligación de leer el Manual de Políticas y Estándares de Seguridad informática de la Unidad Educativa La Libertad, para que tenga un total conocimiento de las obligaciones que tiene como usuario.
- La Unidad Educativa La Libertad tendrá un docente encargado de aclarar los puntos del manual en caso de que se presente alguna duda de parte del personal de nuevo ingreso.

Medidas disciplinarias

- Cuando el departamento de rectorado identifique el incumplimiento del presente Manual emitirá un llamado de atención formal hacia el usuario que haya incumplido con las normas establecidas.

POLÍTICAS Y ESTANDARES DE SEGURIDAD FÍSICA

Política

Los mecanismos de control que se encuentren implementados en la institución para el ingreso del personal perteneciente a la institución o de terceros deberán permitir el acceso a áreas restringidas solo al personal autorizado para asegurar la integridad de los equipos de cómputo y de comunicaciones.

Resguardo y protección de la información

- Es obligación del usuario dar aviso inmediato al departamento de Rectorado en caso de detectar algún riesgo potencial para los equipos de cómputo, sean estos incendios, fugas de agua, contactos eléctricos en mas estado u otros.
- El usuario deberá mantener la protección de dispositivos de almacenamiento extraíbles que se encuentran bajo su disposición además de los dispositivos portátiles que se encuentren bajo su cargo.

Controles de acceso físico

- El personal docente, administrativo, estudiantes y terceros no pueden manipular los equipos de comunicación que se encuentren ubicados en el cuarto de redes o en cada uno de los racks de cada uno de los laboratorios.

Seguridad en áreas de trabajo

- Solo personal autoriza por el departamento de rectorado tiene acceso al cuarto de redes de La Unidad Educativa La Libertad.
- Los equipos de comunicación que se encuentran en los laboratorios de computación son de acceso restringido, solo el personal encargado tiene acceso a estas infraestructuras.
- Los canales de comunicación, cableado, canaletas, puntos de acceso serán únicamente manipulados por el personal encargado del área de redes.

Protección y ubicación de los equipos

- El equipo que de cómputo asignado será únicamente para el desarrollo de las funciones establecidas y para uso educativo.
- Los usuarios no pueden mover los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos sin la autorización del departamento de Rectorado, las misma que deberá ser solicitada al departamento en caso de requerir el servicio.
- Los usuarios tienen prohibido abrir o manipular los componentes de internos de los equipos de cómputo, porque se corre el riesgo de daños físicos.

- Cada usuario tiene la responsabilidad de solicitar la debida capacitación para el manejo de las herramientas informáticas que utilice el equipo que se le haya asignado.
- El usuario no deberá almacenar información personal dentro de los equipos que se encuentren en las estaciones asignadas.
- Deberá mantener los equipos informáticos en un entorno limpio, libre de humedad o algún factor externo que pueda dañar los componentes físicos del mismo.
- Se deberá evitar colocar objetos sobre los equipos.
- En caso de ser necesaria la reubicación de la estación de trabajo, se deberá solicitar el soporte por parte del personal encargado del área de cómputo y telecomunicaciones.

Mantenimiento de los equipos

- El mantenimiento de los equipos será únicamente realizado por el personal autorizado por parte del departamento de rectorado.
- Los usuarios no deberán conectar dispositivos extraíbles sin realizar el respectivo análisis del antivirus ubicado en los equipos de cómputo.
- Es obligación del usuario encargarse de respaldar la información que crea importante para el desarrollo de sus actividades, esto para evitar la pérdida de dicha información cuando el equipo sea enviado a mantenimiento o revisión.
- El personal encargado de realizar el mantenimiento respaldara únicamente la información que crea relevante, carpetas como videos, música, no serán respaldados.

Transferencia de equipos

- El usuario al que se le asigne un dispositivo de cómputo se le hará firmar el acta de entrega respectiva, en la que constara la fecha de entrega, características del dispositivo al igual de la serie de cada uno de los periféricos con los que sea entregado.
- La custodia de las laptops es de carácter personal, de modo que está prohibida su transferencia entre los usuarios.

Daño de equipo

- El equipo de cómputo que presente algún desperfecto o falla deberá ser enviado al personal responsable de mantenimiento, donde se evaluara el estado del equipo y se determinara la causa del problema, en caso de que se detecte mal uso, descuido o negligencia, el usuario deberá cubrir el valor de la reparación.

POLÍTICA Y ESTANDARES PARA EL CORRECTO USO DE INTERNET Y NAVEGACIÓN

Política

El acceso a páginas web a través de la red y los equipos instalados dentro de la misma debe ser responsable, evitar el uso de la red para actividades fuera del ámbito académico y no se deberán descargar programas que puedan dañar o afectar el correcto funcionamiento de los equipos.

Navegación

- La navegación a internet estará controlada por los sistemas de firewall de la red, de modo que las estaciones de trabajo contaran con acceso restringido a sitios que no sean de índole académico.
- El usuario no deberá manejar las configuraciones de red de cada uno de los equipos o estaciones de trabajo.
- En caso de detectarse alguna navegación o ingreso a paginas ajenas al desarrollo de las actividades académicas se generará el debido bloqueo del sitio.
- Los estudiantes que se encuentren autorizados para el ingreso de dispositivos móviles deberán registrar su ingreso en las oficinas de inspectoría académica.

Contraseñas y sitios guardados

- Es obligación del usuario mantener una correcta gestión de contraseñas de acceso a correos institucionales, plataformas educativas entre otras.
- El usuario deberá evitar el guardado de contraseñas automático en los sitios de navegación.

POLÍTICAS Y ESTÁNDARES PARA USO DE EQUIPOS DE LABORATORIOS DE COMPUTACIÓN

Obligación del usuario

Los estudiantes deberán seguir las especificaciones del docente encargado del laboratorio al igual que las normas establecidas para el ingreso y uso de los equipos.

Entrenamiento

Los docentes que impartan sus clases en los laboratorios tendrán la obligación de capacitar a los estudiantes para el conocimiento de las normas y reglas para el ingreso y uso de las instalaciones y equipos de cómputo.

Seguridad física de los equipos

Política

- El acceso a los laboratorios será exclusivamente para los usuarios pertenecientes a la Unidad Educativa La Libertad, sean estos docentes o estudiantes, los cuales deberán regirse al horario de clases establecido, además los equipos que se encuentren dentro de los laboratorios contaran con un usuario establecido para los estudiantes y otro al que tendrá acceso solo personal docente o encargado de laboratorios.

Control de acceso de usuarios

- Los estudiantes tienen permitido el ingreso solo al usuario “Estudiantes” de cada uno de los equipos ubicados en los laboratorios, el ingreso al usuario “administrador” de los equipos se encontrar bloqueado por contraseña.
- Los estudiantes tienen prohibido el ingreso al equipo principal del laboratorio, el cual es únicamente para uso del docente.

Resguardo y protección de infraestructura

- Los estudiantes no tienen permitida la manipulación de los componentes internos de los equipos de cómputo.
- Los estudiantes no deberán manipular, extraer o mover las piezas de hardware de los equipos de las estaciones de trabajo dentro de los laboratorios.

- Las canaletas, cableado de comunicación o eléctrico no deberá ser manipulado por el personal estudiantil.
- Los equipos de telecomunicaciones que se encuentren en los racks ubicados en los laboratorios no deberán ser manipulados por los estudiantes.
- Los estudiantes deberán comunicar de forma inmediata al docente encargado de la materia o al personal encargado del laboratorio en caso de presenciar alguna falla en uno de los equipos o parte de la infraestructura del laboratorio.

Internet y navegación

- Los equipos que se encuentren dentro de los laboratorios contaran con las debidas restricciones de navegación que proporciona el firewall de la institución.
- Los estudiantes no deberán manipular las configuraciones de red de los ordenadores.
- Los estudiantes tienen prohibido el ingreso a páginas de ocio dentro de los equipos de los laboratorios.
- En caso de detectar posibles fallos de conexión el estudiante deberá notificar de forma inmediata al docente encargado del laboratorio.

GESTION DE INCIDENTES

Obligaciones del usuario

Los usuarios serán los encargados de notificar al departamento de dirección los posibles incidentes o problemas que se generen en las estaciones de trabajo con los equipos de cómputo o los equipos de red.

Política

- El usuario al que se le haya asignado un dispositivo será el único responsable del uso que le dé al equipo, en consecuencia, deberá responder en caso de perdida, robo o avería del equipo.
- El aviso en caso de robo, perdida o desaparición deberá hacerse de forma inmediata al departamento de Rectorado.

Posibles incidentes

Robo o perdida de dispositivos de Hardware: perdida de los equipos físicos (computadoras, portátiles, equipos de telecomunicaciones) que sean de propiedad de la Unidad Educativa La Libertad.

Actividad de virus informáticos: Virus, troyano, código malicioso, etc, que pueda llegar a perjudicar el correcto funcionamiento de los equipos de cómputo.

Actividad de reconocimiento (escaneo de vulnerabilidades, intentos de acceso, monitoreos): Actividades que intenten acceder o identificar las estaciones de trabajo, métodos de seguridad, protocolos o servicios implementados dentro de la red.

Reporte de gestión de incidentes

Todos los usuarios, personal académico, administrativo, estudiantes, serán los encargados de reportar de manera inmediata los posibles riesgos que puedan afectar el desarrollo normal de las actividades o vulnerabilidades que se lleguen a detectar dentro de los equipos o red de la Unidad Educativa La Libertad.

Gestión de incidentes

- Todo incidente detectado deberá ser tratado por el personal encargado del área de TI mediante el correcto procedimiento de tratamiento de incidentes que garantice un análisis, investigación, documentación y soluciones del caso.
- El personal encargado del área de TI serán los responsables de analizar y determinar que eventos se pueden llegar a considerar como un incidente de seguridad.
- El equipo de TI deberá estar a disposición para atender los requerimientos o notificaciones de los incidentes.

CAPITULO III

DEFINICIONES

TI: Tecnologías de la Información, se refiere a aquellas herramientas o métodos que se empleen para analizar, monitorear y generar información dentro de un ambiente empresarial, laboral, investigativo o académico.

Firewall: Es un mecanismo de seguridad o dispositivo que supervisa el tráfico de la red sea entrante o saliente, permitiendo así el bloqueo de tráfico especifico mediante el uso de reglas de seguridad.

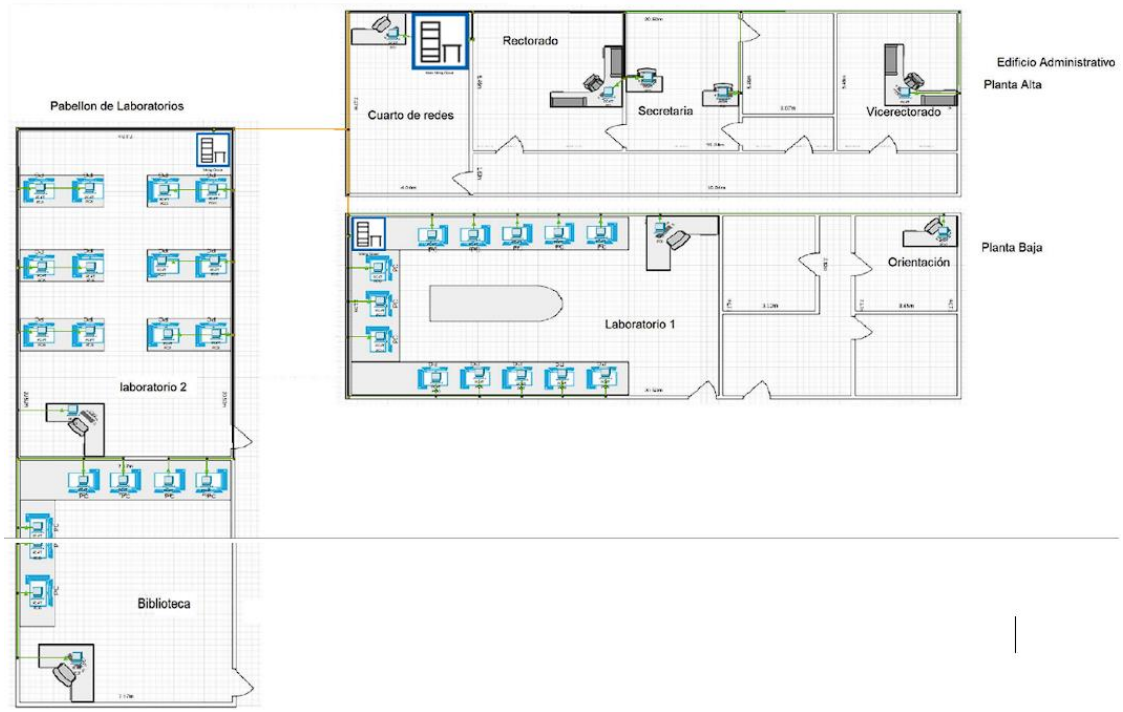
Internet: Red informática de enlace global, redes conectadas mediante distintos protocolos que permiten el uso de servicios y recursos alojados en diferentes dominios.
Red informática: Es un conjunto de dispositivos conectados entre sí mediante un medio físico o lógico los cuales comparten información y recursos.

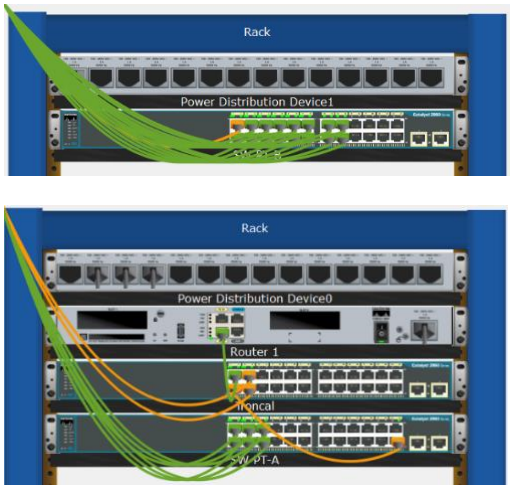
Software: Termino informático que hace referencia al conjunto de programas o rutinas que permiten que un ordenador o dispositivo de cómputo lleve a cabo actividades o tareas.

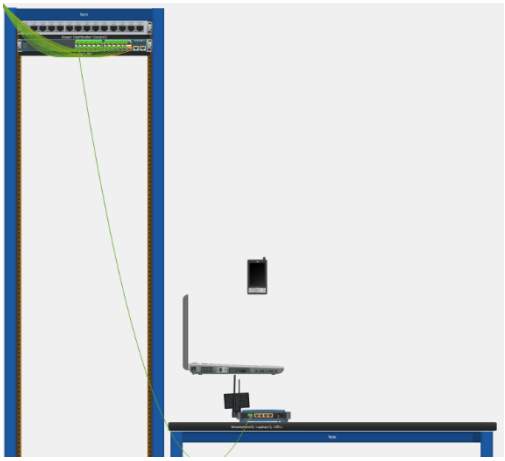
Hardware: Equipo o soporte físico de un ordenador o elemento de red.
Seguridad Lógica: Controles específicos que se establecen para tener una correcta administración de acceso a los sistemas de información que funcionan en conjunto con los mecanismos de seguridad física.
Vulnerabilidades: Falla en los elementos de seguridad que pueda comprometer la integridad de la información o de los equipos pertenecientes a la red informática.
Monitoreo de red: Método que se utiliza para recopilar información de la red en la que se encuentra.

Anexo 5: configuración de la red

Topología y equipos de red







Configuración Switchs

Switch Troncal, creación de Vlans

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name laboratorios
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name administracion
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name invitados
Switch(config-vlan)#
```

Asignación de interfaces modo Trunk

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#swtchport mode trunk
                       ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#switchport mode trunk


Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Listado de vlans creadas dentro del switch troncal

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   laboratorios                      active
20   administracion                    active
30   invitados                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Switch Planta alta (edificio administrativo)

Creación de Vlan

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name administracion
Switch(config-vlan)#exit
Switch(config)#
```

Asignación de puertos de acceso

```
Switch(config)#interface range fa0/1-10
Switch(config-if-range)#swit
Switch(config-if-range)#switchport mode acce
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#swit
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#
```

Asignación de Puerto troncal

```
Switch(config)#interface fa0/24
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Vlans y puertos asignados dentro del switch Planta Alta

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Gig0/1, Gig0/2
20   administracion                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Guardado de configuración

```
Switch#copy ru
Switch#copy running-config sta
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Configuración de Switch laboratorio

Asignación de puertos de comunicación

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1-14
Switch(config-if-range)#swi
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#swi
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#
```

```
Switch(config)#interface range fa0/15-22
Switch(config-if-range)#swi
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#swi
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

Asignación de puerto Troncal

```
Switch(config)#interface fa0/24
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Vlans y puertos asignados dentro del Switch Laboratorio

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/23, Gig0/1, Gig0/2
10   laboratorios                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14
20   administracion                    active
30   invitados                         active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Guardado de configuración

```
Switch#copy run
Switch#copy running-config sta
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Switch planta baja (edificio administrativo)

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name laboratorios
Switch(config-vlan)#exit
Switch(config)#
```

```
Switch(config)#vlan 20
Switch(config-vlan)#name administracion
Switch(config-vlan)#exit
```

Asignación de puertos de comunicación

```
Switch(config)#interface range fa0/1-16
Switch(config-if-range)#swit
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/17-22
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface fa0/24
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Valns y puertos asignados dentro del Switch Planta Baja

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/23, Gig0/1, Gig0/2
10   laboratorios                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
20   administracion                    active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Guardado de configuración

```
Switch#copy run
Switch#copy running-config sta
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Configuración router principal

Asignación de direcciones IP a vlans correspondientes mediante el protocolo dot1Q

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0.1
Router(config-subif)#encap
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#192.168.110.1
                     ^
% Invalid input detected at '^' marker.

Router(config-subif)#ip address 192.168.110.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.120.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.130.1 255.255.255.0
Router(config-subif)#
```

Levantamiento de puertos

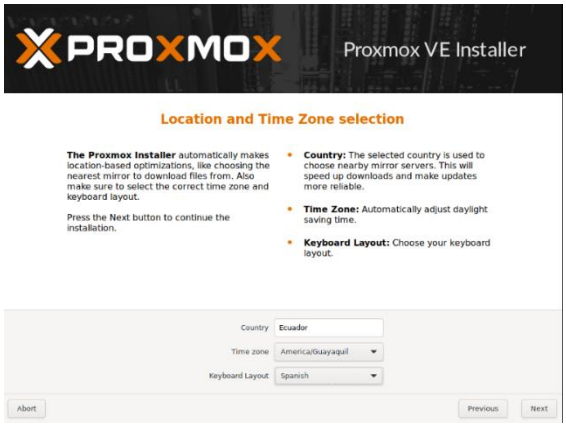
```
Router(config)#interface fa0/0
Router(config-if)#nos
Router(config-if)#no s
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up
```

Guardado de configuración

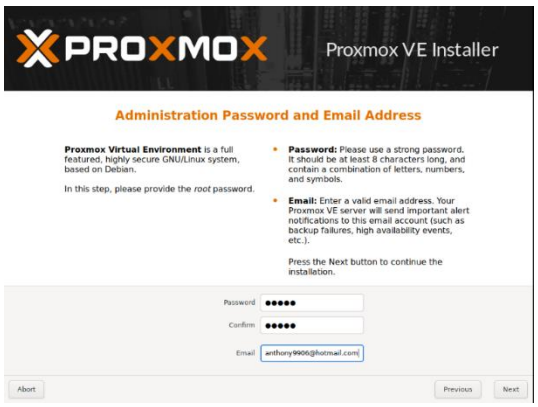
```
Router#copy ru
Router#copy running-config sta
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

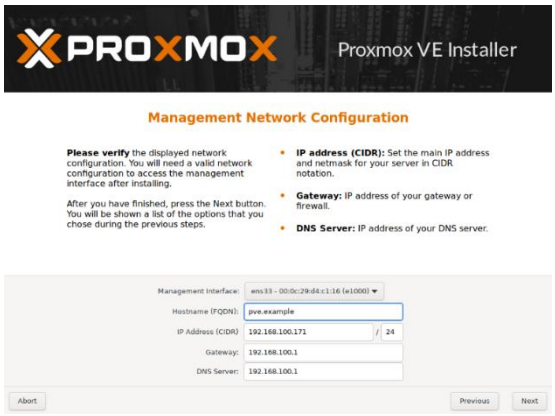
Anexo 6: Instalación de Proxmox

Selección de disco y configuración de zona horaria

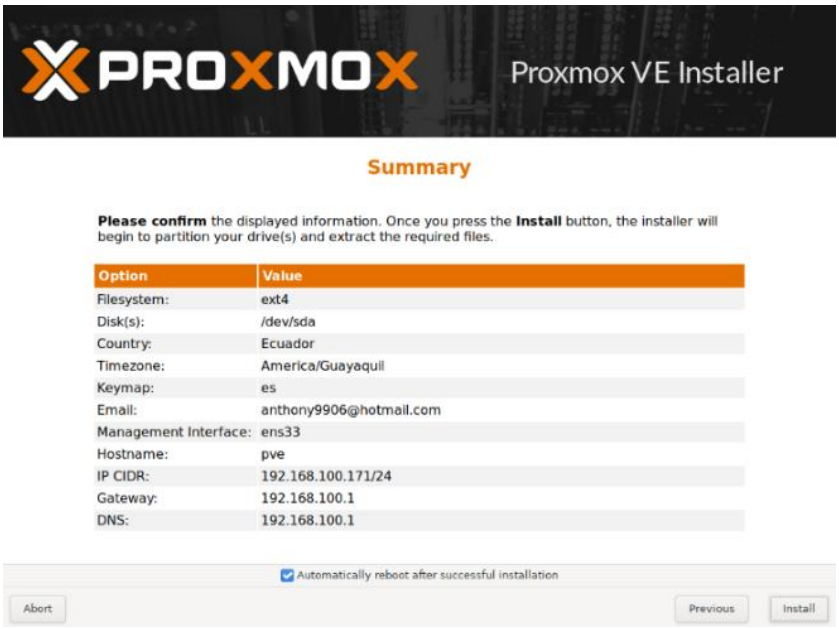


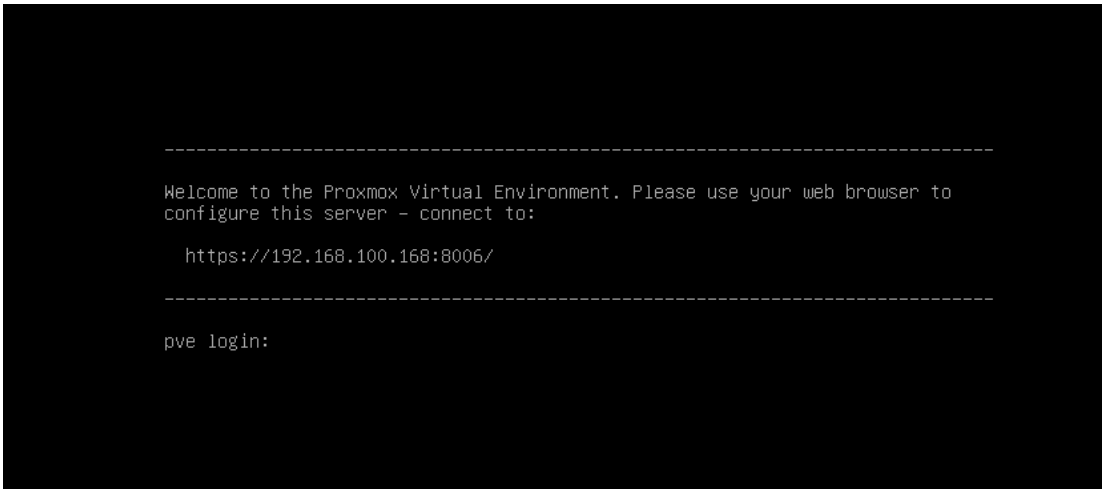
Asignación de contraseña y correo electrónico y configuración de IP



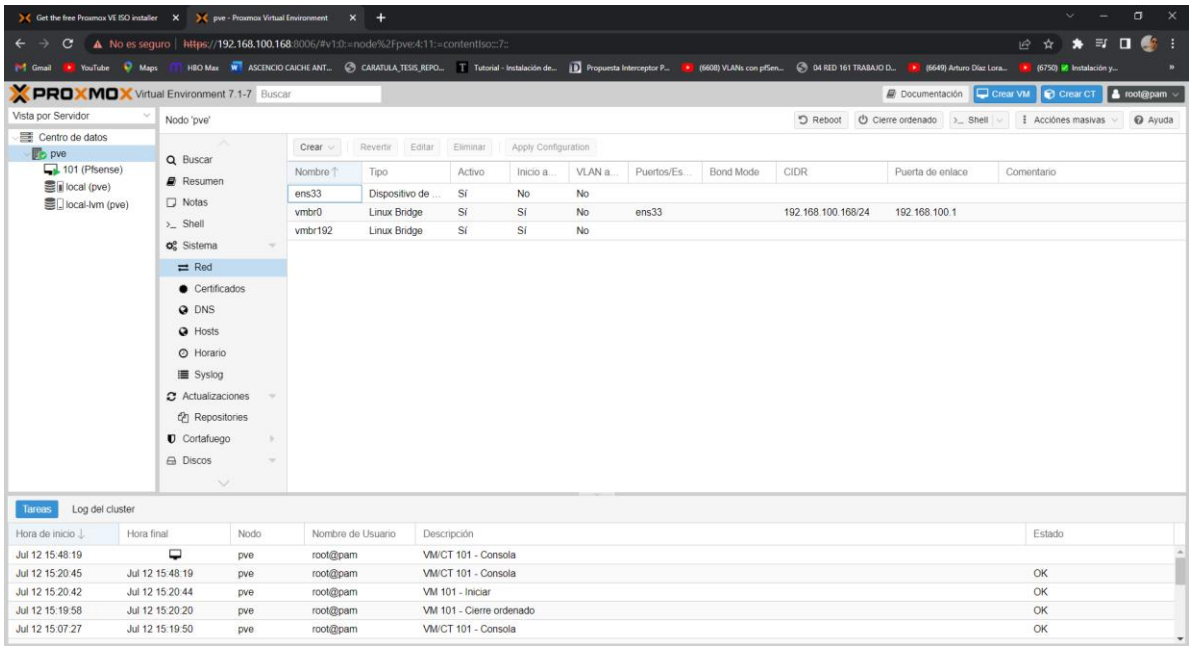


Resumen y final de instalación y consola





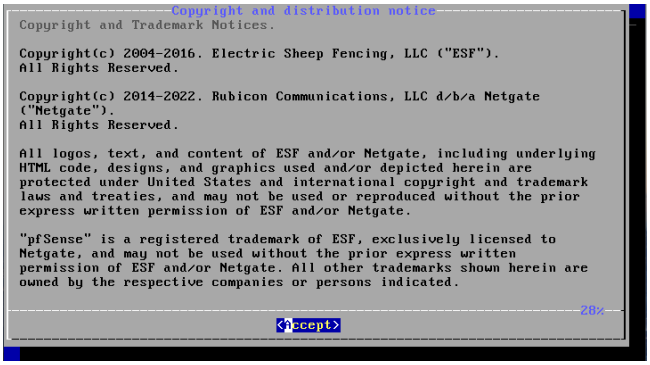
Para acceder a la interfaz gráfica de configuración accedemos desde cualquier navegador de un dispositivo que se encuentre conectado a la red

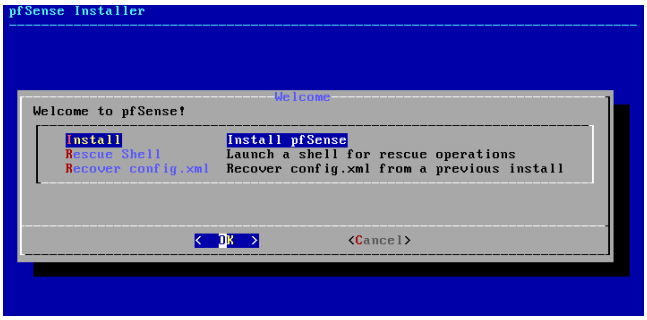


Anexo 7: Configuración de pfsense

Es necesario añadir pfsense a Proxmox, para esto cargamos la imagen iso del sistema operativo

Una vez cargada la imagen iso se procede con la instalación





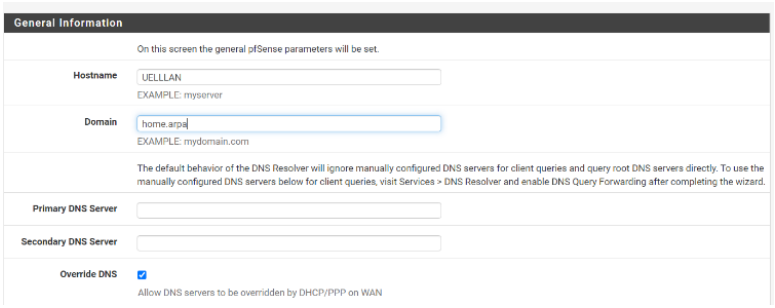
Disco de pfsense e inicio de instalación

Reinicio para finalizar instalación

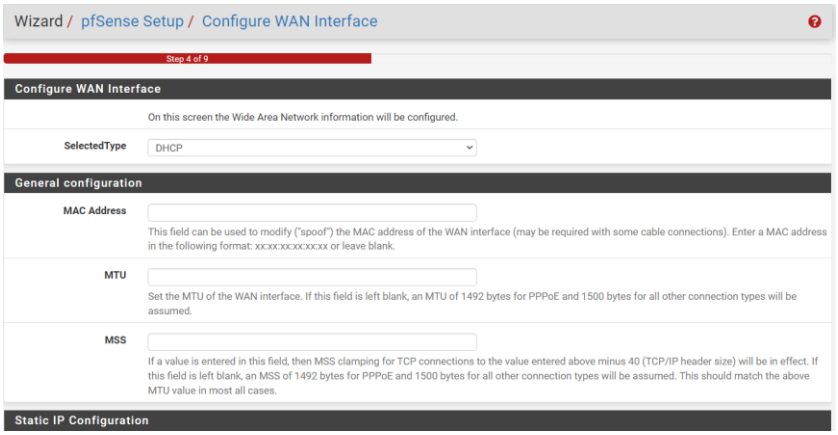
Anexo 8: Configuración inicial de pfsense en apartado web

Al abrir pfsense desde un navegador conectado a la red por primera vez, se nos despliega la interfaz de configuración inicial

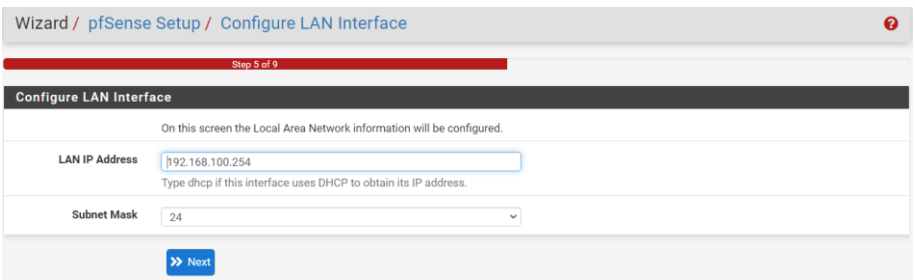
Lo primero que se realiza es el añadir el nombre de hostname que se desee



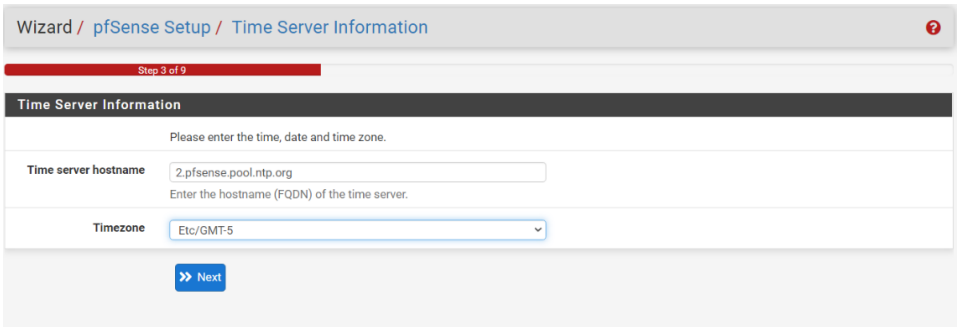
Seguido a eso se deberá activar el direccionamiento DHCP, esto se cambiará más adelante en las futuras configuraciones



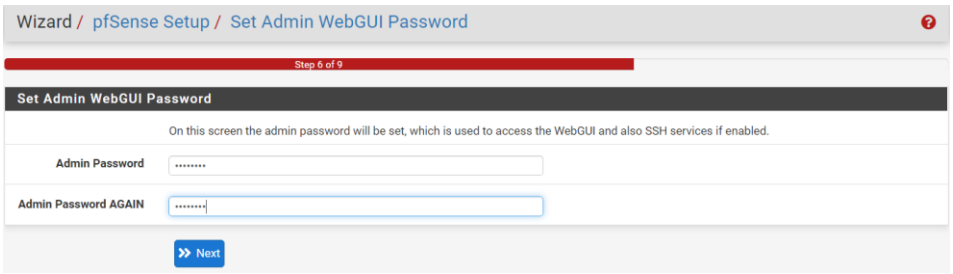
Se puede cambiar la dirección IP de la red LAN, en este caso se mantiene la misma dirección que ya se había configurado desde la consola.



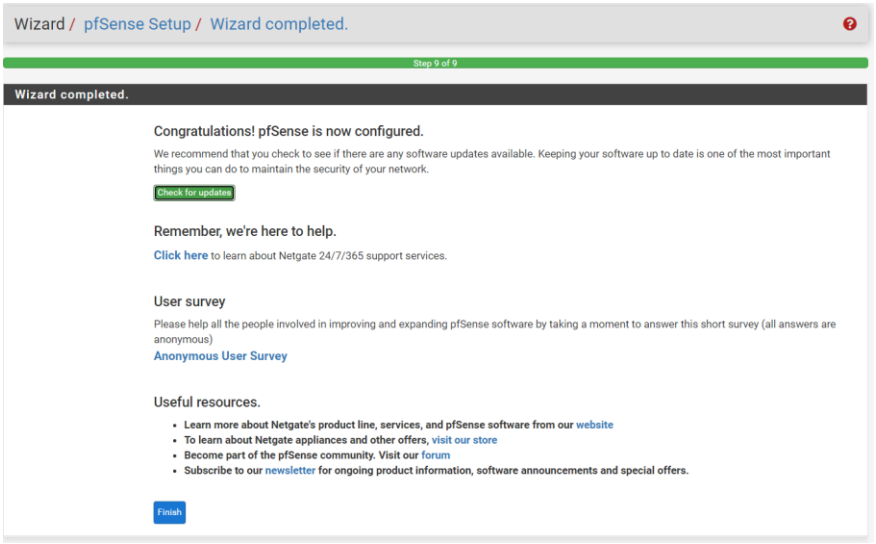
Dentro de las funciones de pfsense está el bloqueo o asignación de horarios, de modo que en la configuración inicial nos pide que agreguemos la zona horaria en la que nos encontramos



Para seguir con las configuraciones pfsense solicita un cambio de contraseña

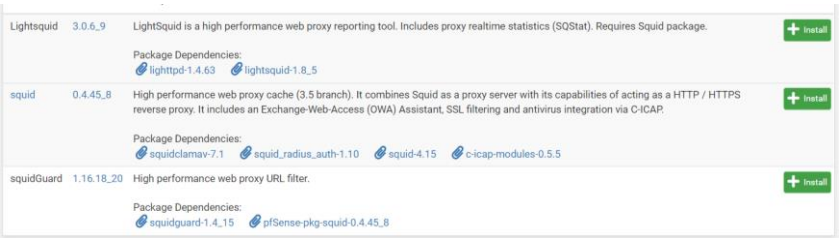


Una vez terminada la configuración inicial se mostrará un mensaje en color verde que indicara que la configuración ha finalizado, seguido a eso se puede acceder al panel principal de la herramienta

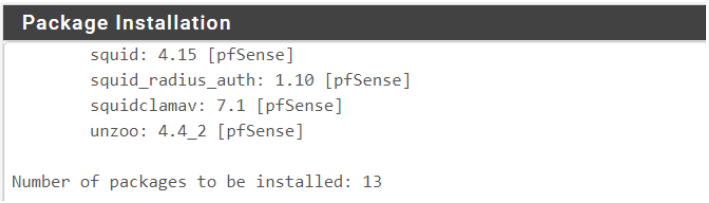


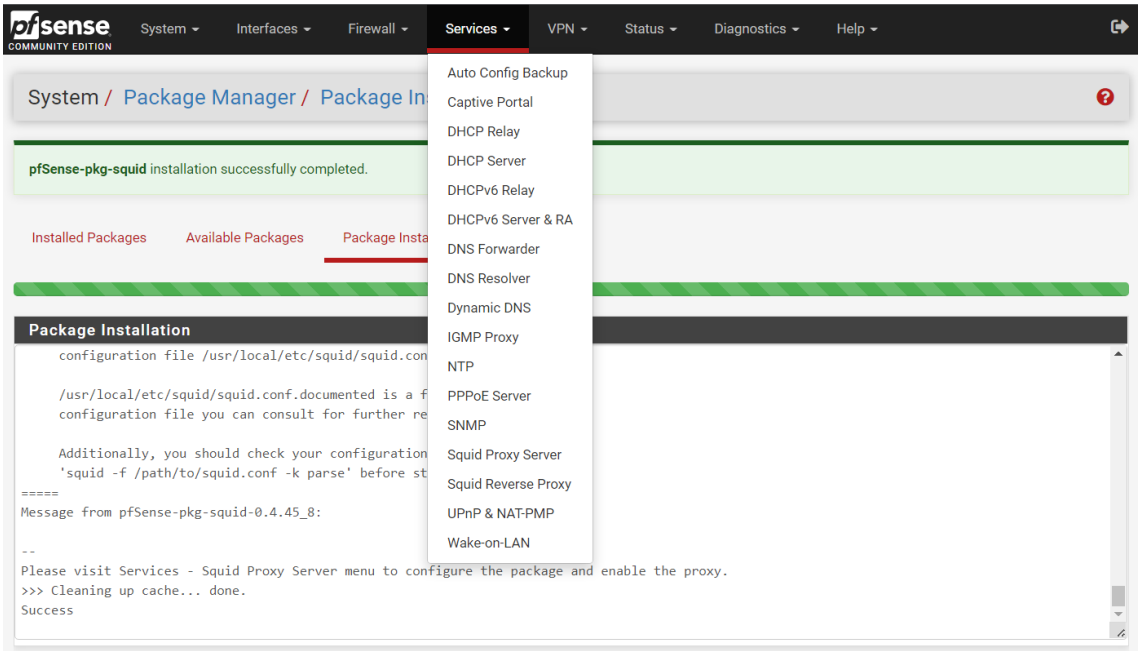
Anexo 9: Instalación de servicio proxy Squid en pfsense

Dirigirse a System / Package Manager / Available Packages, en el buscador escribir Squid y seleccionar la opción del paquete que se desea instalar



Descarga e instalación de Squid

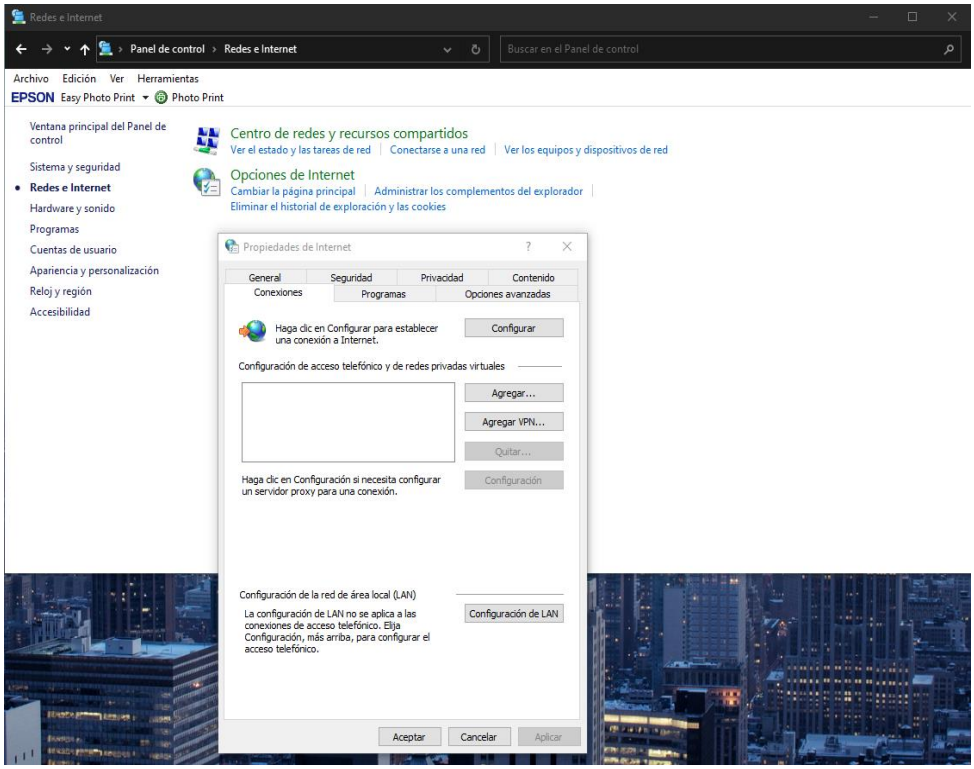




Anexo 10: Activar proxy en dispositivos

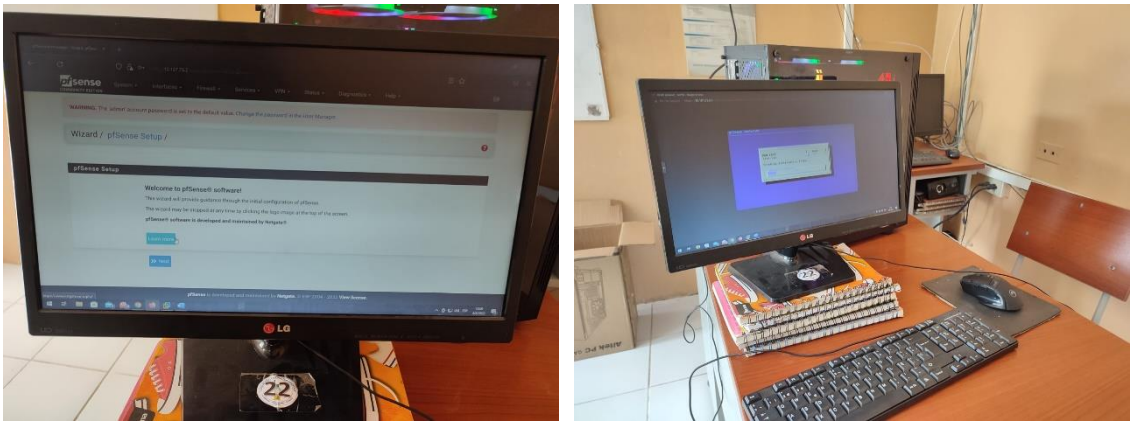
Para activar el proxy en un dispositivo con Windows 10 dirigirse a panel de control/opciones de internet/configuración de LAN

En la dirección ip se deberá establecer la dirección Ip de pfsense, Squid utiliza el puerto 3120 por defecto, en este caso no se cambia el puerto

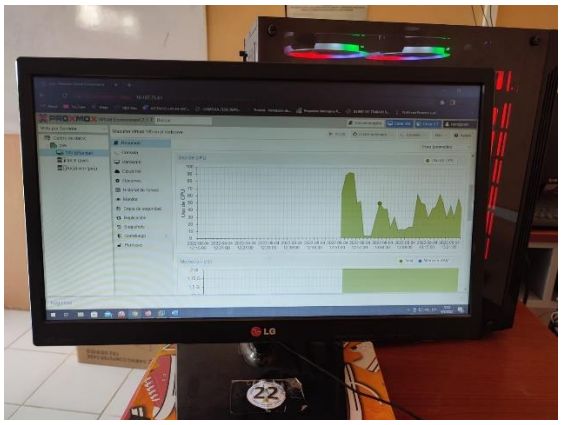


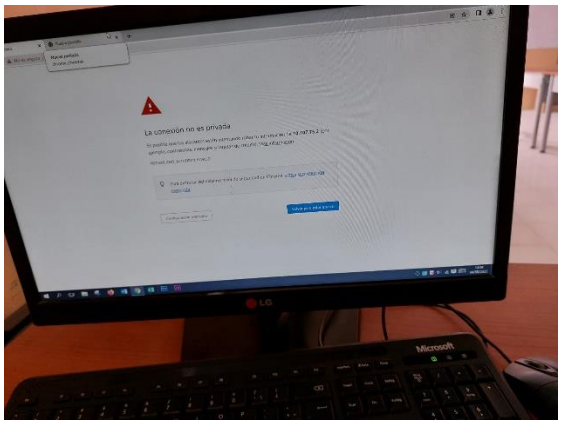
Anexo 11: Instalación dentro del laboratorio

Anexo 12: Instalación de Pfsense dentro del laboratorio

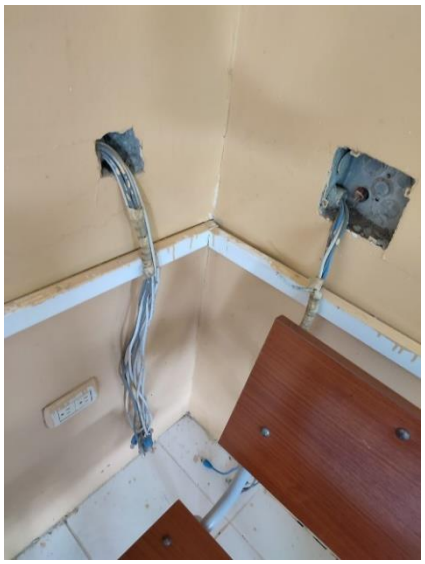


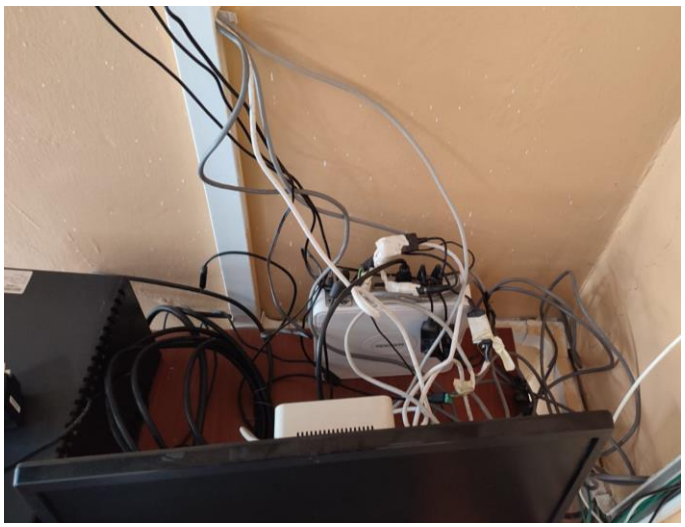
Anexo 13: Pruebas y rendimiento

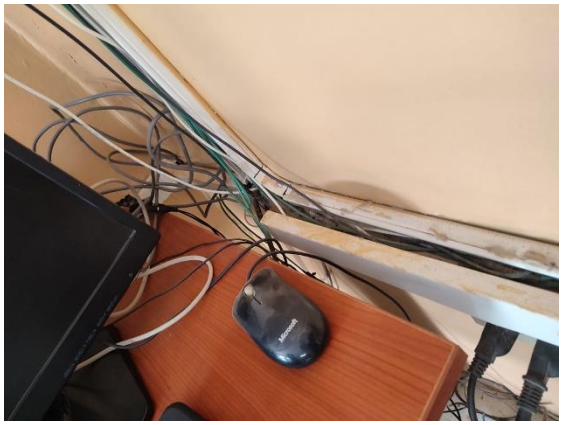


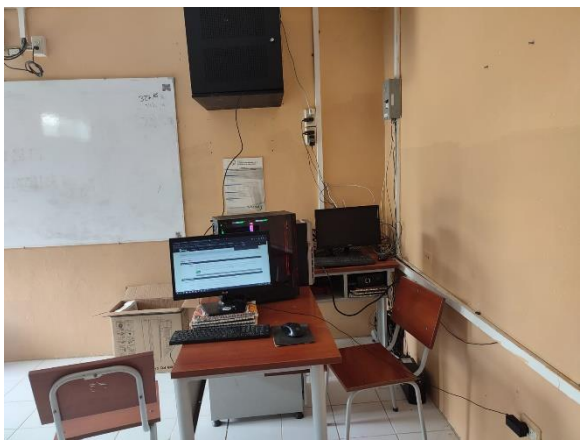


Anexo 14: Estado de las instalaciones









BIBLIOGRAFÍA

[1] N. Selwyn, «Internet y educación,» de *Cambio*, BBVA, 2013, p. 463.

[2] I. Society, «Internet Society,» Noviembre 2017. [En línea]. Available: https://www.internetsociety.org/es/resources/doc/2017/internet-access-and-education/. [Último acceso: 10 Noviembre 2021].

[3] infoescuelas, «Infoescuelas,» 11 Mayo 2017. [En línea]. Available: https://www.infoescuelas.com/ecuador/santa-elena/unidad-educativa-la-libertad-en-la-libertad/. [Último acceso: 29 Octubre 2021].

[4] R. V. Alegre, «Diseño, desarrollo e implementación de una red de área local (LAN) en GA-AUTOTRIM,» 2019. [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/125775/Vivas%20-%20Dise%C3%B1o,%20desarrollo%20e%20implementaci%C3%B3n%20de%20una%20red%20de%20%C3%A1rea%20local%20(LAN)%20en%20GA-Autotrim.pdf?sequence=1. [Último acceso: 31 Octubre 2021].

[5] R. P. J. kenedy, «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,» 2019. [En línea]. Available: https://repositorio.uncp.edu.pe/handle/20.500.12894/5434. [Último acceso: 31 Octubre 2021].

[6] D. C. L. Mera, «reestructuracion de la infraestructura de red LAN basada en normas de cableado estructurado, y la aplicacion de politicas de seguridad para el control de acceso mediante un servicio proxy en la Unidad Educativa HispanoAmericano,» Septiembre 2018. [En línea]. Available: https://dspace.ups.edu.ec/handle/123456789/17336. [Último acceso: 31 Octubre 2021].

[7] Seftic, «Seftic informatica,» 2021. [En línea]. Available: https://seftic.com/vlans-y-segmentacion-de-redes/. [Último acceso: 04 Octubre 2021].

[8] A. N. CASTILLO PORTURAS, «IMPLEMENTACIÓN DE REDES VIRTUALES UTILIZANDO VLAN PARA REDUCIR EL TAMAÑO DEL DOMINIO DE DIFUSIÓNDE LA RED EN EL INABIF,» Lima, 2015.

[9] McAfee, «McAfee,» 16 Junio 2021. [En línea]. Available: https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-es-un-proxy/. [Último acceso: 06 Junio 2022].

[10] HP, «HP,» 30 Agosto 2021. [En línea]. Available: https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona. [Último acceso: 06 Junio 2022].

[11] pfSense, «pfSense,» 2022. [En línea]. Available: https://www.pfsense.org/about-pfsense/. [Último acceso: 06 Junio 2022].

[12] Genos, «Genos,» 2021. [En línea]. Available: https://genos.es/proxmox-ve/. [Último acceso: 10 Julio 2022].

[13] squid-cache, «schid-cache,» 2013. [En línea]. Available: http://www.squid-cache.org/. [Último acceso: 04 octubre 2021].

[14] Ubuntu, «Ubuntu,» 2020. [En línea]. Available: https://ubuntu.com/server/docs/proxy-servers-squid. [Último acceso: 06 Junio 2022].

[15] EcuRed, «EcuRed,» 2019. [En línea]. Available: https://www.ecured.cu/SquidGuard. [Último acceso: 06 Junio 2022].

[16] CISCO, «CISCO,» 13 diciembre 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb3050-configure-ipv6-based-access-control-list-acl-and-access-cont.html. [Último acceso: 04 octubre 2021].

[17] Cisco, «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-to-choose-small-business-routers. [Último acceso: 06 Junio 2022].

[18] Cisco, «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html. [Último acceso: 06 Junio 2022].

[19] «Cad & Lan,» 2020. [En línea]. Available: https://www.cadlan.com/noticias/todo-lo-que-debes-saber-sobre-el-cableado-estructurado/. [Último acceso: 06 Junio 2022].

[20] F. d. S. y. Telecomunicaciones, Resolución RCF-FST-SO-09 No. 03-2021 Lineas de Investigacion Facsistel, Santa Elena: UPSE, 2021.

[21] i. Learnign, «inGenio Learnign,» inGenio Learnign, Junio 2018. [En línea]. Available: https://ingenio.edu.pe/blog/administracion-de-redes-y-comunicaciones-todo-lo-que-necesitas-saber/. [Último acceso: 10 Noviembre 2021].

[22] P. D. A. GAMEZ, «METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES FUNDAMENTADOS EN ITIL 4, PARA EMPRESAS DE SERVICIO,» Bogota, 2012.

[23] M. d. telecomunicaciones, «Ministerio de Telecomunicaciones,» 2017. [En línea]. Available: https://www.telecomunicaciones.gob.ec/1-200-unidades-educativas-contaran-internet-la-cnt/. [Último acceso: 10 Noviembre 2021].

[24] S. n. d. planificacion, «Plan de Creacion de Oportunidades 2021-2025,» Quito, 2021.

[25] P. A. Guadarrama, «Clasificacion de redes de telecomunicaciones alambricas e inalmabricas,» Pachuca, 2005.

[26] M. D. F. V. GAMBOA, «FUNDAMENTOS DE TELECOMUNICACIONES,» Merida.

[27] L. L. Nelly, D. G. Ayabaca y C. B. Flores, «Eficacia y eficiencia de la seguridad de lasredes LAN. CantónPasaje,» Babahoyo, 2021.

[28] E. Networks, «Eni Networks,» 24 Julio 2019. [En línea]. Available: https://www.eninetworks.com/blog-que-es-una-red-lan/. [Último acceso: 04 Junio 2022].

[29] A. Freda, «AVG,» 11 Marzo 2021. [En línea]. Available: https://www.avg.com/es/signal/ipv4-vs-ipv6#topic-1. [Último acceso: 18 Junio 2022].

[30] Vmware, «Vmware,» 2022. [En línea]. Available: https://www.vmware.com/es/topics/glossary/content/network-segmentation.html. [Último acceso: 30 Mayo 2022].

[31] Oracle, «Oracle,» 2013. [En línea]. Available: https://docs.oracle.com/cd/E37929_01/html/E36606/fpjve.html. [Último acceso: 30 Mayo 2022].

[32] F. G. ESPINOZA, «PROYECTO DE REDISEÑO DE LA RED DE COMPUTADORAS DEL HOSPITAL III JOSE CAYETANO HEREDIA UTILIZANDO VLANS,» Piura, 2018.

[33] CCNA, «reuter,» 2020. [En línea]. Available: https://www.reuter.com.ar/CCNA/CCNA2/mod3_ccna2/. [Último acceso: 30 Mayo 2022].

[34] «Institut Sa Palomera,» 23 Julio 2020. [En línea]. Available: https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.1.2.1/3.1.2.1.html. [Último acceso: 04 Junio 2022].

[35] E. Limones, «OpenWebinars,» 24 Septiembre 2021. [En línea]. Available: https://openwebinars.net/blog/enrutamiento-estatico-vs-dinamico/. [Último acceso: 30 Mayo 2020].

[36] U. d. Alcala, «Protocolos de enrutamiento dinámico RIP y OSPF,» Madrir, 2017.

[37] G. T. M. PRIETO, «DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN,» Boyacá, 2018.

[38] J. C. Y. CAZAR, «EVALUACIÓN DEL PROTOCOLO 802.1Q EN LA IMPLEMENTACIÓN DE VLANS EN ENTORNOS WIRELESS MEDIANTE LA APLICACIÓN DE SOFTWARE LIBRE,» Riobamba, 2016.

[39] D. G. IONOS, «Ionos,» 16 Noviembre 2021. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-proxy/. [Último acceso: 30 Mayo 2022].

[40] Squid, «Squid,» 05 Mayo 2013. [En línea]. Available: http://www.squid-cache.org/. [Último acceso: 31 Mayo 2022].

[41] D. G. IONOS, «Digital Guide IONOS,» 25 Septiembre 2020. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/configuracion/squid-el-servidor-proxy-cache-de-codigo-abierto/. [Último acceso: 18 Junio 2022].

[42] L. Console, «Linux Console,» 2019. [En línea]. Available: https://es.linux-console.net/?p=958. [Último acceso: 15 Junio 2022].

[43] S. S. Dash, S. Das y B. K. Panigrahi, INtelligent Computing and Applications, Singapur: Springer, 2019.

[44] J. J. M. Valencia, A. P. Valencia y J. C. A. Bedoya, «Implementación de un sistema de seguridad perimetral informático usando vpn, firewall e ids,» rionegro, Antioquia, 2020.

[45] C. TI, «Consultoria TI,» 2022. [En línea]. Available: https://consultoriati.digitecnia.com/tipos-de-firewall/pfsense-es-firewall-y-ruteador/. [Último acceso: 04 Junio 2022].

[46] T. Club, «Tech Club Tajamar,» 7 Marzo 2019. [En línea]. Available: https://techclub.tajamar.es/listas-de-control-de-acceso-acl/. [Último acceso: 2022 Mayo 2022].

[47] D. Mozilla, «Developer Mozilla,» 08 Diciembre 2020. [En línea]. Available: https://developer.mozilla.org/es/docs/Web/HTTP. [Último acceso: 18 Junio 2022].

[48] A. C. Martínez, «Diseño e implementación de un middleware CoAP-MQTT-HTTP para la mejora de la interoperabilidad de los protocolos de aplicación en redes IoT,» Zaragoza, 2020.

[49] J. Donnelly, «Massive,» 18 febrero 2022. [En línea]. Available: https://massive.io/es/transferencia-de-archivos/what-is-transmission-control-protocol-tcp/. [Último acceso: 18 Junio 2022].

[50] G. H. Hernández, Protocolo de Control de Transferencia (TCP), Hidalgo: Univerdiad Autonoma del Estado de Hidalgo, 2014.

[51] I. J. F. E. Miranda, «POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE ELAÑO 2010,» Ambato, 2011.

[52] G. ATICO34, «Grupo ATICO34,» 21 Agosto 2021. [En línea]. Available: https://protecciondatos-lopd.com/empresas/protocolos-seguridad-informatica/. [Último acceso: 18 Junio 2022].

[53] M. R. HOSPINA GONZALES, «DISEÑO E IMPLEMENTACIÓN DE VLANS PARA MEJORAR LA EFICIENCIA EN LA TRANSMISIÓN DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE HUANCAYO,» Huancato, 2017.

[54] E. C. Reséndiz, «Instalación y Configuración de un switch con vlans para la mejora de rendimiento del ancho de banda de la red,» Veracruz, 2018.

[55] L. O. Yosselin, «Reestructucacion y optimizacion de los servicios de la red de datos cableada e inalambrica mediante la implmentacion de un servidor proxy en linuz en la unidad educativa "America del sur",» Guayaquil, 2017.

[56] J. SENTENO, «PROPUESTA DE INTERCEPTOR PROXY COMO MODELO DE ACCESO SEGURO A UN ENTORNO WEB, PARA EL CONSORCIO INFRAESTRUCTURA EDUCATIVA 2016,» Bogota, 2019.

[57] N. Abatedaga, Epistemologia y Metodologia para planificar consensos, Cordoba: Editorial Brujas, 2008.

[58] D. P. B. L. Dr. Carlos Fernández Collado, METODOLOGIA DE LA INVESTIGACION, McGRAW - HILL INTERAMERICANA DE MÉXICO, S.A., 1991.

[59] P. F. E. GUERRA, «PROPUESTA DE METODOLOGÍA PARA LA IMPLEMENTACIÓN DE PROYECTOS DE REDES – CASO DE ESTUDIO INSTITUCIÓN FINANCIERA LOCAL,» Quito, 2016.

[60] M. A. O. D. L. CRUZ, «DISEÑO DE UN CABLEADO ESTRUCTURADO BAJO LA METODOLOGÍA TOP DOWN NETWORK DESIGN APLICANDO POLÍTICAS DE SEGURIDAD PARA EL COLEGIO EL PINAR DE LA CIUDAD DE HUARAZ 2017.,» Huaraz, 2017.

[61] D. d. T. d. l. I. y. C. d. l. U. E. P. d. S. Elena, «MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA,» Santa Elena, 2018.

[62] CCNA, «redesccna2cisco,» 21 Julio 2012. [En línea]. Available: https://www.sites.google.com/site/redesccna2cisco/enrutamiento-estatico. [Último acceso: 19 Enero 2022].

[63] CISCO, «CISCO,» 25 agosto 2006. [En línea]. Available: cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html. [Último acceso: 19 enero 2022].

[64] J. A. P. GUTIÉRREZ, «PROPUESTA DE OPTIMIZACION DE LA INFRASTRUCTURA DE TELECOMUNICACIONES CORPORATIVA BASADA EN LA METODOLOGIA TOP-DOWN DE CISCO,» Bogota, 2017.

La Libertad, 12 de octubre de 2022

CERTIFICADO ANTIPLAGIO
003-TUTOR IACS-2022

En calidad de tutor del trabajo de titulación denominado **"PROPUESTA DE REDISEÑO Y SIMULACIÓN DE LA INFRAESTRUCTURA DE RED DE LA UNIDAD EDUCATIVA LA LIBERTAD BASADO EN VLANS Y POLÍTICAS DE SEGURIDAD DE ACCESO."**, elaborado por el estudiante, **ASCENCIO CAICHE ANTHONY BRYAN**, egresado de la Carrera de Tecnologías de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniera en Tecnologías de la Información, me permito declarar que una vez analizado en el sistema antiplagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 1% de la valoración permitida, por consiguiente se procede a emitir el presente informe.

Ouriginal

Document Information

Analyzed document	Anthony_Ascencio_Componente_Teorico.docx (D146165278)
Submitted	10/11/2022 11:06:00 PM
Submitted by	
Submitter email	anthony.ascenciocaiche@upse.edu.ec
Similarity	1%
Analysis address	icoronel.upse@analysis.urkund.com

Sources included in the report

SA	**Tesis V1 si.docx** Document Tesis V1 si.docx (D40821231)
SA	**Tesis Pregrado [Coveña Arroyo].docx** Document Tesis Pregrado [Coveña Arroyo].docx (D14245726)
SA	**ASIX-CIBER_M14_Memoria_del_Proyecto_Alfonso_Salido_Cruz.pdf** Document ASIX-CIBER_M14_Memoria_del_Proyecto_Alfonso_Salido_Cruz.pdf (D134501254)
SA	**Tesis.docx** Document Tesis.docx (D12044669)

Atentamente,

Ing. Coronel Suárez Iván Alberto, MSIA.
C.I.:0917255978
DOCENTE TUTOR