Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Kevin Estuardo Esquivel Cuy
Asesorado por el Ing. Edgar René Ornelis Hoil

Guatemala, agosto de 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

KEVIN ESTUARDO ESQUIVEL CUY
ASESORADO POR EL ING. EDGAR RENÉ ORNELIS HOIL

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Vladimir Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Carlos Alfredo Azurdia Morales
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera de Medinilla
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha julio de 2019.

Kevin Estuardo Esquivel Cuy

Guatemala, 11 de mayo de 2020

Ingeniero
Ing. Oscar Argueta Hernández
Director de la Unidad de EPS

Estimado Ingeniero Argueta:

Deseándole éxitos en sus labores diarias, hago de su conocimiento que el estudiante **Kevin Estuardo Esquivel Cuy** quien se identifica con número de registro estudiantil **201403935** y documento personal de identificación **2564 61546 0101** a quien estoy asesorando en su Ejercicio Profesional Supervisado (EPS), ha completado el 100% del proyecto de ejercicio profesional supervisado (EPS) e informe final titulado: **"IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACTULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"**.

Atentamente,

Edgar René Ornelis Hoil
Ingeniero en Ciencias y Sistemas
Colegiado No 4830

Ing. Edgar René Ornelis Hoil
Asesor de EPS
Escuela de Ingeniería en Ciencias y Sistemas

Estos documentos digitales serán reemplazados en el momento de reanudar actividades presenciales.

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA
UNIDAD DE EPS

Guatemala, 19 de mayo de 2020.
Ref.EPS.DOC

Ing. Oscar Argueta Hernández
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Argueta Hernández:

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (EPS) del estudiante universitario de la Carrera de Ingeniería en Ciencias y Sistemas, **Kevin Estuardo Esquivel Cuy, Registro Académico 201403935 y CUI 2564 61546 0101** procedí a revisar el informe final, cuyo título es **IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**.

En tal virtud, **LO DOY POR APROBADO,** solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
Inga. Floriza Ávila Pesquera de Medinilla
ASESORA - SUPERVISORA DE EPS
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Inga. Floriza Felipa Ávila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas

FFAPdM/RA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

UNIDAD DE EPS

Guatemala, 19 de mayo de 2020
REF.EPS. D.227.05.2020

Ing. Carlos Gustavo Alonzo
Director Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Alonzo:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**, que fue desarrollado por el estudiante universitario **Kevin Estuardo Esquivel Cuy, CUI 2564 61546 0101 y Registro Académico 201403935,** quien fue debidamente asesorado por el Ing. Edgar René Ornelis Hoil, y supervisado por la Inga. Floriza Felipa Ávila Pesquera de Medinilla,

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación por parte de la supervisora, como director apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Ing. Oscar Argueta Hernández
Director Unidad de EPS

OAH

Nota: esta carta es una copia de la original, la cual se sustituirá por la original al momento de que se normalicen las actividades en la Universidad.

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 22 de mayo de 2020

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **KEVIN ESTUARDO ESQUIVEL CUY** carné **201403935** y **CUI 2564 61546 0101,** titulado: **"IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACUTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA",*** *realizado por el estudiante, KEVIN ESTUARDO ESQUIVEL CUY aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Digitally signed by Carlos Gustavo Alonzo
DN: 2.5.4.13=Profesional Titulado, c=GT, l=Guatemala / Guatemala, street=Via 5 3-65 zona 4 Ed. El Angel 5to nivel of 52, 2.5.4.20=22347420, ou=NA, o=NA, title=Ingeniero en Ciencias y Sistemas Colegiado. 6358, serialNumber=2278 03167 0101, 2.5.4.45=29020980, 2.5.4.27=06/03/79, emailAddress=calonzo@infoutilitygt.com, cn=Carlos Gustavo Alonzo
Date: 2020.08.30 22:36:52 -06'00'

Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 28 de agosto de 2020

Decanato
Facultad de Ingeniería
24189101- 24189102

DTG. 198.2020.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **IMPLEMENTACIÓN DE PORTAL CAUTIVO PARA CONTROL Y ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE RED DE LOS LABORATORIOS DE LA ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario: **Kevin Estuardo Esquivel Cuy,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Anabela Cordova Estrada
Decana

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Guatemala, agosto de 2020

AACE/asga

ACTO QUE DEDICO A:

Dios	Por ser el pilar de mi vida y mi principal fuente de aliento cuando nadie más me apoyo.
Mis padres	Enemias Esquivel y Gloria Cuy, porque siempre mostraron su apoyo, amor y paciencia aún en los momentos más difíciles.
Mi madrina	Magnolia Guzmán. Por ser la ayuda incondicional y más grande que tuve durante mi carrera.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser mi *alma máter*, casa y una parte importante en mi formación profesional.
Facultad de Ingeniería	Por ser mi segundo hogar y la fuente de mi conocimiento, donde forjé mi carácter y aprendí a valorar las oportunidades.
Mis amigos de la Facultad	Por su apoyo y aprendizaje mutuo durante nuestro proceso de formación que sin su apoyo no hubiese sido posible.
Mi asesor de EPS	Ing. Edgar René Ornelis Hoil, gracias por su apoyo, recomendaciones y brindarme su tiempo durante la realización de este proyecto.
Los ingenieros	William Estuardo Escobar Argueta y Edgar Sabán, gracias por su apoyo y consejos durante mi formación profesional y al inicio de mi carrera profesional.
Licenciada	Anselma del Rosario Jáuregui Contreras, gracias por su apoyo, consejos e incondicional apoyo que impulsó mi carrera.
Dulce López	Por su apoyo, amor y cariño incondicional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
kbit/s	Kilobit por segundo
Mb/s	Megabit por segundo
VLAN	Red de área local virtual
seg	Segundos

GLOSARIO

Base de datos Conjunto de datos que comparten relaciones entre sí para ser interpretados como contenedores de información que puede o no ser utilizada posteriormente pero que es importante almacenar.

Conmutador Dispositivo de red que permite la difusión, interconexión y comunicación punto a punto de dos o más dispositivos dentro de una red.

DBMS Acrónimo en inglés: Data Base Management Systen. Sistema gestor de base de datos conformado por un conjunto de software especializados encargado en la creación y el manejo de los componentes necesarios para realizar operaciones y accesos a las bases de datos, objetivamente su función principal es la intermediación del usuario y los datos.

DMZ Diseño de red perimetral enfocado en el aislamiento de una red interna llamada LAN y una red externa conocida como WAN que generalmente es un proveedor de internet.

Enrutador Dispositivo de red para difusión, interconexión y comunicación de dispositivos dentro de una red.

Firewall	Servidor de corta fuegos, encargado del filtrado de paquetes dentro de una red local y una externa para administración y gestión del tráfico de red.
IPTables	Utilidad de línea de órdenes para configurar el cortafuegos del kernel de Linux.
PfSense	Software de código abierto con funcionalidades de cortafuegos o enrutador para la administración de infraestructuras de red.
RADIUS	Acrónimo del inglés: *Remote Authentication Dial-In User Service.* Protocolo de autenticación y autorización para aplicaciones de acceso a la red IP.

RESUMEN

La Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería provee diversos servicios y recursos a la población estudiantil entre los cuales uno de los más importantes son áreas de trabajo didáctico con acceso a servicio de internet inalámbrico gratuito, surge la necesidad de administrar dichos recursos y el acceso a los usuarios.

El proyecto consiste en la implementación (diseño, desarrollo, configuración e instalación) de un portal cautivo que proporcione un medio de administración y control del recurso de internet inalámbrico en los laboratorios de la Escuela de Ciencias y Sistemas 014, 013, India 1, India 2 e India 3.

Se desarrolla una aplicación web dividida en dos módulos: módulo de administración para los recursos de internet inalámbrico y el portal cautivo, el cual consta de dos sitios web locales existentes en los servidores de los laboratorios, uno de registro y otro de autenticación por clave genérica; el módulo de administración consta de reportes, administración de políticas y gestión de usuarios.

La parte final consiste en la elaboración de actividades de despliegue de la aplicación e incorporación a la infraestructura de red local, capacitación y difusión del portal cautivo y su forma de uso.

OBJETIVOS

General

Implementar un portal cautivo para la administración y control de la red de internet inalámbrico para los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas de la Universidad de San Carlos de Guatemala.

Específicos

1. Permitir a la coordinación de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas, controlar y administrar el acceso de manera automatizada a los recursos de red de internet inalámbrico que se brindan a las personas que asisten a los laboratorios.

2. Aplicar protocolo y servidor de autenticación como mecanismo de seguridad y accesos a la red de internet inalámbrica de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas.

3. Instalar y configurar servidores DNS y DHCP como administradores del tráfico y recursos de red de internet de los laboratorios de la Escuela de Ciencias y Sistemas.

4. Obtener, almacenar y consultar información sobre el recurso y uso del internet inalámbrico de los laboratorios de la Escuela de Ciencias y Sistemas.

5. Filtrar el contenido disponible para los usuarios de la red de internet inalámbrico dentro de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas.

INTRODUCCIÓN

Los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas son instalaciones de acceso público, enfocada primeramente al uso académico, a las cuales los estudiantes de cualquier carrera de la Facultad de Ingeniería y Universidad de San Carlos puede tener acceso y hacer uso de ellas. Como parte de los servicios que brindan los laboratorios a la población estudiantil se cuenta con mobiliario tales como sillas, mesas, además de aire acondicionado, internet inalámbrico, electricidad y proyectores.

La coordinación de los laboratorios y el personal a cargo de la administración de los recursos que existen a disposición en las instalaciones necesitan la implementación de una herramienta informática y de infraestructura de red que les permita oxigenar, administrar y controlar los recursos de internet inalámbrico que se brindan gratuitamente a fin de garantizar el buen uso de dicho recurso. Con el apoyo de las tecnologías y la infraestructura de red actual de los laboratorios se busca no solo permitir obtener un registro de los usuarios de la red sino también proveerles de una mejor calidad en el servicio.

Para satisfacer las necesidades de la coordinación de los laboratorios se creará una aplicación web, dividida en dos módulos. El módulo de administración de recursos que se encargará de la gestión de usuarios administrativos y de la red, así como de la gestión de políticas a aplicar al tráfico generado por los usuarios. El módulo de portal cautivo será el encargado de autenticar a los usuarios por medio de clave genérica, y en su defecto a registrarlos por medio de la redirección del tráfico de conexión por medio de servidores DNS y DHCP

que trabajarán juntamente con el servidor de autenticación, autorización y contabilización RADIUS.

El proyecto oxigenará la red actual de internet inalámbrico, recolectará información de contacto y no privada de los usuarios de la red y principalmente brindará las herramientas necesarias para evitar el mal uso del recurso de internet inalámbrico y evitar las conexiones innecesarias de dispositivos que no estén en uso o dejen sin direcciones IP a los distintos dispositivos enrutadores situados en los laboratorios.

1. FASE DE INVESTIGACIÓN

1.1. Antecedentes de la empresa

La Escuela de Ingeniería en Ciencias y Sistemas es una de las 13 unidades académicas de la Facultad de Ingeniería, encargada de la formación superior en las áreas de ciencias de la computación y sistemas de la información. Además, es la encargada de coordinar e implementar programas de formación, investigación y extensión que promuevan su especialidad científica.

1.1.1. Reseña histórica

La carrera de Ingeniería en Ciencias y Sistemas fue creada en el año de 1970 como una Escuela de formación superior de la Facultad de Ingeniería, a fin de lograr con los objetivos y necesidades de educación a nivel superior que la Universidad de San Carlos busca cumplir como única universidad pública en Guatemala.

Actualmente la Escuela de Ingeniería en Ciencias y Sistemas se encuentra ubicada en el nivel 0 del edificio T3 y posee cinco laboratorios distribuidos en los niveles cero, cuarto y quinto nivel del edificio T3 que están ubicados en los salones 013, 014, India 1, India 2 e India 3. Los laboratorios se encuentran habilitados desde el año 2015 y actualmente son utilizados para llevar cabo las actividades académicas de la carrera de Ingeniería en Ciencias y Sistemas, siendo principalmente capacitaciones, conferencias, clases magistrales y de laboratorio en el área referente a la especialidad de la Escuela y los cursos del pensum de estudios. A las instalaciones además se permite el libre y gratuito

acceso a toda la población estudiantil universitaria para el uso libre de las instalaciones en donde se les provee principalmente de espacios, mobiliario, electricidad e internet inalámbrico.

En la actualidad los laboratorios de la Escuela de Ciencias y Sistemas no poseen medios de control y administración del recurso de internet y tampoco en el área de infraestructura de red y el servicio de internet inalámbrico no es la excepción. Debido a la falta de dichos medios surgió la necesidad de cambiar la forma en que el servicio de internet y red se provee en los espacios públicos de los laboratorios siendo además totalmente necesario porque al no existir estos medios los recursos recurrentemente son mal utilizados por los usuarios o se experimenta saturación en la red, a esto se añaden problemas como que no se tiene información cuantitativa del uso de los recursos y tampoco existen medios para obtener información de esto; razones principales por las que la implementación de un portal cautivo y un módulo administrativo son necesarios a fin de poder evitar las conexiones innecesarias de dispositivos, almacenar información de la red, generar reportes y permitir definir políticas sobre el contenido para los usuarios al utilizar el recurso de internet inalámbrico gratuito de los laboratorios. La implementación de un portal cautivo es sumamente necesaria en espacios públicos siendo ejemplo de estos hoteles, centros comerciales, restaurantes, entre otros.

Debido a que los recursos que pone a disposición los laboratorios de la Escuela de Ciencias y Sistemas son de acceso gratuito y totalmente libre para la población estudiantil universitaria, se busca dar la oportunidad de dar una experiencia de usuario agradable en la cual es prioritario alcanzar el mayor número de beneficiados. Con este enfoque la implementación del portal cautivo para la administración y control de los recursos es el mejor medio disponible para brindar recursos de internet en espacios públicos de forma eficiente como en

centros comerciales y hoteles, los cuales son ejemplos claros que el uso de un portal cautivo en puntos de acceso de internet cableado o inalámbrico con tantos usuarios es totalmente necesario para evitar el uso indebido de los recursos y alcanzar la mayor disponibilidad del servicio para abarcar la mayor cantidad de usuarios posibles.

1.1.2. Misión

"Desarrollar en el estudiante las competencias que garantizan el éxito en la construcción del conocimiento a través de los diferentes estilos de aprendizaje y fomentar la investigación permanente para permitir una mejor calidad de vida para la comunidad. Teniendo en cuenta las opciones del mercado actual en el país (logística, administración, tecnología de la información, finanzas, contabilidad, comercial, entre otros), y también el mercado internacional, hace hoy en día una alta demanda y competitividad global."[1]

1.1.3. Visión

"El estudiante de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala será reconocido como profesional superior, sobre la base de los conocimientos incorporados en el plan de estudios de estudios para capacitar a los estudiantes de manera integral, dándoles las herramientas adecuadas para su desarrollo profesional."[2]

---

[1] Escuela de Ingeniería en Ciencias y Sistemas. *Misión y visión*. https://dtt-ecys.org/about_us.
[2] Ibíd.

1.1.4. Servicios que realiza

La Escuela de Ingeniería en Ciencias y Sistemas es una institución que prepara y titula profesionales en las áreas de las ciencias de la computación y sistemas. Además, brinda las instalaciones de sus laboratorios para el desarrollo de las actividades académicas de alumnos, auxiliares y catedráticos de la Escuela entre las cuales principalmente se encuentran: conferencias, clase magistral de los cursos, laboratorios y capacitaciones.

1.2. Descripción de las necesidades

Los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas poseen actualmente cinco laboratorios diseñados para que los usuarios, en su mayoría estudiantes de la carrera de Ingeniería de sus distintas unidades académicas, puedan realizar sus actividades académicas y de fomentación de su especialidad científica y técnica. Esta coordinación adjunta de la Escuela requiere el desarrollo de una solución de infraestructura y de software que les permita administrar y controlar los recursos de internet inalámbrico que se proveen a la población estudiantil de la Facultad de Ingeniería de forma gratuita en las instalaciones de los laboratorios.

1.2.1. Necesidades identificadas

La coordinación de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas cuenta actualmente con toda la infraestructura de red para prestar el servicio de internet inalámbrico en las instalaciones, pero no posee una plataforma o aplicación de software que permita la administración y control de dicho recurso ni tampoco el diseño de topología y configuración de servidores necesarios para la implementación de dicho software. Adicionalmente no existen

registros o datos que permitan conocer el nivel de uso de dichos recursos ni tampoco hay medios que permitan obtener información de los usuarios.

Los laboratorios cuentan con cableado estructurado, servidores y dispositivos enrutamiento y conmutación, que proveen señal de internet inalámbrico y cableado dentro de las instalaciones por medio de puntos de acceso y puertos *ethernet*. De esta misma manera los laboratorios cuentan con todo lo necesario para la implementación de la solución de software e infraestructura antes descrita.

El portal cautivo captará información básica y no sensible de los usuarios de la red interna que se les solicite al momento del registro de estos, además de la implementación de un método de autenticación por clave genérica basado en el número de carné de los estudiantes y el sistema de administración de recursos almacenará la información de los usuarios y permitirá la visualización de reportes.

1.3. Priorización de las necesidades

En la implementación del portal cautivo se priorizará el proceso de autenticación de usuarios y prevención de conexiones innecesarias para la oxigenación de los dispositivos de puntos de acceso inalámbrico, y la utilización de los servidores e infraestructura existente a la solución de software e infraestructura presentada evitando la modificación de esta.

Se dará una prioridad media a la generación de reportes y monitorización de los usuarios y el tráfico generado por los usuarios conectados, así como la correcta aplicación de los procesos definidos para la administración de la plataforma web y los recursos existentes para cumplir y no modificar de manera indebida el diseño de infraestructura actual de los laboratorios.

Por último, se dará una prioridad baja a la definición y aplicación de políticas al tráfico generado por la conexión y consumo de usuarios de los laboratorios, de la misma forma se dará una baja prioridad a la gestión de usuarios que se refiera a accesos y conexión de usuarios a la red. Cabe resaltar que únicamente se considerarán aquellas políticas que sean compatibles con la infraestructura de red y usuarios.

2. FASE TÉCNICO PROFESIONAL

2.1. Descripción del proyecto

El proyecto consiste en la implementación (diseño, codificación, instalación y configuración) de un portal cautivo y un sistema adjunto para la administración de la infraestructura de red que provee internet inalámbrico a las instalaciones de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas, el proyecto considera también a la configuración y diseño de la infraestructura de red que de soporte al proyecto.

El portal cautivo será utilizado como medio de autenticación de usuarios para acceso a la red, permitiendo o denegando de esta manera la conexión de los usuarios a la red ya sea por los puntos de acceso inalámbricos o puertos *ethernet* para su conexión por cable que se encuentran en los laboratorios de la Escuela de Ciencias y Sistemas.

El sistema adjunto para la administración será una aplicación web utilizada para la generación de reportes de consumos, usuarios y sesiones, así como para llevar a cabo la gestión de usuarios administrativos o de red y de políticas para los recursos de internet inalámbrico.

Se creará una aplicación web a la cual será redireccionado todo usuario de la red que se conecte al punto de acceso inalámbrico o cableado, en donde inicialmente se autenticaran y si en caso no existe registro se registraran por medio de una interfaz de usuario alternativa. Por medio de la autenticación se facilitará el acceso a la red inalámbrica y al recurso de internet por medio de un

único registro de usuarios y la implementación de una clave genérica la cual será el número de carné universitario. Transversal al portal cautivo se implementará un servidor de RADIUS que se encargará de la autenticación, autorización y contabilización de paquetes de los usuarios y a través de la información obtenida tanto la coordinación de los laboratorios como la escuela podrán justificar y comprobar la cantidad de estudiantes y población que utiliza las instalaciones y los recursos.

El principal enfoque del proyecto es brindar los mecanismos para la administración de los recursos de internet de las instalaciones a fin de dar un buen servicio y de mejorar la capacidad de acceso a los usuarios a dicho recurso.

Como parte inicial del proyecto se realizará el diseño de la solución, el modelo de datos, la arquitectura del sistema y el diseño de la topología de red para establecer la forma inicial en la que se implementará cada uno de los componentes finales de la solución. En la segunda parte del proceso de implementación, se realizará el desarrollo y codificación de la aplicación web que funcionará como portal cautivo, la interfaz de registro, el sistema de administración de recursos y por último la instalación y configuración de las distintas herramientas y dispositivos de red involucrados en la solución, topología de red, y la integración de la aplicación con la infraestructura actual de red de los laboratorios.

Como tercera y última parte del proceso de implementación se integrarán los laboratorios restantes a la solución, añadido a esto se realizará una serie de capacitaciones y elaboración de medios de publicidad para dar a conocer la nueva solución a los usuarios de los laboratorios.

2.2. Investigación preliminar para la solución del proyecto

Inicialmente se contó con información acerca del estado de los laboratorios, tomando en cuenta todos los aspectos técnicos que tienen que ver con el servicio de internet inalámbrico y la topología de red existente a fin de establecer los recursos y alcances de la solución, se contó para esta tarea con el apoyo de la coordinación de los laboratorios.

2.2.1. Análisis FODA del proyecto

Por medio de un análisis interno y externo de fortalezas, oportunidades, debilidades y amenazas se definieron los riesgos del proyecto, la especificación de los alcances y los riesgos que la elaboración de este conllevaba.

2.2.1.1. Análisis Interno

El análisis interno del servicio prestado se realizó por medio de entrevistas a los usuarios y a la coordinación de los laboratorios, añadido a esto se realizó una inspección técnica para poder conocer el estado de la infraestructura y los recursos disponibles para la elaboración del proyecto. Como resultado del análisis interno se definen las fortalezas y debilidades del servicio.

2.2.1.1.1. Fortalezas

- Las instalaciones de los laboratorios cuentan con los dispositivos e infraestructura de red de la mejor calidad posible para brindar el servicio de internet inalámbrico y realizar la integración del portal cautivo.
- La coordinación de los laboratorios cuenta con las credenciales de acceso a los dispositivos que serán utilizados para la elaboración del proyecto.

- La infraestructura de red actual cuenta con una configuración capaz de integrar, soportar la implementación del proyecto, y ser soporte de las herramientas y tecnologías seleccionadas para el proyecto.
- El coordinador de los laboratorios y también responsable del equipo está directamente involucrado dentro del proyecto.
- El sistema y solución de infraestructura es novedoso porque actualmente no se cuenta con herramientas que ayuden a la administración de los recursos y usuarios.
- La coordinación cuenta con el personal necesario para la administración de los recursos y usuarios que propone el proyecto como solución.

2.2.1.1.2. Debilidades

- El proyecto tendrá una carga de trabajo y flujo de información constante e intensivo por lo que la aplicación necesitará de monitorización constante para que cumpla con su objetivo.
- Se necesita la implementación de contenedores y sistemas operativos en un entorno de virtualización nuevo y de uso específico que no tienen integración física con la infraestructura de red.
- El correcto funcionamiento de la aplicación y configuración de la infraestructura de red es completamente dependiente del equipo físico.

2.2.1.2. Análisis externo

Se realizó un análisis externo por medio de la observación y testeo de los servicios de internet, equipo físico y de la infraestructura de red, para definir las oportunidades y amenazas del proyecto.

2.2.1.2.1. Oportunidades

- Las instalaciones de los laboratorios y el servicio de internet inalámbrico gratuito día con día van adquiriendo mayor alcance y difusión dentro de la comunidad estudiantil.
- El proyecto beneficiará a los usuarios al mejorar la calidad del servicio de internet y así mismo permitirá que más usuarios puedan hacer uso del servicio al mismo tiempo.
- Mejorar el servicio que actualmente brinda la Escuela de Ingeniería en Ciencias y Sistemas a la población estudiantil y mejorar la eficiencia en el uso de los recursos.

2.2.1.2.2. Amenazas

- El proyecto depende directamente del proveedor del servicio de internet y que el administrador mantenga en observación la infraestructura de red para que esta funcione de manera correcta.
- La infraestructura de red y el portal cautivo deberá evitar la modificación de las configuraciones de dispositivos enrutadores y conmutadores, servidores, red cableada y software de firewall para evitar fallas en el servicio.
- Se requiere que todos los usuarios conozcan o tenga material acerca de cómo utilizar la herramienta y tener acceso fácilmente por medio del portal cautivo.

2.2.2. Análisis y diseño de la infraestructura de red

Este análisis consiste en el reconocimiento de los componentes de hardware y software que serán utilizados para la implementación el alojamiento y ejecución de la solución. La información fue obtenida del hardware se realizó mediante la inspección de cada componente en su estado físico y en el caso del software fue documentada durante la instalación de prueba de cada uno.

2.2.2.1. Hardware de la infraestructura de red

A continuación, se detalla el hardware de infraestructura de red que existe actualmente en los laboratorios y que es utilizado para la elaboración del proyecto.

2.2.2.2. Recursos de hardware para la infraestructura de red utilizado en la elaboración del proyecto

El recurso de hardware utilizado para la elaboración del proyecto fue previamente adquirido por la coordinación de los laboratorios y trabajado por estudiantes que elaboraron su ejercicio profesional supervisado con anterioridad.

2.2.2.3. Cableado estructurado

Dentro de las instalaciones de los laboratorios se cuenta 36 puntos de cableado con conexión *ethernet* con conectores RJ45, situados en distintos puntos dentro de las instalaciones.

2.2.2.4. Dispositivos de enrutamiento, conmutación y puntos de acceso inalámbrico

A continuación, se presenta el listado de los dispositivos de enrutamiento, conmutación y puntos de acceso utilizados para la difusión del servicio y elaboración del proyecto.

2.2.2.4.1. Dispositivos de enrutamiento

Para llevar a cabo la difusión del tráfico de red se utilizaron dos dispositivos de enrutamiento marca Mikrotik capa 3 administrables, modelo CR5226-24G-25+RM. La función principal de estos dispositivos de enrutamiento son la de capa de acceso a la infraestructura de red interna para los laboratorios.

2.2.2.4.2. Dispositivos de conmutación

Para llevar a cabo la conmutación del tráfico de red, fue utilizado un *switch* marca Juniper capa 3 administrables, modelo EX2200. La función principal del dispositivo es ser la capa de distribución de la infraestructura de red para los laboratorios y dispositivos, además por medio de este y su puerto número 10 también se distribuye el servicio de portal cautivo etiquetado con la VLAN 88 hacía los puertos de los enrutadores Mikrotik, puntos de acceso y la capa de núcleo para su distribución e integración con los laboratorios de la India 1, 2 y 3.

2.2.2.4.3. Puntos de acceso inalámbrico

La difusión del servicio y puntos de acceso para dispositivos que posean tarjeta de red inalámbrica son de marca Ruckus, instalados de la forma detallada a continuación.

Tabla I. **Listado de instalación de dispositivos de punto de acceso inalámbrico por salón**

Salón	Marca	Modelo	Dirección IP asignada
013, 014 y oficinas de coordinación.	Ruckus	R710	172.10.0.40 / 16
India 1, India 2	Ruckus	R710	172.10.0.3 / 16
India 3	Ruckus	R310	10.56.0.12 / 16

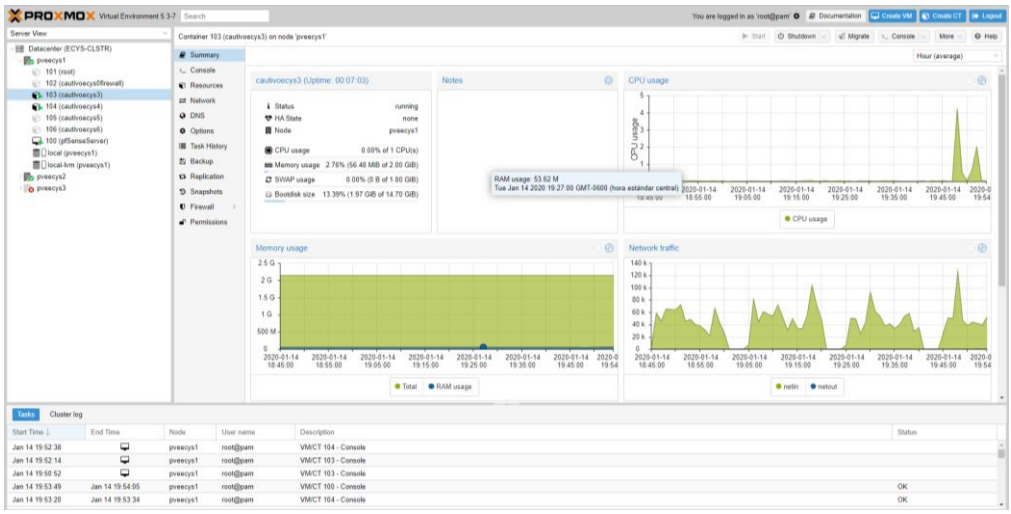
Fuente: elaboración propia.

2.2.2.5. Servidores físicos y plataforma de virtualización para alojamiento de servidores

Debido a que una de las restricciones en la elaboración del proyecto es la utilización de la infraestructura y configuración de red existente, se utilizó la plataforma de virtualización PROXMOX implementada con anterioridad para alojar los servidores del proyecto como contenedores y máquinas virtuales con interfaces de red virtuales.

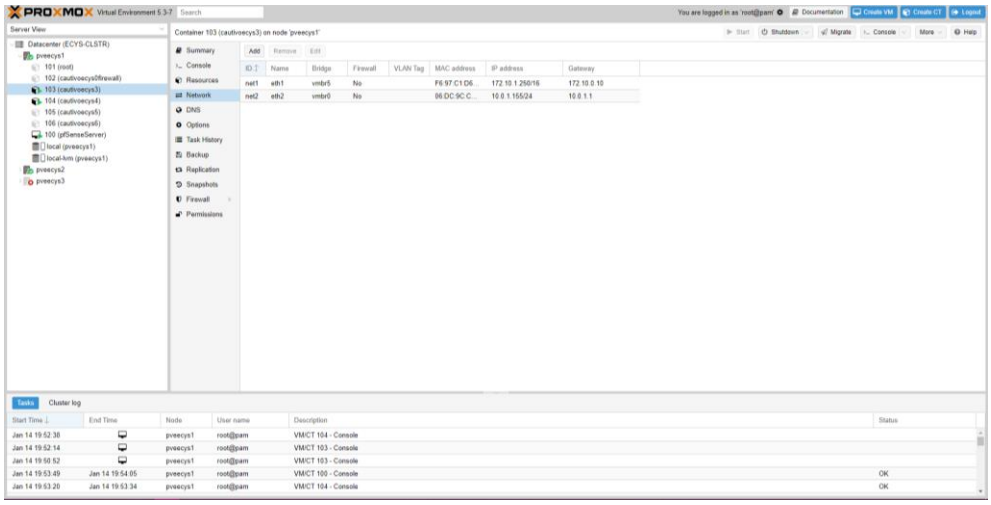
Se presenta a las siguientes imágenes la máquinas virtuales y contenedores creados en PROMOX como los servidores del proyecto.

Figura 1. **Contenedor de PROXMOX para servidor de base de datos**



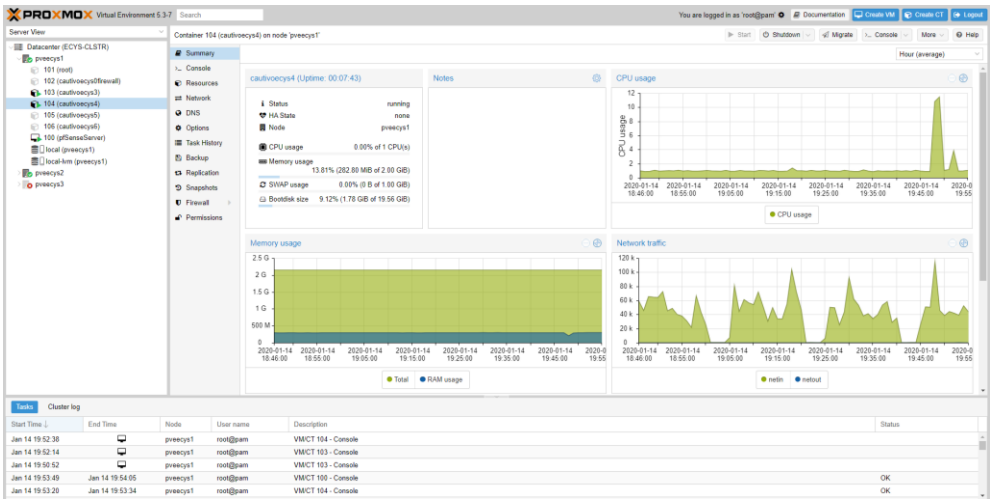
Fuente: elaboración propia, empleando PROXMOX 3.5.7.

Figura 2. **Configuración de red para contenedor de PROXMOX del servidor de base de datos**



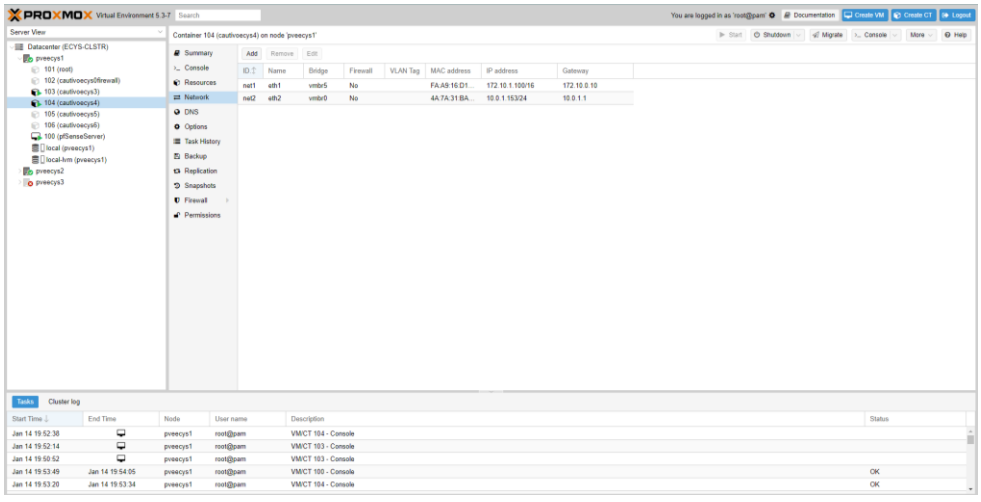
Fuente: elaboración propia, empleando PROXMOX 3.5.7.

Figura 3. **Contenedor de PROXMOX para servidor de aplicaciones web**



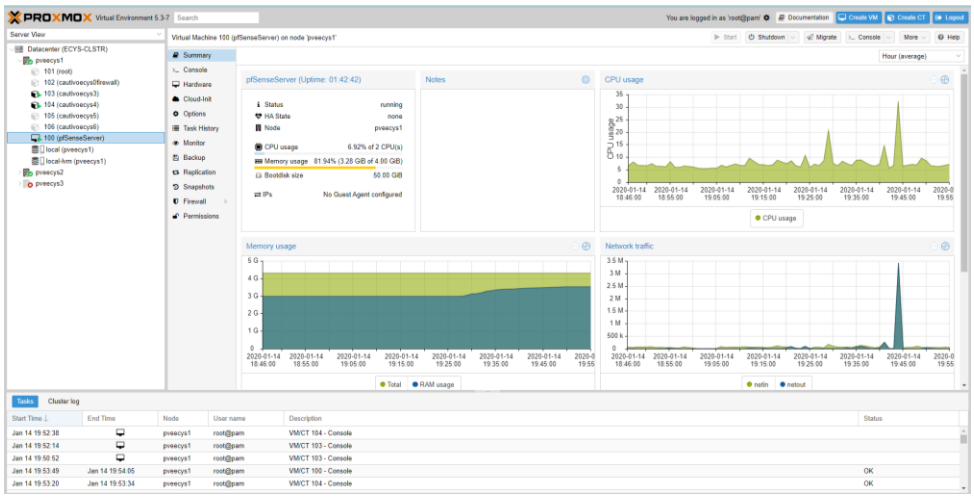
Fuente: elaboración propia, empleando PROXMOX 3.5.7.

Figura 4. **Configuración del contenedor de PROXMOX para servidor de aplicaciones web**



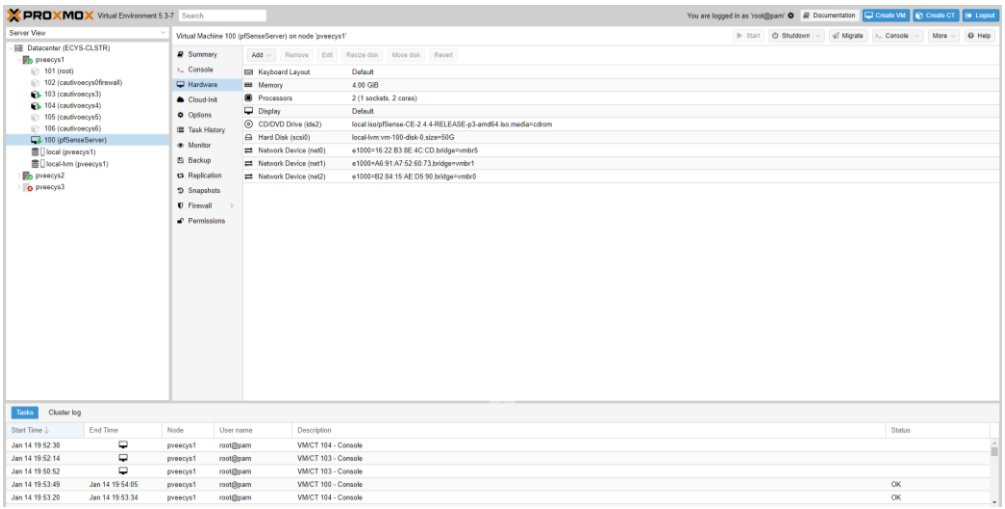
Fuente: elaboración propia, empleando PROXMOX 3.5.7.

Figura 5. **Máquina virtual de PROXMOX para servidor de corta fuegos**



Fuente: elaboración propia, empleando PROXMOX 3.5.7.

Figura 6. **Configuración de interfaz de red de máquina virtual para servidor de corta fuegos en PROXMOX**



Fuente: elaboración propia, empleando PROXMOX 3.5.7.

2.2.3. Análisis e investigación del modelo de datos

El modelo de datos es parte fundamental del proyecto, porque define la estructura de información sobre la que se almacena toda la información de usuarios, tráfico, políticas e historiales de consumo dentro de la red de internet inalámbrico. Este análisis consiste en la investigación y posterior modelación de los datos existentes en el sistema. Debido a que no existe ningún tipo de herramienta, documentación o información previa sobre la estructura o el modelo de datos que se genera del proceso de conexión a usuarios de la red y su consumo, se seleccionará aquellos datos que son característicos y necesarios para dar soporte a la funcionalidad y almacenamiento de información requerido.

2.2.3.1. Análisis de datos

Debido a que no existe registros o sistemas que almacenen, den soporte e integridad a la información de los usuarios, el tráfico de red y datos sobre el consumo del servicio se realizó el análisis de los distintos actores y características de cada uno para así obtener un esquema de tablas y relaciones que permitan definir las características y datos que el sistema obtendrá producto de la elaboración de los objetivos y funcionalidades de este.

Tabla II. **Características seleccionadas para el modelo de datos, establecidas durante la fase de investigación en el mes de julio de 2019**

Característica	Descripción
Datos del usuario de la red	• Nombre y apellido de cada usuario • Número de carné de cada usuario, utilizado como clave de acceso genérica. • Correo electrónico. • Fecha de nacimiento. • Carrera universitaria.

Continuación de la tabla II.

Datos de usuarios administrativos.	• Nombre y apellido del usuario. • Descripción general del usuario. • Contraseña del usuario. • Fecha de registro. • Estado para usuarios administrativos, se definió como habilitado y deshabilitado.
Datos de sesión.	• Identificador de usuario, que para cada usuario será su número de carné. • Tipo de conexión. • Fecha y hora de inicio de conexión. • Fecha y hora en que se finalizó la conexión del usuario. • Fecha y hora en que se realizó la última actualización de datos de conexión.
Datos de dispositivo de acorde a la conexión del usuario en la red.	• Dirección IP asignada del dispositivo utilizado para conectarse a la red. • Dirección MAC del dispositivo con el que el usuario está conectado a la red. • Cantidad de megabytes de descarga consumidos por el usuario. Cantidad de megabytes de subida consumidos por el usuario. • Gateway de conexión.
Políticas de red aplicables al sistema.	• Nombre de la política. • Valor asignado a la política. • Tipo de dato asignado a la política. • Fecha de registro de la política. • Valor de configuración al que corresponde cada una de las políticas.

Fuente: elaboración propia.

La selección de la información se realizó acorde a los requerimientos que le coordinador de los laboratorios. Se obtuvieron detalles técnicos sobre la estructura del modelo de datos con base a los procesos de autenticación de usuarios, uso de la red y la infraestructura actual, así como la especificación técnica solicitada para el manejo de la información tomando en cuenta que el sistema a largo plazo pueda crecer.

2.2.3.2. Herramientas de desarrollo, investigación y su definición

Para la selección de las herramientas de implementación del proyecto se contó con la participación y especificación del coordinador de los laboratorios, porque al ser ingeniero en Ciencias y Sistemas se involucró directamente tomando en cuenta los aspectos técnicos que le favorecerían al proyecto para darle continuidad a largo plazo.

A continuación, se presenta la lista de cada herramienta seleccionada junto a su tipo o uso para la elaboración del proyecto, y una breve descripción.

Tabla III. **Herramientas de desarrollo seleccionadas**

Tipo o uso	Nombre de la herramienta	Descripción y características
Lenguaje de programación *Backend.*	Java	Lenguaje de programación orientado a objetos, el cual es multiplataforma, de uso gratuito cuyo costo para la implementación será gratuito y muy versátil al momento de la elaboración de los *servlet* de comunicación entre interfaz de usuario y *backend.*

Continuación de la tabla III.

Lenguaje de comunicación cliente FauxAPI para configuración de corta fuegos.	PHP	Lenguaje de programación con tipado no estático que permite la implementación de aplicaciones tanto web como de escritorio. Es de uso gratuito y compatible con el cliente de comunicación de la librería FauxAPI para la configuración de características del servidor de corta fuegos PfSense.
Lenguaje de programación *Frontend.*	JavaScript	Lenguaje de programación sin tipado estático y orientado a su uso en *frontend* o comúnmente llamado lado del cliente. Es de uso gratuito y con compatibilidad para todos los navegadores web existentes.
Sistema manejador de base de datos DBMS.	PostgreSQL	PostgreSQL es sistema de base de datos relacional de objetos de código abierto fiable, sólido y con buen rendimiento. (The PostgreSQL Global Development Group).
Protocolo de autenticación, autorización y contabilización (AAA).	RADIUS	Protocolo de autenticación, autorización y contabilización para aplicaciones de acceso a la red por medio de protocolo IP. (FreeRADIUS).
Servidor AAA	FreeRADIUS	Servidor que implementa el protocolo RADIUS para el manejo de sesiones y usuarios conectados a una red por medio del modelo de conexión TCP.
Servidor de corta fuegos, DNS y DHCP.	PfSense 2.4.4	Software de código abierto que implementa múltiples paquetes y servicios para la administración de redes por medio del protocolo TCP. Es compatible con el sistema operativo Linux y tiene muchas implementaciones.

Continuación de la tabla III.

Servidor de aplicaciones *web* para el sistema de administración.	Apache Tomcat	Servidor de aplicaciones web que permite el despliegue de software en entornos de ejecución web. Su especialidad es la ejecución de aplicaciones que implementan el lenguaje de programación Java y tecnologías del ecosistema como *servlet's.*
Servidor http de aplicaciones para el módulo de políticas administrativas.	Apache2	Servidor de aplicaciones web que permite el despliegue de aplicaciones web. Para objetivos del proyecto permitirá la aplicación de modulo intermedio en lenguaje PHP como cliente del servidor de corta fuegos de la librería FauxAPI.
Sistema Operativo	Linux Ubuntu 18.04 y 12.0	Sistema operativo de código abierto que permite la implementación de todas las herramientas seleccionadas para el proyecto generando un costo cero para la elaboración del proyecto.
Librerías y frameworks de desarrollo web.	• Boostrap 4 • JQuery 3.2 • EasyUI	Librerías de ayuda y soporte de software que enriquecen el diseño y desarrollo de software. Las librerías seleccionadas en esta ocasión son orientadas al desarrollo de software web.
IDE de desarrollo	• Netbeans	Aplicación de software para desarrollo de aplicaciones en el lenguaje de programación Java.
Patrón de arquitectura.	MVC	Patrón de diseño de arquitectura de software utilizado para la división de un software en capas tales como interfaz de usuario, datos y la lógica de la aplicación. (Universidad de Alicante).

Fuente: elaboración propia.

2.2.3.3. Infraestructura de red, hardware y herramientas de desarrollo

Los laboratorios de la Escuela de Ciencias y Sistemas cuentan actualmente con instalaciones y hardware necesario para alojar el proyecto, así como la infraestructura de red para la implementación de la arquitectura de la solución. Sin embargo, la configuración e infraestructura actual no fue permitido modificarla sino adecuar la solución a fin de poder compartir los recursos y configuración existentes.

A continuación, se presenta e listado de elementos de hardware y software utilizados para el desarrollo del proyecto enfocado en la infraestructura de red:

Tabla IV. **Herramientas de infraestructura**

Tipo o uso	Número	Dirección IP	Descripción y características
Servidores aplicaciones Web.	1	172.10.1.100	• Contenedor en Proxmox
Servidor de base de datos.	1	172.10.1.250	• Contenedor en Proxmox
Firewall Servidor DNS Servidor DHCP	1	172.10.0.1	• VM en Proxmox
Cableado estructurado.		existente.	El cableado estructurado existente consiste en puertos de red *ethernet* dentro de los laboratorios.
Punto de acceso inalámbrico.	3		Consiste en 3 *access point* de marca Ruckus con capacidad para brindar el servicio de portal cautivo y administrativo para el servicio de internet inalámbrico.

Continuación de la tabla IV.

Hypervisor o entorno de virtualización.	1	PROXMOX	Debido a que la cantidad de servidores físicos es limitada e insuficiente para la elaboración del proyecto, se optó por utilizar el entorno de virtualización existente en los servidores y la utilización de contenedores y máquinas virtuales integradas a la infraestructura de red.

Fuente: elaboración propia.

2.3. Presentación de la solución del proyecto

El proyecto fue realizado utilizando la infraestructura y topología de red existente, y la utilización de la herramienta de software para virtualización que actualmente se implementa en los servidores físicos de los laboratorios, con un añadido de infraestructura y ordenamiento de la red.

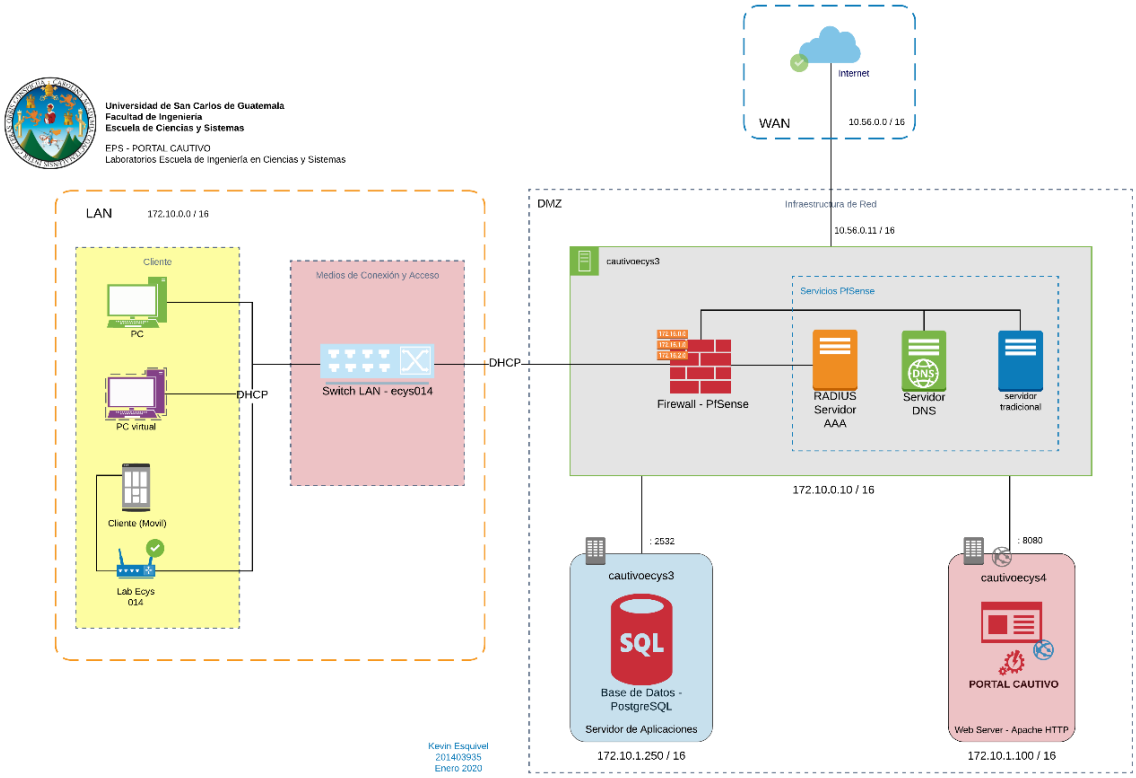
En principal añadido que presenta la solución del proyecto es la esquematización de la red en segmentos de LAN y WAN por medio de una zona desmilitarizada y la implementación de un firewall para la administración de usuarios y recursos de red.

2.3.1. Diseño de infraestructura de la solución del proyecto

Durante la fase de diseño se elaboró el diagrama de infraestructura que presenta los elementos de software y hardware que se utilizaran para la implementación del proyecto. Además, se elaboró el modelo de datos con base

en las entidades y tablas definidas previamente en la fase de investigación para dar soporte a la información del sistema.

Figura 7. **Diagrama de implementación de la solución**



Fuente: elaboración propia, empleando Lucidchart en su versión web.

El diagrama general presenta el diseño de forma gráfica, y la conexión que existirá entre los componentes, considerando esta como bidireccional porque el tráfico de la red actual no tiene restricciones y se debe respetar, para no dañar configuraciones anteriores en la red que fueron establecidas anterior a la elaboración del proyecto; de la misma manera se muestra la interacción portal cautivo y plataforma de administración.

2.3.2. Historias de usuario

Las historias de usuario son la presentación de un requerimiento funcional descrito mediante una frase que regularmente corta en un lenguaje común para el usuario.

En la siguiente tabla se muestra las historias de usuario obtenidas durante las reuniones con la coordinación de los Laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas, y la especificación de los criterios de aceptación.

Tabla V. **Listado de las historias de usuario**

Id	Descripción	Criterios de aceptación
HI 1	Como administrador quiero visualizar los usuarios de la red interna.	• Reporte tabular de los usuarios conectados y activos a la red inalámbrica y un histórico de los datos. • Reporte tabular con información de su consumo y tiempo de conexión de los usuarios conectados.
HI 2	Como administrador quiero que los usuarios se registren en el portal cautivo en su primera conexión a la red inalámbrica.	• Registro de usuarios a través del portal cautivo, previo a su autorización de conexión a la red inalámbrica para consumo de internet.
HI 3	Como administrador quiero que los dispositivos que se conecten a la red inalámbrica deban ingresar una clave genérica (número de registro estudiantil) antes de poder consumir recursos de la red.	• Ingreso previo a conexión por clave genérica (número de registro estudiantil) • Ingreso únicamente de los usuarios registrados.
HI 4	Como usuario debe poder acceder exclusivamente a los recursos de internet definidos por las políticas.	• Consumo de internet delimitado por políticas de la red. • Tiempo de conexión delimitado por las políticas.

Continuación de la tabla V.

HI 5	Como administrador deseo visualizar y exportar reportes de consumo de la red de internet inalámbrico.	• Reporte de consumo de internet por usuario por cada conexión. • Reporte de usuarios conectados por rango de fecha. • Reporte de usuarios conectados actualmente.
HI 6	Como administrador quiero registrar políticas generales para el control del contenido al cual tienen acceso los usuarios de la red de internet inalámbrico.	• Asignación de valor a las políticas de acceso a recursos de internet definidas dentro del módulo administrativo. • Sección del módulo administrativo para la gestión de políticas.
HI 8	Qué el sistema de administración pueda manejar distintos usuarios y roles administrativos para el acceso a reportes, gestión de usuarios y políticas de acceso a los recursos de red inalámbrica.	• Login para manejo de credenciales y acceso de usuarios administrativos. • Creación, eliminación y modificación de usuarios y roles administrativos.
HI 9	Como sistema deberá implementar protocolos o sistemas eficientes de autentificación para el uso de la red y el sistema administrativo.	• Implementación servidor RADIUS. • Integración servidor RADIUS al portal cautivo y administrativo.

Fuente: elaboración propia.

2.3.3. Modelo de datos

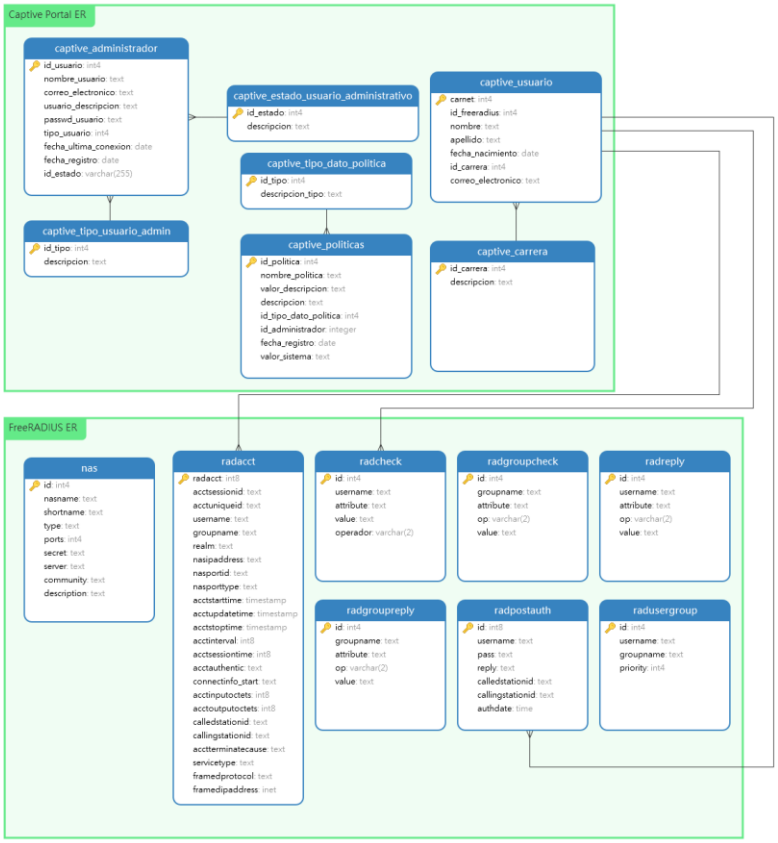
El diseño del modelo de datos muestra la estructura de cómo se dará soporte a la información que se genere del tráfico en la red interna LAN y en el módulo administrativo, mediante una estructura lógica para cumplir con los requerimientos e integridad de los datos.

Es importante resaltar que el modelo de datos provisto por el servidor FreeRADIUS es no relacional porque de esa forma trabaja dicho software.

2.3.3.1. Diagrama entidad-relación

Por medio de una representación gráfica de entidades y relaciones que definen los datos establecidos anteriormente en tablas y la interacción de estos se da la estructura y el modelado lógico de cómo se dará integridad a los datos y serán almacenados para su correspondiente consulta.

Figura 8. **Diagrama entidad-relación**



Fuente: elaboración propia, empleando Navicat 12.1.

Tabla VI. **Entidades del modelo de datos para el sistema administrativo**

Número	Nombre de la entidad	Descripción
1.	captive_administrador	Entidad que contiene el registro de usuarios administradores para la aplicación administrativa.
2.	captive_carrera	Entidad que contiene el catálogo de carreras de la Facultad de Ingeniería.
3.	captive_estado_usuario_administrativo	Entidad que contiene el catálogo de estados en los que podrá estar un usuario de tipo administrativo.
4.	captive_tipo_dato_politica	Entidad que contiene le catálogo de tipos de datos aplicables a una política de red para los usuarios que se conecten por medio del portal cautivo.
5.	captive_tipo_usuario_admin	Entidad que contiene el catálogo de tipo de usuario administrativo.
6.	captive_usuario	Entidad que contiene el registro de los usuarios de la red interna.

Fuente: elaboración propia.

Tabla VII. **Entidades del modelo de datos del servidor FreeRADIUS**

Número	Nombre de la entidad	Descripción
1.	nas	Tabla de especificación de usuarios para servidor RADIUS, estos usuarios no son los que envían o reciben datos en la red sino son los que proveen el servicio de difusión en la red NAT, tales como enrutadores y conmutadores.
2.	radacct	Entidad que almacena la información de un usuario y su conexión en la red NAT. Entre los valores más destacados de almacenamiento se encuentran: • Historial de tiempo de conexión • Historiales de consumos de datos para carga y descarga. • Identificación especifica de los usuarios y el dispositivo físico que utilizo para conectarse.
3.	radcheck	Entidad o tabla que almacena los atributos de control para autenticación, contabilidad y autorización. Cada usuario se almacena en valores pares que contienen un operador y se validan para realizar acciones de los tres tipos mencionados con anterioridad a un usuario que se quiere conectar o está conectado a la red LAN.
4.	radgroupcheck	Entidad que almacena la información referente a los intentos de autenticación realizados por un usuario mediante un cliente NAS, para dar paso a un usuario al uso de la red de internet y este es parte de la red LAN. En esta tabla se almacena únicamente las conexiones en las cuales se intentó realizar un acceso por medio de una clave y contraseña para un grupo definido. Para efectos del proyecto no será utilizada ya que no se implementarán grupos de usuarios.
5.	radgroupreply	Entidad que contiene la respuesta a solicitudes de registro de la tabla radgroupcheck. Para efectos del proyecto no será utilizada ya que no se implementaron grupos de usuarios.

Continuación de la tabla VII.

6.	Radpostauth	Entidad o tabla que almacena la información referente a los intentos de autenticación procesados por el servidor RADIUS mediante un cliente NAS para dar paso a un usuario al uso de la red LAN, en esta tabla se almacena directamente la relación entre usuario y respuesta de acceso.
7.	Radreply	Entidad que contiene la repuesta a las solicitudes de registro a la tabla radcheck.
8.	Radusergroup	Entidad que contiene la definición entre usuarios y grupos. Para efectos del proyecto no será utilizada ya que no se implementaron grupos de usuarios.

Fuente: elaboración propia.

2.3.3.2. Diseño de entidades y dependencias

A continuación, se presenta el listado detallado de las tablas que conforman el modelo de datos para el sistema de administración de recursos de internet con su descripción, funcionalidad, y su función de interrelación con las demás entidades que conforman el modelo de datos.

Tabla VIII. **Detalle de la tabla captive_administrador**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
id_usuario	Identificador único de cada usuario de tipo administrador.	Llave primaria	Serial
nombre_usuario	Nombre del usuario de tipo administrador.	Dato	Text

Continuación de la tabla VIII.

correo_electronico	Correo electrónico del usuario de tipo administrador.	Dato	Text
usuario_descripcion	Descripción del usuario de tipo administrador.	Dato	Text
passwd_usuario	Contraseña del usuario de tipo administrador que se almacena formato de encriptación MD5.	Dato	Text
id_tipo_usuario	Tipo de usuario	Llave foránea	Integer
id_estado	Estado del usuario de tipo administrador.	Llave foránea	Integer
fecha_ultimaconexion	Fecha en que se conectó por última vez el usuario al módulo administrativo.	Dato	Date
fecha_registro	Fecha en que se registró al usuario.	Dato	Date

Fuente: elaboración propia.

Tabla IX. **Detalle de la tabla captive_carrera**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
id_carrera	Identificador único para cada carrera	Llave primaria	Serial
descripcion	Descripción de la carrera.	Dato	Integer

Fuente: elaboración propia.

Tabla X. **Detalle de la tabla captive_estado_usuario_administrativo**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
id_tipo_estado	Identificador del tipo de estado para los usuarios administrativos.	Llave primaria	Serial
descripcion	Descripción del estado para asignación a los usuarios administrativos: habilitado o inhabilitado.	Dato	Text

Fuente: elaboración propia.

Tabla XI. **Detalle de la tabla captive_tipo_dato_politica**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
Id_tipo_dato	Identificador del tipo de dato de asignación a las políticas.	Llave primaria	Serial
nombre_tipo	Nombre del tipo de dato que puede ser asignado a la política de administración de red.	Dato	Text

Fuente: elaboración propia.

Tabla XII. **Detalle de la tabla captive_tipo_usuario_admin**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
id_tipo	Identificador del tipo de usuario administrador.	Llave primaria	Serial
descripcion	Descripción del tipo de usuario para administrativos del sistema de administración.	Dato	Text

Fuente: elaboración propia.

Tabla XIII. **Detalle de la tabla captive_usuario**

Nombre del campo	Descripción	Función de integridad	Tipo de dato
id_usuario	Identificador único de los usuarios de la red.	Llave primaria	Serial
id_freeradius	Número entero utilizado por el servidor FreeRADIUS para identificar de manera única a los usuarios de la red.	Dato	Integer
carnet	Número de carné de los usuarios de la red, utilizado también como clave genérica.	Dato	Text
nombre	Nombre del usuario de la red.	Dato	Text
apellido	Apellido del usuario de la red.	Dato	Text
fecha_nac	Fecha de nacimiento del usuario de la red.	Dato	Text
id_carrera	Identificador único del tipo de carrera que estudia el usuario de la red.	Llave foránea	Integer
correo_electronico	Correo electrónico de contacto del usuario de la red.	Dato	Text

Fuente: elaboración propia.

2.3.4. Sistema para la administración del recurso de internet inalámbrico

El sistema de administración del recurso de internet inalámbrico consta de módulos o secciones de administración individuales con un conjunto de reportes y funcionalidades.

El diseño fue basado en cuatro módulos individuales los cuales se interrelacionan tanto con el modelo de datos del sistema administrativo como del provisto por el servidor RADIUS haciendo uso concurrente de ambos tanto para gestión de recursos como de reportes.

A continuación, se presenta un listado descriptivo de cada uno de los módulos del sistema de administración con su descripción y las funcionalidades correspondientes para cada uno.

Tabla XIV. **Módulos del sistema y plataforma web administrativa**

Nombre	Descripción	Funcionalidades
Dashboard administrativo.	Módulo para la presentación de reportes en tiempo real. Permite la visualización de.	• Presentación de gráfico de pie con el conteo de usuarios de la red, clasificados por la carrera a la que pertenecen.
Generación de reportes.	Módulo para la generación de reportes, abarca la generación de reportes con información tanto de usuarios de la red como de los recursos del internet incluyendo las características de estos.	• Reporte de gráfico de líneas con la cantidad de consumidores del servicio de internet por rango de fecha. Se detalla el conteo por cada fecha dentro del rango especificado no mayor a 30 y 31 días. • Reporte con el detalle de consumidores del servicio de internet por rango de fecha. Se detalle de manera tabular el gráfico de líneas clasificando por días las conexiones existentes, y su estado actual con una representación de colores el estado de los usuarios y su conexión con la red.

Continuación de la tabla XIV.

		• Reporte tabular con el detalle de consumo por usuario y conexión de los recursos de internet en el que muestra un historial de cada usuario, y su dispositivo con la información de su conexión y de consumo de internet, en relación con su tiempo de conexión a la red. • Reporte de características de la población o de usuarios en el cual se presenta un gráfico de barras con el número de estudiantes por carrera, un gráfico de tipo pie con un conteo por año de carnet y un gráfico de radar con el conteo por rangos de edad de la población registrada en el sistema, para uso del recurso de internet. • Reporte de conexiones en el que se muestra el historial de conexiones e intentos de conexión a los recursos de internet por medio del portal cautivo especificando el usuario, respuesta de acceso y la fecha del suceso.

Continuación de la tabla XIV.

Gestión de usuarios.	Módulo para la gestión de usuarios tanto administrativos del sistema como de la red.	• Listado de los usuarios administrativos con la presentación de su información de libre acceso. • Creación de usuarios administrativos. • Eliminación de usuarios administrativos. • Edición de los usuarios administrativos. • Listado de usuarios de la red con su información de registro. • Eliminación de usuarios de la red.
Gestión de políticas.	Módulo para la administración del acceso para los usuarios administrativos y la gestión de las políticas de red.	• Listado de usuarios administrativos. • Cambios de estado a los usuarios administrativos (habilitado o deshabilitado). • Cambio de tipo de usuario administrativo. • Listado de políticas de administración de red en él se muestran las 6 opciones de políticas a administrar, así como de los valores asignados a las mismas con su descripción y tipo. • Asignación de valor a la política administrativa para la red. • Des habilitación de la política administrativa de la red.

Fuente: elaboración propia.

A continuación, se muestra el módulo de portal cautivo que es inherente al sistema administrativo pero que no forma parte de este pero que por su parte esta implementado en el mismo servidor de aplicaciones web internamente dentro del firewall Pfsense como una personalización de este.

Tabla XV. **Módulos del portal cautivo**

Nombre	Descripción	Funcionalidad
Acceso	Módulo de acceso a la red interna de los laboratorios.	• Login de acceso a la red interna para poder tener consumo del recurso de internet.
Registro	Módulo para registro en la red interna de los laboratorios.	• Registro de usuarios por medio del ingreso de información básica de contacto y características de usuario. • Asignación de clave genérica por usuario, en este caso específico el número de carné de cada usuario.

Fuente: elaboración propia.

2.3.5. Instalación y configuración de software para administración de redes como parte de la solución del proyecto

La solución contempla la implementación de una parte de infraestructura de red y otra de desarrollo de software, ambas funcionarán conjuntamente para cumplir con los requerimientos definidos.

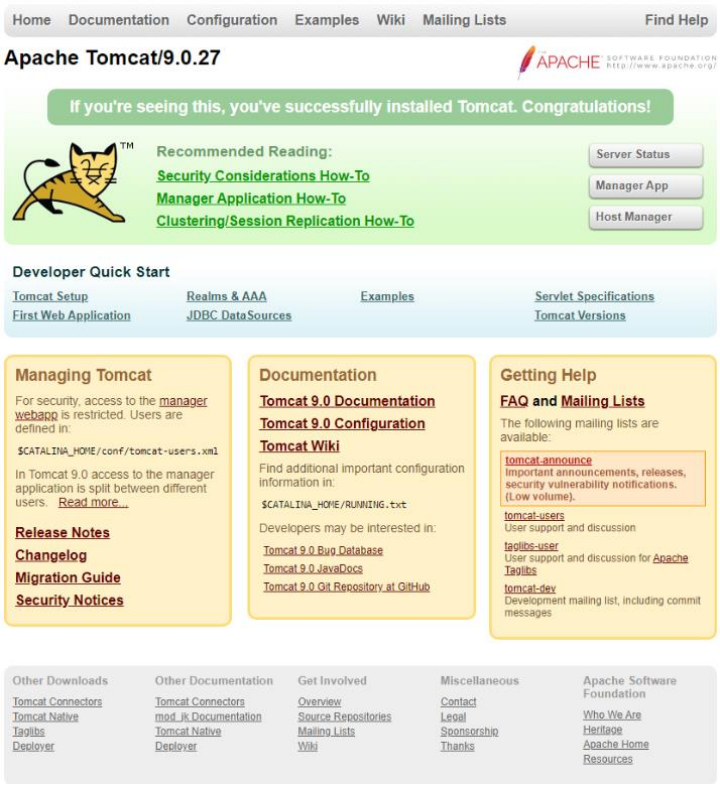
A continuación, se presentan como parte de la infraestructura de red los servidores que alojarán los servicios de la solución del proyecto.

2.3.5.1. Servidor de aplicaciones web

El servidor de aplicaciones web es el encargado de alojar el conjunto los *servlets* para la comunicación bidireccional con los usuarios del sistema para la administración de los recursos de red e internet inalámbrico de los laboratorios.

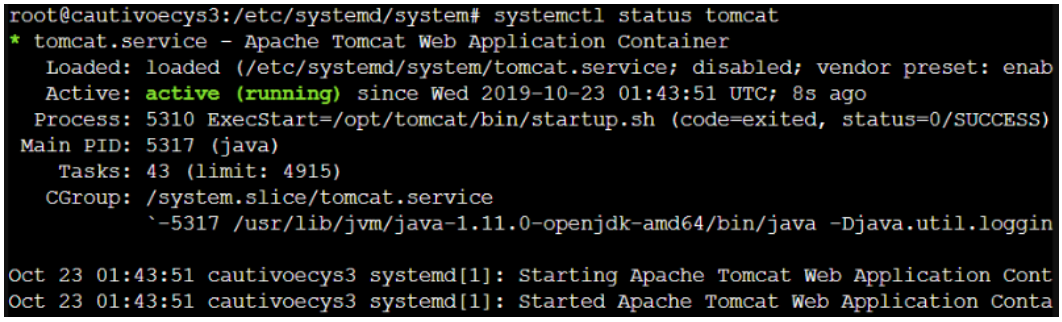
Se presenta a continuación el resultado de la instalación del servidor de aplicaciones web Apache Tomcat en su versión 9.0.27, y la ejecución del servicio en la consola del sistema operativo Linux 18.04 del servidor.

Figura 9. **Resultado final de la instalación del servidor para aplicaciones web Apache Tomcat versión 9.0.27 en el contenedor alojado en el sistema de virtualización PROXMOX**



Fuente: elaboración propia, empleando Apache Tomcat 9.0.27.

Figura 10. **Estado de la ejecución del proceso para el servidor web Apache Tomcat versión 9.0.27, instalado dentro del sistema de virtualización PROXMOX**



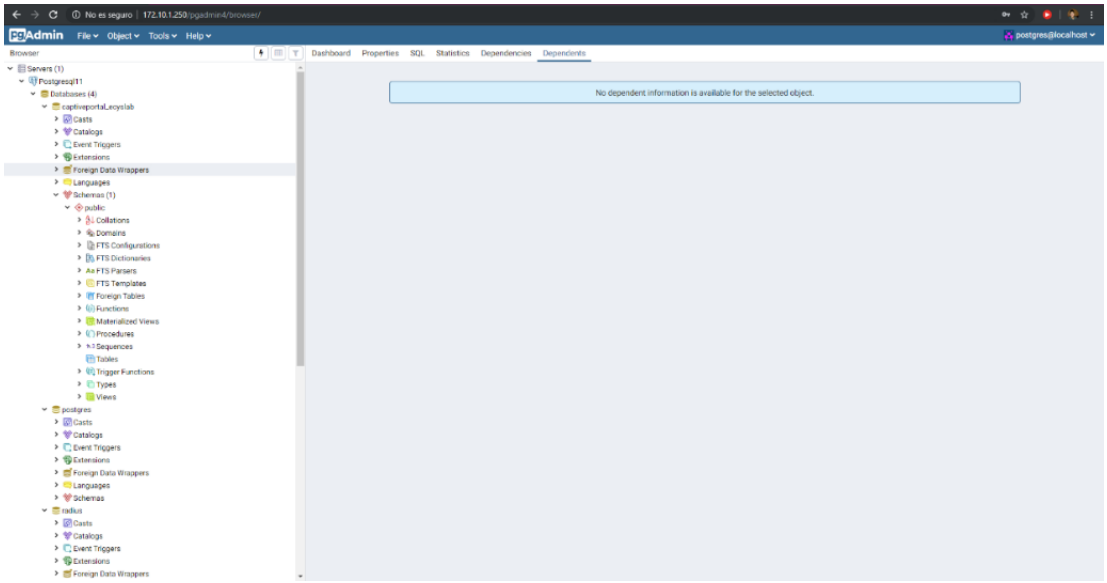
Fuente: elaboración propia, empleando la consola del sistema operativo Linux 18.04.

2.3.5.2. Servidor para el sistema gestor de base de datos

El servidor que aloja el sistema de gestión de base de datos será el encargado de ejecutar el proceso y almacenar la información sobre los usuarios, sus conexiones, consumos y demás información que se solicite y registre por el servidor RADIUS. Para el desarrollo del proyecto se seleccionó la herramienta PostgreSQL como sistema gestor de base de datos.

Se presenta a continuación los resultados de la instalación y configuración de la herramienta antes mencionada.

Figura 11. **Resultado final de la instalación del sistema de gestión de base de datos PostgreSQL versión 11 en el contenedor alojado en el sistema de virtualización PROXMOX**



Fuente: elaboración propia, empleando PgAdmin4 2019.

Figura 12. **Estado de la ejecución del proceso para el sistema gestor de base de datos PostgreSQL versión 11, instalado dentro del sistema de virtualización PROXMOX**

```
root@cautivoecys3:/etc/postgresql/11/main# systemctl status postgresql
* postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: enabled)
   Active: active (exited) since Thu 2019-10-24 03:05:32 UTC; 12min ago
  Process: 13329 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 13329 (code=exited, status=0/SUCCESS)

Oct 24 03:05:32 cautivoecys3 systemd[1]: postgresql.service: Failed to reset devices.list: Operation not permitted
Oct 24 03:05:32 cautivoecys3 systemd[1]: Starting PostgreSQL RDBMS...
Oct 24 03:05:32 cautivoecys3 systemd[1]: Started PostgreSQL RDBMS.
root@cautivoecys3:/etc/postgresql/11/main#
```

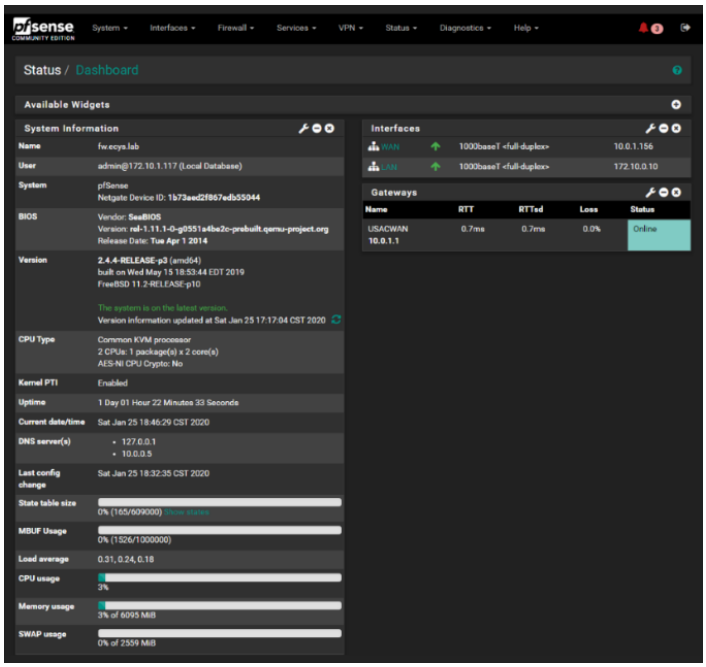
Fuente: elaboración propia, empleando la consola del sistema operativo Linux 18.04.

2.3.5.3. Servidor de corta fuegos

El servidor de corta fuegos es el encargado de la administración de la red y que en conjunto con el servidor RADIUS son los encargados de gestionar el acceso a los usuarios a la red LAN de los laboratorios.

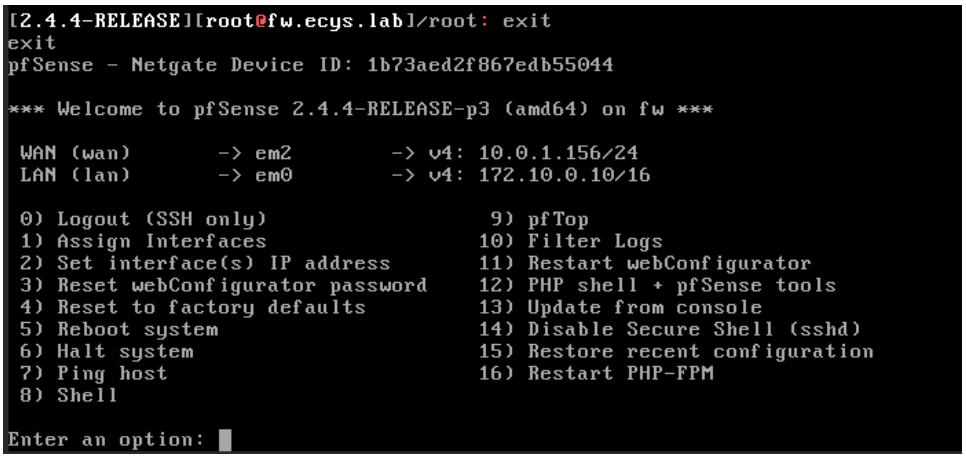
A continuación, se presenta los resultados de la instalación y configuración del servidor de corta fuegos para la solución del proyecto, siendo seleccionada la herramienta PfSense para esta funcionalidad.

Figura 13. **Resultado final de la instalación del servidor de corta fuegos Pfsense versión 2.4.4 en el contenedor alojado en el sistema de virtualización PROXMOX**



Fuente: elaboración propia, empleando PfSense 2.4.4.

Figura 14. **Consola de administración del corta fuegos PfSense para gestión directa desde el sistema operativo**



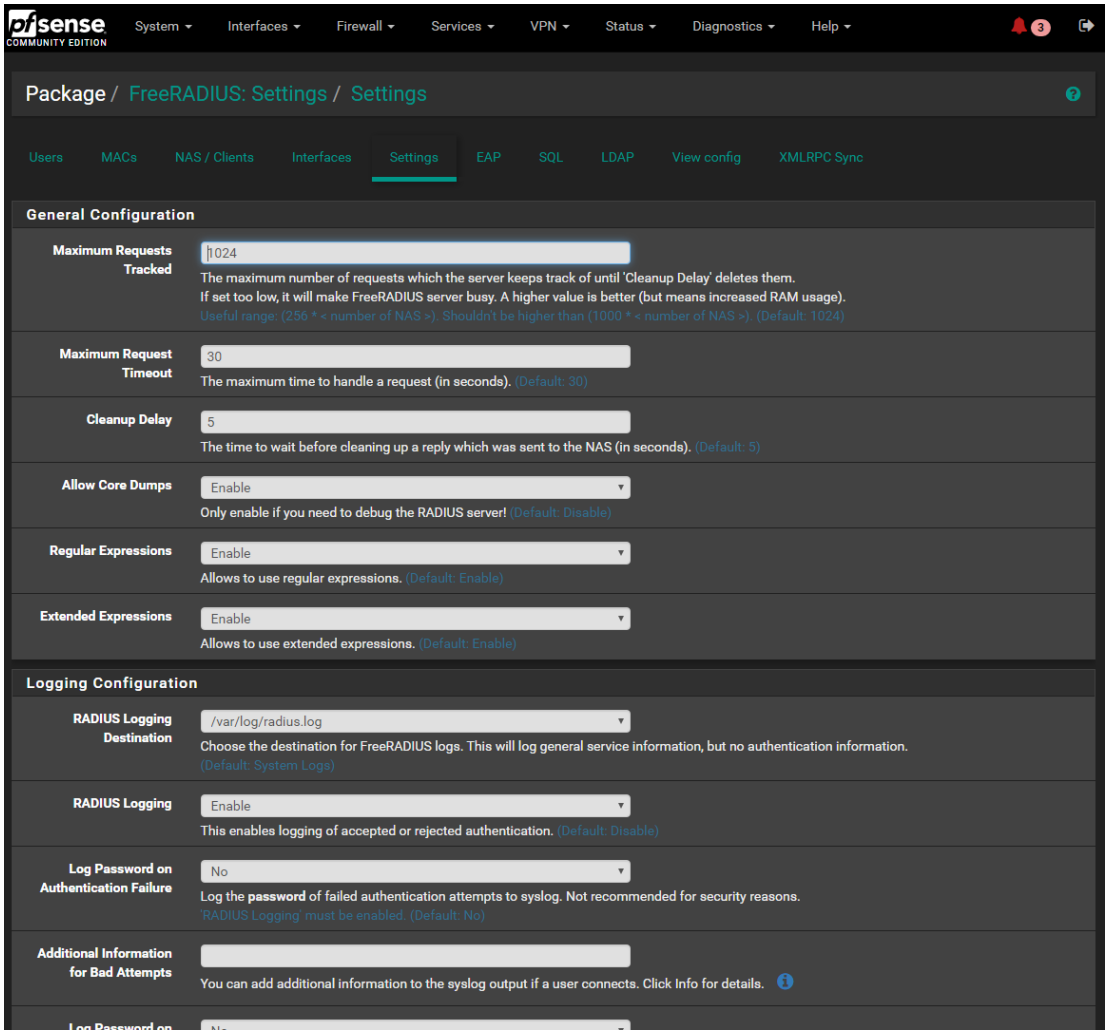
Fuente: elaboración propia, empleando consola de servidor de corta fuegos PfSense 2.4.4.

2.3.5.4. Servidor de autenticación, autorización y contabilización RADIUS

Para realizar la implementación del servidor RADIUS se seleccionó la herramienta FreeRADIUS que es de código abierto, específicamente se integró a la solución el paquete disponible dentro del servidor de corta fuegos PfSense y se instaló por medio del gestor de paquetes integrado. La configuración por su parte también se realizó directamente desde el servidor de corta fuegos y se integró la conexión a la base de datos en PostgreSQL por medio del módulo disponible en FreeRADIUS para conexión a dicho sistema gestor de base de datos.

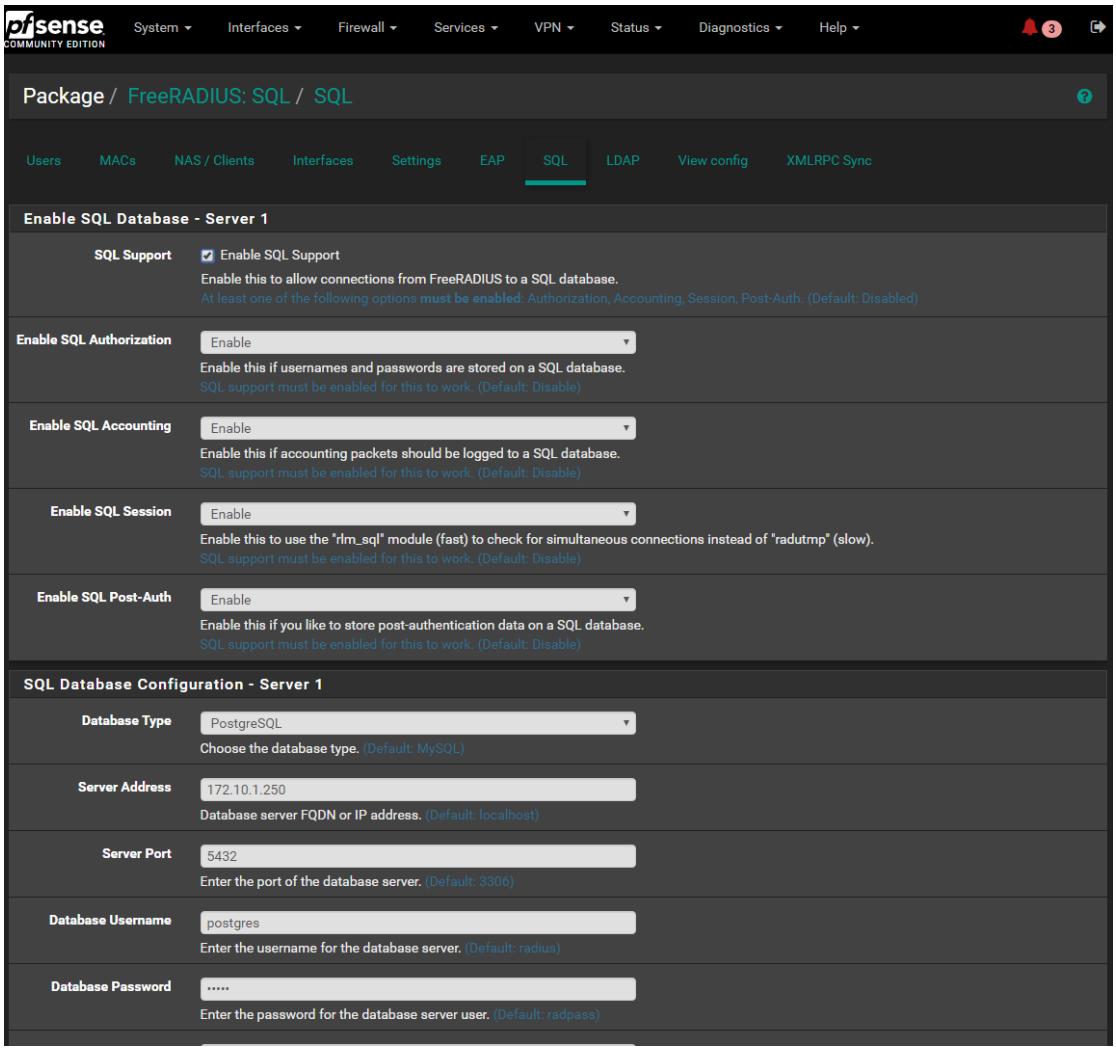
A continuación, se muestra la configuración del servidor FreeRADIUS.

Figura 15. **Configuración del servidor de autenticación, autorización y contabilización FreeRADIUS desde la consola de administración web de servidor corta fuegos PfSense**



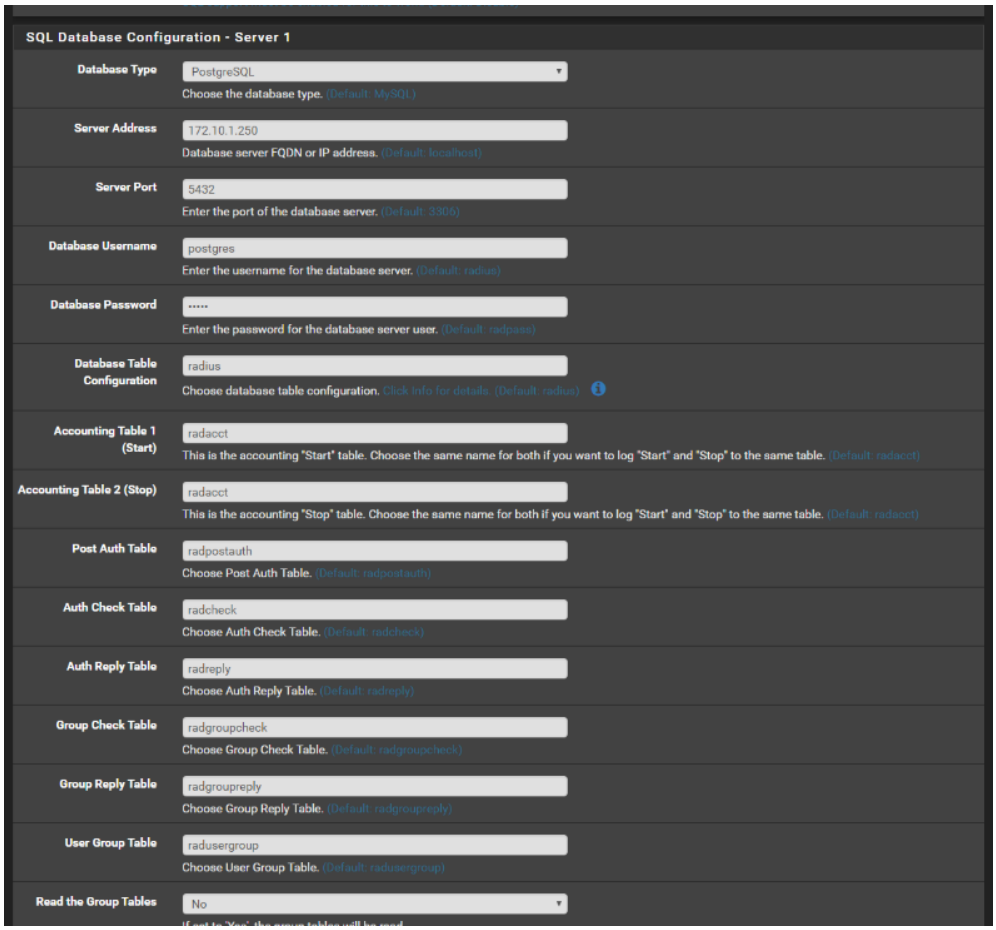
Fuente: elaboración propia, empleando servidor FreeRADIUS.

Figura 16. **Configuración del módulo de conexión SQL para el servidor FreeRADIUS**



Fuente: elaboración propia, empleando servidor FreeRADIUS.

Figura 17. **Configuración y especificación de tablas del modelo de datos para consumo del servidor FreeRADIUS**



Fuente: elaboración propia, empleando servidor FreeRADIUS.

A continuación, se presenta de manera detallada la configuración de modulo SQL para conexión al gestor de base de datos PostgreSQL desde Pfsense para autenticación, autorización y contabilización de usuarios desde el servidor FreeRADIUS.

Tabla XVI. **Configuración de módulo SQL del servidor de autenticación, autorización y contabilización FreeRADIUS para interconexión con el sistema de gestión de base de datos PostgreSQL como contenedor del modelo de datos para la solución del proyecto, elaborado en enero 2020**

Característica de configuración	Descripción	Valor Asignado
Habilitar autorización en SQL.	Opción que permite al servidor FreeRADIUS realizar autentica y autorización de usuarios por medio de la información almacenada en la base de datos para el portal cautivo.	Habilitado
Habilitar de contabilización en SQL.	Opción que permite habilitar la contabilización y registro de información sobre los paquetes de datos que consumen los usuarios autenticados en la red.	Habilitado
Habilitar sesiones en SQL	Opción que permite el manejo de sesiones en la red.	Habilitado
Habilitar repuestas de autorización POST en SQL.	Opción que habilita al servidor para dar respuesta POST a las solicitudes de acceso a la red.	Habilitado
Tipo de base de datos.	Opción que permite seleccionar el tipo de sistema gestor de base de datos que utilizará el servidor FreeRADIUS.	PostgreSQL
Dirección del servidor.	Dirección IP del servidor en el cual se encuentra instalado el sistema gestor de base de datos PostgreSQL y en donde se encuentra almacenada actualmente la base de datos.	172.10.1.250

Continuación de la tabla XVI.

Puerto servidor.	Número de puerto que está habilitada para comunicación con el sistema gestor de base de datos PostgreSQL.	5432
Nombre de usuario de la base de datos.	Nombre de usuario que tiene las credenciales y accesos para conexión remota con la base de datos y que utilizará el servidor FreeRADIUS para comunicarse con el sistema gestor de base de datos PostgreSQL.	Postgres
Contraseña de base de datos.	Contraseña de acceso.	Dato confidencial
Tabla de configuración de la base de datos.	Nombre de tabla y base de datos que contendrá el modelo de datos del servidor FreeRADIUS.	radius
Tabla de contabilización de inicio de sesión.	Nombre de la tabla en donde se registrará toda la información de conexión y paquetes de consumo de ancho de banda de los usuarios de la red LAN de los laboratorios. En esta se almacenarán los inicios de sesión y detalle de consumos.	radacct
Tabla de contabilización de fin de sesión.	Nombre de la tabla en donde se registrará toda la información de las conexiones que han expirado o que fueron eliminadas de la red LAN de los laboratorios. En esta se almacenarán los inicios de sesión y detalle de consumos.	radacct

Continuación de la tabla XVI.

Tabla de repuestas de autenticación.	Nombre de la tabla que almacenará la información de todos los intentos de autenticación que se intentaron realizar por medio del portal cautivo para la red LAN de los laboratorios.	radpostauth
Tabla de validación de autenticación.	Nombre de la tabla que almacenará el nombre y contraseña de los usuarios que pueden autenticarse y tener acceso a la red LAN de los laboratorios. Esta tabla es el medio de verificación de usuarios que posee el servidor FreeRADIUS.	radcheck
Tabla de repuestas.	Nombre de la tabla en la que se registran todas las respuestas de las solicitudes realizadas al servidor FreeRADIUS.	radreply
Tablas de grupo.	Nombre de las tablas que especifican el manejo de grupos y medios de autenticación de grupos de usuarios. Son el homónimo disponible para los usuarios.	• radgroupcheck • radgroupreply • radusergroup
Lectura de tablas de grupos.	Opción que permite el manejo de grupos y su autenticación desde el servidor.	No
Eliminación de sesiones obsoletas.	Opción que permite la eliminación de sesiones obsoletas registradas dentro de la tabla de contabilización. Permite la depuración e integridad de registros en la base de datos.	Si

Continuación de la tabla XVI.

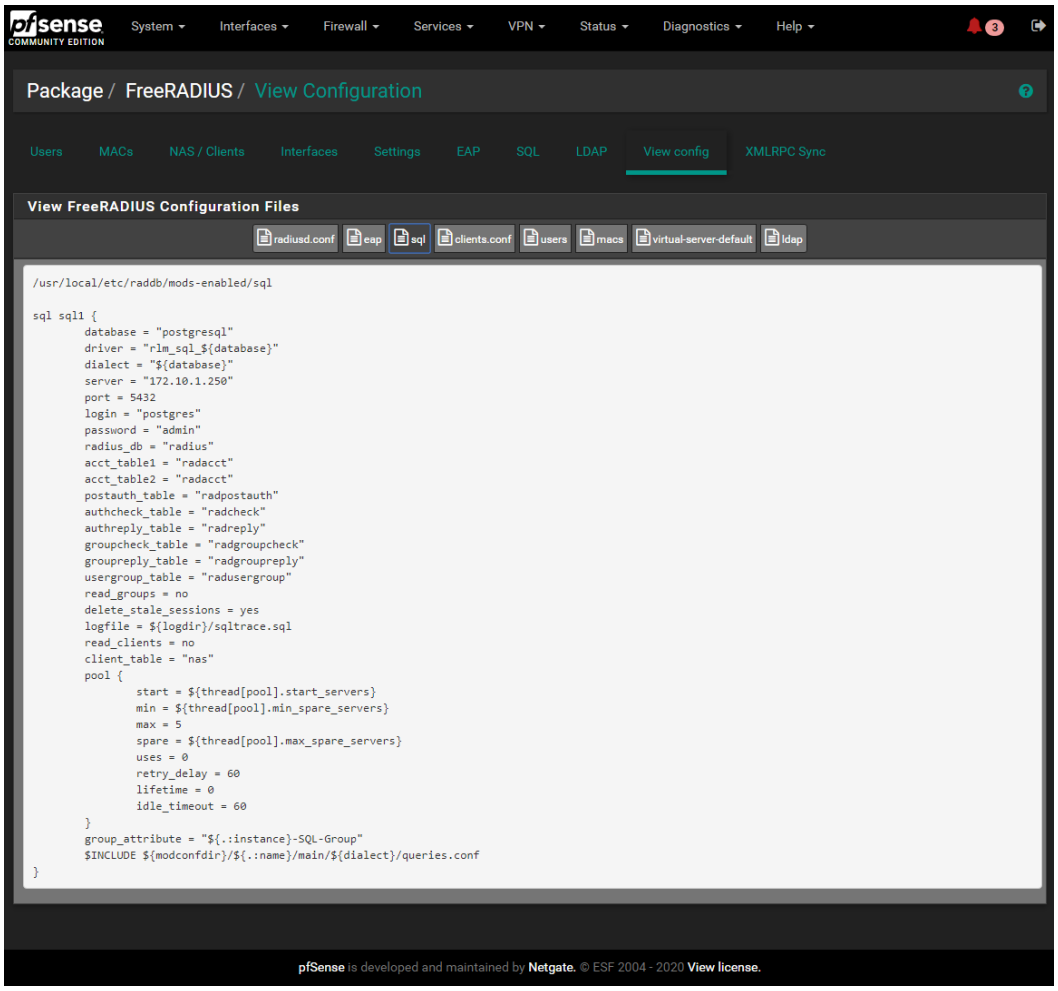
Impresión de todas las sentencias SQL.	Opción que permite mostrar por medio de la consola y log definidos, todas las sentencias SQL que se ejecuten remotamente sobre la base de datos.	Si
Número de conexiones SQL.	Número máximo de conexiones que un servidor FreeRADIUS puede crear a la base de datos para realizar operaciones en paralelo. Permite la alta disponibilidad del servicio.	5
Tiempo de espera por fallos en conexión a base de datos.	Tiempo de espera por cada intento de conexión a la base de datos, después del tiempo definido después de realizada una consulta se considera como fallida o realizada la conexión. Tiempo definido en segundos.	60
Tiempo de vida de enlace de conexión.	Tiempo durante el cual el servidor FreeRADIUS tendrá conexión a la base de datos. Este valor cuando es 0 permite que el tráfico TCP de sesión no termine durante el tiempo de vida de la conexión y permite la espera de solicitudes que tarden mucho tiempo en responder.	0

Continuación de la tabla XVI.

Máximo número de solicitudes por medio de enlace de conexión.	Número máximo de conexiones que se pueden enviar utilizando un mismo enlace de conexión con la base de datos. Previene los errores por enlaces que duren un largo periodo de tiempo permitiendo obtener un mayor rendimiento en las consultas remotas a la base de datos. Este valor por defecto es 0 y permite no tener un máximo de solicitudes por conexión permitiendo la alta disponibilidad de conexión con la base de datos.	0
Lectura de cliente desde la base de datos.	Opción que habilita la lectura de los clientes NAS (proveedores de servicio) desde la base de datos.	No
Tabla de clientes RADIUS.	Nombre de la tabla que almacenará los clientes del servidor FreeRADIUS y que serán los proveedores del servicio para los usuarios de la red. En este caso serán los conmutadores y enrutadores para distribuir el servicio de portal cautivo.	nas

Fuente: elaboración propia.

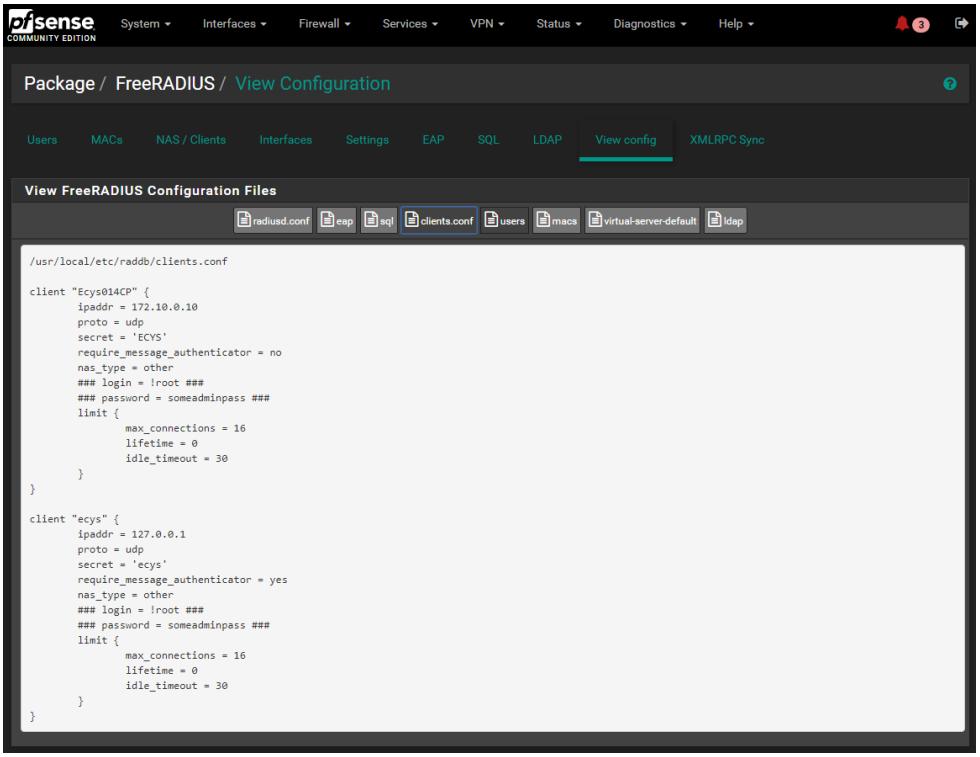
Figura 18. **Archivo de configuración de módulo SQL para el servidor FreeRADIUS**



Fuente: elaboración propia, empleando FreeRADIUS.

A continuación, se presenta la configuración de los clientes NAS como proveedores, especificando la IP de cada uno de los puntos de acceso inalámbrico disponibles para la conexión con los usuarios.

Figura 19. **Configuración de clientes NAS en servidor FreeRADIUS, como proveedores del servicio portal cautivo para la red LAN de los laboratorios**



Fuente: elaboración propia, empleando FreeRADIUS.

A continuación, se presenta el detalle de la configuración del cliente NAS como proveedor principal de servicio del portal cautivo.

Tabla XVII. **Detalle de configuración de cliente NAS, proveedor principal del servicio portal cautivo dentro de la red LAN**

Atributo de configuración	Descripción	Valor asignado
Ipaddr	Dirección IP de la red del dispositivo que provee el servicio de difusión de la red y acceso de usuarios.	172.10.0.10
Proto	Protocolo de red utilizado para la intercomunicación con los usuarios y autenticación de estos.	udp
Secret	Llave de acceso que identifica al dispositivo como proveedor de servicio ante el servidor FreeRADIUS e identifica el origen a la solicitud o paquete de información.	ECYS
require message authenticator	Opción que habilita la solicitud de mensajes extra a la solicitud de conexión desde el autenticador FreeRADIUS.	No
nas_type	Tipo de proveedor de servicio, permite el uso de un catálogo de parámetros específico para políticas de red. El valor por defecto other permite aplicar políticas de administración definidas por el servidor FreeRADIUS, establecidos en la configuración de la zona de servicio para el portal cautivo.	other
Limit	Parametro de configuración que especifica los límites de tiempo y valores de frontera, tiempo de vida y tiempo de espera para caducidad de sesiones.	• max_connections=16 • lifetime = 0 • idle_timeout = 30

Fuente: elaboración propia.

Los valores de configuración definidos dentro de un cliente NAS no son permanentes ni definitivos porque la configuración establecida dentro de la zona de servicio para el portal cautivo, establecerá las políticas con mayor prioridad que cualquier otra configurada desde el servidor FreeRADIUS, atributo de base de datos o configuración de cliente NAS.

2.3.6. Configuración de la infraestructura de red del proyecto

La infraestructura de red para la implementación de la solución consta de hardware y software que debe ser instalado y configurado de manera específica para poder brindar el servicio y ofrecer la funcionalidad requerida.

2.3.6.1. Diseño de la DMZ

Para llevar a cabo la implementación de la DMZ se contó con el apoyo de personal de procesamiento de datos, Ing. Jaime Cabrera y el técnico Mauricio Chávez, logrando así estandarizar el servicio prestado por el portal cautivo con la infraestructura de red existente en la universidad de San Carlos de Guatemala. Como parte de la estandarización de la red interna a la del proveedor, dirección de procesamiento de datos de la Universidad de San Carlos de Guatemala, se establecieron un rango de direcciones IP utilizadas para cada uno de los servicios, el rango de direcciones que deberá utilizar la red interna y servicios, el número de VLAN. A continuación, se presenta la tabla con el detalle de la información de estandarización de la infraestructura de red.

Tabla XVIII. **Detalle de configuración de red interna y servicios para estandarización con la red del proveedor**

Característica de configuración	Valor de configuración	Valor por asignar
Rango de direcciones IP a asignar por el servidor DHCP de la red interna.	Dirección IP	Rango de red 172.10.0.0
Tipo de clase de la red interna.	Mascara de red	Clase B = / 16 = 65,534 *host*
Numero de red de área local virtual.	VLAN / VLAN Tag	88
Nombre de identificación para la red de área local virtual.	Nombre VLAN	cautivoecys
Número de red de área local virtual del proveedor de servicio de internet.	VLAN / VLAN Tag	706
Nombre de la red de área local virtual del proveedor de servicio de internet.	VLAN / VLAN Tag	RiusacAPs
Direcciones IP para receptores de servicio de internet.	Dirección IP para servidor de aplicaciones web, base de datos y corta fuegos.	• Servidor de aplicaciones web: 10.56.0.41 / 16 • Servidor de base de datos: 10.56.0.40 / 16 • Servidor de corta fuegos: 10.56.0.11 / 16 • Enlace de red virtual proxmox: •

Fuente: elaboración propia.

Es importante remarcar que resultado de la estandarización de la red interna conforme a los parámetros de procesamiento de datos la red WAN de la DMZ tiene conexión por la interfaz marcada con la dirección IP 10.56.0.11/16 existente

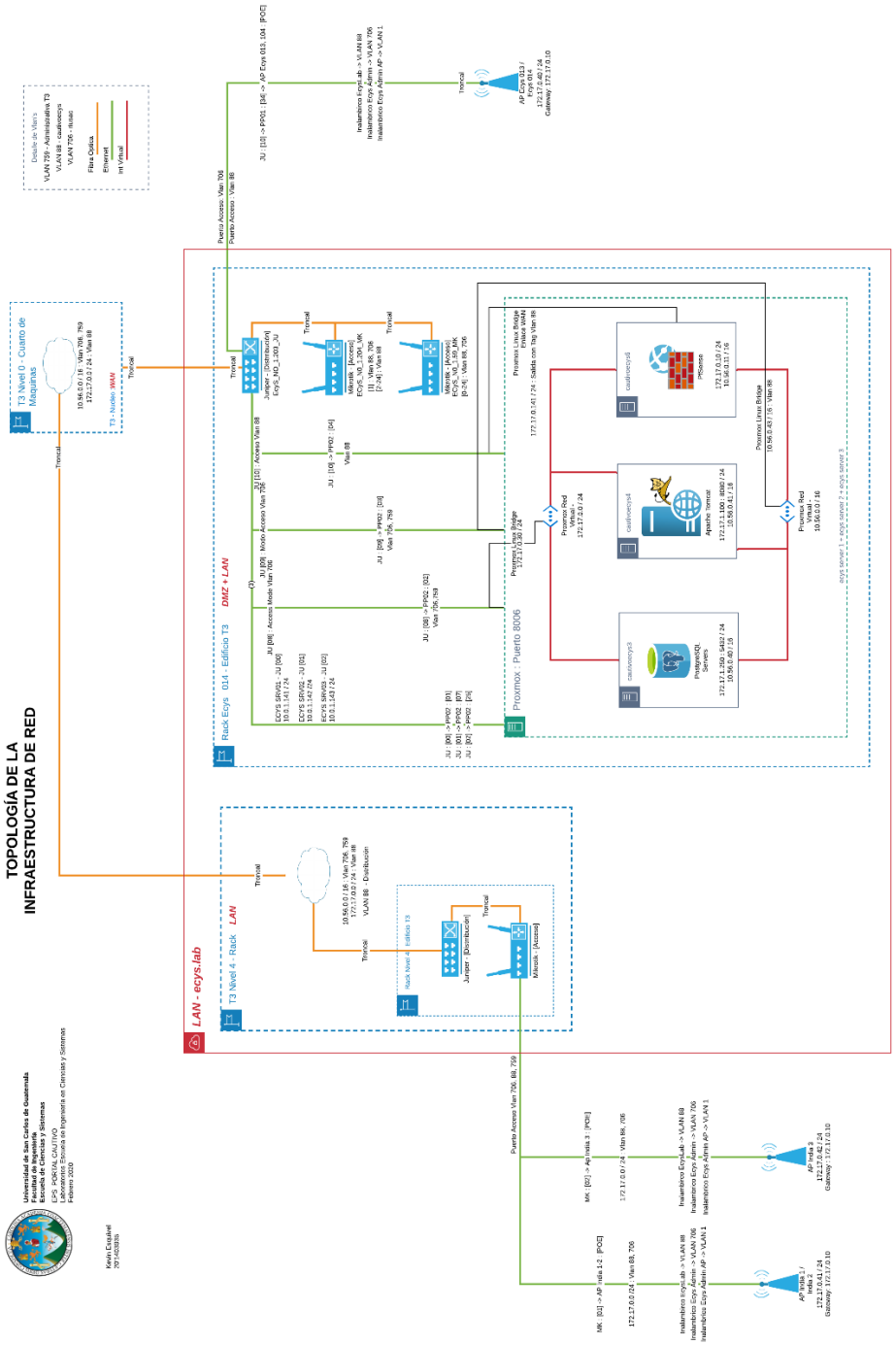
en el servidor de corta fuegos, y que el rango de direcciones IP a asignar a la red interna o LAN en los laboratorios será la 172.10.0.0/16 para evitar conflicto con el servidor DNS ya que existen servidores dentro de la red del proveedor RiusacAPs que están marcadas con direcciones IP existentes en el rango 172.10.0.0 y establecer direcciones en el mismo rango de la red interna puede ocasionar posibles conflictos de acceso.

El cableado estructurado utilizado es exactamente el existente porque la oficina de Procesamiento de Datos de la Universidad ya tenía contemplado y documentado un diseño de red y distribución de puertos para los laboratorios. El diseño se acopló al actual diseño de núcleo, distribución y acceso para una infraestructura de red.

Debido a que la configuración de la DMZ es a nivel lógico por medio de la implementación de VLAN's, físicamente no está distribuida por medio del modelo de implementación físico de hardware tradicional sino por medio de configuración sobre hardware y software que permite o no el paso del tráfico de la red por los puertos configurados según el acceso a la VLAN definida para su uso y acceso.

A continuación, se presenta el diagrama correspondiente al diseño de la topología y de la red interna (LAN) para los laboratorios.

Figura 20. **Topología de red de la solución, generado durante la implementación de la solución en enero y febrero 2020**



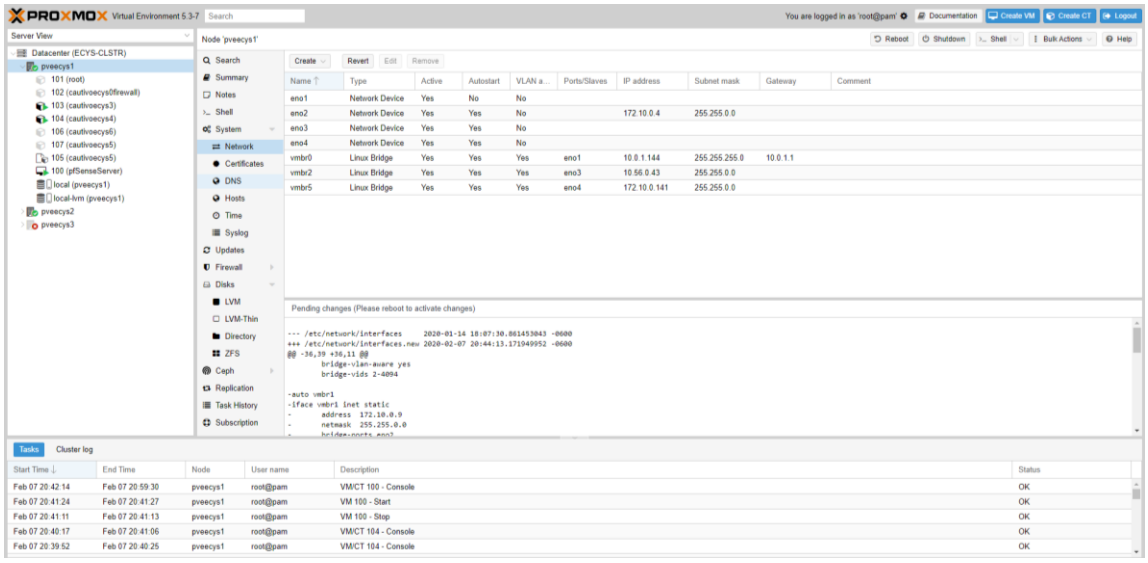
Fuente: elaboración propia, empleando Lucidchart en su versión web.

2.3.6.2. Asignación de interfaces de red virtuales

Parte importante de la implementación de la DMZ para los laboratorios por medio de hardware y software, es la asignación de interfaces de red virtuales y físicas para los servidores dentro del sistema de virtualización PROXMOX.

A continuación, se presenta la configuración realizada de las interfaces de red físicas para cada servidor utilizado en la solución y su asignación dentro del a red virtual como enlaces de tipo puente para sistemas operativos Linux.

Figura 21. **Configuración de las interfaces de red para el servidor de PROXMOX y máquinas virtuales o contenedores**



Fuente: elaboración propia, empleando PROXMOX 5.3.7.

Así mismo a continuación se presenta la tabla que detalla cada una de las funciones de cada interfaz de red configurada.

Tabla XIX. **Detalle de la configuración de interfaces de red del servidor PROXMOX**

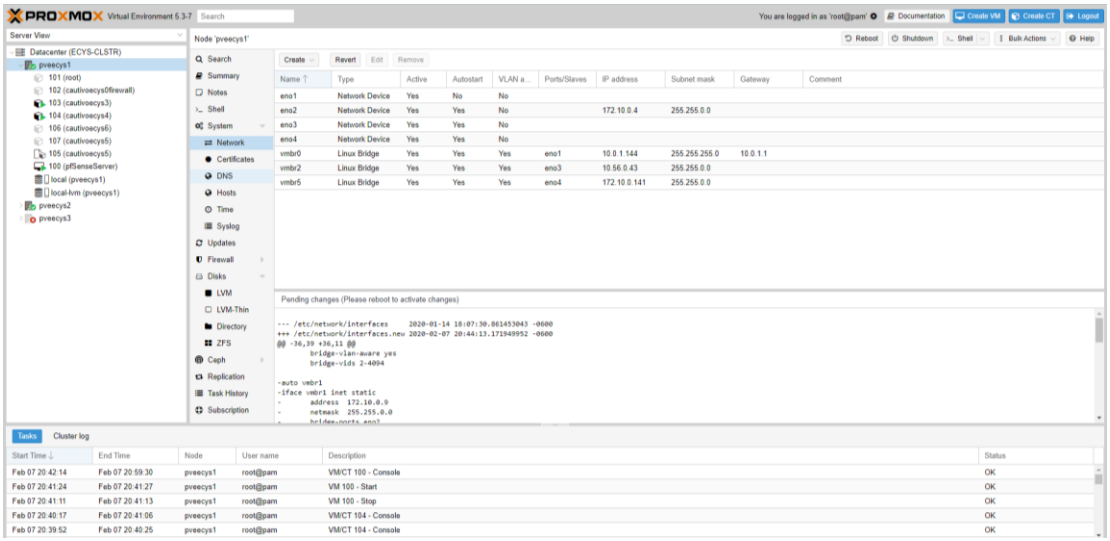
Interfaz de red	Tipo	Descripción	Asignación	Tráfico asignado
eno1	Física	Interfaz de red física número 1 del servidor físico ECYS-SRV0, con punto de conexión al puerto número 1 del *patch panel* PP02.	Sin asignación	Permite el paso tráfico de red perteneciente a cualquier rango de direcciones IP.
eno2	Física	Interfaz de red física número 2 del servidor físico ECYS-SRV0, con punto de conexión al puerto número 2 del *patch panel* PP02.	Dirección IP: 172.10.0.4 / 16	Permite el paso de tráfico de cualquier tipo siempre y cuando sea de la red 172.10.0.0 /16
eno3	Física	Interfaz de red física número 3 del servidor físico ECYS-SRV0, con punto de conexión al puerto número 3 del *patch panel* PP02.	Sin asignación	Permite el paso tráfico de red perteneciente a cualquier rango de direcciones IP.
eno4	Física	Interfaz de red física número 4 del servidor físico ECYS-SRV0, con punto de conexión al puerto número 4 del *patch panel* PP02.	Sin asignación	Permite el paso tráfico de red perteneciente a cualquier rango de direcciones IP.
vmbr0	Puente lógico Linux	Interfaz de conexión virtual para entrada y salida de tráfico de contenedores y máquinas virtuales creados en PROXMOX.	Interfaz física: eno1	Dirección IP pública: 10.0.1.144 / 16

Continuación de la tabla XIX.

vmbr2	Puente lógico Linux	Interfaz de conexión virtual para entrada y salida de tráfico de contenedores y máquinas virtuales creados en PROXMOX.	Interfaz física: eno3	Dirección IP: 10.56.0.43 / 16. Permite el tráfico de la VLAN 706 y proveniente de cualquier equipo dentro de la red 10.56.0.0 / 16
vmbr5	Puente lógico Linux	Interfaz de conexión virtual para entrada y salida de tráfico de contenedores y máquinas virtuales creados en PROXMOX.	Interfaz física: eno4	Dirección IP: 172.10.0.141 / 16 Permite el tráfico de la VLAN 88 y proveniente de cualquier equipo dentro de la red 172.10.0.0 / 16

Fuente: elaboración propia.

Figura 22. **Configuración de las interfaces de red y puentes para interconexión del contenedor utilizado como servidor de base de datos**



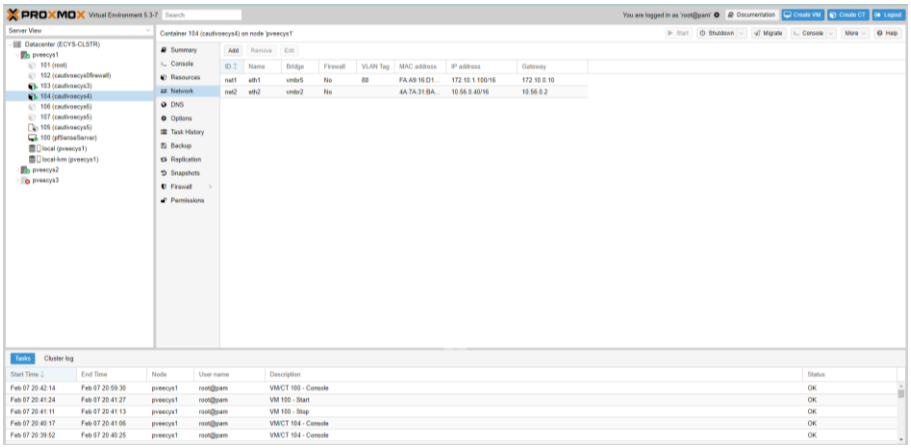
Fuente: elaboración propia, empleando PROMOX 5.3.7.

Tabla XX. **Detalle de la configuración de interfaces de red para el servidor de base de datos**

Interfaz de red	Nombre de interfaz	Asignación de interfaz virtual	Dirección IP	*Gateway*
net1	eth1	• Interfaz: vmbr5 • Tag de vlan: 88 • Permite tráfico de la red 172.10.0.0 / 16	172.10.1.250 / 16	172.10.0.10
net2	eth2	• vmbr2 • Permite tráfico de la red 10.56.0.0 / 16	10.56.0.41 / 16	10.56.0.2

Fuente: elaboración propia.

Figura 23. **Configuración de las interfaces de red y puentes para interconexión del contenedor utilizado como servidor de aplicaciones**



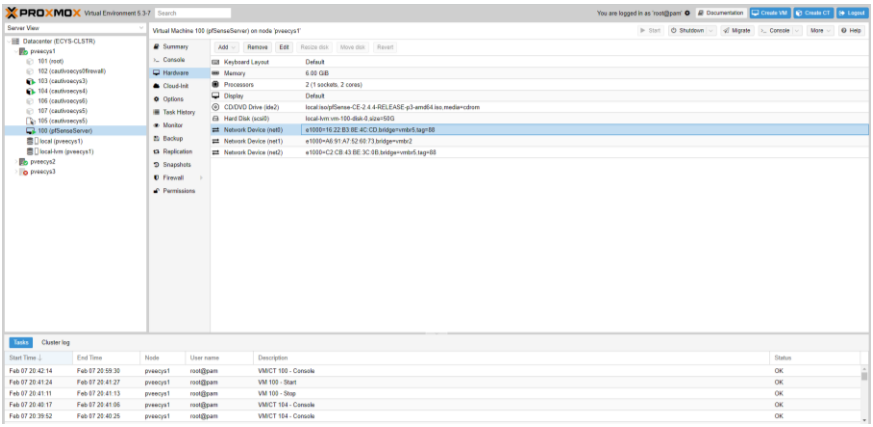
Fuente: elaboración propia, empleando PROMOX 5.3.7.

Tabla XXI. **Detalle de la configuración de interfaces de red para el servidor de base de datos**

Interfaz de red	Nombre de interfaz	Asignación de interfaz virtual	Dirección IP	*Gateway*
net1	eth1	• Interfaz: vmbr5 • Tag de vlan: 88 • Permite tráfico de la red 172.10.0.0 / 16	172.10.1.100 / 16	172.10.0.10
net2	eth2	• vmbr2 • Permite tráfico de la red 10.56.0.0 / 16	10.56.0.40 / 16	10.56.0.2

Fuente: elaboración propia.

Figura 24. **Configuración de las interfaces de red y puentes para interconexión de la máquina virtual utilizado como servidor de corta fuegos**



Fuente: elaboración propia, empleando PROXMOX 5.3.7.

Tabla XXII. **Detalle de la configuración de interfaces de red para el servidor de base de datos**

Interfaz de red	Nombre de interfaz	Asignación de interfaz virtual	Dirección IP	*Gateway*
net0	eth1	• Interfaz: vmbr5 • Tag de vlan: 88 • Permite únicamente el tráfico de la red 172.10.0.0 / 16	172.10.1.100 / 16	172.10.0.10
et1	eth2	• vmbr2 • Permite tráfico de la red 10.56.0.0 / 16	10.56.0.40 / 16	10.56.0.2

Fuente: elaboración propia.

2.3.6.3. Configuración de dispositivo de conmutación de red para aislamiento de la red

Después de la elaboración de la configuración de todos los servidores tanto físicos como virtualizados que serán utilizados para dar solución al proyecto se realizó la configuración de los dispositivos de conmutación y enrutamiento los cuales consta de un switch marca Juniper y dos switch marca Mikrotik que son los dispositivos necesarios para enviar el tráfico por la red cableada del edificio T3. La configuración de salida del tráfico por la red se realizó con apoyo de persona de la oficina de Procesamiento de Datos de la Universidad de San Carlos de Guatemala, ya que el tráfico para ser enviado a los laboratorios del cuarto y quinto nivel deben pasar por medio del cableado de fibra óptica de los edificios era necesario configurar la VLAN y enlaces troncales necesarios para que el servicio fuera de los servidores del laboratorio al gabinete en el cuarto nivel encargado de distribuir el servicio de internet.

Debido a que en el conmutador Juniper existen varios servicios integrados únicamente se detalla a continuación la configuración de los puertos que corresponde a los servicios que corresponden al portal cautivo, siendo estos primeramente la configuración de puertos en modo acceso y troncal para permitir el tráfico en los dispositivos y que esta no se distribuya de forma descontrolada por toda la red tanto interna de los laboratorios como de los edificios.

A continuación, se presenta de forma detallada la configuración de los puertos del conmutador Juniper ECyS_NO_1.203_JU.

Tabla XXIII. **Detalle de configuración de conmutador Juniper ECyS_NO_1.203_JU, realizado durante el mes de febrero 2020**

Número de puerto	Configuración	Descripción de funcionalidad
0-7	Modo troncal para acceso a la VLAN 759 y VLAN 706	Puertos utilizados para dar acceso al recurso de internet y red administrativa, los puertos del 1 al 3 están siendo utilizados para proveer de servicio a los servidores físicos del servidor de virtualización PROXMOX.
8-9	Modo acceso VLAN 706	Puertos utilizados para dar acceso al recurso de internet a los servidores internos de base de datos, aplicaciones y corta fuegos.
10	Modo acceso VLAN 88	Puerto utilizado para recibir el tráfico generado por el servicio de portal cautivo y distribuirlo dentro del conmutador Juniper para ser así enviado a cada uno de los puertos receptores tanto de los laboratorios del nivel 0 como de los correspondientes al nivel 4 y 5 del edificio T3.
11	Modo acceso VLAN 706	Puerto de servicio utilizado para proveer el servicio de internet a la televisión de la oficina de la coordinación de los laboratorios.
12	Modo acceso VLAN 706	Puerto de pruebas con acceso a la VLAN 706 para tener acceso a *pool* DHCP e internet por medio de la red RiusacAps.
13	No aplica a portal cautivo	
14	Modo acceso VLAN 88	Puerto de pruebas con acceso a la VLAN 88, por medio de este se pueden realizar las pruebas necesarias para llevar a cabo la comprobación de la configuración de puertos y distribución del servicio del portal cautivo de una manera sencilla sin necesidad de tener un punto de acceso inalámbrico.

Continuación de la tabla XXIII.

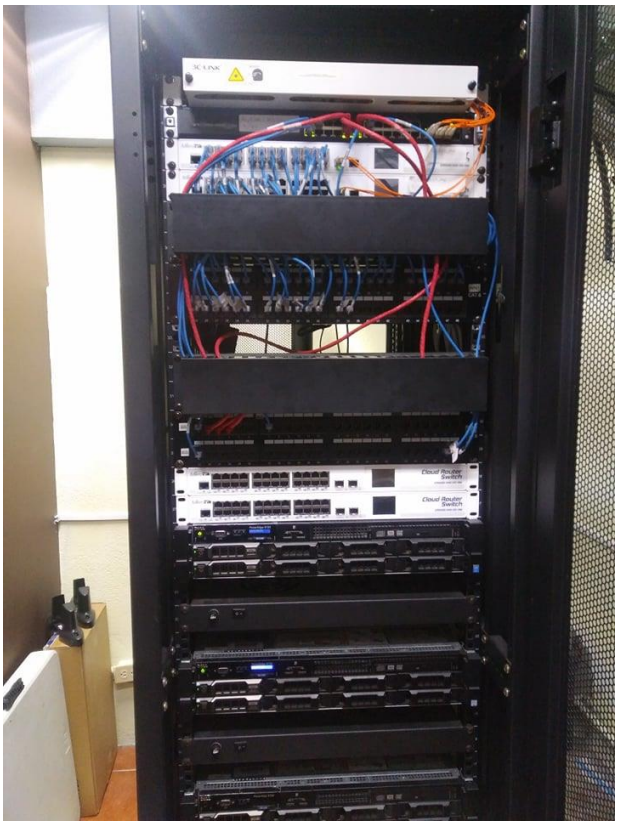
15-20	No aplica a portal cautivo	
21	Modo acceso VLAN 88	Puerto para proveer servicio de internet por medio de servidores y red del portal cautivo.
22	Modo acceso VLAN 88	Puerto para proveer servicio de internet por medio de servidores y red del portal cautivo.

Fuente: elaboración propia.

Figura 25. **Cableado estructurado del conmutador Juniper ECyS_NO_1.203_JU**

Fuente: elaboración propia.

Figura 26. **Cableado estructurado del rack de servidores**



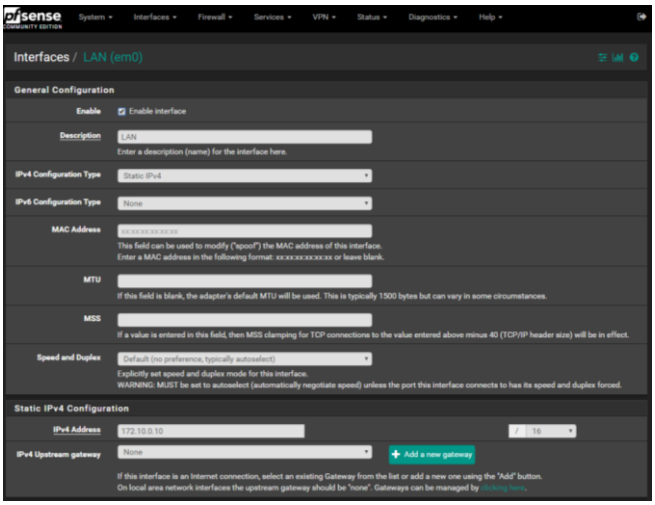
Fuente: elaboración propia.

2.3.6.4. Configuración de red LAN

Por medio del servidor de corta fuegos Pfsense se realizó la configuración de la red LAN o red interna para los laboratorios, a la cual todos aquellos que estén conectados deberán realizar inicialmente su proceso de autenticación por medio del portal cautivo para hacer uso del internet.

A continuación, se detalla la configuración de la red LAN en el servidor de corta fuegos.

Figura 27. **Configuración de interfaz red para creación de red LAN**



Fuente: elaboración propia, empleando PfSense 2.4.4.

Tabla XXIV. **Detalle de configuración de red LAN**

Característica de configuración	Descripción	Valor asignado
Habilitar.	Habilita la creación de una red LAN y utiliza la interfaz asignada como salida del tráfico.	True
Descripción.	Descripción que identifica y define a la red.	LAN
Tipo de configuración IPv4.	Valor que define el tipo de asignación que tendrá la interfaz de salida de la interfaz LAN, en este caso existen muchas opciones sin embargo para establecer un Gateway dentro de la red y su correcto funcionamiento se le asigna una IP estática.	IPv4 estático

Continuación de la tabla XXIV.

Tipo de configuración IPv6.	Valor que define qué tipo de asignación tendrá la interfaz de salida de versión de protocolo IPv6 para la red LAN, a pesar de la gran cantidad de opciones que existen se opta por no realizar una asignación ya que el protocolo IP en su versión 6 no es muy utilizado ni implementado.	Ninguno
Dirección MAC.	Realiza la asignación de una dirección MAC a la interfaz utilizada para difusión y Gateway de la red LAN. Se asigna el valor por defecto de esta manera PfSense asignará un valor random que no se encuentre repetido dentro de la red.	xx:xx:xx:xx:xx:xx
MTU.	No aplica	
MSS.	No aplica	
Speed and Duples.	Asigna el valor explícito de velocidad y modo duplicado para esta interfaz de red en caso se utilice para tener un mayor rango de	Por defecto (autoselección)
Dirección IPv4.	Dirección IP asignada a la interfaz utilizada para difusión de la red LAN. Esta deberá ser la dirección IP de Gateway utilizada para difusión de la red y conexión con los servicios de DNS.	172.10.0.10 / 16
Dirección IPv4 de la puerta de enlace de difusión.	Dirección IP de la interfaz de red utilizada para conexión con el servicio de internet. Por defecto se realizará el ruteo de servicio de internet con el proveedor WAN.	Ninguno

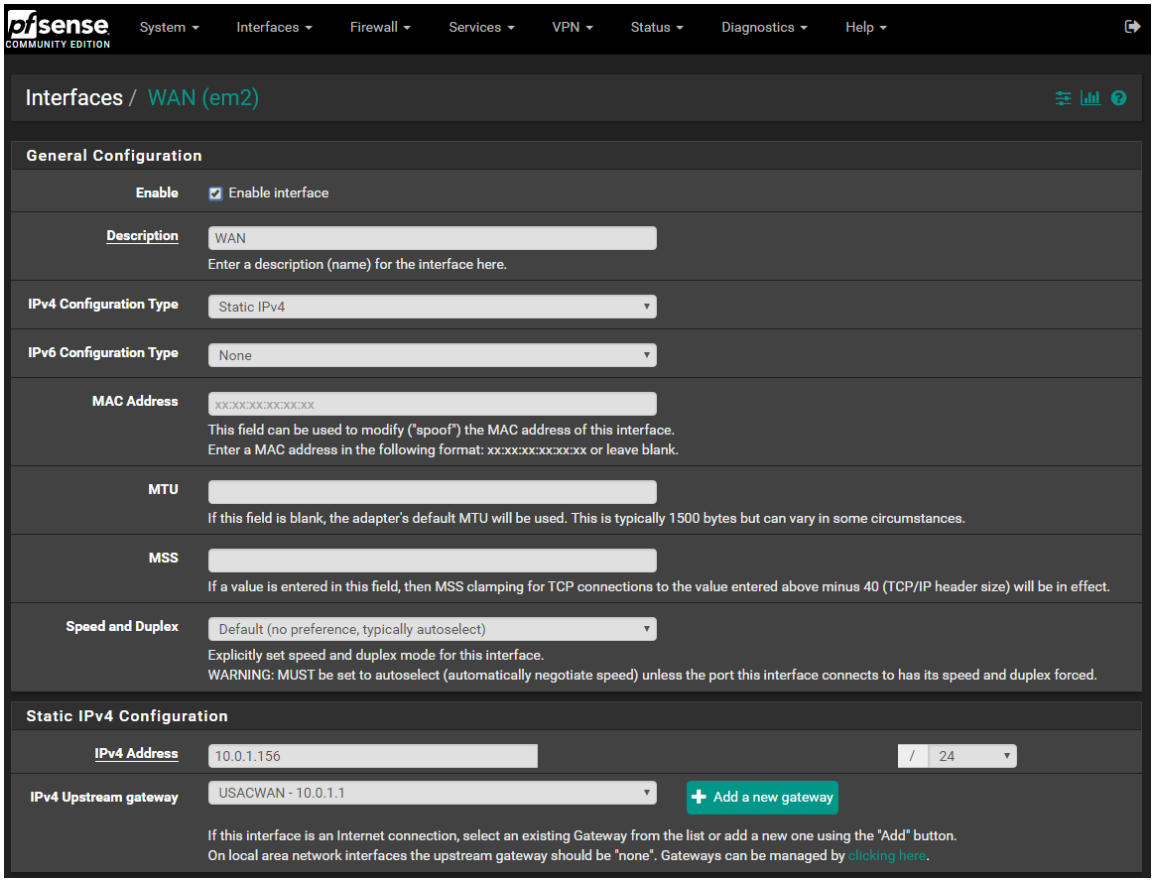
Fuente: elaboración propia.

2.3.6.5. Configuración de red WAN

Se realizó la configuración del servidor de red WAN por medio de la consola de administración de interfaces de red del servidor de corta fuegos PfSense de la misma manera que la red LAN.

A continuación, se presenta el detalle de la configuración y los resultados de esta.

Figura 28. **Configuración de interfaz red para creación de red WAN**



Fuente: elaboración propia, empleando PfSense 2.4.4.

Tabla XXV. **Detalle de configuración de red WAN**

Característica de configuración	Descripción	Valor asignado
Habilitar	Habilita la creación de una red WAN y utiliza la interfaz asignada como proveedor del servicio de internet.	True
Descripción	Descripción que identifica y define a la red.	WAN
Tipo de configuración IPv4	Valor que define el tipo de asignación que tendrá la interfaz de salida de la interfaz WAN, en este caso existen muchas opciones sin embargo para establecer un Gateway de ruteo de tráfico LAN hacía WAN para proveer de servicio dentro de la red se le asigna una IP estática.	IPv4 estático
Tipo de configuración IPv6	Valor que define que tipo de asignación tendrá la interfaz de salida de versión de protocolo IPv6 para la red WAN, a pesar de la gran cantidad de opciones que existen se opta por no realizar una asignación ya que el protocolo IP en su versión 6 no es muy utilizado ni implementado.	Ninguno

Continuación de la tabla XXV.

Dirección MAC	Realiza la asignación de una dirección MAC a la interfaz utilizada para proveer servicio de internet a la interfaz de red LAN por medio de la WAN. Se asigna el valor por defecto de esta manera PfSense asignará un valor random que no se encuentre repetido dentro de la red.	xx:xx:xx:xx:xx:xx
MTU	No aplica	
MSS	No aplica	
Speed and Duplex	Asigna el valor explícito de velocidad y modo duplicado para esta interfaz de red en caso se utilice para tener un mayor rango de velocidad de transferencia.	Por defecto (autoselección)
Dirección IPv4	Dirección IP asignada a la interfaz para poder obtener el servicio de internet del proveedor de servicio hacía la red LAN. Esta deberá ser la dirección IP de Gateway utilizada para difusión de la red y conexión con los servicios de DNS.	10.56.0.11 / 16
Dirección IPv4 de la puerta de enlace de difusión	Dirección IP de la interfaz de red utilizada para conexión con el servicio de internet.	10.56.0.2

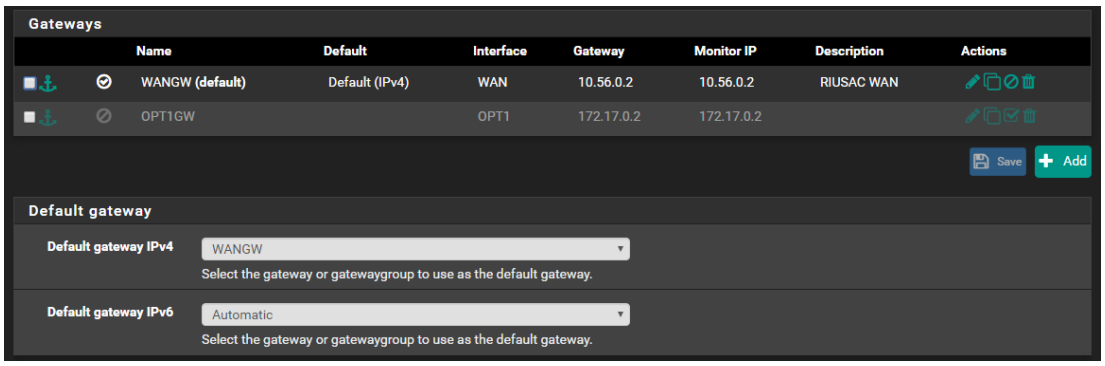
Fuente: elaboración propia.

2.3.6.6. Asignación de interfaz de ruteo para el tráfico de red LAN hacía WAN para proveer de servicio de internet

Para llevar a cabo la implementación del proyecto es necesaria la implementación de una zona de red desmilitarizada, en la que el tráfico desde la red LAN será resuelto por el proveedor de servicio de la red WAN. Parte importante de la creación e implementación de una DMZ es la separación lógica de una red con respecto a su proveedor de servicios, siendo LAN la red interna y WAN la red del proveedor de servicio con comunicación de LAN a WAN, pero sin existir la posibilidad de comunicación desde la WAN hacía la LAN. La implementación del portal cautivo por medio de un servidor de corta fuegos permite la creación lógica de un ruteo entre interfaces de red asignadas a una red LAN y WAN.

A continuación, se presenta la configuración de ruteo de tráfico de red entre LAN y WAN en el servidor de corta fuegos PfSense.

Figura 29. **Configuración de ruteo de interfaces LAN para brindar un proveedor de red WAN**

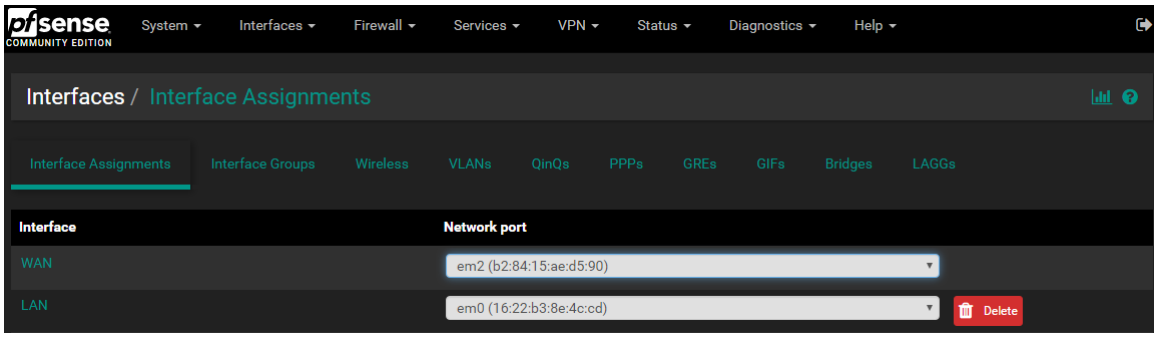


Fuente: elaboración propia, empleando PfSense 2.4.4.

2.3.6.7. Asignación de interfaces de red a red LAN y WAN

A continuación, se presenta la asignación de las interfaces de red virtual creadas en el sistema de virtualización PROXMOX a la red LAN y WAN, esta configuración determina hacía donde el servidor de corta fuegos enviará el tráfico de red.

Figura 30. **Asignación de interfaces de red virtual a red LAN y WAN**

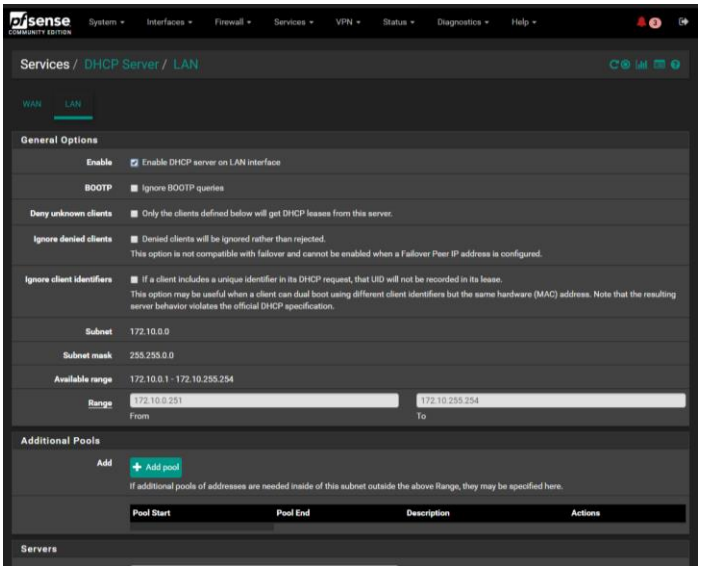


Fuente: elaboración propia, empleando PfSense 2.4.4.

2.3.6.8. Configuración de servidor DHCP para la red LAN

El servidor de configuración dinámica de direcciones IP, permite la asignación de direcciones IP de forma dinámica y automatizada a los dispositivos que se conecten a los puntos de acceso inalámbricos. Todos los dispositivos que se les asigne una dirección IP del *pool* del servidor DHCP serán automáticamente añadidos a la zona de portal cautivo y se les solicitará su autenticación para hacer uso de la red y del recurso de internet.

Figura 31. **Configuración de servidor de configuración dinámica de direcciones IP para la red LAN, implementado en el servidor de corta fuegos PfSense**



Fuente: elaboración propia, empleando PfSense 2.4.4.

Tabla XXVI. **Detalle de configuración de servidor DHCP para la red LAN de la solución**

Característica de configuración	Descripción	Valor asignado
Habilitar	Opción que permite la habilitación del servidor DHCP dentro del dominio para la red LAN de los laboratorios.	Habilitado
Subred	Valor autoasignado dependiendo de la red para la que se configure el servidor DHCP que permite visualizar sobre qué red se establecerá el servicio de configuración dinámica de dirección IP.	172.10.0.0
Máscara de subred.	Mascará de subred de acuerdo con la clase de red de la interfaz de red sobre la que se prestará el servicio de DHCP.	255.255.0.0 = /16

Continuación de la tabla XXVI.

Rango disponible	Rango de direcciones IP que se encuentra disponible para uso en la red establecida.	172.10.0.1 a 172.10.255.254
Servidor DNS	Dirección IP del servidor DNS utilizado para resolución de nombres de dominio tanto locales como de reenvió al proveedor.	172.10.0.10
Gateway	Dirección IP de Gateway de la red	172.10.0.10
Nombre de dominio.	Nombre que identifica al dominio de la red interna y a los huéspedes de esta.	EcysCP

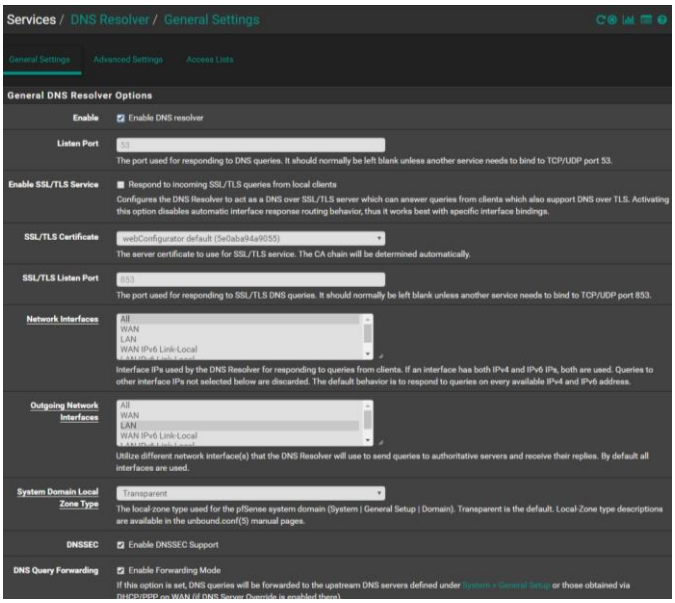
Fuente: elaboración propia.

2.3.6.9. Configuración de servidor de resolución DNS para la red LAN

La implementación de un servidor de resolución de nombre de dominio permite la traducción de direcciones IP en direcciones URL que pueden ser accedidas por cualquier usuario directamente desde su navegador sin embargo en modelos de topología de red para zona desmilitarizada permite la traducción de direcciones IP locales en dirección URL locales sin salir directamente al proveedor para su consulta, su principal funcionalidad como resolutor de peticiones es la de enviar el tráfico de la red LAN hacía la red WAN y poder reconocer su origen y destino local previo a su consulta con el proveedor de servicio de internet.

Se presenta a continuación la configuración e implementación de un servidor de resolución de nombres de dominio desde el servidor de corta fuegos PfSense para la solución del proyecto.

Figura 32. **Configuración de servidor DNS resolver, realizado durante el mes de enero 2020**



Fuente: elaboración propia, empleando PfSense 2.4.4.

Tabla XXVII. **Detalle de configuración de servidor DNS resolver para la red LAN**

Característica de configuración	Descripción	Valor asignado
Habilitar	Determina si el servidor DNS está habilitado para una interfaz de red especifica.	Habilitado
Puerto de escucha	Puerto por el cual el servicio escuchará u obtendrá las solicitudes.	53
Interfaz de red	Interfaz de red IP utilizada por el servidor de nombres de dominio para responder a las solicitudes y consultas de los clientes.	Todas

Continuación de la tabla XXVII.

Interfaz de red de salida o respuesta.	Interfaz de red IP por la cual el servidor de resolución de nombres de dominio realizará responderá a las consultas de los clientes.	LAN
Tipo de sistema de dominio local.	Establece el tipo de zona local que será utilizada por el servidor de nombres de dominio de PfSense.	Transparente
DNSSEC	Establece si la zona de nombres de dominio podrá o no soportar las extensiones de nombre de dominio de seguridad.	Habilitado
Reenvió de consultas DNS.	Opción que permite al servidor DNS el reenvío de las consultas de tráfico que reciba.	Habilitado

Fuente: elaboración propia.

2.3.7. Implementación del portal cautivo en la nueva red interna y DMZ de los laboratorios por medio del servidor de corta fuegos PfSense

La creación de una zona desmilitarizada, así como una red interna contempla todos los aspectos técnicos y de administración del tráfico de red para dar soporte a la implementación de un protocolo de autenticación, autorización y contabilidad permitiendo a su vez establecer todo el entorno de ejecución, administración y mantenimiento de un portal cautivo para un servicio de red local.

2.3.7.1. Configuración de zona de portal cautivo

Se le denomina zona de portal cautivo a la definición independiente de un portal para una interfaz separada en específico. La zona de portal cautivo también

determina la configuración, comportamiento del portal cautivo, y a qué red LAN serán aplicadas las políticas del portal cautivo.

A continuación, se detalla la configuración de la zona de portal cautivo que se aplicará a la red LAN de los laboratorios y en donde los usuarios deberán autenticarse para ingresar, esto aplica tanto a los dispositivos de usuarios conectados por medio de puertos *ethernet* o puntos de acceso inalámbricos.

Tabla XXVIII. **Detalle de configuración de la zona de portal cautivo ECYS014**

Característica de configuración	Descripción	Valor asignado	Aplica
Habilitar	Habilita o deshabilita la zona de portal cautivo dentro de una red LAN. La desactivación permitirá el uso de la red a cualquier usuario y por contraparte la habilitación solicitará a cada usuario la autenticación previa a su ingreso a la red.	True o habilitado.	No
Interfaces	Valor que define sobre que interfaz de red será desplegado el portal cautivo.	LAN	No
Número máximo de conexiones concurrentes.	Define cuantos dispositivos podrá utilizar al mismo tiempo un usuario.	1	No
Idle timemout	Valor que define el tiempo en minutos de espera después de la desconexión de un usuario de la red para ser cerrada su sesión.	3	Si
Hard timeout	Tiempo de sesión, después de la autenticación de un usuario tendrá acceso a la red y los recursos de internet por el tiempo establecido en minutos.	Sin asignar	Si

Continuación de la tabla XXVIII.

Traffic quota	Valor que define en megabytes la cantidad de paquetes de descarga y carga que un usuario tiene disponible por cada sesión.	Sin asignar	No
URL de redirección después de la autenticación.	Indica la dirección URL a la cual los usuarios serán redireccionados después de que su autenticación sea exitosa.	https://dtt-ecys.org	Si
Autenticación concurrente de usuarios.	Habilita la autenticación concurrente de usuarios a la red para que múltiples dispositivos puedan estar activos con un mismo usuario.	Deshabilitado	No
Restricción de ancho de banda por usuario.	Habilita la restricción del ancho de banda disponible para cada usuario, esto aplica tanto para la carga como descarga de datos.	Habilitado	Si
Ancho de banda de descarga disponible (kbit/s).	Si la restricción de ancho de banda está disponible, este valor define el valor número del ancho de banda en kbits por segundo que un usuario tiene disponible. El valor de asignación de megabits por segundo deberá ser considerado como 1 000 kilobits por segundo es equivalente a 1 megabit por segundo de ancho de banda disponible.	1 000	Si
Utilizar una página personalizada de portal cautivo.	Habilita el uso de una página web personalizada de portal cautivo.	Habilitado	No
Servidor de autenticación.	Define el servidor de autenticación a utilizar.	Servidor de FreeRADIUS.	No

Continuación de la tabla XXVIII.

Ancho de banda de carga disponible (kbit/s).	Si la restricción de ancho de banda está disponible, este valor define el valor número del ancho de banda en kbits por segundo que un usuario tiene disponible. El valor de asignación de megabits por segundo deberá ser considerado como 1 000 kilobits por segundo es equivalente a 1 megabit por segundo de ancho de banda disponible.	1 000	Si
Contenido de portal.	Opción que permite subir un archivo con extensión html o php que se presentará como página principal de autenticación del portal cautivo.	Archivo con extensión html.	No
Contenido de la página de error de autenticación.	Opción que permite la carga de un archivo con extensión html o php para mostrar en caso de error de autentición, para la implementación del proyecto se redirige a la página de registro de usuarios.	Archivo con extensión html.	No
Método de autenticación.	Define el método de autenticación de usuarios.	Utilizar un servidor de autenticación.	No
Identificar NAS	Nombre del identificar de cliente de difusión de la red.	Ecys014CP	No
RADIUS	Habilita el envío a servidor RADIUS los paquetes de contabilidad.	Habilitado	No

Continuación de la tabla XXVIII.

Formato de dirección MAC.	Establece el formato en que se registrarán las direcciones MAC, se establece la opción por defecto debido a que asigna un formato que reconoce FreeRADIUS y cualquier dispositivo de enrutamiento.	Por defecto	No
Servidor de contabilización.	Establece hacía qué servidor RADIUS se enviarán los paquetes de contabilización, en caso se desee trabajar con más de uno.	Servidor de Autenticación RADIUS.	No
Envio de actualizaciones de contabilización.	Establece la forma en que se actualizará la información sobre el consumo de paquetes de carga y descarga de datos que ha realizado un cliente.	Interino	No
Estilo de contabilización.	Establece la forma en que se realizará la contabilización y determina en qué sentido se realizará la contabilización de paquetes, si está habilitado RADIUS considera los paquetes del cliente como de descarga y los que reciba del mismo como de subida.	Habilitado	No
Contabilización del tiempo de actualización.	Habilita la contabilización de los tiempos de actualización por cada usuario y sesión.	Habilitado	No

Fuente: elaboración propia.

Todas las demás configuraciones no aplican a los requerimientos funcionales del portal cautivo por lo que no son detalladas y únicamente son ignoradas durante la configuración. Asimismo, se establece las políticas administrativas de la red que fueron incluidas dentro del sistema de administración.

2.3.7.2. Configuración de dispositivos para acceso inalámbrico a la red

Las instalaciones cuentan con los puntos de acceso inalámbricos Ruckus R710 para los laboratorios 013 y 014, otro dispositivo Ruckus R710 para los laboratorios India 1 e India 2 y un dispositivo Ruckus R310 para el laboratorio India 3. La configuración de estos permite el acceso del tráfico correspondiente a la VLAN que provee del servicio de portal cautivo, se detalla a continuación la configuración de los puntos de acceso inalámbricos disponibles para cada laboratorio.

Tabla XXIX. **Detalle de configuración de dispositivos de puntos de acceso inalámbricos**

SSID	Descripción	VLAN de acceso	Usuario destino
Ecys Lab	Punto de acceso inalámbrico para uso del internet inalámbrico en las instalaciones del laboratorio.	88	Estudiantes y usuarios de la red.
Ecys Admin	Punto de acceso inalámbrico habilitado para uso de internet inalámbrico desde el proveedor RiusacAPs directamente y no por medio del portal cautivo.	706	Administrador y coordinación de los laboratorios.

Continuación de la tabla XXIX.

Ecys Admin LAN	Punto de acceso para administración de los dispositivos de puntos de acceso Ruckus.	1	Administrador de la red y coordinación de los laboratorios.

Fuente: elaboración propia.

A continuación, se presenta la configuración de uno de los puntos de acceso inalámbrico dentro de los dispositivos Ruckus utilizados para brindar el servicio de internet inalámbrico dentro de las instalaciones de los laboratorios.

Tabla XXX. **Detalle de configuración de puntos de acceso Ecys Lab en onda de radio 2.4 en puntos de acceso inalámbrico Ruckus, realizado en febrero 2020**

Característica de configuración	Descripción	Valor asignado
Wireless network	Nombre de la red y punto de acceso inalámbrico.	EcysLab
Wireless Availability	Disponibilidad inalámbrica del punto de acceso.	Habilitado
Broadcast SSID	Habilita la difusión del nombre del punto de acceso en los dispositivos que estén en el radio de alcance del punto de acceso inalámbrico.	Habilitado
SSID	Nombre del punto de acceso que se enviará y mostrará en todos los dispositivos.	Ecys Lab
Packet Forward	Determina la forma en que se enviarán los paquetes que son recibidos y enviados por medio del dispositivo de punto de acceso inalámbrico.	Route to Wan

Continuación de la tabla XXX.

Hotspot Service	Indica el servicio de Hotspot que será utilizado por el punto de acceso para emisión de tráfico.	Ninguno
Access VLAN	Nombre del tag de VLAN al cual tendrán acceso los usuarios por medio del punto de acceso inalámbrico. Esta opción configura como puerto de acceso el tráfico que sea transmitido bidireccionalmente por el dispositivo hacia los usuarios y dispositivos.	88
Dynamic VLAN	Establece si el punto de acceso puede transmitir tráfico de red para números de VLAN que pueden cambiar en cualquier momento.	Deshabilitado
Insert DHCP option 92	Establece si se añade a la información de tráfico información adicional sobre el origen.	Deshabilitado
Client Fingerprinting	Habilita la verificación de usuarios por medio de huella digital.	Deshabilitado
Encryption Method	Determina el tipo de autenticación que se tendrá para el punto de acceso, esto no define la autenticación a la red para el portal cautivo sino únicamente al dispositivo.	WPA
WPA Version	Versión de encriptación que se utilizará para los usuarios conectados al dispositivo de puntos de acceso.	WPA+WPA2
WPA Authentication	Establece la forma en que se realizará la autenticación.	PSK
WPA Algorithm	Determina el tipo de algoritmo utilizado para la autenticación.	AES
Passphrase	Contraseña de conexión al dispositivo de punto de acceso inalámbrico.	Dato no disponible.

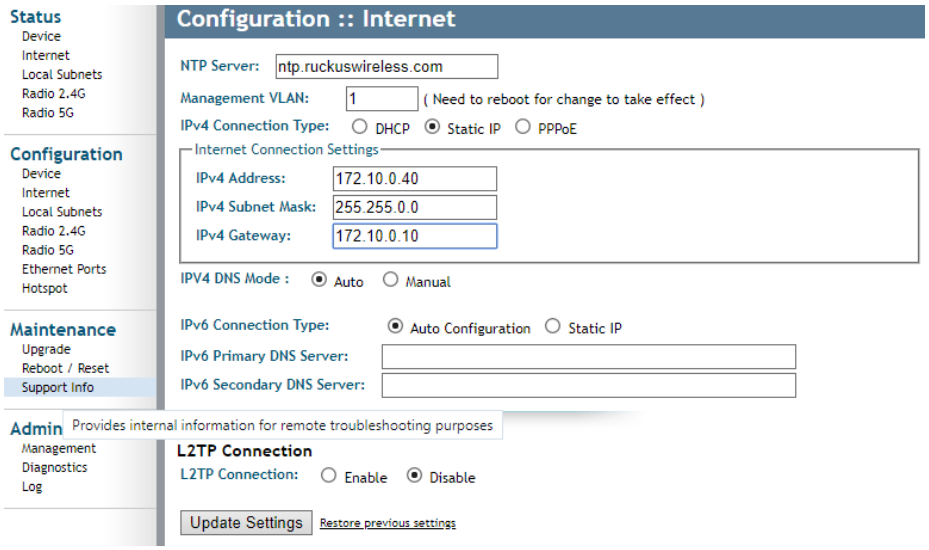
Fuente: elaboración propia.

2.3.7.3. Configuración de interfaz de red para recepción del tráfico de red desde el servidor de corta fuegos en los dispositivos de punto de acceso inalámbricos

Los dispositivos utilizados como punto de acceso a la red inalámbrica se comunican directamente con la capa de distribución y de acceso de la topología de red por medio de una de las dos interfaces ethernet de cada dispositivo.

Se detalla y presenta a continuación la configuración básica de los dispositivos de punto de acceso utilizados para la difusión del portal cautivo y recursos de internet inalámbrico.

Figura 33. **Configuración de dispositivo para asignación de dirección IP dentro de la red**



Fuente: elaboración propia, empleando Ruckus Wireless Admin R710 y R310.

Tabla XXXI. **Detalle de configuración de puntos de acceso inalámbrico**

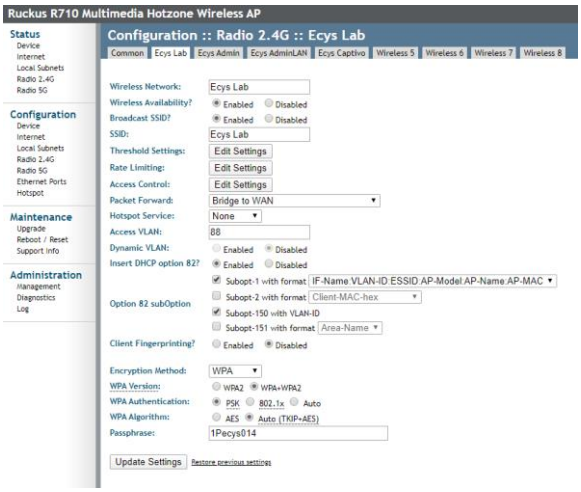
Característica de configuración	Descripción	Valor asignado
Management VLAN.	Valor de configuración que establece el identificador de VLAN que tiene acceso a la configuración del dispositivo por medio de un punto de acceso.	1
Tipo de conexión IPv4.	Tipo de asignación de dirección IP que permitirá la conexión y asignación con el dispositivo.	IP estática
Dirección IPv4.	Dirección IP del dispositivo para acceso a su configuración.	172.10.0.40
Mascara de red.	Mascara de subred utilizada por el segmento y dispositivo de red utilizado para configuración y acceso al dispositivo.	255.255.0.0
Dirección IPv4 de Gateway.	Dirección IP de la puerta de enlace utilizada para la intercomunicación y conexión con el punto de acceso y servidor de corta fuegos.	172.10.0.10

Fuente: elaboración propia.

2.3.7.4. Configuración de puntos de acceso inalámbricos

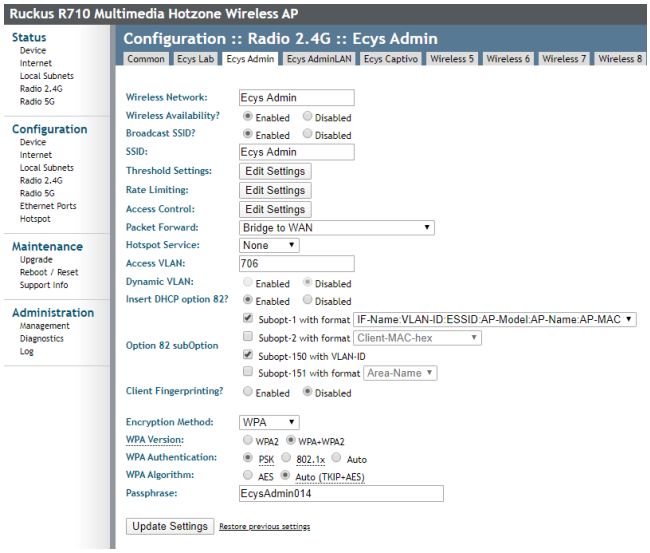
A continuación, se presenta la configuración de los dispositivos de puntos de acceso inalámbricos utilizados para la difusión del servicio de internet dentro de las instalaciones de los laboratorios.

Figura 34. **Configuración de punto de acceso Ecys Lan**



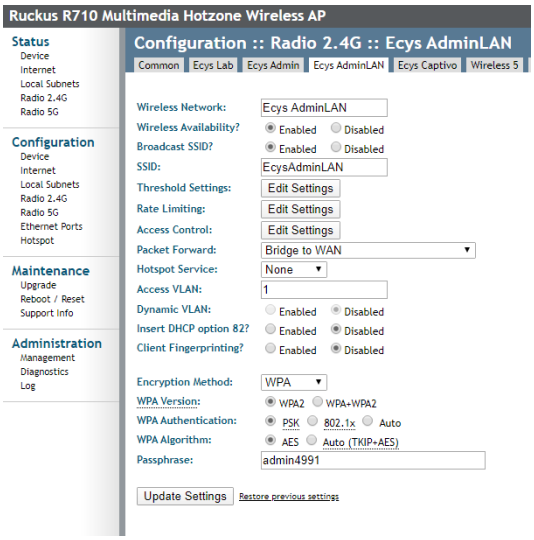
Fuente: elaboración propia, empleando Ruckus Wireless Admin R710 y R310.

Figura 35. **Configuración de punto de acceso inalámbrico Ecys Admin**



Fuente: elaboración propia, empleando Ruckus Wireless Admin R710 y R310.

Figura 36. **Configuración de punto de acceso inalámbrico Ecys Admin LAN**



Fuente: elaboración propia, empleando Ruckus Wireless Admin R710 y R310.

A continuación, se presenta el detalle de la configuración de los dispositivos de punto de acceso Ruckus como proveedores del servicio inalámbrico con cada identificador de red de área local virtual.

Tabla XXXII. **Detalle de configuración de puntos de acceso inalámbricos según las características de difusión y transmisión**

SSID	VLAN	Tipo de adaptador	Descripción uso	Red de acceso
Ecys Lab	88	Bridge to WAN.	Red y servicio de internet por medio de portal cautivo.	172.10.0.0 / 16
Ecys Admin	706	Bridge to WAN.	Red y servicio de internet en red administrativa RiusacAps.	10.56.0.0 / 16

Continuación de la tabla XXXII.

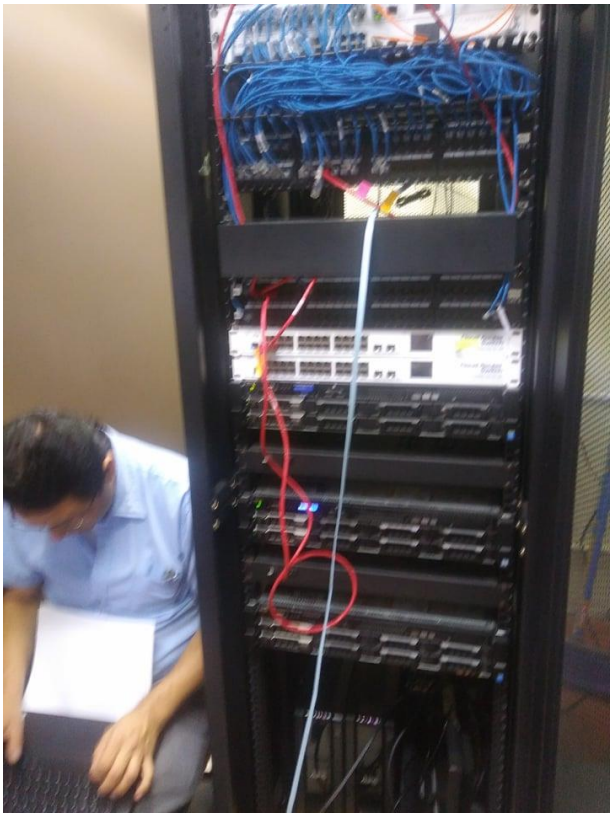
Ecys Admin LAN	1	Bridge to WAN.	Configuración de dispositivo.	172.10.0.0 / 16

Fuente: elaboración propia.

Figura 37. **Configuración de los dispositivos de red y servidores**

Fuente: elaboración propia.

Figura 38. **Configuración de conmutadores y enrutadores de la infraestructura de red con apoyo de personal de Procesamiento de Datos de la Universidad de San Carlos de Guatemala**



Fuente: elaboración propia.

2.3.8. Implementación de políticas administrativas

El diseño del sistema de administración de recursos no contempla los aspectos técnicos de comunicación entre distintas tecnologías, debido a esto se implementa un módulo de políticas administrativas para configuración del servidor de corta fuegos mediante la implementación de una librería de código

abierto con los mecanismos de seguridad necesarios para acoplarse al modelo de infraestructura establecido como solución del proyecto.

FauxApi es una librería de código abierto disponible directamente dentro del gestor de paquetes propio del servidor de corta fuegos PfSense, implementa acceso por clave de seguridad e identificadores de cliente para conexión por medio de encriptación de tipo hash. Por medio de una interfaz TCP y HHTPS FauxApi permite la conexión, configuración y modificación de la configuración de los servicios del servidor de corta fuegos mediante un APIRest que es consumida mediante la dirección IP del servidor de cortafuegos.

Debido a que FauxAPI se ejecuta directamente sobre el servidor de corta fuegos y este provee de sus propios clientes de consumo, las opciones para poder comunicarse con la interfaz de FauxAPI son limitadas siendo dependiendo del lenguaje de programación a utilizar no habiendo disponible un cliente implementado en el lenguaje Java, por facilidad en su implementación para la elaboración de este proyecto se selecciona el cliente de PHP para FauxAPI y el servidor de aplicaciones web Apache2 para brindar una interfaz intermedia de comunicación y ejecución entre el sistema de administración y reportes con el servidor de corta fuegos.

El diseño del módulo de comunicación intermedio para la configuración de políticas del servidor de corta fuegos se presenta a continuación.

Figura 39. **Diagrama de implementación del módulo de comunicación intermedio para gestión de políticas de los recursos de red**

Fuente: elaboración propia, empleando Lucidchart en su versión web.

2.3.8.1. Modulo intermedio de aplicación de políticas a configuración de firewall

Las configuraciones que se pueden aplicar por medio del módulo de políticas, está basado en un controlador programado en el lenguaje de programación PHP y se ejecuta sobre un servidor de aplicaciones web Apache2 que se comunica con el cliente de conexión del paquete FauxAPI del servidor de corta fuegos PfSense.

A continuación, se presentan los valores de comunicación requeridos como parámetro que deben ser enviados al controlador de PHP para poder comunicarse con la librería FauxAPI para aplicar los cambios en la configuración del servidor de corta fuegos.

Tabla XXXIII. **Parámetros de configuración para comunicación del sistema de gestión de recursos con el controlador de comunicación FauxAPI**

Característica de configuración	Descripción	Valor asignado
Uri	Dirección URL con la IP del servidor de corta fuegos PfSense.	https://172.10.0.10
apiKey	Clave de conexión de la librería FauxApi.	X
apiSecret	Clave de desencriptación SHA-256 utilizada por la librería para obtener la clave de autenticación y conexión de un cliente a la librería FauxAPI.	X
Debug	Valor booleano de configuración para permitir la depuración de la ejecución al realizar una llamada de comunicación a la librería FauxAPI en el servidor de cortafeugos.	TRUE

Fuente: elaboración propia.

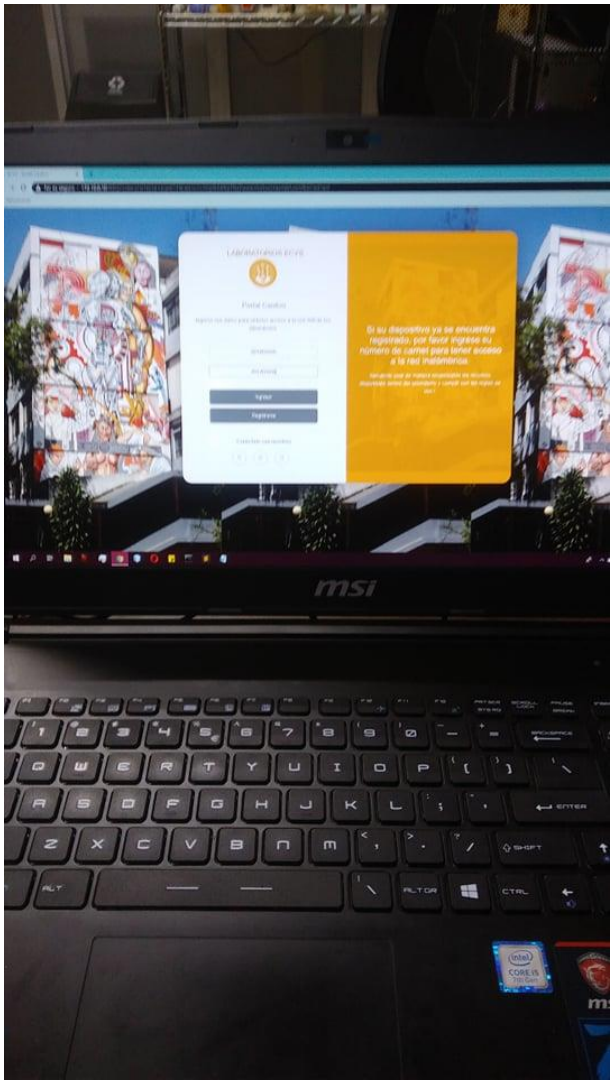
2.3.9. Resultados de la implementación del portal cautivo, sistema de administración de recursos de red y DMZ

Finalizado el proceso de implementación y desarrollo del portal cautivo y sistema de administración, los resultados finales fueron exitosos y con un alto grado de satisfacción para la coordinación de los laboratorios al realizar la integración de un servicio con el equipo existente y la estandarización a la infraestructura de red existente. A continuación, se presenta los resultados finales de la implementación del portal cautivo, su despliegue en dispositivos móviles que se conectan a los puntos de acceso inalámbricos, y en los que se conectan mediante puerto ethernet y cable a los puntos de red de las instalaciones.

Figura 40. **Resultado final de despliegue e implementación de portal cautivo en dispositivos móviles**

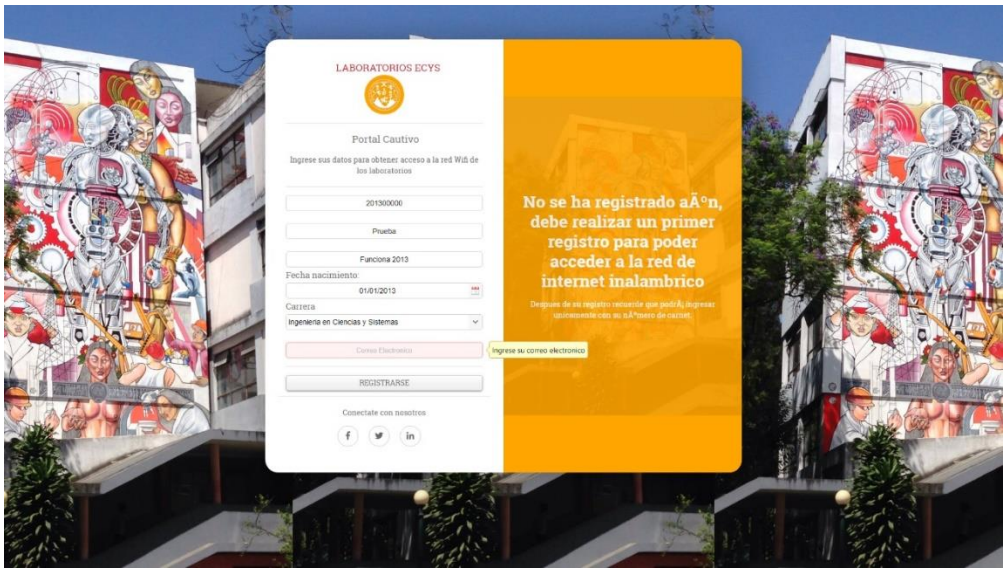
Fuente: elaboración propia, empleando Portal Cautivo Ecys014 año 2020.

Figura 41. **Resultado final de implementación y despliegue de portal cautivo en computadoras portátiles por red cableada e inalámbrica**



Fuente: elaboración propia, empleando Portal Cautivo Ecys014 año 2020.

Figura 42. **Resultado final de página de registro de portal cautivo en computadoras portátiles**



Fuente: elaboración propia, empleando Portal Cautivo Ecys014 año 2020.

2.3.10. Resultados de la implementación del sistema de administración y reportes de los recursos de red

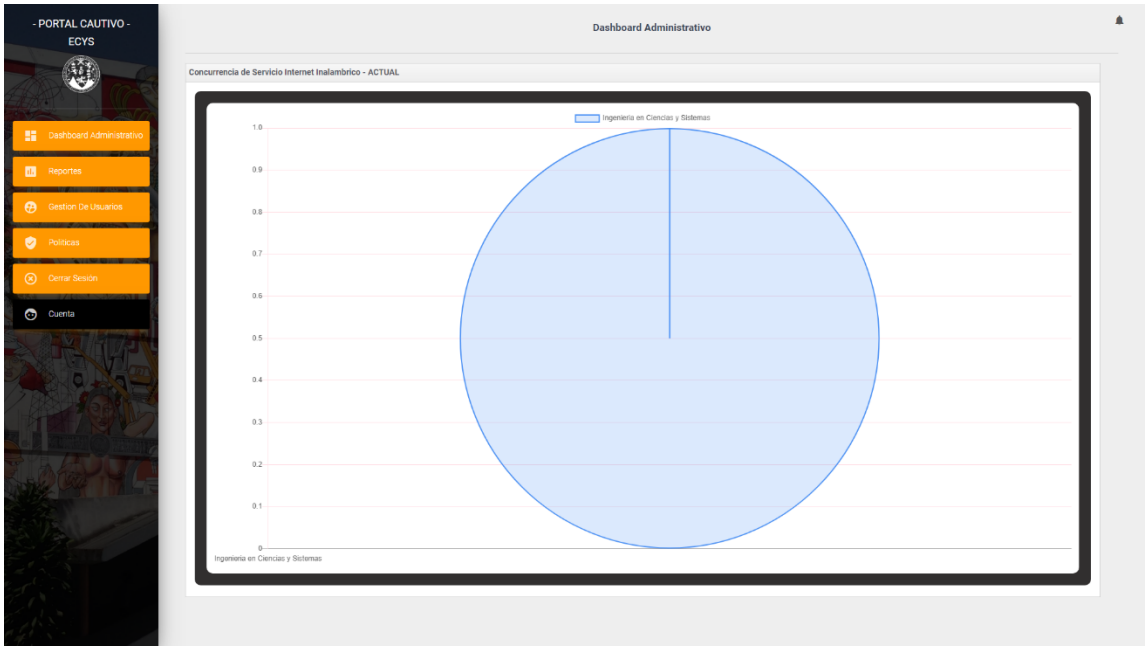
A continuación, se presentan los resultados de la implementación del portal cautivo y sistema de administración de la red.

2.3.10.1. Sistema de administración de red y reportería

El sistema de administración de red y reportería consta de cuatro módulos explicados en la sección de diseño del sistema. A continuación, se presentan los resultados de su implementación y primeras pruebas en campo real.

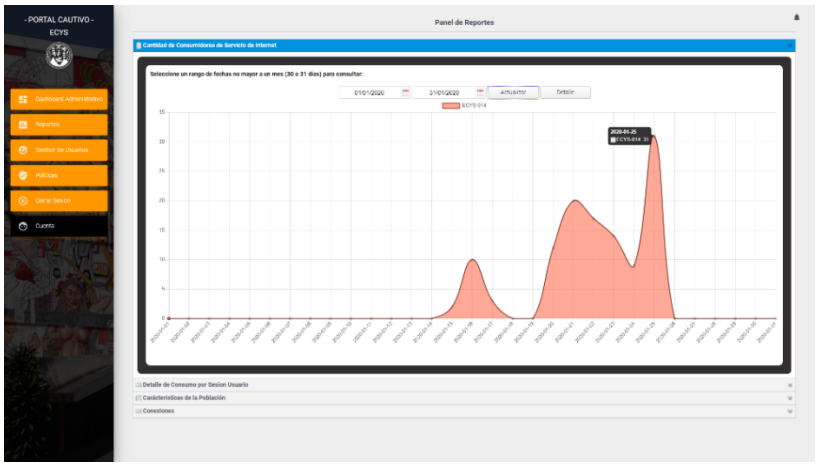
La primera implementación y elaboración de pruebas tanto funcionales como de rendimiento fueron llevadas a cabo durante el mes de enero de 2020 con resultados altamente satisfactorios al obtener los primeros datos reales acerca del consumo y utilización de la red por parte de la población estudiantil.

Figura 43. **Tablero de reporte en tiempo real de la concurrencia de usuarios de la red clasificados por carrera universitaria**



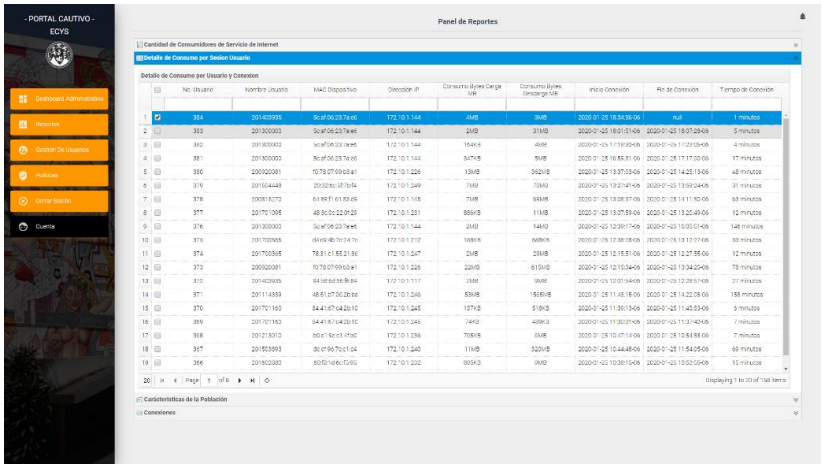
Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

Figura 44. **Módulo de reportes, reporte por cantidad de consumidores por rango de fechas**



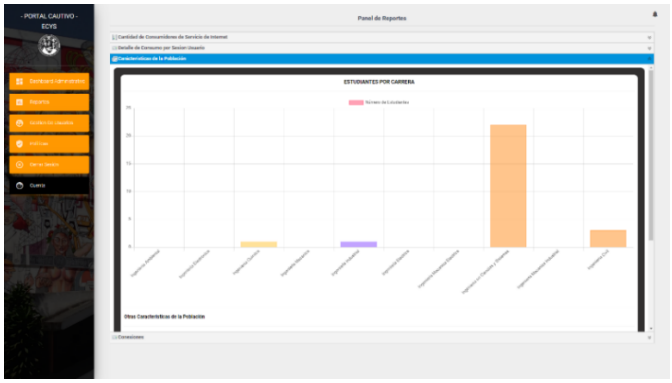
Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

Figura 45. **Módulo de reportes, reporte tabular del detalle de consumo por sesión y usuario**



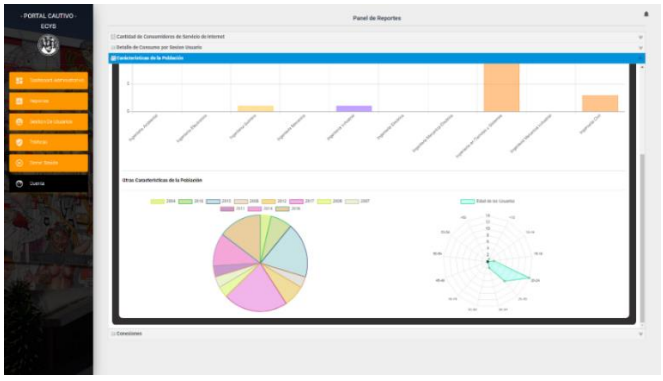
Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

Figura 46. **Módulo de reportes, gráfico de barras con la cantidad de estudiantes por carrera de la Faculta de Ingeniería registrados como usuario de la red con acceso a los recursos de red interna**



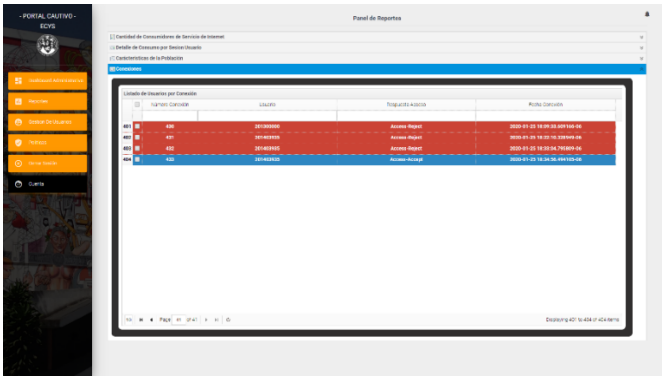
Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

Figura 47. **Módulo de reportes, gráfico de pie y de radar con características de la población sobre el número de carnet al que pertenecen y la edad de los usuarios registrados**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

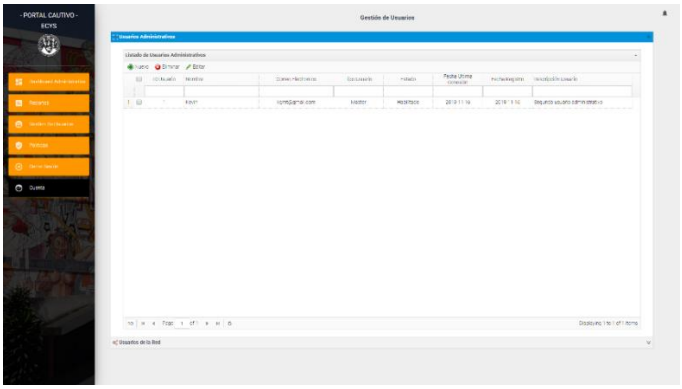
Figura 48. **Módulo de reportes, reporte tabular de los intentos de conexión registrados por el portal cautivo**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

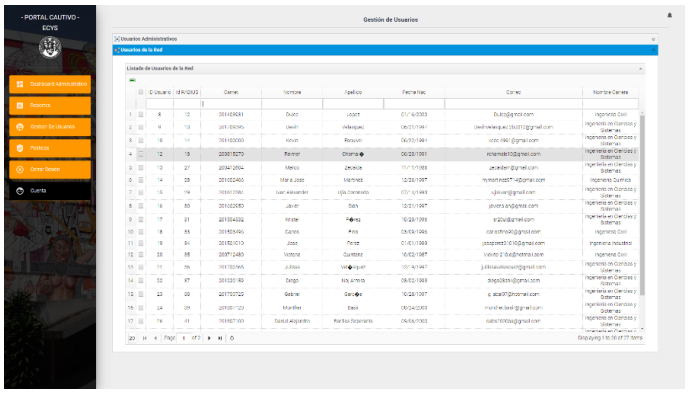
A continuación, se muestran los resultados finales del módulo de gestión de usuarios del sistema de administración de recursos de red y reportes.

Figura 49. **Módulo de gestión de usuarios, interfaz de usuario para gestión de usuarios administrativos**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

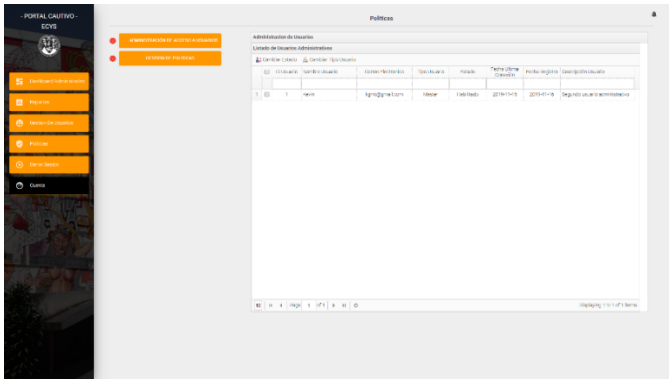
Figura 50. **Módulo de gestión de usuarios, interfaz de usuario para gestión de usuarios de la red**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

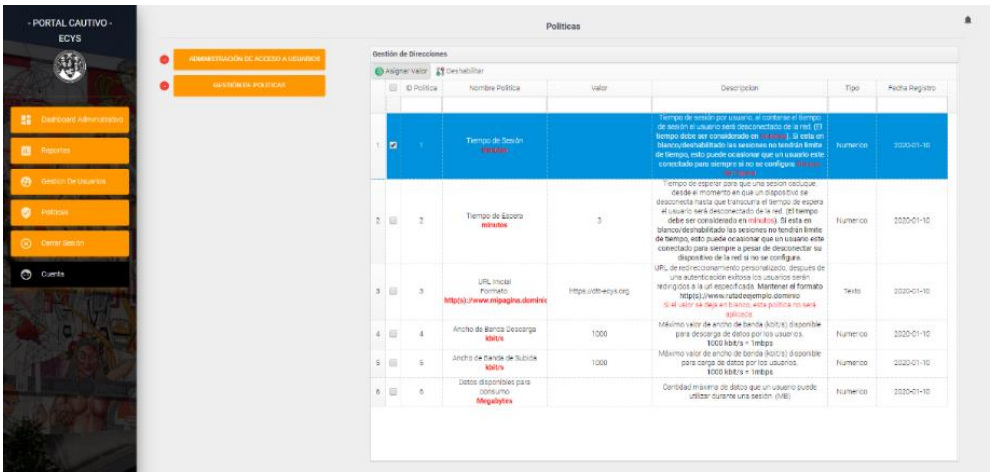
Como parte de los resultados esperados y que si fueron implementados pese a la priorización es el módulo de gestión de políticas de administración de red y acceso de usuarios, el resultado final se presenta a continuación.

Figura 51. **Módulo de gestión de políticas, administración de acceso a usuarios administrativos**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

Figura 52. **Módulo de gestión de políticas, interfaz de usuario asignación y des habilitación de políticas de red**



Fuente: elaboración propia, empleando Sistema de Administración y Reportes Ecys014 año 2020.

2.4. Costos del proyecto

Está conformado por los costos realizados por el estudiante durante la elaboración del proyecto y la implementación de este, costos realizados por los asesores y el recurso físico consumidos durante la elaboración del proyecto.

Tabla XXXIV. **Costos del proyecto**

Recursos	Cantidad	Descripción	Costo	Total
Analista y desarrollador.	1	Durante 6 meses y 4 horas diarias.	Q 30 000,00	Q 30 000,00
Consultores	2	Durante 6 meses y 1 hora semanal.	Q 14 000,00	Q 28 000,00
Servicio de internet.	6 meses	6 meses de servicio.	Q 1 800,00	Q 1 800,00
Energía eléctrica.	6 meses	6 meses de servicio.	Q 1 200,00	Q 1 200,00
			Total	Q 61 000,00

Fuente: elaboración propia.

2.4.1.1. Recurso de infraestructura

- Conmutador Juniper: dispositivo de red encargado de establecer la ruta y dirección del tráfico de red de puerto a puerto identificándolo por medio de números de puerto e identificadores de red virtual VLAN. Es el encargado de la transmisión de paquetes de punto a punto.

- Enrutadores Mikrotik: dispositivo de red encargado de realizar la difusión del servicio de internet del proveedor, y el servicio de portal cautivo dentro de la solución hacia los puertos o dispositivos conectados a este.

- Servidores: contenedores y máquinas virtuales implementados en PROXMOX intercomunicados por medio de interfaces de red físicas y virtuales que contienen dependiendo de su definición los distintos software y sistema operativos para los servidores de base de datos, corta fuegos y aplicaciones web.

- Puntos de acceso: dispositivos de difusión de red inalámbrica por medio del cual ser realiza la comunicación del tráfico de red y servicios dentro de una red privada. Permite la conexión de usuarios y en muchos casos permite la administración de la red.

2.4.1.2. Recurso humano

- Analista y desarrollador: es la persona responsable de las fases de análisis, implementación y pruebas del proyecto. Sus funciones principales son las de codificar, configurar e instalar software, hardware, elaborar las pruebas, realizar la verificación del funcionamiento correcto de los sistemas y configuraciones de hardware.
- Consultores: personas que no están involucradas directamente con el proyecto, pero brindan apoyo durante el diseño de la solución del proyecto, ofrecen también control en el alcance de los objetivos.

2.5. Beneficios del proyecto

Como resultado del proyecto se identificaron los beneficios presentados a continuación.

2.5.1. Beneficios para la población estudiantil de la Facultad de Ingeniería

- Mejorar la disponibilidad de conexión de usuarios a la red por medio de los puntos de acceso inalámbrico y cableado.

- Mejorar la estabilidad y calidad de la conexión de los usuarios conectados a la red de interna de los laboratorios.

2.5.2. Beneficios para la institución

- Crear y almacenar registros sobre los usuarios, su consumo de servicio de la red, cronología de accesos y su interacción con la red y servicio de internet inalámbrico.

- La implementación de múltiples servidores con servicios que brindan la capacidad de publicación de nuevas herramientas y soluciones de software que pueden ser publicados directamente dentro de la red para uso de los usuarios.

- Implementar mecanismos de seguridad para el acceso adecuado de los usuarios a la red interna de los laboratorios.

- Permitir la administración de los recursos de internet inalámbrico y portal cautivo por medio de la gestión de políticas de red y un servidor de corta fuegos.

- Aislar la red interna de los laboratorios para su administración y control individual por medio de herramientas propias y personalizadas.

3. FASE DE ENSEÑANZA APRENDIZAJE

Para la implementación de esta fase se realizaron dos tipos de capacitación, las cuales son presentadas a continuación.

3.1. Capacitación de usuarios administradores del sistema

Se llevaron a cabo una serie de charlas de capacitación a los involucrados en la administración y gestión de los recursos de las instalaciones y laboratorios. La capacitación consistió en la definición y elaboración de demostraciones de cómo funcionaba tanto el portal cautivo como los módulos del sistema de administración. Como parte final de las capacitaciones se desarrollaron resolución de dudas con los presentes.

3.2. Capacitación de estudiantes

Se llevó a cabo la capacitación de los estudiantes por medio de material informativo en las instalaciones de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas. El material elaborado fue colocado en lugares visibles y de fácil acceso a los estudiantes con las instrucciones para ingresar a la red y las condiciones del servicio.

3.3. Material de capacitación

Se elaboró posters informativos con las instrucciones para ingreso de la red, condiciones del servicio y preguntas frecuentes generales.

De forma adicional se elaboró el manual de usuario con la descripción y funcionalidades de los módulos del sistema de administración de recurso.

CONCLUSIONES

1. La coordinación de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas, por medio del portal cautivo y sistema adjunto de administración de los recursos de red y reportería puede administrar y controlar el acceso de los usuarios a los recursos de red de manera automatizada, observando una oxigenación y mejora en la calidad del servicio.

2. El portal cautivo permite la autenticación, autorización de usuarios y la contabilización del consumo de internet de los usuarios como mecanismo de seguridad, administración y gestión de recursos para los usuarios que se conecten por medio de los puntos de acceso inalámbricos de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas.

3. El portal cautivo a través de servidor DNS y DHCP se despliega únicamente dentro de la nueva red interna de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas, permitiendo a los usuarios el uso del recurso de internet inalámbrico.

4. A través del servidor de autenticación, autorización y contabilización con la implementación del portal cautivo se almacena la información sobre el uso de la red y consumo de paquetes de descarga y subida de datos de los usuarios que utilizan el internet gratuito de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas.

5. Con el desarrollo del módulo de políticas para la administración de los recursos de red, el portal cautivo y su sistema adjunto permiten el filtrado de usuarios y contenido para los usuarios que es capaz de realizar el servidor de corta fuegos sobre la red interna de los laboratorios.

RECOMENDACIONES

1. Llevar a cabo un monitoreo de los servidores físicos y virtuales, de forma que los servicios y el portal cautivo prevalezcan en línea siendo estos la fuente principal de servicio de internet para los estudiantes, a fin de prevenir cortes o fallas en el servicio.

2. Establecer niveles de seguridad y acceso a los servidores, de tal manera que no cualquier usuario pueda tener acceso a la configuración, siendo esta muy extensa y con alto nivel de falla en caso de cambios sin conocimiento de la herramienta o diseño de la solución del proyecto.

3. Realizar monitoreos periódicos de los usuarios registrados, debido a que el sistema permite el registro de los usuarios pueden existir falsos positivos en la información, de manera que pueda existir integridad y coherencia en los datos almacenados por el sistema.

4. Apoyar y fomentar la implementación de nuevas funcionalidades al sistema actual, así como la integración de ciencia de los datos para análisis y aprovechamiento de la información obtenida por el sistema de los usuarios, consumos y red interna de los laboratorios.

5. Realizar la verificación de actualizaciones para el software instalado así a fin de evitar la caída y perdida del servicio de internet en los laboratorios.

BIBLIOGRAFÍA

1. Escuela de Ingeniería en Ciencias y Sistemas. *Misión y visión*. [en línea]. <https://dtt-ecys.org/about_us>. [Consulta: 28 de octubre de 2019].

2. FreeRADIUS. *FreeRADIUS Wiki*. [en línea]. <https://wiki.freeradius.org/Home>. [Consulta: julio de 2019].

3. JONG, Nicholas. *Librería fauxAPI documentación github* . [en línea]. <https://github.com/ndejong/pfsense_fauxapi>. [Consulta: enero de 2029].

4. The PostgreSQL Global Development Group. *PostgreSQL Org.* [en línea]. <https://www.postgresql.org/>. [Consulta: septiembre de 2019].

5. Universidad de Alicante. *Modelo vista controlador (MVC)*. [en línea]. <https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html>. [Consulta: agosto de 2019].