



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, febrero 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, FEBRERO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Aurelia Anabela Córdova Estrada
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto Galicia Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Aurelia Anabela Córdova Estrada
EXAMINADOR(A)	Ing. o Inga. dependiendo del género
EXAMINADOR(A)	Colocar examinadora si es Inga.
EXAMINADOR(A)	NO LLENAR SI NO HA REALIZADO PRIVADO
SECRETARIO	Secretario JD cuando realizó su privado.

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 2020.

Kevin Estuardo Esquivel Cuy

ACTO QUE DEDICO A:

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

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser mi <i>alma mater</i> , 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 ayuda, 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 y después de mi carrera, que no fueron únicamente académicos y profesionales sino también de vida.
La licenciada	Anselma del Rosario Jáuregui Contreras, gracias por su apoyo, consejos e incondicional apoyo que impulso mi carrera.
Dulce López	Por su apoyo, amor y cariño incondicional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	V
LISTA DE SÍMBOLOS	IX
GLOSARIO	XI
RESUMEN	XIII
OBJETIVOS.....	15
INTRODUCCIÓN	16
1. FASE DE INVESTIGACIÓN	18
1.1. Antecedentes de la Empresa.....	18
1.1.1. Reseña Histórica	18
1.1.2. Misión	20
1.1.3. Visión.....	20
1.1.4. Servicios que realiza.....	20
1.2. Descripción de las necesidades	21
1.2.1. Necesidades Identificadas	21
1.3. Priorización de las necesidades	22
2. FASE TÉCNICO PROFESIONAL	23
2.1. Descripción del proyecto	23
2.2. Investigación preliminar para la solución del proyecto.....	24
2.2.1. Análisis FODA del proyecto	24
2.2.1.1. Análisis Interno	24
2.2.1.1.1. Fortalezas.....	25
2.2.1.1.2. Debilidades.....	25
2.2.1.2. Análisis Externo	26
2.2.1.2.1. Oportunidades	26
2.2.1.2.2. Amenazas.....	26

2.2.2.	Análisis y diseño de la infraestructura de red	27
2.2.2.1.	Hardware de la infraestructura de red	
	27
2.2.2.2.	Cableado estructurado	27
2.2.2.3.	Dispositivos de enrutamiento y comutación de red.....	27
2.2.2.4.	Servidores físicos y plataforma de virtualización para alojamiento de servidores.....	28
2.2.3.	Análisis e Investigación del modelo de datos	31
2.2.3.1.	Análisis de datos	31
2.2.3.2.	Herramientas de desarrollo, investigación y definición.....	33
2.2.3.3.	Infraestructura de red, hardware y herramientas de desarrollo.....	35
2.3.	Presentación de la solución del proyecto	36
2.3.1.	Diseño de infraestructura de la solución del proyecto.....	37
2.3.2.	Historias de usuario.....	38
2.3.3.	Modelo de datos.....	40
2.3.3.1.	Diagrama entidad-relación	40
2.3.3.1.1.	Entidades del modelo de datos para el sistema administrativo...41	
2.3.3.1.2.	Entidades del modelo de datos del servidor FreeRADIUS	43
2.3.3.2.	Diseño de entidades y dependencias...44	

2.3.4.	Sistema para la administración del recurso de internet inalámbrico	47
2.3.5.	Instalación y configuración de software para administración de redes como parte de la solución del proyecto	51
2.3.5.1.	Servidor de aplicaciones web	51
2.3.5.2.	Servidor para el sistema gestor de base de datos	53
2.3.5.3.	Servidor de corta fuegos.....	54
2.3.5.4.	Servidor de autenticación, autorización y contabilización RADIUS	56
2.3.6.	Configuración de la infraestructura de red del proyecto.....	68
2.3.6.1.	Diseño de la DMZ.....	68
2.3.6.2.	Instalación de dispositivo de conmutación de red para aislamiento de la red.....	72
2.3.6.3.	Configuración de red LAN	81
2.3.6.4.	Configuración de red WAN	84
2.3.7.	Implementación del portal cautivo en la red nueva red interna y DMZ de los laboratorios.....	88
2.3.7.1.	Configuración de zona.....	92
2.3.7.2.	Configuración de dispositivos enrutadores.....	97
2.3.7.3.	Configuración de firewall e interconexión de portal cautivo con base de datos y servidor RADIUS ¡Error! Marcador no definido.	

2.3.8.	Implementación de políticas administrativas	103
2.3.8.1.	Modulo intermedio de aplicación de políticas a configuración de firewall....	103
2.3.9.	Resultados de la implementación del portal cautivo, sistema de administración de recursos de red y DMZ.....	103
2.4.	Costos del proyecto.....	112
2.4.1.1.	Recurso de infraestructura	113
2.4.1.2.	Recurso humano	113
2.4.1.3.	Recurso físico consumible.....	113
2.5.	Beneficios del proyecto	113
CONCLUSIONES.....		115
RECOMENDACIONES		117
BIBLIOGRAFÍA.....		119
APÉNDICES.....		121
ANEXOS.....		123

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Contenedor de PROXMOX para servidor de base de datos	28
2.	Configuración de red para contenedor de PROXMOX del servidor de base de datos.....	29
3.	Contenedor de PROXMOX para servidor de aplicaciones web	29
4.	Configuración del contenedor de PROXMOX para servidor de aplicaciones web.....	30
5.	Máquina virtual de PROXMOX para servidor de corta fuegos	30
6.	Configuración de interfaz de red de maquina virtual para servidor de corta fuegos en PROXMOX	31
7.	Diagrama de implementación de la solución.....	37
8.	Diagrama entidad-relación	40
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	52
10.	Estado de la ejecución del proceso para el servidor web Apache Tomcat versión 9.0.27, instalado dentro del sistema de virtualización PROXMOX.....	53
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	53
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	54

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	55
14.	Consola de administración del corta fuegos PfSense para gestión directa desde el sistema operativo.....	55
15.	Configuración del servidor de autenticación, autorización y contabilización FreeRADIUS desde la consola de administración web de servidor corta fuegos PfSense	56
16.	Configuración del módulo de conexión SQL para el servidor FreeRADIUS.....	57
17.	Configuración y especificación de tablas del modelo de datos para consumo del servidor FreeRADIUS	58
18.	Archivo de configuración de módulo SQL para el servidor FreeRADIUS	64
19.	Configuración de clientes NAS en servidor FreeRADIUS, como proveedores del servicio portal cautivo para la red LAN de los laboratorios	65
20.	Topología de infraestructura de red de la DMZ para la implementación de red LAN y WAN, generado durante la implementación de la solución en enero 2020.....	71
21.	Resumen de gastos mensuales.....	121
22.	Mapa de Guatemala	123

TABLAS

I.	Listado de hardware para la infraestructura de red utilizado para en la elaboración del proyecto	27
II.	Características y datos seleccionados para el modelo de datos, establecidas durante la fase de investigación en el mes de julio de 2019	32
III.	Herramientas de desarrollo seleccionadas	34
IV.	Herramientas de infraestructura	35
V.	Listado de las historias de usuario	38
VI.	Detalle de la tabla captive_administrador.....	45
VII.	Detalle de la tabla captive_carrera.....	45
VIII.	Detalle de la tabla captive_estado_usuario_administrativo.....	46
IX.	Detalle de la tabla captive_tipo_dato_politica	46
X.	Detalle de la tabla captive_tipo_usuario_admin	46
XI.	Detalle de la tabla captive_usuario.....	47
XII.	Módulos del sistema y plataforma web administrativa	48
XIII.	Módulos del portal cautivo.....	51
XIV.	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.....	59
XV.	Detalle de configuración de cliente NAS, proveedor principal del servicio portal cautivo dentro de la red LAN.....	66
XVI.	Costos del proyecto.....	112

LISTA DE SÍMBOLOS

Símbolo	Significado
Mb/s	Megabit por segundo
mts	Metros

GLOSARIO

RADIUS	Acrónimo del inglés: <i>Remote Authentication Dial-In User Service</i> . Protocolo de autenticación y autorización para aplicaciones de acceso a la red IP.
Iptables	Utilidad de línea de órdenes para configurar el cortafuegos del kernel de Linux.
DBMS	Acrónimo en inglés: Data Base Management System. 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.
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.
PfSense	Software de código abierto con funcionalidades de cortafuegos o enrutador para la administración de infraestructuras de red.

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.

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, India1, India2 y de electrónica.

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

- 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.
- Implementar 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.
- Implementar servidores DNS y DHCP como administradores del tráfico y recursos de red de internet de los laboratorios de la Escuela de Ciencias y Sistemas.
- Obtener, almacenar y consultar información sobre el recurso y uso del internet inalámbrico de los laboratorios de la Escuela de Ciencias y Sistemas.
- 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 el cual 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 el cual 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 que la Facultad de Ingeniería, encargada de la formación superior en las áreas de ciencias de la computación y sistemas. 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, a fin de lograr con los objetivos 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, dos de ellos ubicados en el nivel 0, 4 y 5 del edificio T3, dichos laboratorios se encuentran habilitados desde el año 2015 y actualmente en uso y en los cuales se realizan principalmente actividades de desarrollo de laboratorios de la carrera de Ingeniería en Ciencias y Sistemas, capacitaciones y conferencias en el área referente a la especialidad científica de la Escuela y 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 los espacios y mobiliario, electricidad e internet inalámbrico.

En la actualidad los laboratorios de la Escuela de Ciencias y Sistemas no poseen medios de control y administración de recursos en el área de infraestructura de red, y el servicio de internet inalámbrico no es la excepción.

Así inicio la necesidad de implementar el control y administración de los recursos de internet que se proveen en espacios públicos es totalmente necesario ya que al no existir estas herramientas dichos recursos son mal utilizados, no se tiene información de su uso y tampoco existen medios para controlar qué, quién o cuándo se consume determinado contenido o de qué forma se está haciendo uso de dicho contenido, razones principales por las que la implementación de un portal cautivo para poder evitar las conexiones innecesarias de dispositivos y un módulo administrativo que permita definir qué contenido tener acceso por medio del servicio brindado es sumamente necesario siendo como ejemplo el uso de portal cautivo en espacios públicos tales como hoteles, centros comerciales, restaurantes, etc.

Debido a que los recursos que brindan los laboratorios de la Escuela de Ciencias y Sistemas son de acceso libre y gratuito para toda la población estudiantil universitaria dar la oportunidad de utilizarlos y que proporcionen una experiencia de usuario agradable y de calidad es prioritario para 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. Los espacios de uso público con acceso a internet como centros comerciales y hoteles son ejemplos claros que el uso de un portal cautivo en espacios de este tipo con tantos usuarios es totalmente necesario para evitar el uso indebido de los recursos disponibles y la mayor disponibilidad del servicio para la mayor cantidad de usuarios posibles de alcanzar.

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, etc.), 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.”¹

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 de la enseñanza a nivel superior presta sus instalaciones 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 Escuela de Ingeniería en Ciencias y Sistemas. Misión y Visión: https://dtt-ecys.org/about_us. Consulta: 28 de octubre de 2019. (Traducción al español)

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 en cualquiera de sus ramas, 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 sus instalaciones, pero no posee una plataforma o aplicación de software que permita la administración y control de dicho recurso. 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 de enrutamiento que proveen señal de internet inalámbrico dentro de las instalaciones, así como 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 además de implementar 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 ruteo, así como 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 Escuela, así como la gestión de usuarios que se refiera a la gestión de accesos y conexión 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, desarrollo, instalación y configuración) de un portal cautivo y un sistema adjunto para la administración de la infraestructura de recurso de red de inalámbrico, el portal cautivo será utilizado como medio de autenticación de usuarios para acceso a la red, permitiendo o denegando la conexión de los usuarios a la red inalámbrica de 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, gestión de usuarios y gestión 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, en donde inicialmente se autenticaran o se registraran; 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 el cual se encargará de la autenticación, autorización y contabilización de los usuarios. A través de esto tanto los laboratorios como la escuela podrán justificar y comprobar la cantidad de estudiantes y población que utiliza las instalaciones.

El principal enfoque del proyecto es brindar los mecanismos de administración de los recursos de internet que se brindan en las instalaciones de los laboratorios a fin de dar un buen servicio y de mejorar la capacidad de acceso a los usuarios. Como parte inicial del proyecto se realizará el desarrollo el diseño

de la solución, el modelo de datos y la arquitectura del sistema 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 de la aplicación web que funcionará como portal cautivo, la instalación y configuración de las distintas herramientas, así como 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 la información acerca del estado de los laboratorios, tomando en cuenta todos los aspectos técnicos que tienen que ver con el servicio de internet inalámbrico.

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 y 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 las instalaciones, 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 enrutadores para brindar el servicio de internet inalámbrico.
- La coordinación de los laboratorios cuenta con las credenciales de acceso a los equipos que serán utilizados para la elaboración del proyecto.
- La infraestructura de red actual cuenta con una configuración capaz de admitir y soportar la integración del proyecto, así como 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 ya que 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 recurso y usuarios que brinda la plataforma.

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.

- La funcionalidad de la aplicación y configuración es completamente dependiente del equipo físico que contiene la infraestructura de red actual de los laboratorios.

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 testeo de la red, para conocer 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 para que esta funcione de manera correcta.

- La infraestructura de red y el portal web deberá evitar la modificación de las configuraciones de dispositivos de ruteo, 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

2.2.2.1. Hardware de la infraestructura de red

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

Tabla I. Listado de hardware para la infraestructura de red utilizado para en la elaboración del proyecto

Número	Dispositivo	Especificaciones de hardware	Descripción de funcionalidad

2.2.2.2. Cableado estructurado

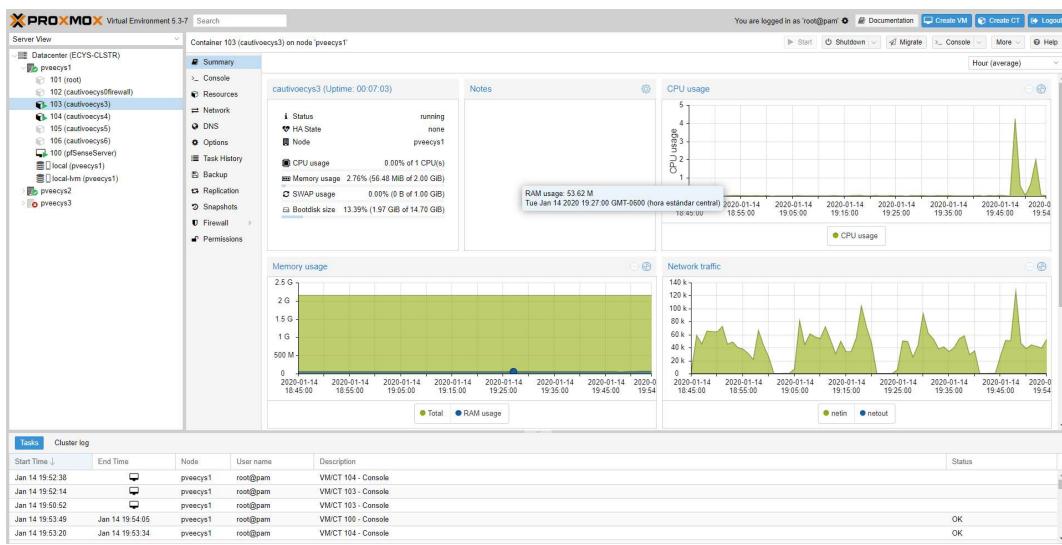
2.2.2.3. Dispositivos de enrutamiento y conmutación de red

2.2.2.4. 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.

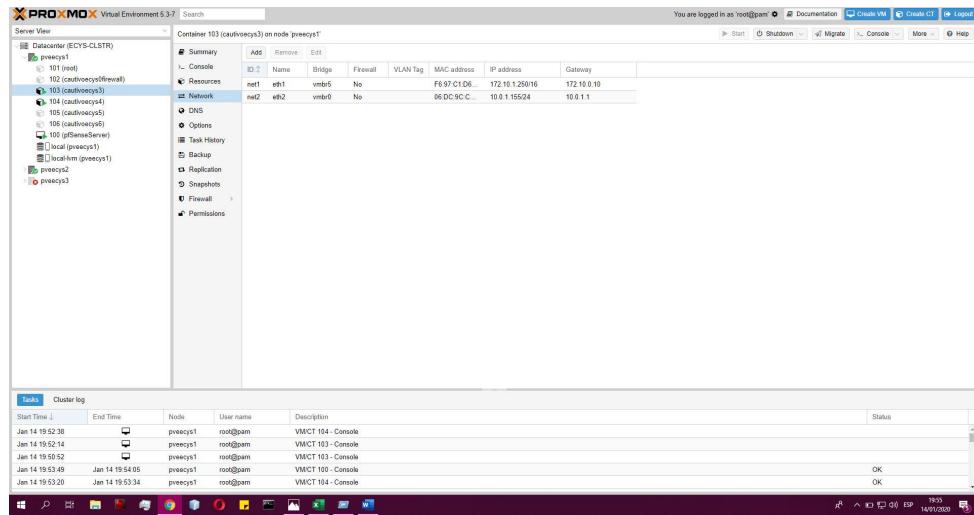
Se presenta a las siguientes imágenes la máquinas virtuales y contenedores creados en PROMOX como los servidores del proyecto.

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



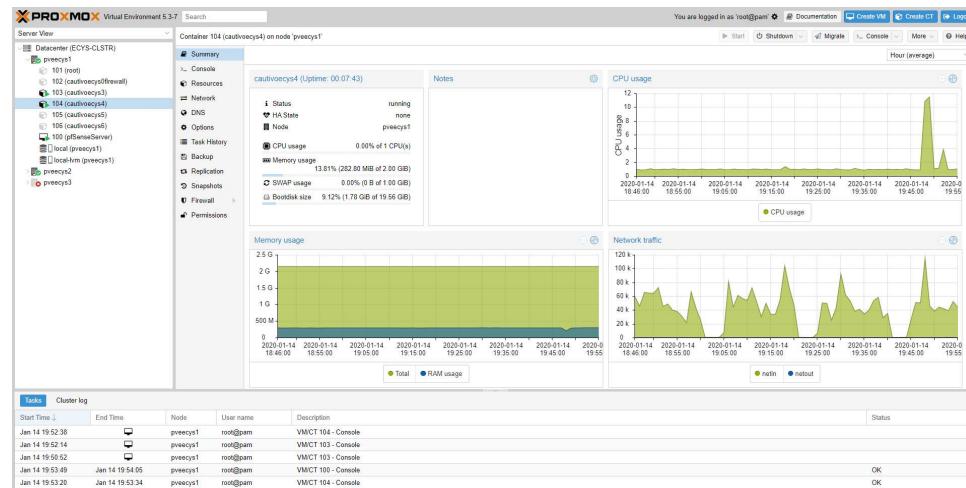
Fuente: especificación de recursos de hardware para el contenedor de PROXMOX utilizado como servidor de base de datos PostgreSQL, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

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



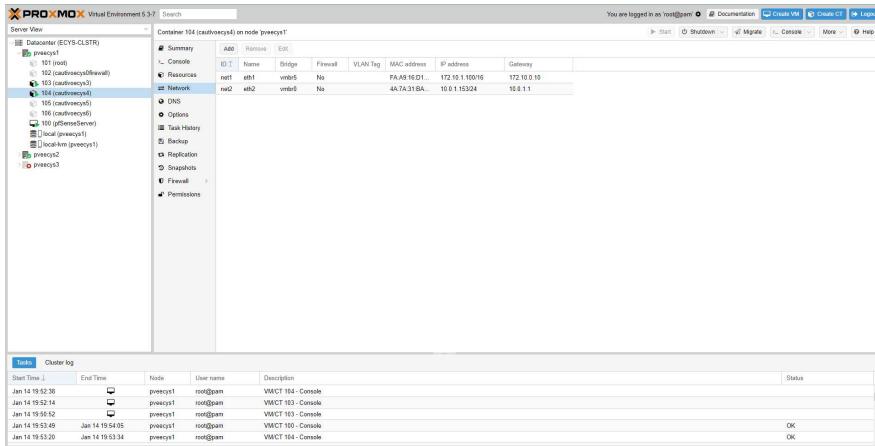
Fuente: configuración de interfaces de red para el contenedor de PROXMOX utilizado como servidor de base de datos PostgreSQL, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

Figura 3. Contenedor de PROXMOX para servidor de aplicaciones web



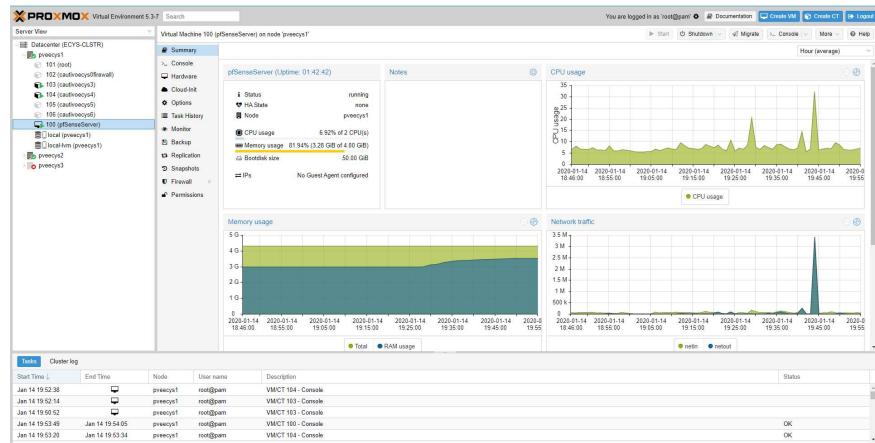
Fuente: especificación de recursos de hardware para el contenedor de PROXMOX utilizado como servidor de aplicaciones web Tomcat, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

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



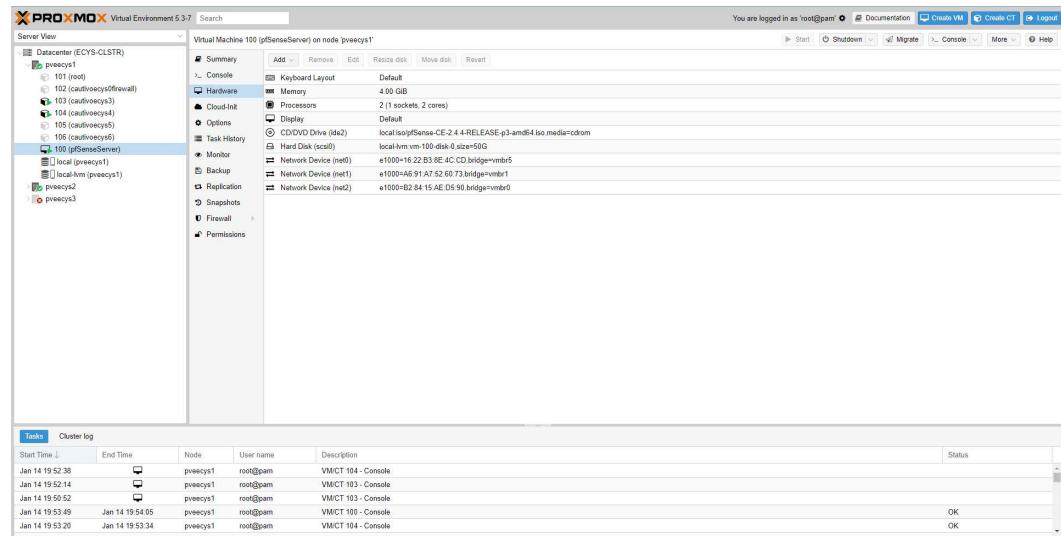
Fuente: configuración de interfaces de red para el contenedor de PROXMOX utilizado como servidor de aplicaciones web Tomcat, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

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



Fuente: especificaciones de recursos de hardware para la máquina virtual de PROXMOX utilizado como servidor de corta fuegos PfSense, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

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



Fuente: configuración de interfaces de red para la máquina virtual de PROXMOX utilizado como servidor de corta fuegos PfSense, servidores físicos de laboratorio 014 de la Escuela de Ingeniería en Ciencias y Sistemas.

2.2.3. Análisis e Investigación del modelo de datos

El modelo de datos es parte fundamental del proyecto, ya que almacena toda la información de usuarios, tráfico, políticas e históricos 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, que debido a que no existe ningún tipo de herramienta, documentación o información previa sobre una estructura o modelo de datos, se selecciona 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 detalles del 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 con las características o datos seleccionados que manejara el sistema de acuerdo con los objetivos y funcionalidades de este.

Tabla II. Características y datos seleccionados 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	<ul style="list-style-type: none"> • Nombre y apellido de cada usuario. • Número de carné de cada usuario, el cual será utilizado como clave genérica de acceso. • Correo electrónico del usuario para poder tener contacto con el mismo. • Fecha de nacimiento, característica seleccionada por su importancia para obtener indicadores. • Carrera que estudia, seleccionada por su importancia para definir parámetros de reportería e indicadores de consumo por carrera.
Datos de usuarios administrativos	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Identificador de usuario, que para cada usuario será su número de carné. • Tipo de conexión • Fecha y hora de inicio de conexión.

	<ul style="list-style-type: none"> • Fecha y hora en que se finalizó la conexión del usuario. • Fecha y hora en que se realizó la ultima actualización de datos de conexión. •
Datos de dispositivo de acorde a la conexión del usuario en la red	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 estructura 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 definición.

Para la selección de las herramientas de desarrollo del proyecto se contó con la participación y solicitud por parte del coordinador de los laboratorios, ya

que al ser ingeniero en ciencias y sistemas se involucró en el aspecto técnico tomando en cuenta los aspectos técnicos que le favorecerían a largo plazo para darle continuidad al proyecto.

A continuación, se presenta la lista de cada herramienta seleccionada junto a su tipo o uso para la elaboración del proyecto, así como 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 <i>servlet</i> de comunicación entre interfaz de usuario y <i>backend</i> .
Lenguaje de programación Frontend	JavaScript	Lenguaje de programación sin tipado estático y orientado a su uso en <i>frontend</i> 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	

Protocolo de autenticación, autorización y contabilización (AAA)	RADIUS	
Servidor AAA	FreeRADIUS	Servidor RADIUS de código abierto y gratuito
Servidor DNS, DHCP y Firewall	PfSense	
Servidor Web	Apache Tomcat	
Sistema Operativo	Linux Ubuntu 18.04 y 12.0	
Librerías y frameworks de desarrollo web	<ul style="list-style-type: none"> • Boostrap 4 • JQuery 3.2 • EasyUI 	
IDE de desarrollo	<ul style="list-style-type: none"> • Netbeans 	
Patrón de arquitectura	MVC	

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	• Container en Proxmox
Servidor de base de datos	1	172.10.1.250	• Container 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 y 40 puntos de red
<i>Hypervisor o entorno de virtualización</i>	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 de red existente, así como la utilización de las herramientas que actualmente implementan en los servidores físicos de los laboratorios con un añadido de infraestructura y ordenamiento de la red.

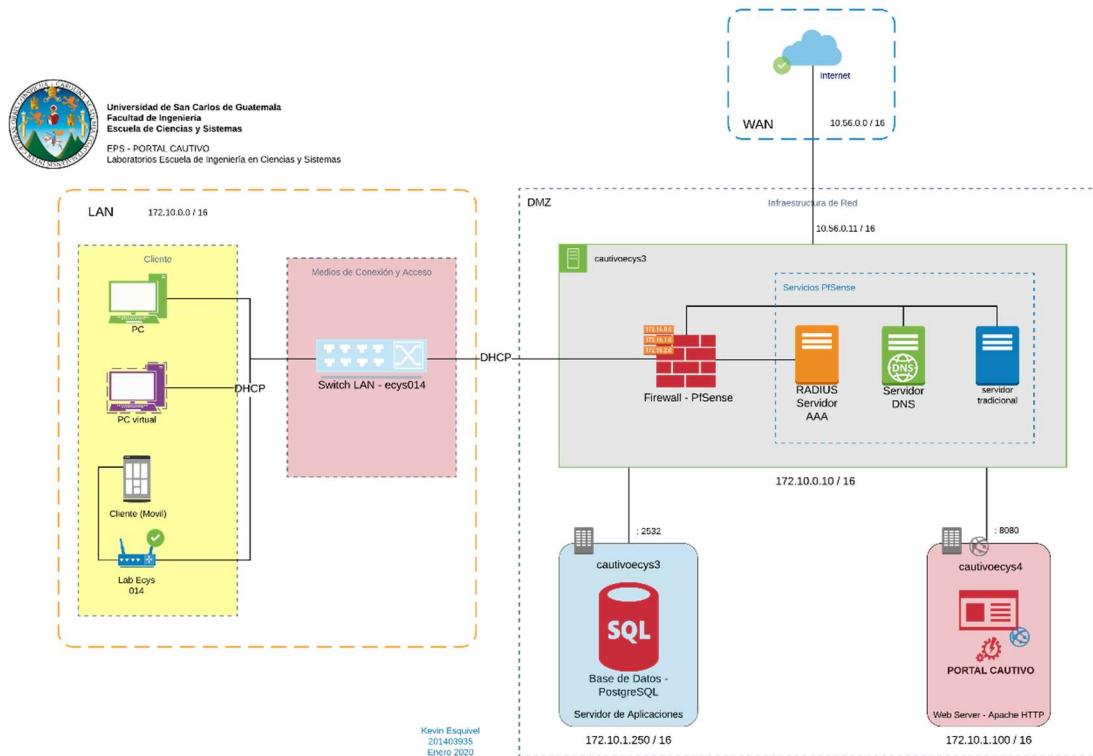
En principal añadido que presenta la solución del proyecto es la esquematización de la red en segmentos de LAN y WAN por medio de una zona

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, así como la conexión que existirá entre los componentes considerando esta como bidireccional ya que 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, así como 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.	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Registro de usuarios a través del portal cautivo, previo a su autorización de conexión a la

	primera conexión a la red inalámbrica.	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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Consumo de internet delimitado por políticas de la red. • Tiempo de conexión delimitado por las políticas.
HI 5	Como administrador deseo visualizar y exportar reportes de consumo de la red de internet inalámbrico	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Implementación servidor RADIUS. • Integración servidor RADIUS al portal cautivo y administrativo.

Fuente: elaboración propia.

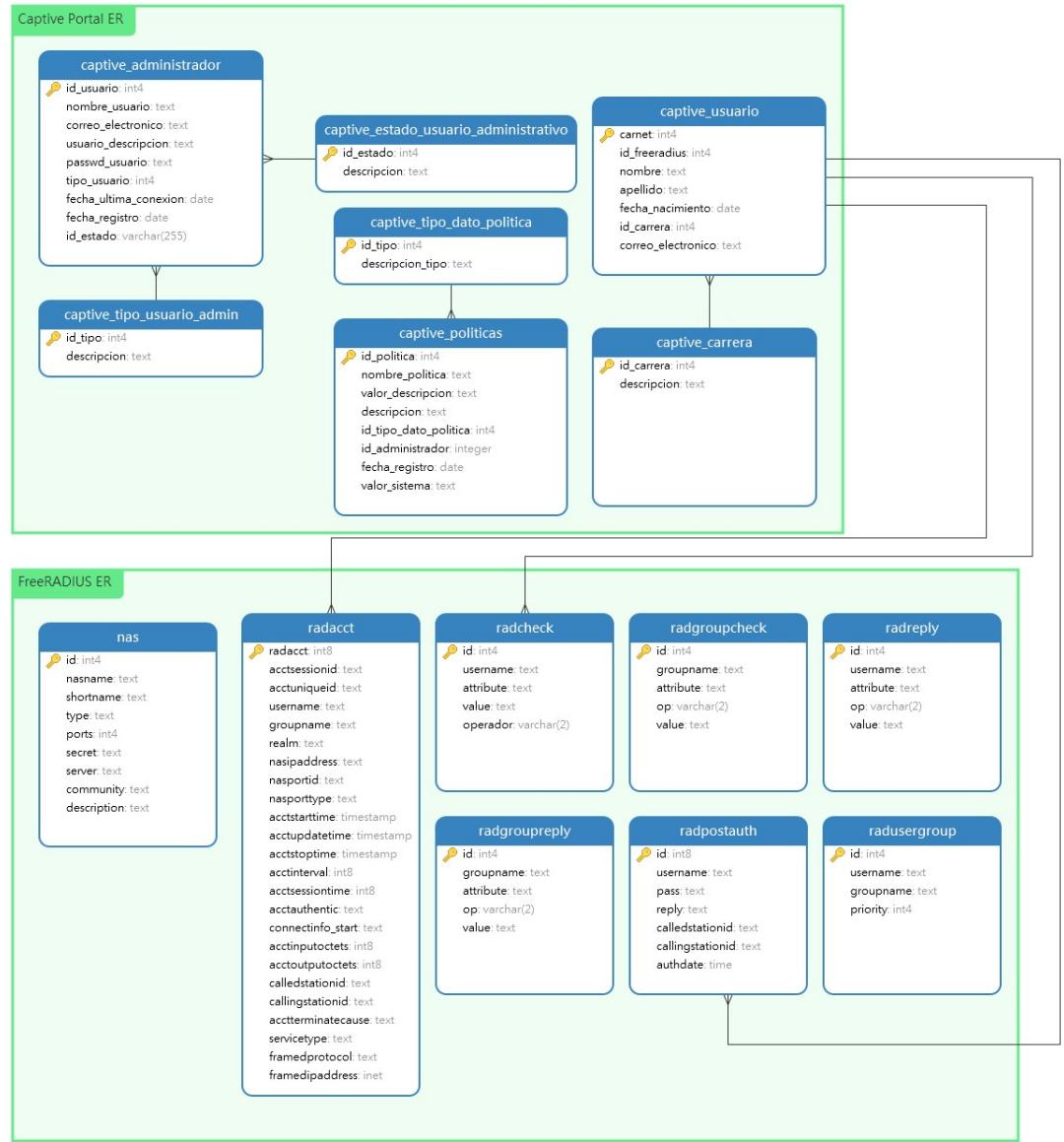
2.3.3. Modelo de datos

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 ya que 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 los mismos 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.

El modelo de datos

2.3.3.1.1. 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 el 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.

2.3.3.1.2. 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: <ul style="list-style-type: none"> • Historial de tiempo de conexión. • Historiales de consumos de datos para carga y descarga. • Identificación específica 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 anteriormente 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.
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 respuesta 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 y funcionalidad, así como su función de interrelación con las demás entidades que conforman el modelo de datos.

Tabla VI. 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
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. Se almacena en cadena de texto en 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 VII. 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 VIII. **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 IX. **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 X. **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 XI. **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 XII. 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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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 detalló de manera tabular el gráfico de líneas clasificando por días las conexiones existentes,

		<p>así como su estado actual con una representación de colores el estado de los usuarios y su conexión con la red.</p> <ul style="list-style-type: none"> • 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 cual 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.
Gestión de Usuarios	Módulo para la gestión de usuarios tanto administrativos del sistema como de la red.	<ul style="list-style-type: none"> • Listado de los usuarios administrativos con la presentación de su información de libre acceso.

		<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 el cual se muestra 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 XIII. Módulos del portal cautivo

Nombre	Descripción	Funcionalidad
Acceso	Módulo de acceso a la red interna de los laboratorios.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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, así como 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

The screenshot shows the Apache Tomcat 9.0.27 homepage. At the top, there is a navigation bar with links to Home, Documentation, Configuration, Examples, Wiki, and Mailing Lists, along with a Find Help button. The main header says "Apache Tomcat/9.0.27". Below the header, a green banner displays the message: "If you're seeing this, you've successfully installed Tomcat. Congratulations!". To the left of the banner is a cartoon cat icon. To the right are three buttons: Server Status, Manager App, and Host Manager. Underneath the banner, there's a section titled "Recommended Reading:" with links to Security Considerations How-To, Manager Application How-To, and Clustering/Session Replication How-To. Below this, there's a "Developer Quick Start" section with links to Tomcat Setup, First Web Application, Realms & AAA, JDBC DataSources, Examples, Servlet Specifications, and Tomcat Versions. The main content area is divided into three columns: "Managing Tomcat" (with links to Release Notes, Changelog, Migration Guide, and Security Notices), "Documentation" (with links to Tomcat 9.0 Documentation, Tomcat 9.0 Configuration, and Tomcat Wiki), and "Getting Help" (with links to FAQ and Mailing Lists, tomcat-announce, tomcat-users, taglibs-user, and tomcat-dev). At the bottom, there are links for Other Downloads (Tomcat Connectors, Tomcat Native, Taglibs, Deployer), Other Documentation (Tomcat Connectors, mod_ajp Documentation, Tomcat Native, Deployer), Get Involved (Overview, Source Repositories, Mailing Lists, Wiki), Miscellaneous (Contact, Legal, Sponsorship, Thanks), and Apache Software Foundation (Who We Are, Heritage, Apache Home, Resources).

Fuente: página web y consola de administración para el servidor web Apache Tomcat en su versión 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

```
root@cautivoecys3:/etc/systemd/system# systemctl status tomcat
* tomcat.service - Apache Tomcat Web Application Container
  Loaded: loaded (/etc/systemd/system/tomcat.service; disabled; vendor preset: enabled)
  Active: active (running) since Wed 2019-10-23 01:43:51 UTC; 8s ago
    Process: 5310 ExecStart=/opt/tomcat/bin/startup.sh (code=exited, status=0/SUCCESS)
   Main PID: 5317 (java)
     Tasks: 43 (limit: 4915)
    CGroup: /system.slice/tomcat.service
            `-5317 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Djava.util.logging.config.file=logging.properties

Oct 23 01:43:51 cautivoecys3 systemd[1]: Starting Apache Tomcat Web Application Container...
Oct 23 01:43:51 cautivoecys3 systemd[1]: Started Apache Tomcat Web Application Container.
```

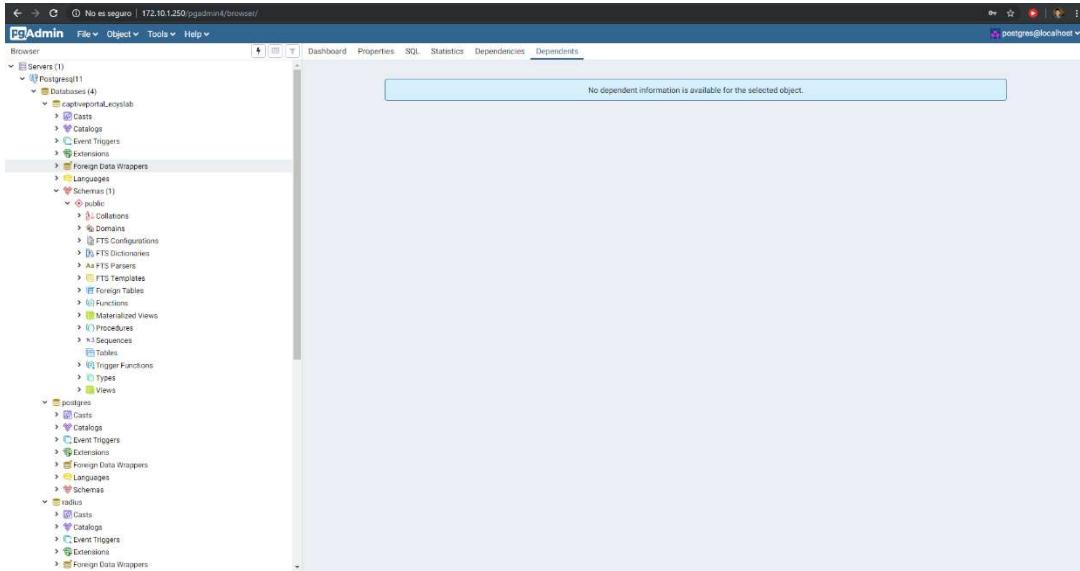
Fuente: consola del sistema operativo Linux 18.04 con el estado del proceso de ejecución del servidor web Apache Tomcat en su versión 9.0.27.

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: página web del servicio PgAdmin4 y editor de base de datos para el sistema gestor de base de datos PostgreSQL en su versión 11.

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#
```

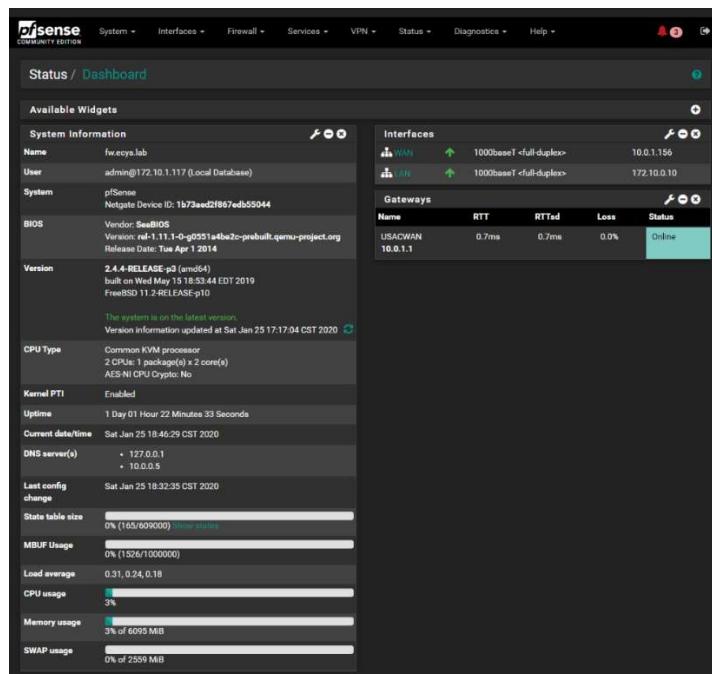
Fuente: consola del sistema operativo Linux 18.04 con el estado del proceso de ejecución del sistema gestor de base de datos en su versión 11.

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: consola de administración web del servidor de corta fuegos PfSense en su versión 2.4.4.

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

```

[2.4.4-RELEASE][root@fw.ecys.lab]/root: exit
exit
pfSense - Netgate Device ID: 1b73aed2f867edb55044

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on fw ***

WAN (wan)      -> em2          -> v4: 10.0.1.156/24
LAN (lan)      -> em0          -> v4: 172.10.0.10/16

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

Fuente: Consola administrativa del servidor de corta fuegos PfSense versión 2.2.4 para gestión directa desde el sistema operativo instalado dentro del sistema de virtualización PROXMOX.

2.3.5.4. Servidor de autenticación, autorización y contabilización RADIUS

Para realizar la implementación del servidor RADIUS se seleccionó la herramienta FreeRADIUS la cual 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

The screenshot shows the PfSense FreeRADIUS Settings page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a notification icon with 3 alerts. The main menu has tabs for Users, MACs, NAS / Clients, Interfaces, Settings (which is selected), EAP, SQL, LDAP, View config, and XMLRPC Sync.

General Configuration

- Maximum Requests Tracked:** 1024 (Default: 1024). Description: The maximum number of requests which the server keeps track of until 'Cleanup Delay' deletes them. If set too low, it will make FreeRADIUS server busy. A higher value is better (but means increased RAM usage). Useful range: (256 * < number of NAS >) Shouldn't be higher than (1000 * < number of NAS >) (Default: 1024).
- Maximum Request Timeout:** 30 (Default: 30). Description: The maximum time to handle a request (in seconds). (Default: 30)
- Cleanup Delay:** 5 (Default: 5). Description: The time to wait before cleaning up a reply which was sent to the NAS (in seconds). (Default: 5)
- Allow Core Dumps:** Enable (Default: Disable). Description: Only enable if you need to debug the RADIUS server! (Default: Disable)
- Regular Expressions:** Enable (Default: Enable). Description: Allows to use regular expressions. (Default: Enable)
- Extended Expressions:** Enable (Default: Enable). Description: Allows to use extended expressions. (Default: Enable)

Logging Configuration

- RADIUS Logging Destination:** /var/log/radius.log (Default: System Log). Description: Choose the destination for FreeRADIUS logs. This will log general service information, but no authentication information. (Default: System Log)
- RADIUS Logging:** Enable (Default: Disable). Description: This enables logging of accepted or rejected authentication. (Default: Disable)
- Log Password on Authentication Failure:** No (Default: No). Description: Log the password of failed authentication attempts to syslog. Not recommended for security reasons. (Default: No)
- Additional Information for Bad Attempts:** (Text input field). Description: You can add additional information to the syslog output if a user connects. Click Info for details. (Info icon)
- Log Password on:** (Text input field). Description: (Default: No)

Fuente: módulo de configuración de servidor FreeRADIUS, empleando servidor de corta fuegos PfSense.

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

Enable SQL Database - Server 1

- SQL Support**: **Enable SQL Support**. Enable this to allow connections from FreeRADIUS to a SQL database. At least one of the following options must be enabled: Authorization, Accounting, Session, Post-Auth. (Default: Disabled)
- Enable SQL Authorization**: Enable this if usernames and passwords are stored on a SQL database. SQL support must be enabled for this to work. (Default: Disable)
- Enable SQL Accounting**: Enable this if accounting packets should be logged to a SQL database. SQL support must be enabled for this to work. (Default: Disable)
- Enable SQL Session**: Enable this to use the 'rlm_sql' module (fast) to check for simultaneous connections instead of "radutmp" (slow). SQL support must be enabled for this to work. (Default: Disable)
- Enable SQL Post-Auth**: Enable this if you like to store post-authentication data on a SQL database. SQL support must be enabled for this to work. (Default: Disable)

SQL Database Configuration - Server 1

- Database Type**: PostgreSQL. Choose the database type. (Default: MySQL)
- Server Address**: 172.10.1.250. Database server FQDN or IP address. (Default: localhost)
- Server Port**: 5432. Enter the port of the database server. (Default: 3306)
- Database Username**: postgres. Enter the username for the database server. (Default: radius)
- Database Password**: Enter the password for the database server user. (Default: radpass)

Fuente: módulo de conexión de servidor FreeRADIUS con servidor de base de datos PostgreSQL, empleando servidor de corta fuegos PfSense.

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

SQL Database Configuration - Server 1

Database Type	PostgreSQL Choose the database type. (Default: MySQL)
Server Address	172.10.1.250 Database server FQDN or IP address. (Default: localhost)
Server Port	5432 Enter the port of the database server. (Default: 3306)
Database Username	postgres Enter the username for the database server. (Default: radius)
Database Password Enter the password for the database server user. (Default: radius)
Database Table Configuration	radius Choose database table configuration. Click here for details. (Default: radius)
Accounting Table 1 (Start)	radacct This is the accounting "Start" table. Choose the same name for both if you want to log "Start" and "Stop" to the same table. (Default: radacct)
Accounting Table 2 (Stop)	radacct This is the accounting "Stop" table. Choose the same name for both if you want to log "Start" and "Stop" to the same table. (Default: radacct)
Post Auth Table	radpostauth Choose Post Auth Table. (Default: radpostauth)
Auth Check Table	radcheck Choose Auth Check Table. (Default: radcheck)
Auth Reply Table	radreply Choose Auth Reply Table. (Default: radreply)
Group Check Table	radgroupcheck Choose Group Check Table. (Default: radgroupcheck)
Group Reply Table	radgroupreply Choose Group Reply Table. (Default: radgroupreply)
User Group Table	radusergroup Choose User Group Table. (Default: radusergroup)
Read the Group Tables	No If checked, You will be prompted to read all the group tables.

Fuente: módulo de conexión de servidor FreeRADIUS con servidor de base de datos PostgreSQL, empleando servidor de corta fuegos PfSense.

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 XIV. 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
Puerto servidor	Número de puerto que está habilitada para comunicación con el	5432

	sistema gestor de base de datos PostgreSQL.	
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
Tabla de repuestas de autenticación	Nombre de la tabla que almacenará la información de todos los intentos de autenticación que se intentaron realizar	radpostauth

	por medio del portal cautivo para la red LAN de los laboratorios.	
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.	<ul style="list-style-type: none"> • 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
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	Si

	remotamente sobre la base de datos.	
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
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	0

	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.	
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

```

/usr/local/etc/raddb/mods-enabled/sql

sql sql1 {
    database = "postgresql"
    driver = "pgsql"
    dialect = "${database}"
    server = "172.10.1.250"
    port = 5432
    login = "postgres"
    password = "admin"
    radius_db = "radius"
    acct_table1 = "radacct"
    acct_table2 = "radacct"
    postauth_table = "radpostauth"
    authcheck_table = "radcheck"
    authreply_table = "radreply"
    groupcheck_table = "radgroupcheck"
    groupreply_table = "radgroupreply"
    usergroup_table = "radusergroup"
    read_groups = no
    delete_stale_sessions = yes
    logfile = ${logdir}/sqltrace.sql
    read_clients = no
    client_table = "nas"
    pool {
        start = ${thread[pool].start_servers}
        min = ${thread[pool].min_spare_servers}
        max = 5
        spare = ${thread[pool].max_spare_servers}
        uses = 0
        retry_delay = 60
        lifetime = 0
        idle_timeout = 60
    }
    group_attribute = "${::instance}-SQL-Group"
    $INCLUDE ${modconfdir}/${::name}/main/${dialect}/queries.conf
}

```

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 [View license](#).

Fuente: archivo de configuración de módulo SQL de servidor 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

The screenshot shows the pfSense FreeRADIUS configuration interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a notification icon with a '3'. Below the navigation is a breadcrumb trail: Package / FreeRADIUS / View Configuration. A sub-navigation bar below the breadcrumb includes tabs for Users, MACs, NAS / Clients, Interfaces, Settings, EAP, SQL, LDAP, View config (which is selected), and XMLRPC Sync. The main content area is titled 'View FreeRADIUS Configuration Files' and displays the contents of the '/usr/local/etc/raddb/clients.conf' file. The configuration file contains two client definitions: 'Ecys014CP' and 'ecys'. Both clients have ipaddr set to 172.10.0.10 and proto set to udp. The 'Ecys014CP' client has a secret of 'ECYS' and nas_type of other. The 'ecys' client has a secret of 'ecys' and nas_type of other. Both clients have a limit section with max_connections = 16, lifetime = 0, and idle_timeout = 30.

```

/usr/local/etc/raddb/clients.conf

client "Ecys014CP" {
    ipaddr = 172.10.0.10
    proto = udp
    secret = 'ECYS'
    require_message_authenticator = no
    nas_type = other
    ### login = !root ###
    ### password = someadminpass #####
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}

client "ecys" {
    ipaddr = 127.0.0.1
    proto = udp
    secret = 'ecys'
    require_message_authenticator = yes
    nas_type = other
    ### login = !root ###
    ### password = someadminpass #####
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}

```

Fuente: archivo de configuración de cliente NAS para proveedor de servicio portal cautivo dentro de la red LAN.

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

Tabla XV. 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	udp

	usuarios y autenticación de los mismos.	
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, identifica al tipo de proveedor y permite el uso de un catálogo de parámetros específico para la aplicación de políticas de red. Por defecto el valor other permite la inclusión de las 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.	<ul style="list-style-type: none"> • 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 ya que 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 XVI. 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	<ul style="list-style-type: none"> • 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: •

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.

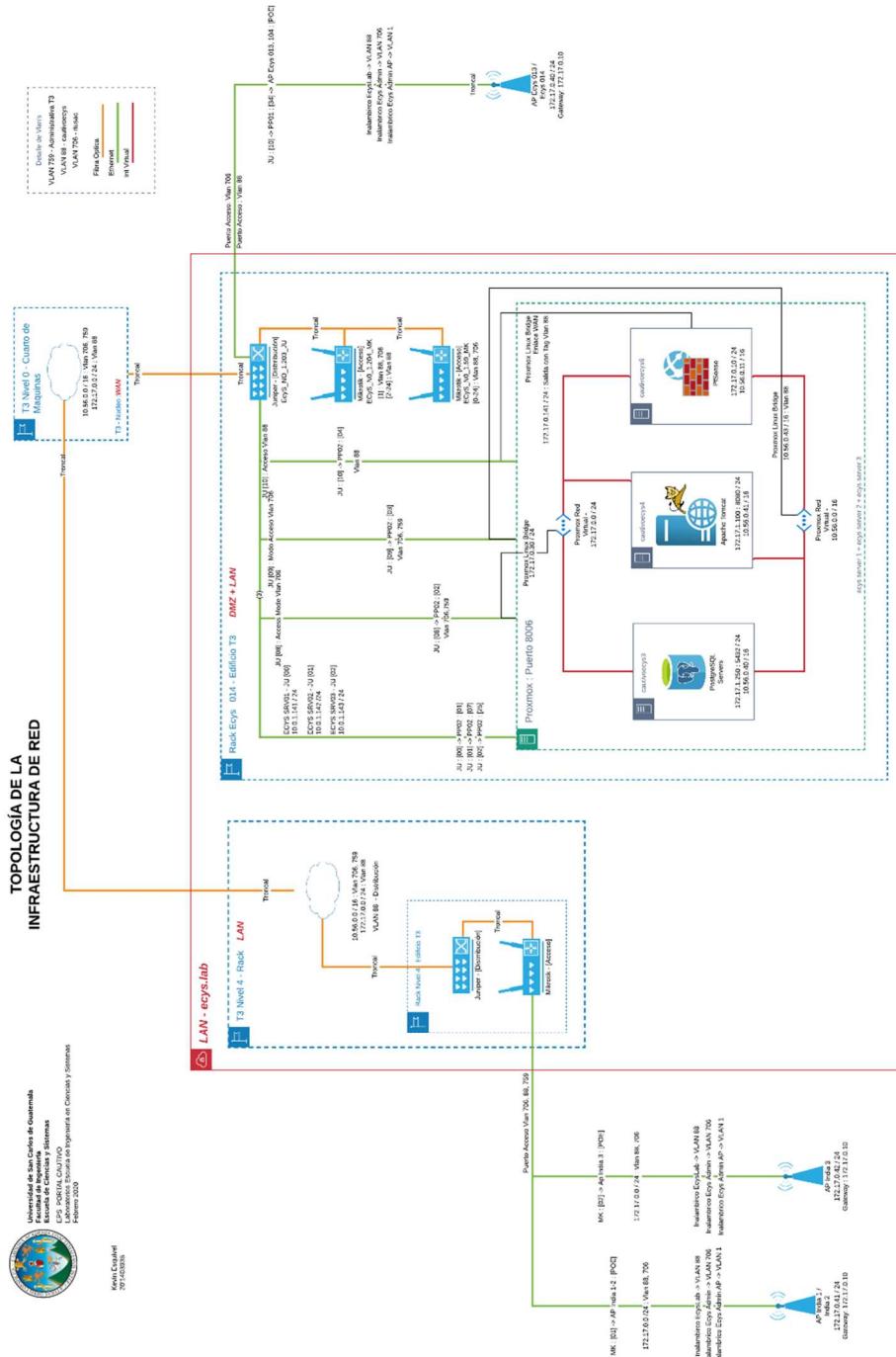
El cableado estructurado utilizado es exactamente el existente ya que la oficina de Procesamiento de Datos de la Universidad ya tenía contemplado y documentado un diseño de red y distribución de puertos para los laboratorios. El

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



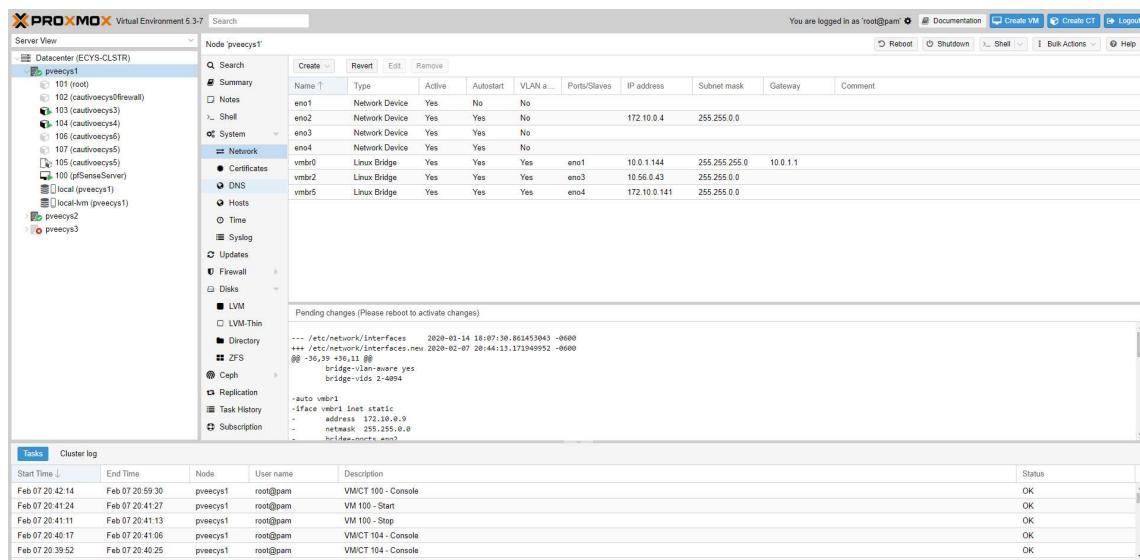
Fuente: elaboración propia, empleando Lucidchart en su versión web.

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 de la 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 puentes para interconexión con contenedores y máquinas virtuales



Fuente: consola de administración Proxmox, servidor físico laboratorios Escuela de Ingeniería en Ciencias y Sistemas.

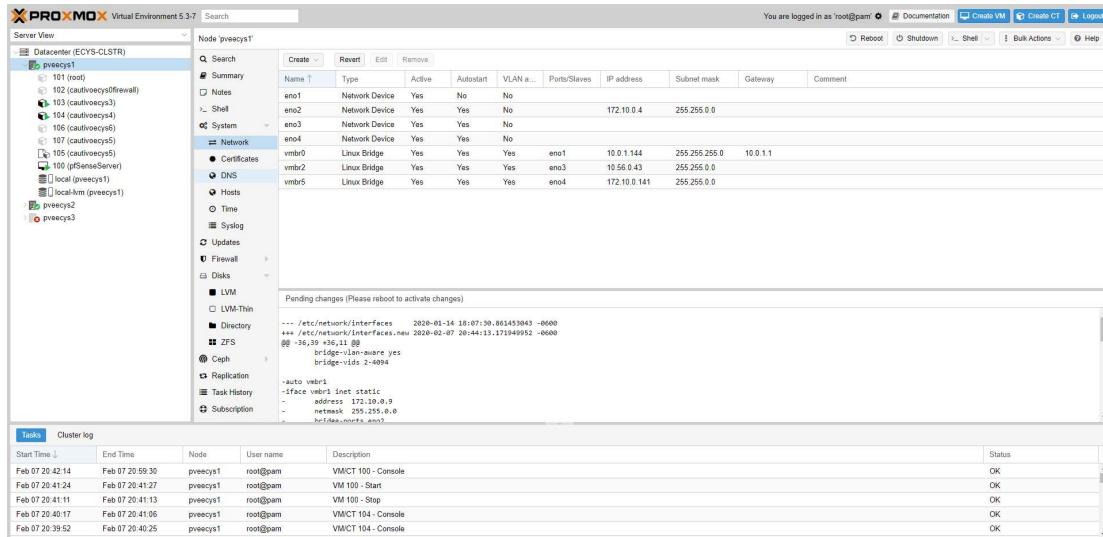
Así mismo a continuación se presenta la tabla que detalla cada una de las funciones de cada interfaz de red configurada.

Tabla XVII. 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 <i>patch panel</i> 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 <i>patch panel</i> 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 <i>patch panel</i> 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 <i>patch panel</i> 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	Interfaz física: eno1	Dirección IP pública: 10.0.1.144 / 16

		máquinas virtuales creados en PROXMOX.		
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

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



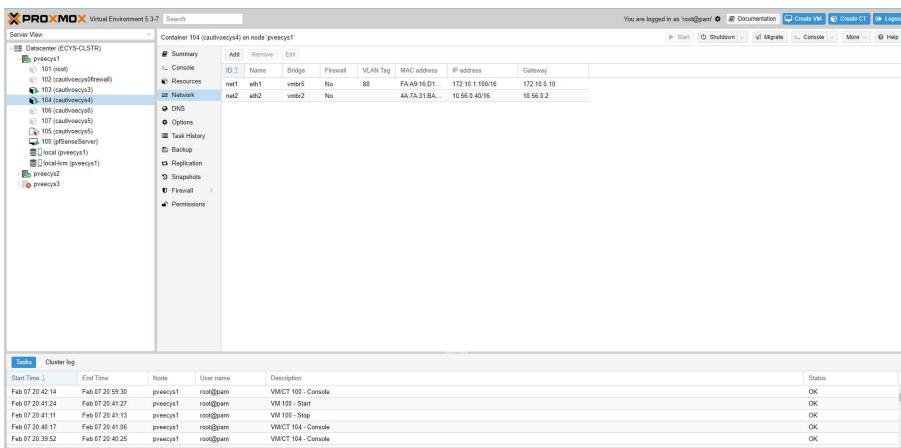
Fuente: consola web de administración de interfaces de red del contenedor cautivoecys3, sistema de virtualización PROMOX.

Tabla XVIII. 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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



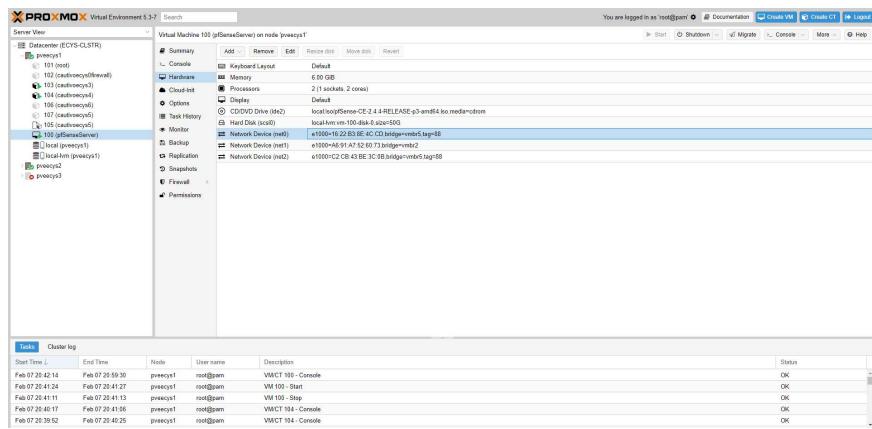
Fuente: consola web de administración de interfaces de red del contenedor cautivoecys4, sistema de virtualización PROMOX.

Tabla XIX. 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 cortafuegos



Fuente: consola web de administración de interfaces de red de la máquina virtual pfSenseServer, sistema de virtualización PROMOX.

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
net0	eth1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 XXI. 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.

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.

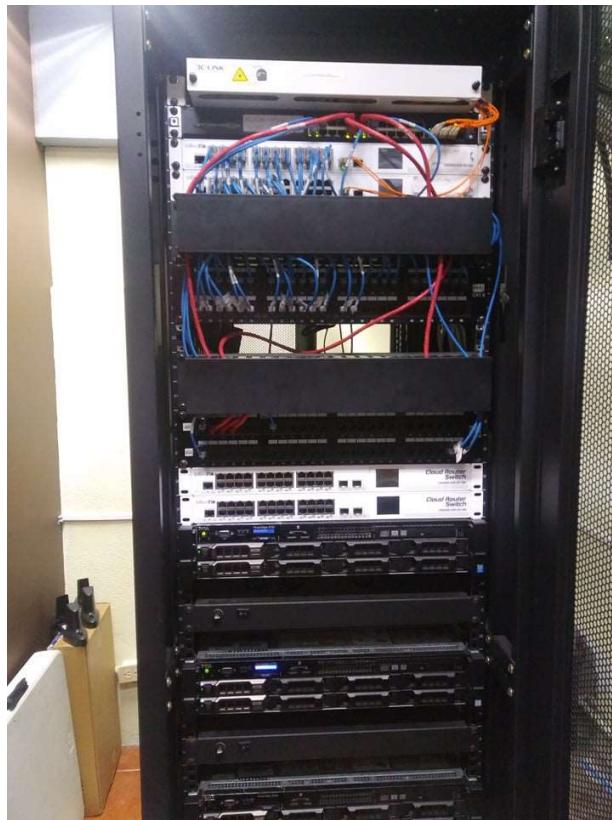
Fuente: elaboración propia.

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



Fuente: elaboración propia.

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



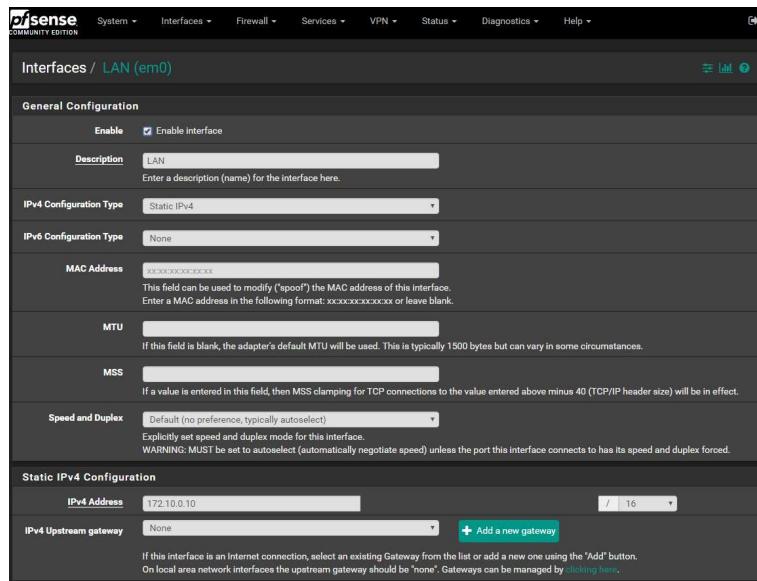
Fuente: elaboración propia.

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, consola de administración de servidor corta fuegos PfSense.

Tabla XXII. 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	IPv4 estático

	dentro de la red y su correcto funcionamiento se le asigna una IP estática.	
Tipo de configuración IPv6	Valor que define que 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	172.10.0.10 / 16

	la red y conexión con los servicios de DNS.	
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

The screenshot shows the 'Interfaces / WAN (em2)' configuration page in pfSense. The 'General Configuration' section includes fields for 'Enable' (checked), 'Description' (WAN), 'IPv4 Configuration Type' (Static IPv4), 'IPv6 Configuration Type' (None), 'MAC Address' (xxxx:xxxx:xxxx:xx), 'MTU' (blank), 'MSS' (blank), and 'Speed and Duplex' (Default). The 'Static IPv4 Configuration' section shows 'IPv4 Address' (10.0.1.156), 'IPv4 Upstream gateway' (USACWAN - 10.0.1.1), and a note about selecting an upstream gateway. A note at the bottom states: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.'

Fuente: elaboración propia.

Tabla XXIII. 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 hacia 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
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 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 para poder obtener el servicio de internet del proveedor de servicio hacia 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 hacia WAN para proveer de servicio de internet

Parte importante de la creación e implementación de una DMZ es la separación lógica de una red con respecto a su proveedor de servicios, para dar solución a el proyecto es necesaria la implementación de una zona de red desmilitarizada en la cual el de tráfico desde la red LAN debe ser ruteado hacia la red WAN y viceversa, pero sin existir la posibilidad de comunicación desde la WAN hacia la LAN. La implementación del portal cautivo por medio de un servidor de corta fuegos permite la creación lógica por medio de un ruteo entre interfaces de red asignadas a una red LAN y WAN.

La configuración de ruteo dentro del servidor de corta fuegos PfSense es presentada a continuación, como una parte importante de la implementación de la DMZ para solución del proyecto y dar capacidad al servidor PfSense de proveer internet desde la red WAN hacia la red LAN.

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

Pendiente...!!!!

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

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 hacia donde el servidor de corta fuegos enviará el tráfico de red.

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

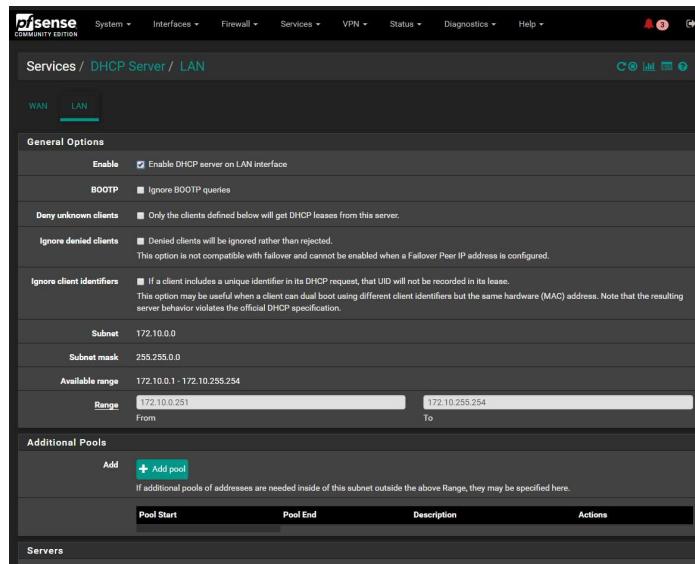
The screenshot shows the pfSense interface under the 'Interfaces' tab, specifically the 'Interface Assignments' section. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a toolbar with icons for signal strength and help. The main content area has tabs for Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIGs, Bridges, and LAGGs. The 'Interface Assignments' tab is selected. A table lists two entries: 'WAN' assigned to 'em2 (b2:84:15:ae:d5:90)' and 'LAN' assigned to 'em0 (16:22:b3:8e:4c:cd)'. A red 'Delete' button is visible next to the LAN entry.

Fuente: elaboración propia, consola de administración de asignación de interfaces en servidor de corta fuegos PfSense.

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, consola de administración de servidor de corta fuegos PfSense.

Tabla XXIV. 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 cual 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 cual se prestará el servicio de DHCP.	255.255.0.0 = /16
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 reenvío 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.

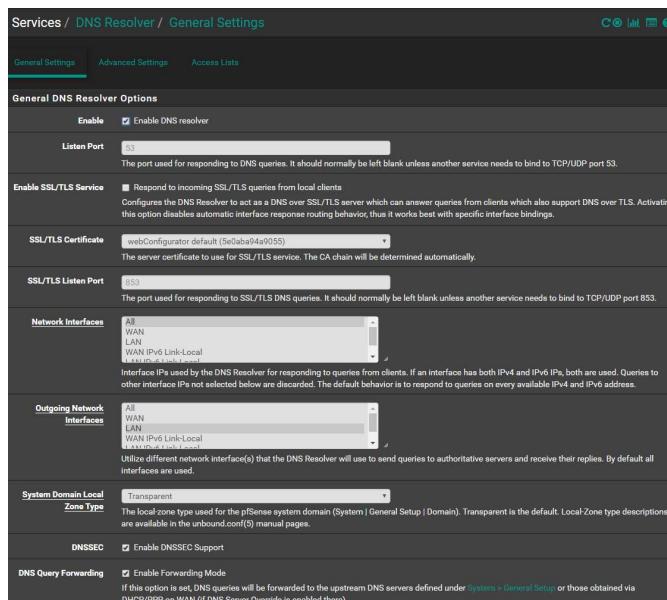
2.3.6.9. Configuración de servidor de resolución DNS para la red LAN

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 hacia 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.

Tabla XXV. Detalle de configuración de servidor DNS resolver para la red LAN y WAN

Característica de configuración	Descripción	Valor asignado
Habilitar	Determina si el servidor DNS está habilitado para una interfaz de red específica.	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
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
Reenvío 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 red nueva red interna y DMZ de los laboratorios por medio del servidor de corta fuegos PfSense

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 y comportamiento del portal cautivo, así como a qué red LAN será 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 XXVI. Detalle de configuración de la zona de portal cautivo ECYS014

Característica de configuración	Descripción	Valor asignado	Aplica a política de administración
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
<i>Idle timemout</i>	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

<i>Hard timeout</i>	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
<i>Traffic quota</i>	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 1000	1000	Si

	kilobits por segundo es equivalente a 1 megabit por segundo de ancho de banda disponible.		
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 1000 kilobits por segundo es equivalente a 1 megabit por segundo de ancho de banda disponible.	1000	Si
Utilizar una página personalizada de portal cautivo	Habilita el uso de una página web personalizada de portal cautivo.	Habilitado	No
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 autenticación, 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

Servidor de autenticación	Define el servidor de autenticación a utilizar.	Servidor de FreeRADIUS	No
Identificar NAS	Nombre del identificar de cliente de difusión de la red.	Ecys014CP	No
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
RADIUS	Habilita el envío a servidor RADIUS los paquetes de contabilidad.	Habilitado	No
Servidor de contabilización	Establece hacia 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 esta habilitado RADIUS considera los paquetes del cliente como de descarga y los que	Habilitado	No

	reciba del mismo como de subida.		
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 enrutadores

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.

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
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 XXVII. 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

<i>Packet Forward</i>	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
<i>Hotspot Service</i>	Indica el servicio de Hotspot que será utilizado por el punto de acceso para emisión de tráfico.	Ninguno
<i>Access VLAN</i>	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
<i>Dynamic VLAN</i>	Establece si el punto de acceso puede transmitir tráfico de red para números de VLAN que pueden cambiar en cualquier momento.	Deshabilitado
<i>Insert DHCP option 92</i>	Establece si se añade a la información de tráfico información adicional sobre el origen.	Deshabilitado
<i>Client Fingerprinting</i>	Habilita la	Deshabilitado
<i>Encryption Method</i>	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
<i>WPA Version</i>	Versión de encriptación que se utilizará para los usuarios conectados al dispositivo de puntos de acceso.	WPA+WPA2
<i>WPA Authentication</i>	Establece la forma en que se realizará la autenticación.	PSK
<i>WPA Algorithm</i>	Determina el tipo de algoritmo utilizado para la autenticación.	AES
<i>Passphrase</i>	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

The screenshot shows the 'Configuration :: Internet' page of the Ruckus web interface. The left sidebar has a 'Configuration' section selected, showing links for Device, Internet, Local Subnets, Radio 2.4G, Radio 5G, Ethernet Ports, and Hotspot. The main configuration area includes fields for NTP Server (ntp.ruckuswireless.com), Management VLAN (1), IPv4 Connection Type (Static IP selected), Internet Connection Settings (IPv4 Address: 172.10.0.40, Subnet Mask: 255.255.0.0, Gateway: 172.10.0.10), IPv4 DNS Mode (Auto selected), and IPv6 Connection Type (Auto Configuration selected). At the bottom, there are buttons for 'Update Settings' and 'Restore previous settings'.

Fuente: elaboración propia, consola de administración web de puntos de acceso inalámbrico Ruckus R710 y R310.

Tabla XXVIII. 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.

Figura 34.

Figura 35. Configuración de los dispositivos de red y servidores



Fuente: elaboración propia, Faculta de Ingeniería.

Figura 36. Configuración de comutadores y enruteadores 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

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

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

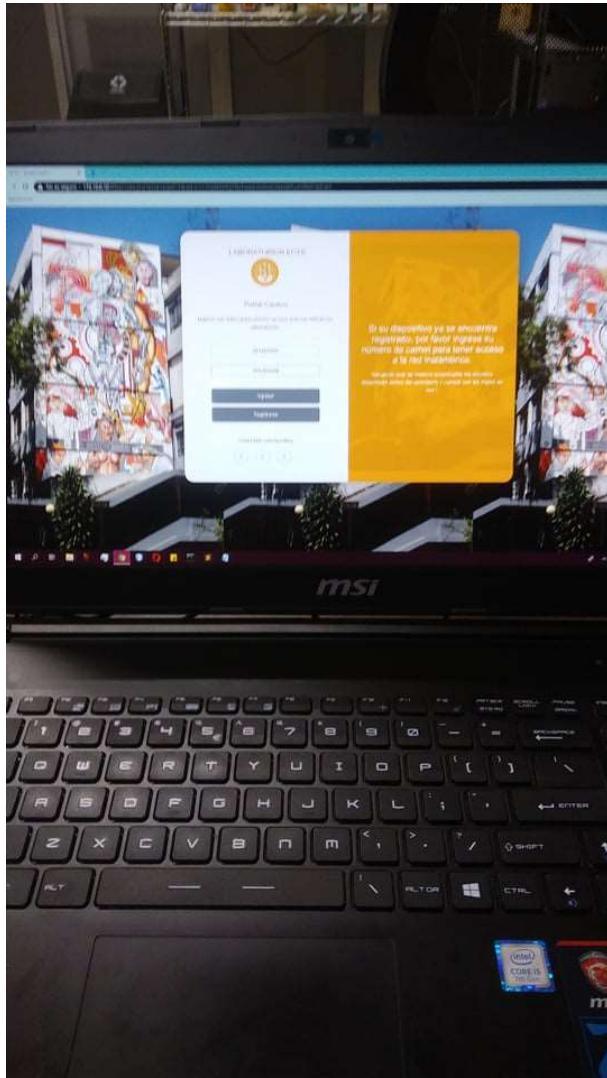
Finalizado el proceso de implementación y desarrollo del portal cautivo y sistema de administración, los resultados finales fueron exitosos y con un alto grado de satisfacción para la coordinación de los laboratorios al realizar la integración de un servicio con el equipo existente y la estandarización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

Figura 37. Resultado final de despliegue e implementación de portal cautivo en dispositivos móviles



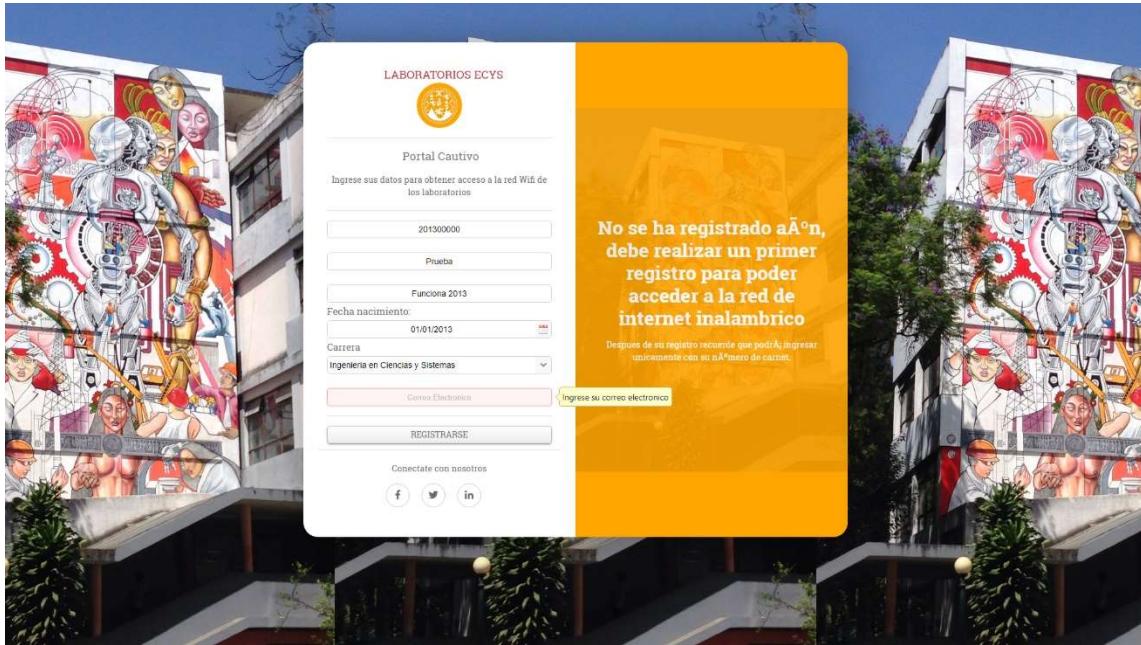
Fuente: elaboración propia, portal cautivo en dispositivos móviles.

Figura 38. Resultado final de implementación y despliegue de portal cautivo en computadoras portátiles por red cableada e inalámbrica



Fuente: elaboración propia, portal cautivo en computadoras portátiles. Laboratorios de Escuela de Ingeniería en Ciencias y Sistemas.

Figura 39. Resultado final de página de registro de portal cautivo en computadoras portátiles



Fuente: elaboración propia.

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

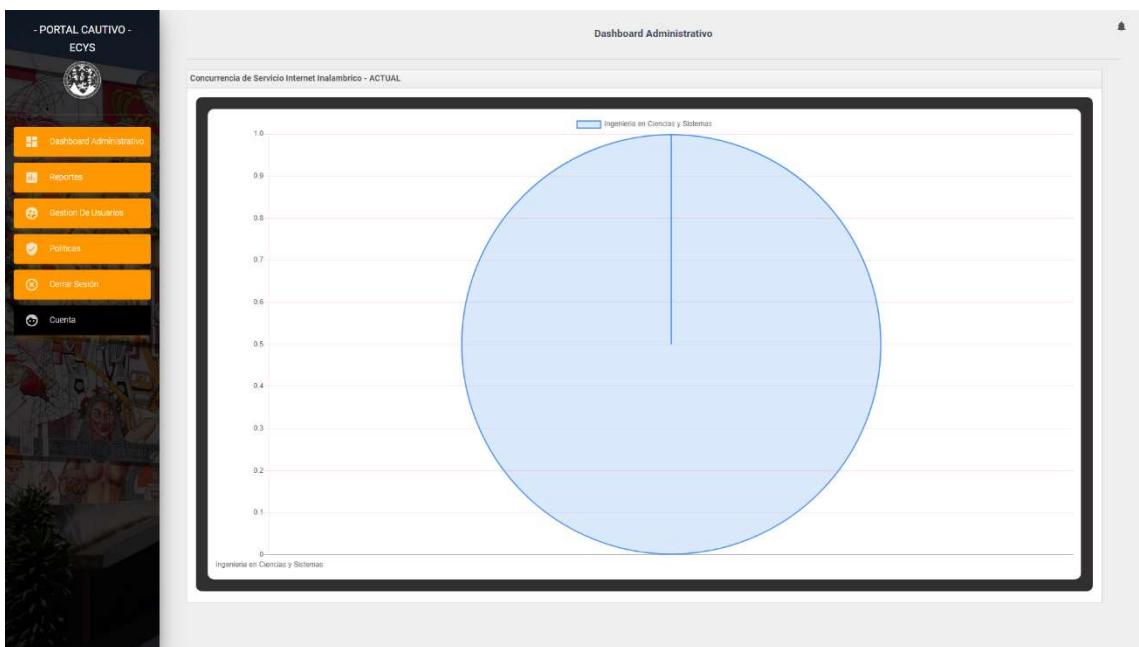
A continuación, se muestran los resultados de la implementación del portal cautivo y sistema de administración de la red.

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.

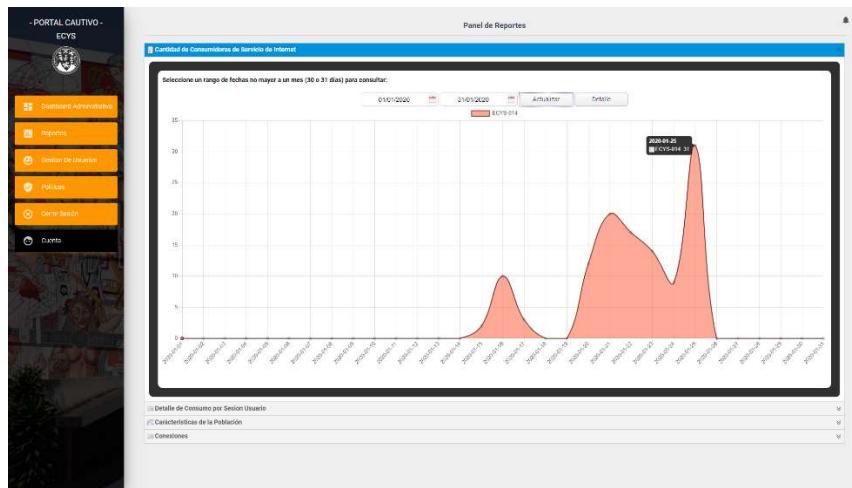
La primera implementación y elaboración de pruebas tanto funcionales como de rendimiento fueron llevadas a cabo durante el mes de enero de 2020 con resultados altamente satisfactorios al obtener los primeros datos reales acerca del consumo y utilización de la red por parte de la población estudiantil.

Figura 40. Tablero de reporte en tiempo real de la concurrencia de usuarios de la red clasificados por carrera universitaria



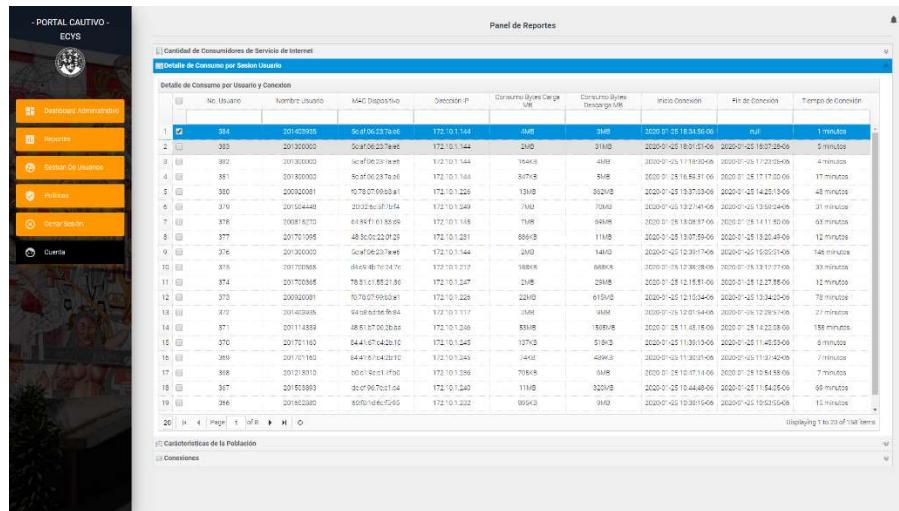
Fuente: elaboración propia.

Figura 41. Módulo de reportes, reporte por cantidad de consumidores por rango de fechas



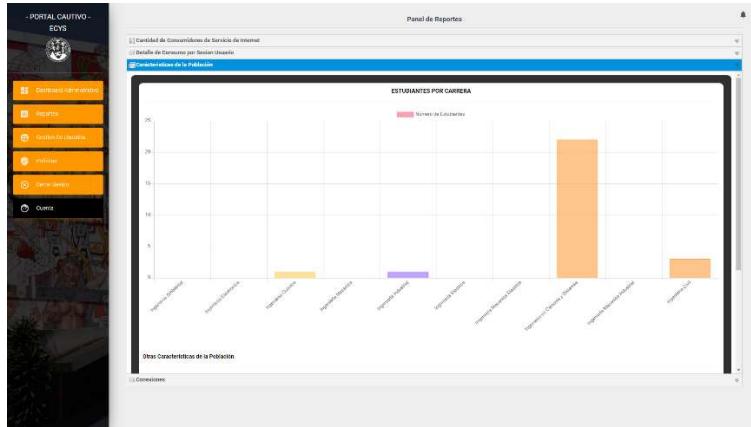
Fuente: elaboración propia.

Figura 42. Módulo de reportes, reporte tabular del detalle de consumo por sesión y usuario



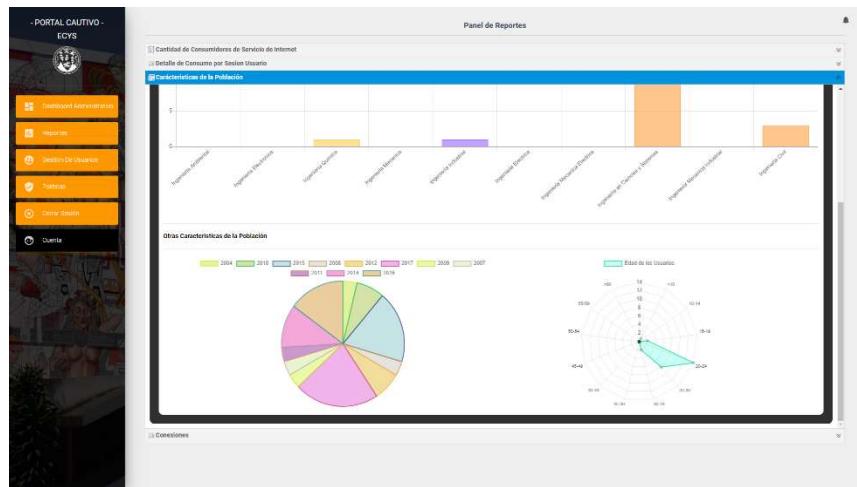
Fuente: elaboración propia.

Figura 43. Módulo de reportes, gráfico de barras del número de estudiantes por carrera de la Facultad de Ingeniería registrados como usuario de la red



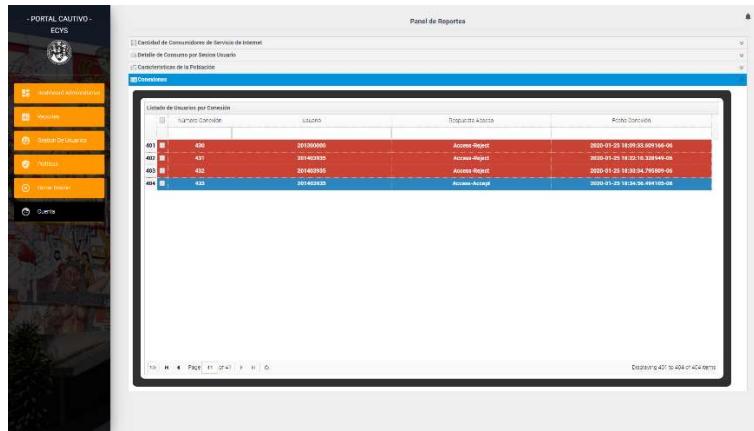
Fuente: elaboración propia.

Figura 44. 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.

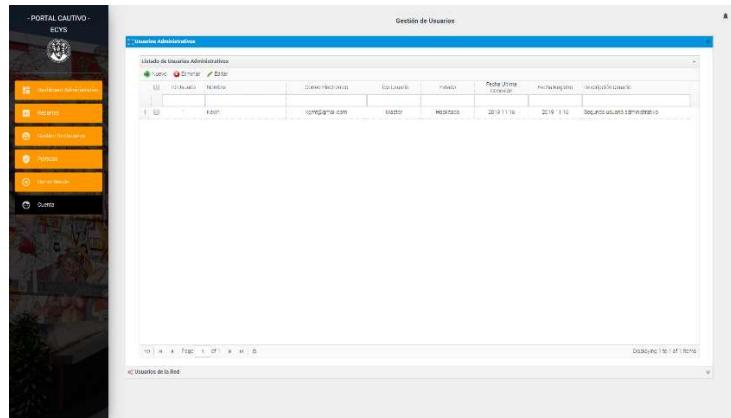
Figura 45. Módulo de reportes, reporte tabular de los intentos de conexión registrados por el portal cautivo



Fuente: elaboración propia.

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

Figura 46. Módulo de gestión de usuarios, interfaz de usuario para gestión de usuarios administrativos



Fuente: elaboración propia.

Figura 47. Módulo de gestión de usuarios, interfaz de usuario para gestión de usuarios de la red

ID Usuario	Código	Nombre	Apellido	Fecha Nac.	Contacto	Nombre Contacto
1	8	José	Díaz	01/09/03	josdiaz@gmail.com	Administrador
2	9	Juan	Velázquez	06/01/99	juanvelazquez2001@gmail.com	Administrador
3	10	Karen	Rodríguez	06/05/04	karenrodriguez90@gmail.com	Administrador
4	12	Pedro	Chavez	06/03/01	pedrochavez01@gmail.com	Administrador
5	13	Mario	Delgado	17/11/03	mardelgado@gmail.com	Administrador
6	14	María	José	12/05/97	marijose12@gmail.com	Administrador
7	15	Diego	Alexander	07/07/93	diegalexander93@gmail.com	Administrador
8	16	Javier	Stah	12/01/97	javierstah01@gmail.com	Administrador
9	17	Fernando	Pérez	10/03/09	fernandoperez09@gmail.com	Administrador
10	18	Carmen	Pérez	08/04/96	carmenperez96@gmail.com	Administrador
11	19	José	Pérez	01/01/03	joseperez03@gmail.com	Administrador
12	20	Victor	Gutierrez	10/03/97	victorgutierrez03@gmail.com	Administrador
13	21	Julián	Moreno	10/10/07	julianmoreno07@gmail.com	Administrador
14	22	Diego	Rodríguez	08/03/09	dierodriguez09@gmail.com	Administrador
15	23	Diego	Castro	10/03/07	dcastro07@gmail.com	Administrador
16	24	Monica	Castillo	09/04/00	monicacastillo00@gmail.com	Administrador
17	25	Fabio	Alvarez	04/06/02	fabioalvarez02@gmail.com	Administrador

Fuente: elaboración propia.

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 48. Módulo de gestión de políticas, administración de acceso a usuarios administrativos

ID Usuario	Nombre usuario	Correo electrónico	Tipo de usuario	Estado	Fecha Creación	Fecha Actualización	Último login	Descripción usuario
1	fernando	fernando@gmail.com	Usuario	Activo	10/01/03	2019/11/5	2019/11/8	Segundo usuario administrador

Fuente: elaboración propia.

Figura 49. Módulo de gestión de políticas, interfaz de usuario asignación y des habilitación de políticas de red

ID Política	Nombre Política	Valor	Descripción	Tipo	Fecha Registro
1	Tiempo de Sesión	30000	Tiempo de sesión por usuario, al contrario el tiempo de sesión el usuario tendrá conectado de la red. (El tiempo de conexión por parte del usuario es de un día en blanco/deshabilitado las sesiones no tendrán límite de tiempo, esto puede ocurrir que un usuario esté conectado para siempre si no se configura el tiempo)	Numerico	2020-01-10
2	Tiempo de Espera	3	Tiempo de esperar para que una sesión expire, después de este tiempo el usuario se desconectará y se deshabilita hasta que transcurra el tiempo de espera al usuario sera desconectado de la red. (El tiempo de espera es de 30 segundos en blanco. Si el usuario esté en blanco/deshabilitado las sesiones no tendrán límite de tiempo, esto puede ocurrir que un usuario esté conectado por siempre a pesar de desconectar su dispositivo)	Numerico	2020-01-10
3	URL Inicial	Formato: https://www.mypagina.dominio	https://dtt-ecys.org	Texto	2020-01-10
4	Ancho de Banda Descarga	1000	Máximo valor de ancho de banda (kbit/s) disponible para descarga de datos por los usuarios. 1000 kbit/s = 1Mbps	Numerico	2020-01-10
5	Ancho de Banda de Subida	1000	Máximo valor de ancho de banda (kbit/s) disponible para carga de datos por los usuarios. 1000 kbit/s = 1Mbps	Numerico	2020-01-10
6	Datos disponibles para consumo	Megabytes	Cantidad máxima de datos que un usuario puede utilizar durante una sesión. (1MB)	Numerico	2020-01-10

Fuente: elaboración propia.

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 XXIX. Costos del proyecto

Recursos	Cantidad	Descripción	Costo	Total
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

2.4.1.2. Recurso humano

2.4.1.3. Recurso físico consumible

2.5. Beneficios del proyecto

El desarrollo del proyecto beneficia directamente a un sector de la población estudiantil pero no únicamente eso, por lo que a continuación se presenta una clasificación de los beneficios que proporciona la elaboración y finalización del proyecto.

- Beneficios para los estudiantes de la Facultad de Ingeniería:
 -

CONCLUSIONES

1. Conclusión

RECOMENDACIONES

1. Recomendación.

BIBLIOGRAFÍA

1. Bibliografía

APÉNDICES

Estas páginas contienen información “elaborada por el estudiante” no deben continuar con la numeración de figuras y tablas.

Apéndice 1. Resumen de gastos mensuales

Concepto	Entradas			Salidas			Existencias		
	Cantidad	Precio	Total	Cantidad	Precio	Total	Cantidad	Precio	Total
Compra (I)	300	122	367		250	1.000			617
					250	1.224			
Dev. compra (I)				50	1.224	612	251	100	556
							250	122	

Tipo	Tamaño		Alineación	
	Máquina 1	Máquina 2	Máquina 1	Máquina 2
Char	8	8	8	64
Short	16	24	16	64
Int	32	48	32	64

Fuente: elaboración propia.

ANEXOS

Estas páginas contienen información “recopilada de otras fuentes” no deben continuar con la numeración de figuras y tablas.

Anexo 1. **Mapa de Guatemala**



Fuente: Instituto Geográfico Nacional. *Mapa de Guatemala*. www.ine.gob.gt.

Consulta: septiembre de 2014.