

## TITULO DEL TRABAJO DE TITULACIÓN

"PROPUESTA DEL DISEÑO DE RED Y POLÍTICAS DE SEGURIDAD A NIVEL DE FIREWALL APLICANDO LA HERRAMIENTA PFSENSE PARA EL CONTROL DEL TRÁFICO DE RED Y ADMINISTRACIÓN DEL ANCHO DE BANDA.CASO DE ESTUDIO HOTEL COPACABANA".

## AUTOR

## ORRALA TOMALA CARLOS ALFREDO

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

## TUTOR ING. HAZ LÓPEZ LÍDICE, MSI.

Santa Elena, Ecuador Año 2023



## TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez A. Mgtr. DIRECTOR DE LA CARRERA

ame Lst. Daniel Quirumbay, MSIA. DOCENTE ESPECIALISTA

Ing Lidice Haz López, Msi. TUTOR

2

Ing. Marjorie Coronel S. Mgti. DOCENTE GUÍA UIC



## CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por ORRALA TOMALA CARLOS ALFREDO, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 17 días del mes de febrero del año 2023

#### TUTOR



ING. HAZ LÓPEZ LÍDICE, MSI.



## DECLARACIÓN DE RESPONSABILIDAD

Yo, ORRALA TOMALA CARLOS ALFREDO

## **DECLARO QUE:**

El trabajo de Titulación, Propuesta del diseño de red y políticas de seguridad a nivel de firewall aplicando la herramienta pfsense para el control del tráfico de red y administración del ancho de banda. Caso de estudio Hotel Copacabana, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 17 días del mes de febrero del año 2023

#### **EL AUTOR**

**Carlos Alfredo Orrala Tomala** 



## **CERTIFICACIÓN DE ANTIPLAGIO**

Certifico que después de revisar el documento final del trabajo de titulación denominado (Propuesta del diseño de red y políticas de seguridad a nivel de firewall aplicando la herramienta pfsense para el control del tráfico de red y administración del ancho de banda. Caso de estudio Hotel Copacabana), presentado por el estudiante, ORRALA TOMALA CARLOS ALFREDO fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 10%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

C

OMPILATIO MAGISTE stemas y Telecomunic	R aciones			🔍 🔀 Caja de h	erramientas
	LA TOMALA CARLOS ALFREDO-PROYECTO FINAL #0d9628			10%	~ :
Ubicación de las sir	militudes en el documento :		1		
CONFIGURACIO Agrupar las fue	i≡ Fuentes		🗟 Puntos	de interés	
↑ Fuentes p	rincipales detectadas				
N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales	
1 🚱	www.foroisp.com   Como Crear un User Profile Hotspot en Mikrotik http://www.foroisp.com/threads/1602-Como-Crear-un-User-Profile-Hotspot-en-Mikrotik#:~-text=	2%	1	Palabras idénticas : 2% (357 palabras)	:
2 🕑	repository.unilibre.edu.co https://repository.unilibre.edu.co/bitstream/handle/10901/8798/monografia.pdf?sequence=1&is v Mostrat las 8 fuentes secundarias	1%		Palabras idénticas : 1% (170 palabras)	:

#### TUTOR



ING. HAZ LÓPEZ LÍDICE, MSI.



## AUTORIZACIÓN

#### Yo, ORRALA TOMALA CARLOS ALFREDO

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 17 días del mes de febrero del año 2021

**EL AUTOR** 

**Carlos Alfredo Orrala Tomala** 

## AGRADECIMIENTO

Le agradezco a Dios por haberme brindado la sabiduría, paciencia, dedicatoria en esta etapa de mi vida como un profesional y por darme la fuerza suficiente para seguir en esos momentos difíciles. A mi familia por darme ese apoyo incondicional. A mis docentes que impartieron sus conocimientos en el transcurso de la carrera.

Carlos Alfredo, Orrala Tomala

#### **DEDICATORIA**

A mi querido padre **Celso Junior Orrala Reyes** y mi querida madre **Antonia Elizabeth Tomala de la Cruz** por haberme apoyado y aconsejado en esta etapa de mi vida.

A mi amada esposa **Jennifer Moreno Arcentales** por ser mi motivación, mi complemento, mi fuerza, mi apoyo en los momentos difíciles que se nos presentaban, por ser esa persona que confió hasta el último momento que lograría esta meta y por ser mi despertador en los días que venía cansado del trabajo, **TE AMO**.

A mi hermano **Junior** y hermanas **María E., María L** por brindarme ánimos en seguir adelante.

A mis docentes y mi tutora que estuvieron en el proceso de enseñanza y aprendizaje.

Carlos Alfredo, Orrala Tomala

# ÍNDICE GENERAL

TITULO DEL TRABAJO DE TITULACIÓN	Ι
TRIBUNAL DE SUSTENTACION	II
CERTIFICACIÓN	III
DECLARACIÓN DE RESPONSABILIDAD	IV
DECLARO QUE:	IV
CERTIFICACIÓN DE ANTIPLAGIO	V
AUTORIZACIÓN	VI
AGRADECIMIENTO	VII
DEDICATORIA	VIII
ÍNDICE GENERAL	IX
ÍNDICE DE TABLAS	XII
ÍNDICE DE FIGURAS	XIII
ANEXOS	XVI
RESUMEN	XVII
ABSTRACT	XVIII
INTRODUCCIÓN	19
CAPITULO I	20
1 FUNDAMENTACIÓN	20
1.1 ANTECEDENTES	20
1.2 DESCRIPCIÓN DEL PROYECTO	23
1.3 OBJETIVOS	27
1.3.1 OBJETIVO GENERAL	27
1.3.2 OBJETIVOS ESPECÍFICOS	27
1.4 JUSTIFICACIÓN DEL PROYECTO	27
1.5 ALCANCE DEL PROYECTO	29
CAPITULO II	30

2 MARCO	CONCEPTUAL, MARCO TEÓRICO, METODOLOGÍA DEL PROY	ЕСТО
		30
2.1 MARC	CO CONCEPTUAL	30
2.1.1 R	REDES INFORMÁTICAS	30
2.1.2 T	TIPOS DE REDES	30
2.1.3 V	/LAN (VIRTUAL LOCAL AREA NETWORK)	31
2.1.4 T	COPOLOGÍA DE ÁRBOL	31
2.1.5 I	NTERNET	31
2.1.6 V	<b>VIRTUALIZACIÓN</b>	32
2.1.7 S	OFTWARE LIBRE	32
2.1.8 F	TREWALL	32
2.1.9 N	<b>AIKROTIK</b>	33
2.2 MARC	CO TEÓRICO	34
2.2.1 ÁRE	A MÁS VULNERABLE DE LAS EMPRESAS HOTELERAS.	34
2.2.2 EL	USO DE LOS PORTALES CAUTIVOS EN REDE A TRAVÉ	'S DE
DISPOSIT	TIVOS MIKROTIK COMO LA MEJOR HERRAMIENTA	PARA
	LAR EL IRAFICO DE DATOS.	35 G DE
2.2.3 LA SEGURID	ARQUITECTURA DE RED RESPALDADA POR POLITICA AD	S DE 35
2.3 METO	DOLOGÍA DEL PROYECTO	35
2.3.1 MET	ODOLOGÍA DE INVESTIGACIÓN	35
2.3.1 TÉCI	NICAS DE RECOLECCIÓN E INFORMACIÓN	36
CAPITULO	Ш	39
3 PROPUI	ESTA	39
<b>3.1 REQU</b>	ERIMIENTOS	39
3.1.1 REQ		
	UERIMIENTO FUNCIONALES	39
3.2 CO	UERIMIENTO FUNCIONALES MPONENTES DE LA PROPUESTA	39 41
3.2 CO 3.2.1 FASH	UERIMIENTO FUNCIONALES MPONENTES DE LA PROPUESTA E 1 PREPARAR	39 41 41

3.2.3FASE 3 DISEÑAR		52
3.2.4	FASE 4 IMPLEMENTACION	56
CONCL	USIONES	87
RECOM	ENDACIONES	87
BIBLIO	GRAFÍA	88
ANEXO	S	91

# ÍNDICE DE TABLAS

Tabla 1: Requerimientos funcionales	40
Tabla 2:Equipo de red existente	48
Tabla 3: Elementos de cableado estructurado existentes	48
Tabla 4: Equipo de red requerido	50
Tabla 5:Elementos de cableado estructurado requeridos	50
Tabla 6: Presupuesto de equipamiento de red	51
Tabla 7: Presupuesto de elementos de cableado estructurado	51
Tabla 8: Presupuesto total del proyecto	52
Tabla 9: Detalles Máquinas Virtuales	57

# ÍNDICE DE FIGURAS

Figura 1: Ciclo de vida PPDIOO	37
Figura 2:Metodología PPDIOO modificada a PPDI	38
Figura 3: Diseño de red actual	43
Figura 4: Estructura actual Primer Piso	44
Figura 5: Estructura actual Segundo Piso	45
Figura 6: Estructura actual Tercer Piso	45
Figura 7: Estructura actual Cuarto Piso o Terraza	46
Figura 8:Diseño de red lógica propuesta	52
Figura 9: Diseño físico de la red 1 planta	54
Figura 10: Diseño físico de la red 2 planta	55
Figura 11:Diseño físico de la red 3 planta	55
Figura 12:Diseño físico de la red de la terraza	55
Figura 13: Maquinas Virtualizadas	57
Figura 14: Diseño prototipo de red EN GNS3	58
Figura 15: Opciones de configuración Pfsense	58
Figura 16 : Interfaces del Pfsense	59
Figura 17 : Interfaz Web pfsense	60
Figura 18: Interfaz principal pfsense	60
Figura 19: Crear Vlan de pfsense	61
Figura 20: Total Vlan creadas	61
Figura 21: Interfaz Agregadas pfsense	62
Figura 22: Asignación de vlan	62
Figura 23: Puerto Trocal	63
Figura 24: Vlan 10	63
Figura 25: Vlan 20 Fuente:	63
Figura 26:Vlan 30	64
Figura 27:Tabla Vlan	64
Figura 28: Configuración Vlans	65
Figura 29:DNS Resolver-General Settings parte 1	65
Figura 30:DNS Resolver-General Settings parte 2	66
Figura 31:DNS Resolver-Advanced Settings parte 1	66

Figura 32: DNS Resolver-Advanced Settings parte 2	67
Figura 33: Reglas NAT	67
Figura 34: Configuración de reglas Nat de acceso al Mikrotik 1	68
Figura 35 : Configuración de reglas Nat de acceso al Mikrotik 2	68
Figura 36 : Interfaces	69
Figura 37: Configuración reglas de la interfaz WAN parte 1	70
Figura 38: Configuración reglas de la interfaz WAN parte 2	70
Figura 39 : Reglas WAN	71
Figura 40: Reglas LAN	71
Figura 41: Reglas WAN2	72
Figura 42: Reglas RED_PUBLICA	72
Figura 43: Reglas ADMINISTRACION	73
Figura 44: Reglas SERVERWEB	73
Figura 45: Instalación de los paquetes Squid y SquidGuard	74
Figura 46: Configuración general Proxy Server parte 1	74
Figura 47:Configuración Proxy Server parte 2	75
Figura 48:Configuración general Proxy Server parte 3	75
Figura 49: Configuración SquidGuard Proxy Filter parte1	76
Figura 50: Configuración SquidGuard Proxy Filter parte2	76
Figura 51: Domain List	77
Figura 52: Parámetros de Bloqueadas	77
Figura 53:Target categories	78
Figura 54; Descarga de la lista negra	78
Figura 55:Configuración Common ACL	79
Figura 56:Estados de Servicios	80
Figura 57: Prueba del SquidGuard Proxy Filter en Administración	80
Figura 58:Pagina Facebook bloqueada Administración	81
Figura 59: Login Mikrotik	81
Figura 60: Servidor hotspot 1Creado	82
Figura 61: Ping al puerto 8.8.8.8	82
Figura 62: Planes o paquetes	84
Figura 63: Usuario Creado	85
Figura 64: Login Hotspot	85
Figura 65: Detalle de conexión	86
Figura 66: Usuario con acceso a internet	86

Figura 67:Usuarios Conectados	86
Figura 68: Página Oficial Pfsense	93
Figura 69: Configuración Máquina Virtual	94
Figura 70: Configuración de red de la Máquina Virtual Pfsense	94
Figura 71: Configuración de almacenamiento de Máquina Virtual Pfsense	95
Figura 72: Configuración de instalación Pfsense	95
Figura 73: Opciones de configuración Pfsense	96
Figura 74: Página Oficial Mikrotik	97
Figura 75: Configuración Máquina Virtual Mikrotik	97
Figura 76: Configuración de almacenamiento de Máquina Virtual Mikrotik	<b>98</b>
Figura 77: Terminal Mikrotik	<b>98</b>
Figura 78: Página Oficial Microsoft	99
Figura 79: Configuración Máquina Virtual Administración	100
Figura 80: Configuración Máquina Virtual Piso 1 Cliente	100
Figura 81: Configuración de almacenamiento de Máquina Virtual Piso 1 Cliente	101
Figura 82: Instalación de Windows	101
Figura 83: Escritorio de Windows	102

## ANEXOS

Anexo 1: Formato de la entrevista	91
Anexo 2: Formato de ficha de observación	92
Anexo 3: Manual de instalación de nuestro entorno virtual	93

## RESUMEN

El presente proyecto de titulación "PROPUESTA DEL DISEÑO DE RED Y POLÍTICAS DE SEGURIDAD A NIVEL DE FIREWALL APLICANDO LA HERRAMIENTA PFSENSE PARA EL CONTROL DEL TRÁFICO DE RED Y ADMINISTRACIÓN DEL ANCHO DE BANDA. CASO DE ESTUDIO HOTEL COPACABANA, tiene la finalidad de diseñar una nueva topología de red para el establecimiento hotelero Copacabana del Cantón La Libertad, luego del estudio realizado se reconoció que no cuenta con una topología de red adecuada para brindar un buen servicio de internet.

En donde se utilizó método científico de recolección de información como la entrevista y observación en donde se reconoció que tiene una topología de red inadecuada para brindar el servicio de internet que conllevando a utilizar la metodología de red con el nombre de PPDIOO el cual se adaptó para el desarrollo.

El resultado del proyecto de titulación es una nueva topología de red virtualizada que distribuirá adecuadamente los departamentos que tiene el establecimiento hotelero, mejorando la seguridad y la distribución de acho de banda de la red.

Palabras claves: Infraestructura, Pfsense, Mikrotik.

## ABSTRACT

The present titling project "PROPOSAL FOR NETWORK DESIGN AND SECURITY POLICIES AT THE FIREWALL LEVEL APPLYING THE PFSENSE TOOL FOR NETWORK TRAFFIC CONTROL AND BANDWIDTH MANAGEMENT. CASE STUDY COPACABANA HOTEL", has the purpose of designing a new network topology for the establishment hotelier Copacabana of Canton La Libertad, after the study carried out, it was recognized that it does not have an adequate network topology to provide a good internet service.

Where the scientific method of collecting information such as the interview and observation was used, where it was recognized that it has an inadequate network topology to provide the internet service that led to the use of the network methodology with the name of PPDIOO which was adapted to the development.

The result of the degree project is a new virtualized network topology that will adequately distribute the departments that the hotel establishment has, improving security and the distribution of network bandwidth.

Keywords: Infrastructure, Pfsense, Mikrotik.

## **INTRODUCCIÓN**

El hotel Copacabana ubicado en el Cantón La Libertad es unos de los hoteles con mayor trayectoria en el cual unos de los servicios que ofrece es el internet de acuerdo a la recolección de información recabada no cuenta con una red adecuada al establecimiento lo que provoca en ocasiones a no bridar un mejor servicio a las personas que visitan este prestigioso hotel.

La propuesta de un nuevo diseño de red permitirá solucionar los problemas de conectividad que se pronuncia los fines de semanas y feriados donde acuden afluencia de personas en el cual un sinnúmero de dispositivos se encuentra utilizando el servicio, la nueva topología de red nos ayudara a segmentara los diferentes departamentos que tiene el establecimiento hotelero permitiendo tener más seguridad, mejorar la conectividad en cualquier área que se encuentre el huésped.

En el presente trabajo de titulación se encuentra dividido de los siguientes capítulos:

El capítulo I, se detalla los antecedentes que conllevó a la propuesta, obteniendo información de la problemática actual se procede a describir el proyecto detalladamente planteado que método y herramientas a utilizará, además presentando los objetivos que deberemos cumplir a cabalidad con su respectiva justificación y el alcance que tendrá la propuesta planteada.

El capítulo II, mediante el marco conceptual definimos conceptos que conllevan a la investigación tomando mucha importancia a sus significados, el marco teórico se recopilo un conjunto de ideas o teorías fundamentales, investigativas y factores que se estudian obteniendo un enfoque completo la cuales deben ir referenciadas, la metodología de investigación nos llevó a usar técnicas de recolección con la entrevista y la observación hacia el establecimiento obteniendo información precisa que fue de gran ayuda optando con una metodología que se adapte a la propuesta.

EL capítulo III, una vez obtenidos los requerimientos del proyecto se procede al desarrollo de las fases de la metodología PPIOO como son preparar, planear, diseñar e implementar las cuales se evidencia en la documentación, finalizando con sus respectivas conclusión y recomendaciones del proyecto.

## CAPITULO I 1 FUNDAMENTACIÓN 1.1 ANTECEDENTES

En los últimos años las redes inalámbricas (WLAN, Wireless Local Área Network) han ganado muchos adeptos y popularidad en mercados verticales tales como hospitales, fábricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acedan información y recursos en tiempo real sin necesidad de estar físicamente en un sólo lugar. Con WLANs la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante incrementa la productividad y eficiencia en las actividades diarias de la empresa. [1].

Hemos visto que la movilidad dentro de las redes es uno de los objetivos más claros para las empresas puesto que ofrecen una opción inalámbrica inteligente, con acceso seguro y estable a todos los recursos de la red para que los usuarios sean productivos independientemente de cómo se conecten. Además, la conectividad inalámbrica también le permite evitar los costes y complicaciones de tener cables tendidos por todo el edificio [1].

El Hotel Copacabana, fue fundada en el año 2006 y se encuentra ubicado en la Av.9 de octubre, Barrio 25 de diciembre A lado de la farmacia SanaSana, 240350 La Libertad desde el primer día realiza el servicio de hospedaje y sala de evento realizado una acogida familiar a sus huéspedes desde hace muchos tiempos. Con su fundador y actualmente dueño el Sr. Lopes Vaz Rogerio de origen brasileño. Las áreas públicas, las 32 habitaciones que cuenta el hotel son muy cómodas, confortables y en la actualidad cuenta con 9 empleados que se encarga de realizar un excelente servicio a los huéspedes.

Para el levantamiento de información dirigido al hotel Copacabana se utilizó la metodología de entrevista (Anexo 1) y metodología de observación (Anexo 2) en donde pudimos constatar y conocer la estructura de red que se utiliza es la topología estrella basada en un punto central que sería el router del proveedor, además se conoció los quipos

conectados a esta red tales como: 2 (Digital video recorder) DVR con 8 puertos, 32 televisores ,4 Router ,1Pc (administración) además los equipos pertenecientes a los huéspedes como equipo móviles y laptop.

Mediante la metodología de observación se dio a conocer la demanda de acceso a internet en épocas de feriado o fines de semanas esto provoca que la red colapse ya que se ocupan todas las habitaciones y los huéspedes que utilizan el servicio de internet es de un aproximado de 100 a 200 personas, en la parte administrativa se manejan los procesos contables y registros de los huéspedes que acuden al hotel que constantemente hace uso de internet, esta dispone de una impresora conectada mediante la red.

Debido a las políticas del hotel todos los huéspedes tienen acceso a internet, como se maneja una topología estrella no existe seguridad en la red, es decir cualquier usuario con conocimiento informático conectado a la red puede acceder a los equipos de seguridad y vigilancia además de acceder a la Pc donde se maneja los procesos contables y datos personales de los huéspedes.

El ancho de banda que ofrece es insuficiente para los huéspedes que necesitan de conexión a internet esto provoca incomodidad ya que no se maneja un control de usuarios conectados, registrados, tiempo de conexión, cantidad de megas, el mantenimiento de los equipos se realiza anualmente esto provoca que los huéspedes antiguos tengan conexión a la red sin necesidad de estar registrado en el hotel dejando sin conexión o ralentizando el acceso a internet a los huéspedes actuales, la parte de distribución de red no cuenta con los equipos suficientes para abastecer todo el hotel la cual tememos problema con los puntos de acceso al momento de llegar al límite de dispositivo conectado los cuales ocasiona disgusto con los huéspedes.

Ese acercamiento a los ordenadores y la informática en general resulta obsoleto e inútil en nuestros días, en gran medida, porque no tiene solución de continuidad en los hogares o fuera de la propia escuela y porque el modelo tecnológico ha cambiado con la incorporación de las redes de forma masiva, cosa que no existía en aquel momento o sólo estaban disponibles en entornos muy concretos e inaccesibles para el gran público [2]. Han establecidos los diferentes departamentos que ayudará a una mejor distribución y saber a cuál permanece, pero no cuenta con portal cautivo que pueda permitirá usar la red de un modo seguro el tal cual no dará prioridad a paginas prohibidas o que pueda ser cáusate de un virus o programa maligno.

Desde de un punto vista operativo es factible la puesta en marcha de la propuesta ya que en el laboratorio de desarrollo de software de la Universidad Técnica de Cotopaxi Extensión La Maná se encuentra en las condiciones necesarias para la ejecución del proyecto; de igual lo hace posible de forma operaria ya que dentro de este laboratorio se requiere de una red de datos que permita tener una adecuada velocidad para la comunicación de datos. La implementación y configuración de la Red LAN es posible de igual forma ya que a través de la aplicación de esta se logrará que los estudiantes y docentes u otro ocupante del laboratorio logren tener una adecuada transmisión y comunicación de datos e información dentro del laboratorio logrando que las actividades que realicen se efectúen de una forma más efectiva y eficaz [3].

El tipo de red establecido nos sirve un área pequeña por lo que carece de un firewall que permitida realizar un monitoreo de la red y podría ser causante de robo de información por lo que optaron realiza una red LAN doméstica. A través de la implementación de la arquitectura de red se demuestra la mejora del servicio a internet que se ofrece a los huéspedes y usuarios que radican en la red mediante la instalación de dispositivos de gestión de red ubicados de manera estratégica, para ofrecer una óptima red informática mejorando la disponibilidad, confiabilidad, seguridad, escalabilidad y desempeño general [4].

Los proyectos anteriores han podido resolver la mala infraestructura de red en que se encontraba el diferente establecimiento lo cual no ayuda a tener noción de cómo podremos establecer una adecuada infraestructura de red para nuestro hotel que constara de un firewall con nos ayuda a la seguridad de red, estableciendo los distintos departamentos que existe en nuestro establecimiento y poder controlar el ancho de banda para una distribución de los Mbps a los usuarios.

#### **1.2 DESCRIPCIÓN DEL PROYECTO**

El nuevo diseño de la red se realizará a través de virtualizaciones para ello se utilizará herramientas tales como virtual box y gns3 en esta se usará algunos equipos como servidores, switch, router board entre otras herramientas necesarias como un firewall principal se utilizará la herramienta pfsense encargado de la seguridad de la red del hotel, también podremos distribuir mediante vlan el diferente departamento perteneciente al establecimiento hotelero.

El desarrollo de este proyecto se basará en la metodología PPDIOO el cual fue adaptado a esta propuesta a la metodología PPDI los cuales contará con las siguientes fases:

#### Fase 1: Preparar

El estudio iniciara con el levantamiento de información al establecimiento hotelero, en donde usaremos la técnica de entrevista y la técnica de observación el cual no ayudara a reconocer el tipo de red que utiliza, también los equipos de comunicación que son utilizados para brindar el servicio de internet y los puntos de conectividad hacia los huéspedes, dicha información recolectada nos servirá para plantear la nueva propuesta para el establecimiento.

#### Fase 2: Planear

Después de la respectiva recolección de información realizamos un análisis de factibilidad el cual nos permitirá saber el costo de implementación del proyecto, también enlistaremos mediante tablas los equipos pertenecientes al establecimiento hotelero que podrán ser utilizados en la nueva propuesta y los equipos necesarios que deberemos adquirir.

#### Fase 3: Diseño

En esta fase de diseño donde se involucra el planteamiento lógico y físico de la red el cual estarán representado mediante graficas el diseño de la red adecuada que tendrá el establecimiento, la ubicación apropiada de los equipos dentro de la estructura del hotel, se establecerá la conexión adecuada de los proveedores de internet y se mostraremos mediante tablas las diferentes segmentaciones y protocolo de red.

#### Fase 4: Implementación.

En esta última fase mediante virtualización se realizará la respectiva simulación de la propuesta planteada donde se efectuará las instalaciones de los equipos necesarios y su debida configuración tales como son las del firewall, swicht, router y demás equipos mediante el proceso se realizará las respectivas pruebas. A continuación, se detalla las siguientes:

#### Instalación Virtual de los equipos y herramientas

En esta primera fase usaremos la aplicación de virtual box la cual nos ayudara a virtualizar los equipos respectivos que estaremos utilizando en el transcurso del proyecto tales como software, firewall, switch, router.

Para el diseño e implementación de la red usaremos gns3-version en la cual nos permitirá vincular los equipos virtuales creados en virtual box con la misma aplicación, esta configuración se realizará mediante una máquina virtual proporcionada por gns3 que nos permitirá trabajar de forma sincronizada.

# Configuración firewall principal pfsense (Vlan, Servidor DHCP, Static DHCP, DNS y DNS Resolver).

Para esta fase se tendrá que configure según las necesidades que presenta el hotel para cada área:

- Para el área de red pública o cliente se crear la vlan 10 en la cual esta tendrá todos los privilegios para acceder a internet se habilitará el servidor DHPC y se creará reglas conexión esta trabaja en conjunto con el router board.
- Para el área administración se creará una vlan 20 en donde tendrá acceso a internet, se habilitará el servidor DHCP se implementará las reglas en el firewall que permita bloquear el acceso a rede sociales.
- Para el área serve seguridad se creará vlan 30 que el cual no tendrá habilitado el servidor DHCP y no tendrá acceso a internet se habilitaran los puertos especifico dependiente de lo serve.

#### Configuración Nat, reglas en el firewall, squid proxy de la red administración

Primeramente, configuraremos el acceso a los servidores desde el afuera el cual nos ayudara con la comunicación y traslado de paquetes a las diferentes redes que existen y crearemos reglas a las diferentes interfaces que nos permitirá un enlace a través del firewall en las diferentes direcciones y permitir el tráfico.

El hotel Copacabana requiere que le personal administrativo este limitado al acceso a internet esto se realizara a travez de pfsense con herramienta tales como Squid Proxy el cual se descargara los paquetes, esto se configurar en la vlan 20 donde se aplicara las reglas necesarias para su funcionamiento.

#### Configuración del hotspot en Mikrotik.

Se asignará en la vlan 10 el router board con acceso a internet donde se virtualizar 2 puertos, uno que conectaran al pfsense y el otro puerto al switch para los clientes. Mediante la aplicación Winbox nos permitirá administrar mikrotik en donde configurara y habilitara host port, para esto se implementará los certificados, se crearán planes de internet donde se limitar el ancho de banda y el tiempo de conexión, los clientes podrán acceder mediante usuarios y claves que le otorga el hotel, la página principal que se presentara para acceder a internet esta enlazado con la página web del hotel. Las herramientas que se utilizaran en la implantación son:

**Pfsense:** es una distribución de firewall de red gratuita, basada en el sistema operativo FreeBSD con un kernel personalizado e incluye paquetes de software gratuitos de terceros para una funcionalidad adicional. El software pfsense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más de los firewalls comerciales comunes, sin ninguna de las limitaciones artificiales [5].

**VirtualBox:** es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico [6].

**Hotspot:** El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente (haciendo lo que se llama Calidad de Servicio). [7]

**EDraw Max:** es la herramienta de diagramación todo en uno más fácil que sirve para todos sus propósitos. Proporciona un espacio de trabajo para crear más de 280 tipos de diagramas, incluidos diagramas de flujo, diagramas de espina de pescado, diagramas UML, planos de planta y más [8].

**CentOS:** se suele utilizar en las etapas de desarrollo e implementación, y no cuenta con ninguna estructura que permita aportar código. No se realizarán lanzamientos nuevos de CentOS Linux entre 2021 y 2024 [9].

**GNS3:** es un software utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. Le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube [10].

**Windows 7:** es un sistema operativo, es decir, un programa de software que admite funciones básicas, como la administración de archivos y la ejecución de aplicaciones, y que usa dispositivos periféricos, como la impresora, el monitor, el teclado y el mouse. En el pasado, Windows podía considerarse como un software que residía solo en tu dispositivo [11].

**Cloud Hosted Router (CHR):** abreviatura de Cloud Hosted Router, es un nuevo enfoque diseñado específicamente para máquinas virtuales tanto locales como en la nube. Controladores optimizados, un esquema de licencias nuevo y más asequible, licencias transferibles y más [12].

**DCS-100 D-ViewCam Video Management:** es un sistema de vigilancia completo que le permite administrar centralmente hasta 32 cámaras de red, mientras muestra información en tiempo real. El modo de mapa le permite crear mapas basados en la

ubicación y orientación de la cámara, y el árbol de dispositivos enumera todas las cámaras conectadas a la interfaz para una fácil visualización [13].

**Router board:** es el sistema operativo que se puede utilizar para modificar el sistema informático como un router de red confiable. Este incluye varias funciones que se hicieron para redes IP y redes inalámbricas, adecuadas para su uso a través de ISPs y proveedores de puntos de acceso [14].

#### 1.3 OBJETIVOS 1.3.1 OBJETIVO GENERAL

Diseñar una propuesta de la red virtualizado del hotel Copacabana a través de firewall pfsense para controlar el tráfico de red y administración el ancho de banda.

#### **1.3.2 OBJETIVOS ESPECÍFICOS**

- Definir las segmentaciones de la red para los diversos departamentos a través del firewall pfsense para mejorar la seguridad y distribución de la red.
- Implementar políticas de navegación restringida para los usuarios del área administrativa a través de los servicios Squid Proxy Server y SquidGuard Proxy mediante máquinas virtuales.
- ✓ Implementar en máquinas virtuales el hotspot para el área de cliente a través del RouterBOARD Mikrotik para controlar el ancho de banda y el tiempo de navegación.

#### **1.4 JUSTIFICACIÓN DEL PROYECTO**

Ante los cambios que se van dando en las redes de los edificios, la infraestructura debe ser capaz de adaptarse a nuevos requerimientos. Lo básico es contar con una topología de cableado estructurado bien planificada, que permita escalar según la demanda sin tener que tocar el cableado troncal. Después, se deberán utilizar componentes modulares que puedan conectarse y desconectarse de manera sencilla y rápida, de forma tal que permita transportar nuevas tecnologías y velocidades más rápidas en la red principal [15].

La operación en todos sus aspectos se traduce en un servicio más eficiente y una mayor satisfacción del cliente. Por otro lado, a la hora de diseñar redes, hoy en día es necesario utilizar tecnologías que nos permitan hacer uso de las tecnologías de la información y la comunicación. Estas tecnologías permiten estandarizar, automatizar y mejorar el servicio que ofrecen al cliente final.

En este estudio al hotel Copacabana se propone diseñar una nueva red basada en la topología árbol donde el nodo principal se alojará en firewall pfsense encargado de la seguridad que se controlará mediante reglas de nateo el acceso a la misma el cual tendrá segmentaciones que nos ayudará a administrar y controlar el tráfico en cada una de ellas. Los huéspedes podrán acceder a internet a través de la autentificación al servidor, los huéspedes tendrán que estar registro por el administrador, el mikrotik podrá controlar el tipo de plan del cliente es decir cantidad de megas, cantidad de tiempo, habilitar, deshabilitar y eliminar usuario. Los Router se configurarán una capa inferior de la red donde tendrá que redireccionar el Gateway al servidor para poder tener salida a través de firewall principal a internet.

Con este proyecto se segmentará lo diferentes departamentos o áreas que existen en el hotel Copacabana, mejorando la seguridad del establecimiento ya sea su información o de los huéspedes los cuales tendrá un mejor servicio de internet y podrá distribuir adecuadamente el ancho de banda y así reducir el tráfico de red.

El tema propuesto está vinculado hacia los objetivos del Plan Nacional de Desarrollo del siguiente eje:

#### 1.4.1 PLAN DE CREACIÓN DE OPORTUNIDADES EJE 3

Objetivo 9: Garantizar la seguridad ciudadana, orden público y gestión de riesgos. Política 9.1: Fortalecer la protección interna, el mantenimiento y control del orden público, que permita prevenir y erradicar los delitos conexos y la violencia en todas sus formas, en convivencia con la ciudadanía en el territorio nacional y áreas jurisdiccionales [16]

#### **1.5 ALCANCE DEL PROYECTO**

El estudio de este presente proyecto que se propone estará relacionado mediante la metodología PPDIOO el cual nos ayudara a desarrollar adecuadamente los diferentes procedimientos que formaran parte de la propuesta el cual nos permitirá la recolección de información que ayudara con todo los requerimientos que necesitara para la implementación y los diferentes equipos que utilizaremos para el mismos establecer una red adecuada para establecimiento hotelero, a continuación se detalla las fases del proyecto:

#### **Fase 1: Preparar**

- ✓ Entrevista a la administración del "Hotel Copacabana".
- ✓ Aplicación de técnica de observación en el estacionamiento.
- ✓ Análisis del diseño de red actual.
- ✓ Estructura actual del establecimiento.

#### **Fase 2: Planear**

- ✓ Factibilidad Operacional.
- ✓ Factibilidad Técnica.
- ✓ Factibilidad Económico.

#### Fase 3: Diseño

- ✓ Diseño lógico de red.
- ✓ Conexión al proveedor.
- ✓ Segmentación de la red y protocolos.
- ✓ Diseño físico de red.

#### Fase 4: Implementación

- ✓ Instalación Virtual de las equipos y herramientas.
- Configuración firewall principal pfsense (vlan, Servidor DHCP, Static DHCP, DNS y DNS Resolver).
- ✓ Configuración Nat, reglas en el firewall.
- ✓ Configuración del squid proxy de la red administración.
- ✓ Configuración del hotspot en mikrotik.

#### **CAPITULO II**

## 2 MARCO CONCEPTUAL, MARCO TEÓRICO, METODOLOGÍA DEL PROYECTO

#### 2.1 MARCO CONCEPTUAL

Actualmente las empresas hoteleras han sido víctimas de robo de información a sus huéspedes mediante el servicio de internet que brindan por lo cual se ha adoptado al uso de software de seguridad los cuales ayudan a monitorear el tráfico de red y la necesidad de controlar los diferentes accesos, por ente definiremos conceptos esenciales para la presente investigación:

#### 2.1.1 REDES INFORMÁTICAS

Una red es un conjunto de ordenadores conectados entre sí que pueden compartir información, (documentos, imágenes, ...), recursos (impresoras, discos duros) y servicios. Una red puede estar formada por dos ordenadores o llegar incluso a tener conectados miles de ordenadores repartidos por todo el mundo (como Internet) [17].

#### 2.1.2 TIPOS DE REDES

#### 2.1.2.1 REDES DE ÁREA LOCAL (LAN - LOCAL AREA NETWORK)

Es una red de datos que cubre un área geográficamente pequeña y limitada, que conectan las estaciones de trabajo, terminales, dispositivos ya sea en un edificio, oficina o campus. Una LAN consiste en computadoras, dispositivos periféricos, dispositivos de Red, Tarjetas de Interface de Red (NICs). Proveen conectividad todas las 24 horas y utilizan las normas de la capa física y la capa de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son algunas de las tecnologías LAN más comunes, aunque el estándar más utilizado es el Ethernet [18].

### 2.1.2.2 REDES DE ÁREA METROPOLITANA (MAN - METROPOLITAN AREA NETWORK)

Son redes de dimensiones a nivel regional. Suelen interconectar tanto a sistemas individuales como a otras LAN, y cuando su dimensión se limita a edificios también se las conoce como Redes de Campus [19].

#### 2.1.2.3 REDES DE ÁREA EXTENSA (WAN - WIDE AREA NETWORK)

Superan en extensión a las MAN (también podrían considerarse WAN a nivel regional), aunque no necesariamente en número de puestos. Suelen ser utilizadas para la interconexión de oficinas o sucursales en distintos puntos geográficos, siendo el ejemplo más actual y de mayor dimensión la red internet [19].

#### 2.1.3 VLAN (VIRTUAL LOCAL AREA NETWORK)

Un grupo de dispositivos que están configurados de un modo que puedan comunicarse como si estuvieran conectados por el mismo cable. Las VLAN segmentan lógicamente las redes conmutadas basándose en las funciones. Se utilizan las VLAN para escalar, mayor seguridad y administrar el flujo de tráfico [18].

#### 2.1.4 TOPOLOGÍA DE ÁRBOL

La topología en árbol es una generalización de la topología en bus en la que el cable se desdobla en varios ramales mediante el empleo de dispositivos de derivación. Dependiendo del elemento utilizado podemos encontrarnos situaciones muy diferentes:

- Si utilizamos un Repetidor estaríamos realmente prolongando el bus, con lo que nos veríamos limitados por el número de estaciones conectadas (un máximo de 30 estaciones en segmentos de 185 metros en la red Ethernet), ya que todas accederían al bus.
- ✓ Si utilizamos un Bridge (puente) evitamos dicho problema, ya que este elemento solamente deja pasar aquella información del bus que realmente vaya dirigida a alguna estación del otro segmento (en el ejemplo, ahora con un bridge duplicaríamos el número máximo de estaciones a conectar) [19].

#### 2.1.5 INTERNET

Internet se encarga de ser el vínculo entre las redes más pequeñas y a su vez permite que se amplíe su cobertura al convertirlas en parte de una red global. Esta gran red o red global tiene como característica de que utiliza un lenguaje común, el cual garantiza la intercomunicación de las diferentes estaciones; este lenguaje común o protocolo (un protocolo es el lenguaje que se utiliza en las computadoras al compartir sus recursos) es el TCP/IP [20].

#### 2.1.6 VIRTUALIZACIÓN

La virtualización es una tecnología en apogeo con gran potencial, que permite administrar de forma eficiente los recursos de hardware, software, consolidación de servidores, costos, espacio físico, y recurso humano en una infraestructura de TI, mejorando de igual manera la capacidad de gestión y seguridad de los escritorios virtuales [21].

#### 2.1.7 SOFTWARE LIBRE

La libertad en su máxima expresión, así lo catalogan muchos desarrolladores de software que gustan de este tipo de programas. Para que un programa cumpla los requisitos para ser considerado software libre es que pueda ser utilizado sin ningún tipo de limitaciones, debe ser distribuido libremente y no tener limite al copiar, instalar y distribuirse, el código fuente debe distribuirse junto con su código fuente original, y la última cualidad es que las personas que modifican este tipo de programas puede ser comercializado y distribuido, siempre y cuando los mismos respeten los nombres de los autores originales del mismo [20].

#### 2.1.8 FIREWALL

Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización [22].

#### 2.1.8.1 PFSENSE

Es una distribución de cortafuegos de red gratuita, basada en el sistema operativo FreeBSD con un núcleo personalizado e incluye paquetes de software gratuitos de terceros para funcionalidad adicional. El software pfsense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más que los firewalls comerciales comunes, sin ninguna de las limitaciones artificiales [23].

#### 2.1.8.2 SERVICIOS DE PFSENSE

 Permite que se pueda crear grupos con varias direcciones y puertos, esto ahorraría tiempo en crear reglas para cada uno.

- ✓ Se puede dar una franja horaria para el firewall.
- ✓ Permite limitar el ancho de banda.
- ✓ El firewall permite que se pueda bloquear conexiones no permitidas.
- ✓ VPN de acceso remoto.
- ✓ Obliga al usuario identificarse para poder dar acceso a la red.

#### **2.1.9 MIKROTIK**

Mikrotik es una empresa de Letonia que desarrollo un software que gestiona placas conmutadoras llamadas RouterOS las mismas que se encuentran acentuadas en Linux lo cual da al usuario la posibilidad de conectarse, accesar a la configuración y administrar la red. Esta tecnología brinda la posibilidad de establecer VPNs, DHCP Server, QoS, Firewall, entre otros además de la implementación de Puntos de acceso inalámbrico [24].

#### **2.1.9.1 HOTSPOT**

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso) a los usuarios antes de permitirles el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente en todas los equipos móviles y sistemas operativos [25].

#### 2.1.9.2 WINBOX

Es una aplicación de configuración del RouterOS ya que permite la administración de Mikrotik RouterOS utilizando una interfaz GUI sencilla.

#### 2.1.9.2.1 BENEFICIOS DE LA TECNOLOGÍA

- $\checkmark$  Permite el control de ancho de banda por usuario.
- ✓ Posee software de configuración Winbox de fácil uso.
- ✓ No se necesita de conocimientos previos para su implementación.
- ✓ Posibilidad de bloquear aplicaciones y páginas web no deseadas.

#### 2.2 MARCO TEÓRICO

#### 2.2.1 ÁREA MÁS VULNERABLE DE LAS EMPRESAS HOTELERAS.

Los avances tecnológicos y el furor de los dispositivos móviles han logrado que el acceso a internet haya migrado a una forma móvil también, de manera que la conexión a internet ahora es fácilmente implementada fuera de los hogares y, sobre todo, fuera de las redes privadas. Actualmente, es muy fácil conectarse a internet fuera de casa mediante un dispositivo móvil, y en diferentes ubicaciones como instituciones educativas, lugares de trabajo y puntos de acceso públicos, de manera gratuita [26].

#### 2.2.1.1 LAS CONEXINES(WIFI) INALÁMBRICAS.

Al ser público, los atacantes pueden sentarse en el lobby (o reservar una habitación) y buscar debilidades con calma. Si la red wifi del hotel no está debidamente asegurada, los atacantes podrían crear un puente desde la red pública de la propiedad hasta la red privada de su oficina. Aún peor, entonces podrían esconderse más para utilizar información útil y/o datos internos de valor, de la propiedad [27].

#### 2.2.1.2 PUNTOS DE VENTAS (POS POR SUS SIGLAS EN INGLES)

Al controlar información de pagos desde los puntos de venta, estos se convierten en un objetivo para los criminales cibernéticos. Tal como hemos visto en algunos de los principales ataques en la última década, ganar acceso al sistema de punto de venta de un hotel, permite a los criminales cibernéticos mantenerse inactivos y capturar un flujo continuo de datos de pago [27].

#### 2.2.1.3 PERSONAL DEL HOTEL

El tercer punto más vulnerable en las operaciones de un hotel es el personal. Ya sea el recepcionista, un agente de reservas o un contable, los atacantes ven al personal como oportunidades para la filtración de datos privados y acceso con técnicas engañosas [27].

## 2.2.2 EL USO DE LOS PORTALES CAUTIVOS EN REDE A TRAVÉS DE DISPOSITIVOS MIKROTIK COMO LA MEJOR HERRAMIENTA PARA CONTROLAR EL TRÁFICO DE DATOS.

Afirma que la seguridad en las redes inalámbricas es la parte más importante y las más olvidada, ya que es muy fácil instalar una red, pero no hay que dejar de lado que el gran problema de seguridad está en este tipo de red, ya que uno de los problemas más grandes que puede llegar a tener una red es que no se puede controlar el medio por donde se envían y se reciben datos, debido a esto es que muchas de los ciberdelincuentes buscan principalmente vulnerabilidades en las redes de manera inalámbrica, por lo tanto, es el punto donde hay que tener mucho más cuidado al momento de querer implementar Hostport o querer conectarse a uno de ellos [26].

# 2.2.3 LA ARQUITECTURA DE RED RESPALDADA POR POLÍTICAS DE SEGURIDAD

La política de seguridad informática debe entenderse como un conjunto de reglas que deben ser implementadas en las diferentes actividades que se efectúen en la organización, asimismo estas incluyen la seguridad física, administrativa y de la red. La política de seguridad, evalúan y determinan lo que los usuarios del sistema desean proteger, de acuerdo con su valor. De este modo se realiza la planificación para proporcionar una base a la seguridad informática, de tal manera generar requisitos para la expansión de la red actual o para el diseño de nuevas aplicaciones. Asimismo, se describe al usuario las responsabilidades que debe acatar para proteger la información confidencial [28].

#### 2.3 METODOLOGÍA DEL PROYECTO 2.3.1 METODOLOGÍA DE INVESTIGACIÓN

En esta propuesta se utilizó la investigación exploratoria que permite profundizar el concomiendo de la propuesta lo cual se indaga y analizo diferentes trabajos similares que nos ayudara a mejorar ciertas características del nuevo diseño de red para el establecimiento hotelero [29].

Utilizando la investigación diagnóstica se logrará analizar la problemática del servicio de internet que brinda el hotel utilizando la metodología de entrevista y la metodología

de observación con esta propuesta ayudara al tráfico de red y con la implementación del portal cautivo podremos distribuir el ancho de banda a los distintos departamentos que existe en el hotel también permitirá mejorar la seguridad de la información tanto como del establecimiento y de los huéspedes [30].

La variable: Distribución de ancho de banda de la red pública virtualizada.

#### 2.3.1 TÉCNICAS DE RECOLECCIÓN E INFORMACIÓN

Primeramente, se utilizó la técnica de entrevista que consiste en tener un cuestionario de preguntas el cual se le realizara dentro del establecimiento hotelero "Hotel Copacabana" (Anexo 1) hacia la administración y así conocer las diferentes falencias que tiene unos de los servicios que ofrece, además plantear una innovación tecnológica que lograra mejorar el servicio de internet hacia los huéspedes.

La entrevista hacia la administración del hotel debe ser concreta y poder recaudar los datos más importantes que puedan proporcionar para así realizar un análisis que revelara las diferentes decisiones que ayudara a mejorar el servicio de internet, con esta solución los trabajadores y huéspedes del hotel se beneficiaran directamente.

También para este presente caso se procedió a usar la técnica de observación [31], la cual nos ayudó a analizar la infraestructura de la red que tiene adoptada para brindar el servicio, en esta técnica usaremos una ficha que posee todos los campos necesarios que nos ayudara con la recolección de información que nos permitió determinar las principales causas o falencias que tiene el establecimiento hotelero y adoptar una nueva propuesta tecnológica que ayudara de forma positiva.

#### 2.3.3 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Para el desarrollo del proyecto propuesto se manifiesta la ejecución de la metodología PPDIOO en donde su principal enfoque es la definición de actividades determinadas para el nuevo diseño de red del Hotel Copacabana.
La Metodología PPDIOO se basa estrictamente en el cumplimiento de lineamientos propuestos en el ciclo de vida PPDIOO que usa Cisco para la correcta administración y gestión de la red. Por lo tanto, su ciclo de vida está diseñado para ayudar a cumplir objetivos trazados durante la investigación, asimismo su objetivo principal es la disminución del costo total de administración de la red y el aumento de la disponibilidad de la información en la red, a su vez ser una mejora constante para futuras implementaciones de cambios en la estructura de la red [32].

La metodología PPDIOO, brinda un marco de desarrollo para la implementación de redes con un bajo presupuesto que se adapta con facilidad al establecimiento hotelero, y así, de esta manera elaborar un plan de trabajo que facilita la implementación de redes en determinadas áreas estratégicas del hotel, para así utilizar de manera óptima el despliegue paso a paso de la red inalámbrica. De este modo, a partir de la implementación y operación de la red desplegada mediante la metodología planteada, se observa el comportamiento de la implementación para tomar algunos puntos deficientes y realizar la optimización del servicio de internet para el establecimiento hotelero "San Pablo" [33].

La metodología se despliega en seis fases bien estructuradas que describen los pasos a seguir para el diseño e implementación de la red; y su ejecución se da en forma cíclica, estas fases son:



Figura 1: Ciclo de vida PPDIOO

Para la implementación de este estudio, se tuvo que modificarse la metodología PPDIOO, el cual se adaptad para el desarrollo las cuales no sirvió de mucha ayuda a continuación describo cuales fase se utilizaron ya que se tomó como referencia la diferente fase de la metodología.

- Preparar: Se realizo el levantamiento de información mediante la técnica de entrevista a la administración de hotel y la técnica observación en el establecimiento en el cual se obtuvo diferentes problemas y analizamos los objetivos que ayudaría a mejorar unos de los servicios que ofrece.
- Planear: En la siguiente fase se procede realizamos los estudios de factibilidad el cual nos determinara el costo de implementación representándolos mediante tablas, los equipos de pertenecen al hotel y se podrán ser reutilizado para la nueva propuesta.
- ✓ Diseñar: En esta fase determinamos los diseños lógicos y físicos que tendrá la red del establecimiento en la cual estableceremos la ubicación adecuada de los equipos tecnología y los dispositivos que utilizaremos en la red del establecimiento hotelero y se representará mediante esquemas de la red.
- ✓ Implementar: Elaboramos mediante virtualización la simulación de la red propuesta con la ayuda de las herramientas necesarias para el debido funcionamiento.



Figura 2:Metodología PPDIOO modificada a PPDI Elaborado por Carlos Orrala

## **CAPITULO III**

## **3 PROPUESTA**

## **3.1 REQUERIMIENTOS**

## 3.1.1 REQUERIMIENTO FUNCIONALES

ID REOUERIMIRNTO	DESCRIPCIÓN DEL REQUERIMIENTO
RF-001	El análisis que se obtuvo mediante el formato de la ficha de
	observación determino los problemas de seguridad que
	acontecía el establecimiento hotelero.
RF-002	Para la virtualizado usaremos VirtualBox en el cual se creará
	una máquina virtual que nos ayudará a simular el componente.
<b>RF-003</b>	La herramienta GNS3 nos ayudara a virtualizar la red
	establecida que usaremos.
RF-004	Para la instalación de virtualizado usaremos VirtualBox en el
	cual se creará una máquina virtual con la aplicación GNS3 en
	cual se vinculará y simulará el diseño de red.
<b>RF-005</b>	Creamos todos los componentes necesarios que utilizaremos
	para la virtualización de la red.
RF-006	El diseño de red tendrá de segmentaciones o Vlans:
	Vlan1: Red Pública.
	Vlan2: Administración.
	Vlan3: Serve Seguridad.
<b>RF-007</b>	Configuraciones de políticas de seguridad en la herramienta
	Pfsense.
RF-008	Las diferentes segmentaciones nos permitirán administrar el
	tráfico de red.
<b>RF-009</b>	Se instalará el Centos8 en un servidor web en donde se
	almacenará nuestra página web del hotel.
<b>RF-010</b>	Se limitará el acceso a internet atreves del pfsense utilizando
	la herramienta SquidProxy.
<b>RF-011</b>	En el equipo de Administración se instalará la aplicación Main
	Console el cual permitirá controlará las cámaras ip.

<b>RF-012</b>	El Router Board se virtualizará 2 adaptadores que conectará al		
	pfsense y switch para los clientes.		
<b>RF-013</b>	Mediante la Aplicación Winbox nos permitirá administrar el		
	Mikrotik el cual se habilitará Hotspot.		
<b>RF-014</b>	Crear e implementación de los certificados al hostport el cual		
	nos validara el acceso y seguridad.		
<b>RF-015</b>	Crear y subir los certificados correspondientes para su		
	respectivo funcionamiento.		
<b>RF-016</b>	A los clientes se le otorgara un usuario y contraseña para poder		
	acceder al servicio de internet que brinda el hotel		
<b>RF-017</b>	Los clientes tendrán planes específicos de acuerdo con los días		
	de estadía.		
RF-018	El sistema mostrara el listado correspondiente de todos los		
	usuarios creados.		
RF-019	El sistema mostrara el listado correspondiente de todos los		
	usuarios conectados.		
RF-020	Dar mantenimientos a los equipos, mantener los sistemas y		
	programas siempre actualizados.		

**Tabla 1:** Requerimientos funcionales Elaborado por Carlos Orrala

#### **3.2 COMPONENTES DE LA PROPUESTA**

#### **3.2.1 FASE 1 PREPARAR**

## APLICACIÓN DEL MÉTODO DE RECOLECCIÓN MEDIANTE UNA ENTREVISTA.

La visita al hotel se realizó el fin de semana donde se conoce que existe más personas que acuden al hotel por motivo de vacaciones o visitar los diferentes balnearios de la provincia, dentro del establecimiento se inició con la entrevista hacia la administración de dicho hotel en donde nos detalló las diferentes falencias que tiene el servicio de internet nos comentó que se ha realizado cambio de equipos nuevos, pero no vio ningún cambio al respecto.

#### Análisis y aspectos exactos de la entrevista

- 1. Existe mala ubicación de los equipos que brinda el servicio de internet.
- 2. Carece de una infraestructura adecuada para el servicio.
- 3. Se dio a conocer que existe congestión con el servicio de internet debido a la demanda de usuarios que necesitan del servicio.
- 4. El mantenimiento o revisiones de los equipos no se hace adecuadamente ya que los trabajadores conoces muy poco de la tecnología.
- Al momento de un inconveniente con el servicio del internet los colaboradores del hotel realizar un apagado manual del proveedor principal los cual podría ocasionar inconveniente con los demás dispositivos.
- 6. Se ha realizado cambio de los equipos para poder tener más capacidad de usuarios, pero el problema preside.
- 7. Carece de seguridad hacia la información del hotel y sus huéspedes.

## APLICACIÓN DEL MÉTODO DE RECOLECCIÓN MEDIANTE OBSERVACIÓN.

Con este método identificamos todos los requerimientos para esto se realizó un análisis de la situación actual en el Hotel Copacabana del Cantón La Liberad, tomando en cuenta la ficha de observación el diseño actual donde podemos observar las necesidades y falencias que tiene el establecimiento hotelero.

Se realizó la visita al ente privado como es el Hotel Copacabana del Cantón La Libertad el cual el lapso de 1 día en donde se analizó y diagnostico los siguiente:

Se observó que no tiene establecida una topología de red adecuada el cual no se determina el diseño y estructura de la red para el hotel la cual afecta al buen funcionamiento de los componentes que se asocia a la entidad, lo cual esto nos da a notar que carece de una protección lo que genera vulnerabilidad y dar acceso a terceros o programas no deseados.

Falta de puntos de conexión a la red esto genera un problema a la limitación de acceso a los diferentes dispositivos que opta por utilizar el servicio de internet lo cual genera una pérdida de conectividad, falta de rendimiento y congestionamiento a la parte administrativa y a los huéspedes que optan por usar el servicio de internet.

Falta de seguridad de los datos del establecimiento hoteleros los cuales recopilan información de las personas que visitan tanto como el personal que labora en el establecimiento esta optante a recibir ataques o alguna amenaza externa.

Notamos que no está distribuyendo adecuadamente el tráfico de red lo cual genera un mal rendimiento a realizar diferentes tareas en nuestro equipo de trabajo los cuales llevan a cometer acciones no deseadas y no trabajar con eficacia. Para ver el formado completo (Anexo 2).

#### ANÁLISIS DEL DISEÑO DE RED ACTUAL.

Como observamos en la (Figura 3) de la red del establecimiento hotelero primeramente notamos que no existe una infraestructura adecuada para el mismo, carece de un firewall y la ausencia de switches en la infraestructura actual perjudica a la distribución de los equipos y eso no nos permitirá las segmentar de la red para cada uno de sus departamentos.

También tomamos en cuenta que los equipos que poseen el establecimiento hotelero para la comunicación se encuentran mal ubicados los cuales están propenso a vulnerabilidades y ser manipulados por personas no autorizadas, es notorio que las conexiones fuero realizada empíricamente en cual nos dificulta llevar un mal control administrativo de la red conjuntamente hace falta de equipo que permita la seguridad, alta disponibilidad y escalabilidad.

La falta de seguridad al acceso de la red es un inconveniente el cual no existe un control adecuando del tráfico y restricciones en la navegación para los trabajadores en sus horas laborables.



Figura 3: Diseño de red actual Elaborado por Carlos Orrala

#### 3.2.4 ESTRUCTURA ACTUAL DEL ESTABLECIMIENTO.

Con la visita técnica realizada al hotel Copacabana del Cantón La Libertad se pudo realizar un plano del establecimiento para representar donde actualmente se encuentran los equipos que se utilizan para brindar el servicio de internet.

Como observamos en la (Figura 4), el establecimiento hotelero tiene su router principal y el DVR en la zona de cafetería y una cámara análoga en el lobby por el cual el router principal es el que distribuye el internet a los repetidores que se encuentran en los diferentes piso del hotel, vemos que el router principal se encuentra vulnerable a personas que no forman parte del equipo de trabajo del hotel a esto el router puede ser manipulado por las personas que visitan el establecimiento también observamos que solo se encuentra un router como repetidor el cual brinda internet a las habitaciones.

El la (Figura 5), observamos que en este piso encontramos 2 router Tp-link el cual realizan la función de repetidores, uno de los router tiene problema de conexión cuando los huésped tratan de acceder al servicio y una cámara análoga, como se observa en la (Figura 6) solo dispone de un solo router y una cámara análogo, pero cabe recalcar que este router es de mejor calidad a los demás en la última (Figura 7) ,notamos que a pesar de tener pocas habitaciones existen espacios de recreación donde acuden los huésped en el cual solo hay un router que brinda el servicio de internet y encontramos dos cámaras análogas.



Figura 4: Estructura actual Primer Piso Elaborado por Carlos Orrala



Figura 5: Estructura actual Segundo Piso

Elaborado Por Carlos Orrala



Figura 6: Estructura actual Tercer Piso Elaborado por Carlos Orrala



Figura 7: Estructura actual Cuarto Piso o Terraza Elaborado por Carlos Orrala

## ANÁLISIS FINAL Y CONCLUSIÓN.

Se analizo que el establecimiento hotelero tiene un diseño de red básico donde el servicio de internet que brinda no es óptimo, también observamos que tiene pocos puntos de conexión a internet los cuales no abastecen al número de usuarios que requieren el servicio, su router principal o del proveedor se encuentra en una ubicación vulnerables. Además, la implementación de esta propuesta ayudara a la seguridad y servicio de internet que ofrecen el establecimiento hotelero y que su visitante tenga una grata estadía.

#### 3.2.2 FASE 2 PLANEAR.

#### ANÁLISIS DE FACTIBILIDAD

Mediante la metodología propuesta para el presente proyecto se determinó la situación actual del establecimiento en el cual presentamos el estudio de factibilidad que nos a establecer el valor de costo acorde a los equipos necesarios que ayudaran a mejorar el servicio de calidad del internet que ofrece el establecimiento hotelero y poder establecer la factibilidad de la implementación a la actual propuesta planteado, dentro de la propuesta se consideran los problemas de infraestructura, seguridad, administración y acceso a la red. Cabe recalcar que el estudio podrá ser utilizado para su futura implementación en el establecimiento. Este análisis se destacan tres pilares fundamentales:

- Factibilidad Operacional: Se refiere a todos aquellos recursos donde interviene algún tipo de actividad (procesos), depende de los recursos humanos que participen durante la operación del proyecto [34].
- Factibilidad Técnica: Se refiere a los recursos necesarios, tales como herramientas, conocimientos, habilidades, experiencias, siendo necesarios para efectuar actividades y procesos para el estudio [35].
- Factibilidad Económica: Son los recursos financieros que son necesarios para el desarrollo y para llevar a cabo los procesos básicos de la infraestructura [35].

#### FACTIBILIDAD OPERACIONAL

En la visita técnica que se realizó al Hotel Copacabana resalto cierta falencia las cuales necesitarían mejorar, en la cual se planea una nueva propuesta que solucionara las inconsistencias observadas las cuales desfavorece la seguridad y el servicio de internet que ofrece del establecimiento hotelero lo cual ocasiona que los huéspedes no disfruten adecuadamente del mismo.

Cabe Recalcar que no solo nos visitan personas que vienen de vacaciones también existe personas que asisten al establecimiento hotelero por motivos laboral los cuales hacen uso de nuestros servicios de internet y en ocasiones han tenido problemas con la conectividad las cuales han sugerido y recomendado la mejora del servicio de internet que ofrecen.

#### FACTIBILIDAD TÉCNICA

Para determinar los problemas que tiene el establecimiento hotelero en su infraestructura y poder mejorar el servicio que ofrece el mismo se realizó un análisis donde observamos y enumeramos los equipos que pertenecen al establecimiento por los cuales podrá ser reutilizado para el diseño de la nueva propuesta. El análisis también nos ayudó a reconocer los equipos que hacen falta en la red los cuales serán incluidos.

A continuación, presentamos mediante tablas los equipos de red existentes en la infraestructura actual del establecimiento hotelero:

Ubicación	Cantidad	Equipo	Modelo	Estado
Cafetería	1	Router inalámbrico Huawei		Utilizable
Piso 1	1	Router inalámbrico Tp Link Rompe Muros	TL-WR941HP	Utilizable
Piso 2	2	Router inalámbrico Tp Link	TL WR840N	No Utilizable
Piso 2	1	Switch 4 Puerto	TL-SF1008D	No Utilizable
Piso 3	1	Router inalámbrico Tp Link Rompe Muros	WR941HP	Utilizable
Piso 3		Router inalámbrico Tp Link	TL WR840N	No Utilizable
Piso 3	1	Switch 4 Puerto	TL-SF1008D	No Utilizable
Terraza	1	Router inalámbrico Tp Link Rompe Muros	WR941HP	Utilizable

Tabla 2:Equipo de red existente Elaborado por Carlos Orrala

Ubicación	Elementos	Utilización en el diseño
Piso 1-2-3	Cable UTP	NO
y Terraza	categoría 5	

Tabla 3: Elementos de cableado estructurado existentes Elaborado por Carlos Orrala

A continuación, presentamos mediante tablas los equipos de red y elementos que se requieren para el diseño de la nueva propuesta:

Modelo	Características	Equipo	Costo
Switch Small	Cisco Small Business		245,00
Business	SG300-10SFP		
SG300-	Capa L3		
10SFP	Administrable		
	08 puertos Gigabit 10/100/1000 SFP 02 puertos Gigabit para fibra SFP Rack montable.		

Mikrotik RouterBoard RB951Ui- 2nD HAP	Sistema operative RouterOS Estándar 802.11b/g/n Frecuencia 2.4 GHz 5 puertos		45,00
Router inalámbrico Tp Link Rompe Muros	Puertos: 4 LAN 10/100Mbps Puertos: 1 WAN 10/100Mbps Antenas fijas: 2 de 9dBi Frecuencia: 2.4GHz Compatible con estándar IEEE 802.11b/g/n para 2.4GHz Soporta encriptación WEP64/128 bit WEP, WPA, WPA2 Soporta: DHCP server, DHCP cliente	<image/>	46,50
Dell OptiPlex 3050	Intel Core i5-7400 3.0GHz (c/TB 3.5GHz) vPro Memoria RAM: 8 GB DDR4 Disco Duro 1TB 7200 RPM DVD-RW, Teclado y mouse		543,70
Switch Tp- link	Modelo: TL-SF1008D Puertos: 8 RJ-45 Fast Ethernet 10/100 Mbps Estándar: IEEE 802.3x Puertos: MDIX automático, dúplex medio o completo	Peire Pe	14,50

Rack gabinete	Modelo: NET- 77385127-GD		500,00
	Rack gabinete 27ur		
	Dimensiones Al x An x		
	Prf: 129 x 61 x 96 cm		
	Soporta Servidores,	r	
	Switches, Routers,		
	Patch Panel,		
	Organizadores, etc.		

Tabla 4: Equipo de red requerido Elaborado Por Carlos Orrala

Modelo	Características	Equipo	Costo
Rollo Cable	Cat 5E UT Cable sólido 305 metros • Velocidad de transmisión: 100 Mbps Ancho de banda: 100 MHz Distancia máxima del enlace: 90 m		44,50
Conector RJ45	Modelo: AM-CON-C5- 100PACK Para cable Cat5e Cobertura: metálica		8,65
Bota Capucha	Marca: AMPXL Modelo: CAPRJ45-GRIS 100 unidades Compatible con conectores: RJ-45 (no incluidos)		8,93

Tabla 5:Elementos de cableado estructurado requeridos Elaborado por Carlos Orrala

#### FACTIBILIDAD ECONÓMICA

Mediante la factibilidad económica se analizará el costo de la propuesta establecida y permitirá conocer detalladamente los valores de los equipos que se utilizaran, ya que esto ayudara al mejoramiento del servicio ya sea en su infraestructura o conectividad a la red para los huéspedes y administración, en caso de que se implemente tendrá la facilidad de conocer la parte económica que conllevará la propuesta.

A continuación, presentamos mediante tablas detalladamente el presupuesto del proyecto:

Descripción	Cantidad	Costo Unitario	Costo Total
Switch Small Business SG300- 10SFP	1	245	245
Mikrotik RouterBoard RB951Ui-2nD HAP	1	45	45
Router inalámbrico Tp Link Rompe Muros	3	46,5	139,5
Dell OptiPlex 3050	2	543,7	1087,4
Switch Tp-link	6	14,5	87
RACK GABINETE	1	500	500
Total			2103,9

Tabla 6: Presupuesto de equipamiento de red Elaborado por Carlos Orrala

Descripción	Cantidad	Costo Unitario	Costo Total
Rollo Cable	1	44,5	44,5
Conector RJ45	1	8,65	8,65
Bota Capucha	1	8,93	8,93
Total			62,08

Tabla 7: Presupuesto de elementos de cableado estructurado Elaborado por Carlos Orrala

A continuación, presentamos mediante tablas presupuesto total del proyecto:

Descripción	Costo Total
Presupuesto de equipamiento de red	2103,90
Presupuesto de elementos de cableado estructurado	62,08
Total	2165,98

Tabla 8: Presupuesto total del proyecto

#### **3.2.3FASE 3 DISEÑAR**

Las conexiones con los proveedores se generan mediante los routers que distribuye la entidad privada que deseen contratar el establecimiento hotelero los cuales vine con su propia configuración establecida, cabe recalcar que dichas configuraciones no serán modificadas por motivo de seguridad, ya que en la nueva propuesta sé usar un servidor Pfsense que estará conectado a los 2 proveedores de preferencia el cual nos ayudara con la seguridad de la red aplicando políticas de seguridad.

## DISEÑO LÓGICA DE LA RED

Esta fase se determina el diseño de la red propuesta el cual se puede observas en la (Figura 8), este lo representamos mediante un esquema de red y se especifica todos los elementos de la red a utilizar y la disposición de conexión.



Figura 8:Diseño de red lógica propuesta

#### **CONEXIÓN AL PROVEEDOR**

Las conexiones con los proveedores se generan mediante los router que distribuye la entidad privada que deseen contratar el establecimiento hotelero los cuales vine con su propia configuración establecida, cabe recalcar que dichas configuraciones no serán modificadas por motivo de seguridad ya que en la nueva propuesta se usar un servidor Pfsense que estará conectado a los 2 proveedores de preferencia el cual nos ayudara con la seguridad de la red aplicando políticas de seguridad.

#### SEGMENTACIÓN DE LA RED Y PROTOCOLO

La segmentación de la red parte de la dirección ip 192.168.100.1/24, pensada para proporcionar estabilidad al establecimiento hotelero que puede seguir ampliando su infraestructura para brindar mayor prestación tecnológica a los huéspedes, en los siguientes cuadros se detalla la división de la red en subredes para cada departamento:

Dispositivo Nombre de host	Interfaz	Dirección IP	Mascara de subred
ISP	192.168.100.1	192.168.100.1	255.255.255.0
SwitchCisco	VLAN 11 Red Publica	192.168.11.1	255.255.255.0
	VLAN 12 Red Administración	192.168.12.1	255.255.255.0
	VLAN 13 ServerWeb	192.168.13.1	255.255.255.0
Mikrotik		192.168.11.1	255.255.255.0
Admistración-PC		192.168.12.17	255.255.255.0
Recepción-PC		192.168.12.16	255.255.255.0
Clientes-PC		192.168.11.11	255.255.255.0
Pfsense		192.168.100.2	255.255.255.0
Serverweb		192.168.13.253	255.255.255.0

Figure 1: Tabla de direccionamiento Fuente: Elaboración propia

Puerto	Protocolo	Descripción
80	ТСР	HTTPS Protocolo de Transferencia de HiperTexto
8080	ТСР	Tomcat lo usa como puerto por defecto.
443	ТСР	HTTPS/SSL usado para la transferencia segura de páginas web
53	UDP	DNS Sistema de Nombres de Dominio
22	ТСР	SSH, SFTP
21	ТСР	Ping, solo usado para pruebas de conexión

Figure 2: Puerto y protocolo Fuente: Elaboración propia

#### FÍSICO DE LA RED

En esta fase se muestra las instalaciones del establecimiento hotelero en el cual especificamos la ubicación adecuada de los diferentes equipos que se necesitan para la elaboración de la propuesta y se plantea establecer un rack principal para los equipos de comunicación, a continuación, mostraremos las siguientes figuras de las diferentes plantas del Hotel Copacabana:



Figura 9: Diseño físico de la red 1 planta Fuente: Elaboración propia



Figura 10: Diseño físico de la red 2 planta Fuente: Elaboración propia



Figura 11:Diseño físico de la red 3 planta Fuente: Elaboración propia



Figura 12:Diseño físico de la red de la terraza Fuente: Elaboración propia

En la bodega de la segunda planta se establecerá el rack principal esta contendrá los equipos y los servidores que utilizaremos para la propuesta los cuales está ubicado en un lugar estratégico que nos permita tener un mejor control y seguridad de terceras personas que no son pertenecen al equipo de trabajo del hotel (Figura 10).

De acuerdo con la (Figura 9) plata observamos la recepción cuenta con un computador el cual se realiza el manejo de las cámaras de seguridad y las aplicaciones que utilizaremos en el proyecto propuesto, además contara con 2 router inalámbricos rompe muros que nos ayudara a brindar un mejor servicio de internet a los huéspedes en su estadía y 3 cámaras ip. En las demás plantas se ubicarán en lugares estratégicos los respectivos router inalámbricos y cámaras ip tales se observan las figuras.

#### 3.2.4 FASE 4 IMPLEMENTACION

Para la creación de la topología se utilizará la herramienta GNS3 donde simularemos un entorno virtual de la topología de red. Como observamos, este entorno tendrá un grado de abstracción al momento de diseñar y realizar las respectivas pruebas. Para la simulación de las máquinas virtuales, firewall, servidores web y RouterOS se usará el software de virtualización VirtualBox, en donde las 2 herramientas establecerán conexión para así tener una simulación de un entorno real.

#### INSTALACIÓN VIRTUAL DE LAS EQUIPOS Y HERRAMIENTAS.

Una vez finalizados las instalaciones de las herramientas en nuestro entorno virtual que encontraran detalladamente en nuestro manual de instalación (Anexo 3), nuestra área de trabajo estará completa para para realizar las respectivas configuraciones para su manejo (Figura 13).

Máquinas Virtuales	Sistema Operativo	Sistema	Almacenamiento	Red
GNS3	Ubuntu 64-bit	4gb ram	500Gb	2 adaptador
Firewall Pfsense	FreeBSD 64-bit	4gb ram	64Gb	3 adaptador
Servidor Web	Linux 64-bit	4gb ram	51Gb	1 adaptador
Mikrotik	Linux 64-bit	2gb ram	504,55 Mb	2 adaptador
Administración	Windows 7 64-bit	4gb ram	32Gb	1 adaptador
Recepción	Windows 7 64-bit	4gb ram	32Gb	1 adaptador
Clientes	Windows 7 64-bit	4gb ram	32Gb	1 adaptador

Tabla 9: Detalles Máquinas Virtuales Elaborado por Carlos Orrala



Figura 13: Maquinas Virtualizadas Elaborado por Carlos Orrala



Figura 14: Diseño prototipo de red EN GNS3 Elaborado por Carlos Orrala

# CONFIGURACIÓN FIREWALL PRINCIPAL PFSENSE (Vlan, Servidor DHCP, Static DHCP, DNS y DNS Resolver).

Una vez terminada la instalación nos mostrara mediante la terminal el menú de opciones

de configuración de Pfsense (Figura 15).

Generating RRD graphsdone.	
Starting syslogdone.	
Starting CRON done.	
pfSense (pfSense) 2.3.3-RELEASE amd64	Thu Feb 16 06:59:53 CST 2017
Bootup complete	
FreeBSD/amd64 (pfSense.localdomain) (†	ttyv0)
*** Welcome to pfSense 2.3.3-RELEASE	(amd64 full-install) on pfSense ***
WAN (wan) -> em0 ->	
LAN (lan) $\rightarrow$ em1 $\rightarrow$ v4:	192.168.1.1/24
0) Logout (SSH onlu)	9) nfTon
1) Assign Interfaces	10) Filter Logs
Z) Set interface(s) IP address	11) Restart webConfigurator
<ol> <li>Reset webConfigurator password</li> </ol>	12) PHP shell + pfSense tools
4) Reset to factory defaults	13) Update from console
5) Reboot system	14) Enable Secure Shell (sshd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) She11	
Enter an option:	

Figura 15: Opciones de configuración Pfsense Elaborado por Carlos Orrala

A continuación, realizamos las configuraciones de las interfaces de red y elegimos la opción 1 "Assign Interfaces", donde su configuración se realizará manualmente de la siguiente manera:

- ✓ No a la opción de usar VPN
- ✓ Interfaz WAN em0
- ✓ Interfaz LAN em1
- ✓ Interfaz WAN2 em2

Configurando las interfaces que utilizaremos, asignaremos las respectivas dirección IP y elegimos la opción "Set Interfaces IP Address" (Figura 16):

- Interfaz WAN, configuración manual
- ✓ IP: 192.168.100.2
- ✓ IP: 255.255.255.0 = 24
- ✓ Gateway: 192.168.40.1
- Interfaz LAN, configuración manual
- ✓ IP: 192.168.10.1
- ✓ IP: 255.255.255.0 = 24
- ✓ Gateway: Enter
- ✓ Enable DHCP: no
- Interfaz OPT1, configuración manual
- ✓ IP: 192.168.1.27
- ✓ IP: 255.255.255.0 = 24
- ✓ Gateway: Enter
- ✓ Enable DHCP: no

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a08dcaa9b2dcc30b882b
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)       -> em0       -> v4/DHCP4: 192.168.1.40/24         LAN (lan)       -> em1       -> v4: 192.168.10.1/24         WAM2 (opt1)       -> em2       -> v4/DHCP4: 192.168.1.27/24

Figura 16 : Interfaces del Pfsense Fuente: Elaboración propia

Una vez obtenida la dirección ip 192.168.10.1 realizamos la prueba de conexión hacia un computador para acceder a la interfaz web, nos mostrara el login donde iniciaremos sesión con el usuario: admin y clave: pfsense predeterminada

$\leftarrow \rightarrow G$ 0	8 192.168.10.1	45	80%	☆	${igsidential}$	பி	≡
<b>pf</b> sens	e.				Login to p	fSens	e
	SIGN IN						
	admin						
	•••••						
	SIGN IN						
	pfSense is developed and maintained by Netgate. ©	) ESF 2004 - 2023 View lid	ense.				

Figura 17 : Interfaz Web pfsense Fuente: Elaboración propia

Ya realizadas las configuraciones correctamente y listo para utilizarlos nos presentara su interfaz principal (Figura 18) con las siguientes opciones en donde nos dirigiremos a Interface→ Assignments→VLANs: seleccionamos la interfaz física e ingresamos el número que identificara la VLAN y una pequeña descripción para saber dónde pertenece (Figura 19).

👂 🗾 pf:	Sense.home.arpa - Status: Das × +		$\sim$	
$\leftrightarrow$ $\rightarrow$	C 🛇 👌 192.168.10.1		80% 🖒	ල එ ≡
	9, System → Interfaces → Firewall → Services	;     VPN	<ul> <li>Help →</li> </ul>	G
WARNING: T	The 'admin' account password is set to the default value. Chan	ge the password in the User Manager.		
Status / D	Jashboard			+ 0
System Info	ormation 🥕 🗢	Netgate Services And Supp	port	• •
Name	pfSense.home.arpa			
lser	admin@192.168.10.1[192.168.12.2] (Local Database)	Retrieving support information 😽		
ystem	VirtualBox Virtual Machine Netgate Device ID: a08dcaa9b2dcc30b882b			ដ
BIOS	Vendor: innotek GmbH	Interfaces		۶ ⊂ ۶
	Version: VirtualBox Release Date: Fri Dec 1 2006	🚠 WAN 🛧 1000baseT	<full-duplex></full-duplex>	192.168.1.40
lersion		•		
- craron	2.6.0-RELEASE (amd64)	LAN T 1000basel	<full-duplex></full-duplex>	192.168.10.1

Figura 18: Interfaz principal pfsense Fuente: Elaboración propia

•	of pfSense.	home.arpa - Interfaces: × + ·	- F	
$\leftarrow$	$\rightarrow$ C	○ 👌 192.168.10.1/interfaces_vlan_edit.php?id=0 ☆	ତ ମ	≡
p	sense	2		
	WARNING: T	he 'admin' account password is set to the default value. Change the password in the User Manager.		
1	Interfaces	/ VLANs / Edit	₩ 0	
V	/LAN Conf	guration		
<u>Pa</u>	arent Interfac	em1 (08:00:27:2d:7d:57) - Ian  Only VLAN capable interfaces will be shown.		
	<u>VLAN Ta</u>	10 Real Real Real Real Real Real Real Real		
	VLAN Priori	ty 0 802.1Q VLAN Priority (between 0 and 7).		
	Descriptio	RED PUBLICA A group description may be entered here for administrative reference (not parsed).		

#### Figura 19: Crear Vlan de pfsense Fuente: Elaboración propia

of Sense.ho	me.arpa - Interfaces: ×	+					$\sim$		Ē
$\rightarrow$ C	🔿 掻 192.168.1	0.1/interfaces_vl	an.php				ŝ	$\bigtriangledown$	பி
of sense									
WARNING: The	'admin' account password	is set to the defaul	lt value. Chan	ge the passv	vord in the	User Mana	iger.		
Interfaces /	VLANs							₩.	•
Interface Assignn	nents Interface Group	os Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	
LAGGs									
VLAN Interfa	ces								
Interface	VLAN tag	Priority		Descriptio	n		Actions		
	10			RED PUBLI	CA		e 🖉 🖉		
em1 (lan)	10								
em1 (lan) em1 (lan)	20			ADMINIST	RADOR		A 🗊		

Figura 20: Total Vlan creadas Fuente: Elaboración propia Una vez creadas las Vlan son dirigimos a Interface Assignments seleccionaremos las nuevas Vlan y las agregaremos (Figura 21).

•	🗾 pfSens	e.home.arpa - Interfaces: × + ·	
$\leftarrow$	$\rightarrow$ C	○ À 192.168.10.1/interfaces_assign.php E 80% ☆ ♡	മ ≡
pfs		System + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +	•
WAI	RNING: The 'ad	dmin' account password is set to the default value. Change the password in the User Manager.	
Inte	erfaces / Ir	nterface Assignments	<b>M (</b> )
Inter	rface Assignmei	nts Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs	
Interfa	ace		
WAN		Network port	
		Network port           em0 (08:00:27:79:c4:25)	
LAN		Network port           em0 (08:00:27:79:c4:25)	
LAN WAM2	2	Network port           em0 (08:00:27:79:c4:25)         v           em1 (08:00:27:2d:7d:57)         m Delete           em2 (08:00:27:68:54:b1)         m Delete	
LAN WAM2 VLAN1	2	Network port           em0 (08:00:27:79:c4:25)	
LAN WAM2 VLAN1	2 10 20	Network port           em0 (08:00:27:79:c4:25)	
LAN WAM2 VLAN1 VLAN2 VLAN2	2 LO 20	Network port         em0 (08:00:27:79:c4:25) <ul> <li>em1 (08:00:27:2d:7d:57)</li> <li>im Delete</li> </ul> em2 (08:00:27:68:54:b1) <ul> <li>im Delete</li> <li>VLAN 10 on em1 - Ian (RED PUBLICA)</li> <li>im Delete</li> <li>VLAN 20 on em1 - Ian (ADMINISTRADOR)</li> <li>im Delete</li> <li>VLAN 30 on em1 - Ian (SERVER)</li> <li>im Delete</li> </ul>	

Figura 21: Interfaz Agregadas pfsense Fuente: Elaboración propia

Ahora se realizó la configuración del puerto troncal y Vlans en el conmutador de red, se creó las nuevas vlan respectivas de acuerdo a los departamentos que tiene el hotel y se asignó los puertos correspondientes.

Switch(config)#vlan 10	
Switch(config-vlan)#name	red publica
Switch(config-vlan)#exit	
Switch(config)#vlan 20	
Switch(config-vlan)#name	administracion
Switch(config-vlan)#exit	
Switch(config)#vlan 30	
Switch(config-vlan)#name	server
Switch(config-vlan)#	
Switch(config-vlan)#	
Switch(config-vlan)#	
Switch(config-vlan)#exit	
Switch(config)#	

Figura 22: Asignación de vlan Fuente: Elaboración propia

Switch(config)#
Switch(config)#in
Switch(config)#interface r
Switch(config)#interface range g
Switch(config)#interface range gigabitEthernet
Switch(config)#interface range gigabitEthernet 0/0-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mod
Switch(config-if-range)#switchport mod
Switch(config-if-range)#switchport mod
Switch(config-if-range)#switchport mod access
Switch(

Figura 23: Puerto Trocal Fuente: Elaboración propia

Switch(config)#
Switch(config)#in
Switch(config)#interface r
Switch(config)#interface range g
Switch(config)#interface range gigabitEthernet
Switch(config)#interface range gigabitEthernet 0/0-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mod
Switch(conf

Figura 24: Vlan 10 Fuente: Elaboración propia

```
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mo
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#no shut
Switch(config-if-range)#no shut
Switch(config-if-range)#end
```

Figura 25: Vlan 20 Fuente: Elaboración propia

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#int
Switch(config)#interface r
Switch(config)#interface range g
Switch(config)#interface range gigabitEthernet 2/0-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#exit
Switch#copy
*May 13 18:15:15.533: %SYS-5-CONFIG I: Configured from console by console
Switch#copy ru
Switch#copy_running-config_c
Switch#copy running-config s
Switch#copy running-config s
Switch#copy running-config st
Switch#copy running-config startup-config
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration
Compressed configuration from 4018 bytes to 1751 bytes[OK]
*May 13 18:15:42.502: %GRUB-5-CONFIG WRITING: GRUB configuration is being updated on disk. Please wait
Switch#



VLAN	Name	Status	Ports				
1 10 20 30 1002 1003 1004 1005	default red publica administracion server fddi-default token-ring-default fddinet-default trnet-default	active active active act/unsup act/unsup act/unsup act/unsup	Gi3/1, Gi0/0, Gi1/0, Gi2/0,	Gi3/2, Gi0/1, Gi1/1, Gi2/1,	Gi3/3 Gi0/2, Gi1/2, Gi2/2,	Gi0/3 Gi1/3 Gi2/3	

Figura 27:Tabla Vlan Fuente: Elaboración propia

Continuamos ingresamos al Menú $\rightarrow$  Interfaces y seleccionamos las interfaces agregadas las cuales realizaremos las siguientes configuraciones habitamos la interfaz, en caso que quisiera cambiar de nombre le agregamos, el tipo de configuración ya sea IPV4 o IPV6, la velocidad y dúplex por último configuramos la IP y guardamos $\rightarrow$  aplicamos.

Interfaces / RED_PL	JBLICA (em1.10) 🛎 🖬 \Theta
General Configuration	
Enable	✓ Enable Interface
Description	RED_PUBLICA Enter a description (name) for the Interface here.
IPv4 Configuration Type	Static IPv4 v
IPv6 Configuration Type	None v
MAC Address	X000000000X The MAC address of a VLAN Interface must be set on its parent interface
мти	(     (     )
MSS	Also is ansared in this field, then MSS damping for TCP connections to the value ansared above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autosalect)         v           Explicitly set speed and duplex mode for this interface.         WARVENUS: MUST be set to autosalect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192168.11.1 / 24 ~
IPv4 Upstream gateway	None   Add a new gateway  Melo tendets is to Tetrane exactles, called to a control from the life a cell to a units the "deb" to me

Figura 28: Configuración Vlans Fuente: Elaboración propia

Nos dirigimos a Services  $\rightarrow$  DNS Resolver  $\rightarrow$ General Settings, habilitamos configuramos Network interfaces que son: WAN, WAN2, RED\_PUBLICA, ADMINISTRACION y localhost esto nos permitirá que el pfsense se pregunte a si mismo sobre los DNSA, también determinamos la interfaz de salida que en este caso será All y guardamos cambios.

🔹 🗾 pfSense.hor	ome.copacabana - Sei X +	<b></b>
$\leftarrow \rightarrow $ C	○ 월 192.168.100.2/services_unbound.php 80% ☆ ♡ 환	
Services / DNS Re	esolver / General Settings C 💿 🖬 🗐	•
General Settings Adv	dvanced Settings Access Lists	
General DNS Resolv	lver Options	- 1
Enable	Enable DNS resolver	
Listen Port	53	
	The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.	
Enable SSL/TLS Service	Respond to incoming SSL/TLS queries from local clients Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS Activating this option disables automatic interface response routing behavior thus it works best with specific interface bindings.	5.
SSL/TLS Certificate	webConfigurator default (627e878599d62)	
	The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.	
SSL/TLS Listen Port	853	
	The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.	
<u>Network Interfaces</u>	RED_PUBLICA IPv6 Link-Local ADMINISTRACION IPv6 Link-Local SERVIDORWEB IPv6 Link-Local Localhost	
	Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used.	~

Figura 29:DNS Resolver-General Settings parte 1

😆 🗾 pfSense.ho	zme.copacabana - Sei X +	<u> </u> _X
$\leftarrow \ \rightarrow \ \mathbf{G}$	⑦ 월 192.168.100.2/services_unbound.php 67% ☆ ♡ 指	≡
<u>System Domain Local Zone</u> <u>Type</u>	Transparent   The local-zone type used for the pfSense system domain (System   General Setup   Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(S) manual pages.	
DNSSEC	Enable DNSSEC Support	
Python Module	Enable Python Module Enable the Python Module.	
DNS Query Forwarding	Enable Forwarding Mode If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (# DNS Server Override is enabled there).	
	Use SSL/TLS for outgoing DNS Queries to Forwarding Servers When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.	
DHCP Registration	Register DHCP leases in the DNS Resolver      Hostname when requesting an IP-4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved      Note that this will cause the Resolver to reload and fluch its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.	
Static DHCP	Register DHCP static mappings in the DNS Resolver     If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also     be set to the proper value.	
OpenVPN Clients	Register connected OpenVPN clients in the DNS Resolver If this option is set, then the common name (INI) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.	
Display Custom Options	🕸 Display Custom Options	5
	C Save	

Figura 30:DNS Resolver-General Settings parte 2

A continuación, nos vamos para las opciones Services  $\rightarrow$  DNS Resolver  $\rightarrow$  Advanced Settings habilitamos realizamos las configuraciones como es el aumento de cache de 4MB a 512 MB guardamos y aplicamos los cambios.

🔰 🗾 pfSense.ho	me.copacabana - Sei X +	~	
$\leftarrow \rightarrow $ G	O 👌 192.168.100.2/services_unbound_advanced.php	67% 🖒	ල
Services / DNS Resolution	ver / Advanced Settings		C® ∓ ⊨ ∎ 0
General Settings Advanced	d Settings Access Lists		
Advanced Privacy Options	5		
Hide Identity	✓ id.server and hostname.bind queries are refused		
Hide Version	version.server and version.bind queries are refused		
Query Name Minimization	Send minimum amount of QNAME/QTHPE information to upstream servers to enhance privacy Only send minimum required labels of the QNAME and set QTMPE to A when possible. Best effort approach: full i replies with a RCODE other than NOERROR, except when receiving NXDOMAN from a DNSSEC signed zone. De Refer to RFC 7815 for in-depth information on Query Name Minimization.	QNAME and original QTYPE wil fault is off.	l be sent when upstream
Strict Query Name Minimization	Do not fall-back to sending full QNAME to potentially broken DNS servers QNAME minimization in strict mode. A significant number of domains will fail to resolve when this option in e option only has effect when Query Name Minimization is enabled. Default is off.	nabled. Only use if you know v	vhat you are doing. This
Advanced Resolver Option	ns		
Prefetch Support	Message cache elements are prefetched before they expire to help keep the cache up to date When enabled, this option can cause an increase of around 10% more DNS traffic and load on the server, but fr	equently requested items will r	tot expire from the cache.
Prefetch DNS Key Support	DNSKEW are fatched earlier in the validation process when a Delegation signer is encountered This helps lower the latency of requests but does utilize a little more CPU. See: Wikipedia		
Harden DNSSEC Data	DNSSEC data is required for trust-anchored zones. If such data is absent, the zone becomes bogus If Disabled and no DNSSEC data is received, then the zone is ma	ide insecure.	
Serve Expired	Serve cache records even with TL of 0 When enabled, allows unbound to serve one query even with a TL of 0, if TL is 0 then new record will be reque cache is updated without latency on service of the DNS request.	asted in the background when	the cache is served to ensure
1 ·			

Figura 31:DNS Resolver-Advanced Settings parte 1

💊 🛛 🗹 pfSense.hon	ne.copacabana - Ser × +	$\sim$	
$\leftarrow \rightarrow $ G	🔿   192.168.100.2/services_unbound_advanced.php	67% 🖒	ତ ଧ =
	this amount. The RRSet cache contains the actual RR data. The default is 4 megabytes.		
Outgoing TCP Buffers	$10$ $\checkmark$ The number of outgoing TCP buffers to allocate per thread. The default value is 10. If 0 is selected then TCP queri	es are not sent to authoritative se	irvers.
Incoming TCP Buffers	$10$ $\checkmark$ The number of incoming TCP buffers to allocate per thread. The default value is 10. If 0 is selected then TCP queri	es are not accepted from clients.	
EDNS Buffer Size	Automatic value based on active interface MTUs Number of bytes size to advertise as the EDNS reassembly buffer size. This is the value that is used in UDP datagra Auto mode sets optimal buffer size by using the smallest MTU of active interfaces and subtracting the IPv4/IPv6 M If fragmentation reassemble problems occur, usually seen as timeouts, then a value of 1422 should help. The 512/1222 values bypasses most IPv4/IPv6 MU gath problems, but it can generate an accessive amount of TCP	ims sent to peers. eader size. fallback.	
Number of Queries per Thread	512  The number of queries that every thread will service simultaneously. If more queries arrive that need to be service dropped.	d, and no queries can be jostled,	then these queries are
Jostle Timeout	200  This timeout is used for when the server is very busy. This protects against denial of service by slow queries or high	h query rates. The default value is	200 milliseconds.
Maximum TTL for RRsets and Messages	86400 The Maximum Time to Live for RRsets and messages in the cache. The default is 86400 seconds (1 day). When the in configured to force the reactiver to query for data more often and not trust (very large) TL values.	nternal TTL expires the cache iter	his expired. This can be
Minimum TTL for RRsets and Messages	O The Minimum Time to Live for RRsets and messages in the cache. The default is 0 seconds. If the minimum value k owner intended, and thus lear queries are made to look up the data. The Ovalue ensures the data in the cache is a trouble as the data in the cache might nor match up with the actual data anyone.	icks in, the data is cached for Ion as the domain owner intended. H	ger than the domain igh values can lead to
TTL for Host Cache Entries	Is minutes     Time to Live, in seconds, for entries in the infrastructure host cache. The infrastructure host cache contains round DNS servers. The default value is 15 minutes.	d trip timing, lameness, and EDN	S support information for
Number of Hosts to Cache			

Figura 32: DNS Resolver-Advanced Settings parte 2

### CONFIGURACIÓN NAT, REGLAS EN EL FIREWALL

#### Configuración NAT en el firewall

A continuación, configuramos los servicios NAT en el firewall que nos servirá para la traslación de paquetes de las distintas redes que existen para ello accedimos a la pestaña Firewall  $\rightarrow$  NAT  $\rightarrow$  Porta forward (Figura 33).

DÍ	pfSer	nse.hor	ne.copaca		🗦 traductor	r - Buscar co	on × ε	တ္တိ Ajustes		×	+ ~	l
$\rightarrow$	С		$\bigcirc$	3 192.	168.100.2,	/firewall_na	at.php			8	7% 公	6
	pf		SC.					k				
	w	ARNING	i: The 'admi	n' account	password is se	t to the defaul	lt value. Char	nge the pass	word in the User	Manager.		
	Fi	rewal	I/ NAT	/ Port	Forward							0
	Por	rt Forwa	rd 1:1	Outbo	ound NP	τ						
	Por Ru	rt Forwa	rd 1:1	Outbo	ound NP	τ						
	Por Ru	rt Forwa les	rd 1-1 Interface	Outbo	Source Address	t Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	Por Ru	Ies	Interface	Outbo Protocol TCP	Source Address	Source Ports *	Dest. Address WAN address	Dest. Ports 8081	NAT IP 192168.11.253	NAT Ports 8080	<b>Description</b> mikrotik	Actions
	Por Ru	rt Forwal les ✓ >⊄	Interface WAN	Outbo Protocol TCP TCP	Source Address *	* *	Dest. Address WAN address WAN address	Dest. Ports 8081 8291	NAT IP 19216811253 19216811253	NAT Ports 8080 8291	Description mikrotik mikrotik wb	Actions
	Por Ru	rt Forwar les ✓ × ✓ ×	Interface WAN WAN	Outbo Protocol TCP TCP	Source Address * *	* Source Ports  *	Dest. Address WAN address WAN address *	Dest.           Ports           8081           8291           5555	NAT IP 192168.11.253 192168.13.253	NAT Ports 8080 8291 22 (SSH)	Description mikrotik mikrotik wb ssh	Actions
	Por Ru D	rt Forwar Ies ✓ >4 ✓ >4 ✓ >4	Interface WAN WAN WAN	Cutbe Protocol TCP TCP TCP	Source Address * *	t Source Ports * * *	Dest.       Address       WAN       address       WAN       address       WAN       address       WAN       address	Dest.           Ports           8081           8291           5555           8080	NAT IP 19216811253 19216813253 19216813253	NAT Ports 8080 8291 22 (SSH) 80 (HTTP)	Description mikrotik mikrotik wb ssh nat server	Actions

Figura 33: Reglas NAT Elaborado por Carlos Orrala

Al momento de crear una nueva regla nos mostrara opciones de configuraciones en donde esencialmente completaremos las siguiente como son: Interface, Protocol, Source Address. Dest. Address, Dest. Ports, NAT IP, NAT Ports, Description, las reglas varían de acuerdo al puerto al cual quiere acceder (Figura 34 - Figura 35).

Edit Redirect E	ntry	
Disabled	Disable this rule	
No RDR (NOT)	Disable redirection for traffic matching this rule	
	This option is rarely needed. Don't use this without thorough knowledge of the implications.	
Interface	WAN	~
	Choose which interface this rule applies to. In most cases "WAN" is specified.	
Address Family	IPv4	~
1	Select the Internet Protocol version this rule applies to.	
Protocol	ТСР	~
	Choose which protocol this rule should match. In most cases "TCP" is specified.	
Source	🔁 Display Advanced	
Destination	🗌 Invert match. 🛛 WAN address 🗸 🗸 🗸	~
	Tora	

Figura 34: Configuración de reglas Nat de acceso al Mikrotik 1 Elaborado por Carlos Orrala

Red Sct target	Other	~	8080
port	Port		Custom
	Specify the port on the machine with the ID	address enterer	above In case of a port range specify the beginning
	port of the range (the end port will be calcul	lated automatic	allv).
	This is usually identical to the "From port" at	oove.	
Description	mikrotik		
	A description may be entered here for admir	nistrative referen	ice (not parsed).
No XMLRPC	Do not automatically sync to other CAR	P members	
Sync	This prevents the rule on Master from auton	natically syncing	to other CARP members. This does NOT prevent th
	rule from being overwritten on Slave.		
NAT reflection	Use system default		
Filter rule	Rule NAT mikrotik		
association	View the Electrole		
	view the filter fulle		
Rule Informati	on		
Created	1/23/23 01:08:39 by admin@192.168.11.4 (Lo	cal Database)	
Updated	1/23/23 01:08:39 by admin@192.168.11.4 (Lo	cal Database)	

Figura 35 : Configuración de reglas Nat de acceso al Mikrotik 2 Elaborado por Carlos Orrala

#### Configuración Reglas en el firewall

Debemos tomar en cuenta que las reglas creadas en el firewall son de suma importancia para fragmentar nuestra red en donde permitiremos y negaremos cierto tráfico de red especifico que fluye a través de varias interfaces físicas y lógicas creadas, para esto accederemos a la pestaña de Firewall → Rules donde observamos las diferentes interfaces como son: WAN, LAN, WAN2, RED\_PUBLICA, ADMINISTRACION, SERVIDORWEB.





Para configura las reglas debemos tomar en cuenta las acciones y parámetros principales como son:

- Pass: Permite el tráfico al destino.
- Reject: Rechaza el paquete y avisa al emisor.
- Block: Rechaza el paquete de manera silenciosa.
- Disabled: Deshabilitar temporal la regla sin eliminarla.
- Interface: A que interfaz se dirigirá.
- Protocol: Protocolo a utilizar en la regla de firewall.
- Source: Se define el host origen o la dirección de red.
- Destination: Se define el host o la dirección de red destino.

#### Configuración Reglas en la interfaz WAN

Sense Syste	em 🕶 Interfaces 🕶	Firewall 👻	Services 🕶	VPN 🕶	Status 🕶	Diagnostics 👻	Help 👻	
WARNING: The 'admin' acc	count password is set to th	e default value. (	Thange the pass	word in the U	lser Manager.			
Firewall / Rules /	Edit							≢ Ш 🗏
Edit Firewall Rule								
Action	Pass				~			
	Choose what to do with Hint: the difference betv whereas with block the p	packets that may veen block and re packet is dropped	tch the criteria s ject is that with I silently. In eithe	pecified belov reject, a pack r case, the or	v. et (TCP RST or iginal packet is	ICMP port unreacha discarded.	able for UDP) is retu	rned to the sender,
Disabled	Disable this rule Set this option to disable	e this rule withou	t removing it from	m the list.				
Associated filter rule	This is associated with a Editing the interface, pro	NAT rule. ptocol, source, or	destination of a	sociated filte	er rules is not p	ermitted.		
<u>Interface</u>	WAN Choose the interface fro	om which packets	must come to n	natch this ruk	<b>v</b>			
Address Family	IPv4				~			
	Select the Internet Proto	col version this ru	le applies to.					

Figura 37: Configuración reglas de la interfaz WAN parte 1 Elaborado por Carlos Orrala

Source							
Source	Invert match	any		~	Source Address	1	~
	Cisplay Advanced						
	The Source Port Range for a its default value, any.	connection is typically random a	and almost never equal	to the d	estination port. In most cases this settin	g must	remain at
Destination							
Destination	Invert match	LAN address		~	Destination Address	1	~
Destination Port Range	HTTP (80)	Curtom	HTTP (80)	~			
	Specify the destination port or	port range for this rule. The "To	field may be left empt	y if only	filtering a single port.		
Extra Options							
Log	Log packets that are hand Hint: the firewall has limited lo Status: System Logs: Settings (	led by this rule cal log space. Don't turn on logg page).	ing for everything. If do	ing a lot	of logging, consider using a remote sysl	og serv	er (see the
Description	NAT WAM80						
	A description may be entered log.	here for administrative referenc	e. A maximum of 52 ch	aracters	will be used in the ruleset and displayed	d in the	firewall
Advanced Options	Cisplay Advanced						

Figura 38: Configuración reglas de la interfaz WAN parte 2 Elaborado por Carlos Orrala

WARNIN	EDITION	System -	Interface ssword is se	s • t to the de	Firewall + Servio	the password in	the User Man	s ≠ Di ager.	agnostics 👻	Help <del>v</del>	(-
Firewa	all / Rule	es / WAN									≠ Ш 🗉 😧
Floating	WAN	LAN	WAN2	RED_PU	BLICA ADMINIS	TRACION	SERVIDORWE	в			
Rules (	(Drag to	Change C	)rder)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
] 🗸	States 2 /24 KiB	Protocol IPv4 *	source	Port *	Destination	Port *	Gateway *	Queue none	Schedule	Description	Actions
] ] <b>/</b> ] <b>/</b>	States           2 / 24 KiB           0 / 0 B	Protocol IPv4 * IPv4 ICMP any	Source * *	Port *	VAN net	Port *	Gateway * *	Queue none none	Schedule	Description wan net	Actions ⊕♪♪□○亩 ⊕♪♪□○亩
	States           2 / 24 KiB           0 / 0 B           0 / 0 B	Protocol IPv4 * IPv4 ICMP any IPv4 TCP	Source * * * * * *	Port * * *	VAN net LAN address	Port           *           *           80 (HTTP)	Gateway * * * *	Queue none none none	Schedule	Description wan net NAT WAM80	Actions
	States           2 / 24 KiB           0 / 0 B           0 / 0 B           0 / 0 B	Protocol IPv4 * IPv4 ICMP any IPv4 TCP IPv4 TCP	Source * * * * * * * * * * * * * * * * * * *	Port * * * *	bestination     *     WAN net     LAN address     192.168.13.253	Port           *           80 (HTTP)           80 (HTTP)	Gateway * * * * * * * *	Queue none none none none	Schedule	Very Very Very Very Very Very Very Very	Actions ♣ ♪ ₽ □ ○ 前 ♣ ♪ ₽ □ ○ 前 ♣ ♪ ₽ □ ○ 前
	States           2 / 24 KiB           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B	Protocol IPv4 * IPv4 ICMP any. IPv4 TCP IPv4 TCP IPv4 TCP	Source * * * * * * * * * * * * * * * * * * *	Port * * * * * * * * * * *	Destination           *           WAN net           LAN address           192.168.13.253           192.168.13.253	Port  *  80 (HTTP)  80 (HTTP)  22 (SSH)	Gateway  *  *  *  *  *  *  *  *  *  *  *  *  *	Queue none none none none	Schedule	Description wan net NAT WAM80 NAT nat server NAT ssh	Actions
	States           2 / 24 KiB           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B           0 / 0 B	Protocol           IPv4 *           IPv4 ICMP           any           IPv4 TCP           IPv4 TCP           IPv4 TCP           IPv4 TCP           IPv4 TCP           IPv4 TCP	Source * * * * * * * * * * * * * * * * * * *	Port  *  *  *  *  *  *  *  *  *  *  *  *  *	Destination           *           WAN net           LAN address           192.168.13.253           192.168.13.253           192.168.13.253	Port  *  80 (HTTP)  80 (HTTP)  22 (SSH)  8080	Gateway	Queue none none none none none	Schedule	Description wan net NAT WAM80 NAT nat server NAT ssh NAT mikrotik	Actions       ♣ ✔ □ ○ 前       ♣ ✔ □ ○ 前       ♣ ✔ □ ○ 前       ♣ ✔ □ ○ 前       ♣ ✔ □ ○ 前       ♣ ✔ □ ○ 前

Figura 39 : Reglas WAN Elaborado por Carlos Orrala

## Configuración Reglas en la interfaz LAN

								une open mi	unugu.		
Firev	vall / R	ules / LA	N								≑ ਘ 🗉 🖗
Floating	WA	N LAN	WAN2	RED	PUBLICA A	DMINISTR	ACION	SERVIDOR	WEB		
	_		•								
Rules	(Drag t	to Change	e Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/0 B	*	*	*	LAN Address	80	ż	*		Anti-Lockout Rule	۵.
~					*	*	*	none		Default allow LAN to any rule	ᢤ∥᠒⊘面
• •	0 /0 B	IPv4 *	*	•						-	

Figura 40: Reglas LAN Elaborado por Carlos Orrala

OMMUNIT	PINSE	System	▼ Interfaces ▼ F	Firewall 🔻	Services 🕶	VPN	≠ Stat	US <del>v</del>	Diagnostics 👻	Help 🔻	G
WARN	IING: The '	admin' accour	nt password is set to the de	fault value	. Change the pas	sword in t	the User Mai	nager.			
Firev	vall / R	lules / W	AN2								≢ ਘ 🗉 0
Floating	) WA	IN LAN	WAN2 RED_PUE	BLICA	ADMINISTRACI	ON :	SERVIDORW	/EB			
	Contrag	to Chang	e Order)	Baat	Destination	Peat	Catalogue	0	Cabadala	Description	Antines
	States	to Chang Protocol	e Order) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<pre>x</pre>	States 0/0B 0/0B	to Chang Protocol * *	e Order) Source RFC 1918 networks Reserved Not assigned by IANA	Port *	Destination * *	Port *	Gateway *	Queue * *	Schedule	Description Block private networks Block bogon networks	Actions O
<ul> <li>□</li> <li>×</li> <li>×</li> <li>✓</li> </ul>	States           0/0 B           0/0 B           0/0 B	to Chang Protocol * * IPv4 *	e Order) Source RFC 1918 networks Reserved Not assigned by IANA WAN2 net	Port * *	Destination * * * * *	Port * *	Gateway * * *	Queue * * none	Schedule	Description Block private networks Block bogon networks internet	Actions Actions

Configuración Reglas en la interfaz WAN2

Figura 41: Reglas WAN2 Elaborado por Carlos Orrala

## Configuración Reglas en la interfaz RED PUBLICA

Firewall	/ Rules	s / RED_	PUBLIC	A							≑ ਘ 🗉 0
Floating	WAN	LAN	WAN2	RED_P	UBLICA AD	MINISTRACION	SERVIDOR	RWEB			
Rules (Dr	agto C	hange O	rder)								
]	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X	0/0 B	IPv4 TCP	*	*	This Firewall	puerto_pfsense	*	none		Bloqueo de Interfazpfsense	₺∥₽०₸
	0.000	TD-4 8				*	halancan	0000		internet	

Figura 42: Reglas RED\_PUBLICA Elaborado por Carlos Orrala
Firewal	II / Rules	/ ADMINI	STRACION							ŧ	E 💷 🗐 🕼
Floating	WAN	LAN WAN	12 RED_PUBLICA	ADM	INISTRACION SERVI	DORWEB					
Rules (D	)rag to Cl	hange Orde	n								
]	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
] <b>∕≎</b>	0 /0 B	IPv4 TCP/UDP	ż	*	192.168.11.253	8080	WANGW1	none		mikrotik	⊕∥Ω⊘ ≣
] 🗸 🗄	5 / 27.27 MiB	IPv4 TCP/UDP	ADMINISTRACION net	*	ADMINISTRACION address	3128	*	none		proxy	&∥ΩО ≣
] <b>∕≎</b>	0 /0 B	IPv4 *	ż	*	2	2	preferenciawl	none		internet	€∥₽₽
] ×≘	0 /456 B	IPv4 TCP	*	*	ż	*	*	none		denegar todo	<b>∛</b> ∕⊡⊘

Configuración Reglas en la interfaz ADMINISTRACIÓN

Figura 43: Reglas ADMINISTRACION Elaborado por Carlos Orrala

# Configuración Reglas en la interfaz SERVIDOR WEB

Firewall /	Rules	/ SERVIDO	RWEB								≑ ਘ 🗉 😡
Floating	WAN	LAN WAN	2 RED.	PUBLICA	ADMINIST	RACION SERV	DORWEB				
Rules (Dra	g to Cł	nange Order	0								
Rules (Dr	g to Ch States	nange Order Protocol	) Source	Port	Destination	Port	Gateway	Queue S	chedule	Description	Actions
Rules (Dra	g to Ch States 0/0B	Protocol IPv4 TCP/UDP	Source	Port *	Destination This Firewall	Port puerto_pfsense	Gateway	Queue S	chedule	Description bloqueopfsense	Actions
Rules (Dra	g to Ch States 0/0B 0/0B	Protocol IPv4 TCP/UDP IPv4 ICMP any.	Source * *	Port * *	Destination This Firewall	Port puerto_pfsense *	Gateway *	Queue S none none	chedule	Description bloqueopfsense denegar ping	Actions ♣✔₽⊘亩 ♣✔₽⊘亩
Rules (Dra	g to Ch States 0/0B 0/0B 0/0B	Protocol IPv4 TCP/UDP IPv4 ICMP <u>any</u> IPv4 TCP	Source * * * *	Port * *	Destination This Firewall *	Port puerto_pfsense * 22 (SSH)	Gateway * *	Queue S none none none	chedule	Description bloqueopfsense denegar ping ssh	Actions ♣ I O m ♣ I O m ♣ I O m

Figura 44: Reglas SERVERWEB Elaborado por Carlos Orrala

## 3.5.4 CONFIGURACION DEL SQUID PROXY DE LA RED ADMINISTRACIÓN

A continuamos ingresamos al Menú $\rightarrow$  System $\rightarrow$  Package Manager $\rightarrow$  Available Packages una vez aquí nos ubicamos en el buscador y escribimos Squid y SquidGuard si nos aparecerá los paquetes de instalación e instalamos al finalizar nos dirigimos a Installed Packages en donde visualizaremos los paquetes y las características.

-	istalled P	ackages			
	Name	Category	Version	Description	Action
~	acme	security	0.7.3	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies:	âね)
~	squid	*****	0.4.45_9	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies:	前は
~	squidGuard		1.16.18_20	High performance web proxy URL filter. Package Dependencies: ∲ squidguard-1.4.15 ∲ pfSense-pkg-squid-0.4.45_9	≣₽₽

Figura 45: Instalación de los paquetes Squid y SquidGuard Elaborado por Carlos Orrala

Acedemos al Menú $\rightarrow$  Services  $\rightarrow$  Squid Proxy Server $\rightarrow$  General, habilitamos el Squid Proxy, en interfaz destino que va dirigido hacia Administración, su puerto por defecto 3128.

Package / Proxy Ser	ver: General Settings / General	C°⊙ ፰ ਘ ₪ 0
General Remote Cache	Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync	
Squid General Settings		
Enable Squid Proxy	Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.	
Keep Settings/Data	If enabled, the settings, legs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.	
Listen IP Version	□Py4 ✓ Select the IP version Squid will use to select addresses for accepting client connections.	
CARP Status VIP	none  Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.	
Proxy Interface(s)	LAN WAN2 RED_PUBLICA ADMINISTRACION The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.	
Outgoing Network Interface	Default (auto)   The interface the proxy server will use for outgoing connections.	
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128	

Figura 46: Configuración general Proxy Server parte 1

#### Elaborado por Carlos Orrala

Transparent HTTP Proxy	Enable transparent mode to forward all requests for destination port 80 to the proxy server.
	Transparent proxy mode works without any additional configuration being necessary on clients. Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)	LAN WAN2 RED_PUBLICA ADMINISTRACION
	The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces

Figura 47:Configuración Proxy Server parte 2 Elaborado por Carlos Orrala

Buscamos Logging Settings y realizamos la siguiente configuración habilitamos el registro de acceso y escribimos el directorio en donde se almacenará /var/squid/logs finalmente guardamos los cambios para habilitar el servicio.

Logging Settings	
Enable Access Logging	This will enable the access log.
	Warning: Do NOT enable if available disk space is low.
Log Store Directory	/var/squid/logs
	The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	
	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by	✓ Makes it possible for SquidGuard denied log to be included on Squid logs.
SquidGuard	Click Info for detailed instructions.

Figura 48:Configuración general Proxy Server parte 3 Elaborado por Carlos Orrala.

## **Configuración SquidGuard Proxy Filter**

Acedemos al Menú $\rightarrow$  Services  $\rightarrow$  SquidGuard Proxy Filter  $\rightarrow$  General no activamos aun el servicio $\rightarrow$  nos dirigimos a Logging options y activamos los siguientes parámetros $\rightarrow$ una vez activado Blacklist pegamos la siguiente URL <u>http://dsi.ut-</u> capitole.fr/blacklists/download/blacklists for pfsense.tar.gz y guardamos cambios.



Figura 49: Configuración SquidGuard Proxy Filter parte1 Elaborado por Carlos Orrala.

Logging option	15
Enable GUI log	Check this option to log the access to the Proxy Filter GUI.
Enable log	Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation	Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous	
Clean Advertising	Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
Blacklist option	ns
Blacklist	Check this option to enable blacklist
Blacklist proxy	
	Blacklist upload proxy - enter here, or leave blank. Format: host[port login:pass] . Default proxy port 1080. Example: '192.168.0.1:8080 user:pass'
Blacklist URL	http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
	Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Figura 50: Configuración SquidGuard Proxy Filter parte2 Elaborado por Carlos Orrala.

Accedemos a Target categories para poder crear los filtros y agregamos, para esto tendremos 2 filtros que son: Bloqueadas y Permitidas

Proxy filter S	SquidGuard: 1	farget categ	jories / Edit /	Target c	ategories			•
Seneral settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	
(MLRPC Sync								
eneral Optio	ns							
Name	bloqueadas							
	Enter a unique n The name must	ame of this rule h consist between 2	ere. and 15 symbols [a-Z_0	)-9]. The first	one must be a	a letter.		
Order								
	Select the new p from the top do	osition for this tar wn in sequence.	get category. Target cate	egories are lis	sted in this ord	er on ACLs an	d are match	e
Domain List	www.youtuk es.pornhuk	pe.com es-la	a.facebook.com xx.com onlyfans	www.xvic .com ins	leos.com	om		
	es.teiegra	am.org rtve	e.es backtracka	cademy.c	om es.ti	.KTOK.COM		

## Figura 51: Domain List Elaborado por Carlos Orrala.

	Example: host.com/xxx 12.10.220.125/alisa	
Regular Expression	livestreaming  facebook   sexo  porno  juegos         desnudos  onlyfnas  crimen  muerte  casino         Enter word fragments of the destination URL To separate them use   Examples mail/rasinolname) roffs	
Redirect mode	(interror page (enter error message)	~
	Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options:ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.	
Redirect	Pagina no permitida	
	Enter the external redirection URL, error message or size (bytes) here.	
Description	Paginas Prohibidas You may enter any description here for your reference.	

Figura 52: Parámetros de Bloqueadas Elaborado por Carlos Orrala.

Package / Proxy filter SquidGuard: Target categories / Target categories         @											
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log				
XMLRPC Sync											
Name	Redirect		Descrip	otion							
bloqueadas	Pagina no p	ermitida	Pagina	s Prohibidas		ø	ii i				
permitidas			permiti	das		Ø 1	iii				
						+	Add				
Save											

Figura 53:Target categories Elaborado por Carlos Orrala.

Una vez ya habilitado el SquidGuard Proxy Filter  $\rightarrow$  Blacklist donde nos aparecerá la URL anterior y descargamos el paquete del filtro.

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync
Blacklist Updat	e							
0.5 http://www.sha	lalist.de/Downloads	/shallalist.tar.gz						
🛓 Download 🧧	Cancel DRest	ore Default						
Enter FTP or HTTP pa	th to the blacklist an	chive here.						
🙁 Blacklist up	date Log							
Begin blacklist	update				]			
Download archiv Download comple	e http://www.shi te	allalist.de/Do	wnloads/shallalis	t.tar.gz				
Unpack archive Scan blacklist	categories.							
Copy DB to work Reconfigure Squ	dir. dir. id proxy.							
Blacklist updat	e complete.							

Figura 54; Descarga de la lista negra Elaborado por Carlos Orrala.

Nos dirigimos Common ACL→ botón +, en donde nos mostrara las categorías creadas anteriormente y la lista negra que hemos descargado en las cuales tenemos 3 categorías como:

- Whitelist: siempre permitida confiable.
- Deny: bloqueada.
- Allow: permitir siempre y cuando no este bloqueada en otra ACL.

En la lista nos aparecerá un sinnúmero de categoría las cuales no va hacer necesario activar todas las ACL, dependiendo podemos ir bloqueando o permitiendo la paginas de acuerdo a lo requerido, no olvidar que cada cambio que realicemos deveras seleccionar el botón aplicar para guardar cambios.

Package / Proxy	filter SquidGuard: Common Access Control List (ACL) / Common ACL	0
General settings Com	nmon ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync	
General Options		
Target Rules	!bloqueadas ^permitidas !blk_blacklists_adult !blk_bl	
	Target Rules List 🕈 🗢	
	ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.	
	Target Categories	
	Paginas Prohibidas (bloqueadas)	access deny 🗸
	permitidas (permitidas)	access whitelist 🗸
	[blk_blacklists_adult]	access deny 🗸 🗸
	[blk_blacklists_agressif]	access V
	[blk_blacklists_arjel]	access ( V)
	[blk_blacklists_associations_religieuses]	access deny 🗸
	[blk_blacklists_astrology]	access V
	[blk_blacklists_audio-video]	access Y
	[blk_blacklists_bank]	access V
	[blk_blacklists_bitcoin]	access V
	[blk_blacklists_blog]	access 🗸
	[blk_blacklists_celebrity]	access V
	[blk_blacklists_chat]	access V

Figura 55: Configuración Common ACL Elaborado por Carlos Orrala

Una vez ya habilitado para comprobar que el servicio Squid Proxy y SquidGuard Proxy Filter este activo acedemos al Menú $\rightarrow$  Status  $\rightarrow$  Services en donde encontraremos la tabla de servicios activos.

WARNING: 1	WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.							
Status /	Services		0					
Services								
Service	Description	Status	Actions					
c-icap	ICAP Interface for Squid and ClamAV integration	0	C' 💿					
clamd	ClamAV Antivirus	<b>Ø</b>	C 💿					
dhcpd	DHCP Service	0	C® ≢ш⊟					
dpinger	Gateway Monitoring Daemon	0	C'⊙ ≢Ш⊟					
squid	Squid Proxy Server Service	0	C					
squidGuard	Proxy server filter Service	0	C' 🔍					
syslogd	System Logger Daemon	<b>Ø</b>	C'® ≢≣					
unbound	DNS Resolver	0	C'® ≢ш⊟					

## Figura 56:Estados de Servicios Elaborado por Carlos Orrala

G facebook - Buscar con Google × + · · ·						
$\leftarrow$ $\rightarrow$ C $\cdot$ O A https://www.google.com/search?client=firefox-b-d&q=facebook	$\bigtriangledown$	එ ≡				
Google facebook × •	٩	,				
Q Todos 🗈 Imágenes 🕩 Videos 🖽 Noticias ◊ Maps 🚦 Más Herramie	entas	_				
Cerca de 25,140,000,000 resultados (0.29 segundos)						
https://es-la.facebook.com *						
Facebook - Inicia sesión o regístrate						
Crea una cuenta o inicia sesión en <b>Facebook</b> . Conéctate con amigos, familiares y otras		Me				
personas que conozias. Compane lotos y videos, envía mensajes y		Red sc				
Iniciar sesión						
Inicia sesion en Facebook para empezar a compartir y						
Iniciar sesión en Facebook						
Inicia sesión en Facebook para empezar a compartir y conectar		redes :				
Inicia sesión o regístrate		Wikipe				
c						

Figura 57: Prueba del SquidGuard Proxy Filter en Administración Elaborado por Carlos Orrala



#### No se puede conectar

Firefox no puede establecer una conexión con el servidor en es-la.facebook.com.

• El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.

Reintentar

- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

Figura	58:Pagina	Facebook	bloquead	a Administración
	Elabo	orado por	Carlos Or	rala

## CONFIGURACIÓN DEL PORTAL CAUTIVO EN MIKROTIK.

Primeramente, nos conectamos a nuestro Winbox e ingresamos con nuestro usuario y contraseña observaremos un menú, nos dirigiremos IP→ Hotspot→ Hotspot Setup el cual nos permitirá crear un servidor hotspot una terminados el parámetro correspondiente.

🗉 🕄 Ajustes	× ConterOS router configuration ( × +	$\sim$		3-) <mark>-×-</mark>
$\leftarrow \  \  \rightarrow \  \  \mathbf{G}$	○ A or 192.168.11.253:8080	☆	ල එ	≡
	Conteros testas	© mikrotik		

Figura 59: Login Mikrotik

😆 🕓 MikroTik - I	Hotspot at	admin@	)1× +						~		- đ	×
$\leftarrow \   \rightarrow \   G$	$\bigcirc $	3 192	.168.11.253	:8080/we	bfig/#IP:Hots	pot		2	22	$\bigtriangledown$	ර =	Ξ
CAPSMAN	Route	rOS v	6.49.6 (stable	e)	Qu	ick Set	WebFi	ig Te	erminal	2		1^
Q Wireless	Server		aver Brefiles	Lisers	Llear Brofiles	Activ	ua Hasta	ID Rinding			atenat	
Interfaces	Servers	s   Sei	rver Profiles	Users	User Profiles	Activ	Ve   Hosts	IP binding:	s	н	JISPOL	
PPP									Servic	e Ports		
💥 Bridge	Walled G	arden	Walled Gar	den IP Lis	t Cookies							
" Mesh												
155 IP 🔻	Add Ne	w Ho	tspot Setup									
ARP												
Accounting	1 item											
Addresses							Address		Add	ress		
DHCP Client			<b>▲</b> Name		Interface	Ē	Pool	Profile	Per	MAC		
DHCP Relay	- D	s	🔒 hotspot1		ether2-lan	c	dhcp_pool0	hsprof2	2			
DHCP Server												
DNS												
Firewall												
Hotspot												
IPsec												
Kid Control												
Neighbors												
Packing												
Pool								_			1.00	0.00
Routes						]		m	hiercoles, 08	de feb	rero de 20	023
😏 🧭 [		0	(1)	9		011		ES 😼	🛱 🛍 ሳ	) 08/	13:44 ′02/2023	

Figura 60: Servidor hotspot 1Creado

## **Hotspot por PIN**

Ladmin	n@MikroTik] >				
Eadmin	n@MikroTik] > ping 8.8.8.8				
SEQ	HOST	SIZE	TTL	TIME	STATUS
Ø	8.8.8	56	115	75ms	
1	8.8.8	56	115	81ms	
2	8.8.8	56	115	83ms	
3	8.8.8	56	115	86ms	
4	8.8.8	56	115	72ms	
5	8.8.8	56	115	76ms	
6	8.8.8	56	115	74ms	
7	8.8.8	56	115	91ms	
8	8.8.8	56	115	82ms	
9	8.8.8	56	115	73ms	
10	8.8.8	56	115	77ms	
11	8.8.8	56	115	64ms	
12	8.8.8	56	115	90ms	

Figura 61: Ping al puerto 8.8.8.8

#### **Configuraciones generales de User Profile**

Nos conectamos a nuestro Winbox e ingresamos con nuestro usuario y contraseña observaremos un menú, nos dirigiremos IP→ Hotspot→ User Profiles esto es un perfil

donde definiéremos atributos en esta ventana encontraremos parámetros necesarios que utilizara nuestros planes como son:

- Name: Este será el identificador del nuestro profile (se recomienda que coloque como identificador el nombre de su plan)
- Address Pool: Pool de direcciones que serán asignadas a los usuarios. El pool debe estar definido en el servidor.
- Session Timeout: Cada cuando se le estará pidiendo el acceso al usuario cuando esté conectado.
- Idele Timeout: período de inactividad para clientes no autorizados. Cuando no hay tráfico desde este cliente (literalmente, la computadora del cliente debe estar apagada), una vez que se alcanza el tiempo de espera, el usuario se elimina de la lista de host de HotSpot, su dirección utilizada está disponible
- Keepalive Timeout: Tiempo que debe pasar el usuario desconectado para que se elimine de la lista de activos
- Status Autoferros: Intervalo de actualización automática de la página de estado de HotSpot.
- Shared Users: Numero de dispositivos que podrán utilizar el usuario
- Rate Limit (rx/tx): rx= velocidad de subida y tx= velocidad de descarga
- Mac Cookie Timeout: Tiempo que estará almacenada la MAC del dispositivo del usuario y así no pedir que ingrese su usuario nuevamente
- Addess List: Se puede agregar los usuarios a una addres list.
- Inconming Filter: Nombre de la cadena de firewall aplicada a los paquetes entrantes de los usuarios de este perfil, se requiere una regla de salto desde la cadena incorporada (entrada, reenvío, salida) a cadena = punto de acceso
- Outgoing Filter: Nombre de la cadena de firewall aplicada a los paquetes salientes de los usuarios de este perfil, se requiere una regla de salto desde la cadena incorporada (entrada, reenvío, salida) a la cadena = punto de acceso
- Incoming Packet Mark: Marca de paquete puesta en paquetes entrantes de cada usuario de este perfil
- Outgoing Packet Mark: Marca de paquete en paquetes salientes de cada usuario de este perfil

- Open Status Page: Opción para mostrar la página de estado para el usuario autenticado con el método de inicio de sesión mac. Por ejemplo, para mostrar publicidad en la página de estado (alogin.html)
- Transparent Proxy: Utilice un proxy HTTP transparente para los usuarios autorizados de este perfil.

$\leftarrow$ $\rightarrow$ (	C 💫 192	.168.11.253:8080/webfig/#IP:Hotspot.User_Profiles.nev 70% ☆ ♡ ♪ Ξ									
CAP5MAN	RouterOS v649.6 (stable)	Quick Set WebFig Terminal 📓 📓 🗖									
🔉 Wireless											
Interfaces		New Hotspot User Profile									
PPP	OK Cancel Apply										
👯 Bridge											
. Mesh	default										
∰ IP ¥											
ARP		General									
Accounting	Name	2M									
Addresses											
DHCP Client	Address Pool	dhcp_pool0 v									
DHCP Relay	Session Timeout	<b>▼</b>									
DHCP Server											
DNS	Idle Timeout	none v									
Firewall	Keepalive Timeout	▲ 01:0:00									
Hotspot											
IPsec	Status Autorefresh	00:01:00									
Kid Control	Shared Users	▲ 1									
Neighbors											
Packing	Rate Limit (rx/tx)	▲ <u>512K/2M</u>									
Pool	Add MAC Cookie										
Routes											
SMB	MAC Cookie Timeout	1d 00:00:00									
SNMP	Address List	•									
SSH											
Services	Incoming Filter	•									
Settings	Outgoing Filter	•									
Socks		V									

Figura 62: Planes o paquetes

Una vez creada los diferentes planes se irán almacenando en nuestro User Profile lo cual podemos hacer pruebas de speedtest desde nuestros equipos o usuarios para la verificación de la velocidad del paquete que fue asignado.

## Crear Users en nuestro hotspot

Una vez creada los diferentes planes se irán almacenando en nuestro User Profile lo cual podemos hacer pruebas de speedtest desde nuestros equipos o usuarios para la verificación de la velocidad del paquete que fue asignado.

Una vez aquí accederemos a ajustes generales para crear los usuarios en donde asignaremos los parámetros de autenticación como son:

- Server: Seleccionamos nuestro servidor creado.
- Name: Nombre del usuario con el que iniciara el login del hotspot
- Password: Contraseña para el login.

👋 🕓 MikroTik	: - New Hotspot User at × +		~ <b>-</b>				
$\leftarrow \  \  \rightarrow \  \  \mathbf{G}$	○ A ⊶ 192.168.11.253:8080/webfig/s	#IP:Hotspot.Users.new 90	%☆ ♡ ☆ ≡				
CAPSMAN	RouterOS v6.49.6 (stable)	Quick Set WebFig	Terminal 📃 📓 ^				
Interfaces			New Hotspot User				
ta ppp Bridge	OK Cancel Apply Reset Counters						
°l; Mesh							
TP Y	Enabled 🔽						
ARP							
Accounting			General				
Addresses	- [						
DHCP Client	Server hotspot1 v						
DHCP Relay	Name 0998812989	1					
DHCP Server		-					
DNS	Password						
Firewall	Address 🔻						
Hotspot							
IPsec	MAC Address 🔻						
Kid Control	Profile default v						
Neighbors							
Packing	Routes 🔻						
Pool	Email 🔻						
Routes							
SMB	WinBox v3.37 (Add	resses)	Limits				
			*				

Figura 63: Usuario Creado

Ya obtenido nuestro usuario y contraseña nos conectaremos a la red del hotel en donde nos pedirá los datos de acceso, una vez iniciado la sección podrá navegar.

Debe iniciar sesión en esta red antes de que pue	da acceder a Internet.	Abrir página de inicio de sesión en la re	d ×
		<b>A</b> FRI •	
	Hotel copaCaba	ana vassword	
		mi	ércoles, 08 de febrero de 20

Figura 64: Login Hotspot

Hola 0998812989!
IP address: 192.168.8.254 bytes up/down: 138.4 KiB / 164.6 KiB connected: 1m11s
status refresh: 1m
desco <del>i)</del> ectar

Figura 65: Detalle de conexión



Figura 66: Usuario con acceso a internet

$\leftarrow \   \rightarrow \   G$	⑦ A ⊶ 192.168.11.253:8080/webfig/#IP:Hotspot.Active 90% ☆ ⑤ ⑤ Ξ								
CAPsMAN	RouterOS v6.49.6 (stable)				Quick Set	WebFig	Termi	nal 📃	
Interfaces	Servers Ser	ver Profiles	Users Use	er Profiles	Active Hosts	IP Binding:	s Service Po	orts Hot	spot
The pop	Walled Garden	Walled Garden IP List Cookies							
💥 Bridge									
" Mesh	1 11-11-11								
IP 🕨	1 item	1 item							
📲 IPv6 🕨 🕨		Server	User	Domain	Address	Uptime	Idle Time	Session Time Left	Rx Rate
OpenFlow	-	🖯 hotspot1	0998812989		192.168.8.253	00:05:51	00:00:01	time tert	7.6

Figura 67: Usuarios Conectados

#### CONCLUSIONES

Se logro definir las segmentaciones para los diversos departamentos que existen en el hotel, mediante el firewall pfsense; además, se implementaron políticas de seguridad para garantizar la confiabilidad y la disponibilidad a la información de la empresa y sus clientes, así como mejorar el servicio de internet.

Se implementaron restricciones para los colaboradores del hotel con la ayuda de los servidores Squid Proxy Server y SquidGuard Proxy, además, se parametrizó la configuración del ancho de banda en el router mikrotik, y el fritado de tráfico malicioso en el firewall pfsense.

Se configuraron paquetes de navegación según el tipo de habitación, con el fin de controlar y optimizar el ancho de banda mediante paquetes que se asigna durante el tiempo de estadía de los huéspedes, garantizando mayor seguridad y conexión.

## RECOMENDACIONES

Realizar un análisis detallado sobre el orden de las reglas dando prioridad de la más alta a la más baja ya que el funcionamiento del firewall es perspectiva vertical de arriba abajo.

Se recomienda mantener actualizados los paquetes de Squid Proxy Server y SquidGuard Proxy para el ahorro de ancho de banda y mantener las restricciones al departamento de administración.

Se recomienda ampliar el ancho de banda contratado con el ISP con el fin de mejorar la velocidad en el servicio de internet.

## BIBLIOGRAFÍA

- J. Barbosa y D. Orjuela, Artists, *Diseño de la red inalambrica wifi para la empresa procibernetica*. [Art]. Universidad Libre, 2010.
- [2 J. Marugán, Artist, Diseño de infraestructura de y soprte informatico para un centro
  ] público de educacion infanti y primaria. [Art]. Universiataria Politécnica de Madrid, 2010.
- [3 J. Moran y J. Falcon, Artists, Implementacion y configuracion de una red lan para mejorar
   ] la conectividad en el laboratorio de desarrollo de software de la Univerdad Técnica de Cotopaxi extensión la Maná periodo octubre 2014-Febrero 2015. [Art]. Universidad Técnica de Cotopaxi, 2016.
- [4 J. E. Álvarez Pinto, «Universidad de Guayaquil. Facultad de Ingeniería Industrial.,» 21
- ] ABRIL 2022. [En línea]. Available: http://repositorio.ug.edu.ec/handle/redug/59969.
- [5 pfSense, «pfSense,» [En línea]. Available: https://www.pfsense.org/getting-started/.
  [Último acceso: 20 04 2021].
- [6 O. Corporation, «VirtualBox,» [En línea]. Available: https://www.virtualbox.org/. [Último] acceso: 20 04 2021].
- [7 Universidad Politécnica de Marid, «DBpedia español,» Creative Commons Attribution] ShareAlike 3.0, [En línea]. Available: https://es.dbpedia.org/page/Portal\_cautivo. [Último acceso: 26 04 2021].
- [8 Edraw by wondershare, «Edraw by wondershare,» EdrawMax ®, All-in-One Software
- ] Diagrama, [En línea]. Available: https://www.edrawsoft.com/ad/edraw-max-softt.html?gclid=Cj0KCQjwppSEBhCGARIsANIs4p4tu\_3ytbAxOrV1HZX1zu2\_PnoPWB04rj TuQ6ulUeqxRj318SYv4fYaAncdEALw\_wcB. [Último acceso: 25 04 2021].
- [9 Red Hat, «Red Hat,» 23 Marzo 2021. [En línea]. Available:
- ] https://www.redhat.com/es/topics/linux/what-is-centos. [Último acceso: Junio 2022].
- [1 Studocu, «Studocu Simuladores de Redes.,» 2021. [En línea]. Available:
- 0] https://www.studocu.com/latam/document/universidad-de-elsalvador/informatica/simuladores-de-redes-informaticas/20048372. [Último acceso: 12 Junio 2022].
- [1 Microsoft, 2022. [En línea]. Available: https://privacy.microsoft.com/es-
- 1] mx/windows10privacy#:~:text=Windows%20es%20un%20sistema%20operativo,el%20tecl ado%20y%20el%20mouse.. [Último acceso: 25 Julio 2022].

mikrotik, «mikrotik,» [En línea]. Available: https://mikrotik.com/software. [Último acceso:
 2] 25 Julio 2022].

- [1 «D-VIEWCAM,» 2022. [En línea]. Available: https://la.dlink.com/la/dviewcam/. [Último
- 3] acceso: 22 Mayo 2022].

- [1 «Macrotics,» 25 Agosto 2021. [En línea]. Available: https://macrotics.com/mikrotik-
- 4] routerboard/. [Último acceso: 22 Mayo 2022].
- [1 «Business Publications Spain,» 19 Junio 2019. [En línea]. Available:
- 5] https://www.redestelecom.es/infraestructuras/noticias/1112681001803/consejos-tener-red-lan-mas-confiable.1.html. [Último acceso: 2 Junio 2022].
- [1 M. d. alineación, Plan Nacional de Desarrollo 2021-2025 Agenda 2030, 2021. [En línea].
- 6] [Último acceso: 18 Mayo 2022].
- [1 V. Juan, «IES Santa Bárbara.,» 2015. [En línea]. Available:
- 7] http://www.iessantabarbara.es/departamentos/tic/4ESO/MWQComunicacion/Tema%20red es%20y%20seguridad.pdf. [Último acceso: 7 Junio 2022].
- [1 Z. Li, «DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA
- 8] PALINDA,» Quito, 2017.

[1 G. Alberto, Protocolos de Interconexión de Redes, Cantabria, 2012.

9]

- [2 R. Rody, «SISTEMA DE CONTROL DE ACCESO PARA LAS PEQUEÑAS Y
- 0] MEDIANAS EMPRESAS. IMPLEMENTACIÓN DE UN PORTAL CAUTIVO,» Guayaquil, 2016.
- [2 J. Casierra, X. Quiñónez, L. Herrera y C. Egas, «Virtualización de Redes y Servidores
- 1] Emulando Infraestructuras Tecnológicas,» *VIRTUALIZACIÓN DE REDES Y SERVIDORES*, vol. III, p. 11, 13 Marzo 2018.
- [2 J. Cuenca, «ResearcGate,» Febrero 2016. [En línea]. Available:
- 2] https://www.researchgate.net/profile/Jackson-Cuenca/publication/295256426\_FIREWALL\_O\_CORTAFUEGOS/links/56c8a7ed08ae96c dd06baf7c/FIREWALL-O-CORTAFUEGOS.pdf. [Último acceso: 2 Junio 2022].
- [2 Pfsense, «Pfsense,» [En línea]. Available: https://www.pfsense.org/getting-started/. [Último
- 3] acceso: 2 Junio 2022].
- [2 L. Caiza Falconi, ESTUDIO COMPARATIVO DE LA IMPLEMENTACIÓN DE UN
- 4] PORTAL CAUTIVO MEDIANTE LAS TECNOLOGÍAS MIKROTIK Y CISCO PARA MEJORAR EL RENDIMIENTO DE UNA RED INALÁMBRICA EN MIPYMES, Riobamba, 2017.
- [2 P. Galarza y D. Pablo, DISEÑO E IMPLEMENTACIÓN DE UN PORTAL CAUTIVO
- 5] UTILIZANDO UN ENRUTADOR INALÁMBRICO DE BAJO COSTO Y UN SISTEMA OPERATIVO DE CÓDIGO ABIERTO., Quito: Quito: Universidad Internacional SEK, 2009.
- [2 J. Ricardor y M. Chérigo, «PORTAL CAUTIVO PARA EMPRESAS PRIVADAS,»
- 6] Panamá, 2017.

- [2 Cloudbeds, «Seguridad hotelera en el mundo digital: cómo prevenir la filtración de datos en
- 7] tu hotel,» Enero 2021. [En línea]. Available: https://www.cloudbeds.com/es/articulos/seguridad-hotelera-en-el-mundo-digital-comoprevenir-la-filtracion-de-datos-en-tu-hotel/. [Último acceso: 3 Junio 2022].
- [2 J. E. Álvares Pinto, «IMPLEMENTACIÓN DE UNA ARQUITECTURA DE RED,COMO
- 8] APORTE A LA GESTIÓN DE SEGURIDAD INFORMÁTICA DEL HOTEL "SAN PABLO" DE LA,» Guayaquil, 2022.
- [2 D. Cabezas, D. Andrade y J. Torres, de *Introducción a la metodología de la investigación*9] *científica*, Sangolquí, Comisión Editorial ESPE, 2018, p. 71.
- [3 F. J. Doorman, La metodología del diagnóstico en el enfoque"investigación adaptativa",0] Heredia, 2002.
- [3 M. Escalada, S. Soto y F. Maria, *El diagnóstico Social Proceso de conocimiento e*
- 1] intervención profesional., Buenos Aires ed., Buenos Aires, 2004.
- [3 C. P. Lagla Gallardo, «Propuesta de rediseño de red de datos de la empresa Cobrafacil
- 2] Fabrasilisa S.A bajo metodología PPDIOO y diseño TOP-DOWN.,» Quito, 2019.
- [3 J. A. Morales Chapman y N. Torres Leiva, «Implementación de una red privada virtual
- basada en la metodología PPDIOO para mejorar la seguridad informática en la red de Lima Traylers S.A.C,» Trujillo, 2021.
- [3 O. Rojas y J. Carlos, «UNIDAD III ESTUDIO DE FACTIBILIDAD,» 2017.[4]
- [3 Digital, «Tesis,» [En línea]. Available:
- 5] http://tesis.uson.mx/digital/tesis/docs/22832/Capitulo3.pdf.

# ANEXOS

## Anexo 1: Formato de la entrevista



# Universidad Estatal Península de Santa ElenaFacultad de Sistemas y Telecomunicaciones

**Objetivo:** Levantar información mediante el método de recolección de entrevista, para contribuir con el servicio de internet que brinda el hotel "Hotel Copacabana".

## Estimado(a) Participante:

El presente documento tiene como propósito recabar información sobre el servicio de internet que ofrece el hotel a sus huéspedes, si es que existe alguna problemática. Consta de una serie de preguntas, al leer cada una de ellas, concentre su debida atención de manera que la respuesta que emita sea fidedigna y confiable.

Es de interés los datos que puedan aportan de forma sincera y la colaboración pueda contribuir a mejorar el servicio de internet que ofrece el hotel.

- 1. ¿Crees usted que el hotel brinda un servicio de internet de calidad a los huéspedes?
- 2. ¿Alguna vez su proveedor de internet a tenido inconveniente para brindar el servicio?
- 3. ¿Ha presentado inconvenientes o quejas de parte de los huéspedes por la caída del servicio de internet, haría para mejorar?
- 4. ¿Si mejoraran el servicio de internet en el establecimiento este ascenderá de forma notoria en el sector turístico?
- 5. ¿Por qué considera usted beneficioso una propuesta de un nuevo diseño de red para aportar a la seguridad informática del hotel?

# Anexo 2: Formato de ficha de observación



# Universidad Estatal Península de Santa ElenaFacultad de Sistemas y Telecomunicaciones

# FORMATO DE FICHA DE OBSERVACION

Nombres del ente privado:	Lugar:					
Hotel Copacabana	Santa Elena - La Libertad					
Periodo sujeto a revisión: 8 horas						
Tipo de observación: Directa	Clasificación de la observación: AR					
Objetivo:						
Exploracion de los posibles problemas que	presenta el establecimiento notelero a					
Causas:						
Falta de implementación de una mejor top	ología de red firewall con sus respectivas					
políticas de seguridad y un maneio adecua	ndo de distribución del tráfico de red para					
brindar un mejor servicio.	nao ao amin'ny fisiana amin'ny fisiana fisiana					
Efectos:						
El establecimiento hotelero tiene vulnerab	ilidad a robo de datos confidenciales que					
llevaría a presentar problema con los clien	tes.					
Recomendaciones:						
Correctivas:	1. ~ 1 1 . 1 1 1 1					
Implementación adecuada de la topologia	y diseno de red mejorando la seguridad de					
na entidad privada a travez de un firewall o	lue nos permitira tener control y ayude a					
mejorar la candad de servicio.						
Preventiva:						
Establecer las políticas de seguridad neces	aria para prevenir robo de información o					
intervención de terceras personas que no pertenecen al establecimiento hotelero.						

## Anexo 3: Manual de instalación de nuestro entorno virtual

## Instalación del firewall Pfsense

Primeramente, debemos descargar la imagen ISO del firewall el cual es gratuito y la podemos encontrar en su sitio web oficial "<u>https://www.pfsense.org/download/</u>", al estar en la página oficial debemos elegir la plataforma que sea compatible con el equipo donde se va a instalar en esta propuesta se usara una arquitectura AMD64(64 bits) y su instalador de imagen de DVD(ISO)

(Figura 68).

y 🛅 😳 👼					I	Buy Cloud   Bu	y Appliance   Supp	oort   Blog
pf sense	Get Started	Cloud	Products	Services	Support	Training	Community	Download
🖺 RELEASE NOTES 👼 SOL	IRCE CODE							
Select Image To Download Version: 2.6.0 Architecture: AMD64 (64-bit) • • Installer: DVD Image (ISO) Install Mirror: Austin, TX USA • Support	er v		Subscri Product inf offers. See Email* Email Addr I underst announceme	ibe To Th formation, pl our newslet ress and I am signin nts, and specia tod in	he Netg fSense softw ter archive f g up to receiv al offers from	ate New ware annour for past anno e the newslette Netgate.*	<b>rsletter</b> incements, and so pouncements.	special
DOWNLOAD  SHA256 Checksum for compressed (.gz) file: 941a68c7f20c4b635447cceda429a027f816bdb78d54b	netgate	<b>9</b> .	pfSense P pfSense P pfSense P TNSR App TNSR on A	Plus Appliances Plus on AWS Plus on Azure pliances AWS	;			

Figura 68: Página Oficial Pfsense

Una vez obtenida la imagen ISO nos dirigimos a la herramienta VirtualBox donde creamos una máquina virtual y creamos un disco dura virtual en el cual nos da por defecto donde estará ubicado nuestro archivo C:\Users\23car\VirtualBox VMs\pfsense\pfsense.vdi, le asignamos un tamaño de memoria que será 2045 MB, que tipo de archivo será VDI (VirtualBox Disk Image) y donde será el almacenamiento de la unidad de disco duro físico es reservado dinámicamente (Figura 69).

				?	$\times$
Crear máquina vi	tual				
Nombre y sistema op	arativo				
Nombre	pfsense				
Carpeta de máquina	C:\Users\23car\VirtualBox VMs				$\sim$
Tipo	Linux			•	-
Versión	Ubuntu (64-bit)				
Tamaño de memoria					
				2048	MB
4 MB			16384 MB		
Disco duro					
🔿 No añadir un dis	o duro virtual				
Crear un disco d	iro virtual ahora				
Usar un archivo	e disco duro virtual existente				
Vado				Ψ.	14

Figura 69: Configuración Máquina Virtual Elaborado por Carlos Orrala

Para la creación de las interfaces de Red, se accede a "Configuración"  $\rightarrow$  "Red" y realizamos las siguientes configuraciones (Figura 70).

General   Sistema   Pantalia   Almacenamiento   Adio   Adio   Red   Partos serie   VISB   Carpetas compartidas   Interfaz de usuario	pfsense - Configur	nción	?	×
Image: Sistema       Adaptador 1       Adaptador 2       Adaptador 3       Adaptador 4         Pantalia       Image: Sistema       Ima	General	Red		
	General General Sistema Pantalla Almacenamien Audio Red VIS8 Carpetas comp Interfaz de usu	Red       Adaptador 1       Adaptador 2       Adaptador 3       Adaptador 4       Image: State in the state in		

Figura 70: Configuración de red de la Máquina Virtual Pfsense

Elaborado por Carlos Orrala

Una vez creada la máquina virtual pulsamos en "Configuración" nos aparecerá una ventana el cual podremos modificar los ajustes de la máquina virtual y nos dirigimos "Almacenamiento" donde agregamos una unidad óptica que nos ayudará a dar el inicio el cual era la ISO pfSense-CE-2.5.1-RELEASE-amd64.iso (617,20 MB) (Figura 71).



Figura 71: Configuración de almacenamiento de Máquina Virtual Pfsense Elaborado por Carlos Orrala

Ya terminado las configuraciones iniciamos la máquina virtual, donde aparecerá el menú de instalación del firewall donde seleccionamos la opción "Install Pfsense" (Figura 72).

Install				·····]
Rescue Shell Recover config.x	Install p Launch a Becover o	<mark>fSense</mark> shell for rescue config.xml from a	operations previous instal	1
	<mark>( )</mark> ( )	<cancel></cancel>		

Figura 72: Configuración de instalación Pfsense Elaborado por Carlos Orrala

Una vez terminado el proceso de instalación del software Pfsense retiramos la imagen ISO desde VirtualBox y reiniciamos la máquina virtual, nos aparece el menú de configuración de Pfsense desde la terminal (Figura 73).



Figura 73: Opciones de configuración Pfsense Elaborado por Carlos Orrala

## Instalación Mikrotik Routeros

Primeramente, debemos descargar la imagen VDI del Cloud Hosted Router el cual es gratuito y la podemos encontrar en su sitio web oficial "<u>https://mikrotik.com/download</u>", al estar en la página oficial debemos elegir la plataforma que sea compatible con el equipo donde se va a instalar en esta propuesta se usara Cloud Hosted Router 6.49.6 Stable y su instalador de imagen de VDI(ISO) (Figura 74).

🕅 Μικγοτικ		Home About	Buy Jobs Hardware S	Software Support Training Accour	ıt
Software		Downloads	Changelogs Download archive	RouterOS The Dude Mobile apps	
	6.48.6 Long-term	6.49.6 Stable	7.4.1 Stable	7.5rc1 Testing	
Images	vmdk, vhdx, vdi, ova, img				
Main package	Ē				
VHDX image	B				
VMDK image	B				
VDI image	Ē			E	
VirtualPC image	B				
OVA template	B	Ē			
Raw disk image		Ē			
Extra packages					
The Dude client	B				
Changelog	I	I	1 === 1 ===		
Checksum		~			

#### Figura 74: Página Oficial Mikrotik

Una vez obtenida la imagen ISO nos dirigimos a la herramienta VirtualBox donde creamos una máquina virtual y creamos un disco dura virtual en el cual nos da por defecto donde estará ubicado nuestro archivo C:\Users\23car\VirtualBox VMs\MIKROTIK\MIKROTIK.vdi, le asignamos un tamaño de memoria que será 2074 MB, que tipo de archivo será VDI (VirtualBox Disk Image) y donde será el almacenamiento de la unidad de disco duro físico es reservado dinámicamente (Figura 75).

n		2 🗸
а		1 ~
n Ól	🔶 Crear máquina vi	rtual
n	Nombre y siste	ma operativo
•	Seleccione un nombr virtual y seleccione el ella. El nombre que s máquina.	e descriptivo y una carpeta destino para la nueva máquina tipo de sistema operativo que tiene intención de instalar en eleccione será usado por VirtualBox para identificar esta
	Nombre:	MIKROTIK
	Carpeta de máquina:	📒 C:\Users\23car\VirtualBox VMs 🗸 🗸
	Tipo:	Other 🔹 🚺
1	Versión:	Other/Unknown
s		

Figura 75: Configuración Máquina Virtual Mikrotik Elaborado por Carlos Orrala

Una vez creadas la máquina virtual pulsamos en "Configuración" nos aparecerá una ventana el cual podremos modificar los ajustes de la máquina virtual y nos dirigimos "Almacenamiento" donde agregamos una unidad óptica que nos ayudará a dar el inicio el cual era la ISO Mikrotik.6.49.6 (Figura 76).

Θ м	IKROTIK - Configuración				?	×
	General	Almacenamiento				
	Sistema	Dispositivos de almacenamiento	Atributos	Inc		
	Pantalla	Controlador: IDE	Tipo:	PIIX4		-
$\bigcirc$	Almacenamiento	Vacío		Usar cache de I/O anfitrio	in	
	Audio					
-	Red					
	Puertos serie					
	USB					
	Carpetas compartidas					
-	Interfaz de usuario					
				Aceptar	Cano	elar

Figura 76: Configuración de almacenamiento de Máquina Virtual Mikrotik Elaborador por Carlos Orrala

Una vez terminado el proceso de instalación del software RouterOS retiramos la imagen ISO desde VirtualBox y reiniciamos la máquina virtual, nos aparece en la terminal el cual nos pide el login: admin y contraseña: enter <u>(Figura 77)</u>.

Sictoma						_	
MIKROTIK [Cori	riendo] - Oracle	VM VirtualBox			_		×
Archivo Máquina	Ver Entrada	Dispositivos	Ayuda				
MikroTik 6.49.6 MikroTik Login: Password:	(stable) admin						
ммм ммм	ννν					עעע	
мммм мммм	ккк					KKK	
ммм мммм ммм	III KKK K	KK RRRRRR	000000	TTT	III	ККК ККК	
MMM MM MMM	III KKKKK	RRR RRR	000 000	ТТТ	III	KKKKK	
ммм ммм	III KKK KK	K RRRRRR	000 000	ТТТ	III	KKK KKK	
MMM MMM	III KKK K	KK RRR RRR	000000	ТТТ	ΙΙΙ	ккк ккк	
MikroTik Route	rOS 6.49.6	(c) 1999-202	2 ht	tp://www.mik	rotik	.com/	
Do you want to s	ee the soft	are license	? [Yzn]:				
			No 🕅 📑	∕∕□□₽₽₽		CTRL DERE	CHA

Figura 77: Terminal Mikrotik Elaborado por Carlos Orrala

**Instalación de máquinas con windows 7 (Administración, Recepción, Cliente)** Primeramente, debemos descargar la imagen ISO Windows el cual es gratuito y la podemos encontrar en su sitio web oficial "<u>https://www.microsoft.com/es-es/software-download/windows10ISO</u>", al estar en la página oficial debemos elegir la plataforma que sea compatible con el equipo donde se va a instalar en esta propuesta se usara Windows 10(64 bits) y su instalador de imagen de (ISO) ().

Microsoft Descarga de software Mindows V Windows Insider Preview V	Todo Microsoft U Buscar O CARLOS (B) Buscar en Microsoft.com
Descargar imagen de disco de Windows 10 (archi Antes de actualizar, consulta el <b>estado de la información de la versión de Windows</b> para sab que no afecta a tu dispositivo.	IVO ISO) er si hay algún problema conocido y confirmar
Antes de empezar  Descargas  Haz clic en uno de los siguientes vínculos para iniciar la descarga. Si no estás seguro de cuál elegir, consulta las preguntas frecuentes.	
Windows 10 Español 64-bit Descargar 32-bit Descargar	

Figura 78: Página Oficial Microsoft

Una vez obtenida la imagen ISO nos dirigimos a la herramienta VirtualBox donde creamos dos máquinas virtuales que serán para Administración <u>Figura 79</u>, Piso 1 Cliente <u>Figura 80</u> y creamos un disco dura virtual en el cual nos da por defecto donde estará ubicado nuestro archivo C:\Users\23car\VirtualBox VMs, le asignamos un tamaño de memoria que será 2048 MB, que tipo de archivo será VDI (VirtualBox Disk Image) y donde será el almacenamiento de la unidad de disco duro físico es reservado dinámicamente.

🗁 Crear máquina vi	irtual
Nombre y siste	ema operativo
Seleccione un nombre virtual y seleccione el ella. El nombre que s máquina.	e descriptivo y una carpeta destino para la nueva máquina l tipo de sistema operativo que tiene intención de instalar er eleccione será usado por VirtualBox para identificar esta
Nombre:	Administracion
Carpeta de máquina:	C:\Users\23car\VirtualBox VMs
	Microsoft Windows
Tipo:	
Tipo: Versión:	Windows 10 (64-bit)
Tipo: Versión:	Windows 10 (64-bit)
Tipo: Versión:	Windows 10 (64-bit)

Figura 79: Configuración Máquina Virtual Administración Elaborado por Carlos Orrala

		?	$\times$
<ul> <li>Crear máquina vi</li> </ul>	tual		
Nombre y siste	ma operativo		
Seleccione un nombro virtual y seleccione el ella. El nombre que s máquina.	descriptivo y una carpeta destino para la n tipo de sistema operativo que tiene intenció leccione será usado por VirtualBox para ide	ueva mác n de insta ntificar e	quina alar en sta
Nombre:	Piso1 - Cliente		
Carpeta de máquina:	C:\Users\23car\VirtualBox VMs		~
Tipo:	Microsoft Windows	•	64
Versión:	Windows 10 (64-bit)	•	10
	Modo experto Next	Can	relar
	Modo experto Next	Can	Leiai

Figura 80: Configuración Máquina Virtual Piso 1 Cliente Elaborado por Carlos Orrala

Una vez creada las dos máquinas virtuales pulsamos en "Configuración" nos aparecerá una ventana el cual podremos modificar los ajustes de la máquina virtual y nos dirigimos "Almacenamiento" donde agregamos una unidad óptica que nos ayudará a dar el inicio el cual era la ISO Windows.64 bit (Figura 81).

General	Almacenamiento	
<ul> <li>General</li> <li>Sistema</li> <li>Pantalla</li> <li>Almacenamiento</li> <li>Audio</li> <li>Red</li> <li>Puertos serie</li> <li>USB</li> <li>Carpetas compartidas</li> <li>Interfaz de usuario</li> </ul>	Dispositivos de almacenamiento	Atributos Unidad óptica: Puerto SATA 1 CD/DVD vivo Conectable en caliente Información Tipo: Imagen Tamaño: 4,27 GB Ubicación: C:\Users\23car\Downloads\Windows Conectado a:
	s (* 1997)	Aceptar Cancelar

Figura 81: Configuración de almacenamiento de Máquina Virtual Piso 1 Cliente Elaborado por Carlos Orrala

Iniciamos el proceso de instalación de Windows, nos aparecerá un botón de instalar ahora el cual realizaremos clic y seguiremos el proceso de instalación <u>(</u>Figura 82<u>)</u>



Figura 82: Instalación de Windows Elaborador por Carlos Orrala

Una vez terminado el proceso de instalación del software Windows retiramos la imagen ISO desde VirtualBox y reiniciamos la máquina virtual, nos aparece el escritorio (Figura 83).



Figura 83: Escritorio de Windows Elaborado por Carlos Orrala