



UNIVERSIDAD AUTÓNOMA DEL  
ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

---

**SSH, Firewall y VPN como sistema de  
seguridad de red en una placa Raspberry Pi 3  
Modelo B+ para una red de sensores**

---

TESIS

PARA OBTENER EL GRADO DE  
**INGENIERÍA EN REDES**

PRESENTA

**ALFREDO ANTONIO AGUILAR CRISTO**

DIRECTOR DE TESIS

**JOSÉ ANTONIO LEÓN BORGES**

ASESORES

**Dr. David Ernesto Troncoso Romero**

**Dr. Homero Toral Cruz**

**Dr. Julio César Ramírez Pacheco**

**Dr. Ismael Osuna Galán**



CANCÚN QUINTANA ROO, MÉXICO, SEPTIEMBRE DE 2023



UNIVERSIDAD AUTÓNOMA DEL  
ESTADO DE QUINTANA ROO

## DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

Tesis elaborada bajo la supervisión del Comité de Tesis del  
programa de licenciatura y aprobada como requisito para  
obtener el grado de:

# INGENIERÍA EN REDES

### COMITÉ DE TESIS

Director: Dr. José Antonio León Borges

Asesor: Dr. David Ernesto Troncoso Romero

Asesor: Dr. Homero Total Cruz

Asesor: Dr. Julio César Ramírez Pacheco

Asesor: Dr. Ismael Osuna Galán



## **Dedicatoria**

Esta tesis va dedicada a las personas más importantes de mi vida; a mis padres, que con bastante esfuerzo, dedicación y tiempo me han apoyado para llegar hasta estas instancias y emocionalmente me inspiraron a ser una persona mejor, gracias a la formación de ambos, hoy en día esos conocimientos y valores se han convertido en los impulsos para poder construir este momento paso a paso y poder lograr el objetivo; quiero agradecer a mis amigos, que a pesar de todos los buenos y malos momentos, han estado ahí como amistades incondicionales y a toda mi familia que ha estado motivándome para seguir creciendo personalmente, también va con dedicatoria hasta el cielo para mis familiares y amigos que se convirtieron en familia de igual forma y que ya no están físicamente conmigo pero que me motivaron durante todo el proceso y lamentablemente no podrán estar a mi lado para poder darles las gracias por sus palabras y sus consejos. Por último, darle gracias a dios por permitirme darme salud y tener fe y esperanza de que todo se puede en esta vida. Alfredo, cada vez que leas esto siéntete orgulloso de lo que has logrado y de lo que eres capaz de hacer a futuro, nunca te rindas.

## **Agradecimientos**

Quiero expresar mis agradecimientos a todo el personal académico que forma parte de la Universidad Autónoma del Estado de Quintana Roo, por darme la oportunidad de crecer y formarme durante toda la estadía dentro de la institución. Después, agradecer a cada una de las personas que han entrado en mi vida y me han motivado y apoyado para cumplir cada reto que la vida me pone. Por último, agradecer a todos los profesores que participaron en mi educación desde que inicie mi etapa estudiantil, agradecer porque han sido mis guías hacia el conocimiento y aprendizaje para poder lograr este objetivo. En general agradecer a todos por apoyarme y motivarme para poder cumplir satisfactoriamente este gran logro en esta etapa de mi vida.

## Resumen

Hoy en día se ha incrementado el avance tecnológico y con ello las personas y empresas usan la tecnología para sus diferentes propósitos. Una de esas tecnologías es aquella relacionada con el constante envío y almacenamiento de datos a través de internet. Esto es algo común entre los usuarios, ya sea individualmente o de forma corporativa. Debido a la constante circulación de información, se han detectado casos de robos de datos confidenciales de personas y/o empresas que son vulnerables en cuanto a su seguridad de datos a través de la red.

El proyecto presentado en este documento es la configuración de seguridad de red con firewall mediante una tarjeta Raspberry Pi. Esta tarjeta estará conectada a una red de sensores de cuerpos de agua, con el fin de que se puedan gestionar y compartir los datos obtenidos y almacenados en la aplicación web de forma segura. Es decir, la finalidad es que se tenga una mayor seguridad y control de acceso de usuarios al momento de consultar la información y evitar el robo de datos de la red. Este trabajo aborda los conceptos básicos de configuración de una tarjeta Raspberry Pi, protocolos de seguridad de red para la ciberseguridad de datos y también aborda el desarrollo de la seguridad de la red en el prototipo.

**Palabras Clave:** Raspberry pi, Firewall, SSH, Control de acceso, Direccionamiento, ciberseguridad.

## **Abstract**

Nowadays, technological progress has increased and with it, people and companies use technology for their different purposes. One of these technologies is that related to the constant sending and storage of data through the Internet. This is common among users, either individually or corporately. Due to the constant circulation of information, cases of theft of confidential data from people and/or companies that are vulnerable in terms of their data security through the network have been detected.

The project presented in this document is the network security configuration with firewall using a Raspberry Pi card. This card is connected to a network of water body sensors, so that the data obtained and stored in the web application can be managed and shared safely. In other words, the purpose is to have greater security and user access control when consulting information and to avoid network data theft. This work addresses the basics of configuring a Raspberry Pi card, network security protocols for data cybersecurity, and also addresses the development of network security in the prototype.

## Contenido

<b>Resumen</b> .....	<b>4</b>
<b>Abstract</b> .....	<b>5</b>
<b>Introducción</b> .....	<b>10</b>
<b>Antecedentes</b> .....	<b>11</b>
<b>Capítulo I. Planteamiento del Problema</b> .....	<b>14</b>
1.1 Problemática.....	14
1.1.1 Amenazas de la Raspberry .....	14
1.1.2 Vulnerabilidades de la Raspberry Pi 3 B+.....	15
1.2. Objetivos .....	16
1.2.1. Objetivo General.....	16
1.2.2. Objetivos Específicos .....	16
1.3 Alcances y limitaciones.....	17
1.3.1 Alcances.....	17
1.3.2 Limitaciones .....	17
1.4 Viabilidad .....	18
1.5 Justificación.....	18
<b>Capítulo II. Marco Teórico.</b> .....	<b>20</b>
2.1. Sistema de seguridad de red. ....	20
2.1.1. Funcionamiento. ....	20
2.1.2. ¿Qué es la seguridad en redes? .....	21
2.1.3. Modos de seguridad de red.....	21
2.2. Tipos de seguridad de red.....	22
2.2.1 Firewall.....	22
2.2.2 Firewall proxy.....	23
¿Cómo funciona Firewall Proxy? .....	24
2.2.3 Firewall de inspección activa .....	24
2.2.4 Firewall UTM.....	25
Ventajas de UTM.....	26
2.2.5 Firewall de próxima generación (NGFW).....	26
2.2.6 NGFW centrado en amenazas .....	27
2.3. Control de acceso .....	27

2.3.1 RBAC (Role Based Access Control) .....	28
2.3.2. Tipos de control de acceso más habituales.....	29
2.4. Red de Sensores. ....	30
2.5. Raspberry Pi. ....	31
¿Qué es la Raspberry PI 3 B+.....	31
2.6. Ciberseguridad. ....	32
2.7 SSH.....	32
2.8 VPN.....	33
<b>Capítulo III. Marco Metodológico.....</b>	<b>35</b>
3.1. Enfoque de estudio.....	35
3.2. Diseño de investigación .....	35
<b>Capítulo IV. Marco de desarrollo.....</b>	<b>37</b>
4.1. Requerimientos.....	37
4.1.1 Raspberry Pi 3 modelo B+.....	37
4.1.2 HDMI.....	37
4.1.3 Micro SD .....	38
4.1.4 Raspberry Pi Imager .....	38
4.1.5 Computadora .....	39
4.2 Implementación.....	40
4.2.1 Instalación de Raspbian para Raspberry Pi 3 modelo B+ .....	40
4.3 Configuración.....	43
4.3.1 Configuración de firewall.....	43
4.3.2 Configuración de SSH .....	48
4.3.3 Configuración de VPN .....	58
<b>Capítulo V. Pruebas.....</b>	<b>68</b>
5.1 Prueba VPN.....	68
4.3 Prueba de Firewall.....	77
Conclusiones .....	80
<b>Referencias.....</b>	<b>81</b>



## Índice de Figuras

Figura 1. Componentes de una Raspberry pi 3 Modelo B+.....	37
Figura 2. HDMI estándar .....	38
Figura 3 Sistema Operativo Raspberry Pi Imager .....	39
Figura 4.Computadora Sony Vaio .....	40
Figura 5. Software Raspberry Pi Imager.....	41
Figura 6. Selección de sistema Raspbian.....	41
Figura 7. Selección de la tarjeta SD para instalación de SO.....	42
Figura 8. Escritura de datos en la memoria SD .....	42
Figura 9. Interfaz gráfica de Raspbian al iniciar correctamente .....	43
Figura 10. LXTerminal de Raspbian .....	44
Figura 11. Descarga de actualizaciones con la instrucción sudo apt-get update .....	45
Figura 12. Estado de los puertos activados para firewall.....	46
Figura 13.Activación del servicio de firewall.....	47
Figura 14. interfaz gráfica de firewall en Raspberry .....	47
Figura 15. Configuración gráfica de Raspberry Pi .....	49
Figura 16. Activación del protocolo Secure Shell en la interfaz Gráfica de Raspberry Pi.....	49
Figura 17. Resultado de ingresar el comando sudo raspi-config.....	50
Figura 18. Confirmación de activación del protocolo SSH .....	50
Figura 19. Verificación del funcionamiento de SSH .....	51
Figura 20. Ubicación del número de puerto dentro de la configuración de SSH .....	52
Figura 21. Instrucción de edición de las configuraciones de SSH.....	53
Figura 22. Edición del número de puerto para acceso de SSH de 22 a 42000 .....	53
Figura 23.Consola de Raspberry Pi .....	54
Figura 24.Interfaz de cambio de contraseña de Raspberry Pi para acceso remoto.....	55
Figura 25. Interfaz de putty para conexión remota a Raspberry Pi .....	56
Figura 26. Dirección IP de la tarjeta mediante la instrucción ifconfig .....	56
Figura 27. Conexión remota vía SSH a Raspberry Pi.....	57
Figura 28. Escritura de usuario y contraseña nueva para acceso a Raspberry .....	58
Figura 29. Comprobación de PiVPN .....	59
Figura 30. Mensaje del instalador de PiVPN.....	59
Figura 31. Mensaje del instalador PiVPN.....	60
Figura 32. Selección de interfaz de red para direccionamiento de OpenVPN.....	60
Figura 33. Confirmación de configuración de red de OpenVPN.....	61
Figura 34. Mensaje de selección de usuario. ....	62
Figura 35. Selección de usuario para VPN .....	62
Figura 36. Selección del protocolo OpenVPN para configuración.....	63
Figura 37. Configuración por defecto de OpenVPN .....	63
Figura 38. Carga de configuración de VPN en Raspberry Pi 3 B+ .....	64
Figura 39. Modificación de puerto VPN.....	64
Figura 40. Selección de DNS.....	65
Figura 41. Selección de IP publica para DNS.....	66
Figura 42. Confirmación de clave de autenticación.....	66



Figura 43. Selección de actualizaciones automáticas en PiVPN .....	67
Figura 44. Creación de usuario de VPN en PiVPN .....	68
Figura 45. Fichero de VPN en Raspberry Pi.....	69
Figura 46. Edición fichero VPN .....	69
Figura 47. Configuración rango de red en VPN .....	70
Figura 48. OpenVPN descargado desde Windows. ....	71
Figura 49. Importación de configuración a cliente VPN .....	72
Figura 50. Acceso a OpenVPN de Raspberry Pi .....	72
Figura 51. Comprobación de conectividad de VPN en Windows. ....	73
Figura 52. Comprobación de la implementación de VPN desde una computadora cliente.....	73
Figura 53. Instalación del servidor FTP en Raspberry Pi .....	74
Figura 54. Habilitación de escritura de archivos de Raspberry Pi a usuarios.....	75
Figura 55. Muestra del software FileZilla.....	76
Figura 56. Conexión FTP por SSH a Raspberry Pi .....	76
Figura 57. Transferencia de archivos entre Raspberry y Windows de manera remota .....	77
Figura 58. Bloqueo de Youtube.com .....	78
Figura 59. Firewall Funcionando correctamente. ....	78
Figura 60. Verificación de firewall con OpenVPN de Raspberry Pi 3 B+ .....	79

## Índice de Instrucciones

Instrucción 1. Lista de instrucciones para firewall .....	44
Instrucción 2. Actualización para Raspberry Pi.....	45
Instrucción 3. Verificación de firewall .....	46
Instrucción 4. Habilitación de firewall.....	46
Instrucción 5. obtención de interfaz gráfica de firewall .....	47
Instrucción 6. Comando para activar SSH de forma manual.....	49
Instrucción 7. Habilitación de SSH por comandos .....	51
Instrucción 8. Verificación de SSH .....	51
Instrucción 9. Acceso a Configuración de puerto de SSH.....	52
Instrucción 10. Fichero de configuración de puerto de SSH .....	52
Instrucción 11. Cambio de clave de acceso a Raspberry Pi.....	54
Instrucción 12. Comando para saber la dirección IP de Raspberry Pi.....	56
Instrucción 13. Instalación de OpenVPN.....	58
Instrucción 14. Creación de usuario en PiVPN .....	68
Instrucción 15. Instalación del servidor FTP .....	74
Instrucción 16. Comando de reinicio para FTP en Raspberry Pi.....	75
Instrucción 17. Edición del fichero de configuración de firewall.....	77

## Introducción

Actualmente, el estado de Quintana Roo impulsa el desarrollo tecnológico para las empresas públicas y privadas que existen, por lo que se implementaron sistemas de seguridad para proteger información recabada entre estos.

El concepto de ciberseguridad se originó debido al avance tecnológico que compañías y usuarios tuvieron con el manejo de internet para poder proteger sus datos informáticos de malwares o accesos no autorizados que ponga en riesgo su confidencialidad e integridad de su información (kaspersky, 2022).

Hoy en día se cuenta con un sistema de red de sensores para la recopilación de datos de los cuerpos de agua en el estado de Quintana Roo, Pero existe un problema en general de protección de datos, ya que hoy en día se busca un sistema que pueda brindar una garantía de que los datos recabados estén seguros dentro del back end que los investigadores van a usar y usuarios que requieran de esa información almacenada dentro de la red de sensores.

Esto nos lleva a buscar soluciones que nos ayude a brindar seguridad en los datos recabados por la red de sensores de cuerpos de agua y dar alguna solución para dar protección a la información y evitar problemas como el robo de datos. El proyecto busca realizar un prototipo de un sistema de seguridad de red configurado para una Raspberry Pi 3 B+ modelo B+ que está conectada a una red de sensores.

El estudio trata del uso del Microordenador Raspberry Pi 3 modelo B+, para la implementación de un prototipo de seguridad de red a través de su sistema operativo Raspbian, con el objetivo de brindar una mayor seguridad a los datos recabados por la red de sensores.

## Antecedentes

La Raspberry Pi fue creada en febrero del 2012 por la fundación Raspberry Pi, esta tarjeta tenía el objetivo principal de ser usado para dar a conocer y enseñar los conceptos básicos de la computación en las escuelas y las universidades de Reino Unido. Al principio se dieron a conocer dos modelos, el Modelo A y el Modelo B. Poco después de su lanzamiento, se formó una comunidad formada por miles de “amantes de la tecnología” que obtuvieron una Raspberry Pi para a experimentar con proyectos inicialmente por primera vez. Por su bajo precio en el mercado de la tarjeta, se alcanzó una gran popularidad del producto, por su versatilidad y facilidad de poder modificarse para diferentes proyectos y la capacidad de implementar el sistema operativo Linux, un sistema operativo popular por ser de software libre. (Raspberry Pi, 2018)

El significado de la palabra “ciberseguridad” nace a raíz del avance tecnológico de los años, con el propósito u objetivo de que los usuarios de internet y empresas puedan proteger sus sistemas informáticos de alguna anomalía como por ejemplo, ataques maliciosos que comprometan el uso del sistema y se pueda realizar robo de datos importantes para uso indebido, para buscar afectar al usuario u obtener algún beneficio económico (kaspersky, 2022). Su objetivo es proteger y prevenir, de manera que el sistema de seguridad pueda contrarrestar los ataques que se avecinen y al mismo tiempo poder enseñar a los usuarios sobre cómo mantener su información más segura y evitar riesgos.

En la actualidad la ciberseguridad es un requisito muy necesario para empresas públicas y privadas para el monitoreo de la red y la prevención de robo de información hechas por hackers.

A continuación, se describen y presentan distintos trabajos realizados de ciberseguridad implementadas a través de Raspberry Pi en diversos países:

Los ingenieros Jefferson Omar Córdoba Ledesma y Ricardo Alexander Flor Jácome (2018), presentan en su tesis titulada "Prototipo para gestión y monitoreo de la seguridad del laboratorio de científicos", en donde demuestran la implementación de un prototipo de aplicación móvil en el que se controla el acceso a la puerta principal mediante códigos QR, y cuando se abre se recibe una notificación. También es posible ver el interior de la habitación a través de una transmisión de video, en las cuales las computadoras se pueden encender y apagar (Jefferson Omar Córdoba Ledesma, 2018).

Las ingenieras Castro Hernández Pamela Michelle y Moreira Plúas Alenny Libeth (2021) en su tesis "Desarrollo de un prototipo de un sistema de análisis y monitoreo de una red utilizando la herramienta open source snort para identificar las vulnerabilidades de la red y brindar seguridad a las conexiones de los diferentes dispositivos finales con servidor VPN y Raspberry Pi" mencionan que debido al avance continuo de la tecnología y las vulnerabilidades que trae consigo, se ha pensado mucho en la seguridad de los datos en los dispositivos que se conectan a Internet a escala global. Como resultado, tomaron la decisión de presentar un proyecto para monitorear una red empresarial, identificar sus vulnerabilidades y aplicar un servicio de monitoreo VPN con el objetivo de bloquear cualquier intrusión no autorizada o no deseada a la red de la empresa o servicio y prevenir de esta manera el robo de datos.

El trabajo de tesis denominada "Interfaz USB de red para acceso seguro basada en Raspberry Pi" por el autor Raúl Jornet Calomarde (2018) presenta el desarrollo de un dispositivo hardware basado en Raspberry Pi Zero W que sirve de punto de acceso a red y proporcione herramientas en base a la seguridad de la red, como lo son el firewall, control de intrusos, configuración de seguridad inalámbrica y proxies.

Los autores Carate Pilatuña Bryan Ricardo y Pozo Mendoza Diego Francisco Arate (2019) en su trabajo de tesis llamada “Diseño de un sistema de detección de intrusos (NIDS) para una red simulada pymesen GNS3, implementada en un módulo Raspberry Pi portátil” presentan el diseño de un sistema de detección de intrusos (NIDS) para una red simulada en GNS3, implementada en un módulo Raspberry Pi a través de software libre y con una baja inversión con el objetivo de obtener una seguridad de red económica y personalizable para cualquier PYME.

## Capítulo I. Planteamiento del Problema

### 1.1 Problemática

Actualmente, el internet es uno de los medios más usados para la comunicación de las personas, el uso diario permite el envío de información a través de la red y esto ha permitido a hackers adentrarse y hacer robo de datos importantes para las empresas y/o usuarios que mandan datos a través de la red.

#### 1.1.1 Amenazas de la Raspberry

Entre las amenazas más comunes en la actualidad se encuentran:

- 1- Malware y bots: Malware es un término o palabra que en general se usa para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en su dispositivo sin un conocimiento previo. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente. Para esto, existen métodos con dos rasgos definitorios: son comunes y trabajan de manera contradictoria a los intereses de la persona afectada. (Ivan Belcic, 2019).
- 2- Phishing: El phishing está definido como el envío de correos que parecen venir de fuentes comunes de confianza (como bancos, compañías de energía etc.) pero que tienen la intención de robar información confidencial al receptor para robar información importante. (Panda Security, 2015)
- 3- Ataques por Wi-Fi: Según una nueva investigación hecha por la empresa Norton Security (2020), un ataque por wifi consiste en configurar una red Wi-Fi completamente nueva y engañar a los usuarios sin pedir alguna clave para hacer que se conecten a esa red. De esta forma, el propietario de la red puede ver todos los datos

que se envían. Este es comúnmente vista y es demasiado peligrosa para los usuarios que se conectan a cualquier red abierta.

- 4- Spam: Es conocido como los mensajes no solicitados o no autorizados por el remitente, el cual contiene publicidad y son enviados de forma masiva con el fin de perjudicar al receptor de dicho mensaje. (¿Qué Es El SPAM? - Áudea, 2018)
- 5- Robo de información: Este método consiste en obtener la información de un usuario para realizar una suplantación de identidad y hacer uso indebido de la información y datos almacenadas por el usuario (kaspersky, 2022).

### ***1.1.2 Vulnerabilidades de la Raspberry Pi 3 B+***

Uno de los principales puntos débiles de este dispositivo son las aplicaciones de terceros, debido a la inyección de malware que pueda poner en riesgo nuestro dispositivo, todo esto derivado de las descargas de paqueterías, aplicaciones y juegos. El uso frecuente de descargas de fuentes que no sean de confianza puede ocasionar que se descargue un juego o aplicación que esté infectado y dañar el equipo, además de que las aplicaciones y juegos pueden contener vulnerabilidades que el servidor SSH del Raspberry no pueda detectar.

La configuración incorrecta de un servidor dentro de la Raspberry Pi puede ocasionar un ataque informático debido a la falta de contraseñas seguras, esto permite a los hackers tomar el control de acceso de manera remota y realizar un ataque a servidores.

Otro de los puntos en contra de la Raspberry Pi es tener los puertos abiertos, para este caso es recomendable configurar y bloquear los puertos USB de la tarjeta para evitar un posible ataque a través de estos puertos y de esta forma abrir los que se requieran por el usuario.



Con el proyecto de tesis del estudiante Oswaldo Mauricio May Canul (2021) de la Universidad de Quintana Roo campus Cancún llamado “Desarrollo de un prototipo de redes de sensores para monitoreo de cenotes del estado de Quintana Roo implementado en Raspberry Pi 3 B+”, se busca hacer una solución para la protección de datos, mediante un sistema de seguridad que pueda brindar una garantía de que los datos recabados estén seguros dentro del back end que los investigadores van a usar y usuarios que requieran de esa información almacenada dentro de la red de sensores.

Como iniciativa, este proyecto buscar implementar un prototipo de seguridad de red en una tarjeta Raspberry Pi 3 B+ para que prevenga y proteja los datos almacenados dentro de la red de sensores y estén protegidos dentro de ella.

## **1.2. Objetivos**

### ***1.2.1. Objetivo General***

Implementar un prototipo de un sistema de seguridad de red basada en firewall, SSH y VPN con una tarjeta Raspberry Pi 3 modelo B+ para dar seguridad a sensores y datos almacenados en la tarjeta.

### ***1.2.2. Objetivos Específicos***

1. Identificar amenazas que puedan romper la seguridad en Raspberry Pi 3 modelo B+.
2. Definir los riesgos que conlleva la seguridad de la Raspberry Pi.
3. Configurar los protocolos de seguridad como el SSH en la placa Raspberry Pi 3 B+ para protección de datos.
4. Configurar la seguridad de firewall y VPN de una red de sensores implementada en una tarjeta Raspberry pi 3 modelo B+.

5. Implementar pruebas de seguridad en la Raspberry Pi 3 B+ para verificar la seguridad implementada dentro de la tarjeta Raspberry Pi 3 B+.

### **1.3 Alcances y limitaciones**

En este apartado se mencionan los alcances y limitaciones que presenta la realización del presente proyecto.

#### ***1.3.1 Alcances***

Este proyecto de investigación busca crear un prototipo de sistema de seguridad implementado en una tarjeta Raspberry Pi 3 modelo B+, basado en Linux Debian, usando los distintos protocolos de seguridad de red conocidos, para evitar amenazas en el equipo.

- Se implementará la configuración de seguridad de firewall en la tarjeta Raspberry Pi.
- Se configurará la seguridad a través de terminal SSH dentro de la tarjeta Raspberry Pi.
- Se implementará la configuración de una VPN para mayor seguridad en la tarjeta Raspberry Pi.

#### ***1.3.2 Limitaciones***

- La configuración se hará en una tarjeta Raspberry Pi 3 Modelo B+.
- Se realizará únicamente las configuraciones de seguridad dentro de la Raspberry Pi 3 Modelo B+
- Estará implementado en un sistema operativo de Raspberry Pi conocido como Raspbian
- Se aplicarán únicamente protocolos de seguridad de red en la placa Raspberry Pi.

## **1.4 Viabilidad**

Esta tesis es viable debido a que hay acceso al campo de estudio a causa de que el responsable del proyecto estudia en la institución donde se realizan las investigaciones para llevar a cabo la tesis, personalmente, se cuenta con las herramientas y dispositivos para llevar a cabo el trabajo y el tiempo que se requiere para llevar a cabo las investigaciones necesarias y realizar el trabajo.

Dentro del campus universitario, se brinda la oportunidad y el apoyo para desarrollar el proyecto, ya que se proporciona la documentación para su investigación y análisis de la problemática, por lo que se tiene el respaldo y apoyo para la realización de este proyecto.

Además, se brinda el solvento económico por parte de los tutores para gastos como materiales de apoyo, impresiones y apoyo para traslado para poder hacer el proyecto. En cuestión a materiales, se cuenta con una laptop para poder trabajar la parte teórica y práctica del proyecto, así como poder leer y visualizar libros y documentos para elaborar el análisis teórico, se cuenta con la tarjeta Raspberry Pi modelo B para realizar el desarrollo de campo, etc.

## **1.5 Justificación**

El proyecto busca desarrollar un prototipo de ciberseguridad en una placa Raspberry Pi 3 modelo B+ que estará conectado a una red de sensores desarrollado por el estudiante Oswaldo Mauricio May Canul (2021) de la Universidad de Quintana Roo campus Cancún, trabajo donde se obtendrán muestreos en cuerpos de agua para su uso posterior.

Los investigadores de diversas áreas ocupan estas muestras que se encontrarán en una aplicación web para realizar análisis de patrones, de minería de datos, de machine learning, así como otros estudios relacionados a la biotecnología.

En este proyecto, dicho previamente, se busca desarrollar un prototipo de un sistema de seguridad configurada en una placa Raspberry Pi, que estará conectada a una red de sensores de cuerpos de agua, para que brinde a los usuarios garantía de seguridad de sus datos recabados dentro de la red.

Todo esto con el objetivo principal de tener un control para evitar robos de información, y evitar vulnerabilidades en cuestión con el control de acceso de usuarios no deseados que puedan poner en riesgo la información de los investigadores. El desarrollo del trabajo será a través de una placa Raspberry Pi 3 modelo B+ que nos permitirá administrar las configuraciones del desarrollo de la seguridad de la red de sensores desde la tarjeta.

## Capítulo II. Marco Teórico.

### 2.1. Sistema de seguridad de red.

Un sistema de seguridad en red es el conocimiento de la disposición de herramientas para poder disponer de una protección de datos e información que esté almacenada en un computador o sistema. Se le llama de forma genérica “seguridad informática” a todo grupo de herramientas que estén hechas o tengan el objetivo de proteger la información y evitar intrusión de hackers (Stallings, 2004).

La seguridad de red es la que no solo se limita a eliminar virus y evitar a hackers, la seguridad de red abarca los procedimientos a tener para que una empresa y sus trabajadores o usuarios puedan proteger datos confidenciales y de sistemas y enfrentar las amenazas actuales. Los términos de seguridad de información, seguridad informática y de red tienen objetivos comunes como lo son

- Protección de confidencialidad
- Protección de integridad
- Disponibilidad de la información. (Miguel Soriano, 2002)

#### 2.1.1. *Funcionamiento.*

La seguridad informática es el nombre que se le asigna a las herramientas diseñadas para proteger los datos almacenados en un equipo y evitar anomalías de piratas informáticos. El funcionamiento de la seguridad de red es definido por el autor Miguel Soriano (2002) como “proteger los datos y los sistemas de información de algún acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados”. Seguridad en la red es

el nombre que se asigna al conjunto de herramientas que tienen como objetivo proteger los datos durante su envío a través de la red (Miguel Soriano, 2002).

### ***2.1.2. ¿Qué es la seguridad en redes?***

La Escuela de Postgrado de la Universidad Católica San Pablo (Capybara, 2022) hace alusión a la seguridad de redes como “un término amplio que cubre una gran cantidad de tecnologías, dispositivos y procesos. En fácil comprensión, es un conjunto de configuraciones y reglas hechas para poder cuidar la integridad, confidencialidad y acceso a las redes y datos utilizando tecnologías de software y hardware.” Es decir, es el conjunto de instrucciones que se usan para brindar seguridad a un software o hardware. Con esta definición se entiende que la seguridad en redes es todo aquello que nos brindará seguridad en nuestros datos en el uso de internet. (Capybara, 2022)

### ***2.1.3. Modos de seguridad de red***

La Escuela de Postgrado de la Universidad Católica San Pablo nos enlista que existen 3 tipos de controles de redes entre las cuales existe la seguridad física en redes, para comenzar, es aquel compuesto por los dispositivos que están físicamente tangibles y pueden ser configurados, por ejemplo, los routers, switches, el cableado para hacer conexión de dispositivos y más. Otros componentes en seguridad física son las cerraduras y los accesos por medio de biometría.

La seguridad técnica en redes, es aquella que se encarga de proteger la información que está en la red o que esté viajando en internet.

El modo administrativo de la red es aquella basada y constituida en procesos de seguridad y políticas para controlar el comportamiento del usuario, teniendo un procedimiento de cómo se

autentican los usuarios, el cómo acceden y cómo el personal de tecnología de la información (TI) realiza modificación en la red. (Capybara, 2022).

La seguridad informática o ciberseguridad es un término usado para la protección de transacciones financieras, archivos personales, comercios, acuerdos contractuales, entre otros. Es una disciplina que hoy en día es necesaria, obligatoria y crítica que debe ser un componente clave en cualquier tipo de trabajo o proyecto de sistemas de información (Areitio Bertolín, 2008).

## **2.2. Tipos de seguridad de red**

### **2.2.1 Firewall**

El autor Álvaro Alonso González en su trabajo “Implementación de medidas de ciberseguridad en un vehículo conectado” menciona que un cortafuegos, o firewall, es un sistema de seguridad que filtra el flujo de tráfico entrante y saliente de una red en base a unas reglas.(Grado, 2022)

Un Firewall, es un componente informático encargado de denegar acceso no autorizado a un usuario que quiera conectarse a una red que esté conectada a Internet. Este servicio tiene la tarea de monitorear cada uno de los paquetes entrantes y salientes de la red para denegar la llegada de aquellos que no cumplan con los criterios de seguridad, de lo contrario, al cumplir con ciertos criterios, se da un acceso libre a la comunicación a los equipos que si estén reglamentados (SoftwareLab.org, 2018).

Los firewalls funcionan como un dispositivo que vigila todo lo entrante y saliente de un perímetro de la red, y por medio de criterios estipulados, el firewall decide si se permite o niega el acceso de tráfico entrante, lo que da una barrera para las redes externas a la que se encuentra conectada el firewall. (Arcentales & Arcentales, 2020)



Es un servicio que permite el filtrado de información, a través del monitoreo constante en la red, donde con políticas establecidas se toma la decisión de permitir o denegar el tráfico. Para un sistema ya establecido, el firewall es un encargado de proteger a la red local del tráfico externo no deseado y evitar amenazas e intrusiones. (Marín Valencia et al., 2020)

### **2.2.2 Firewall proxy**

Un proxy es uno de los tipos de cortafuegos que tiene la función principal de poder actuar como una puerta conexión entre redes para algún específico uso. Este tipo de firewall da al usuario o sistema funciones adicionales, uno de ellos es el almacenamiento de datos proporcionando de esta forma más seguridad a la red, evitando así las conexiones no autorizadas o que pongan en riesgo a la red. Una de sus desventajas principales es, que, al brindar estos beneficios, puede verse afectada la capacidad de procesamiento y de la admisión de aplicaciones que puede tener. (CISCO, 2016)

El firewall Proxy se considera el más seguro debido a que no da un acceso directo a la red. El servidor de seguridad proxy posee la capacidad de poder analizar todo el paquete de red detalladamente a nivel superficial como son el número de puerto del paquete entrante y su dirección IP. Al realizar esta acción, este firewall da seguridad de que el paquete entrante no contenga algún contenido malicioso. Una desventaja del firewall proxy es que por cada paquete que entra y sale de la red, realiza una conexión adicional, esto puede causar en el sistema un mal rendimiento y puede ser causante de un ataque externo a través de este punto frágil de la red (HP,2021).

Investigaciones hechas por el autor A. Alex, menciona en su artículo web que un firewall Proxy es un sistema de seguridad de red que se encarga de proteger los recursos de la red mediante el filtrado de mensajes en la capa de aplicación. Además, menciona que un firewall

proxy también es llamado como firewall de la aplicación o firewall de puerta de enlace (Alex, 2021).

### ***¿Cómo funciona Firewall Proxy?***

Los firewalls de proxy monitorean el tráfico de la red para los protocolos centrales de Internet, como los protocolos de Capa 7, y deben ejecutarse contra cada tipo de aplicación que admita. Estos incluyen el Sistema de nombres de dominio (DNS), FTP, HTTP, Protocolo de mensajes de control de Internet (ICMP) y Protocolo simple de transferencia de correo (SMTP). (Fortinet, n.d.)

### ***2.2.3 Firewall de inspección activa***

Un firewall de inspección activa, llamado también firewall “tradicional”, accede o deniega el tráfico conforme al estado, el protocolo y el número de puerto. Este firewall, en toda su actividad, se encarga de monitorear la red, desde la apertura de una conexión hasta su cierre. El filtrado se hace de acuerdo con las reglas hechas por el administrador y con el contexto, lo que tiende a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.(CISCO, 2018)

Un firewall tradicional, se encarga de permitir o impedir el tráfico en función del estado, el puerto y protocolo, todo mediante políticas. Este monitorea toda la actividad desde que se origina una conexión de un dispositivo, hasta que finalmente se cierra la conexión. El firewall tradicional, toma las realiza acciones de acuerdo a las normas que sean puestas por el administrador, el cual puede obtener para dar o denegar acceso tomando en cuenta las últimas conexiones hechas al sistema (Sotelo, M. I, 2021).

Firewall de inspección activa, permite o el bloqueo de tráfico en base al estado, puerto y protocolo, realiza la vigilancia de toda la actividad desde el comienzo de la conexión hasta la conclusión. La toma de decisión para el filtrado se rige en base a reglas que define el administrador y el contexto. (Fco. Javier Vazquez Pantaleon, 2022)

Un Firewall de inspección activa o conocido comúnmente como un cortafuego tradicional, es el responsable de supervisar las conexiones de una red desde que se abre la conexión, hasta que se cierra. De esta manera tiene la función principal de permitir o bloquear el tráfico de una red externa analizando los paquetes según el puerto de origen, el protocolo ya sea UDP o TCP y su estado. Las decisiones de filtrado de paquetes se toman en función a las reglas que son implementadas por el administrador de la red y al uso de las últimas conexiones que se hayan hecho en la red (Del, 2020).

#### ***2.2.4 Firewall UTM***

El Firewall UTM es el encargado de poseer un conjunto de soluciones para la seguridad de una red. De esta manera, se permite para el administrador de la red un ahorro económico en la infraestructura de red haciendo de manera más simple la incorporación de servicios mediante distintos dispositivos. Esta se define como un cortafuegos que trabaja a nivel de aplicación pudiendo así ser usados con servicios como un servidor VPN para equipos, antivirus, bloqueo y autorización de contenidos y monitoreo para la prevención de ataques de intrusos (Sanz Marcos, P., 2021).

UTM, es una herramienta de seguridad encargada de bloquear o permitir conexiones. Este tiene la función de proteger al sistema de intrusiones, ataques o amenazas que puedan poner en riesgo la información de un usuario o compañía, su función de filtrado de contenido para bloquear o autorizar accesos dentro del perímetro de la red, detección de spam, entre otros, Su

objetivo principal es la prevención de robo de datos y funciones de protección de malware, todo configurado y gestionado gestionadas por varios dispositivos (Olivo & Lascano, 2020).

### ***Ventajas de UTM***

Entre las ventajas más destacadas del Firewall UTM están como primer punto, que tiene un índice de menor complejidad, el cual significa que, de varios productos de seguridad de Firewall, permite que de todos se haga uno solo más completo. Se caracteriza de igual forma por su fácil instalación, es decir, puede ser trabajado de manera remota para su instalación y configuración sin necesidad de presencia de personal.

UTM cuenta con una automatización de detección de amenazas y vulnerabilidades, con el fin de poder mejorar la seguridad del sistema y de esta forma dar fácil solución a los problemas que se presenten dentro de los filtro del Firewall UTM (Olivo & Lascano, 2020).

### ***2.2.5 Firewall de próxima generación (NGFW)***

Hoy en día, se usa para el tráfico de datos los firewalls de próxima generación en los equipos en una red para poder tener mayor índice de seguridad sobre las amenazas modernas, como ataques en los equipos, malware, virus, spam, entre otros.

Gartner, Inc., define a un firewall de próxima generación como aquel firewall capaz de poder tener seguridad para la prevención de ataques informáticos en la red, en las cual, este firewall caracterizarse de la siguiente manera:

- Debe tener la capacidad de un firewall estándar, por ejemplo, la inspección activa.
- Tener capacidad para prevenir ataques e intrusiones de hackers.

- Reconocer y controlar el acceso de aplicaciones para ver y de esta manera bloquear aplicaciones que pongan en riesgo a la red.
- Técnicas en constante evolución para enfrentar y eliminar las amenazas de seguridad.

Un firewall de próxima generación (NGFW) cumple la función de realizar la inspección de paquetes más completa, inspeccionando más a fondo de las políticas implementadas por el administrador, esto con el fin de dar una inspección a través la capa de aplicación (dispositivos), para así poder prevenir intrusiones y dar seguridad y monitoreo inteligente desde fuera del firewall. (MCM, 2021)

### ***2.2.6 NGFW centrado en amenazas***

Este tipo de firewalls contienen las funcionalidades de un firewall tradicional y brindan trabajos de detección y corrección de amenazas avanzadas. El NGFW centrado en las amenazas, puede realizar acciones como monitorear y detectar actividad sospechosa o evasiva con correlación a conexiones en la red y de esta manera reducir significativamente el tiempo desde la detección hasta la eliminación de la amenaza de seguridad que esta monitoreada de manera continua. Además, se encarga de brindar facilidad a la administración para poder reducir los riesgos con políticas que brinden protección en toda la secuencia del ataque. (CISCO, 2016)

### **2.3. Control de acceso**

Lorena Fernández (2020) mediante la página web de Redes Zone, define a un control de acceso como un método que permite garantizar que los usuarios prueben ser quienes dicen que son, es decir, es una serie de restricciones que se le darán al usuario dependiendo de los datos a los que se quieran acceder mediante un numero de procesos y autorizaciones.

El control de acceso es la parte de un sistema de seguridad que sirve como herramienta importante para el uso del usuario con el sistema, ya que se hace cargo de la interacción entre estos y mediante esta herramienta se puede configurar o dar los accesos a los recursos necesarios de un sistema a los usuarios mediante normas. (Sánchez, M., Jiménez, B., 2022)

El concepto de control de acceso se refiere a una tecnología de seguridad informática diseñado con la capacidad de identificar, autenticar, permitir o negar autorización de acceso a usuarios a áreas de datos no especificadas o no permitidas. Contar con un sistema de control de acceso informático nos dará beneficios y seguridad a nuestro sistema.

El control de acceso a la red es definido como una tecnología que tiene la función de controlar el acceso de los usuarios a la red mediante políticas de seguridad, todo esto mediante la validación de identidad para el correcto cumplimiento de políticas, esto significa que, el usuario que trate de acceder cumpla los requerimientos establecidos por la empresa que implementó las políticas, etc. Además, este método puede dar el control de lo que se puede hacer dentro de la red, dar acceso o bloqueo a contenidos e información a usuarios y que usuarios o equipos serán admitidos en la red. (Daniel, Especialidad en Redes Facultad de Informática Universidad Nacional “Control de Acceso a Redes ” Egresado : Daniel Omar Esmoris Director : Ing . Luis Marron.)

### ***2.3.1 RBAC (Role Based Access Control)***

El control de acceso basado en roles (RBAC) es un estándar que se desarrolló para proporcionar a los usuarios acceso y control. RBAC se compone de dos características clave: RBAC y su especificación funcional.

Entre el conjunto de elementos fundamentales de RBAC existen los usuarios, roles, permisos, operaciones y objetos. Los objetivos de RBAC son los siguientes:

-Dar conocimiento de las características RBAC incluidas en el conjunto estándar e identificar las cualidades clave que debe tener RBAC en todo su sistema.

-Para definir su elaboración funcional, dar un lenguaje preciso y consistente de elementos y funciones (Ruiz, 2007).

El role based access control, cuyas siglas son RBAC, traducida como “control de acceso basado en roles”, es un modelo de seguridad permite dar funciones y autorizaciones en la estructura de una red. Es conocido como “basado en roles” debido por cómo funciona, ya que se distingue de distintos métodos de seguridad por asignar funciones como bloquear, autorizar y dar acceso a cierta información a usuarios que estén en la red. En este modelo, el administrador del sistema le asigna a un usuario un nivel y una categoría de seguridad a cada usuario y actividades o tareas dependiendo de que rol tenga en la red. De esta manera, el sistema operativo se encarga de enlazar automáticamente los niveles y luego concede o deniega el acceso. (IONOS, 2020)

### ***2.3.2. Tipos de control de acceso más habituales***

Los controles de acceso se identifican según sus funciones. Un sistema de control de acceso se caracteriza por sus tres funciones principales:

-La autenticación: Esta función de un control de acceso es la que tiene la función de realizar la identificación de los usuarios o máquinas que soliciten acceso a una conexión a una red.



- La autorización: Al realizar el primer paso, esta segunda función que realiza los requerimientos que contiene la red y de esta forma se toma la decisión de dar o denegar el acceso o conexión al usuario que quiere acceder a la red.

-La trazabilidad: Esta función es la que facilita a la red poder obtener una lista de los usuarios que estén dentro de una red (SPEC, 2022).

Existen otros tipos de control de acceso, tales como los sistemas de acceso autónomos, los cuales necesitan de una memoria para la gestión de los usuarios. Es caracterizado por ser un sistema de seguridad baja y por tener una limitada capacidad.

Por otra parte, existen los sistemas de acceso en red, los cuales son conocidos por usar herramientas tales como los softwares y de esta manera brindar una alta seguridad al sistema de red. Estos pueden ser controlados al mismo tiempo en zonas diferentes de alguna empresa que disponga de seguridad en red para sus datos.(SPEC, 2022)

#### **2.4. Red de Sensores.**

Las redes de sensores son dispositivos autónomos que funcionan de manera en conjunta con el fin de poder obtener cierta información de algún ámbito específico, ya sea del clima o del ambiente. Cada parte de una red de sensores es de bajo costo y por lo general trabaja de forma inalámbrica, teniendo la ventaja de poder contar con un sistema flexible y fácil de instalar de muchas maneras y en grandes cantidades (Tekniker, 2019).

Los sensores de red inalámbrica (WSN- Wireless Sensor Network), son aquellos dispositivos de bajo costo que tienen la capacidad de obtener información de su alrededor, para poder procesarla de forma local y comunicarla a de manera inalámbrica hasta una central de coordinación. Cuentan con nodos, los cuales son una parte de estos que actúan como elementos

de la infraestructura de comunicación, tienen la función de reenviar los mensajes transmitidos por otros nodos más lejanos hacia al centro de control de los nodos para poder procesar la información recopilada (Fernandez Barcell, Manuel, 2008)

## **2.5. Raspberry Pi.**

La página oficial de Raspberry Pi define a su tarjeta como “una computadora de bajo costo y con un tamaño compacto, del porte de una tarjeta de crédito, puede ser conectada a un monitor de computador o un TV, y usarse con un mouse y teclado estándar” (2018).

La definición de una Raspberry Pi indica que es una computadora pequeña con Linux capaz de permitir computación. Esta tarjeta nos brinda el hacer la mayoría de las tareas que normalmente se realizan desde una computadora normal, desde navegar en internet, realizar documentos informáticos, hasta reproducir videojuegos. Entonces, ¿Qué es Raspberry Pi 3 B+?

### ***¿Qué es la Raspberry PI 3 B+?***

La Raspberry Pi 3 Modelo B+ es la Raspberry Pi de tercera generación es una computadora de bajo costo de tamaño pequeño como una tarjeta, la cual da la posibilidad de hacer todo tipo de proyectos de informática, programación, mecatrónica, entre otros. La Raspberry Pi 3 Modelo B+ es una versión más reciente de la primera generación de Raspberry Pi, cuenta con la característica de ser 10 veces más rápido que su antecesora y cuenta con conectividad LAN inalámbrica y Bluetooth, por lo que sus componentes la hacen una tarjeta confiable, ideal y de bajo costo para poder realizar trabajos de potencia. Entre sus usos, la Raspberry Pi puede ser usada como una PC/Laptop de bajo costo, una cámara Web, consola de videojuegos, como Servidor Web y sirve como medio para dar seguridad informática de igual forma. (Rasberrypi, 2018)

## **2.6. Ciberseguridad.**

(Microsoft, 2023) define a la ciberseguridad como seguridad digital, la cual es la práctica de proteger la información digital, dispositivos y activos. Esto incluye información personal, archivos, cuentas, dinero y fotos. Divide a la ciberseguridad en 3 acrónimos: CIA

El acrónimo "CIA" se usa a menudo para representar los tres pilares de la ciberseguridad.

La confidencia, la cual se encarga de mantener oculto y confidencial los datos y dar garantía al usuario de que solo él pueda tener acceso a su información personal. La integridad, que da garantía de que la información no ha sido alterada sin el permiso del usuario y el acceso, que garantiza que se puede tener acceso a la información y sistema cuándo se requiera o necesite (Microsoft, 2023)

La empresa Kaspersky define la ciberseguridad a la tarea que tiene como objetivo brindar seguridad a todo dispositivo tecnológico como computadoras, teléfono y servidores, para poder defenderlos de ataques maliciosos en la red (Kaspersky, 2021).

El Centro Criptológico Nacional de España define a la ciberseguridad como un conjunto de actos que tienen el objetivo de dar seguridad a las redes y equipos que trabajan en conjunto en una empresa o un espacio en específico. Trabaja de manera que detecta y enfrenta amenazas; de esta forma protege la integridad y confidencialidad de la información en riesgo (David Reinares Lara, 2020)

## **2.7 SSH**

El protocolo SSH (Secure Shell) del modelo TCP/IP, es un protocolo que permite crear una conexión remota con la consola de administración de una máquina. El protocolo fue

diseñado para sustituir otros protocolos inseguros como el Telnet o RSH debido que transmitían información sin cifrar. (Velasco, M. A. C., & Serrano, DC, 2021)

Es un protocolo que es usado para el iniciar y poder ejecutar procesos de manera remota. Entre sus principales funciones se encuentra el poder compartir archivos de manera remota entre distintos hosts, hacer login en servidores remotos y ejecutar comandos remotamente. Este protocolo es un reemplazo con mejores opciones que telnet y tiene la ventaja de brindar comunicaciones seguras entre cliente y servidor debido a que sus datos son cifrados (Smaldone, 2004).

El protocolo SSH es un protocolo usado para realizar tareas de administración en servidores remotos, a través de redes. Este protocolo tiene su función siempre bajo una arquitectura de cliente-servidor ya que lleva distintas implicaciones de seguridad con respecto a telnet (Mario Luis Avila Pérez, 2021)

## **2.8 VPN**

Es conocida como un tipo de red la cual sus siglas significan “Virtual Private Network”, su implementación tiene el objetivo poder proporcionar integridad y confidencialidad a los datos a través de esta red. Este tipo de conexión es comúnmente usada para poder acceder remotamente a una empresa (Marchionni, 2011).

“VPN es conocida como una tecnología de red que da acceso a una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, todo esto a través de un procedimiento donde encapsula y encripta de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. A través

de ello, se da el acceso para que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada” (Álvarez Delgado et al., 2014).

La autora Maldonado Alva define a una VPN como “un servicio de red privada que es creado sobre una infraestructura de red pública (en otras palabras, Internet)”. Aclarando que hay dos principales características, en las cuales se encuentra, la virtual y la privada. Una de las principales razones del uso de VPN es por su economía, ya que es una opción a la conectividad a través de líneas dedicadas (Alva Maldonado, 2013).

Es una tecnología que puede ser generalmente usado para estudiantes o asuntos de administración. Además, a través de la VPN se puede hacer una conexión remota a algún lugar a través de una red pública que es internet. Una de las grandes ventajas de este tipo de arquitectura es la confidencia e integridad de la información, transmite datos de manera cifrada por un canal, brindado de esta manera una mayor seguridad a la información.(Marín Valencia et al., 2020).

## **Capítulo III. Marco Metodológico**

### **3.1. Enfoque de estudio**

El presente será diseñado bajo el planteamiento metodológico del enfoque mixto, debido a que este enfoque es el que mejor se adapta a las características y necesidades de la investigación realizada.

Esto surge por la necesidad de poder afrontar y resolver los problemas complejos de investigaciones planteadas en distintas ramas de todas las ciencias conocidas y de esta manera poder hacer un enfoque más centrado a la resolución de los problemas a investigar. Un investigador puede usar las técnicas de los enfoques cuantitativos y cualitativos para realizar investigaciones acerca de una problemática. Para los autores Hernández, Fernández y Batista (2010), la función de una investigación mixta es usar las características principales de ambos tipos de investigación, haciendo una combinación de las fortalezas de una investigación cuantitativa y cualitativa para disminuir las debilidades de ambas indagaciones. La investigación mixta no busca en ningún momento reemplazar las indagaciones cualitativa ni cuantitativa.

Del enfoque mixto se tomarán las técnicas de investigación para describir la problemática de la ciberseguridad basada en Raspberry Pi 3 B+, así como información de los problemas en Raspberry Pi presentados en dicha investigación.

### **3.2. Diseño de investigación**

La modalidad de la investigación que se utilizara para llevar a cabo el presente proyecto es de un nivel comprensivo, en donde vamos a proponer el estudio de factibilidad, para la posterior implementación de un sistema de seguridad de red para una placa Raspberry Pi conectado a una red de sensores para poder solucionar el problema planteado.

El tipo de investigación que se va a realizar es descriptiva-exploratoria, en donde vamos a describir el problema de la falta de seguridad para la información recopilada por la red de sensores y en donde se pretende diseñar un prototipo de seguridad de red hecho a través de dispositivo Raspberry Pi. El proyecto es de manera descriptiva ya que nos interesa saber acerca de la seguridad de la información de los datos y exploratoria porque se va a diseñar un prototipo para la solución a un problema existente en la red de sensores.

## Capítulo IV. Marco de desarrollo

### 4.1. Requerimientos

#### 4.1.1 Raspberry Pi 3 modelo B+

“Es un modelo de las diferentes versiones de Raspberry Pi 3 B+ con presencia desde 2016, cuenta con un microprocesador Broadcom BCM2837 de 64 bits, 1gb de memoria RAM, conexión LAN e inalámbrica, 4 puertos USB, bluetooth, salida HDMI y audio; 40 pines GPIO y espacio para memoria Flash (MicroSD)” (López Aldea, Arduino: guía práctica de fundamentos y simulación, 2015) (López Aldea, 2017).

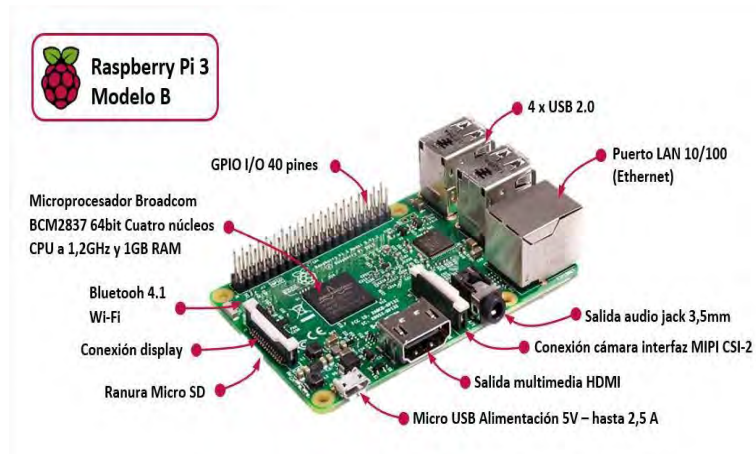


Figura 1. Componentes de una Raspberry pi 3 Modelo B+

#### 4.1.2 HDMI

Los cables HDMI estándar están diseñados para aplicaciones de uso común para transmitir 720p a 1080p, lo que se conoce como resolución de alta definición (HD). Se recomiendan los cables HDMI estándar para televisión por satélite, proyectores de pantalla, reproductores de DVD y otras pantallas comunes, en este caso se requerirá de un cable HDMI estándar para proyectar la pantalla de la Raspberry Pi 3 B+.





*Figura 2. HDMI estándar*

#### **4.1.3 Micro SD**

Tarjeta microSD: tan sólo 15 mm de alto x 11 mm de ancho x 10 mm de grosor. Se ocupará este tipo de almacenamiento debido a que es el más común en teléfonos móviles o tabletas.

En caso de que se encuentren varios modelos que cumplan los criterios, elige la capacidad de almacenamiento que requiera (16, 32, 64 o 128 GB), en este caso se ocupa una Micro SD de 16 GB para el funcionamiento de la Raspberry Pi, ya que es recomendable usar a partir de 8 GB para que la tarjeta SD funcione correctamente.

#### **4.1.4 Raspberry Pi Imager**

Un programa que permite instalar cualquiera de los sistemas operativos compatibles con la minicomputadora Raspberry Pi a la memoria extraíble microSD. La ejecución del programa es compatible para cualquier Sistema Operativo, es fácil de usar y para descargar se puede realizar la descarga desde la página web oficial de Raspberry Pi.



*Figura 3 Sistema Operativo Raspberry Pi Imager*

#### **4.1.5 Computadora**

En este proyecto se ocupa una computadora Sony VAIO SVF14211CLB que cuenta con una arquitectura del sistema operativo de 64-bit y las siguientes características:

**Procesador:** Intel Pentium 2117U (2 núcleos / 2 hilos / 1800 MHz)

**RAM:** 4 GB DDR3 (1333 MHz)

**Pantalla:** LED 14.0" (1366x768) / 60 Hz

**Batería:** 6 celdas

**Almacenamiento:** HDD 750GB (5400rpm)

**Tarjetas de video:** Intel HD Graphics (Ivy Bridge) (Integrada)

**Puertos:**

1. 1x HDMI
2. 1x RJ45 (10 / 100 / 1000 Mbps)
3. 4x USB



*Figura 4. Computadora Sony Vaio*

## **4.2 Implementación**

Esta es la parte del proyecto donde se aplican las configuraciones necesarias para la implementación del prototipo mencionado haciendo uso de los componentes documentados en el punto anterior. Para comenzar, aquí se describen los pasos para configurar el prototipo, se muestran en ilustraciones los pasos a seguir para configurar la Raspberry Pi 3 Modelo B+ y hacer implementación de la parte práctica del marco teórico. Se aplican los conocimientos adquiridos por las investigaciones hechas para el manejo del sistema operativo Raspbian y configurar la seguridad de red en la Raspberry Pi de manera correcta.

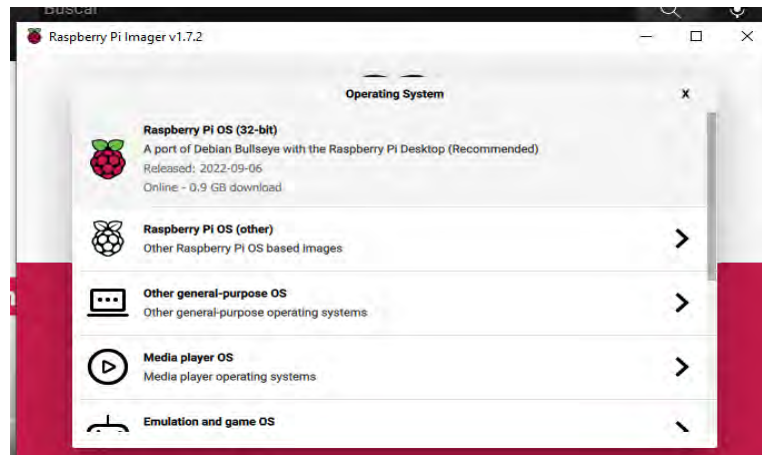
### ***4.2.1 Instalación de Raspbian para Raspberry Pi 3 modelo B+***

Como primer paso, descargue e instale Raspberry Pi Imager en una computadora con un lector de tarjetas SD para poder instalar el Sistema dentro de la tarjeta SD. Coloque la tarjeta SD que usará con su Raspberry Pi en el lector y ejecute Raspberry Pi Imager. El software se puede descargar desde la página oficial de Raspberry sin ningún problema.



*Figura 5. Software Raspberry Pi Imager*

En el segundo paso, se va a elegir la opción “choose OS” y seleccionamos por defecto la primera opción que nos aparece que es un sistema recomendado por el software para nuestra computadora.



*Figura 6. Selección de sistema Raspbian*

De esta manera, se elige la opción “Choose storage” el cual nos pide que se seleccione la unidad en la cual se va a guardar el sistema operativo. En esta opción tenemos que elegir por defecto la tarjeta SD.

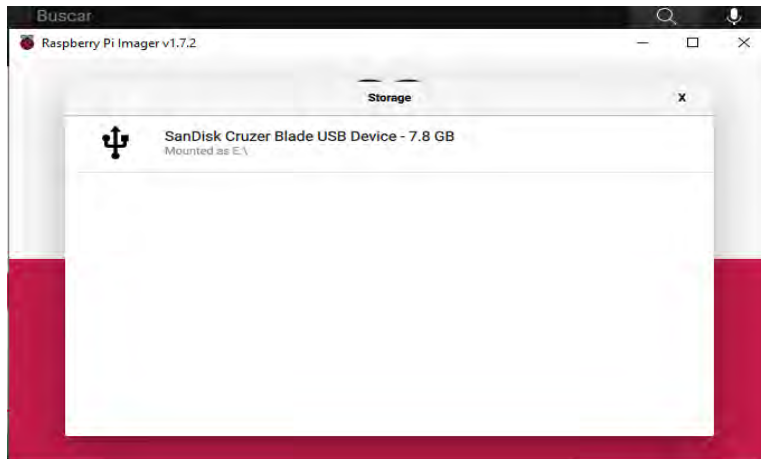


Figura 7. Selección de la tarjeta SD para instalación de SO

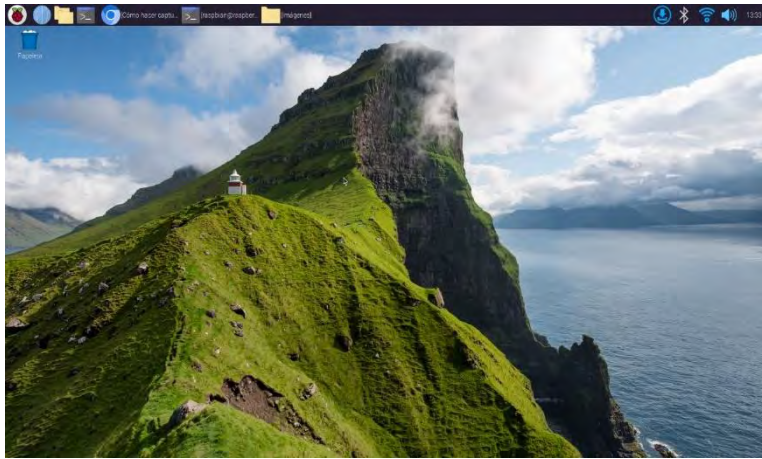
Al seleccionar la SD, se escriben los datos del sistema operativo en la tarjeta y se elige la opción “Write”, nos abre una ventana confirmando si queremos escribir los datos ahí y de esta manera borrar el contenido de la tarjeta, confirmamos dando la opción “Yes” y esperamos un momento a que escriba el sistema operativo en la SD.



Figura 8. Escritura de datos en la memoria SD

Al finalizar el proceso, inserta la microSD en la ranura correspondiente localizada en la tarjeta Raspberry Pi, se conecta y automáticamente iniciará nuestra máquina con el sistema de Raspberry Pi. Nos pide configurar nuestro sistema con cosas básicas como el país, en este caso

México, la fecha y hora del lugar donde habitamos. Al configurar correctamente los parámetros, se inicia nuestra interfaz gráfica Raspbian en la tarjeta que se ve de esta manera:



*Figura 9. Interfaz gráfica de Raspbian al iniciar correctamente*

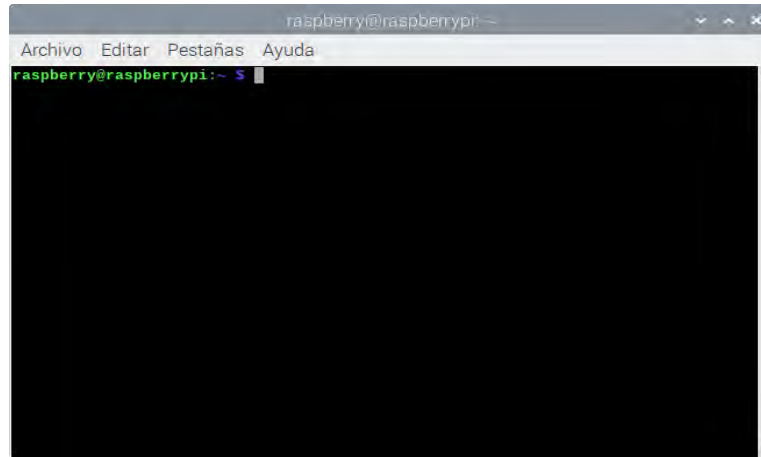
Al iniciar la Raspberry Pi con el sistema Raspbian ya instalado y configurado correctamente, procedemos a configurar los parámetros de ciberseguridad en una Raspberry Pi.

## **4.3 Configuración**

### ***4.3.1 Configuración de firewall.***

En este proyecto, se configurará el sistema de firewall o cortafuegos, ya que sin un firewall activo la tarjeta Raspberry Pi está expuesta a posibles ataques. El firewall permite vigilar los puertos de comunicación de la Raspberry y controlar toda la información que entra y sale a la tarjeta. En este apartado se configura el firewall ufw o firewall sin complicaciones.

Para comenzar, la configuración de la Raspberry se configura a través de la línea de instrucciones, para esto se da un clic en el icono de Raspberry Pi ubicado en la esquina superior izquierda, sección “accesorios” y selecciona la opción “LXTerminal”. Al dar clic, abre una ventana donde se puede configurar la tarjeta.



*Figura 10. LXTerminal de Raspbian*

No obstante, para iniciar a configurar los parámetros del sistema de seguridad de firewall dentro de la Raspberry Pi 3 Modelo B+, se cuenta con las siguientes instrucciones para su implementación:

- 1- pi@raspberrypi:~ \$ sudo apt install ufw
- 2- pi@raspberrypi:~ \$ sudo ufw default deny incoming
- 3- pi@raspberrypi:~ \$ sudo ufw default allow
- 4- pi@raspberrypi:~ \$ sudo ufw default allow outgoing
- 5- pi@raspberrypi:~ \$ sudo ufw status
- 6- pi@raspberrypi:~ \$ sudo ufw allow 3456/udp
- 7- pi@raspberrypi:~ \$ sudo ufw allow 80/tcp
- 8- pi@raspberrypi:~ \$ sudo ufw allow 443/tcp
- 9- pi@raspberrypi:~ \$ sudo ufw allow 22/tcp

*Instrucción 1. Lista de instrucciones para firewall*

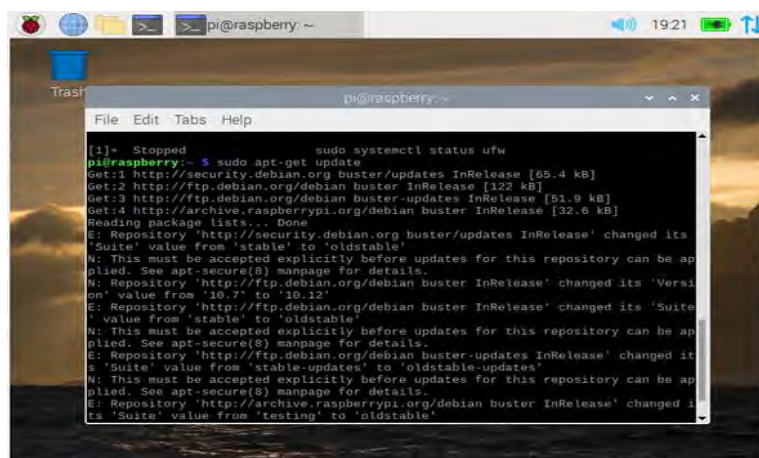
Del enlistado anterior podemos especificar lo siguiente:

La primera instrucción de la lista de instrucciones observada en la **¡Error! No se encuentra el origen de la referencia.** tiene la función de instalar todos los paquetes de firewall para su respectiva configuración, si se desea mantener actualizada la Raspberry, es necesario ingresar la siguiente instrucción dentro de la terminal de la Raspberry:

```
pi@raspberrypi:~ $ sudo apt-get update
```

*Instrucción 2. Actualización para Raspberry Pi*

La instrucción anterior, realiza la descarga de las últimas actualizaciones del sistema de la Raspberry para poder trabajar de manera adecuada. Ingresando la instrucción, se obtiene una descarga de los datos de actualización como se ve en la Figura 11.



*Figura 11. Descarga de actualizaciones con la instrucción sudo apt-get update*

Con la instrucción *deny incoming* en la segunda línea, se deniegan las conexiones entrantes y permitir las salientes con el comando de la línea 3 y cuatro. La línea 5 logra visualizar el estado del firewall, las instrucciones con el número 6 a la 9 se encargan de especificar la configuración de cada puerto que se va a permitir el tráfico en la red, el puerto 3456 nos permite todo el tráfico UDP que provenga de la red y sea usado para nuestra VPN, el

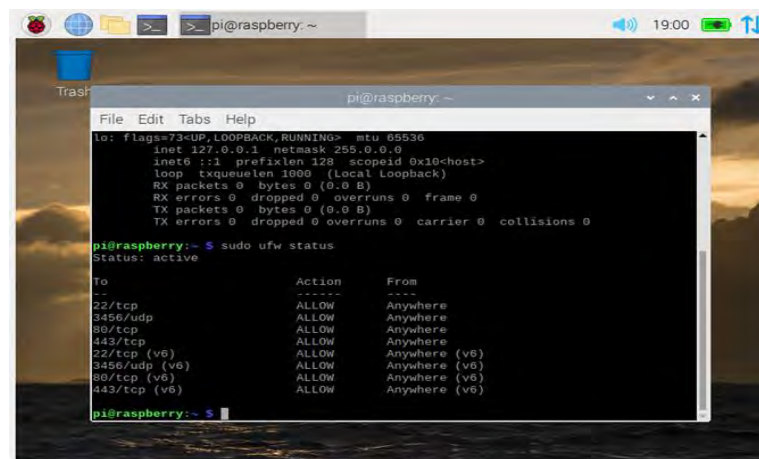


puerto 80 es para el servidor web, para protección de nuestro servidor, el puerto 443 para recibir tráfico proveniente por HTTPS y por último el puerto 22, que nos servirá para podernos conectar por medio de Secure Shell (SSH).

Si se desea verificar que está activo nuestro firewall, se escribe la siguiente instrucción:

```
pi@raspberrypi:~ $ sudo systemctl status ufw
```

*Instrucción 3. Verificación de firewall*



*Figura 12. Estado de los puertos activados para firewall*

No obstante, si el firewall aparece en un status “inactivo”, solo es necesario ingresar a la terminal y escribir la instrucción que lo habilite, la instrucción para habilitarlo es el siguiente:

```
pi@raspberrypi:~ $ sudo ufw enable
```

*Instrucción 4. Habilitación de firewall*

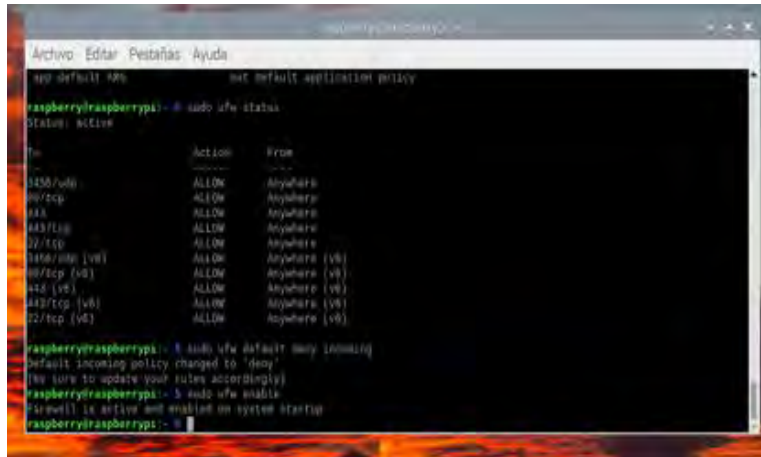


Figura 13. Activación del servicio de firewall

Para más facilidad, se puede obtener la interfaz gráfica en Raspberry del cortafuegos y de esta manera ver las reglas configuradas dentro de la Raspberry Pi, para obtener la interfaz gráfica se escribe la instrucción:

```
pi@raspberrypi:~ $ sudo apt-get install gufw
```

*Instrucción 5. obtención de interfaz gráfica de firewall*

Ingresando la instrucción se obtiene una interfaz como la siguiente:



Figura 14. interfaz gráfica de firewall en Raspberry

En la Figura 14 se observa cómo están establecidas las normas de firewall básicas, para permitir el tráfico de la red y hacer conexión por medio de SSH desde el puerto 22.

#### ***4.3.2 Configuración de SSH***

Una nueva investigación hecha por Javier Jiménez nos dice que el Secure Shell es uno de los protocolos que existen para poder conectarnos de forma remota a un servidor (Jiménez, 2022).

Una ventaja que tenemos al configurar SSH en Raspberry Pi es que con esto podemos configurar la seguridad de nuestra red remotamente sin necesidad de estar físicamente en donde esté la tarjeta, para esto hay que brindar seguridad de que nuestra Raspberry trabaje óptimamente para evitar inconvenientes.

Para comenzar a configurar SSH lo primero que se hace es activarlo, ya que por defecto Raspberry trae desactivado el SSH. Si se cuenta con la interfaz visual o gráfica, lo que hay que hacer es ir al icono superior izquierdo y seleccionar el logotipo de Raspberry, mantener el cursor hasta la opción “preferencias” y seleccionar “Configuración de Raspberry Pi”, siguiente de esto nos muestra una ventana como esta:

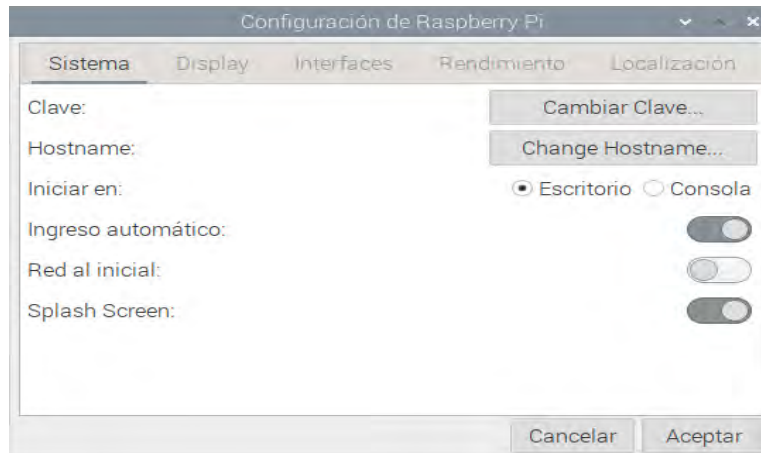


Figura 15. Configuración gráfica de Raspberry Pi

Al aparecer esta ventana, se elige a la opción “interfaces” y se activa la opción SSH y da clic al botón “aceptar”.



Figura 16. Activación del protocolo Secure Shell en la interfaz Gráfica de Raspberry Pi

En caso de trabajar desde la consola, se tiene que ingresar la siguiente instrucción:

```
raspberrypi@raspberrypi:~ $ sudo raspi-config
```

Instrucción 6. Comando para activar SSH de forma manual

Aparece lo siguiente:

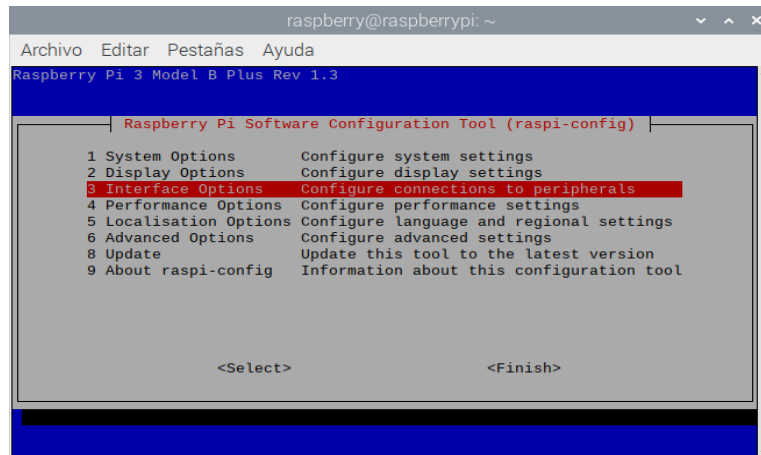


Figura 17. Resultado de ingresar el comando `sudo raspi-config`

Se elige la opción número 3 “Interface options”, da un enter y en la siguiente ventana se selecciona la opción número 12 “SSH” las opciones que arroja es para confirmar que se encenderá de esta manera el protocolo SSH en la tarjeta Raspberry Pi, continuamos con la selección a la opción “yes”.

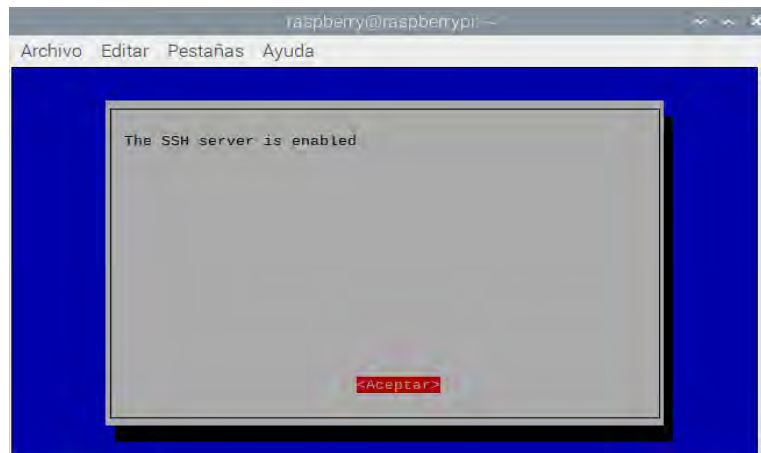


Figura 18. Confirmación de activación del protocolo SSH

Al confirmar la activación de SSH, la tarjeta nos devuelve al menú mostrado en la Figura 17. De esta manera hay que dirigirse hasta la parte inferior a la opción “finish” y regresamos a la terminal de consola para ingresar las instrucciones

Para activar a través de la terminal, se tiene que anexar las siguientes instrucciones para habilitarlo:

```
1-raspberry@raspberrypi: ~ $ sudo systemctl enable ssh
```

```
2- raspberry@raspberrypi:~ $ sudo systemctl start ssh
```

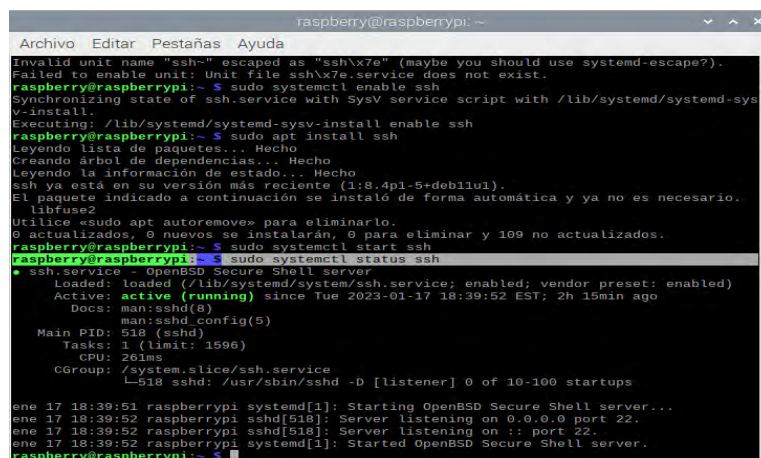
*Instrucción 7. Habilitación de SSH por comandos*

Con las 2 líneas de la Instrucción 7 ingresados solo confirma que el SSH ya esté trabajando. La línea 1 de la Instrucción 7, habilita el SSH mediante la terminal sin realizar los pasos anteriores y la línea 2 inicia el SSH comenzar a trabajar, para verificar que esté activo, ingresa la instrucción siguiente

```
raspberrypi@raspberrypi:~ $ sudo systemctl status ssh
```

*Instrucción 8. Verificación de SSH*

Esta instrucción verifica que SSH, efectivamente ya esté trabajando y corriendo como se observa en la Figura 19, aparece de manera “Activa” en la línea resaltada en color verde.



```
raspberrypi@raspberrypi: ~
Archivo Editar Pestañas Ayuda
Invalid unit name "ssh-" escaped as "ssh\x7e" (maybe you should use systemd-escape?).
Failed to enable unit: Unit file ssh\x7e.service does not exist.
raspberrypi@raspberrypi:~ $ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
raspberrypi@raspberrypi:~ $ sudo apt install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ssh ya está en su versión más reciente (1:8.4p1-5+deb11u1).
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  libfuse2
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 109 no actualizados.
raspberrypi@raspberrypi:~ $ sudo systemctl start ssh
● ssh.service - OpenSSH secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-01-17 18:39:52 EST; 2h 15min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 518 (sshd)
     Tasks: 1 (limit: 1596)
        CPU: 261ms
   CGroup: /system.slice/ssh.service
           └─518 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

ene 17 18:39:51 raspberrypi systemd[1]: Starting OpenSSH Secure Shell server...
ene 17 18:39:52 raspberrypi sshd[518]: Server listening on 0.0.0.0 port 22.
ene 17 18:39:52 raspberrypi sshd[518]: Server listening on :: port 22.
ene 17 18:39:52 raspberrypi systemd[1]: Started OpenSSH Secure Shell server.
raspberrypi@raspberrypi:~ $
```

*Figura 19. Verificación del funcionamiento de SSH*

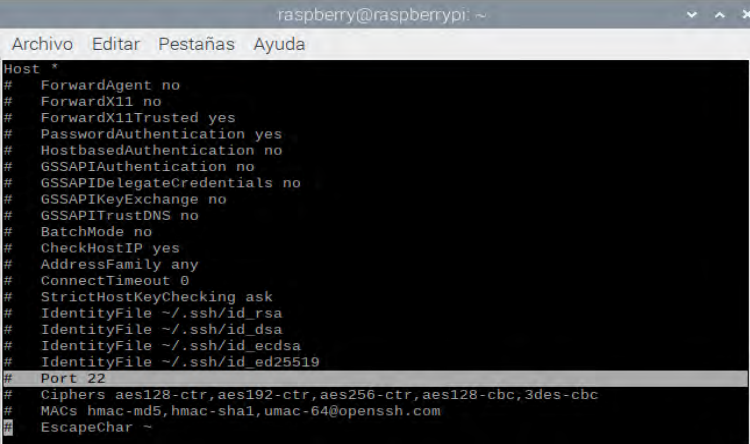
Para avanzar, el siguiente procedimiento para darle seguridad a la Raspberry Pi conectada a la red y se quiere brindar seguridad, el principal punto es modificar el número de puerto por el que se puede conectar remotamente a la Raspberry Pi, para evitar que se acceda de forma sencilla mediante ataques a la tarjeta.

Para cambiar el puerto, desde la terminal se ejecuta la instrucción:

```
raspberrypi@raspberrypi:~ $ vi /etc/ssh/ssh_config
```

*Instrucción 9. Acceso a Configuración de puerto de SSH*

De esta manera se logra visualizar las configuraciones predeterminadas de SSH, dentro de ella ubica la línea que diga el número de puerto que en inglés es “Port”.



```
raspberrypi@raspberrypi: ~
Archivo  Editar  Pestañas  Ayuda
Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
```

*Figura 20. Ubicación del número de puerto dentro de la configuración de SSH*

Ahora hay que regresar al menú anterior y para edición del número de puerto se ingresa la instrucción:

```
raspberrypi@raspberrypi:~ $ sudo nano /etc/ssh/ssh_config
```

*Instrucción 10. Fichero de configuración de puerto de SSH*

La función de la instrucción en Raspberry es la edición del fichero de configuración de SSH, por esa razón se escribe “sudo nano” al principio, para poder editar lo que contiene el fichero.

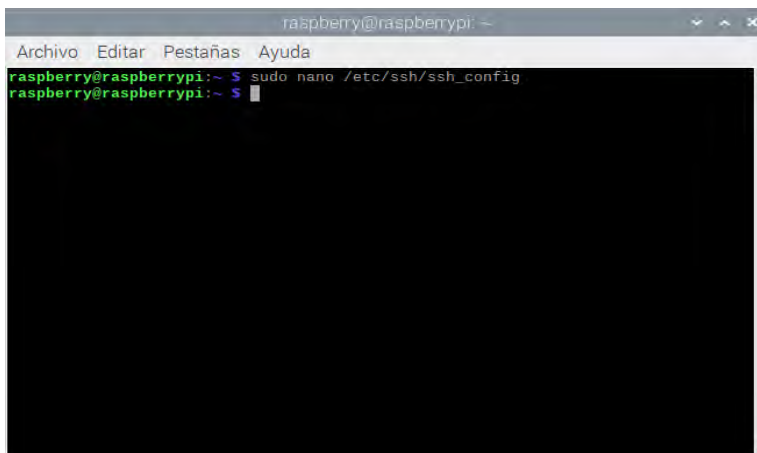


Figura 21. Instrucción de edición de las configuraciones de SSH

En la configuración, la línea donde se encuentre el número de puerto, hay que borrar el por defecto, que tiene el 22 y escribe un número cualquiera del 1024 hasta 65534. Esto con intención de que no sea un número común que ponga vulnerable a la Raspberry Pi, en este caso, se usa el puerto 42000.

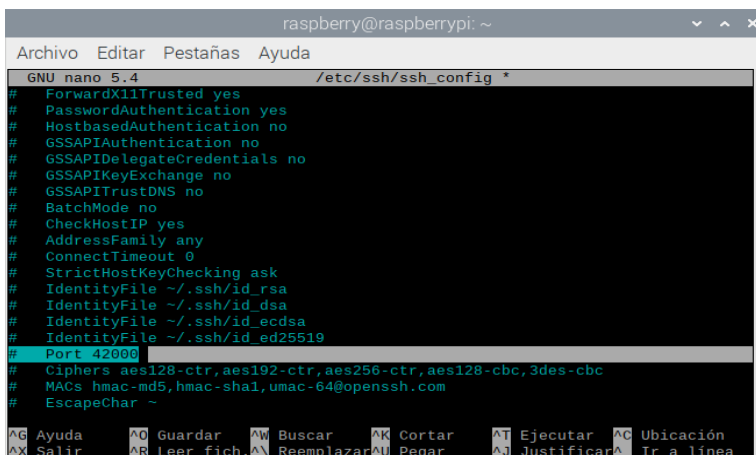
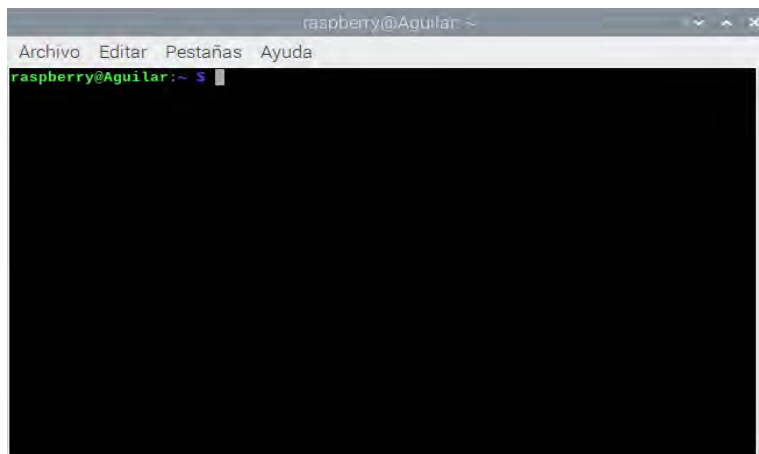


Figura 22. Edición del número de puerto para acceso de SSH de 22 a 42000



Al modificar el número de puerto, presiona “Control + O” para guardar los cambios hechos, seguidamente hay que confirmar que se sobre escribirá el fichero y presionar enter para que automáticamente el sistema nos regrese al menú anterior.

Para mayor seguridad de nuestro servidor SSH, se cambia la contraseña por defecto de la Raspberry Pi 3 B+ por otra clave, con el objetivo de evitar accesos no autorizados a la tarjeta, para esto, primero hay que acceder a la consola de la Raspberry Pi como se muestra en la Figura 23.



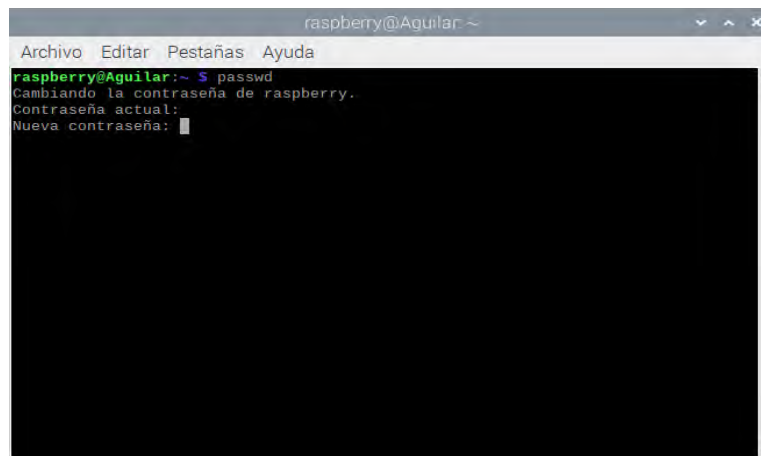
*Figura 23. Consola de Raspberry Pi*

Dentro de la consola, se escribe la instrucción que sirve para realizar el cambio de contraseña sirve para acceder a la Raspberry Pi 3 B+ como se puede visualizar en la Instrucción 11.

```
raspberrypi@raspberrypi:~ $ passwd
```

*Instrucción 11. Cambio de clave de acceso a Raspberry Pi*

Mediante esta línea de instrucción, se cambia la clave para acceder a la tarjeta, nos pide 2 opciones, una para escribir la contraseña actual, que por defecto es “pi” y al dar enter hay que escribir la contraseña nueva, se recomienda que sea larga para evitar que sea fácil de acceder a la tarjeta, la Figura 24 da un ejemplo de cómo aparece la pantalla en la tarjeta.



*Figura 24. Interfaz de cambio de contraseña de Raspberry Pi para acceso remoto.*

De igual forma, al cambiar la clave de la Raspberry Pi, le brinda más seguridad a la red, de esta manera evita un acceso no autorizado a usuarios no reconocidos, para verificar que la clave se haya modificado, en Windows hay que acceder de forma remota por medio del software “Putty”, el cual sirve para hacer conexiones de forma remota como por ejemplo a Raspberry Pi, por medio de la dirección IP de la tarjeta.

Para comenzar, se inicia la aplicación “Putty” en la computadora cliente que va a conectar a la tarjeta y aparece la siguiente interfaz como muestra la Figura 25.

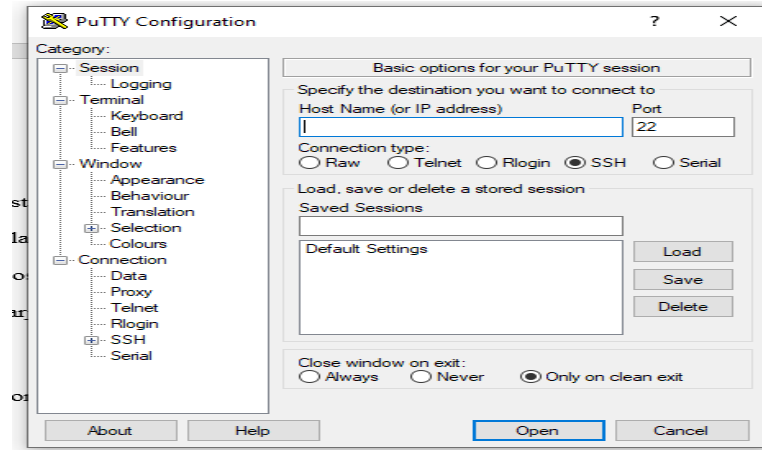


Figura 25. Interfaz de putty para conexión remota a Raspberry Pi

No obstante, dentro de Putty, en la opción “IP address”, la dirección IP que tiene asignada la tarjeta Raspberry es la que se escribe en el apartado mencionado anteriormente, para saber la dirección IP, es necesario dirigirse a la consola de Raspberry y escribir la instrucción:

```
raspberrypi@raspberrypi:~ $ ifconfig
```

Instrucción 12. Comando para saber la dirección IP de Raspberry Pi

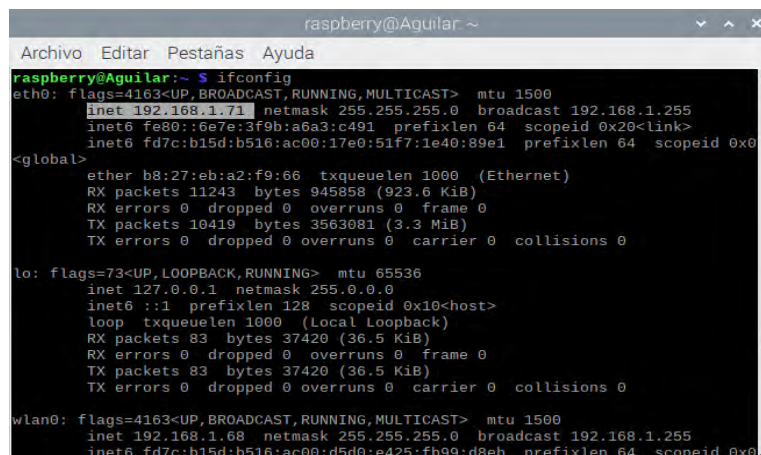


Figura 26. Dirección IP de la tarjeta mediante la instrucción ifconfig

La Instrucción 12 muestra las direcciones IP de la tarjeta Raspberry, en este caso, está conectada por medio de ethernet, por lo que la dirección IP en este caso para conexión remota es 192.168.1.71, esta dirección se escribe en el apartado de IP address de Putty y se cambia el puerto por el cual se va a realizar la conexión, en este caso configuró el puerto 42000 como en la Figura 22, por lo tanto, se observa en la interfaz la escritura del apartado mostrado en la Figura 27.

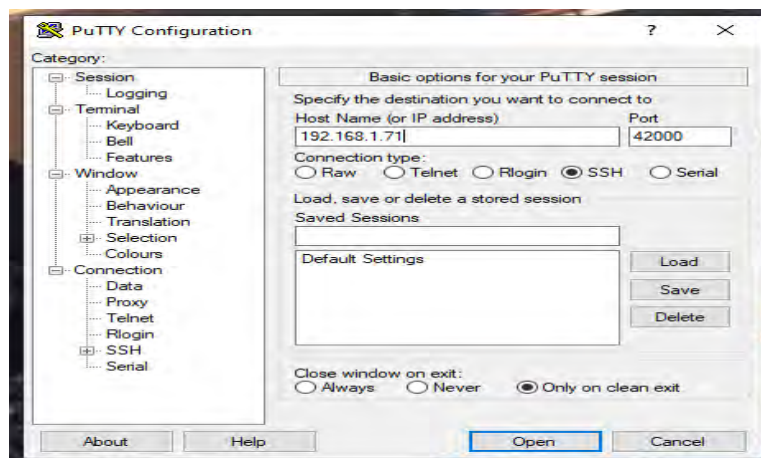


Figura 27. Conexión remota vía SSH a Raspberry Pi

Al termino de escritura de los datos, da clic en la opción “entrar”, la tarjeta pide acceder con un usuario, en este caso “raspberry” y al dar enter nos pide contraseña, para esto, ingresa la clave modificada en el punto anterior de SSH (Figura 24).

```
raspberry@Aguilar: ~  
login as:  
login as: raspberr  
raspberry@192.168.1.71's password:  
Linux Aguilar 5.15.61-v7+ #1579 SMP Fri Aug 26 11:10:59 BST 2022 armv7l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Tue Feb 7 21:49:26 2023 from 192.168.1.72  
raspberry@Aguilar:~ $
```

Figura 28. Escritura de usuario y contraseña nueva para acceso a Raspberry

Si todo es escrito de forma correcta, deja acceder como se observa en la Figura 28, sin ningún problema y así poder trabajar de manera remota para configurar, entre otras cosas.

### 4.3.3 Configuración de VPN

Continuando la configuración de ciberseguridad, se va a configurar VPN, la herramienta para poder usar es PiVPN, esta herramienta nos permite el uso de OpenVPN y da la facilidad de poder configurar por medio de instrucciones

Para comenzar, escribimos la instrucción

```
raspberry@raspberrypi:~ $ curl -L https://install.pivpn.io | bash
```

*Instrucción 13. Instalación de OpenVPN*

Con la instrucción, la Raspberry se conecta en línea a PiVPN, descarga y ejecuta las instrucciones correspondientes para instalar OpenVPN.

```
pi@raspberrypi:~$ curl -L https://install.pivpn.io | bash
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 162 100 162 0 0 625 0 --:--:-- --:--:-- --:--:-- 627
100 83088 100 83088 0 0 201k 0 --:--:-- --:--:-- --:--:-- 201k
:::
::: sudo will be used for the install.
::: Hostname length OK
::: Verifying free disk space...
:::
::: apt-get update has not been run today. Running now...
done!
:::
::: Checking apt-get for upgraded packages...
```

Figura 29. Comprobación de PiVPN

Una vez instalado y comprobado el servicio de OpenVPN a través de PiVPN como se muestra en la Figura 29, la Raspberry Pi lanza un mensaje donde indica que la Raspberry se puede usar como un servidor de OpenVPN, continúa dando clic o enter en la opción “OK”.

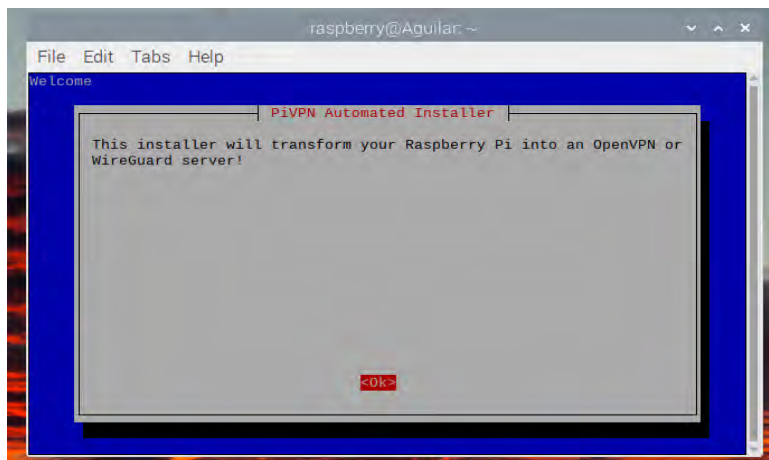


Figura 30. Mensaje del instalador de PiVPN

Al realizar esto se muestra un mensaje dónde se explica que la Raspberry necesita una dirección IP estática para funcionar adecuadamente, o de lo contrario, se puede asignar direccionamiento a través de DHCP para que tome una dirección IP dentro del rango de la red a la que está conectada.

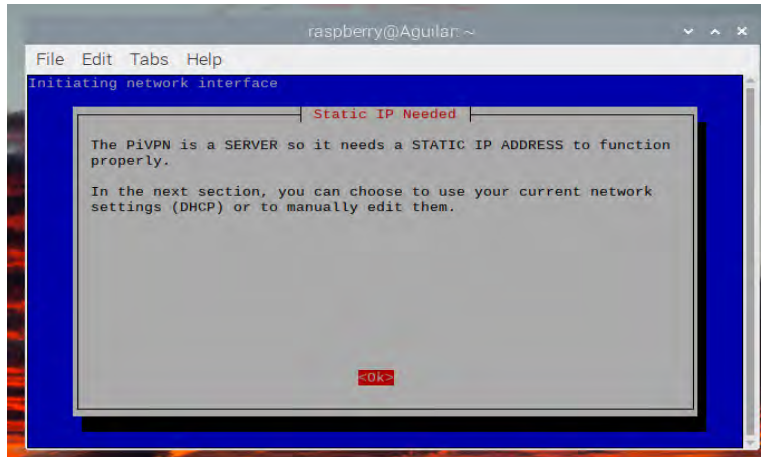


Figura 31. Mensaje del instalador PiVPN

Para continuar, en la ventana de la Figura 31, presione enter a la opción “OK” y se arroja una ventana preguntando que interfaz va a usar Raspberry Pi para el direccionamiento, donde aparecen las opciones

Ethernet (si la Raspberry está conectada por cable de red) o WLAN (si está conectada a través de Wi-fi). Se puede observar las opciones en la Figura 32.

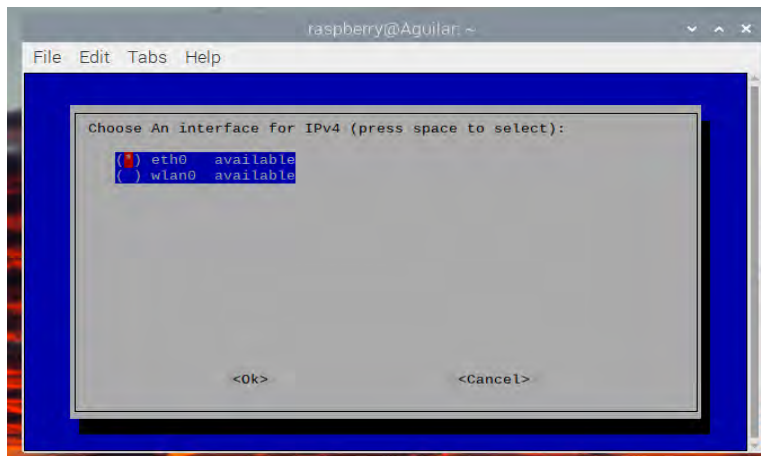


Figura 32. Selección de interfaz de red para direccionamiento de OpenVPN

En este caso se elige “eth0” debido a que la tarjeta está conectada a través de cable de red, al seleccionar la opción y dar “OK” para el siguiente paso, la siguiente ventana arroja la confirmación de lo que se ha seleccionado junto con la dirección IP que toma la Raspberry Pi como se puede ver en la Figura 33.

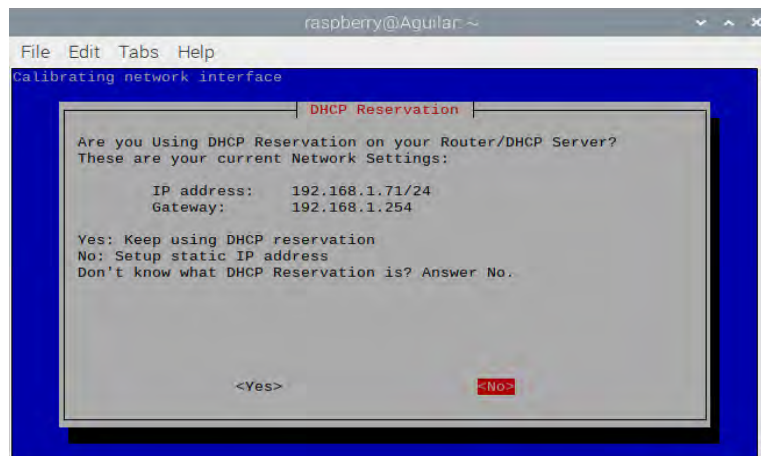


Figura 33. Confirmación de configuración de red de OpenVPN

La Raspberry Pi por defecto con cable trae la dirección IP 192.168.1.71/24, con esto se confirma que el direccionamiento es correcto a través de Ethernet. Comprobando esta opción, se continúa presionando enter a la opción “YES” para continuar.

Seguidamente, PiVPN arroja un mensaje en donde se avisa que se tiene que elegir un usuario para uso de VPN y responsable de su configuración.



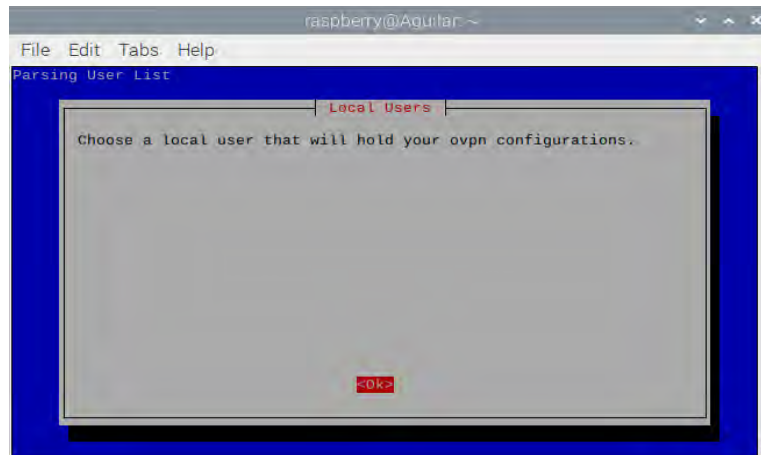


Figura 34. Mensaje de selección de usuario.

En la siguiente ventana, se elige el usuario en donde quiere hacer las configuraciones de VPN, no obstante, la tarjeta solo cuenta con el usuario “raspberry” que es dónde se han hecho las configuraciones anteriores, por lo tanto, seleccione esta opción.

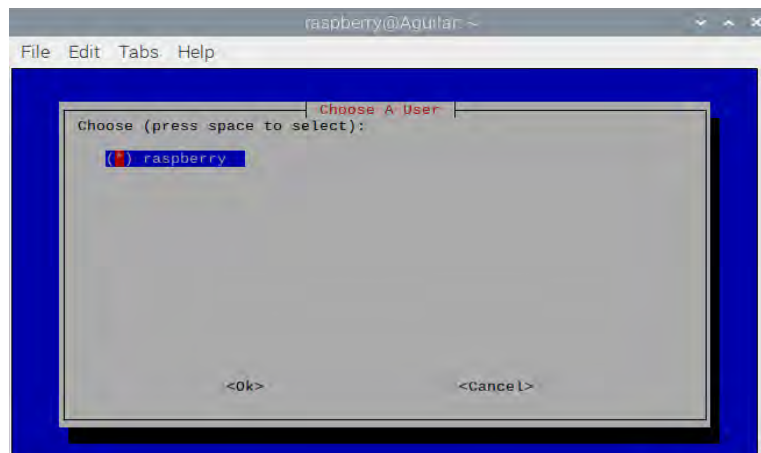


Figura 35. Selección de usuario para VPN

Después de seleccionar el usuario como se muestra en la Figura 35, ahora hay que elegir qué tipo de instalación se desea realizar, aparecen los protocolos “WireGuard” y “OpenVPN”, en este caso, se elige OpenVPN por lo flexible que es en su configuración y debido a que tiene capacidad para tener clientes en móviles y escritorio (Figura 36).

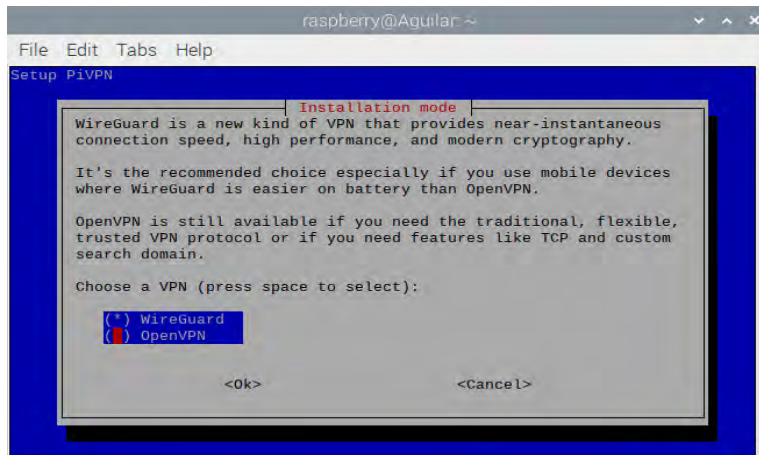


Figura 36. Selección del protocolo OpenVPN para configuración

Realizar la selección de OpenVPN nos arroja un mensaje el cual nos indica que es lo que incluye por defecto el protocolo UDP, aquí se selecciona la opción “NO” para continuar, esto con intención de que no tome una configuración por defecto la VPN.

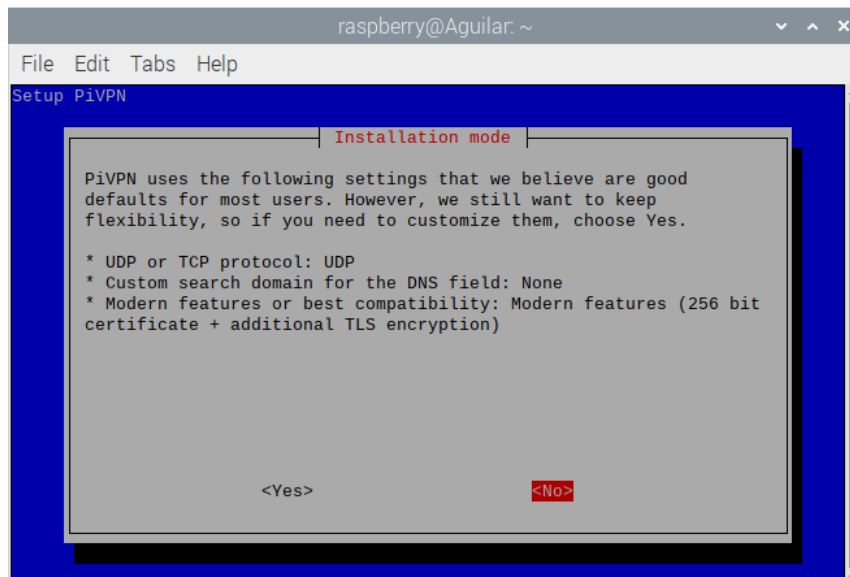
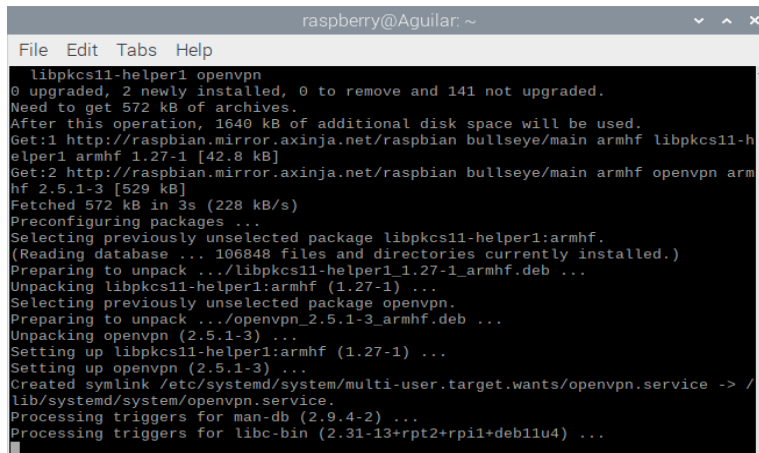


Figura 37. Configuración por defecto de OpenVPN



```
raspberry@Aguilar: ~  
File Edit Tabs Help  
libpks11-helper1 openvpn  
0 upgraded, 2 newly installed, 0 to remove and 141 not upgraded.  
Need to get 572 kB of archives.  
After this operation, 1640 kB of additional disk space will be used.  
Get:1 http://raspbian.mirror.axinja.net/raspbian bullseye/main armhf libpks11-h  
elper1 armhf 1.27-1 [42.8 kB]  
Get:2 http://raspbian.mirror.axinja.net/raspbian bullseye/main armhf openvpn arm  
hf 2.5.1-3 [529 kB]  
Fetched 572 kB in 3s (228 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package libpks11-helper1:armhf.  
(Reading database ... 106848 files and directories currently installed.)  
Preparing to unpack .../libpks11-helper1_1.27-1_armhf.deb ...  
Unpacking libpks11-helper1:armhf (1.27-1) ...  
Selecting previously unselected package openvpn.  
Preparing to unpack .../openvpn_2.5.1-3_armhf.deb ...  
Unpacking openvpn (2.5.1-3) ...  
Setting up libpks11-helper1:armhf (1.27-1) ...  
Setting up openvpn (2.5.1-3) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn.service -> /  
lib/systemd/system/openvpn.service.  
Processing triggers for man-db (2.9.4-2) ...  
Processing triggers for libc-bin (2.31-13+rpt2+rp1+deb11u4) ...
```

Figura 38. Carga de configuración de VPN en Raspberry Pi 3 B+

Avanzando a la configuración de VPN, al terminar de cargar la configuración, da la opción de modificar nuestro puerto para VPN, para esto OpenVPN tiene asignado el puerto 1194 por defecto, puede modificarse en este caso a otro puerto cualquiera, aquí se eligió el puerto 2023.

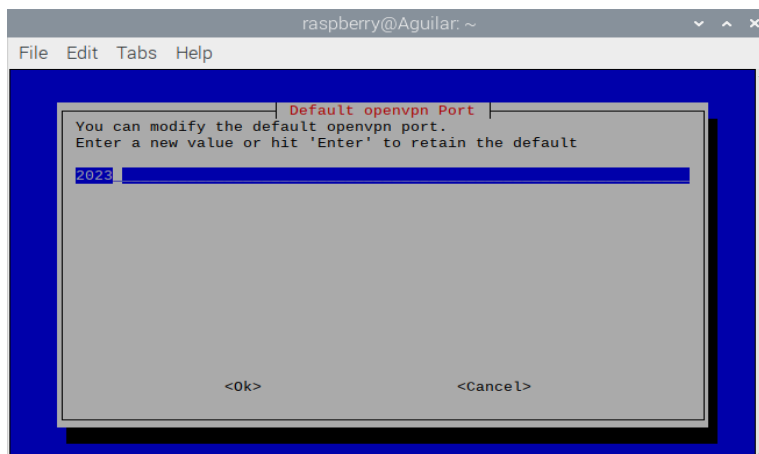


Figura 39. Modificación de puerto VPN

Al término de la selección de puertos, presione la opción “OK” y nos arroja un mensaje de confirmación de cambio de puerto, a lo que tiene que confirmar que es correcto la modificación en caso de cambiarse y se presiona “YES” (Figura 39).

No obstante, hay que seleccionar un DNS para la VPN, en la cual aparece una lista para seleccionar que servidor de DNS se desea usar, con las flechas del teclado se baja hasta encontrar el DNS de Google y se presiona espacio en el teclado y enter para confirmar la selección como se observa en la Figura 40.

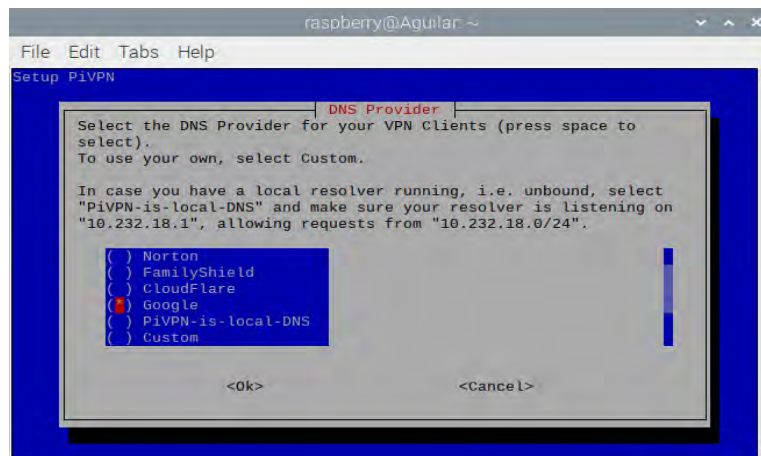


Figura 40. Selección de DNS

Al seleccionar el DNS de Google y dar “OK”, se tiene que seleccionar por consiguiente la opción de IP pública con la que se cuenta, en caso de no aparecer la opción, debe introducir manualmente, en este caso, es mejor usar la IP pública que se asigna, al seleccionarla, se continua con un enter en “OK” como se muestra en la Figura 41.

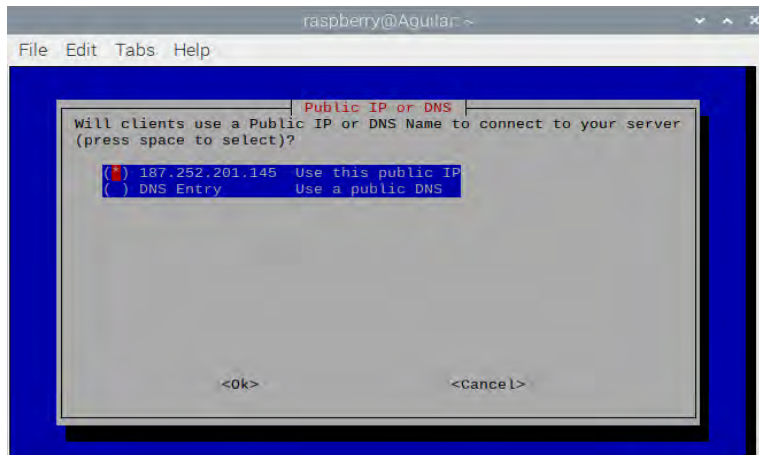


Figura 41. Selección de IP publica para DNS

El siguiente paso es seleccionar “OK”, en esta ventana solo confirma que se hará la generación de clave para autenticación de funcionamiento para PiVPN.

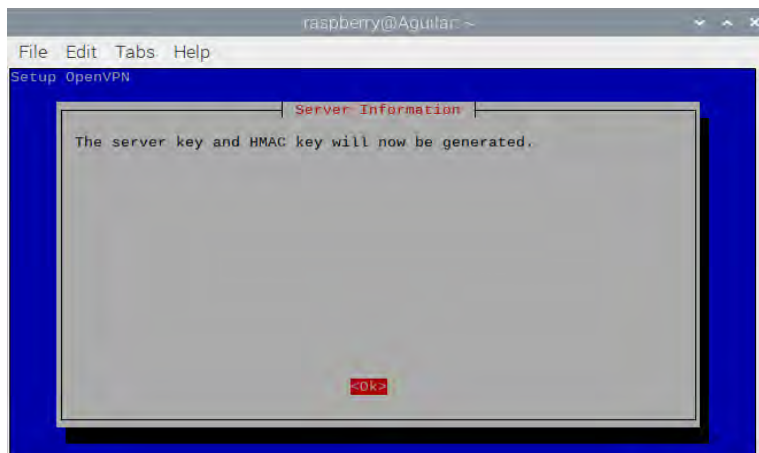
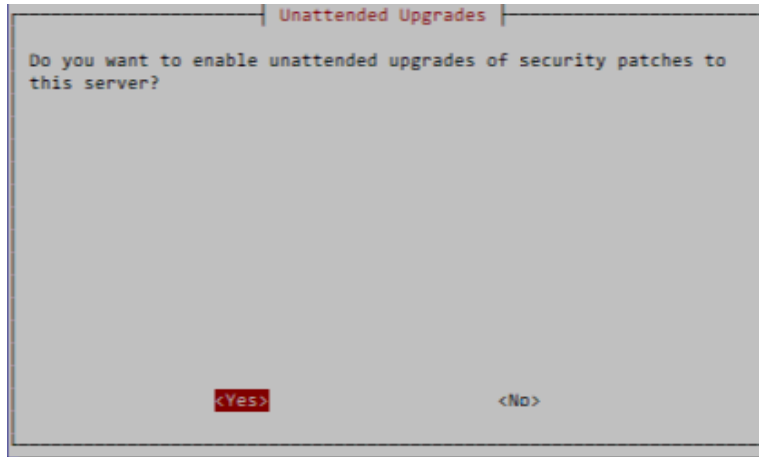


Figura 42. Confirmación de clave de autenticación

Finalmente, PiVPN comprueba si se encuentran instaladas las actualizaciones más recientes de seguridad, por lo que se tiene que aceptar el mensaje para que PiVPN se actualice de forma automática cada vez que haya algo disponible, aunque se puede deshabilitar las actualizaciones automáticas si se desea presionando “NO”, aunque no se recomienda, puesto que así, el sistema se mantendrá actualizado de forma automática (Figura 43).



*Figura 43. Selección de actualizaciones automáticas en PiVPN*

De igual forma, al término de la configuración, Raspberry muestra una ventana dónde se indica que PiVPN ha quedado listo, para continuar, presione “OK” y reinicie la Raspberry para llevar a cabo la configuración, por lo que, de esta manera, al reiniciar solo se espera a que encienda de nuevo la Raspberry.

## Capítulo V. Pruebas

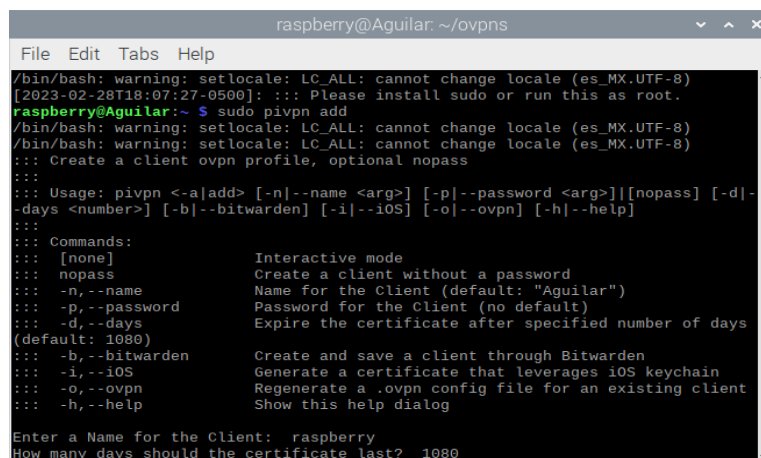
### 5.1 Prueba VPN

Una vez reiniciada la Raspberry Pi, se puede hacer uso de la instrucción `pivpn`, esto con la intención de crear un usuario para el uso y conexión de la VPN.

```
raspberrypi@raspberrypi:~ $ sudo pivpn add
```

*Instrucción 14. Creación de usuario en PiVPN*

Con esta instrucción, hay que registrar un nombre de usuario y una contraseña para crear certificados para usar VPN en la Raspberry. Al crear el usuario y la clave de autenticación, con un `enter` se confirma la instrucción y se espera a que se cree el archivo de fichero dónde contendrá las configuraciones y códigos de las certificaciones de VPN.



```
raspberrypi@Aguilar: ~/ovpns
File Edit Tabs Help
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (es_MX.UTF-8)
[2023-02-28T18:07:27-0500]: :: Please install sudo or run this as root.
raspberrypi@Aguilar:~ $ sudo pivpn add
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (es_MX.UTF-8)
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (es_MX.UTF-8)
:: Create a client ovpn profile, optional nopass
::
:: Usage: pivpn <-a|add> [-n|--name <arg>] [-p|--password <arg>][nopass] [-d|--days <number>] [-b|--bitwarden] [-i|--iOS] [-o|--ovpn] [-h|--help]
::
:: Commands:
:: [none] Interactive mode
:: nopass Create a client without a password
:: -n,--name Name for the Client (default: "Aguilar")
:: -p,--password Password for the Client (no default)
:: -d,--days Expire the certificate after specified number of days (default: 1080)
:: -b,--bitwarden Create and save a client through Bitwarden
:: -i,--iOS Generate a certificate that leverages iOS keychain
:: -o,--ovpn Regenerate a .ovpn config file for an existing client
:: -h,--help Show this help dialog
Enter a Name for the Client: raspberrypi
How many days should the certificate last? 1080
```

*Figura 44. Creación de usuario de VPN en PiVPN*

Seguidamente, la Raspberry crea un fichero, el cual se encuentra dentro de los archivos de la Raspberry Pi, creado el fichero, se tiene que mandar a una computadora cliente para hacer la prueba de este mediante un cliente OpenVPN, el archivo a mandar se muestra en la Figura 45:

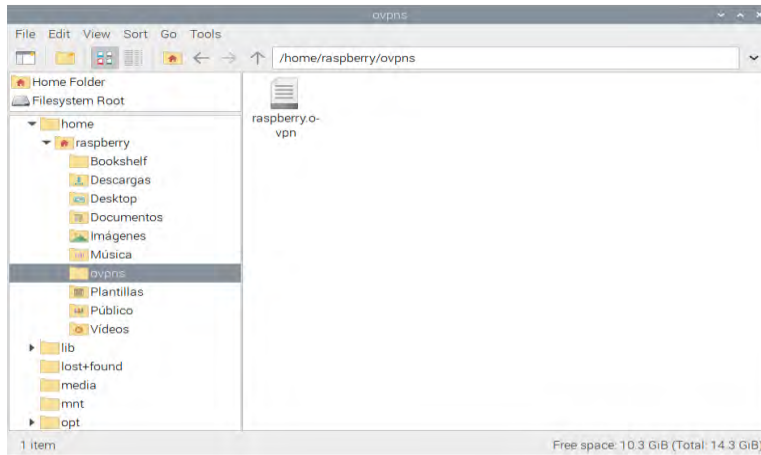


Figura 45. Fichero de VPN en Raspberry Pi

Al enviar, acceda al archivo y se editan las líneas que se ve resaltada a continuación en la Figura 46.

```

1 client
2 dev tun
3 proto udp
4 remote 187.252.201.145 2023
5 resolv-retry infinite
6 nobind
7 remote-cert-tls server
8 tls-version-min 1.2
9 verify-x509-name Aguilar_b1a8fbae-968f-41e1-ae2-56f142041f2d name
10 cipher AES-256-CBC
11 auth SHA256
12 auth-nocache
13 verb 3
14 <ca>
15 -----BEGIN CERTIFICATE-----
16 MIIBvzCCAwwGAWIBAgIUyk+alu1MxZmz5Tl1MbJVED64HggwCgYIKoZIzj0EAwIw
17 FjEUMBIGAIUEAwWLRWFzeS1SU0EgQ0EwHhcNMjMwMjE0MTg1MzU4WhcNMzMwMjEx

```

Figura 46. Edición fichero VPN

De tal forma que queda de la siguiente manera:



```

client
dev tun
proto udp
remote 187.252.201.145 2023
resolv-retry infinite
nobind
remote-cert-tls server
tls-version-min 1.2
verify-x509-name Aguilar_b1a8fbae-968f-41e1-ae2-56f142041f2d name
cipher AES-256-CBC
auth SHA256
auth-nocache
verb 3
route-nopull
route 10.8.0.0 255.255.0.0
route 192.168.1.0 255.255.255.0
<ca>
-----BEGIN CERTIFICATE-----
MIIBvzCCAWGgAwIBAgIUyk+alu1MxZmz5Tl1MbJVED64HggwCgYIKoZIzj0EAwIw
FjEUMBIGA1UEAwLRWFzeS1SU0EgQ0EwHhcNMjMwMjE0MTg1MzU4WhcNMzMwMjEx

```

Figura 47. Configuración rango de red en VPN

Al configurar y hacer los cambios en el fichero, ahora se verifica la conexión de la VPN para verificar que está funcionando, para esto se necesita en este caso para un sistema operativo Windows un cliente OpenVPN que se puede descargar desde la página web <https://openvpn.net/community-downloads/>.

En la primera línea de la Figura 47, se le está haciendo indicación al cliente para que use las rutas que tiene aprendido el router para hacer la salida de paquetes hacia internet.

La siguiente configuración que se nota en la línea siguiente, es la asignación de una IP al adaptador virtual o túnel, el cual se le agrega la dirección IP 10.8.0.0 / 16, ya que esta dirección es la que por defecto nos brinda PiVPN para configurar el túnel.

La línea siguiente le brinda al cliente la conexión a la red a través de ruteo mediante la dirección IP 192.168.0.0 / 24 hecho por el túnel VPN. Las asignaciones más comunes para ruteo por lo general son 192.168.0.0 y 192.168.1.0, en caso de coincidir las direcciones IP de la red local cliente y la red del servidor, puede haber problema de conexión, para este caso es recomendable que las direcciones de una y otra red sean diferentes.

Al descargarlo lo que se puede apreciar como en la Figura 48 de la siguiente forma en sistema operativo Windows.



Figura 48. OpenVPN descargado desde Windows.

Una vez descargado, se importa el fichero de configuración de VPN, para que el cliente se pueda conectar a la Raspberry mediante la VPN, para esto, hay que dirigirse al icono de OpenVPN y le damos clic en la opción “importar archivo” o “import file” para que de esta manera confirme la configuración a tomar de nuestra Raspberry (Figura 49).

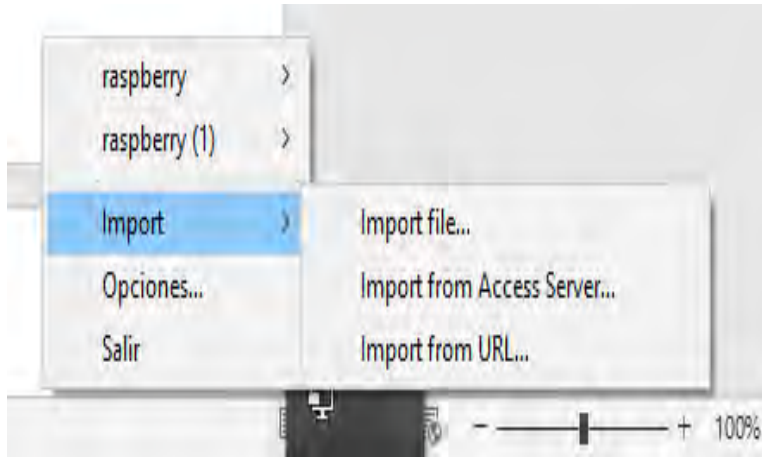


Figura 49. Importación de configuración a cliente VPN

La VPN automáticamente abre una ventana en la cual nos pide la clave del usuario que se creó de VPN (Figura 44), una vez puesto los datos correctamente, se muestra un mensaje en el cual se asigna un ip privada al cliente.

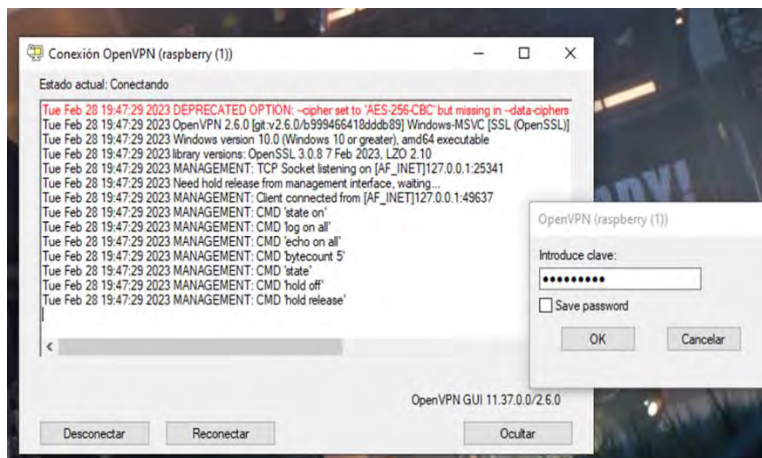


Figura 50. Acceso a OpenVPN de Raspberry Pi

El mensaje es como el siguiente:

```
Tues Feb 28 19:25:13 2023 MANAGEMENT: >STATE:1605464713, CONNECTED, SUCCESS,10.8.0.2,
84.121.148.11, 2023,
```

Para comprobar la conectividad, se hace un ping desde cmd de windows al equipo cliente.

```
Traza a 10.8.0.1 sobre caminos de 30 saltos como máximo.  
  
1 28 ms 26 ms 26 ms 10.8.0.1  
  
Traza completa.
```

Figura 51. Comprobación de conectividad de VPN en Windows.

Por último, para comprobar que el cliente esté conectado a VPN de Raspberry, solo basta con escribir la instrucción “ipconfig” en cmd y de esta manera corroborar que el servidor VPN implementado en Raspberry Pi está funcionando.

```
Configuración IP de Windows  
  
Adaptador desconocido OpenVPN Wintun:  
  
Estado de los medios. . . . . : medios desconectados  
Sufijo DNS específico para la conexión. . . :  
  
Adaptador de Ethernet Ethernet:  
  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::59f5:685c:dcd3:823a%8  
Dirección IPv4. . . . . : 192.168.1.2  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1  
  
Adaptador desconocido OpenVPN TAP-Windows6:  
  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::4c1e:c287:f943:6793%25  
Dirección IPv4. . . . . : 10.8.0.2  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . :
```

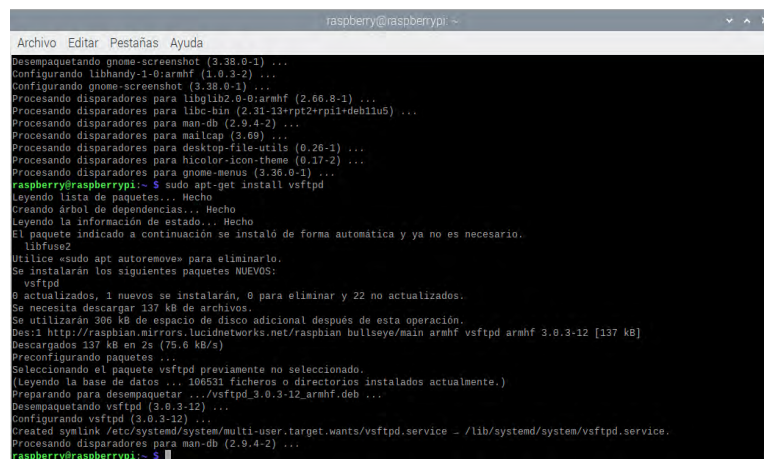
Figura 52. Comprobación de la implementación de VPN desde una computadora cliente

## 5.2 Prueba SSH

Para esta prueba, relativamente se usa el protocolo FTP (File Transfer Protocol) el cuál es un protocolo que permite la transferencia de archivos de manera indirecta entre 2 sistemas, en este caso, permite la visualización y creación de archivos en una Raspberry conectándose de manera remota a este desde una PC con sistema operativo Windows para comprobar la configuración de SSH en Raspberry Pi 3 B+, para esto, como primer paso, se requiere descargar el servidor de FTP en Raspberry, se dirige a la terminal y escribimos la siguiente instrucción.

```
pi@raspberrypi:~ $ sudo apt-get install vsftpd
```

*Instrucción 15. Instalación del servidor FTP*



```
raspberrypi@raspberrypi:~$ sudo apt-get install vsftpd
Desempaquetando gnome-screenshot (3.38.0-1) ...
Configurando libhandy-1-0:armhf (1.0.3-2) ...
Configurando gnome-screenshot (3.38.0-1) ...
Procesando disparadores para libglib2-0:armhf (2.66.8-1) ...
Procesando disparadores para libc-bin (2.31-13+rpt2+rpil+deb11u5) ...
Procesando disparadores para man-db (2.9.4-2) ...
Procesando disparadores para mailcap (3.69) ...
Procesando disparadores para desktop-file-utils (0.26-1) ...
Procesando disparadores para hicolor-icon-theme (0.17-2) ...
Procesando disparadores para gnome-menus (3.36.0-1) ...
raspberrypi@raspberrypi:~$ sudo apt-get install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  libfuse2
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes NUEVOS:
  vsftpd
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 22 no actualizados.
Se necesitan 396 kB de espacio de disco adicional después de esta operación.
Des:1 http://raspbian.mirrors.lucidnetworks.net/raspbian bullseye/main armhf vsftpd armhf 3.0.3-12 [137 kB]
Descargados 137 kB en 2s (75.0 kB/s)
Preparando paquetes ...
Seleccionando el paquete vsftpd previamente no seleccionado.
(Leyendo la base de datos ... 106531 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../vsftpd_3.0.3-12_armhf.deb ...
Desempaquetando vsftpd (3.0.3-12) ...
Configurando vsftpd (3.0.3-12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Procesando disparadores para man-db (2.9.4-2) ...
raspberrypi@raspberrypi:~$
```

*Figura 53. Instalación del servidor FTP en Raspberry Pi*

Una vez descargado el servidor, se edita el archivo de configuración del FTP con la instrucción `sudo nano /etc/vsftpd.conf`, al entrar, descomentamos las opciones:

- 1- `local_enable=YES`
- 2- `write_enable=YES`





Figura 55. Muestra del software FileZilla

Al entrar a FileZilla se pide rellenar 3 campos, en los cuales en servidor se pone la dirección IP de la Raspberry Pi, en este caso es 192.168.1.64, el usuario y la clave configurada para acceder de forma remota a Raspberry, así como el puerto, en este caso se cambió anteriormente de 22 a 42000, al ingresar los datos, se da clic en conectar.

Si todo es correcto, nos mostrará los archivos de nuestro cliente y nuestro servidor que es la Raspberry Pi, véase en la Figura 56.

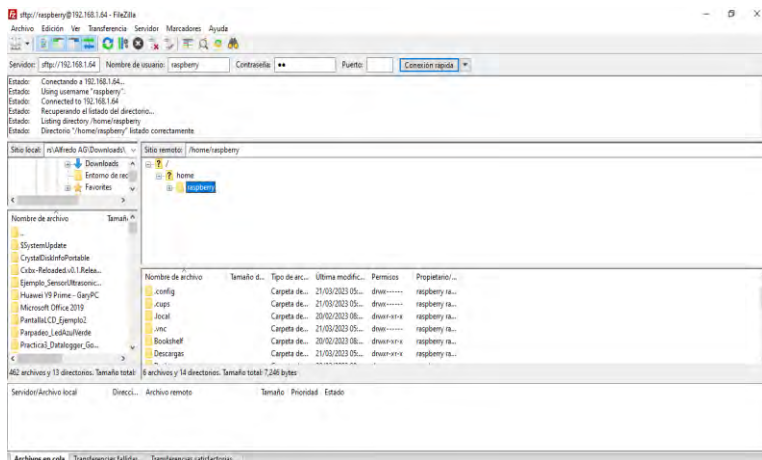


Figura 56. Conexión FTP por SSH a Raspberry Pi



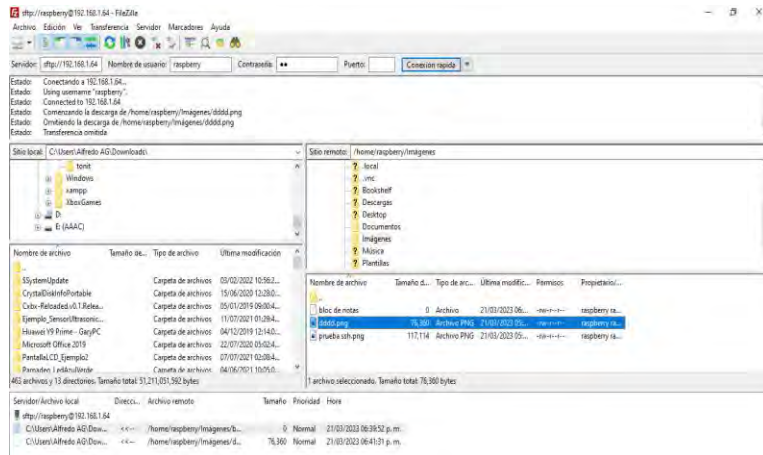


Figura 57. Transferencia de archivos entre Raspberry y Windows de manera remota

### 4.3 Prueba de Firewall

Para hacer la prueba de funcionamiento del firewall, lo primero que se debe hacer, es entrar a la terminal de la Raspberry Pi y poner la siguiente instrucción:

```
pi@raspberrypi:~ $ sudo nano /etc/rc.local
```

*Instrucción 17. Edición del fichero de configuración de firewall*

En la lista de la Instrucción 1 se realiza la configuración de nuestro firewall configurado en Raspberry Pi 3 B+, de esta manera se realiza una prueba bloqueando el acceso a una página web como, por ejemplo, YouTube, dentro del fichero se modifica la configuración solo para el bloqueo de esta página web, se ve como en la Figura 58:



```
raspberrypi@raspberrypi: ~  
Archivo Editar Pestañas Ayuda  
GNU nano 5.4 /etc/rc.local  
# /bin/sh -e  
# cerramos el acceso de la lan a la web  
sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "youtube.com" >  
# rc.local  
#  
# This script is executed at the end of each multiuser runlevel.  
# Make sure that the script will "exit 0" on success or any other  
# value on error.  
#  
# In order to enable or disable this script just change the execution  
# bits.  
#  
# By default this script does nothing.  
.  
./etc/firewall_INI  
# Print the IP address  
IP=$(hostname -I) || true  
if [ "$IP" ]; then  
  printf "My IP address is %s\n" "$IP"  
fi  
_23 líneas leídas |  
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación  
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea
```

Figura 58. Bloqueo de Youtube.com

Para comprobar, se guarda dentro del fichero de configuración de firewall las modificaciones realizadas en la Figura 58, el cual está resaltado para especificar el bloqueo de dicha página, para hacer la prueba en nuestra computadora cliente, se accede a internet y al intentar entrar a YouTube, se deniega el acceso debido a que se prohibió por medio del firewall acceder a esta página web. El funcionamiento del firewall se puede observar como en la siguiente figura.



Figura 59. Firewall Funcionando correctamente.

En el caso de la VPN configurada en el capítulo anterior con el puerto número 2023, si se desea probar la funcionalidad de firewall, sucede un caso similar, en el cuál si se niega el acceso desde el puerto 2023, el firewall toma la regla y al querer conectarse al servidor VPN desde la computadora cliente, la conexión falla debido a la modificación de reglas de VPN.

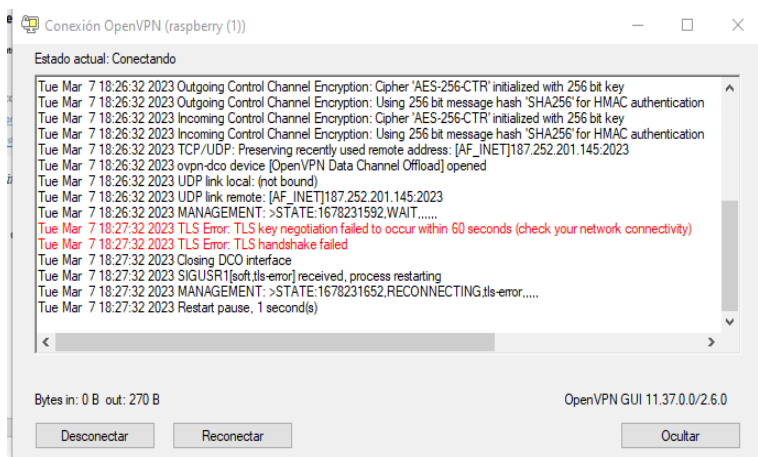


Figura 60. Verificación de firewall con OpenVPN de Raspberry Pi 3 B+

Este error remarcado en rojo en la Figura 60 es un mensaje que se da debido a que la VPN no puede establecer conexión debido a que existe un detalle en el firewall, como puede ser la modificación del puerto, inhabilitar o denegar el acceso o una mala comunicación entre el puerto y el firewall (especificar en la regla de la habilitación si es UDP o TCP), de esta manera, queda comprobado que el firewall funciona de manera correcta con sus respectivas reglas.

## Conclusiones

El trabajo presentado en el presente documento cumple con el objetivo de configurar un sistema de seguridad hecho en una tarjeta Raspberry Pi 3 B+ para una red de sensores, la cual tiene como principal meta el cuidado de la información y la seguridad de los usuarios al hacer uso de una red protegida por medio de SSH, Firewall y el uso de una VPN, así como favorecer y comprobar que una tarjeta Raspberry Pi 3 B+ pueda ser un medio seguro para la ciberseguridad.

El proyecto presentado se realizó en etapas como lo son: la investigación, el análisis de los requerimientos, su implementación, la configuración de los protocolos y las fases de pruebas. Para destacar, el desarrollo y las pruebas de dicho trabajo se realizó mediante un sistema operativo Raspbian, el cual es un sistema operativo basado en la distribución de Linux llamada Debian, esto permitió un trabajo más optimizado por su forma de trabajo mediante instrucciones e interfaz gráfica lo que es vital para poder dar seguimiento en un tiempo para trabajos a futuros y de esta manera poder trabajar de manera más eficaz para permitir actualizaciones de seguridad informática basadas en la tarjeta Raspberry Pi 3B+

## Referencias

- Alva Maldonado, E. (2013). Desarrollo e implementación de una herramienta gráfica para la configuración remota de una VPN con routers Cisco. Pontificia Universidad Católica Del Perú. <http://tesis.pucp.edu.pe/repositorio/handle/123456789/4918>
- Álvarez Delgado, D., Jorquera Cáceres, C., Sepúlveda Jorquera, G., & Zamora Esquivel, C. (2014). Redes Privadas Virtuales (VPN). 9. <http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes Privadas Virtuales %28VPN%29.pdf>
- Areitio Bertolín, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Ediciones Paraninfo, SA.
- Arcentales, C., & Arcentales, G. (2020). Universidad Politécnica Salesiana Sede Guayaquil DIRECTOR. Revista EIA, ISSN 1794-1237, Volumen 17, 12–32. <http://dspace.ups.edu.ec/handle/123456789/10070>
- Canul, O. M. M. (2021). Desarrollo de un prototipo de redes de sensores para monitoreo de cenotes del estado de Quintana Roo implementado en Raspberry Pi 3 B+. Universidad de Quintana Roo
- CISCO. (2016). ¿Qué es un firewall? - Cisco. Recuperado de <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- CISCO. (2018). ¿Qué es un firewall? ¿Qué Es Un Firewall? recuperado de <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- David Reinares Lara. (2020). Origen e importancia de la ciberseguridad | OpenWebinars. 27 de Septiembre . Obtenido de <https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/>
- Del, A. A. (2020). DIRECCIONAMIENTO IP EN TUYA SA Autor ( es ) Christian Yohary Amaya Gómez Universidad de Antioquia Departamento Ingeniería Electrónica / Telecomunicaciones. 1–38.
- Fernandez Barcell, Manuel, U. de C. (2008). Introducción a las redes de sensores inalámbricas. Wireless Sensor Network, 1–20. <http://www.mfbarcell.es/conferencias/wsn.pdf>
- Fortinet. (n.d.). What Is a Proxy Firewall and How Does It Work? | Fortinet. Recuperado de <https://www.fortinet.com/resources/cyberglossary/proxy-firewall>
- Grado, T. F. I. N. D. E. (2022). Implementación de medidas de ciberseguridad en un vehículo conectado. Recuperado de <https://uvadoc.uva.es/handle/10324/57413>

- Hernández, R. Fernández C. y Baptista P. (2010). Metodología de la Investigación. México DF: Mc Graw Hil
- Ivan Belcic. (2019). ¿Qué es el malware y cómo funciona? | Definición de malware | Avast. recuperado de <https://www.avast.com/es-es/c-malware>
- Jefferson Omar Córdova Ledesma, R. A. (2018). Prototipo para gestión y monitoreo de la seguridad del laboratorio de científicos.
- Jornet Calomarde, R. (2018). Interfaz USB de red para acceso seguro basada en Raspberry Pi. Universitat Politècnica de València.
- Kaspersky. (2021, 1 de diciembre). Recuperado de ¿Qué es la ciberseguridad? [latam.kaspersky.com](https://latam.kaspersky.com)
- kaspersky. (2022). ¿Qué es la ciberseguridad? <https://Latam.Kaspersky.Com/Resource-Center/Definitions/What-Is-Cyber-Security>.
- Ledesma, J. O. C., & Jácome, R. A. F. (2018). Prototipo para gestión y monitoreo de la seguridad del laboratorio de interconectividad de la EPN usando Raspberry Pi. ESCUELA POLITÉCNICA NACIONAL.
- López Aldea, E. (2015). Arduino: guía práctica de fundamentos y simulación. Paracuellos de Jarama, Madrid, España: RA-MA Editorial. Recuperado el 16 de mayo de 2022 de [https://books.google.es/books?hl=es&lr=&id=Wo6fDwAAQBAJ&oi=fnd&pg=PP1&dq=L%C3%B3pez+Aldea,+E.+\(2015\).+Arduino:+gu%C3%ADa+pr%C3%A1ctica+de+fundamentos+y+simulaci%C3%B3n.+Paracuellos+de+Jarama,+Madrid,+Espa%C3%B1a:+RA-MA+Editorial.+Recuperado+el+16+de+mayo+de+2022+&ots=0I0ZkPdVsR&sig=xD97pSTP-ECOJ8JPnt5VzGWf7wc#v=onepage&q&f=false](https://books.google.es/books?hl=es&lr=&id=Wo6fDwAAQBAJ&oi=fnd&pg=PP1&dq=L%C3%B3pez+Aldea,+E.+(2015).+Arduino:+gu%C3%ADa+pr%C3%A1ctica+de+fundamentos+y+simulaci%C3%B3n.+Paracuellos+de+Jarama,+Madrid,+Espa%C3%B1a:+RA-MA+Editorial.+Recuperado+el+16+de+mayo+de+2022+&ots=0I0ZkPdVsR&sig=xD97pSTP-ECOJ8JPnt5VzGWf7wc#v=onepage&q&f=false)
- López Aldea, E. (2017). Raspberry Pi. Fundamentos y aplicaciones. Paracuellos de Jarama, Madrid, España: RA-MA Editorial. Recuperado el 16 de septiembre de 2022
- Lorena Fernández. (2020). Control de acceso: Qué es, características, tipos y su importancia en seguridad. BLOCK. Recuperado el 12 de octubre de <https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/>
- Marchionni, E. A. (2011). Administrador de servidores (Vol. 210). Recuperado el 02 de junio de <https://books.google.es/books?id=CfhGJ7yylRgC&lpg=PA34&ots=5J7lZQ1Rv7&dq=que%20es%20un%20firewall&lr&hl=es&pg=PA34#v=onepage&q=que%20es%20un%20firewall&f=false>
- Marín Valencia, J. J., Patiño Valencia, A., & Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. Revista Universidad Católica de Oriente, 31(45), 84–99. <https://doi.org/10.47286/01211463.284>

- Mario Luis Avila Pérez, I. A. (01 de Julio de 2021). Evaluación práctica de los protocolos Telnet y SSH. Gestión Competitividad e Innovación. Recuperado el 02 de Julio de <https://pca.edu.co/editorial/revistas/index.php/gci/article/view/133/126>
- MCM. (2021). ¿QUÉ ES UN FIREWALL DE NUEVA GENERACIÓN? Recuperado de <https://www.mcmtelcom.com/blog/negocios/que-es-un-firewall-de-nueva-generacion>
- Michelle, C. H. P., & Libeth, M. P. A. (2021). Desarrollo de un prototipo de un sistema de análisis y monitoreo de una red utilizando la herramienta open source snort para identificar las vulnerabilidades de la red y brindar seguridad a las conexiones de los diferentes dispositivos finales con servidor VPN y Raspberry Pi. UNIVERSIDAD DE GUAYAQUIL.
- Microsoft. (2013). Conceptos básicos sobre bases de datos. Soporte Access 2007. Recuperado de <https://support.microsoft.com/es-es/office/conceptos-básicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204>
- Miguel Soriano. (2002). Seguridad en redes Y seguridad. Recuperado el 1 de mayo de 2023 de [http://improvet.cvut.cz/project/download/C2ES/Seguridad\\_de\\_Red\\_e\\_Informacion.pdf](http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf).
- Olivo, D., & Lascano, S. (2020). ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO EVALUACIÓN DE TECNOLOGÍAS UTM ( UNIFIED THREATMENT MANAGEMENT ) Y NGFW ( NEXT GENERATION FIREWALL ) PARA DETECCIÓN DE VULNERABILIDADES EN LA RED.
- Online, T. H. P. (2021, agosto 30). ¿Qué es un firewall de red y cómo funciona? Www.hp.com. Recuperado de <https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona>
- Ortega, A. O. (2018). Enfoques de investigación. Extraído de [https://www.researchgate.net/profile/Alfredo\\_Otero\\_Ortega/publication/326905435\\_ENFOQUES\\_DE\\_INVESTIGACION\\_TABLA\\_DE\\_CONTENIDO\\_Contenido/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION-TABLA-DECONTENIDO-Contenido.pdf](https://www.researchgate.net/profile/Alfredo_Otero_Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION_TABLA_DE_CONTENIDO_Contenido/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION-TABLA-DECONTENIDO-Contenido.pdf) e114.
- Paguayo. (2019, febrero 14). ¿Que es Raspberry Pi? Raspberry Pi. recuperado de <https://raspberrypi.cl/que-es-raspberry/>
- Panda Security. (2015). Phishing: ¿qué es y como evitarlo? - Panda Security. In Revista. <https://www.pandasecurity.com/es/security-info/phishing/>
- Rasberrypi. (2018). Raspberry Pi 3 Modelo B+ – Raspberry Pi. <https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/>

- RBAC: ¿Qué es y cómo funciona el role based access control? - IONOS. (2020).  
<https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-role-based-access-control-rbac/>
- Ruiz, M. (2007). Gestión de usuarios y control de acceso basado en roles.
- Sanz Marcos, P. (2021). Estudio, diseño e implantación de un cortafuegos UTM libre para pequeñas organizaciones. Recuperado de  
<https://uvadoc.uva.es/bitstream/handle/10324/50441/TFG-G5281.pdf?sequence=1&isAllowed=y>
- Smaldone, J. (20 de enero de 2004). Obtenido de chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/http://ftp.nl.freebsd.org/ibiblio/docs/LuCaS/Tutoriales/doc-ssh-intro/introduccion\_ssh-0.2.pdf
- SoftwareLab.org. (2018). ¿Qué es un firewall? La definición y los tipos principales.  
<https://softwarelab.org/es/que-es-un-firewall/>
- Sotelo, M. I. (2021, diciembre 29). ¿Qué es un firewall? Tec Innova. Recuperado de  
<https://www.tec-innova.mx/que-es-un-firewall/>
- Staff Risoul. (s/f). ¿Qué es un firewall? Com.Mx. Recuperado el 4 de mayo de 2022, de  
<https://www.risoul.com.mx/blog/que-es-un-firewall>
- Stallings, W. (2004). Fundamentos de Seguridad en Redes Aplicaciones y Estándares, 2da Edición. Pearson Education.
- SPEC, G. (2022). ¿Cuáles son los tipos de control de acceso? Grupo SPEC. Recuperado de  
<https://www.grupospec.com/es/blog/91-tipos-control-acceso>
- Tekniker. (2019). Redes de sensores - TEKNIKER. <https://www.tekniker.es/es/redes-de-sensores>
- Velasco, M. Á. C., & Serrano, D. C. (2021). El libro del Hacker. Edición 2022. Anaya Multimedia.