Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA

Kevin Gerardo Rodas Pineda
Asesorado por el Ing. Edgar Francisco Rodas Robledo

Guatemala, marzo de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

KEVIN GERARDO RODAS PINEDA
ASESORADO POR EL ING. EDGAR FRANCISCO RODAS ROBLEDO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, MARZO DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Christian Daniel Estrada Santizo
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

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

DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 2 de agosto de 2017.

Kevin Gerardo Rodas Pineda

Guatemala 23 de julio de 2018

Ingeniero
Julio Cesar Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares,

Me permito dar aprobación al trabajo de graduación titulado **"Diseño de un sistema del control a distancia de una casa u oficina a través de VPN segura"**, del señor **Kevin Gerardo Rodas Pineda**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesor, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Ing. Edgar Francisco Rodas
Colegiado 8558
Asesor

Ing. Edgar Francisco Rodas R.
Ciencias y Sistemas
Colegiado 8558

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 85. 2018.
23 DE OCTUBRE 2018.

Señor Director
Ing. Otto Fernando Andrino González
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me **permito dar aprobación al trabajo de Graduación titulado: DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA, del estudiante; Kevin Gerardo Rodas Pineda, que cumple con los requisitos establecidos para tal fin.**

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCIÓN ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 85. 2018.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen el Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante: KEVIN GERARDO RODAS PINEDA titulado: DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA
DE IERIA
MECAN ECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 31 DE OCTUBRE 2018.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.148.2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica del trabajo de graduación titulado: **"DISEÑO DE UN SISTEMA DEL CONTROL A DISTANCIA DE UNA CASA U OFICINA A TRAVÉS DE VPN SEGURA"** presentado por el estudiante universitario: **Kevin Gerardo Rodas Pineda** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERÍA

Guatemala, Marzo de 2019

/echm

ACTO QUE DEDICO A:

Dios	Por darme la vida, sabiduría, fuerza, salud y permitirme crecer como persona y ser humano.
Mis padres	Gerardo Rodas y Alba Pineda, por ser las personas más importantes en mi vida, ser esos ejemplos que Dios me dio como guías y amigos apoyándome en todo momento. Los respeto, los aprecio y quiero con todo mi corazón.
Mis hermanas	Yadira y Andrea Rodas por ser mis amigas y compañeras incondicionales en todo momento, se los agradezco por ser parte importante dentro de mi carrera y compartir buenos y malos momentos.
Mis amigos	A todos quienes me han apoyado siempre a través de su amistad a lo largo de la carrera.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios en donde me he formado profesionalmente.
Ing. Francisco Rodas	Por su asesoramiento, confianza, amistad y apoyarme el desarrollo en este proyecto.
Nohelia Juares	Por su ayuda, confianza, cariño, amistad y apoyarme en el desarrollo de este proyecto.
Pueblo de Guatemala	Porque gracias al pueblo, pude seguir con mis estudios superiores.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
D1	Diodo semiconductor número 1
D2	Diodo semiconductor número 2
in1	Entrada 1
in2	Entrada 2
NC	Indicación de estado Normalmente cerrado
NO	Indicación de estado Normalmente abierto
IC	Referencia a circuito integrado
R1	Resistencia número 1
R2	Resistencia número 2
Q1	Transistor número 1
vcc	Voltaje de corriente continua

GLOSARIO

ACL Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

AES Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

Administración remota Funcionalidad de algunos programas que permiten realizar ciertos tipos de acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto.

Algoritmo Es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite llevar a cabo una actividad mediante pasos sucesivos que

	no generen dudas a quien deba hacer dicha actividad.
Aplicación	En informática, una aplicación es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas.
ARPANET	ARPANET fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos (DOD) para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales.
Autenticación	Autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador.
CHAP	CHAP es un método de autenticación usado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

Cifrado Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

COMM Conexión común o punto en común del circuito.

Debian Debian o Proyecto Debian es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra pre-compilado, empaquetado y en formato “deb” para múltiples arquitecturas de computador y para varios núcleos.

DES Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

DNS El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más

importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Enrutamiento

El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Básicamente se trata de encontrar la mejor ruta posible.

Firewall

Un corta-fuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o en una

	combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del corta-fuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.
GND	Palabra inglesa para hablar de un punto a Tierra.
Hardware	En informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.
HTML	HTML, sigla en inglés de HyperText Markup Language (lenguaje de marcas de hipertexto), hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado código HTML) para la definición de contenido de una página web, como texto, imágenes, videos, juegos, entre otros.
HTTP	El Protocolo de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol o HTTP) es el protocolo

de comunicación que permite las transferencias de información en la red informática mundial. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

HTTPS El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transport Protocol Secure o HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP. El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.

Internet El internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial.

IP El protocolo de internet (en inglés Internet protocol o IP) es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI.

ISO	La Organización Internacional de Normalización es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.
LAN	Local Área Network o red de área local en español, es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
MD5	MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Uno de sus usos es el de comprobar que algún archivo no haya sido modificado.
Nat	La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.
Navegador web	Un navegador web es un software, aplicación o programa que permite el acceso a la Web,

interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados. La funcionalidad básica de un navegador web es permitir la visualización de documentos de texto, posiblemente con recursos multimedia incrustados. Permite visitar páginas web y hacer actividades en ella, es decir, enlazar un sitio con otro, imprimir, enviar y recibir correo, entre otras funcionalidades más.

OSI Es un estándar desarrollado en 1980 por la ISO. Es una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de comunicaciones un dispositivo a otro sobre una red.

PHP PHP, acrónimo recursivo en inglés de PHP Hypertext Preprocessor (procesador de hipertexto), es un lenguaje de programación de propósito general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en un documento HTML en lugar, de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera el HTML resultante.

Protocolo de comunicación	Conjunto de reglas y estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red, como teléfonos o computadoras.
Puerto	En informática, un puerto es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos. La interfaz puede ser de tipo física (hardware) o puede ser a nivel lógico o de software, en cuyo caso se usa frecuentemente el término puerto lógico.
PAP	Password Authentication Protocol o PAP es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es un sub-protocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o passwords en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.
PPP	Protocolo punto a punto (PPP), es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún

	equipo u otro dispositivo de red entre medias de ambos.
Puerto lógico	Se denomina puerto lógico a una zona o localización de la memoria de acceso aleatorio (RAM) de la computadora que se asocia con un puerto físico o un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.
Radius	Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.
Raspbian	Raspbian es una distribución del sistema operativo GNU/Linux y por lo tanto libre basado en Debian Strech (Debian 9.4) para la placa computadora (SBC) Raspberry Pi, orientado a la enseñanza de informática. El lanzamiento inicial fue en junio de 2012.
Red Informática	Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Router	Un router o enrutador es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red o un switch), y que por tanto tienen prefijos de red distintos.
RSA	RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
Seguridad Informática	Área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.
Software	Según el estándar 729 de la IEEE. Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

SSH	Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera (también llamada backdoor). Permite manejar por completo el servidor mediante un intérprete de comandos. Se le asignó el puerto TCP 22.
Switch	Conmutador o Switch es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.
TCP/IP	Conjunto de protocolos de red en los que se basa internet y que permiten la transmisión de datos entre computadoras.
TCP	Es uno de los protocolos fundamentales en Internet. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

Tecnología Constituye un conjunto de conocimientos científicamente ordenados, que permiten diseñar y crear bienes o servicios que facilitan la adaptación al medio ambiente y la satisfacción de las necesidades esenciales y los deseos de la humanidad.

UDP Es un protocolo del nivel de transporte basado en el intercambio de datagramas, encapsulado de capa 4 o de Transporte del Modelo OSI. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, dado que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, porque no hay confirmación de entrega o recepción.

USB El Bus Universal en Serie (BUS) (en inglés: Universal Serial Bus), más conocido por la sigla USB, es un bus de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

Vulnerabilidades Son puntos débiles de un sistema informático, compuesto por hardware, software e incluso humanos, que permiten que un atacante comprometa

la integridad, disponibilidad o confidencialidad del mismo.

WAN Una red de área amplia, o WAN, (Wide Área Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet para proveer conexión a sus clientes.

Wifi El wifi es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi (tales como computadoras personales, teléfonos, televisores, videoconsolas, reproductores de música, etc.) pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica.

RESUMEN

Es impresionante la demanda, en los últimos años, de sistemas de seguridad informática en todas las grandes, medianas y micro empresas sin importar el giro de negocio que se tenga, hoy en día toda empresa necesita el acceso a Internet para agilizar su producción y efectividad, y no menos importante es también el acceso a Internet en una casa o en oficina. Con el mundo del Internet incluso muchos trabajos se desarrollan desde la comodidad del hogar. Con esto se va generando un nuevo mundo y una nueva tendencia en la que todo dispositivo eléctrico tiende a poseer una conexión al mundo de la Internet o también llamado el Internet de la cosas.

Cada día los dispositivos que utilizamos cotidianamente como el televisor, microondas, refrigerador e incluso la iluminación, van mejorando de una forma en las que van adquiriendo nuevas características, como su integración con aplicaciones móviles, su acceso a Internet para ejecutar ciertas acciones, entre otras. Estas nuevas características hacen que los nuevos dispositivos sean capaces de realizar nuevas o mejoradas tareas e incluso que puedan ser manipuladas a distancia.

Con estas mejoras también los sistemas se van volviendo objetivos de ataques o blancos para quebrantar la funcionalidad de los mismos y más, si estos sistemas son capaces de acceder a una red interna o pública como Internet, es por ello que se deben crear o desarrollar sistemas seguros y confiables ante las amenazas continuas.

El sistema de control de dispositivos cotidianos promete ser eficiente en cuanto al aprovechamiento de recursos y ha satisfecho de cierta forma, las velocidades del usuario en cuanto a cobertura e información del sistema a controlar en tiempo real. Basando en la velocidad de transmisión que se desea ofrecer al usuario, el sistema de control y seguridad para una casa u oficina que se va a proporcionar, obtiene el mayor porcentaje de eficiencia posible.

El desarrollo de este estudio se logró hacer de manera exitosa, se obtuvieron los recursos previos que se listan en este documento por lo que esta tesis también representa una base para futuros estudios para la domótica.

La parte de control de todo el sistema estará embebida en una Raspberry Pi, que es donde estarán todos los algoritmos de programación, para la correcta activación y puesta a punto del proyecto. Llevando a cabo todo la parte lógica del proyecto. Siendo completado con la parte de potencia que será la encargada de manejar las tareas finales, haciendo uso de un diseño de circuito electrónico.

OBJETIVOS

General

Proponer un sistema de control a distancia de una casa u oficina a través de VPN segura.

Específicos

1. Presentar los diferentes tipos de VPN que permiten una comunicación segura a través del establecimiento de un túnel cifrado.

2. Describir una estrategia de conexión, control y manejo de los diferentes dispositivos del sistema.

3. Enseñar el modelo teórico del sistema que permite ejecutar una acción sobre un dispositivo a controlar a través de una interface gráfica.

INTRODUCCIÓN

El uso de Internet ha adquirido un gran auge en los últimos años, hoy en día el poseer una conexión a Internet ya no es un servicio que únicamente las empresas utilizan, su uso se ha expandido a tal punto que cada casa, oficina o pequeño negocio tienen un dispositivo con acceso a la red pública, esto abre un mundo de posibilidades para el desarrollo de proyectos que sean efectivos y ayuden a realizar un mejor trabajo.

La presente investigación propone un sistema para el control de cierta cantidad de dispositivos de una casa, desde la iluminación con el encendido y apagado de los mismos, activación o desactivación de un portón eléctrico, acceso a cámaras de vigilancia, entre otros. Esto utilizando como medio de comunicación el Internet, estableciendo una conexión segura a través de un túnel cifrado de VPN, garantizando integridad, confiabilidad, disponibilidad y confidencialidad de los datos o procesos a manejar; la conexión se realizará utilizando un servidor de VPN que será montado sobre una pequeña computadora llamada Raspberry Pi, esta a su vez controla el circuito electrónico haciendo uso de una interfaz web que tendrá comunicación con los dispositivos finales, ya sea iluminación, motor del portón eléctrico o cámaras de vigilancia. Para tener acceso al manejo de los dispositivos finales, será necesario realizar previamente una autenticación para la creación del túnel de VPN, garantizando su uso únicamente a los usuarios autorizados.

El sector de telecomunicaciones en Guatemala aporta importantes recursos no solo económicos sino también tecnológicos, contribuyendo al crecimiento del país en materia de oportunidades de acceso al manejo de nuevas tecnologías.

.

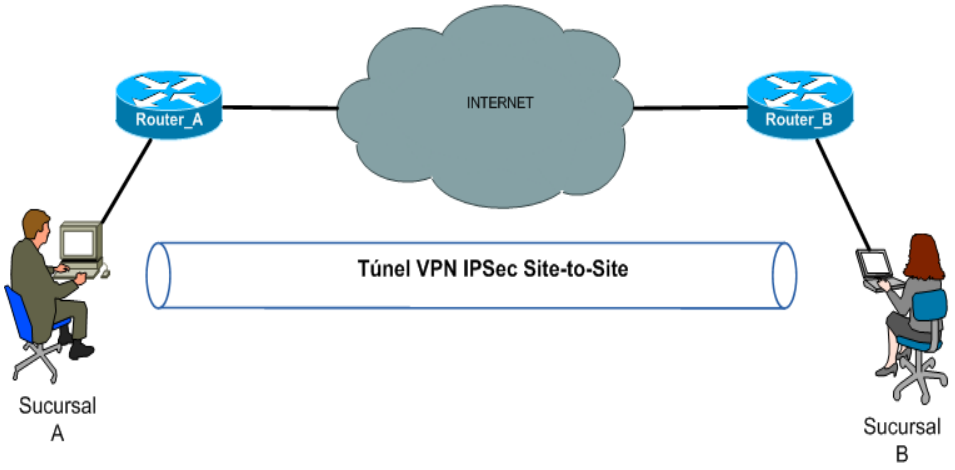
1. RED PRIVADA VIRTUAL (VPN)

Una Red Privada Virtual, es una red que crea un túnel capaz de conectar dos o más dispositivos como si estos se encontrasen físicamente en el mismo lugar, esta red virtual emula una conexión privada local. Permite que las computadoras en la red envíen y reciban datos sobre redes públicas como si esta fuera una red privada con todas las funcionalidades de la misma.

Una conexión a través de VPN, es considerada una unión Wide Área Network (WAN, en español, Red de Área Amplia), esto entre los sitios remotos que establecen el túnel virtual, y los usuarios experimentan como si se tratara de un enlace dedicado o privado.

Esta conexión permitirá agregar al proyecto una capa de seguridad debido a que brindara un nivel de cifrado al tráfico, siendo esto de vital importancia porque se estará trabajando con accesos e información críticos.

Figura 1. **Conexión Red Privada Virtual (VPN)**



Fuente: REDESCISCO. *Conexión de una red privada virtual*. http://www.redescisco.net/images/VPN1.png. Consulta: 12 de marzo de 2018.

1.1. Historia de una Red Privada Virtual

La Red Privada Virtual conecta ubicaciones remotas a través de una red pública con esto se puede decir que el Internet comenzó como una investigación sobre un método electrónico para comunicarse con ubicaciones remotas, esto comenzó en la década de 1960 por la inteligencia militar de Estados Unidos. Ellos crearon una red de conmutación de paquetes llamada ARPANET (Advanced Research Projects Agency Network) y el primer uso de TCP/IP. TCP/IP significa Transfer Control Protocol/Internet Protocol, las dos unidades funcionales de la primera red de redes que dieron inicio al internet y con ello la investigación de las comunicaciones cifradas.

El conjunto de protocolos TCP/IP estableció un estándar para las redes de ordenadores como se conocen hoy en día. Al final esta investigación condujo a la institución de la Familia de Protocolos de Internet como un estándar de comunicación militar en 1982 y luego la adopción del estándar por la industria de informática comercial en 1985.

Los protocolos TCP/IP detallan cómo toda la información se empaqueta, aborda, transmite y recibe a través de internet. Esta trabaja en 4 capas; enlace, internet, transporte y aplicación. La capa de enlace es donde los dispositivos dentro de una red funcionan y donde están más seguras. La capa de internet es donde las redes locales y dispositivos se conectan a otros sitios web y a internet en general, y donde corren el mayor riesgo. Cuando los paquetes de datos son enviados desde una red local a una red de destino, el paquete se marca con información identificando dónde se originó y hacia dónde se dirige. La comunicación funciona perfectamente, pero es deficiente en cuanto a que es vulnerable en cuanto a que pueden monitorear el tráfico, interceptar los datos e incluso seguir el flujo de datos de nuevo a la fuente e identificarlo.

La tecnología de seguridad fue investigada por primera vez en 1993 por John Ioannidis y sus contemporáneos como Matt Blaze en grupos de reflexión como la Universidad de Columbia y AT&T Bell Labs. Su trabajo condujo al Software IP Encryption Protocol, también conocido como SWIPE, la primera forma de VPN. Fue un trabajo experimental que pretendía proporcionar confidencialidad, integridad y autenticación para los usuarios de la red.

A raíz de esto el trabajo se fue mejorando y se centró en la seguridad IP y se mejoró los protocolos IP que, finalmente, condujeron al desarrollo del sistema IPsec.

IPsec es una familia de protocolos de seguridad de internet que autentica y cifra cada paquete de información compartido a través de internet. A medida que la tecnología fue avanzando, de la misma manera lo hizo la velocidad de la conexión.

1.2. Tipos de Red Privada Virtuales

Es posible clasificar una Red Privada Virtual por el método de acceso físico a la red remota, esto es decir, si un usuario se conecta desde una oficina, un centro comercial, otra red corporativa o desde una red propiamente interna de la empresa. Es por ello que a continuación se describen los tipos de Red Privadas Virtuales:

1.2.1. VPN de acceso remoto

Es posiblemente el modelo más utilizado en la actualidad, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos ya sea estos oficinas, comerciales, domicilios, hoteles, aviones preparados, etcétera. Utilizando teléfonos móviles, ordenadores portátiles y/o tablets entre otros, por supuesto, utilizando Internet como vínculo de acceso. Una vez realizada la conexión estos usuarios tienen un nivel de acceso muy similar al que tienen en la red local de la empresa u oficina.

1.2.2. VPN punto a punto

Este esquema es utilizado para conectar oficinas remotas ya sea con la sede central de la organización o con otras organizaciones. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN.

Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales o también llamados enlaces dedicados (realizados comúnmente mediante conexiones de cable o fibras físicas entre los nodos), sobre todo en las comunicaciones internacionales.

Una VPN de sitio a sitio, también llamada VPN de router a router, se usa mayormente en operaciones corporativas. Debido al hecho de que muchas empresas tienen oficinas ubicadas dentro y fuera del país, una VPN de sitio a sitio se utiliza para conectar la red de la oficina principal con otras oficinas diferentes.

1.2.3. Tunneling

La técnica de *tunneling* consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo), determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil, porque se necesita que los paquetes conserven su estructura y contenido original como su dirección IP de origen y destino, sus puertos, etc.

1.2.4. VPN sobre LAN

Este esquema es muy utilizado dentro de las empresas. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN), de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi) e incluso las redes cableadas.

Un ejemplo clásico es un servidor con información sensible, ubicado detrás de un equipo VPN, y provee autenticación adicional más el agregado del cifrado, haciendo posible que solamente el personal habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

1.3. Protocolos para la creación de Redes Privadas Virtuales

Para la creación de VPNs es posible utilizar varios tipos de protocolos los cuales serán utilizados dependiendo las necesidades o requerimientos que se tenga. Los protocolos tienen diferentes niveles de seguridad, desde los más sencillos que son los más fáciles de configurar hasta los más complejos en los que el nivel de configuración es mayor.

1.3.1. Protocolo IPSec

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP), autenticando y cifrando cada paquete IP en un flujo de datos, este también incluye protocolos para el establecimiento de claves de cifrado. IPsec actúa en la capa de red, la capa 3 del modelo OSI, esto hace que IPsec sea más flexible, y pueda ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA), como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros o se puede decir que son las claves que se están usando, para cifrar y autenticar un flujo particular en una dirección. En el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación de los cuales existe una lista definida, le corresponde al administrador de la VPN IPsec.

El uso de IPsec fue proyectado para proporcionar seguridad en dos diferentes modos de operación, uno es el modo transporte (extremo a extremo), del tráfico de paquetes, en el los ordenadores de los extremos finales realizan

el procesado de seguridad, y el modo túnel (puerta a puerta), en el la seguridad del tráfico de paquetes es proporcionada a varias máquinas o incluso a toda la red de área local por un único nodo.

IPsec puede utilizarse para crear VPNs en los dos modos, pero hay que tener en cuenta, que las implicaciones de seguridad son bastante diferentes entre los dos modos de operación.

1.3.1.1. Modo transporte

En modo transporte, sólo la carga útil, es decir los datos que se transfieren del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, porque eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera, por ejemplo traduciendo los números de puerto TCP y UDP. El modo transporte es utilizado para comunicaciones ordenador a ordenador.

1.3.1.2. Modo túnel

En el modo túnel, todo el paquete IP es decir, datos más cabeceras del mensaje, es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red, túneles seguros entre routers para VPNs o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

1.3.1.3. Protocolos

IPsec consta de tres protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- Authentication Header (AH), proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

- Encapsulating Security Payload (ESP), proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.

- Internet key exchange (IKE), emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión. Se suelen usar sistemas de Criptografía de clave pública o clave pre-compartida.

1.3.2. PPTP (Point to Point Tunneling Protocol)

PPTP es la abreviatura de Protocolo de Túnel Punto a Punto (en inglés, Point-to-Point Tunneling Protocol y permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET.

Como su nombre lo indica, una VPN PPTP crea un túnel y captura los datos. Las VPN PPTP son empleadas por usuarios remotos para conectarse a la red de VPN mediante su red de internet existente. Resulta útil para empresas

y uso hogareño. Para acceder a la VPN, los usuarios inician sesión con una contraseña aprobada. Las VPN PPTP son ideales, para uso personal y empresarial porque no requieren la compra o instalación de hardware adicional y funciones habitualmente ofrecidas, como programas complementarios baratos. Las VPN PPTP se usan ampliamente también por su compatibilidad con Windows, Mac y Linux.

La tecnología PPTP encapsula los paquetes ppp en un tunel GRE, que se transporta en paquetes IP, para su transmisión mediante un tunel en la red y se hace uso de un canal de control del tunel, en el puerto 1723 TCP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPNs sobre public-switched telephone networks (PSTNs), que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

Aunque parezca tener muchos beneficios, hay una desventaja de esta VPN, y es que no brinda codificación, que es usualmente la razón por la que se conseguiría una VPN, esto quiere decir que tiene un cierto nivel más bajo de seguridad. Otra desventaja es que depende del PPP o Protocolo de Punto a Punto para implementar medidas de seguridad.

1.3.3. L2TP (Layer to Tunneling Protocol)

L2TP es la abreviatura de Protocolo de Establecimiento de Túneles (en inglés, Layer to Tunneling Protocol), y fue desarrollado por Microsoft y Cisco.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a la VPN PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas esto significa que, el nivel de seguridad no es muy alto porque:

- Sólo se realiza autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.

- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control, que den por acabado el túnel L2TP o la conexión PPP subyacente.

- L2TP no cifra en principio el tráfico de datos de usuario, esto puede dar problemas cuando sea importante mantener la confidencialidad de los datos.

- A pesar de que la información contenida en los paquetes PiPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

Debido a los riesgos de seguridad que supone el uso de la VPN L2TP, se consideró la opción de crear un nuevo conjunto de protocolos para esta VPN, pero debido al trabajo que esto conllevaría, se tomó la decisión de usar los mismos protocolos de VPN IPsec para proteger los datos que viajan por el túnel L2TP.

L2TP es en realidad una variación o combinación de un protocolo de encapsulamiento IP. Una VPN L2TP forma un túnel entre dos puntos de conexión L2TP, y otra VPN como el protocolo IPSec encripta los datos y se focaliza en asegurar la comunicación entre los túneles.

1.3.4. SSL/TLS

Transport Layer Security (TLS; en español «seguridad de la capa de transporte»), y Secure Sockets Layer (SSL; en español «capa de puertos seguros») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. Ambas funcionan como un protocolo, utilizadas para crear una conexión VPN.

Se usan certificados X.509 y criptografía asimétrica para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica. Esta sesión se utiliza para cifrar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, y códigos de autenticación

de mensajes para integridad y como un producto lateral, autenticación del mensaje. Varias versiones del protocolo están en aplicaciones ampliamente utilizadas como navegación web, correo electrónico, fax por Internet, mensajería instantánea, y voz-sobre-IP (VoIP).

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL conlleva una serie de fases o pasos básicos:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard).

- Con funciones hash: MD5 o de la familia SHA.

Se trata de una conexión de VPN donde el navegador web funciona como cliente, y el acceso del usuario está restringido a aplicaciones específicas en lugar de poder acceder a toda la red. Una VPN SSL y TLS brinda una sesión segura desde el navegador de la PC hacia el servidor de la aplicación. Esto se debe a que los navegadores web cambian a SSL fácilmente y casi no requieren ninguna acción por parte del usuario. Los navegadores ya vienen con SSL y TLS integrado.

1.4. Usos y ventajas de utilizar VPNs

Las conexiones VPN lo que permiten es crear una red local sin necesidad que sus participantes estén físicamente conectados entre sí, sino a través de Internet u otra red. Esta característica agrega un buen número de usos y ventajas en las VPN.

El uso más común de una conexión VPN es la posibilidad de interconectar redes que no se encuentran físicamente conectadas, como sería el caso de una empresa que desea comunicar varias sucursales ubicadas en diferentes puntos geográficos o el caso de trabajadores, que no se encuentran físicamente en determinado momento en la oficina, pero que necesitan acceder a la red de la corporación.

Realizar una conexión de este tipo agrega una gran ventaja para las empresas o las personas que lo estén utilizando, porque se agrega un nivel más de seguridad a la conexión, permitiendo crear un túnel que se encargará de transportar, autenticar y cifrar los datos que por allí transiten. De esta manera las sucursales de una empresa o sus trabajadores, trabajaran de una

forma segura y experimentaran una conexión como si fuera local. Por ejemplo si el usuario se encuentra en una red Wifi de acceso público utilizar una conexión VPN será más seguro que conectarse solamente a la red pública, porque utilizaría la conexión VPN para realizar la navegación a los sitios y la red Wifi se utilizaría para formar el túnel.

El uso de una conexión VPN puede ir variando dependiente el tipo de necesidad que se tenga y el nivel de seguridad que se desea agregar, porque se podría usar para conectarse a las cámaras de una vivienda y mantener el monitoreo sobre un túnel cifrado, realizar una conexión a un servidor con datos importantes, comunicarse con un minicomputador que maneje los motores de los portones eléctricos de una casa, el alumbrado eléctrico de la misma, incluso en sistemas de riego de jardines u agrícola que se manejan remoto.

Otro uso que se está dando a las conexiones VPN pero que no va orientado tanto a beneficios laborales o de domótica es la evasión de bloqueos geográficos, es decir en algunos países o regiones se permite el acceso de cierto contenido únicamente a los habitantes de esa región, y al utilizar la propiedad de la conexión VPN de simular una conexión local, para los servidores se hace de cuenta que te encuentras físicamente conectado dentro de la región permitida, esto lo hacen básicamente los usuarios para obtener contenido censurado o bloqueados para un país.

Dentro de las ventajas de usar una conexión VPN están:

- La compatibilidad con casi todos los dispositivos móviles, es decir laptops, celulares, *tablets,* entre otros.

- Compatibilidad con todas las aplicaciones, porque en ruta todo el tráfico hacia el servidor VPN.

- Una vez se encuentra configurada la conexión VPN, se puede conectar y desconectar en cualquier momento.

- Como se mencionaba, agrega una capa de seguridad más, permitiendo cifrar las comunicaciones y los datos.

- Aunque su uso no este orientado al ámbito laboral o de domótica, permite evadir bloqueos regionales de contenido.

- Dependiendo la necesidad que se tenga o el uso que se quiera dar a la conexión VPN, estas no son tan difíciles de configurar.

- En cuestión de precios, puedes construir tu propio servidor de VPN con materiales en casa o compara soluciones que se dedican a realizar este tipo de conexiones. Esto dependerá de la posibilidad de la empresa o el usuario.

- Es compatible con básicamente todos los sistemas operativos, iOS, Android, Windows, Unix, etc.

- Las conexiones VPN reducen los costos y son sencillas de usar.

1.5. Equipos para la creación de conexiones VPN

La utilidad de las conexiones VPN y las ventajas que estas conllevan, existen varios métodos de poder acceder a este tipo de conexiones, que van

desde los más bajo hasta los más elevado en precios. Esto de igual forma dependerá de las necesidades que se requieran. Incluso se puede crear un concentrador de conexiones VPN gratuito y creado en casa. Para la creación de una conexión VPN debe existir un servidor que se encargue de concentrar las conexiones, que guarde las claves o certificados, el que guardara todo la parte de configuración necesaria para establecer el túnel, que sea el receptor a la conexión de los clientes que se conectaran y todo lo que esto conlleva, cabe mencionar que para la conexión VPN a parte del servidor es necesario tener conexión a internet y un servicio de IP pública o un servicio de DNS Dinámico.

Las opciones de servidor que existen para la creación de una conexión VPN están:

- Software gratuito: Computadora con un sistema operativo instalado, este puede ser Windows o una versión de Linux, normalmente este tipo de servidor de VPN es muy accesible y configurable, se hace uso de un software como OpenVPN, y se instala sobre el sistema operativo y únicamente se debe tener un ligero conocimiento sobre la configuración de una conexión VPN, esto lo hace una solución sencilla y económica. Este tipo de solución es mayormente utilizado en proyectos de domótica, oficina o micro empresas.

- Minicomputadoras como servidores de VPN: es el mismo concepto que el anterior, pero cabe mencionar que es necesario adquirir la minicomputadora como por ejemplo una Raspberry Pi, esta agrega cierto valor a la inversión y se requiere un conocimiento mayor, para el manejo de estos dispositivos, pero el concepto de instalación de un software que se encarga de generar los protocolos de comunicación, sigue siendo necesario.

- Router o Firewall Virtuales: Se debe poseer un hardware para la instalación del software del Router o Firewall, existen varios software que son gratuitos pero son escasos en funcionalidades. Una solución es utilizar versiones demo de los fabricantes que normalmente tienen descargas al público de sus soluciones. El problema es que normalmente estas versiones demo tienen un tiempo límite de uso, y se debe tener conocimiento de la funcionalidad de sus productos. Normalmente el valor de licencia de estos productos suelen ser elevados, aunque las funcionalidades son mucho mejores.

- Router o Firewall dedicados: Estos básicamente son equipos dedicados a realizar una función de red, incluyen varias características como ruteos, políticas, ACLs, Nats, Dashboards, entre otros. Existen de varios fabricantes, desde los más conocidos que son los más cotizados pero de mayor precio, hasta las nuevas marcas que realizan básicamente las mismas funciones pero a precios más accesibles. Las versiones de más pequeñas de estos equipos son perfectas para proyectos de domótica, oficina o micro empresas que no requieren demasiadas conexiones. Son más estables y solamente se requiere un poco de conocimiento dependiendo el fabricante, aunque usualmente suelen ser bastante intuitivos para su configuración.

1.6. OpenVPN

(Secure Sockets Layer), VPN Virtual Private Network (red virtual privada). Su lanzamiento inicial fue el 23 de marzo de 2002, esta plataforma está desarrollada sobre el lenguaje de programación C y tiene un sistema operativo multiplataforma. Ser una herramienta multiplataforma ha hecho que se simplifique la configuración de VPN's frente a otras más antiguas y difíciles de

configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología. Ofrece una combinación de seguridad, facilidad de uso y riqueza de características, lo que hace que sea una herramienta muy atractiva para para proyectos de VPNs. OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente. Resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11), y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

Para cifrar datos de una VPN se usan Passwords o claves de cifrado. OpenVPN tiene dos modos de cifrar considerados seguros, uno que está basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA.

Cuando ambos lados usan la misma clave para cifrar y descifrar los datos es decir cliente y servidor, estamos usando el mecanismo conocido como “clave simétrica” y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN, lo que significa que todas las maquinas podrán verse entre sí, o bien dicho hablaran el mismo idioma. Si bien SSL/TLS + claves RSA no es considerada la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad.

1.6.1. Ventajas y desventajas de OpenVPN

Se presenta las ventajas y desventajas de utiliza OpenVPN.

- Ventajas

- OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de IPsec.
- Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).
- Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, sólo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.
- Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y como servidor (simplemente esperando conexiones entrantes), o como cliente (iniciando conexiones).
- Sólo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.
- Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.
- Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.
- Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.

- Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.
- Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.
- Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son muy simples.
- Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

- Desventajas

  - No tiene compatibilidad con IPsec que es el actual estándar para soluciones VPN.
  - Todavía son relativamente pocos los que saben cómo usar OpenVPN.
  - A día de hoy mayormente se puede conectar a otras computadoras o dispositivos con IOS y Android .3 Sin embargo, esto está cambiando, dado que existen compañías desarrollando dispositivos con clientes OpenVPN integrados y haciendo llegar esta tecnología a otros ámbitos como la automatización industrial.

2. RASPBERRY PI

Raspberry Pi es un proyecto desarrollado con el objetivo de estimular el estudio y enseñanza de la computación en escuelas. Y básicamente es una computadora en una pequeña placa o placa reducida, que incluye todas funcionalidades de una computadora de tamaño normal de escritorio. Este proyecto fue desarrollado en Reino Unido por la fundación que lleva su mismo nombre “Fundación Raspeberry Pi”. Esta fundación permite el uso libre tanto a nivel educativo como particular de la Raspberry Pi, se puede adquirir fácilmente, con algún tipo de distribuidor o pueden pedirse desde internet.

2.1. Modelos

Existe varios modelos que pueden ser adquiridos dependiendo el tipo de necesidad o proyecto a realizar, cada modelo tiene diferentes características ya sea en memoria, CPU, o puertos de conexión.

2.1.1. Raspberry Pi 1 Modelo A

Este fue el primer modelo lanzado de Raspberry. No posee puerto Ethernet, por lo que para su conexión a Internet requiere de un adaptador Wi-Fi por USB. Tiene 26 conectores GPIO, salida de vídeo vía HDMI y Video RCA, un conector Jack de 3.5 milimetros, un único conector USB, MicroUSB (De alimentación), y un conector de cámara. Su procesador es un Broadcom BCM2835, Single-Core a 700MHz. También tiene 256 MB de RAM y una gráfica Broadcom VideoCore IV. Requiere de una fuente de alimentación de 5 voltios y

2 amperios, elemento común al resto de versiones. Su lanzamiento fue en el año 2012.

2.1.2. Raspberry Pi 1 Modelo B y B+

Es una variante del Modelo A, trajo consigo diversas mejoras, la inclusión del doble de memoria RAM, pasando de 256MB a 512MB. Trajo consigo un puerto USB más, un conector Ethernet (RJ-45), y se mantuvo su tamaño. No hubo variaciones ni en el procesador ni en la parte gráfica. Tiempo después se lanzó el Modelo B+, que incluyó 4 puertos USB y pasó de usar una SD a una MicroSD. Estos modelos fueron lanzados en 2012.

2.1.3. Raspberry Pi 2 Modelo B

Es el primer modelo que no incluye el mismo procesador usado en los tres anteriores: se sustituye por uno de la misma marca, pero de modelo BCM2836. Paso de tener un solo núcleo a cuatro nucleos, y de 700MHz a 900MHz. No obstante emplea la misma gráfica, la VideoCore IV. Dobla la cantidad de memoria RAM, pasando de 512MB a 1GB, esta memoria está compartida con la gráfica. También incluye 40 pines GPIO, y mantiene los cuatro puertos USB y se Suprime la conexión RCA. Este modelo fue lanzado en el año 2014.

2.1.4. Raspberry Pi 3 Modelo B

Renueva su procesador, con la compañía Broadcom, una vez más un Quad-Core, pero pasa de 900MHz a 1.20GHz. Mantiene la RAM en 1GB. Su mayor novedad fue la inclusión de Wi-Fi y Bluetooth (4.1 Low Energy), sin necesidad de adaptadores. Su lanzamiento se realizó en el año 2016.

2.2. Características de la Raspberry Pi

A continuación se detalla los diferentes modelos de Raspberry Pi disponibles en el mercado y las características correspondientes de cada modelo, los cambios son en procesador, memoria RAM, puertos disponibles, periféricos de bajo nivel (GPIO), entre otros las dimensiones son básicamente las mismas.

Tabla I. **Características de la Raspberry Pi**

	Raspberry Pi 1 Modelo A	**Raspberry Pi 1 Modelo B**	**Raspberry Pi 1 Modelo B+**	**Raspberry Pi 2 Modelo B**	**Raspberry Pi 3 Modelo B**
SoC:	Broadcom BCM2835 (CPU + GPU + DSP + SDRAM + puerto USB).			Broadcom BCM2836 (CPU + GPU + DSP + SDRAM + Puerto USB).	Broadcom BCM2837 (CPU + GPU + DSP + SDRAM + Puerto USB).
CPU:	ARM 1176JZF-S a 700 MHz (familia ARM11).			900 MHz quad-core ARM Cortex A7.	1.2GHz 64-bi quad-core ARMv8.

Continuación tabla I.

Juego de instruc-ciones:	RISC de 32 bits		RISC de 64 bits
GPU:	Broadcom Video Core IV,, OpenGL ES 2.0, MPEG-2 y VC-1 (con licencia), 1080p30 H.264/MPEG-4 AVC.		
Memoria (SDRAM):	256 MiB(compartidos con la GPU).	512 MiB (compartidos con la GPU) desde el 15 de octubre de 2012.	1 GB (compartidos con la GPU).
Puertos USB2.0:	1	2 (vía hub USB integrado).	4
Entradas de vídeo:	Conector MIPI CSI que permite instalar un módulo de cámara desarrollado por la RPF.		
Salidas de vídeo:	Conector RCA (PAL y NTSC), HDMI (rev1.3 y 1.4), Interfaz DSI para panel LCD.		
Salidas de audio:	Conector de 3.5 mm, HDMI		
Almacenamiento integrado:	SD / MMC / ranura para SDIO.	MicroSD	

Continuación tabla I.

Conectividad de red:	Ninguna	10/100 Ethernet (RJ-45) via hub USB		10/100 Ethernet (RJ-45) vía hub USB, Wifi 802.11n, Bluetooth 4.1.
Periféricos de bajo nivel:	8 x GPIO, SPI, I²C, UART		17 x GPIO y un bus HAT ID	
Reloj en tiempo real:	Ninguno			
Consumo energé-tico:	500 mA, (2.5 W)	700 mA, (3.5 W)	600 mA, (3.0 W)	800 mA, (4.0 W)
Fuente de alimen-tación:	5 V vía Micro USB o GPIO header			
Dimen-siones:	85.60mm × 53.98mm (3.370 × 2.125 inch)			
Siste-mas opera-tivos soporta-dos:	GNU/Linux: Debian (Raspbian), Fedora (Pidora), Arch Linux (Arch Linux ARM), Slackware Linux, SUSE Linux Enterprise Server for ARM. RISC OS			

Fuente: Wikipedia. *Raspberry Pi*. https://es.wikipedia.org/wiki/Raspberry_Pi. Consulta: 05 de octubre de 2017.

2.3. Sistemas operativos soportados

Aunque el sistema operativo más utilizado para esta minicomputadora es Raspbian, y es una versión modificada del sistema operativo Debian, existen otros sistemas operativos que son soportados por Rasberry Pi, esto también dependerá del proyecto que se desea realizar o las necesidades que se tengan, a continuación un listado de los sistemas operativos soportados o en los que se está trabajando para que sean soportados.

2.3.1. Sistemas operativos completos

Se les llama sistemas operativos completos porque su ejecución es más pesada, es decir que requieren muchos más recursos de la máquina para su funcionamiento.

- AROS

- GNU/Linux para procesador ARM

    - Android97
    - Arch Linux ARM
    - Debian Whezzy Soft-Float, versión de Debian sin soporte para coma flotante por hardware
    - DietPi, distribución ligera basada en Raspbian y de sencilla configuración mediante menús
    - Firefox OS
    - Gentoo Linux98
    - Google Chromium OS
    - Kali Linux

- Open webOS99
- PiBang Linux,100 distribución Linux derivada de Raspbian con diferente escritorio y aplicaciones
- Pidora, versión Fedora Remix optimizada101
- QtonPi, distribución linux con un framework de aplicaciones multiplataforma basado en Qt framework
    - Raspbian,102 versión de Debian Wheezy para ARMv6 con soporte para coma flotante por hardware
    - Slackware ARM, también conocida como ARMedslack
    - Ubuntu MATE
    - Void Linux

- Plan 9 from Bell Labs103104

- RISC OS 52

- Unix

    - FreeBSD105
    - NetBSD106107

- Windows 10

    - Windows CE

2.3.2. Sistemas operativos ligeros multipropósito

Como su nombre lo indica este tipo de sistema operativo es más ligero para el minicomputador, es decir que hacer mejor uso de los recursos del

computador, estas versiones regularmente no traen interfaz gráfica para ahorrar recursos como CPU, Memoria Ram y Video, es decir el manejo se hace a través de un CLI (Command Line Interface), entre los más utilizados se encuentra:

- Minibian, distribución ligera basada en Raspbian
- Moebius, distribución ligera ARM HF basada en Debian que usa el repositorio de Raspbian y que cabe en una tarjeta SD de 1GB, usa pocos servicios y está optimizada para usar poca memoria.
- Squeezed Arm Puppy, una versión de Puppy Linux (Puppi) para ARMv6 (sap6) específicamente para Raspberry Pi.

2.3.3. Sistemas operativos ligeros de único propósito

Este tipo de sistema operativo está dedicado a realizar un único proceso o tarea, al igual que los sistemas operativos ligeros, hacen un mayor aprovechamiento de los recursos para dedicarlos a un solo propósito, como por ejemplo una central telefónica.

- Instant WebKiosk, sistema operativo con solo un navegador
- IPFire
- Micro Elastix, solución de código abierto para comunicaciones unificadas, centrales telefónicas
- OpenELEC
- LibreELEC
- OSMC
- Raspbmc
- Xbian

2.4. Ventajas y usos de las minicomputadoras

Desde el lanzamiento de la Raspberry Pi su principal objetivo era el promover la educación de las ciencias informáticas en escuelas y universidades, pero con el paso del tiempo se ha demostrado que el uso de estas pequeñas computadoras no se limita a dicho objetivo. Se pueden encontrar diversos proyectos que utilizan como dispositivo principal las mini computadoras, realizando proyectos como, centrales telefónicas, utilizadas también en automatización de procesos en la grandes industrias, soluciones para el hogar (domótica), proyectos universitarios, servidores WEB, servidores de VPN, lo que lleva a la conclusión de que Raspberry Pi no se limita solamente a proyectos de hogar y ciencias, sino que puede ser ampliamente utilizado como solución IoT de manera industrial y alcanzar los objetivos de la Industria.

Dentro de sus ventajas se encuentra su pequeño tamaño, y es una ventaja en cuanto a la ocupación de un espacio, y debido al mismo tamaño es fácil de encontrar un lugar dedicado para el mismo, fácil para mover de un lado a otro, y lo puede hacer un dispositivo portátil únicamente agregando una batería para su alimentación.

Algo importante a considerar dentro de sus ventajas, es su bajo coste, es decir los precios del mismo son básicamente accesible a todo mundo, la inversión en una pequeña computadora lo hace atractivo al público, contando con muchas capacidades a un precio realmente considerable, incluso en los accesorios se puede encontrar que el precio no será un limitante para su uso.

Su bajo consumo de energía es otra ventaja de utilizar una de estas pequeñas computadoras, por su pequeño tamaño, y la mínima cantidad de dispositivos electrónicos, se requiere mucho menos energía que una

computadora convencional. Ya sea para uso en el hogar o en una industria el incremento en el pago de energía eléctrica será mínimo.

Debido a sus capacidades, con estas minicomputadoras se pueden llevar a cabo una serie de proyectos para uso doméstico, de micro empresa y/o automatización en las grandes industrias, básicamente el uso de estos equipos está limitado a la imaginación.

2.5. Lenguaje y programación Python

Python es un lenguaje de programación que es fácil de usar, es decir fácil de leer y escribir y con Raspberry Pi permite crear diversidad de proyectos, ya que prácticamente se puede controlar todos los puertos de la minicomputadora, y es el lenguaje de programación que promueve utilizar la Raspberry Pi. Python posee un gran número de librerías o complementos que ayudan al desarrollo de cualquier proyecto a realizar, facilitando así muchos procesos que podrían llevar un cierto grado de dificultad, programarlos desde cero. La sintaxis de Python es muy clara, con énfasis en la legibilidad y usa palabras clave estándar en inglés.

Python es un lenguaje de programación interpretado cuya filosofía hace hincapié en una sintaxis que favorezca un código legible. Se trata de un lenguaje de programación multiparadigma, esto significa que más que forzar a los programadores a adoptar un estilo particular de programación, permite varios estilos porque soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, y es multiplataforma.

Una característica útil de Python para las personas que ingresan a este lenguaje de programación como las personas que ya tienen conocimiento del

lenguaje, es el intérprete de Python que incluye un modo interactivo en el se escriben las instrucciones en una especie de intérprete de comandos, las expresiones pueden ser introducidas una a una, pudiendo verse el resultado de su evaluación inmediatamente, lo que da la posibilidad de probar porciones de código en el modo interactivo antes de integrarlo como parte de un programa.

El lenguaje de programación Python fue diseñado para ser leído con facilidad. Una de sus características principales es el uso de palabras donde otros lenguajes de programación utilizarían símbolos, facilitando así su lectura y escritura. Permite fácilmente la manipulación de todos los puertos disponibles de la Raspberry Pi, entre los más utilizados los puertos GPIO. Si el sistema operativo utilizado en la Raspberry Pi es Raspbian, este sistema por defecto trae incorporado Python entre sus programas.

3. ARQUITECTURA DEL PROTOTIPO

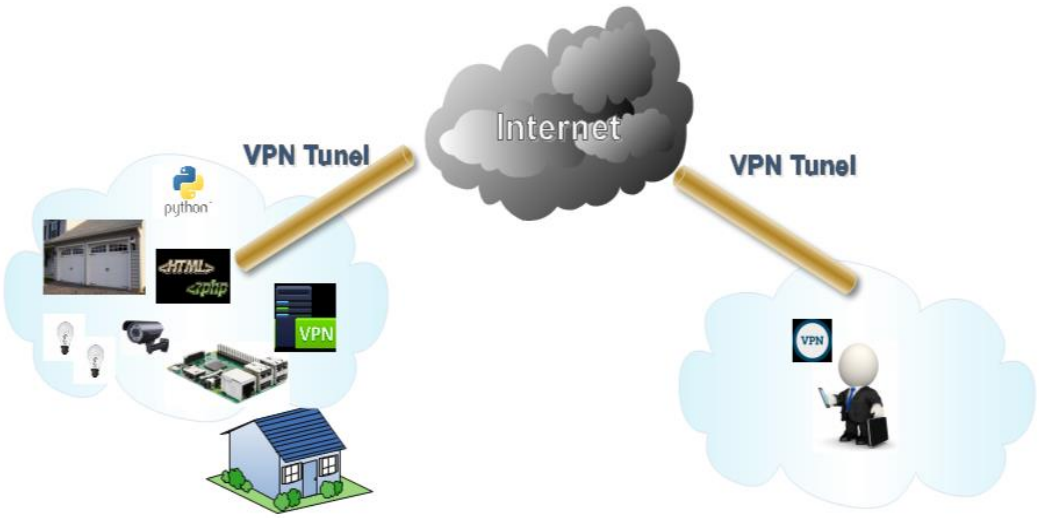
3.1. Características y fundamentos

El sistema está conformado por una Raspberry Pi que actúa como sistema de mando y como servidor de las conexiones VPN, permitiendo así el control de la casa u oficina a través de un dispositivo móvil desde cualquier parte del mundo. El usuario realizara la conexión al servidor VPN proporcionando un usuario y contraseña previamente creado en el servidor de VPN, una vez conectado el usuario tendrá acceso a la red interna y a la Raspberry Pi, permitiendo controlar iluminación, motores de portones eléctricos, cámaras de vigilancia, etc. Todo esto a través de una interfaz WEB que será vista desde el navegador del dispositivo móvil.

3.2. Diseño del diagrama de la conexión VPN

En el diagrama de conexión intervienen varios factores vitales y que permitirán la conexión a los recursos de la red interna y a los servicios que serán controlados, basándose en la siguiente figura (figura 2), se detallan los diferentes factores para el correcto funcionamiento del sistema.

Figura 2. **Túnel VPN**



Fuente: elaboración propia.

Servidor VPN: dispositivo encargado de concentrar las conexiones de los clientes que se conectaran al mismo, en este se encuentra toda la configuración de la VPN, como usuarios, IPs, DNS, llaves de cifrado, contraseñas de usuarios, certificados, etc. El papel de servidor VPN esta desempeñado por la Raspberry Pi.

Cliente VPN: usuario con dispositivo móvil, y contará con un software cliente que se encargará de establecer la conexión al servidor de VPN, a través de una conexión a Internet utilizando las credenciales de usuario y contraseña o certificado, previamente configurados en el servidor VPN.

Control de GPIO: para el control de los puertos de la Raspberry es necesario escribir un programa que convierta el lenguaje humano en lenguaje máquina. Este programa será el encargado de dar la orden de activación o

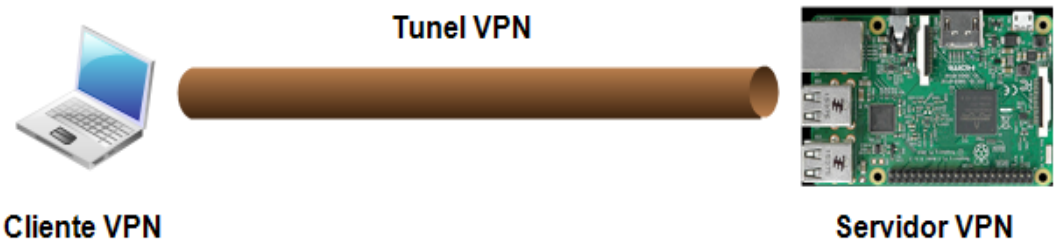
desactivación de los puertos GPIO de la Raspberry Pi, dicho programa se desarrolla en lenguaje Python.

Interfaz de usuario: interfaz gráfica utilizada para la interacción del usuario con el lenguaje de programación Python, y así la ejecución de las ordenes configuradas previamente.

Circuito de control: diseño electrónico encargado de realizar las órdenes electrónicas indicadas por la Raspberry Pi, ya sea de activación o desactivación.

El sistema está diseñado de tal manera para que brinde confianza, facilidad, seguridad, disponibilidad e integridad para el usuario, es decir que el usuario sienta que el sistema le brindara el apoyo en el tiempo que sea requerido y lo haga sentir seguro de utilizarlo.

Figura 3. **Cliente y servidor VPN**

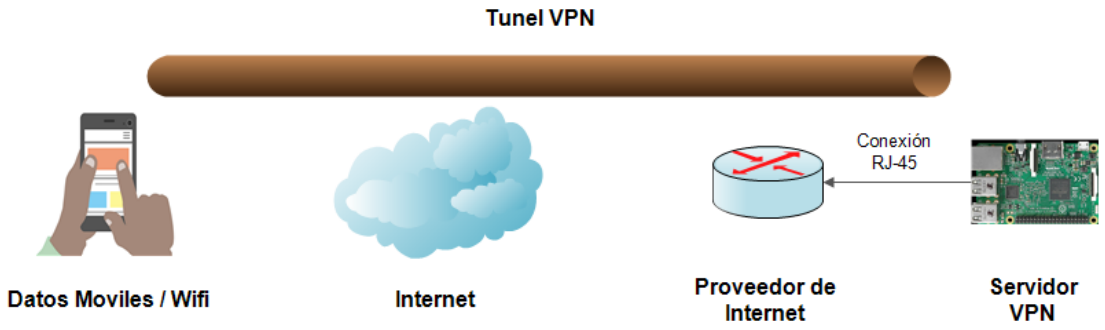


Fuente: elaboración propia.

El diseño es bastante sencillo y básico, si se basan en la figura 3 necesitan, un cliente VPN que contenga la configuración necesaria para

conectarse al servidor VPN, que tiene cierta configuración para aceptar la conexión del cliente VPN, el túnel VPN es creado al realizarse la conexión cliente-servidor que se realiza bajo una conexión a Internet, tanto para el cliente y servidor VPN.

Figura 4. **Establecimiento de túnel VPN**



Fuente: elaboración propia.

En la figura 4 se puede ver a detalle el proceso para la conexión VPN, primero el usuario con dispositivo móvil y acceso a internet solicita una conexión al servidor VPN que es alcanzable desde Internet, el servidor VPN aceptara la conexión una vez el cliente tenga la configuración y claves de acceso necesaria, si el cliente VPN cumple con los requisitos solicitados por el servidor VPN la conexión se realiza y se crea el túnel de VPN. Teniendo establecido el túnel VPN es posible realizar cualquier acción configurada en la Raspberry Pi.

3.3. Modelo de las configuraciones básicas de un servidor VPN

Para adquirir o hacerse de un servidor VPN existe más de una forma de hacerlo, ya sea adquiriendo un equipo dedicado a este tipo de tecnologías, de los cuales existen muchos en el mercado, diferentes marcas, precios, tamaños y capacidades, como siempre esto dependerá de las necesidades que se tengan o el proyecto a realizar. También existe el software libre, y es una buena opción para proyectos que no exigen demasiado, en pocas palabras para proyectos pequeños, como por ejemplo, un proyecto para el hogar, o para microempresas. Se debe tener en cuenta que la única condición es tener un computador o minicomputador que soporte la instalación del software, que se esté utilizando y por supuesto también es requerida una conexión a Internet.

El proyecto está dedicado para el hogar o una microempresa, el uso de software libre como servidor VPN es una muy buena opción. Y como plataforma para la instalación del software se utilizará la minicomputadora Raspberry Pi, esta funciona perfectamente para este tipo de tecnología. El software utilizado es OpenVPN para Raspberry Pi. Antes de realizar la instalación del software es necesario tomar en cuenta los siguientes puntos:

- Raspberry Pi con Raspbian Jessie instalado y actualizado
- Disponer de IP interna fija
- Disponer de IP externa fija o en su defecto servicio de DNS dinámico
- Acceso a router de proveedor de internet para apertura de puertos para conexión VPN.
- El servidor de OpenVPN dispondrá de las siguientes características:
- El servidor VPN es del tipo cliente a cliente, y los clientes conectados al servicio VPN podrán verse y comunicarse entre ellos.

- El servidor dispondrá de autenticación TLS. Esto ayudará a evitar ataques de denegación de servicio o que un tercero realice un escaneo de puertos para evitar vulnerabilidades.
- El servidor dispondrá de actualizaciones de seguridad de forma completamente automáticas, y es una característica esencial.
- Permitirá conectarse a servicios de la red local desde cualquier lugar del mundo.
- Al tratarse de un servidor OpenVPN cliente-to-cliente, el tráfico entre clientes estará gestionado íntegramente por el servidor OpenVPN y no habrá ninguna intervención del Kernel.

Se trata de una configuración que es funcional y tiene en cuenta la seguridad y privacidad de los usuarios conectados. El proceso se puede realizar vía SSH, vía VNC o directamente en la Raspberry Pi conectada a un monitor.

3.3.1. Pasos para configuración del servidor OpenVPN

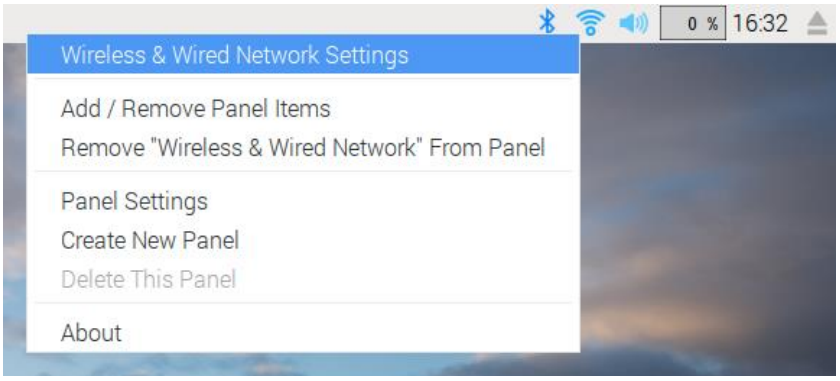
Es importante mencionar que la configuración del servidor VPN está realizada con un servicio de IP pública contratada, y pueden existir diferentes escenarios en los que la configuración podría variar, como siempre todo depende de los recursos que se tengan. En este escenario la IP pública está directamente asignada a la interface de Red cableada de la Raspberry Pi y la interface WIFI está conectada a la red interna. No es necesario adquirir un servicio de DNS dinámico y se realizan menos pasos de configuración.

3.3.1.1. Configuración de IP fija

El primer paso a realizar es asignar una IP fija a la Rasperry Pi. Para conseguir este propósito existen varios métodos, pero se utilizará el siguiente:

Dirigirse al panel superior derecho sobre el indicador de WIFI, presionar el botón derecho del ratón y cuando aparezca el menú contextual dar click encima de la opción Wireless & Wired Network Settings, como se muestra en la figura 5

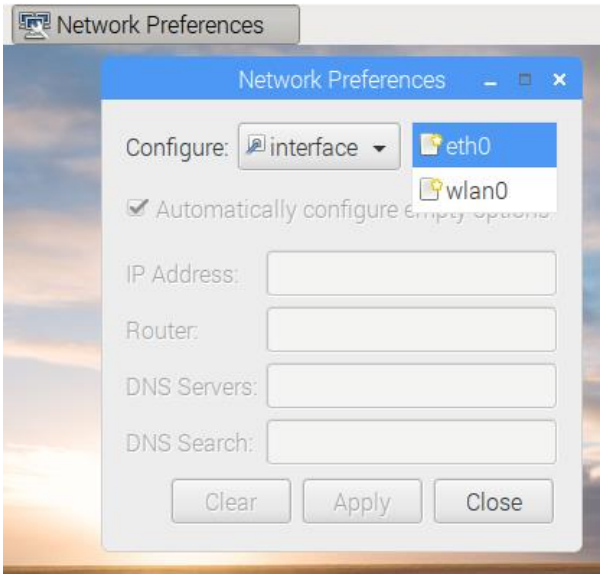
Figura 5. **Acceso a configuración de red en Raspberry Pi**



Fuente: elaboración propia.

Cuando aparezca la ventana de configuración seleccionar la interfaz de red que se usara para el servidor VPN. Este paso dependerá de la conexión a Internet que se esté utilizando, y puede ser cableado o por WIFI. Si la conexión es por cable seleccionar eth0 y si es por WIFI seleccionar wlan0. Es recomendable configurar una IP estática a las dos interfaces de Red.

Figura 6. **Configuración interfaz de red en Rapberry Pi**

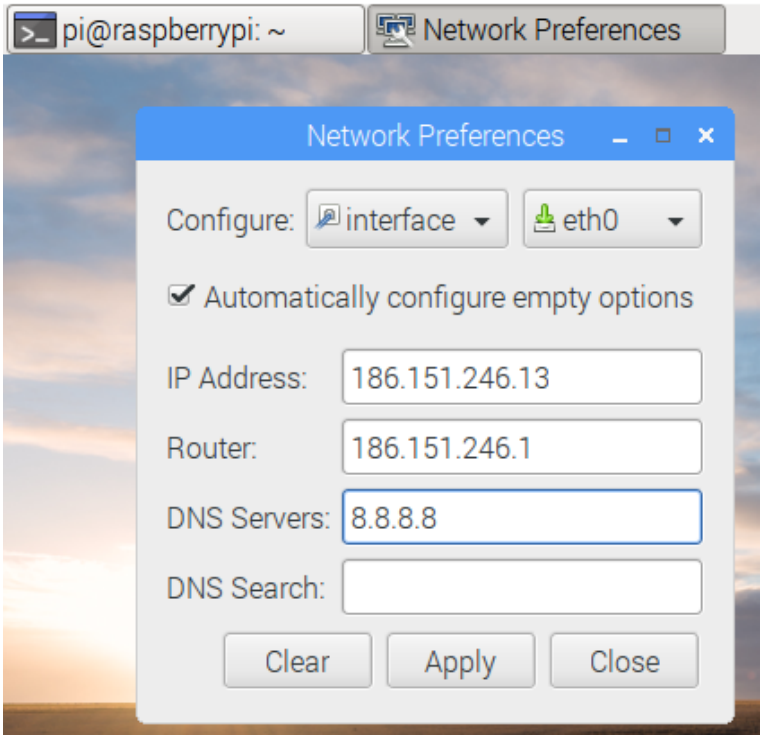


Fuente: elaboración propia.

A continuación rellenar los parámetros de configuración de la conexión que se haya seleccionado de la siguiente forma:

Nota. Cabe mencionar que la información que se coloque en los campos dependerá de la IP pública asignada o la red que distribuya el router del proveedor de Internet.

Figura 7. **Configuración IP estática Raspberry Pi**



Fuente: elaboración propia.

- Dirección IP: Escribir la IP estática que tendrá el servidor VPN. Esto dependerá de la IP pública contratada o de la red que distribuye el Router del proveedor de Internet. Se está trabajando bajo el escenario de un servicio de IP pública contratado, se debe asignar dicha IP a una de las interfaces de Red de la Raspberry Pi.

- Router: Introducir la puerta de entrada del Router que provee el Internet.

- DNS Servers: Indicar el servidor DNS que se desean usar o los indicados por el proveedor de Internet.

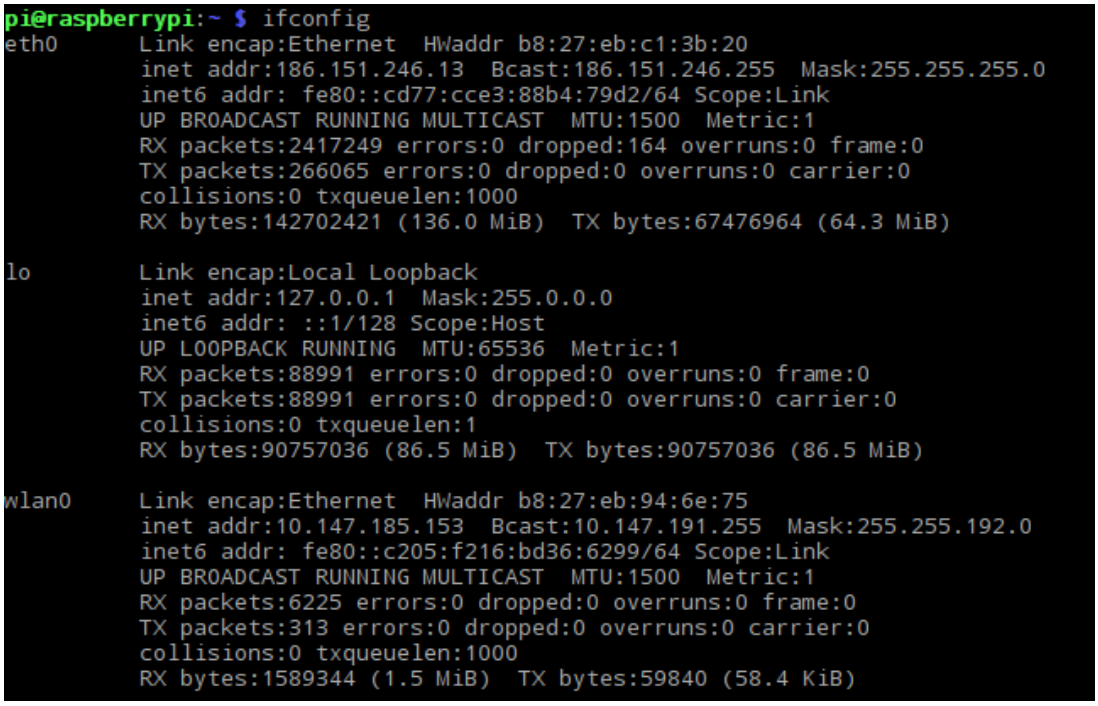
- DNS Search: Dejar este campo en blanco. Para este propósito este campo no tiene ninguna utilidad.

Aplicar cambios y luego reiniciar la Raspberry Pi. Después del reinicio es necesario verificar los cambios realizados. Para asegurarse de ello abrir una terminal y ejecutar el siguiente comando:

- pi@raspberrypi:~ $ ifconfig

- Identificar el nombre de la interface modificada y verificar la IP asignada

Figura 8. **Revisión de configuración de red en Rasbperrry Pi**



Fuente: elaboración propia.

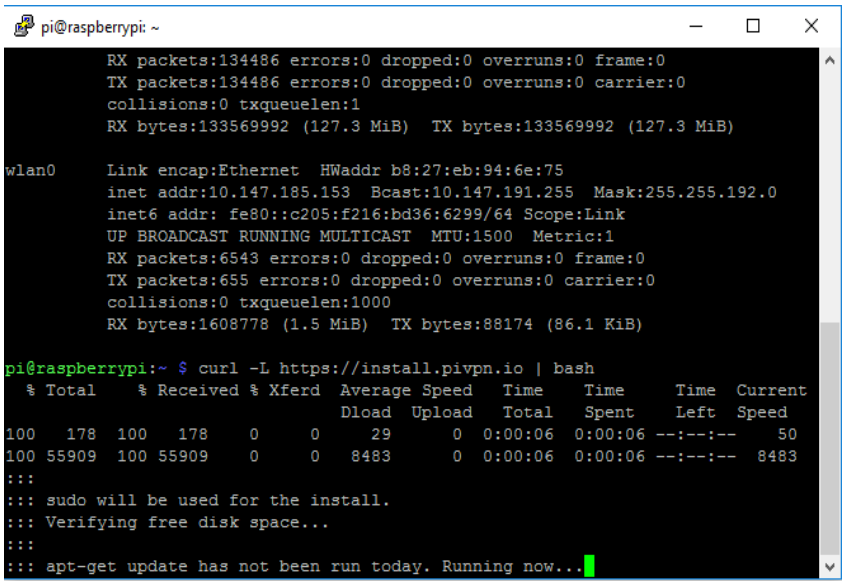
3.3.1.2. Instalar y configurar el servidor OpenVPN

Luego de asignar y verificar las IPs correspondientes a la Raspberry se procede a realizar la instalación y configuración del servidor de OpenVPN, para ello se debe abrir una terminal de línea de comandos y se ejecuta el siguiente comando:

curl -L https://install.pivpn.io | bash

El comando anterior descargara y ejecutara un script para empezar la instalación del servidor de OpenVPN, este consiste de una serie de pasos que se deben ir configurando, dependiendo el escenario que se esté manejando, cabe resaltar que se está manejando un escenario con servicio de IP pública contratado.

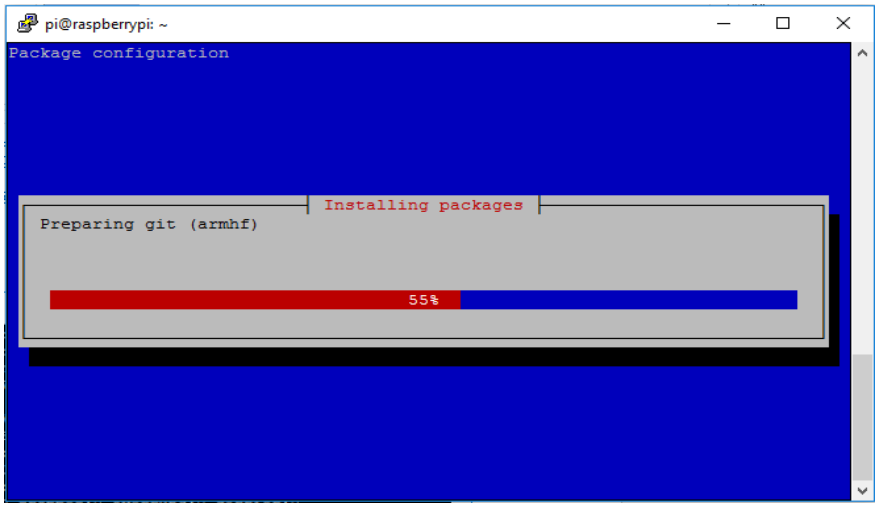
Figura 9. **Inicio de instalación servidor VPN**



Fuente: elaboración propia.

Luego de ejecutar el comando, el script descargado verifica si la Raspberry Pi se encuentra actualizada, si no se encuentra con las últimas actualizaciones el script automáticamente empieza a realizar la actualización como se evidencia en la figura 9.

Figura 10. **Inicio de la instalación de paquetes de configuración**



Fuente: elaboración propia.

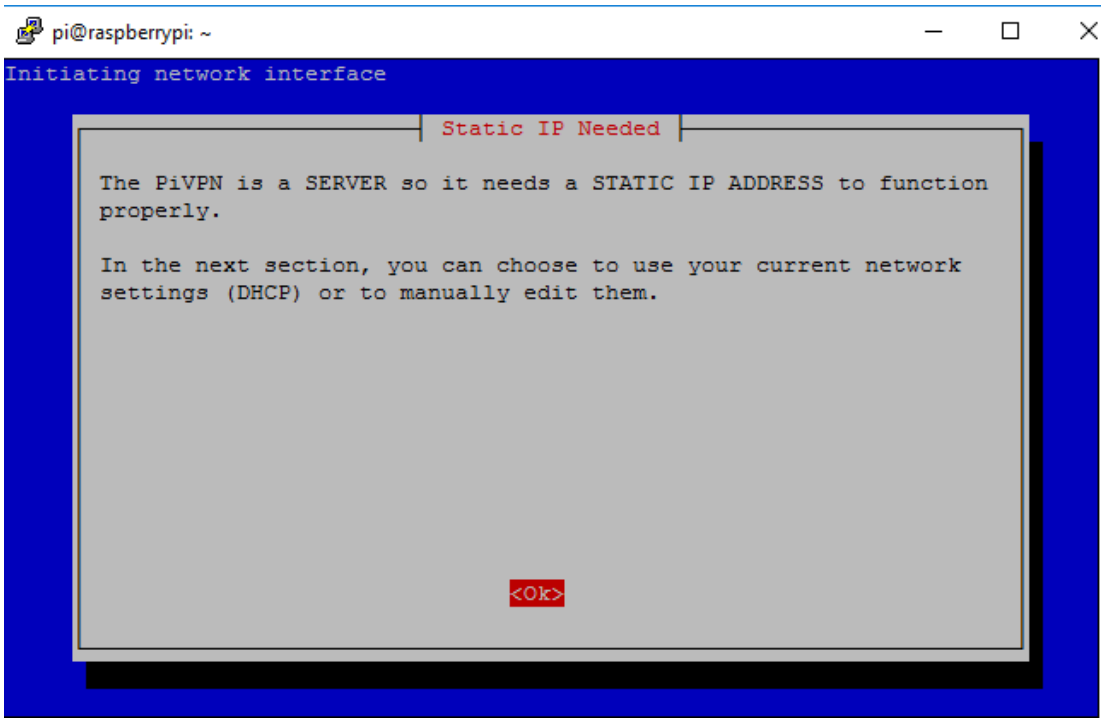
Después de finalizar el proceso de actualización, se iniciará la etapa de preparación e instalación de paquetes como se muestra en la figura 10, este proceso suele demorar unos minutos.

Figura 11. **Preparación de instalación del servidor VPN**

Fuente: elaboración propia.

Seguido el instalador, presenta una pantalla con un mensaje de bienvenida indicando que la Raspberry será transformada en un servidor de OpenVPN. Para tal pantalla se debe presionar el botón “OK”. Durante todo el proceso de instalación se presentara una guía donde indica los parámetros a configurar y una breve descripción de su uso, como se evidencia en la figura 12. Indica que se debe poseer una IP estática configurada en el servidor para evitar cambios en un futuro.

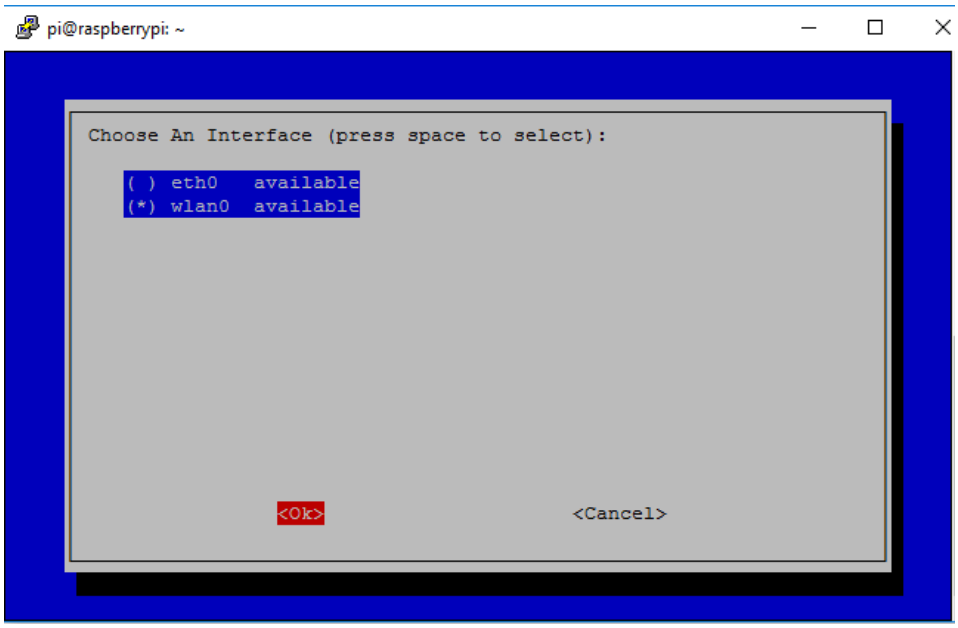
Figura 12. **Indicación de IP estática en servidor VPN**



Fuente: elaboración propia.

El primer paso de configuración que se presenta es la selección de una interface de Red para la publicación del servidor VPN, esta será la interface por donde se realiza la conexión lógica del servidor VPN. Esto como siempre depende del escenario que se maneja. Indicar la interface y luego presionar “Ok” para continuar con la instalación.

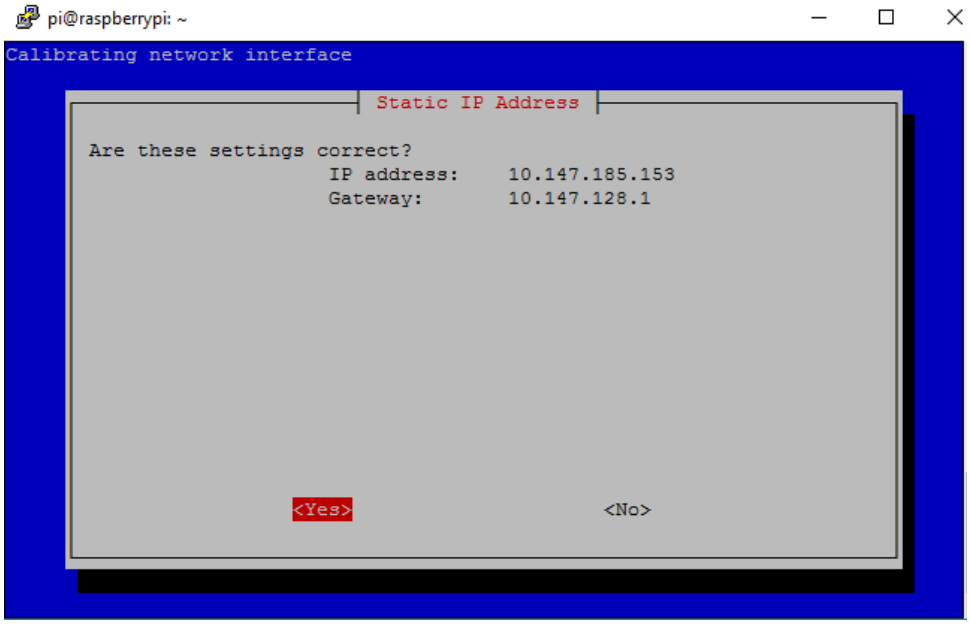
Figura 13. **Selección de interface de red para servidor VPN**



Fuente: elaboración propia.

Luego de seleccionar la interface, solicitara la IP estática de la interface y el Gateway de dicha interface, esto para la conexión a la Red interna y salida a Internet. Ver figura 14

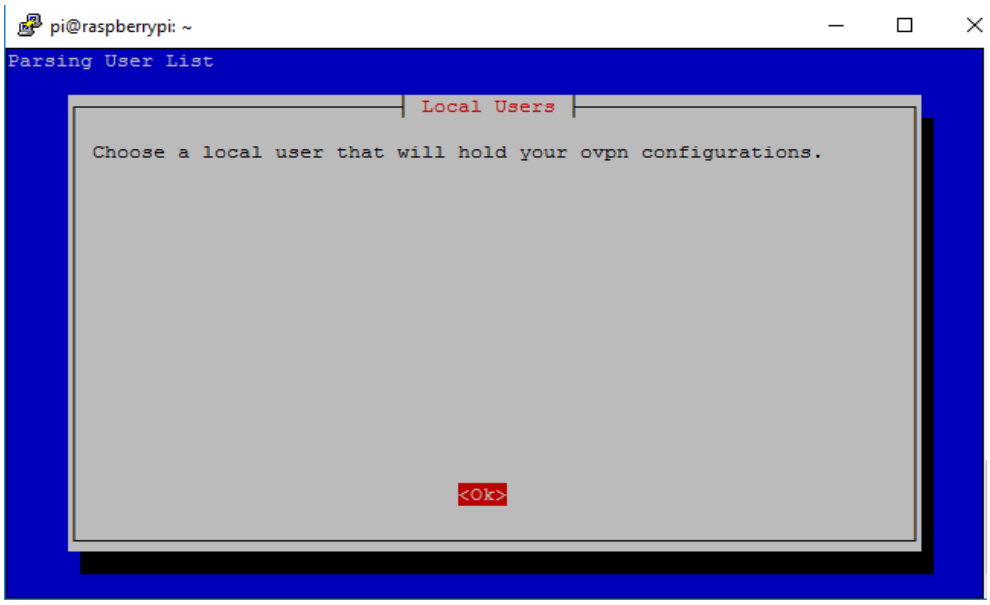
Figura 14. **Asignación de IP para publicar servidor VPN**



Fuente: elaboración propia.

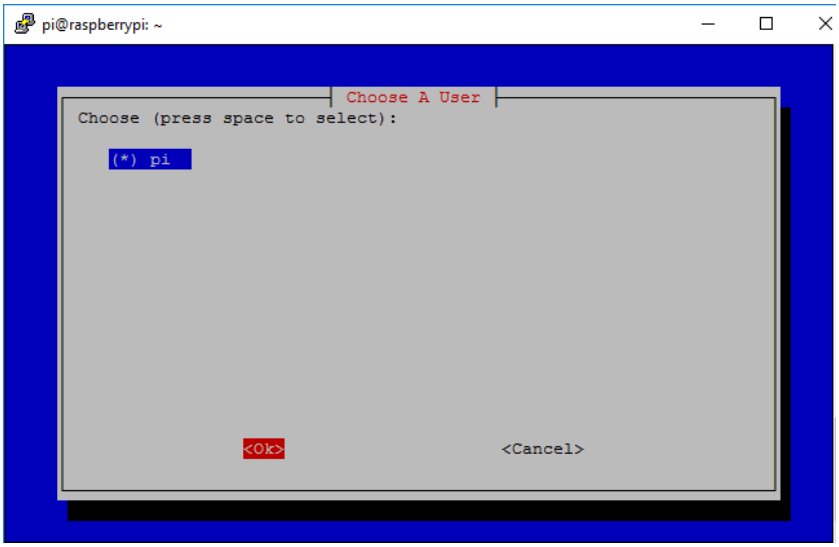
Se debe indicar un usuario que guardara las configuraciones del servidor VPN, por defecto se utiliza el usuario “pi”, pero es altamente recomendable crear y utilizar otro usuario, por motivos de seguridad.

Figura 15. **Comienzo de configuración de usuarios VPN**



Fuente: elaboración propia.

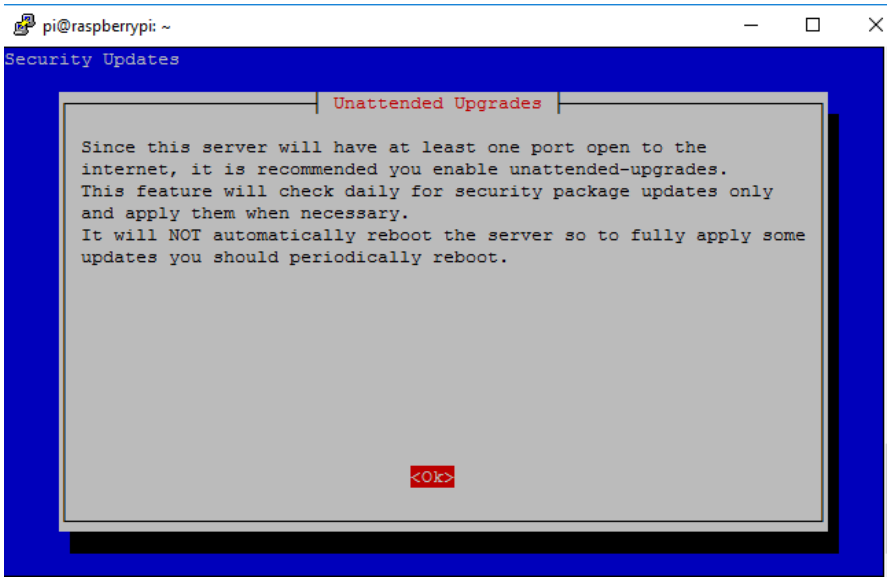
Figura 16. **Selección de usuario VPN**



Fuente: elaboración propia.

Luego de seleccionar el usuario a utilizar, el programa indica que al menos un puerto debe estar publicado a Internet para realizar la conexión del túnel VPN, y recomienda, realizar periódicamente actualizaciones al sistema, esto para cubrir brechas de seguridad que pudieran afectar al servidor.

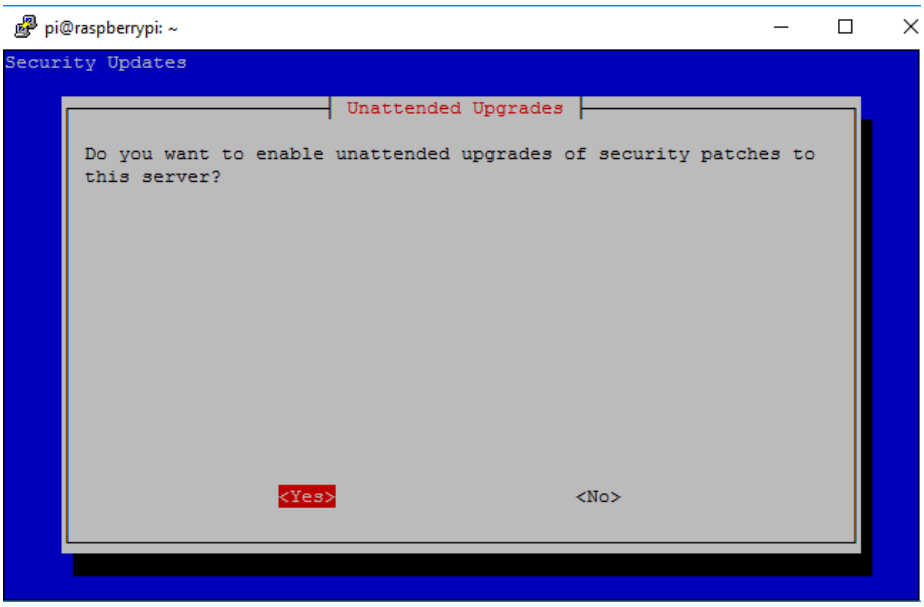
Figura 17. **Inicio de actualización del servidor VPN**



Fuente: elaboración propia.

En base a las indicaciones de la guía de instalación y por buena práctica de seguridad se habilitan las actualizaciones para el nuevo servidor VPN.

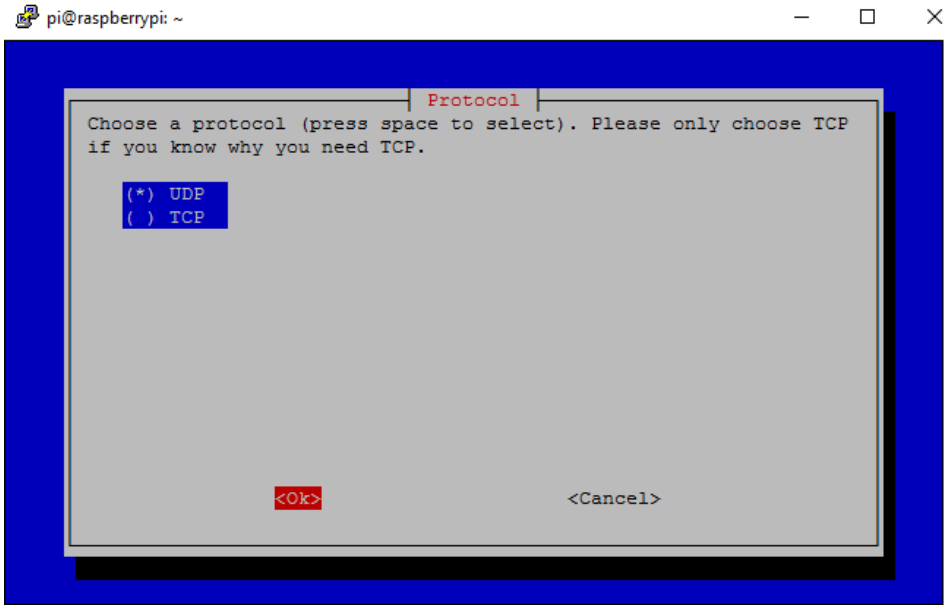
Figura 18. **Confirmación de actualización del servidor**



Fuente: elaboración propia.

El siguiente paso es indicar el protocolo que será utilizado para la comunicación del servidor y cliente VPN, se debe tener en cuenta que ambos protocoles tienen sus ventajas y desventajas, en cuanto al protocolo UDP, es de cierta forma menos seguro pero más rápido para la transmisión de datos, mientras que TCP es más seguro pero relativamente lento a comparación con el protocolo UDP.

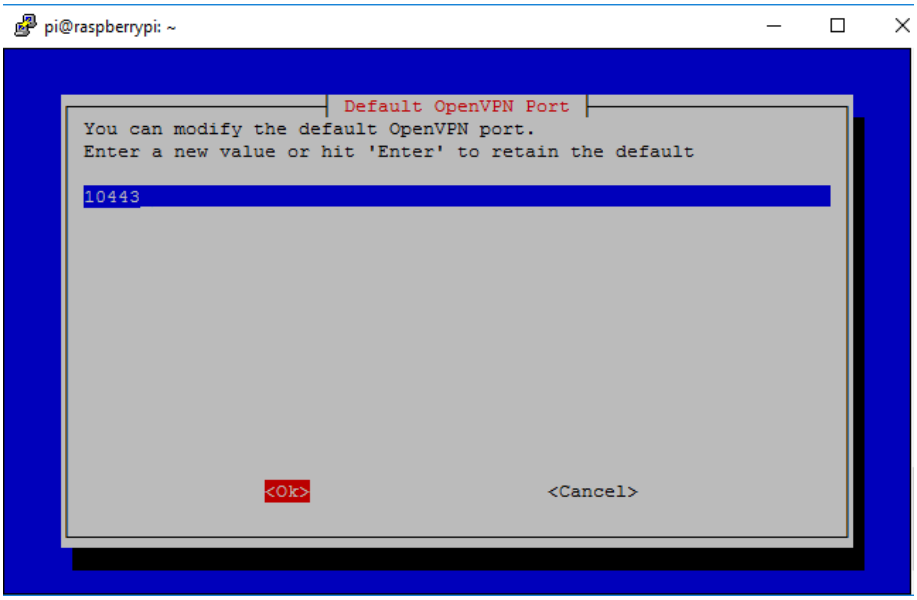
Figura 19. **Selección de protocolo del servidor VPN**



Fuente: elaboración propia

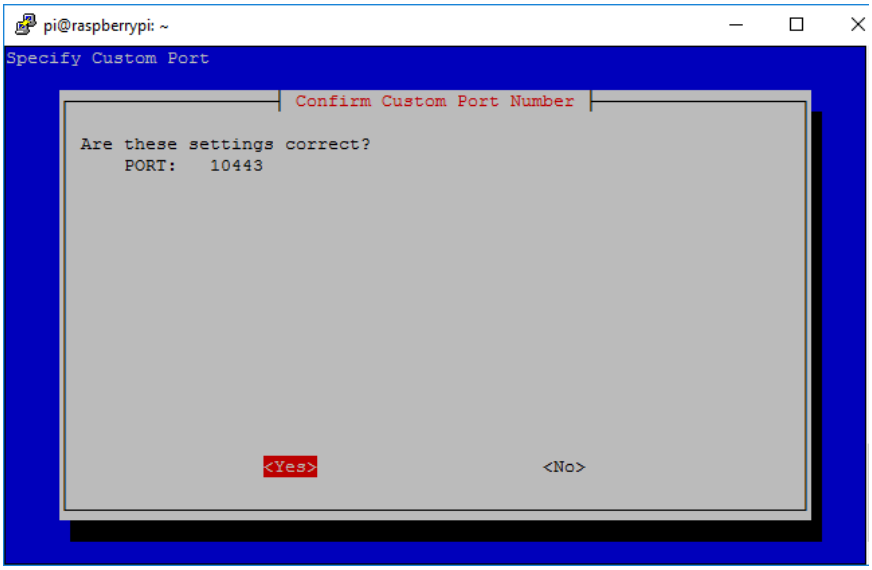
Una vez seleccionado el protocolo, se debe seleccionar el puerto escucha para la conexión VPN, no es recomendable el puerto por defecto, por lo que se procede a utilizar otro puerto conocido o común, y seleccionar “Ok”. Luego de indicar el puerto, el instalador solicitara confirmación del puerto a utilizar.

Figura 20. **Selección de puerto de conexión VPN**



Fuente: elaboración propia.

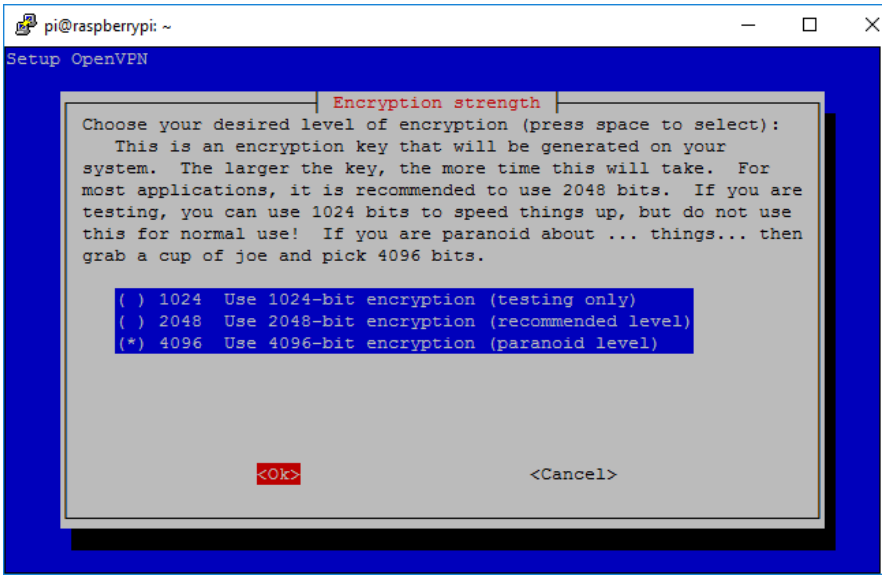
Figura 21. **Confirmación de uso de puerto lógico**



Fuente: elaboración propia.

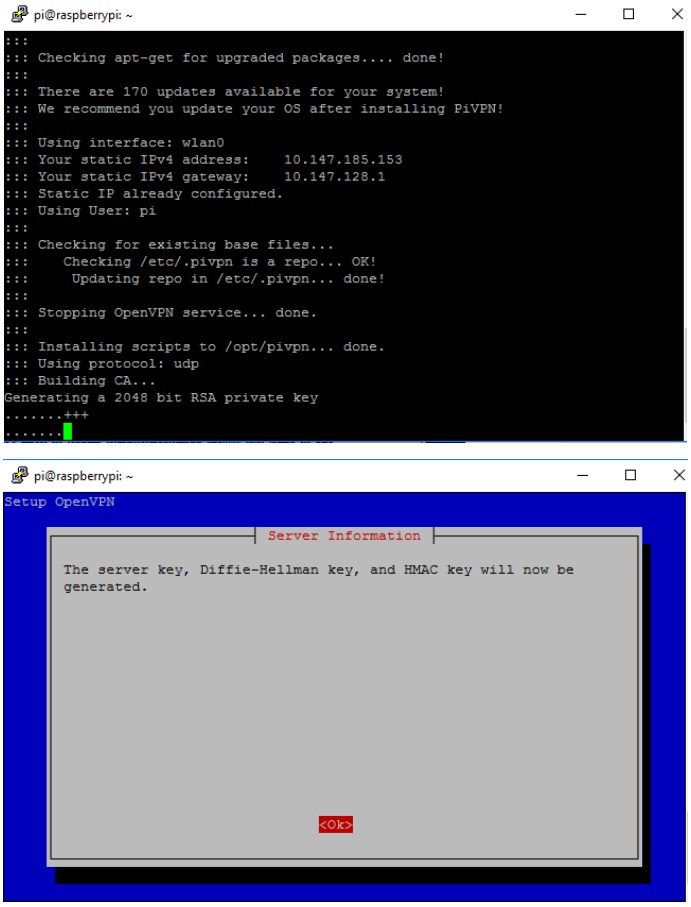
A continuación se debe seleccionar la longitud de cifrado de la llave privada del servidor VPN, hay que tomar en cuenta que entre más largo es la longitud de la llave, más tiempo y potencia será necesaria para que un ataque de fuerza bruta tenga efecto, en pocas palabras hace más seguro el servidor VPN. Este proceso requiere más tiempo, porque se debe crear la llave del servidor y también dependerá del nivel de cifrado que se elija, porque el proyecto es para tener acceso a red interna se recomienda utilizar la llave de 4096 bits de longitud.

Figura 22. **Selección de longitud de cifrado**



Fuente: elaboración propia.

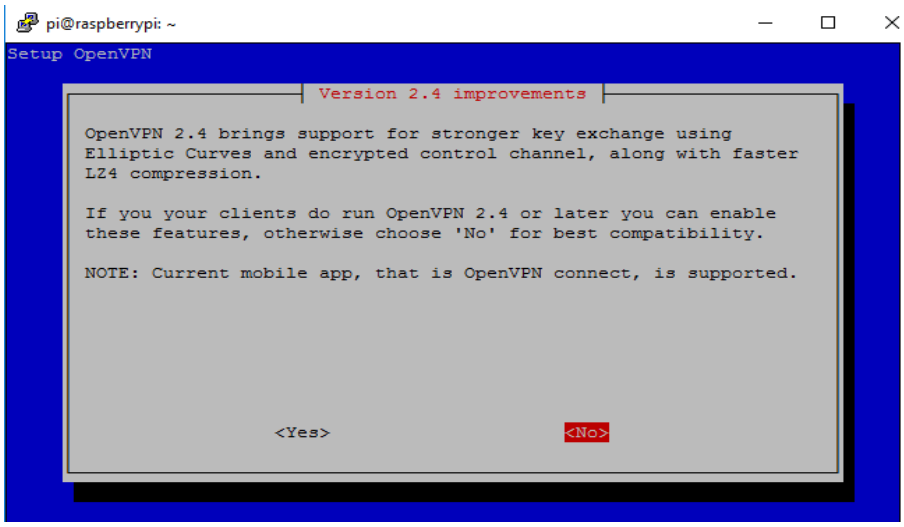
Figura 23. **Proceso de configuración de cifrado**



Fuente: elaboración propia.

Las nuevas versiones de OpenVPN ofrecen un nivel más de seguridad utilizando curvas elípticas y cifrado del canal de control, pero se debe tener presente que este nivel de seguridad no es compatible con todas las versiones de OpenVPN cliente. El cliente OpenVPN debe ser versión 2.4 o superior para ser compatible.

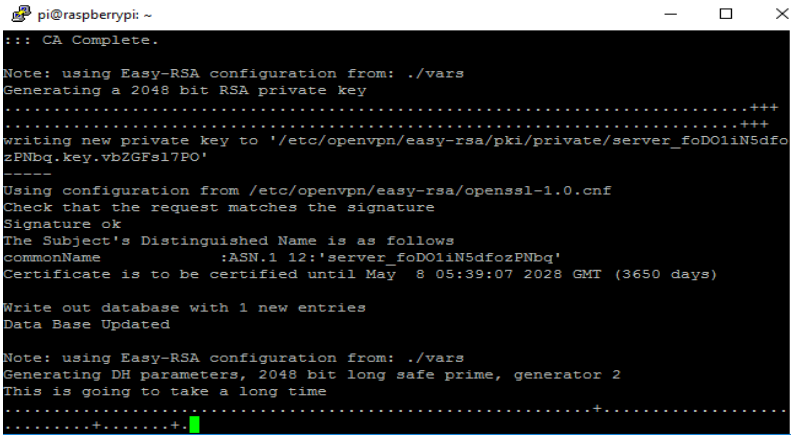
Figura 24. **Elección de compatibilidad**



Fuente: elaboración propia.

Se debe confirmar la creación de llave del servidor y una vez confirmado, iniciará el proceso como se muestra en la figura 25.

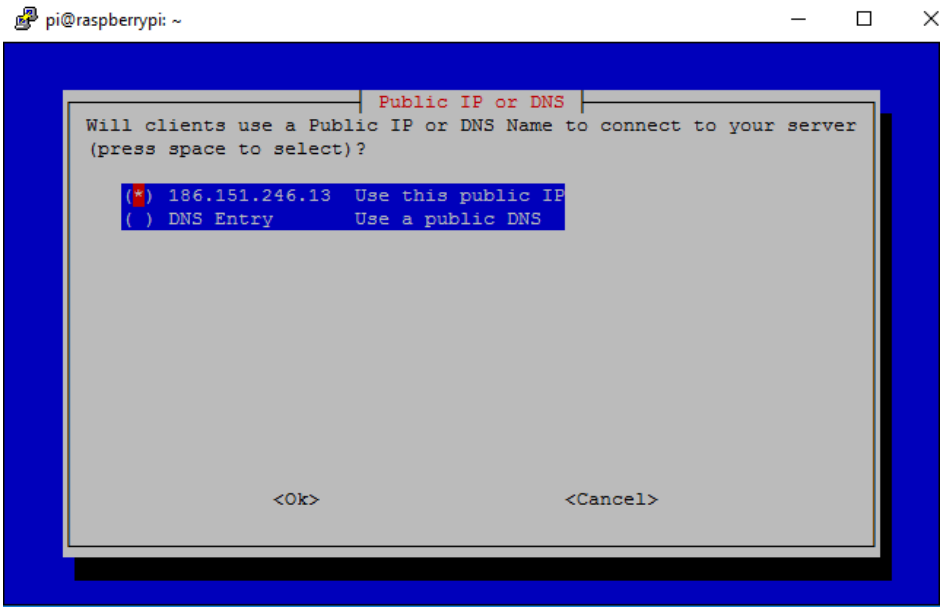
Figura 25. **Proceso de generación de cifrado**



Fuente: elaboración propia.

Indicar la IP pública o el servicio DNS para ser encontrado en Internet, si se posee un servicio de DNS, se debe indicar el nombre del mismo. Si se está manejando servicio de IP pública contratado, se debe colocar la IP con la que será visto el servidor VPN desde Internet.

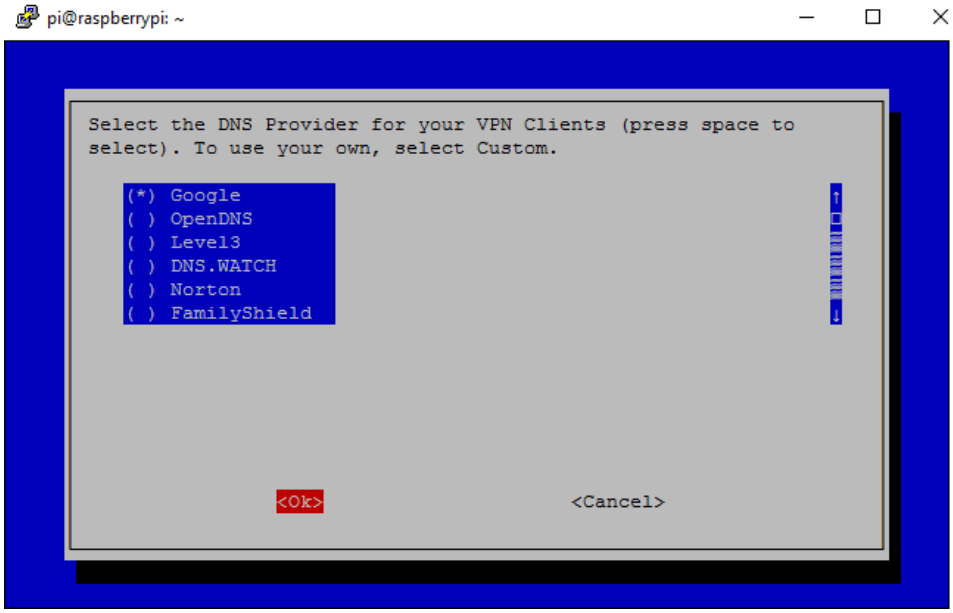
Figura 26. **Selección de IP pública**



Fuente: elaboración propia.

Seleccionar los DNS que se asignaran a los clientes de OpenVPN para la navegación de Internet.

Figura 27. **Selección de DNS**



Fuente: elaboración propia.

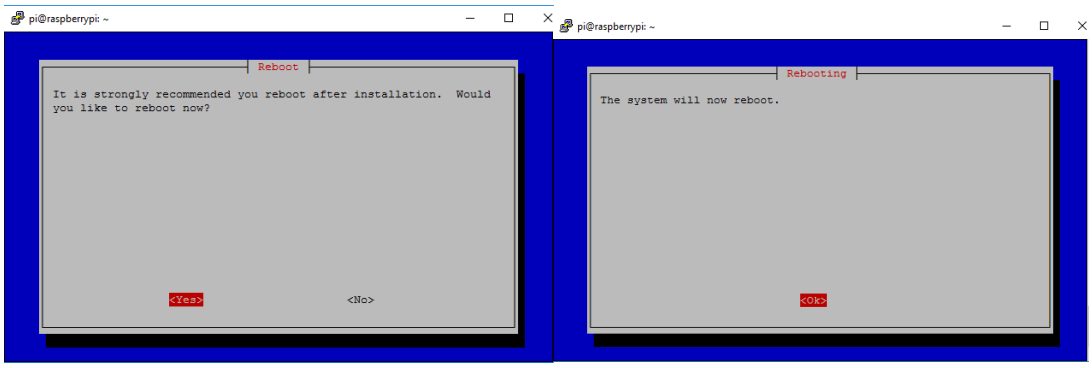
Una vez seleccionado los servicios DNS para los clientes, la guía indica que se deben crear usuarios para VPN, y también indica la forma de crearlos y la dirección donde se almacena el archivo de configuración para los clientes creados.

Figura 28. **Indicación de instalación completa**

Fuente: elaboración propia.

Como último paso de configuración del servidor VPN, es mandatorio y recomendable realizar un reinicio de la Raspberry Pi.

Figura 29. **Indicación de reinicio de servidor**



Fuente: elaboración propia.

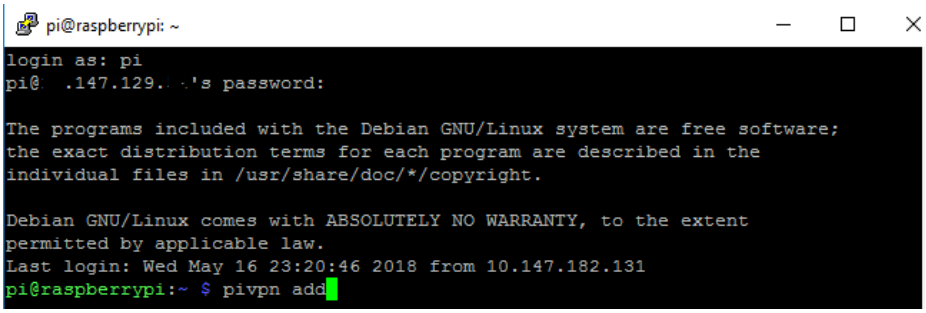
3.3.1.3. Adición de usuarios

Luego de instalar el servidor y haber realizado las configuraciones correspondientes, es necesario crear los usuarios que se conectaran al servidor de VPN, estos usuarios y sus credenciales deben ser proporcionados únicamente a las personas que se conectaran a la VPN. La creación se realiza en el servidor VPN y se asignara un nombre y contraseña para crear el archivo que debe ser importado al cliente de VPN. El proceso de creación es el siguiente.

En la Raspberry Pi donde se instaló el servidor de OpenVPN, se debe ejecutar el siguiente comando:

“pivpn add”

Figura 30. **Adición de usuarios de VPN**

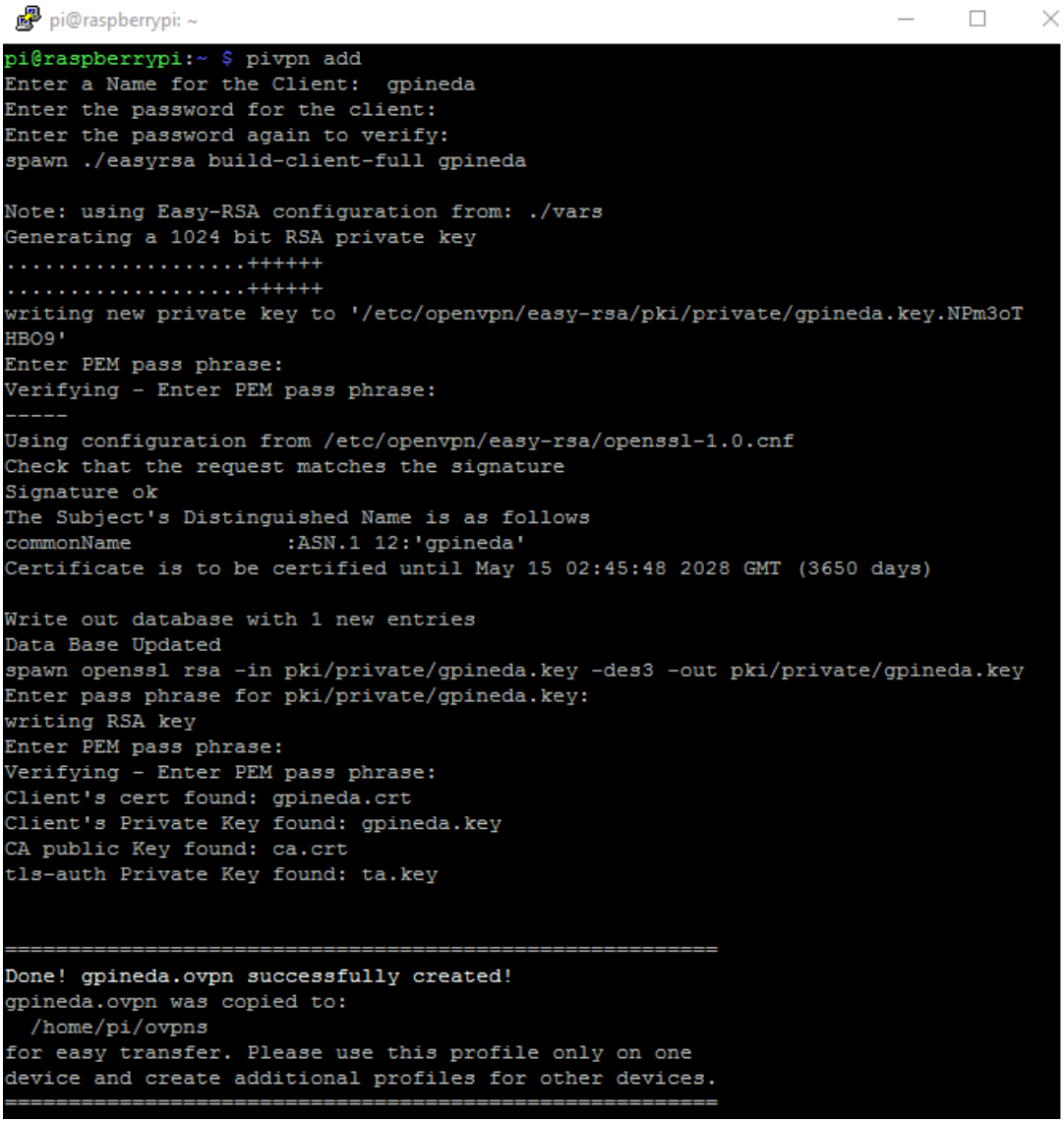


Fuente: elaboración propia.

Al momento de ejecutar el comando, se solicitará un nombre y una contraseña que serán utilizados para la creación del archivo que será importado al cliente VPN, dicho nombre y contraseña asignados, deben ser guardados para llevar a cabo la conexión al servidor de OpenVPN. Luego de asignar un

nombre y contraseña, el servidor empezara a crear el archivo e indicará cuando se haya terminado de crear, también indica la ruta donde se crea el archivo, esto se debe tener presente porque se debe descargar dicho archivo para ser importado al cliente de VPN.

Figura 31. **Adición de usuario exitosa**



Fuente: elaboración propia.

En la ruta indicada “home/pi/ovpns”, se encuentra el archivo de configuración del nuevo usuario creado, dicho archivo se identifica con el nombre de usuario asignado. Este archivo puede ser enviado por correo, descargado usando un cliente FTP, etc. Y es mandatorio que sea copiado al dispositivo que será utilizado para la conexión VPN, ya sea una computadora, celular o tablet.

3.4. Clientes VPN y establecimiento de una conexión

Existen diferentes aplicaciones para dispositivos móviles que pueden ser utilizados para establecer un túnel de VPN, en este caso porque se está utilizando un servidor de OpenVPN, se procede a utilizar el cliente de OpenVPN, esto para evitar problemas de compatibilidad entre software. Dicho cliente se encuentra disponible para sistemas operativos, iOS, Android, Mac, Linux y Windows. El proceso de instalación varía dependiendo el sistema operativo a utilizar, para dispositivos móviles celulares la instalación se realiza desde la tienda de Android o iOS y es una aplicación gratuita en ambos casos.

3.4.1. Conexión cliente – servidor

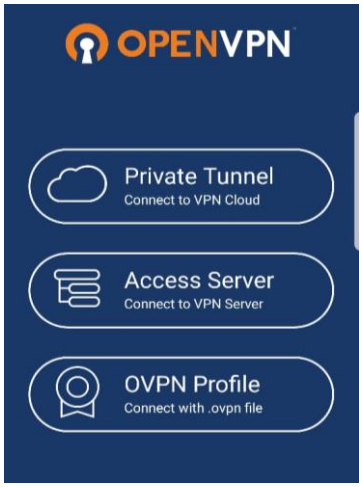
Establecer el túnel de VPN, es prácticamente realizar la conexión cliente – servidor, para realizar este proceso se deben tener en cuenta los siguientes puntos.

- Tener instalado en el dispositivo a utilizar el cliente de OpenVPN
- Poseer el archivo de configuración del cliente en el dispositivo a utilizar para la conexión, y fue generado por el servidor de OpenVPN.

Una vez realizados los puntos anteriores, el proceso de conexión cliente servidor se realiza de la siguiente manera: El proceso se realizará en dispositivo Android.

Lo primero es ejecutar la aplicación del cliente de OpenVPN, dependiendo la versión que se esté corriendo tendrá las siguientes características (ver figura 32), de estas se seleccionará “OVPN Profile”

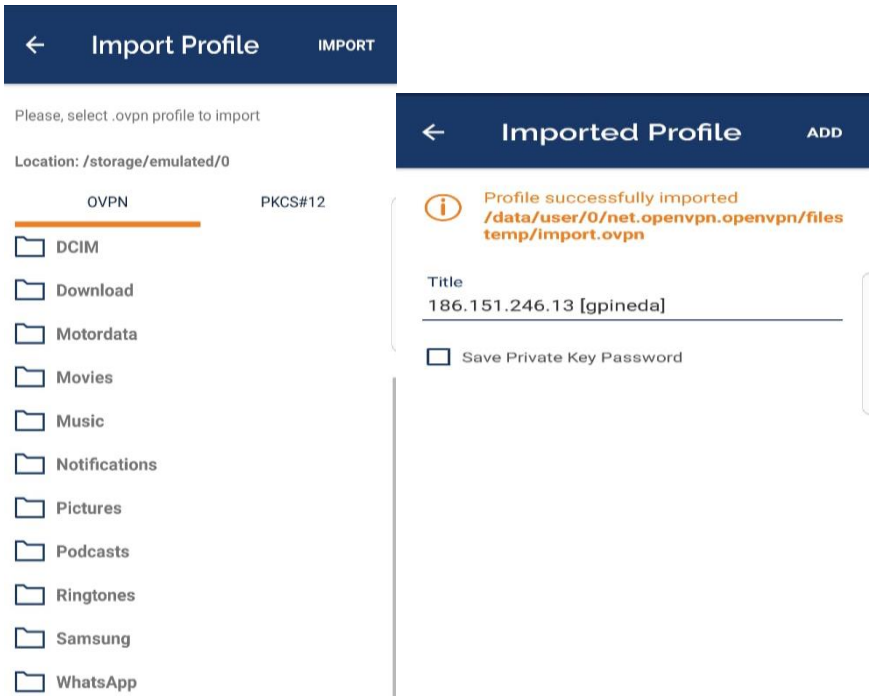
Figura 32. **Cliente VPN en SO Android**



Fuente: elaboración propia.

Una vez seleccionada la opción indicada, se debe localizar la ubicación del archivo con extensión “.ovpn” descargado en el teléfono y seleccionar importar. Luego de haber realizado la importación solicitara confirmación para agregar el perfil del nuevo usuario, a lo que se selecciona “agregar” (ADD).

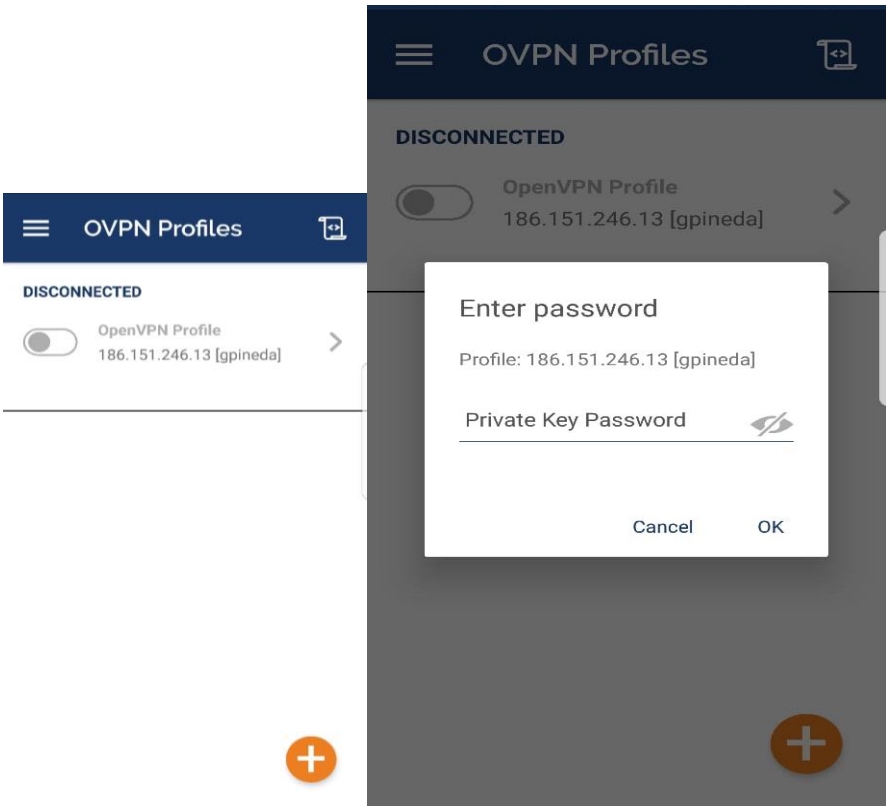
Figura 33. **Importación de archivo de configuración en OpenVPN**



Fuente: elaboración propia.

Con la importación del archivo correctamente, presionar el interruptor para habilitar la conexión VPN y establecer el túnel, con esto también se solicitara la clave configurada para el usuario en el servidor VPN, esta debe ser ingresada correctamente para establecer la conexión hacia el servidor de VPN.

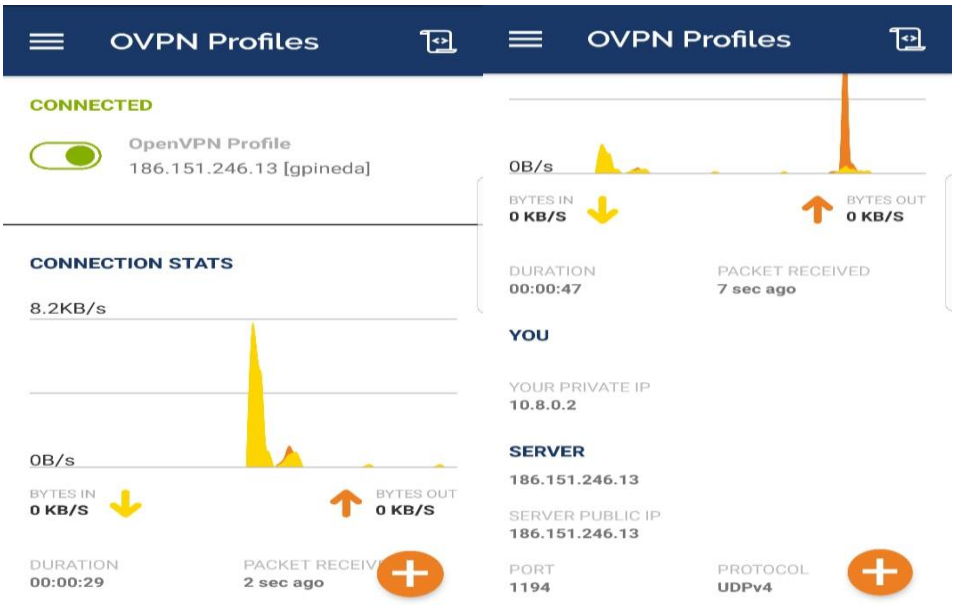
Figura 34. **Inicio de sesión con OpenVPN**



Fuente: elaboración propia.

Al ingresar la contraseña del cliente, se iniciará la conexión y se mostraran algunos datos de conexión como el indicador de conexión exitosa al servidor VPN, IP pública con la que se realiza la conexión, usuario conectado, gráfico del tráfico entrante y saliente, IP privada asignada al cliente, entre otros.

Figura 35. **Establecimiento de conexión exitosa**



Fuente: elaboración propia.

Con la VPN establecida, ya es posible acceder a la red interna de la casa u oficina, y se hace posible realizar cualquier tarea desde cualquier lugar, esto a través de una conexión segura.

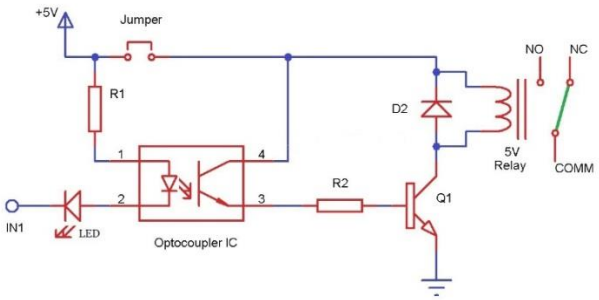
4. MODELO TEÓRICO DEL SISTEMA

4.1. Circuito para encendido y apagado de un foco a través de Raspberry pi

Es necesario que la Raspberry Pi tenga interacción con los objetos o dispositivos a controlar, se hace necesario el uso de un circuito capaz de ser controlado por la Raspberry Pi y que pueda manejar mayor corriente de la que puede llegar a manejar la Raspberry Pi. Para ello se utiliza un circuito con relés este permite manejar mayores corrientes DC, y por supuesto manejar corriente alterna (AC).

El circuito con relés puede ser construido o ser adquirido en una venta de circuitos electrónicos. Si el circuito es construido básicamente el diseño es el siguiente:

Figura 36. **Diagrama de circuito electrónico para manejo de Relé desde GPIO de Raspberry Pi**



Fuente: ELECTRONICS HUB. *Controlled Power Outlet*. https://www.electronicshub.org/arduino-controlled-power-outlet/. Consulta: 15 de abril de 2018.

Del diseño del circuito de la figura 36, es necesario adquirir todos los materiales y realizar el diseño de la placa de cobre donde será soldado para luego realizar la conexión a la Raspberry Pi, en dicha figura el pin “IN1” es la conexión que se realiza en uno de los pines GPIO de la Raspberry Pi y es el pin que recibe la señal de activación o desactivación del Relé. La conexión de la carga o el foco se realiza en los pines “NO” y “COMM” del Relé, estos se encargan de cerrar el circuito y activar la carga. Si es necesario controlar más dispositivos u objetos eléctricos, solamente se debe replicar el circuito y realizar la conexión a otro GPIO de la Raspberrry Pi.

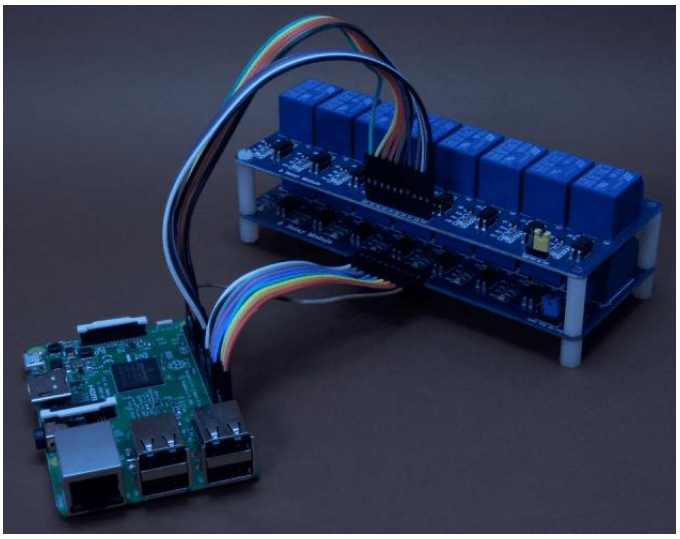
El mismo circuito se puede adquirir ya construido en su placa de cobre en una venta de componentes electrónicos y con esto se reduce el trabajo de implementación, dicho circuito tiene una forma similar al de la figura 37. Se pueden encontrar en diferentes módulos y solo depende de la cantidad de relés que se desean utilizar.

Figura 37. **Placa de relés**

Fuente: Carrod electrónica. *Placa de Relés.* https://www.carrod.mx/products/modulo-de-reles-4-canales-5-v-con-optoacoplador-generico. Consulta: 16 de abril de 2018.

Utilizando la placa de relés, solamente se debe identificar los GPIO de la Rasbperry Pi a usar y también se debe verificar las conexiones en la placa de relés, que básicamente son las conexiones de alimentación del circuito y los pines de control de dicha placa electrónica. La conexión utilizando una placa con mayor cantidad de relés se vería como la figura 38.

Figura 38. **Conexión placa de relés y Raspberry Pi**



Fuente: RASPBERRYPI. *Conexión placa relés y Raspberry Pi.* https://www.raspberrypi.org/forums/viewtopic.php?t=141494. Consulta: 18 de abril de 2018.

4.2. Diseño de programa en Python para el manejo de GPIO de Raspberry Pi

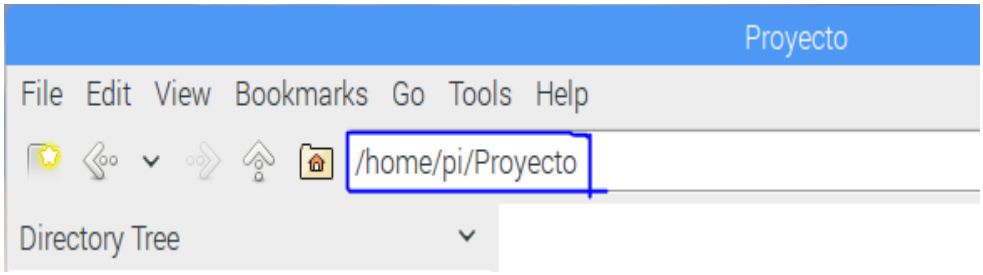
Como es necesario que la Raspberry Pi pueda interactuar con el mundo exterior o mejor dicho con los dispositivos a controlar, se necesita crear un programa que pueda interpretar y controlar las señales o impulsos eléctricos sobre los puertos de la Raspberry Pi. Dicho programa permitirá activar y

desactivar un puerto GPIO, o tomar una lectura del mismo. De esta forma la Rasberry Pi tendrá conocimiento de lo que sucede en el mundo exterior.

Para el desarrollo del programa es necesaria la instalación de Python que será el programa que interpretará las líneas de código, que serán escritas en un archivo con extensión ".py", por defecto la Raspberry Pi tiene instalada una versión de Python.

El programa a escribir se desarrollará sobre una interfaz de línea de comandos, y antes de empezar a escribir dicho programa, se debe elegir la ubicación del archivo que contendrá las líneas de código. Es recomendable crear una ubicación para todos los programas a crearse, esto para mantener un orden y fácil búsqueda de todos los programas relacionados al proyecto. Se vuelve único punto de falla en cuestión de ubicación, lo que reduce el tiempo en resolver algún problema o en realizar una modificación.

Figura 39. **Ubicación de archivos de programas Python**



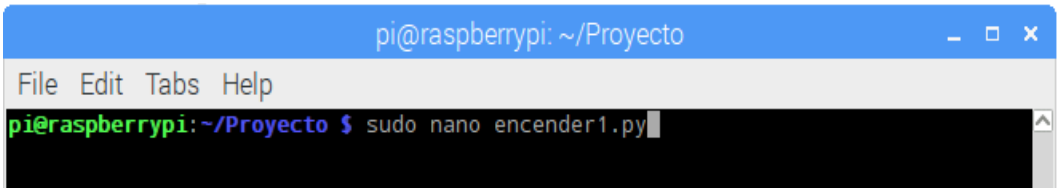
Fuente: elaboración propia.

4.2.1. Programa para encender un puerto GPIO

Luego de elegir la ubicación de los programas a utilizar, se procede a escribir el programa que se encargará de controlar los puertos GPIO de la Raspberry Pi. Para el manejo de los GPIO se debe tener instalada la librería “RPi” en la Raspberry Pi, dicha librería ya viene instalada por defecto en el sistema operativo Raspbian. En dado caso no se posee la librería, se puede descargar ejecutando en la Raspberry Pi el comando “sudo apt-get install python-rpi.gpio” y se instalará la versión más reciente de dicha librería.

Para iniciar, lo primero es dirigirse a la ubicación antes seleccionada esto a través de la interfaz de línea de comandos, una vez posicionado en la ubicación seleccionada, se procede a crear el archivo con extensión “.py” con el editor nano, como se muestra en la figura 40.

Figura 40. **Ejecución de programa en Python desde CLI**



Fuente: elaboración propia.

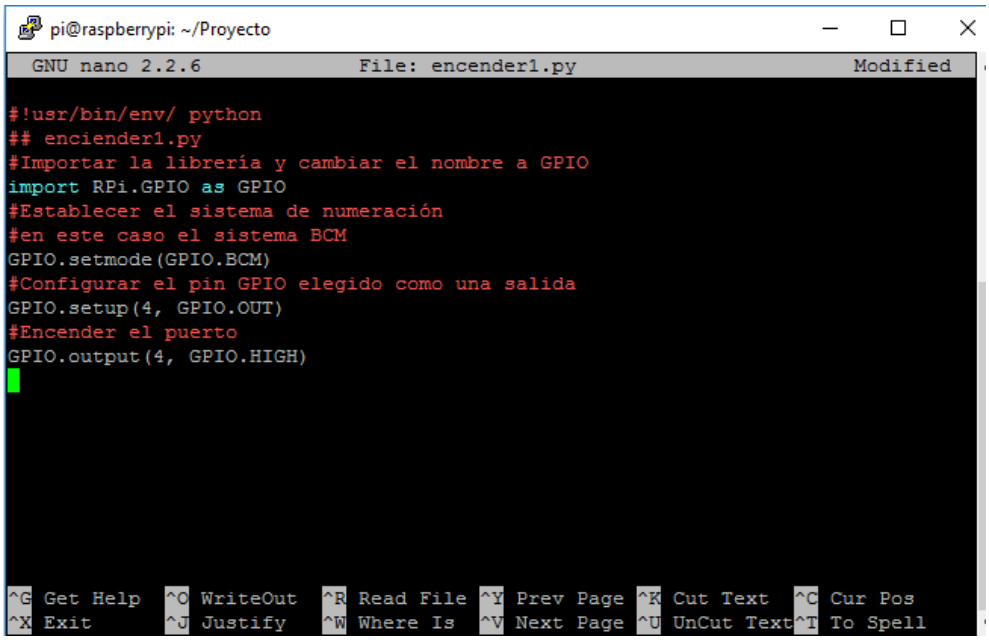
Esto ejecutará el editor “nano” y este permitirá la escritura del código deseado, siendo las líneas de código utilizadas para encender un puerto GPIO especifico, quedando de la siguiente forma:

```
#!usr/bin/env/ python
```

```
## enciender1.py
#Importar la librería y cambiar el nombre a GPIO
import RPi.GPIO as GPIO
#Establecer el sistema de numeración
#en este caso el sistema BCM
GPIO.setmode(GPIO.BCM)
#Configurar el pin GPIO elegido como una salida
GPIO.setup(4, GPIO.OUT)
#Encender el puerto GPIO
GPIO.output(4, GPIO.HIGH)
```

Visto en el editor “nano” queda de la siguiente forma:

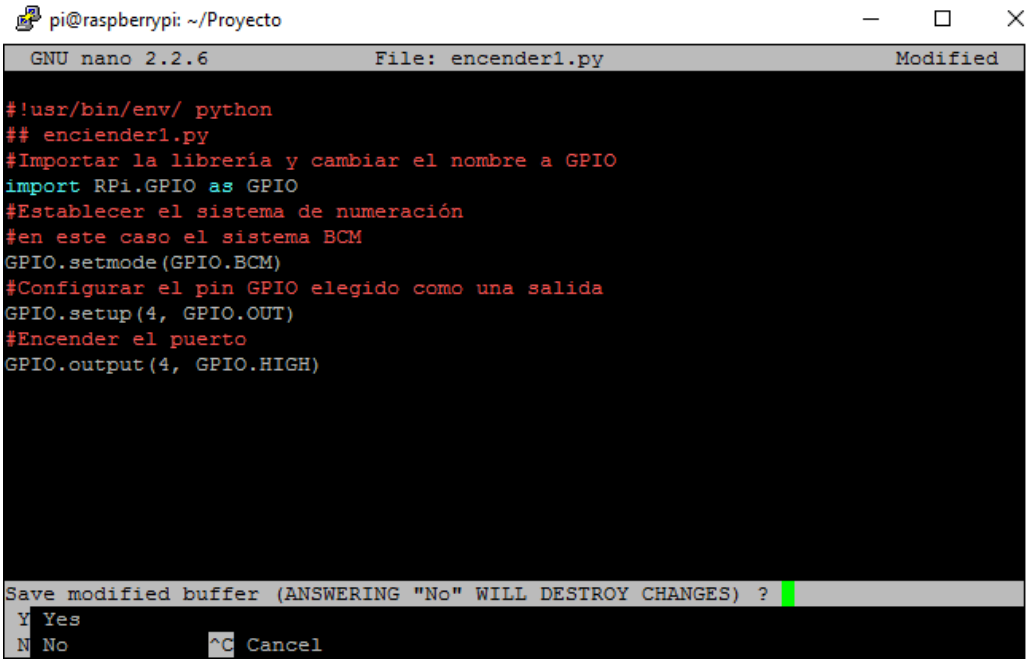
Figura 41. **Editor de texto “nano” en Raspberry Pi**



Fuente: elaboración propia.

Luego guardar los cambios, presionando el conjunto de teclas “ctrl + x” y luego confirmar los cambios como se muestra en la figura 42.

Figura 42. **Creación de programa en Python, encender puerto GPIO**



Fuente: elaboración propia.

4.2.2. Programa para apagar un puerto GPIO

El programa para apagar el puerto GPIO de la Raspberry Pi, básicamente tiene la misma sintaxis que el programa para encender el puerto, el cambio se realiza en el estado del puerto, como se muestra a continuación:

```
#!usr/bin/env/ python
## apagar1.py
```

```
#Importar la librería y cambiar el nombre a GPIO
import RPi.GPIO as GPIO
#Establecer el sistema de numeración
#en este caso el sistema BCM
GPIO.setmode(GPIO.BCM)
#Configurar el pin GPIO 4 como una salida
GPIO.setup(4, GPIO.OUT)
#Apagar el puerto GPIO
GPIO.output(4, GPIO.LOW)
```

El procedimiento para guardar el programa es el mismo que se utilizó para en el programa para encender el puerto de la Raspberry Pi.

Figura 43. **Programa apagar puerto GPIO Raspberry Pi**

Fuente: elaboración propia.

4.3. Interface de control en página web

Como es necesaria una interface gráfica, en la que el usuario final pueda visualizar los controles de los dispositivos integrados o conectados a la Raspberry Pi, que en este caso es activar o desactivar uno o varios puertos de las Raspberry Pi. Se crea entonces un pagina web interna que unicamente es alcanzable desde la conexión VPN, asegurando asi el uso de la pagina web y haciendo este control más seguro, y solo es alcanzable para las personas interesadas y no a todo el publico.

4.4. Instalación del servidor web

Para la creación de la pagina web que contendra los controles de los dispositivos, es necesario realizar la instalación de los programas que harán posible levantar dicha pagina web. Estos programas se instalaran en la misma Raspberry Pi que contiene el servidor VPN.

Lo primero es realizar una conexión via SSH en la Raspberry Pi, para ir ejecutando los comando que realizaran la instalación del servidor web. Luego de realizar la conexión, se procede a realizar la instalación del servidor Apache, que es un servidor web de codigo abierto y que es soportado para la mayoria de sistemas operativos, entre ellos Raspbian.

Para la instalación se ejecuta el comando:

“sudo apt-get install apache2”

Con esto se inciara el proceso de descarga e instalación, unicamente pedirá confirmación de la instalación. Una vez instalado para comprobar que la

instalación se ha llevado a cabo con éxito, escribir la dirección IP de la Raspberry Pi en la barra de direcciones de un navegador. Si Apache se ha instalado correctamente, aparecerá en el navegador una página predeterminada con el mensaje “It works!”. Esta página web en formato HTML se encuentra en Raspbian Jessie en el directorio /var/www/html/index.html. La página puede revisarse en el directorio y en él pueden incluirse otros tipos de páginas web.

“sudo nano /var/www/html/index.html”

Como es necesario que la pagina web sea capaz de realizar otras tareas de ejecución, y brinde mayores alcances, se realiza la instalción de PHP, este da ciertas caractaristicas para la interacción de la pagina web con funcionalidades propias de Raspberry Pi, ademas hace posible que se puedan procesar otros archivos aparte de html, CSS o JavaScript, archivos PHP. Para la instalción al igual que Apache, unicamente se debe ejecutar el siguiente comando y confirmar la instalación:

“sudo apt-get install php5 libapache2-mod-php5”

Con esto el servidor ahora es capaz de interpretar archivos con extensión “.php” y agregando más posibilidades de desarrollo a la pagina web. Se realizará una pagina web sensilla con las instalaciones realizadas es considerado suficiente para realizar una potente interface gráfica.

4.4.1. Desarrollo de página web

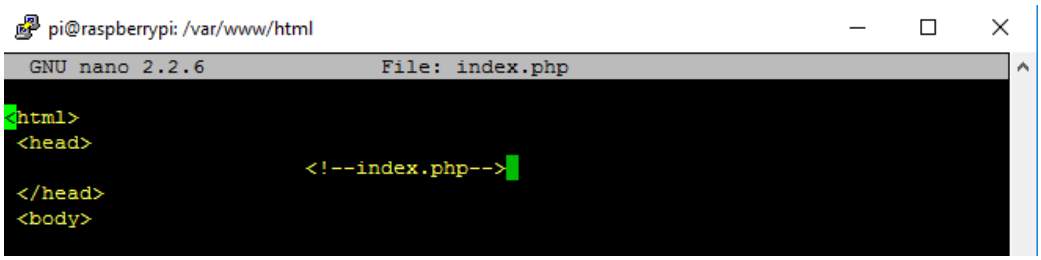
Para el desarrollo de la pagina web que se encargará de dar las instrucciones a la Raspberry y de hacer uso de los programas creados en Python, es necesario dirigirse al archivo que sera modificado para realizar dicha pagina web, la ubicación del archivo es la siguiente:

“sudo nano /var/www/html/index.html”

Esta ubicación de archivo ya era conocida, en el momento que se realizó la instalación del servido Apache. Lo que sigue acontinuación es dirigirse a esta ubicación por linea de comandos en la Raspberry Pi, y crear un archivo llamado “index.php", lo que se realizara es sustituir el archivo “index.html” por el nuevo archivo “index.php”, que sera el archivo donde se desarrollara la pagina web. Para realizar la sustitución y que el programa utilice el nuevo archivo, unicamente se renombra el archivo viejo. Por ejemplo “archivoviejo.html”, cabe destacar que este proceso se debe realizar con permisos de adminstrador.

Para la creación del nuevo archivo se debe utilizar el editor “nano” y se debe escribir de la siguiente forma “sudo nano index.php”, luego aparecera la ventana del editor con el nombre del archivo a crear.

Figura 44. **Creación de página web en código html**



Fuente: elaboración propia.

El código a escribir dependerá de la cantidad de puertos GPIO que se desea controlar, y de la cantidad de dispositivos a integrar para el control. El programa a desarrollar, estará escrito una parte en código html y otra parte en código php. El código html será usado para los botones y la parte en php es utilizada para el manejo o llamado de los programas escritos en Python. El programa tiene la siguiente forma y cotrola únicamente un puerto GPIO, en especifico el puerto numero 4.

Inicio del programa en HTML

```
<html>
 <head>
                    <!--index.php-->
 </head>
 <body>

 <br></br>

  <!--GPIO4-->
  <form action="" method="post">
```

```
PIO04&amp;nbsp;<inputtype="submit"name="encender4"value="Encender>
        <input type="submit" name="apagar4" value="Apagar">

        <br></br>


        </body>
       </html>
```

Final del programa en HTML e inicio del pragrama en PHP

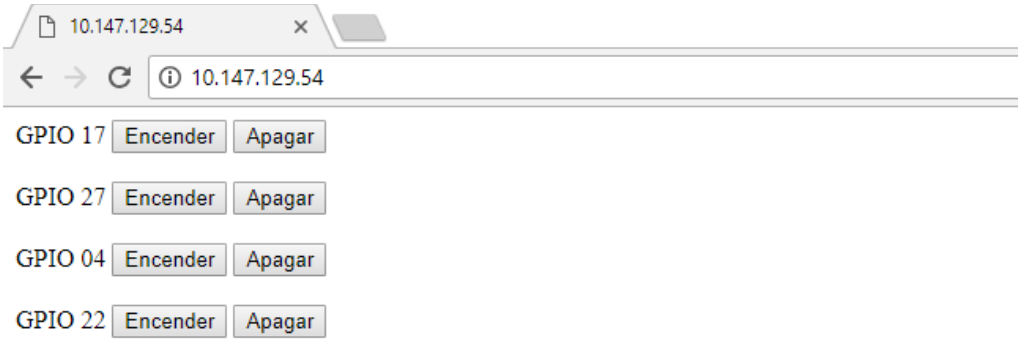
```
<?php

// Funciones PHP del pin GPIO 4

  if ($_POST[encender4]) {
   “$a- exec("sudo python /home/pi/Proyecto/encender1.py");
   echo $a;
  }

  if ($_POST[apagar4]) {
   “$a- exec("sudo python /home/pi/Proyecto/apagar1.py");
   echo $a;
  }

// Fin de las funciónes del pin GPIO 4

?>
```

Final del programa en código PHP

En la parte del programa con codigo PHP existe la siguiente linea de código “$a- exec("sudo python /home/pi/Proyecto/encender1.py");”, esta tiene la función de ejecutar el programa en Python creado anteriormente para encender el puerto numero 4 de los pines GPIO de la Rasbperry Pi, de la misma forma se ejecuta el comando para apagar el puerto, con la diferencia que se utiliza el programa en Python correspondiente para realizar dicha tarea, dicho programa fue llamado “apagar1.py”. Cabe mencionar que se debe colocar la ubicación del archivo para que este se pueda ejecutar. Una vez escrito el programa, unicamente se deben guardar los cambios.

Para verificar el resultado de la pagina, dirigirse a un navegador y en la URL colocar la IP de la Raspberry Pi y se debera desplegar el botón o los botones configurados.

Figura 45. **Página web creada en código HTML Y PHP**



Fuente: elaboración propia.

4.5. Flujo final del proceso

Las acciones o efectos finales como encender/apagar un foco, abrir/cerrar un porton electrico del proyecto se deben a una serie de pasos o un flujo que se lleva a cabo para completar dichas tareas.

Para ello el flujo final del proyecto es de la siguiente forma:

- Una persona con un dispositivo movil, posee un cliente de VPN instalado, dicho dispositivo tiene acceso a Internet. Se realiza la conexión al servidor VPN con las credenciales asignadas.
- Una vez realizada la conexión VPN, el dispositivo tiene acceso a la red interna, por lo que puede ingresar a servicios internos.
- Dirigirse a un navegador disponible e ingresar a la pagina web creada, esta se encarga de realizar las tareas que se hayan programado.
- Seleccionar la tarea o accion a realizar, y el botón elegido se encargará de ejecutar el programa en Python correcto para realizar la acción.
- Dependiendo el tipo de acción el programa activará o desactivará el puerto GPIO seleccionado. Ejecutando la acción de encendido o apagado del dispositivo final, ya sea un foco de alumbrado electrico o el motor de un porton electrico.

5. COSTOS

5.1. Costos del proyecto

El costo total del proyecto, la puesta en marcha y el mantenimiento del mismo son calculados y presentados en base a los precios en el mercado actual, estimando un promedio de todos los materiales y servicios a utilizar. Se incluye gastos administrativos, de mantenimiento, soporte, contrataciones y todo lo relacionado al buen funcionamiento del proyecto.

El proyecto en cada implementación representa la instalación de todos los materiales y servicios para su funcionamiento, lo que significa que el precio en en todos los casos es el mismo.

Se debe tomar en cuenta que el costo presentado es para la implementación en un sitio unicamente lo que significa que es para una casa u oficina.

En la siguiente tabla, se muestran los equipos que se utilizarán para el proyecto; y se toma en cuenta que el precio de los mismos se mantendrá en un plazo de 5 años, aunque normalmente estos precios tienden a bajar conforme el tiempo, lo que significa que esto puede hacer el proyecto más barato con el tiempo.

Tabla II. **Costo del hardware**

Tabla de Costos del Hardware			
Concepto	**Cantidad**	**Costo Unitario**	**Costo total**
Raspberry Pi	1	Q 400,00	Q 400,00
Módulo Relés (8 relés)	1	Q 100,00	Q 100,00
Accesorios para Rasberry Pi (memoria microSD y cargador AC/DC)	1	Q 150,00	Q 150,00
IP pública para servidor y conexión a internet en servidor	1	Q 200,00	Q 200,00
Cableado para conexión de dispositivos	1	Q 200,00	Q 200,00
		Total hardware	**Q 1 050,00**

Fuente: elaboración propia.

Debido a que el software utilizado para el proyecto es OpenSource, este no representa algun gasto en un tiempo de 5 años, normalmente estos se mantienen gratuitos por tiempo indefinido. Los programas que se utilizarán y no representan costos son servidor de VPN, servidor Web, Python para el manejo de puertos y el cliente VPN.

Los costos que debe tener en cuenta el cliente para mantener el proyecto incluyendo los servicios de instalación, mantenimiento y soporte en un tiempo de un año son los siguientes:

Tabla III. **Costos de uso del proyecto**

Tabla de Costos Uso del proyecto en Cliente				
Concepto	**Cantidad**	**Costo Unitario**	**Costo Mensual**	**Costo anual**
Servicio de Internet e IP pública	1	Q 200,00	Q 200,00	Q 2 400,00
Servicio de Instalación y soporte	1	Q 100,00	Q 100,00	Q 1 200,00
		Total Costos	**Q 300,00**	**Q 3 600,00**

Fuente: elaboración propia.

CONCLUSIONES

1. Se realizó el diseño de un sistema de control a distancia de dispositivos electronicos de una casa u oficina a través de VPN segura.

2. Se presentaron los distintos tipos de VPN que existen, explicando su uso y las ventajas de su implementación en domotica.

3. Se diseño la arquitectura física y lógica del sistema, integrando de la mejor manera los factores que componen el sistema, para su correcto funcionamiento.

4. Se presentó el modelo de la correcta configuración, de los factores que integran la comunicación, en una VPN cliente – servidor.

5. Se presentó el modelo de la integración de tres lenguajes de programación para el manejo de los dispositivos finales.

6. Se detallaron las caracteristicas y tareas que ejecuta cada parte del sistema para su correcta integración.

7. Se mostraron los alcances de las minicomputadoras en proyectos de domotica y empresas pyme.

8. Se mostró los alcances de una VPN, las ventajas de su uso, y el nivel de seguridad que brinda a las conexiones remotas.

9. Se detallaron los gastos de implementación, mantenimiento y soporte del proyecto.

RECOMENDACIONES

1. Como todo sistema informático, es ideal realizar actualizaciones del software y programas utilizados, para que el proyecto se mantenga actualizado y a la vanguardia de las mejoras tecnológicas, y se encuentra cubierto contra las nuevas amenazas.

2. Mantener un monitoreo constante del funcionamiento de las herramientas que integran el sistema es de vital importancia, no solo para llevar un control, sino para detectar puntos que pudieran ser vulnerables o mejorados.

3. Debido a que la Rasbperry Pi se está utilizando como un servidor y como punto de control y procesamiento, y que es posible realizar copias de respaldo, no está de más mantener guardada más de una copia, por motivos de seguridad y emergencias.

4. Como el sistema posee la capacidad de almacenar registros de eventos, toda esta información debe ser almacenada para llevar un análisis y diagnosticar comportamientos y buscar puntos de mejora para el sistema.

5. Para el circuito electrónico, desarrollar mantenimientos preventivos continuos de los dispositivos, soldaduras, limpieza, entre otros. Para mantener un circuito estable, y disponible en todo momento.

6. Los costos deben recalcularse continuamente en un promedio de seis meses, para obtener datos más exactos, porque los valores van variando continuamente, en cuanto a precios de materiales y servicios.

BIBLIOGRAFÍA

1. 1 and 1**.** *Configurando servidor web en Raspberry Pi*. [en línea]. <https://www.1and1.es/digitalguide/servidores/configuracion/como-configurar-un-servidor-web-raspberry-pi-con-lamp/>. [Consulta: 20 de septiembre de 2017].

2. Carrod**.** *Módulo de relés*. [en línea]. <https://www.carrod.mx/products/modulo-de-reles-4-canales-5-v-con-optoacoplador-generico>. [Consulta: 15 de octubre de 2017].

3. Electricidadtonin**.** *Raspberry Pi creando red privada virtual*. [en línea]. <https://www.electricidadtonin.com/raspberry-creando-red-privada-virtual-vpn/>. [Consulta: 20 de enero de 2018].

4. Electronicshub**.** *Circuito de relés*. [en línea]. <https://www.electronicshub.org/arduino-controlled-power-outlet/>. [Consulta: 15 de octubre de 2017].

5. Geekland**.** *Instalación de servidor OpenVPN en Raspberry PI*. [en línea]. <https://geekland.eu/instalar-servidor-openvpn-raspberry-pivpn/>. [Consulta: 20 de enero de 2018].

6. Le vpn**.** *Historio de la VPN*. [en línea]. <https://www.le-vpn.com/es/la-historia-de-la-vpn/>. [Consulta: 2 de diciembre de 2017].

7. Nobbot**.** *Que es una VPN*. [en línea]. <http://www.nobbot.com/tecnologia/mi-conexion/vpn-%C2%BFque-es-y-para-que-sirve/>. [Consulta: 2 de diciembre de 2017].

8. Peatonet**.** *Control de pines GPIO desde interfaz web*. [en línea]. <https://www.peatonet.com/raspberry-pi-y-los-pines-gpio-controlando-el-led-desde-una-interfaz-web/>. [Consulta: 9 de septiembre de 2017].

9. _____**.** *Controlando pines GPIO usando Python*. [en línea]. <http://www.peatonet.com/raspberry-pi-y-los-pines-gpio-controlando-un-led-con-bash-y-con-python/>. [Consulta: 9 de septiembre de 2017].

10. Raspberry Pi**.** *Conexión para relés y Raspberry Pi*. [en línea]. <https://www.raspberrypi.org/forums/viewtopic.php?t=141494>. [Consulta: 15 de diciembre de 2017].

11. _____**.** *Usando Python*. [en línea]. <https://www.raspberrypi.org/documentation/usage/python/>. [Consulta: 20 de febrero de 2018].

12. Redeszone**.** *Configuración de servidor VPN*. [en línea]. <https://www.redeszone.net/2017/02/17/pivpn-es-la-opcion-mas-facil-y-rapida-para-configurar-un-servidor-openvpn-en-tu-raspberry-pi/>. [Consulta: 10 de enero de 2018].

13. Rogueaxis**.** *Configuración VPN utilizando OpenVPN*. [en línea]. <https://www.rogueaxis.com/blog/raspberry/pivpn-configura-una-vpn-casera-en-una-raspberry-pi-utilizando-openvpn/>. [Consulta: 12 de noviembre de 2017].

14. Vpnmentor**.** *Diferentes tipos de VPN y cuando usarlas*. [en línea]. <https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/>. [Consulta: 3 de septiembre de 2017].

15. Wikipedia**.** *Red Privada Virtual*. [en línea]. <https://es.wikipedia.org/wiki/Red_privada_virtual>. [Consulta: 25 de septiembre de 2017].

16. _____**.** *Matt Blaze*. [en línea]. <https://en.wikipedia.org/wiki/Matt_Blaze>. [Consulta: 10 de septiembre de 2017].

17. _____**.** *Protocolo SwIPe*. [en línea]. <https://en.wikipedia.org/wiki/SwIPe_(protocol)>. [Consulta: 18 de septiembre de 2017].

18. _____**.** *IPsec*. [en línea]. <https://es.wikipedia.org/wiki/IPsec>. [Consulta: 20 de octubre de 2017].

19. _____**.** *PPTP*. [en línea]. <https://es.wikipedia.org/wiki/PPTP>. [Consulta: 20 de octubre de 2017].

20. _____**.** *OpenVPN*. [en línea]. <https://es.wikipedia.org/wiki/OpenVPN>. [Consulta: 12 de marzo de 2018].

21. _____**.** *Raspberry Pi*. [en línea]. <https://es.wikipedia.org/wiki/Raspberry_Pi>. [Consulta: 05 de octubre de 2017].

22. _____**.** *Python*. [en línea]. < https://es.wikipedia.org/wiki/Python>. [Consulta: 17 de marzo de 2018].

23. Xataka**.** *Usos y ventajas de una conexión VPN*. [en línea]. <https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>. [Consulta: 25 de septiembre de 2017].