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

DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA

Pedro Josué Chamale Perez
Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, septiembre de 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

PEDRO JOSUÉ CHAMALE PEREZ
ASESORADO POR LA INGA. INGRID RODRIGUEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, SEPTIEMBRE DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

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

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Francisco García
EXAMINADOR	Ing. Julio Solares
EXAMINADOR	Inga. Ingrid Rodríguez
SECRETARIO	Ing. Hugo Humberto Rivera Perez

HONORABLE TRIBUNAL EXAMINADOR

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

DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 27 de septiembre 2019.

Pedro Josué Chamale Perez

Guatemala 11 de marzo de 2020

Ingeniero
Julio César 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 e implementación de un sistema de comunicación bidireccional, mediante el servicio VoIP con el estándar SIP, utilizando GNU/LINUX en una computadora de placa reducida**¨, del señor **Pedro Josué Chamalé Pérez**, por considerar que cumple con los requisitos establecidos.

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

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 13 de mayo de 2020

Señor Director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA,** desarrollado por el estudiante **Pedro Josué Chamalé Pérez**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

REF. EIME 243.2020.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área , al trabajo de Graduación del estudiante Pedro Josué Chamalé Pérez titulado: **"DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA" ,** procede a la autorización del mismo.

Ing. Armando Alonso Rivera Carrillo

Guatemala, 27 de julio de 2020.

Decanato
Facultad de Ingeniería
24189101- 24189102

DTG. 255.2020.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Eléctrica, al Trabajo de Graduación titulado: **DISEÑO E IMPLEMENTACION DE UN SISTEMA DE COMUNICACIÓN BIDIRECCIONAL, MEDIANTE EL SERVICIO VOIP CON EL ESTANDAR SIP, UTILIZANDO GNU/LINUX EN UNA COMPUTADORA DE PLACA REDUCIDA** presentado por el estudiante universitario: **Pedro Josué Chamale Perez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Anabela Cordova Estrada
Decana

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Guatemala, septiembre de 2020

AACE/asga

ACTO QUE DEDICO A:

Dios	Por ser mi principal guía a lo largo de esta carrera, por darme la fuerza necesaria para seguir adelante y no rendirme.
Mis padres	Luis Chamalé y Miriam Pérez. Son las personas que más admiro en mi vida, son mi motivación y mi inspiración. No lo habría logrado sin su ejemplo de padres trabajadores, por todo su apoyo, amor, comprensión, consuelo y por tantas noches de desvelos juntos.
Daniel Chamalé	Por ser mi primer maestro a lo largo de la carrera, ser una gran influencia en mi persona y ser un gran consejero en los momentos cuando más lo he necesitado.
Roberto Chamalé	Por ser la persona que me ha enseñado a ser paciente, que me ha brindado todo su apoyo necesario para continuar durante este duro recorrido.
Astrid Chamalé	Por ser la princesa de la familia y el ángel que nos motiva a todos a seguir adelante sin importar lo difícil que parezca.

Gracias a ustedes por la ayuda que me brindaron, por tantas tristezas que supimos superar como familia y sobre todo por tanta felicidad que este día ha traído. Que este triunfo sea de ejemplo para su futura formación.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala

Por permitirme formar parte de esta gloriosa casa de estudios y ayudarme en mi formación académica.

Facultad de Ingeniería

Por ser mi segundo hogar y por haberme permitido pasar dentro de sus aulas viviendo buenos y difíciles momentos, gracias a todas las personas que fueron participes de este proceso, ya sea de manera directa o indirecta.

Escuela de Mecánica Eléctrica

A la ingeniera Ingrid Rodríguez por todo el conocimiento transmitido y por todo su apoyo incondicional brindado. Por permitirme conocer a excelentes compañeros y amigos; especialmente, a mi grupo de proyectos, Erwin Lemus, Marco Gómez, Eduardo López, Kevin Duarte, Juan Valdez, Jeffrey Hipp, Enrique Coloch, José Carlos, Pacifico Us, Brandon Mayorga, Dennis Perez y a todos los demás con los que trabaje un proyecto; porque en innumerables ocasiones y circunstancias a pesar de la dificultad de los retos presentados durante la carrera, se logró culminar de la mejor manera.

Departamento de Matemática

Al ingeniero Samayoa por permitirme culminar mi etapa de estudiante formando parte de este excelente lugar y conocer a personas extraordinarias; especialmente, a Kevin Itzep, Juan Carlos Martini, Josue Slansky, Erick Mendoza, Axel Ruiz, Jorge Castañeda, Luis Ramírez, Melvin Calel, Carlos Osorio, B'alam Lol, Carlos Maldonado, Jorge Cardona, Christian Estrada y a todas las demás personas del departamento de matemática, por darme el privilegio de conocer a excelentes colegas, que siempre me brindaron su conocimiento y apoyo incondicional. Que quede siempre en la memoria los buenos momentos que vivimos.

Mis compañeros de promoción

A todos aquellos con los que tuve la oportunidad de estar en un mismo salón de clases, resolviendo algún problema, comparando respuestas después de un examen o realizando algún deporte; la etapa de estudiantes que vivimos juntos será inolvidable. Gracias por su amistad y apoyo.

A Todas las personas

Que hoy me acompañan en este momento tan importante de mi vida y que me honran con su presencia. Muchas Gracias.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

LISTA DE SÍMBOLOS

Símbolo	Significado
b	bit
bps	bit por segundo
G	Giga
Gbps	Giga bit por segundo
K	Kilo
Kbps	Kilo bit por segundo
M	Mega
Mbps	Mega bit por segundo

GLOSARIO

ACL	Access Control List.
ALU	Arithmetic Logic Unit.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System.
DSL	Digital Subscriber Line.
FTP	File Transfer Protocol.
HTTP	Hypertext Transfer Protocol.
IANA	Internet Assigned Numbers Authority.
ICANN	Internet Corporation for Assigned Names and Numbers.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.

IPS	Intrusion Prevention System.
ISP	Internet Service Protocol.
ITU	International Telecommunications Union.
LAN	Local Area Network.
MAN	Metropolitan Area Network.
MOS	Metal Oxide Semiconductor.
NAT	Network Address Translation.
NIC	Network Interface Card.
OSI	Open System Interconnection.
PAN	Personal Area Network.
PC	Personal Computer.
PCM	Pulse Code Modulation.
PDU	Protocol Data Unit.
QoS	Quality of Service.
SAN	Storage Area Network.

TCP	Transmission Control Protocol.
VPN	Virtual Private Network.
WAN	Wide Area Network.
WWW	World Wide Web.

RESUMEN

La comunicación es el proceso de transmisión y recepción de ideas, información y mensajes. El acto de comunicar es un proceso complejo en el que dos o más personas se relacionan intercambiando información, por medio de códigos similares utilizando un canal que actúa de soporte a la transmisión de información.

Los dispositivos y los medios son los elementos físicos o hardware de la red. Por lo general el hardware este compuesto por los componentes visibles de la plataforma de red, como una PC, un interruptor, un enrutador, un punto de acceso inalámbrico o el cableado que se utiliza para conectar estos dispositivos.

Los dispositivos intermedios conectan los terminales individuales a la red y pueden conectar varias redes individuales para formar una red de trabajo. Estos dispositivos proporcionan conectividad y garantizan el flujo de datos en toda la red. Un dispositivo con escalabilidad, con una etapa de monitoreo y otra etapa de comunicación, reúne las características deseadas para poder facilitar el proceso de comunicación interna según sea el caso que se requiera.

La etapa de monitoreo debe contar con la disponibilidad de observar la hora exacta en la cual cada uno de los dispositivos se conectan o desconectan al servidor, así como también la dirección lógica, usuario, notificaciones de llamada, la etapa de comunicación debe contar con la disponibilidad de realizar una comunicación bidireccional con cada uno de los usuarios que se encuentran conectados a la red del servidor.

OBJETIVOS

General

Desarrollar un dispositivo con escalabilidad con etapa de comunicación y monitoreo, con comunicación bidireccional adaptable a cualquier tipo de topología.

Específicos

1. Definir los conceptos de comunicación interna y sus efectos dentro de una organización.

2. Determinar la teoría de los componentes electrónicos utilizados en el dispositivo.

3. Establecer las topologías existentes en las infraestructuras de red, para un mejor rendimiento del dispositivo.

4. Realizar el enlace de comunicación entre la computadora de placa reducida con los dispositivos finales, monitoreando el estado de conectividad de los dispositivos finales.

INTRODUCCIÓN

La comunicación es la herramienta más importante y potente que tenemos los seres humanos. Se trata sobre todo de un proceso de intercambio. La capacidad de comunicar permitirá hablar, motivar, corregir, interactuar con un grupo de personas dependiendo el enfoque que se le dé.

La información es el contenido de la comunicación y es la base de las decisiones, por ese motivo las organizaciones tienen la necesidad de tener la información disponible para poder tomar las decisiones adecuadas.

Los principales tipos de comunicación que existen dentro de una organización son: a.) sentido horizontal: esta comunicación se da entre las personas que ocupan un mismo puesto de trabajo; b), sentido vertical: esta comunicación se puede dar de arriba hacia abajo (de jefe a trabajador) o de abajo hacia arriba (de trabajador a jefe); c), sentido diagonal: esta comunicación se refiere a la interacción que se puede dar entre trabajadores o jefes que no pertenecen a un mismo departamento.

Las estrategias de comunicación interna se han convertido en un elemento indispensable y clave para dirigir el éxito empresarial de cualquier compañía o negocio. No es posible llevar adelante el trabajo en equipo sin una comunicación fluida, y no se trata solo de evitar malentendidos, sino de maximizar las potencialidades y lograr una organización fuerte y sólida.

Conocer periódicamente las opiniones de todas las personas que entran en contacto con las organizaciones: trabajadores, clientes, proveedores,

colaboradores, instituciones, etc. Por esta razón es importante fomentar la comunicación interna, construyendo el ambiente apropiado para ello y estableciendo un plan de comunicación interno.

Todas las organizaciones deben de satisfacer sus necesidades diferentes de comunicación según el ámbito de cada una de ellas, pero es importante que se realice un monitoreo y selección en los mensajes y medios que se utilicen para cumplir con dichas necesidades, tomando en cuenta el enfoque de la organización.

Una estación de trabajo, que pueda ser empleada de manera interna de la organización, así como el monitoreo de los dispositivos conectados a la red, facilitando la comunicación entre los empleados adaptándolo a las necesidades de una pequeña organización modelo, permitiendo realizar llamadas y monitorear a cada uno de los usuarios, es útil para monitorear y fortalecer un ambiente apropiado dentro de una organización.

1. LA COMUNICACIÓN Y SU IMPACTO EN UNA ORGANIZACIÓN

La comunicación es el proceso de transmisión y recepción de ideas, información y mensajes. El acto de comunicar es un proceso complejo en el que dos o más personas se relacionan intercambiando información por medio de códigos similares utilizando un canal que actúa de soporte a la transmisión de información.

La comunicación es el acto por el cual un individuo establece con otro un contacto que le permite transmitir una información en específico. En ella intervienen diversos elementos que pueden facilitar o dificultar el proceso.

La comunicación interna es lo que mantiene unida a una organización y no debe tratarse como una idea posterior que no es importante tratar. Sin ella, una compañía es solo una colección de individuos desconectados, cada uno trabajando individualmente en su propio trabajo sin importarle el desempeño que estén realizando sus compañeros de trabajo.

Se presentan los aspectos técnicos y teóricos para el desarrollo de un dispositivo con escalabilidad capaz de monitorear a cada uno de los dispositivos que se encuentren conectados a la red por medio del servidor Asterisk mediante el estándar SIP utilizando el servicio de voz por IP, diseñado para una red de una organización interna, capaz de poder extenderse a una red externa con los dispositivos intermedios (*router, switch, multilayer-switch, hub*), adecuados.

1.1. Comunicación laboral

Es el conjunto de actividades efectuadas por cualquier organización para la creación y mantenimiento de buenas relaciones entre sus miembros, a través del uso de diferentes medios de comunicación que los mantengan informados, integrados y motivados para que puedan alcanzar las metas y objetivos de la organización.

Se enlistan las principales formas de comunicación dentro de una organización.

1.1.1. Formal

Se refiere a la comunicación que se enfoca a los aspectos laborales, generalmente se realiza de forma escrita, cumpliendo con cada una de las formalidades burocráticas.

1.1.2. Informal

Es la comunicación que se enfoca a los aspectos laborales, pero su estructura no cumple con las formalidades burocráticas de la comunicación formal.

1.2. Comunicación interna

La mejor manera de lograr que una organización genere resultados positivos, que cumplan con las metas y objetivos planteados es crear vínculos fuertes entre los miembros de su equipo, para evitar malentendidos, toma de decisiones y realizar debates constructivos.

1.2.1. Comunicación horizontal

Es la comunicación que se desarrolla entre los empleados de un mismo nivel corporativo. Muy pocas veces utiliza canales oficiales y es totalmente informal.

1.2.2. Comunicación ascendente

Es la comunicación que se desarrolla desde abajo hacia arriba en la jerarquía de una organización.

1.2.3. Comunicación descendente

Es la comunicación que se desarrolla desde arriba hacia abajo en la jerarquía de una organización.

1.3. Consecuencias de una mala comunicación interna

La falta de comunicación es una de las principales causas por la que una empresa puede perder de vista los objetivos que fueron planteados. La gestión del departamento encargado de desarrollar la comunicación interna es vital, tanto como su posterior filtrado para que cada empleado se sienta motivado y que tenga claro los objetivos de la organización.

1.3.1. Moral de los empleados

La moral de los empleados disminuirá poco a poco, ya que se sentirá que la empresa no se preocupa por ellos. Pueden limitarse a hacer su trabajo y a no contribuir activamente en los objetivos de la empresa.

1.3.2. Disminución de la productividad

La mala comunicación dentro de la organización provoca una ruptura con la productividad; que el jefe no se comunique bien con los empleados y que no pueda transmitir los objetivos de manera correcta o que entre los diferentes jefes o altos cargos no fluya la comunicación.

1.3.3. Errores de los empleados

Los errores generalizados de los empleados dentro de una organización vienen dados por una falta de entendimiento. Si los empleados no conocen lo que se está haciendo en la empresa o no entiende los mensajes no podrá llevar a cabo su tarea correctamente.

1.3.4. Descontento de los clientes

Como efecto colateral de la falta de comunicación interna, los clientes pueden percibir un deterioro en el producto, servicio que se ofrece o simplemente sentirse molestos por como el mal clima laboral repercute en la atención que reciben por parte de los empleados.

1.4. Importancia de los mensajes en la comunicación interna

La información es una herramienta muy útil dependiendo el enfoque que se le pueda dar, por lo mismo es importante conocer la manera mediante la cual se puede obtener la información, conforme el tiempo pasa la tecnología va evolucionando y es importante que las empresas estén actualizadas con los diferentes medios que se utilizan para adquirir la misma.

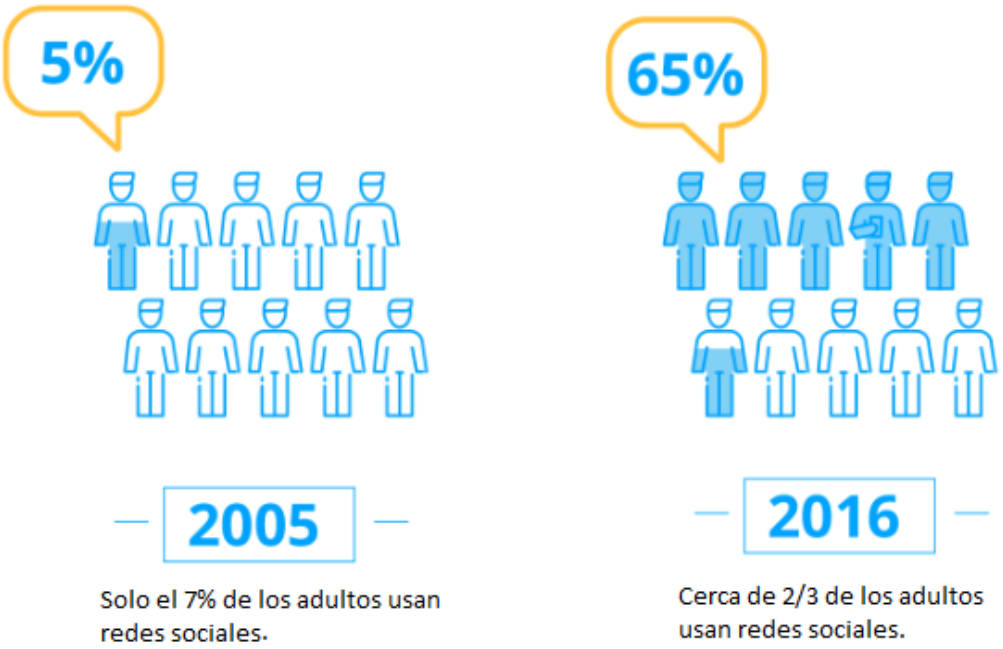
1.4.1. Fuente y origen del mensaje

En una empresa sin importar si es pequeña o grande, se debe formar un fuerte vínculo de confianza con los empleados para mejorar la productividad y el desarrollo de la empresa, esto se debe hacer informando a todos los empleados de los acontecimientos que suceden dentro de la empresa sin dejar que ellos se enteren por fuentes externas a la empresa, para esto se debe hacer uso de la tecnología que hoy en día es una herramienta muy utilizada, además se puede hacer uso de aplicaciones Android que son compatibles con la mayoría de los celulares comerciales, computadoras personales, tablets, entre otras.

Debido a la desinformación que se puede producir dentro de una organización, se puede producir un descontento entre los empleados, si se toma en cuenta solo a ciertos empleados y no a todos, produciendo de esta manera conflictos internos y malentendidos entre el personal de la organización.

De la misma manera el medio que se utilice para difundir la información debe ser confiable, no se puede permitir que dentro de la organización exista información errónea sobre los temas que se discuten, por lo cual es importante realizar ciertas restricciones para controlar las personas que se encuentren dentro de la red de la organización.

Figura 1. **Estadísticas de redes sociales**

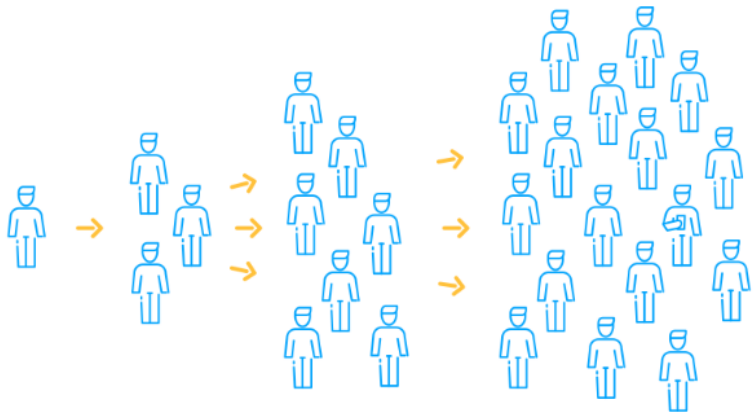


Fuente: Staffbase. *7 razones por las cuales la comunicación interna es importante para el éxito*. https://staffbase.com/blog/7-reasons-why-internal-communication-is-important-for-success. Consulta: 4 de noviembre de 2019.

1.4.2. Jerarquía de comunicación dentro de la organización

Debido a que el presidente de una organización debe cumplir con cada una de sus funciones, él debe de informar los acontecimientos que suceden a sus subalternos para que ellos sean los encargados de enviar la información a cada uno de los empleados que correspondan conocer dicha información, se suelen hacer estructuraciones en cada uno de los departamentos que forman la organización para que todo el personal este informado según sea requerido, se deben de escoger personas claves que se encarguen de hacer la divulgación de la información.

Figura 2. **Jerarquía organizacional**



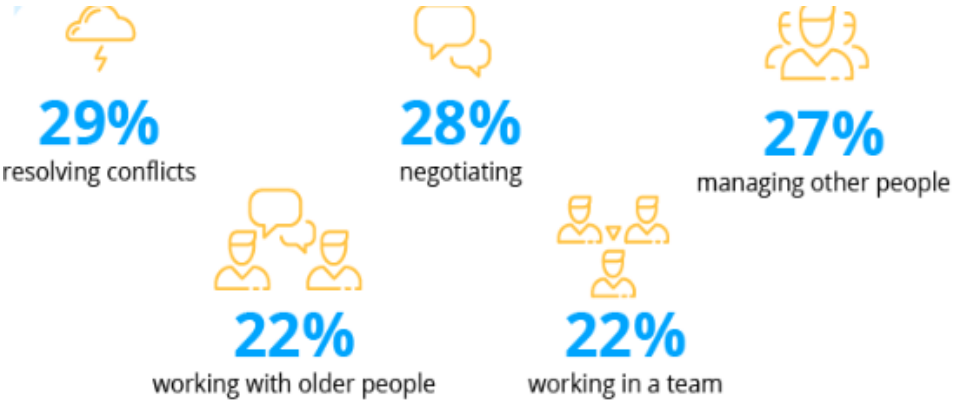
Fuente: Staffbase. *7 razones por las cuales la comunicación interna es importante para el éxito.* https://staffbase.com/blog/7-reasons-why-internal-communication-is-important-for-success. Consulta: 4 de noviembre de 2019.

Debido a que si se manejara un único grupo o medio para poder transmitir la información a cada una de las personas que forman parte de la organización, llegaría un punto en el cual el medio se saturaría de información, provocando que la información importante no llegue de manera correcta a las personas que realmente hacen el trabajo. Por lo cual la mejor opción sería enfocarse en la comunicación interna que puede hacer que este proceso sea mucho más efectivo.

La comunicación interna presenta una valiosa oportunidad para que las organizaciones comprendan mejor su fuerza laboral, capacitando de una mejor forma a sus empleados.

La comunicación interna ayuda en varios frentes, no solo para comprender de mejor manera la fuerza laboral, sino también para crear una mejor comunicación bidireccional.

Figura 3. **Porcentajes de comunicación interna**



Fuente: Staffbase. *7 razones por las cuales la comunicación interna es importante para el éxito.* https://staffbase.com/blog/7-reasons-why-internal-communication-is-important-for-success. Consulta: 4 de noviembre de 2019.

2. TEORÍA ELECTRÓNICA DEL DISPOSITIVO

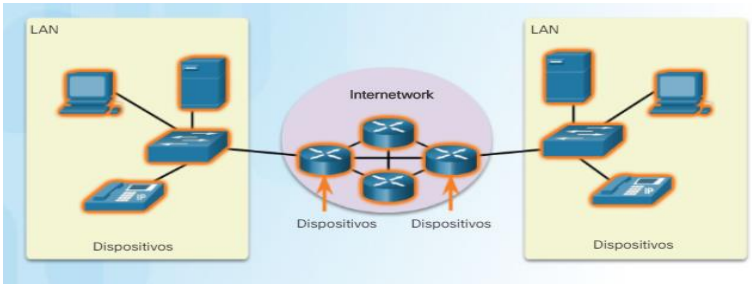
2.1. Componentes de red

La ruta que toma un mensaje desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una PC con otra o tan compleja como una red que literalmente abarque el mundo. Esta infraestructura de la red proporciona el canal estable y confiable por el cual se producen las comunicaciones. La infraestructura de red contiene tres categorías de componentes de red.

2.1.1. Dispositivos y medios de red

Los dispositivos y los medios son los elementos físicos o hardware de la red. Por lo general el hardware está compuesto por los componentes visibles de la plataforma de red, como una PC, un *switch*, un *router*, un punto de acceso inalámbrico o el cableado que se utiliza para conectar estos dispositivos.

Figura 4. **Dispositivos de red**



Fuente: Cisco Networking Academy. *Dispositivos y medios de red*. https://www.netacad.com/portal/learning. Consulta: 5 de noviembre de 2019.

2.1.1.1. Dispositivos intermedios

Los dispositivos intermedios conectan los terminales individuales a la red y pueden conectar varias redes individuales para formar una red de trabajo. Estos dispositivos proporcionan conectividad y garantizan el flujo de datos en toda la red.

Un dispositivo de red intermediario puede admitir algunas de estas funciones o todas ellas, volver a generar y transmitir las señales de datos, conservar información acerca de las rutas que existen a través de la red, notificar a otros dispositivos los errores y las fallas de comunicación, dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace, clasificar y dirigir mensajes de acuerdo a prioridades, permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad.

2.1.1.1.1. *Switch* o conmutador

Es un dispositivo de interconexión utilizado parar conectar equipos en red formando lo que se conoce como una red de área local y cuyas especificaciones técnicas siguen el estándar IEEE 802.3.

El *switch* usa aplicaciones de circuitos integrados específicos para construir y mantener sus filtros de tablas, pero la razón de usar este dispositivo es la misma; dividir el dominio de colisiones.

El *switch* es más rápido que los enrutadores porque no se toman el tiempo para verificar la información de encabezado de la red. En cambio, miran las direcciones de hardware de las tramas de datos antes de decidir si son reenviados o eliminados.

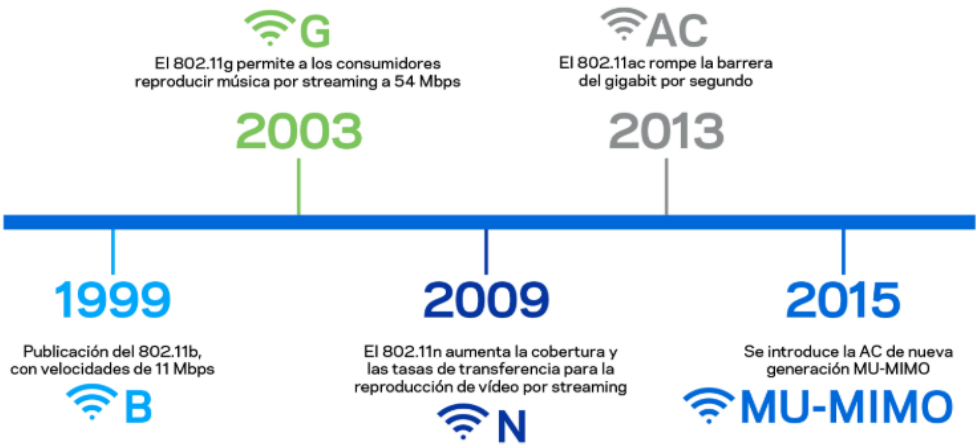
2.1.1.1.2. Router o enrutador

El funcionamiento básico de un enrutador consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen.

Cada enrutador se encarga de decidir el siguiente salto en función de su tabla de reenvió o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cual es el camino más adecuado o corto.

Este dispositivo de red es el primero que debe adaptarse a los avances de la tecnología, adaptándose a los estándares de la tecnología Wi-Fi, mientras que los dispositivos clientes suelen incorporar las nuevas tecnologías entre 6 y 12 meses después. Por esta razón es mejor preparar la red para el futuro dotándola con el estándar Wi-Fi más moderno.

Figura 5. **Estándares Wi-Fi**



Fuente: Lynksys. *¿Qué es un router WI-FI?* https://www.linksys.com/es/r/resource-center/wifi-router/. Consulta: 17 de noviembre de 2019.

2.1.1.1.3. Host

Este término se utiliza para referirse a las computadoras u otros dispositivos que son capaces de adquirir una dirección IP y que se encuentra interconectado con uno o más equipos que funcionan como el punto de inicio o el punto final de la transferencia de datos.

2.1.1.2. Medios de red

Son los distintos entornos a través de los cuales se logra hacer una conexión entre dispositivos finales y dispositivos intermedios, esta conexión puede ser por medio de un entorno físico o un entorno inalámbrico.

2.1.1.2.1. Cobre

Es el medio de transmisión físico más utilizado dentro de las organizaciones, además de ser el más abundante y accesible en el mercado, teniendo buenas propiedades conductoras siendo resistente a la corrosión y la oxidación.

La mayoría de los cables telefónicos están hechos de cobre, este es utilizado para tener acceso a internet. La alternativa a este medio de transmisión es la fibra óptica o los sistemas inalámbricos.

2.1.1.2.2. Fibra óptica

Este medio de transmisión es el más utilizado en los sistemas de telecomunicaciones debido a las características que posee este material, debido

a la flexibilidad del material óptico se puede agrupar formando cables, presentando una pérdida de transmisión menor a la del cobre.

La fibra óptica se utiliza más comúnmente como un medio para poder transmitir luz de un punto a otro, estas transmisiones se realizan a grandes distancias y a velocidades mayores.

2.1.1.2.3. Medios inalámbricos

También llamados medios no guiados debido a que no se limitan a conductores como el cobre y la fibra óptica. Los medios inalámbricos transportan señales electromagnéticas mediante frecuencia de microondas y radiofrecuencias.

Estas tecnologías de comunicación de datos inalámbricos funcionan bien en entornos abiertos. Sin embargo, existen ciertos materiales de construcción utilizados en edificios y estructuras que limitan la cobertura efectiva de los mismos. Este medio es susceptible a interferencias y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

2.1.1.3. Representación de red

Los diagramas de redes utilizan símbolos para representar los diferentes dispositivos y conexiones que componen una red. Un diagrama permite comprender fácilmente la forma en la que se conectan los dispositivos en una red grande. Este tipo de representación de una red se denomina diagrama de topología. La capacidad de reconocer las representaciones lógicas de los

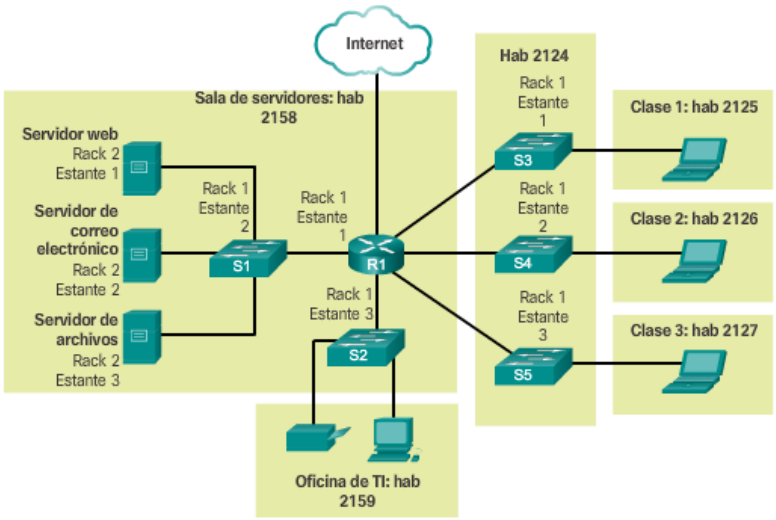
componentes físicos de red es fundamental para poder visualizar la organización y el funcionamiento de una red.

Los diagramas de topología son obligatorios para todos los que trabajan con redes. Estos diagramas proporcionan un mapa visual que muestra cómo está conectada la red.

Existen dos tipos de diagramas de topología:

- Diagrama de topología física: identifican la ubicación física de los dispositivos intermediarios y la instalación de los cables.

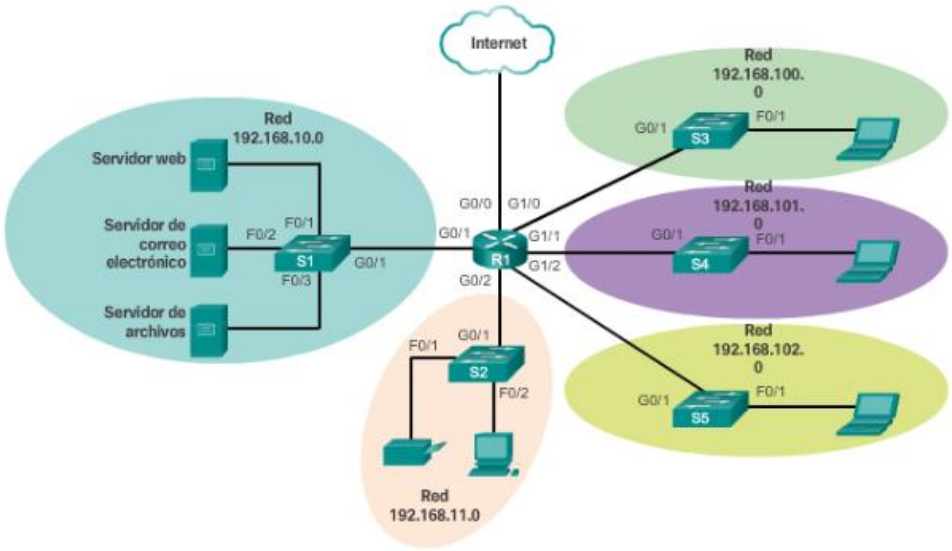
Figura 6. **Topología física**



Fuente: Cisco Networking Academy. *Fundamentos esenciales en la estructura de una red.* https://interpolados.wordpress.com/2017/02/28/representaciones-de-red/. Consulta: 9 de diciembre de 2019.

- Diagrama de topología lógica: identifican dispositivos, puertos y el esquema de direccionamiento.

Figura 7. **Topología lógica**



Fuente: Cisco Networking Academy. *Fundamentos esenciales en la estructura de una red*. https://interpolados.wordpress.com/2017/02/28/representaciones-de-red/. Consulta: 9 de diciembre de 2019.

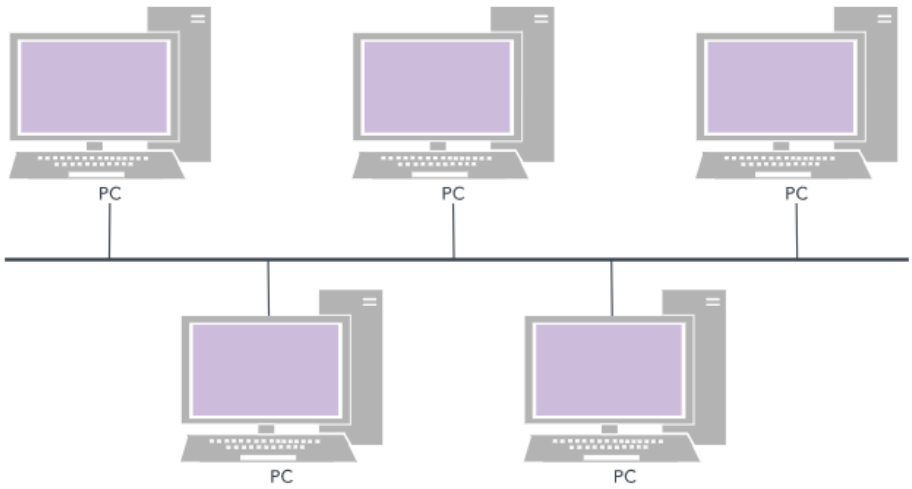
2.1.1.3.1. Topología de red

La topología de red se refiere a la disposición de los elementos dentro de una red. Al igual que los diagramas de red, las topologías de red pueden describir tanto los aspectos físicos como los lógicos de una red.

Las topologías diferentes son mejores para determinadas situaciones, porque pueden afectar el rendimiento, la estabilidad y otros resultados.

- Topología de bus: del resto por que todos sus nodos se conectan a un medio central que tiene exactamente dos puntos de conexión. Las topologías de bus se configuran fácilmente y requieren un cable más corto que otras topologías. Sin embargo, si el bus central se avería, caerá toda la red.

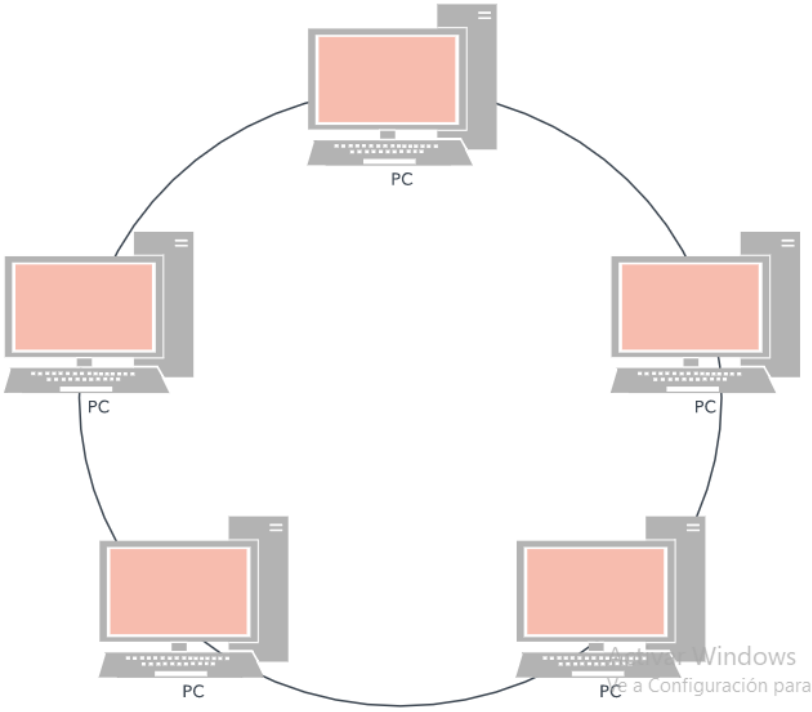
Figura 8. **Topología bus**



Fuente: Lucidchart. *¿Qué es un diagrama de red?* https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red#:~:targetText=La%20topolog%C3%ADa%20de%20red%20se,como%20%22topolog%C3%ADa%20de%20se%C3%B1al%22. Consulta: 9 de diciembre de 2019.

- Topología de anillo: Los nodos están conectados en un patrón circular, y los paquetes de información se envían mediante el anillo hasta que llegan a su destino. Las redes en anillo pueden superar a aquellas basadas en la topología de bus y se pueden reconfigurar fácilmente para agregar o eliminar dispositivos. Pero aún siguen siendo relativamente vulnerables porque toda la red falla si un solo nodo falla.

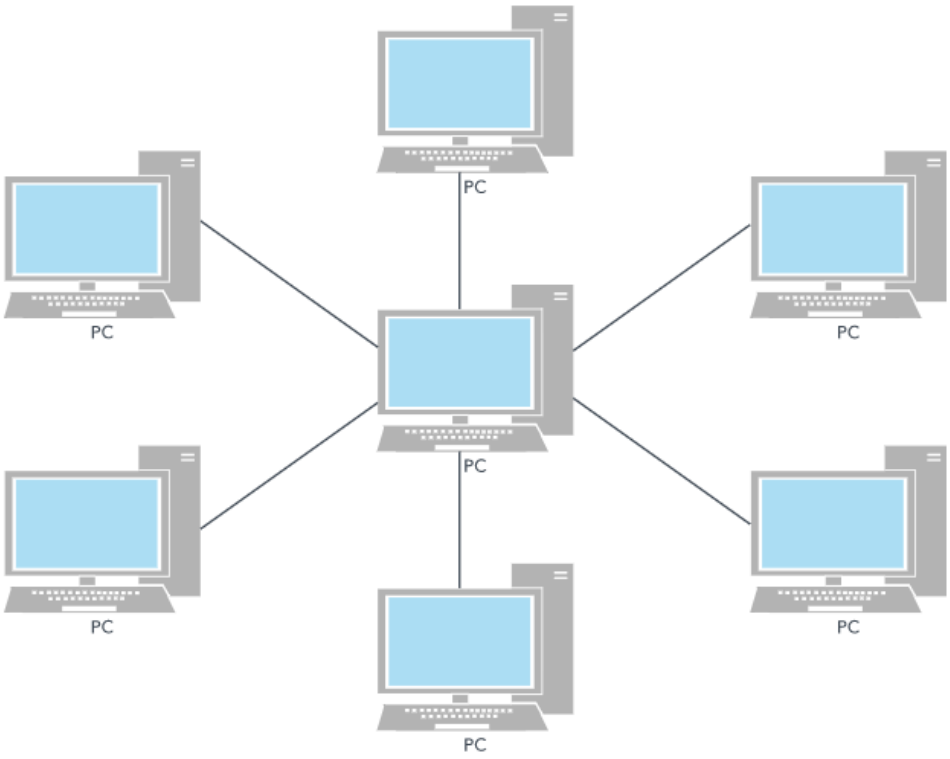
Figura 9. **Topología anillo**



Fuente: Lucidchart. *¿Qué es un diagrama de red?* https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red#:~:targetText=La%20topolog%C3%ADa%20de%20red%20se,como%20%22topolog%C3%ADa%20de%20se%C3%B1al%22. Consulta: 9 de diciembre de 2019.

- Topología de estrella: una de las topologías más comunes, consiste en un conmutador o un concentrador central mediante el cual se transfieren todos los datos, junto con todos los nodos periféricos conectados a ese nodo central. Las topologías de estrella tienden a ser confiables porque los equipos individuales pueden averiarse sin afectar al resto de la red. Pero si el *switch* o *hub* central falla, ninguno de los nodos conectados podrá acceder al mismo.

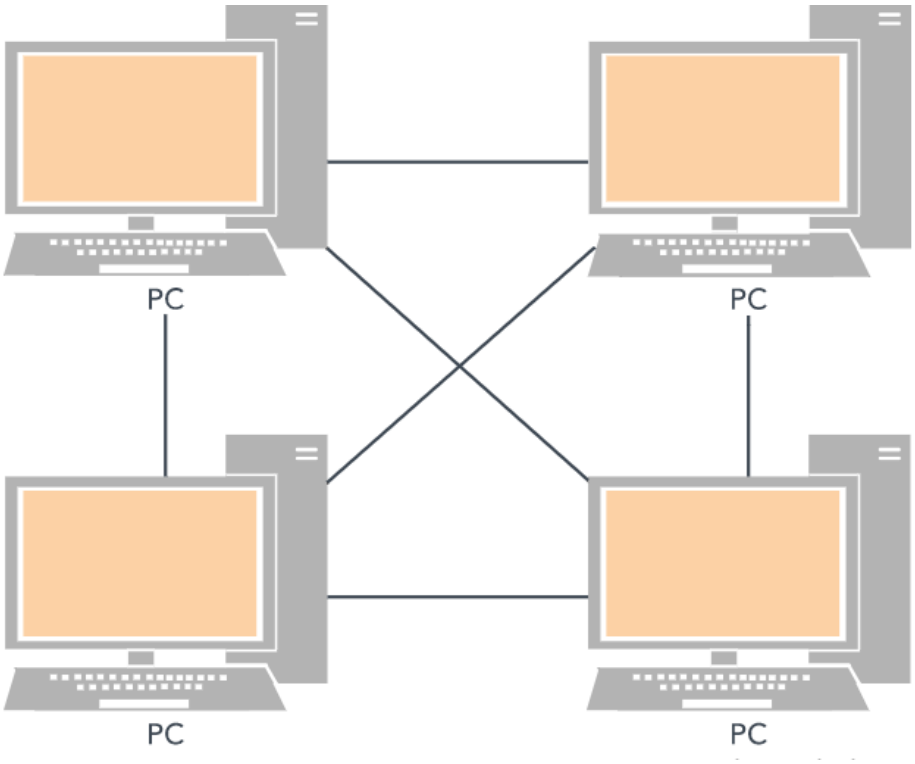
Figura 10. **Topología de estrella**



Fuente: Lucidchart. *¿Qué es un diagrama de red?* https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red#:~:targetText=La%20topolog%C3%ADa%20de%20red%20se,como%20%22topolog%C3%ADa%20de%20se%C3%B1al%22. Consulta: 9 de diciembre de 2019.

- Topología de malla: Hay dos tipos, en la primera, denominada topología de malla completa, cada nodo se conecta directamente a todos los otros nodos. El segundo tipo, malla parcial, los nodos se conectan solo a aquellos nodos con los que más interactúan. La mayoría de las redes usan combinaciones de topologías para producir lo que se denomina una topología híbrida. La topología lógica y física de una red particular pueden parecerse entre sí o pueden ser totalmente distintas.

Figura 11. **Topología de malla**



Fuente: Lucidchart. *¿Qué es un diagrama de red?* https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red#:~:targetText=La%20topolog%C3%ADa%20de%20red%20se,como%20%22topolog%C3%ADa%20de%20se%C3%B1al%22. Consulta: 9 de diciembre de 2019.

2.1.2. Tipos de redes

Las infraestructuras de red pueden variar en gran medida en términos de: el tamaño del área que abarcan, la cantidad de usuarios conectados, el área de responsabilidad, la cantidad y los tipos de servicios disponibles.

Una red de computadoras es un grupo de computadoras conectadas entre sí que le permite a la computadora comunicarse con otra computadora y compartir sus recursos, datos y aplicaciones.

2.1.2.1. LAN

Una red de área local Local Area Network, es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología. Una red de área local es una red en su versión más simple. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps y 1 Gbps. Una red de área local puede contener 100, o incluso 1 000, usuarios.

2.1.2.2. WAN

Una red de área amplia Wide Área Network, es una red de computadoras que une varias redes locales (LAN) aunque sus miembros no están 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 (ISP), para proveer conexión a sus clientes. Hoy en día, internet brinda conexiones de alta velocidad, de manera que un alto porcentaje de las redes WAN se basan en ese medio, reduciendo la necesidad de redes privadas WAN, mientras que las virtuales que utilizan cifrado y otras técnicas para generar una red dedicada sobre comunicaciones en internet, aumentan continuamente.

2.1.2.3. PAN

Una red de área personal Personal Area Network, es básicamente una red integrada por todos los dispositivos en el entorno local y cercano de su usuario,

es decir que la componen todos los aparatos que están cerca del mismo. La principal característica de este tipo de red que le permite al usuario establecer una comunicación con sus dispositivos de forma sencilla, práctica y veloz. Esta tecnología permite una alta transferencia de datos dentro de las soluciones de sistemas o redes inalámbricas.

2.1.2.4. MAN

Una red de área de metropolitana Metropolitan Area Network, es una red de alta velocidad que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas, ofrecen velocidades de 10 Mbit/s o 20 Mbit/s, sobre pares de cobre y 100 Mbit/s, 1 Gbit/s y 10 Gbit/s mediante fibra óptica.

2.1.2.5. SAN

Una red de área de almacenamiento *Storage Area Network*, es una red con una arquitectura completa que agrupa los siguientes elementos: Una red de alta velocidad de canal de fibra, un equipo de interconexión dedicado y elementos de almacenamiento de red.

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Aparte de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red

específica que se conecta a la SAN. El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza.

2.1.2.6. VLAN

Las VLAN (LAN virtuales) son agrupaciones lógicas de dispositivos en el mismo dominio de difusión. Generalmente se configuran en los conmutadores colocando algunas interfaces en un dominio de difusión y algunas interfaces en otro. Las VLAN pueden extenderse a través de múltiples conmutadores, y cada VLAN se trata como su propia subred o dominio de difusión. Esto significa que las tramas transmitidas en la red se cambiarán solo entre los puertos dentro de la misma VLAN.

Una VLAN actúa como una LAN física, pero permite que los hosts se agrupen en el mismo dominio de difusión, incluso si no están conectados al mismo conmutador. Estas son las razones principales por las que se debe usar VLAN:

- Las VLAN aumentan la cantidad de dominios de difusión mientras disminuyen su tamaño.
- Las VLAN reducen los riesgos de seguridad al reducir la cantidad de hosts que reciben copias de tramas que inundan los conmutadores.
- Puede mantener hosts que contienen datos confidenciales en una VLAN separada para mejorar la seguridad.
- Puede crear diseños de red más flexibles que agrupen a los usuarios por departamento en lugar de por ubicación física.
- Los cambios en la red se logran fácilmente con solo configurar un puerto en la VLAN apropiada.

2.1.3. Conexión a internet

Acceso a Internet o conexión a internet es el sistema de enlace con que la computadora, dispositivo móvil o red de computadoras cuenta para conectarse a Internet, lo que les permite visualizar las páginas web desde un navegador y acceder a otros servicios que ofrece Internet, como correo electrónico, mensajería instantánea, protocolo de transferencia de archivos File Transfer Protocol, entre otros.

Se puede acceder a internet desde una conexión por línea conmutada, banda ancha fija (a través de cable coaxial, cables de fibra óptica o cobre), vía satélite, banda ancha móvil y teléfonos celulares o móviles con tecnología 2G, 3G, 4G y 5G. Las empresas que otorgan acceso a Internet reciben el nombre de proveedores de servicios de Internet, Internet Service Provider.

La red de telefonía mundial fue diseñada para reproducir con claridad voces humanas, para realizarlo utiliza un sistema que es capaz de transmitir señales entre 350 Hz y 3 400 Hz. La conversión de estas señales análogas a digitales es llamada PCM Pulse Code Modulación.

Además del acceso desde el hogar, la escuela y el lugar de trabajo, el acceso a Internet puede estar disponible desde lugares públicos como bibliotecas y cibercafés, donde hay computadoras con conexión a Internet. Algunas bibliotecas proporcionan estaciones para conectar físicamente las computadoras portátiles de los usuarios a las redes de área local (LAN).

2.1.3.1. Internet

Internet no pertenece a una persona o un grupo. Garantizar una comunicación efectiva en esta infraestructura heterogénea requiere la aplicación de estándares y tecnologías uniformes, y comúnmente reconocidas, así como también la cooperación de muchas agencias de administración de redes. Existen organizaciones que se desarrollaron con el fin de ayudar a mantener la estructura y la estandarización de los protocolos y los procesos de Internet. Entre estas organizaciones, se encuentran el Grupo de trabajo de ingeniería de Internet (IETF), la Corporación de Internet para la Asignación de Nombres y Números (ICANN) y el Consejo de Arquitectura de Internet (IAB), entre muchas otras.

El término internet (con i minúscula), se utiliza para describir un conjunto de redes interconectadas. Para referirse al sistema global de redes de computadoras interconectadas, o World Wide Web, se utiliza el término Internet (con I mayúscula).

Existen varias formas diferentes de conectar a usuarios y organizaciones a Internet. Generalmente, los usuarios domésticos, los trabajadores a distancia y las oficinas pequeñas requieren una conexión a un proveedor de servicios de Internet (ISP), para acceder a Internet. Las opciones de conexión varían considerablemente según los ISP y la ubicación geográfica. Sin embargo, las opciones más utilizadas incluyen banda ancha por cable, banda ancha por la línea de suscriptor digital (DSL), redes WAN inalámbricas y servicios móviles.

Normalmente, las organizaciones necesitan acceder a otros sitios corporativos y a Internet. Para admitir servicios empresariales, como telefonía IP, videoconferencias y el almacenamiento en centros de datos, se requieren conexiones rápidas.

2.1.3.2. Intranet

Una intranet es una red informática que utiliza la tecnología del protocolo de internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.

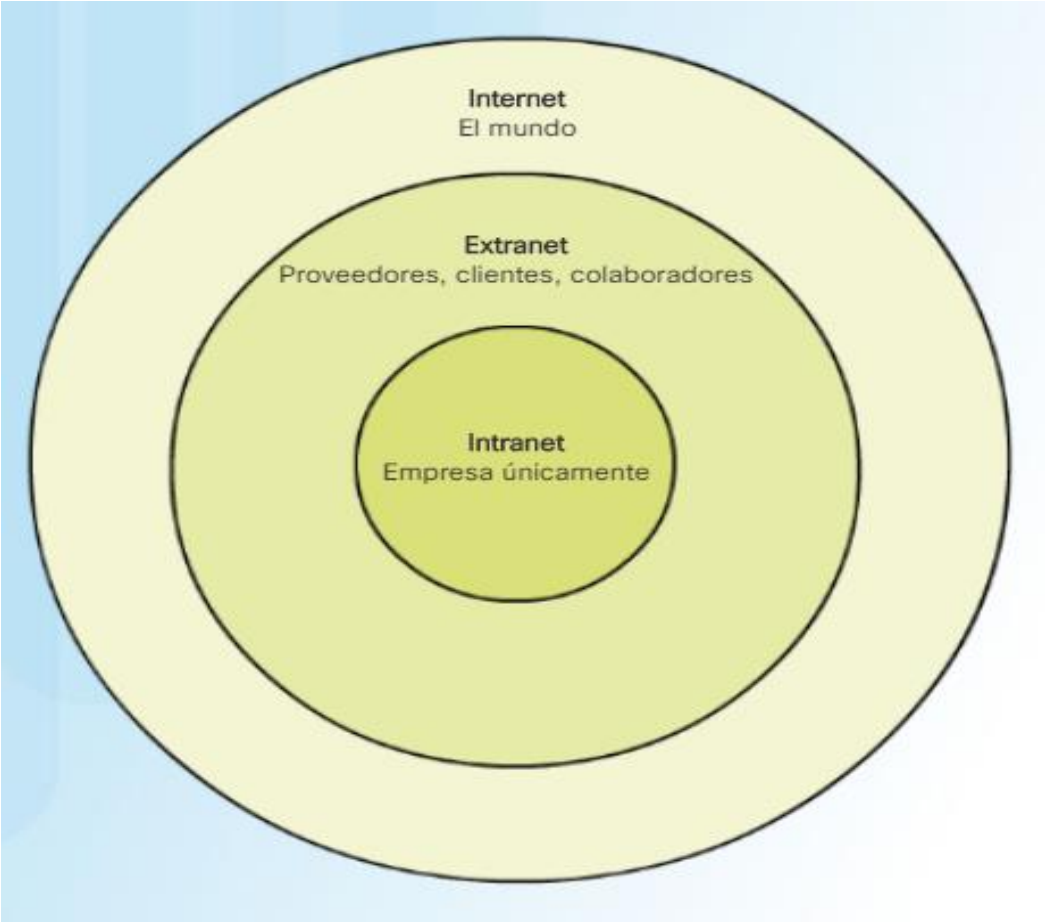
El término intranet con frecuencia se utiliza para hacer referencia a una conexión privada de LAN y WAN que pertenece a una organización y está diseñada para que accedan a ella solo los miembros y los empleados de la organización u otras personas autorizadas.

2.1.3.3. extranet

Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella, usualmente utilizando Internet y sus protocolos.

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa.

Figura 12. **Internet, intranet y extranet**



Fuente: Cisco Networking Academy*. Introducción a redes*. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.2.3.2. Consulta: 10 de diciembre de 2019.

2.1.4. Arquitectura de red

La arquitectura de red es el diseño de una red informática. Es un marco para la especificación de los componentes físicos de una red, su organización, configuración funcional, sus principios y procedimientos operativos, así como los protocolos de comunicación utilizados.

En telecomunicaciones, la especificación de una arquitectura de red también puede incluir una descripción detallada de productos y servicios entregados a través de una red de comunicaciones, así como tarifas detalladas y estructuras de facturación bajo las cuales se compensan los servicios.

La arquitectura de red de Internet se expresa predominantemente por el uso de Internet Protocol Suite, en lugar de un modelo específico para interconectar redes o nodos en la red, o el uso de tipos específicos de enlaces de hardware.

Las redes deben admitir una amplia variedad de aplicaciones y servicios, así como funcionar a través de los distintos tipos de cables y dispositivos que componen la infraestructura física. En este contexto, el término arquitectura de red se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red.

A medida que las redes evolucionan, se descubre que existen cuatro características básicas que las arquitecturas subyacentes necesitan para cumplir con las expectativas de los usuarios:

2.1.4.1. Tolerancia a fallas

Se espera que Internet esté siempre disponible para los millones de usuarios que confían en ese servicio. Para lograrlo, se requiere una arquitectura de red desarrollada para tener tolerancia a fallas. Una red con tolerancia a fallas es aquella que limita el impacto de las fallas, de modo que la cantidad de dispositivos afectados sea la menor posible. Igualmente, se arma de forma tal que permita una recuperación rápida cuando se produce una falla. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una

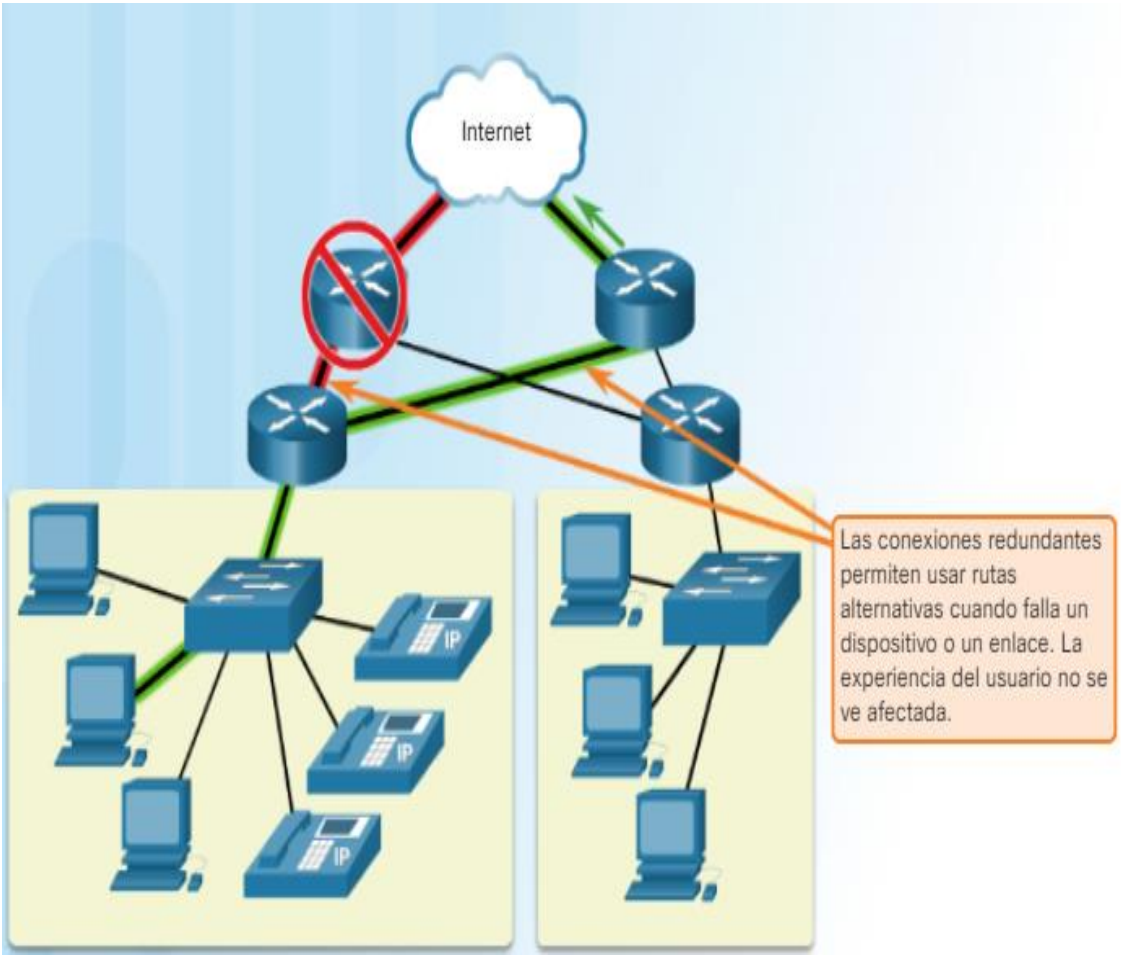
ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia.

Una de las formas en la que las redes confiables proporcionan redundancia es mediante la implementación de una red conmutada por paquetes. La conmutación por paquetes divide el tráfico en paquetes que se enrutan a través de una red compartida. Un solo mensaje, como un correo electrónico o una transmisión de vídeo, se divide en múltiples bloques de mensajes, llamados paquetes. Cada paquete tiene la información de dirección necesaria del origen y el destino del mensaje. Los enrutadores dentro de la red conmutan los paquetes según la condición de la red en ese momento. Esto significa que todos los paquetes en un mismo mensaje pueden tomar distintas rutas para llegar a destino.

Esto no sucede en las redes de conmutación de circuitos que, tradicionalmente, se utilizan para las comunicaciones de voz. Una red de conmutación de circuitos es aquella que establece un circuito dedicado entre el origen y el destino antes de que los usuarios se puedan comunicar. Si la llamada se termina de forma inesperada, los usuarios deben iniciar una conexión nueva.

En la figura 13, el usuario no se da cuenta y no se ve afectado por el cambio dinámico de rutas que hace el enrutador cuando falla un enlace.

Figura 13. **Tolerancia a fallas**



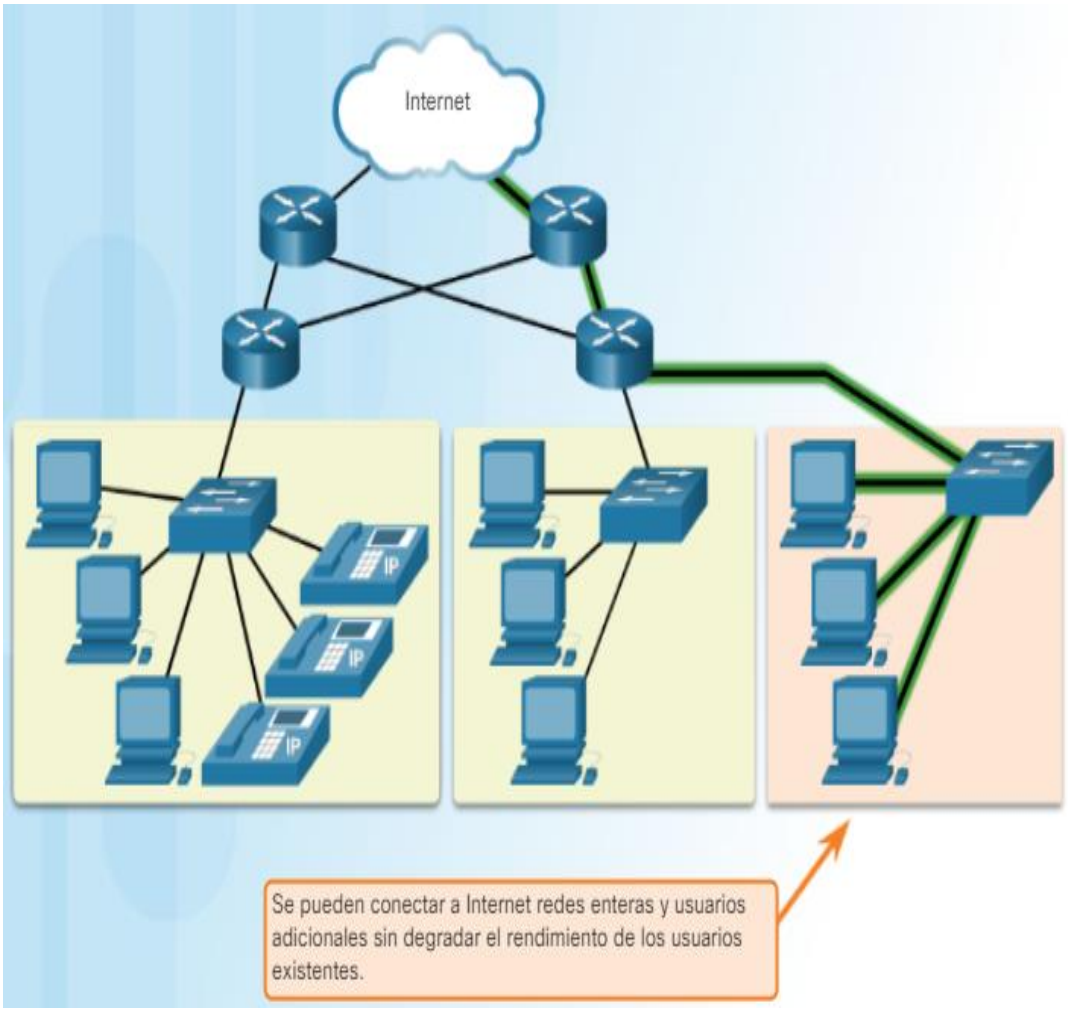
Fuente: Cisco Networking Academy. *Introducción a redes*. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.3.2.2. Consulta: 11 de diciembre de 2019.

2.1.4.2. Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. En la figura 13, se muestra cómo puede agregarse una red nueva a una red existente con facilidad. Además, las redes son escalables porque

los diseñadores siguen los estándares y protocolos aceptados. Esto permite que los proveedores de software y hardware se centren en mejorar los productos y servicios sin tener que preocuparse en la elaboración de un nuevo conjunto de reglas para poder funcionar en la red.

Figura 14. **Escalabilidad**



Fuente: Cisco Networking Academy. *Introducción a redes.* https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.3.2.3. Consulta: 11 de diciembre de 2019.

2.1.4.3. Calidad de servicio

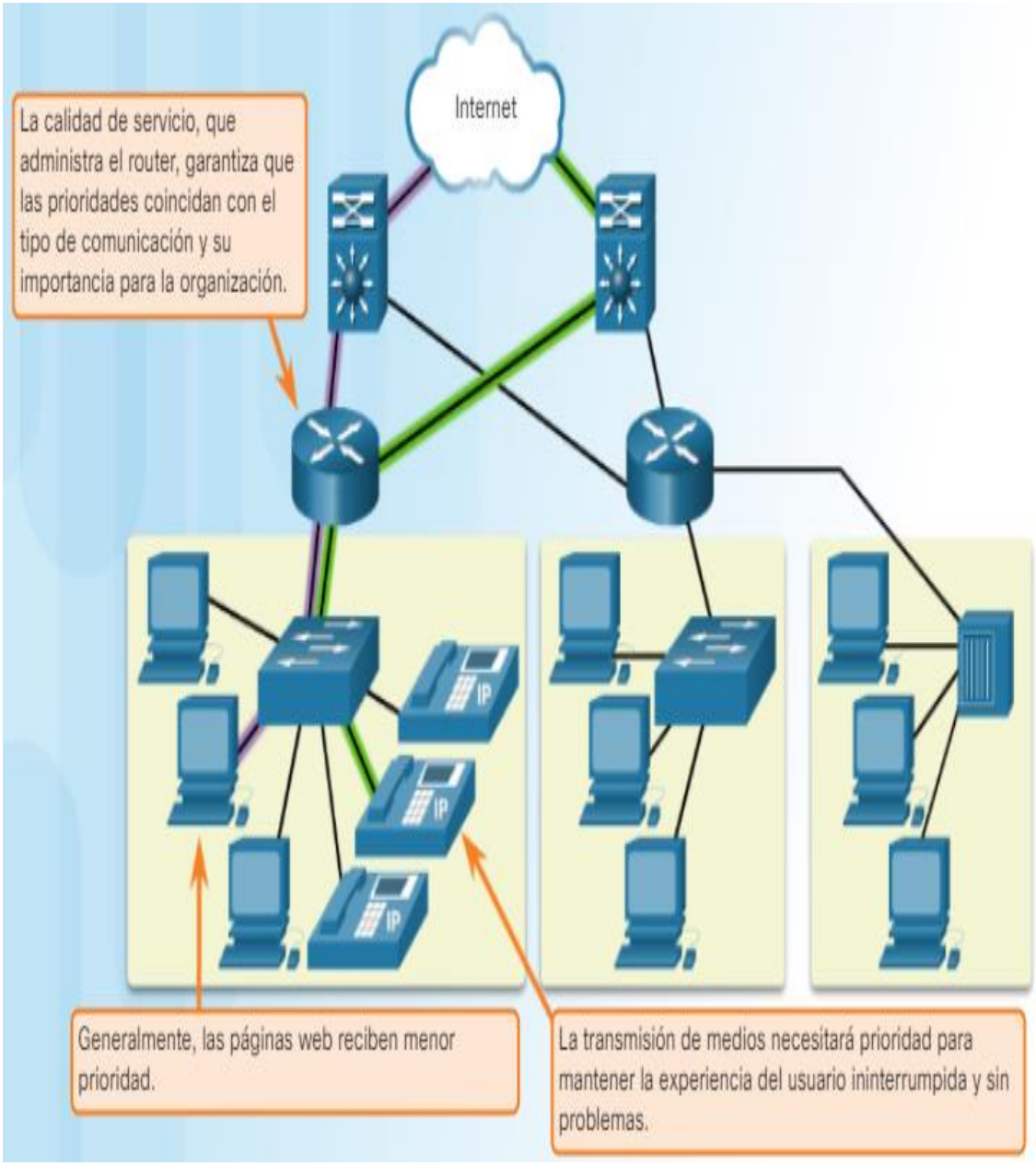
La calidad de servicio (QoS, Quality of Service), también es un requisito cada vez más importante para las redes hoy en día. Las nuevas aplicaciones disponibles para los usuarios en *internetworks*, como las transmisiones de voz y de vídeo en vivo generan expectativas más altas sobre la calidad de los servicios que se proporcionan. ¿Alguna vez intentó mirar un vídeo con interrupciones y pausas constantes? A medida que el contenido de datos, voz y vídeo sigue convergiendo en la misma red, QoS se convierte en un mecanismo principal para administrar la congestión y garantizar el envío confiable de contenido a todos los usuarios.

La congestión se produce cuando la demanda de ancho de banda excede la cantidad disponible. El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps). Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red.

Cuando el volumen de tráfico es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos.

En la figura 15, un usuario solicita una página web y otro está realizando una llamada telefónica. Con una política de QoS, el enrutador puede administrar el flujo de datos y el tráfico de voz, dando prioridad a las comunicaciones de voz si la red se congestiona.

Figura 15. **Calidad de servicio**



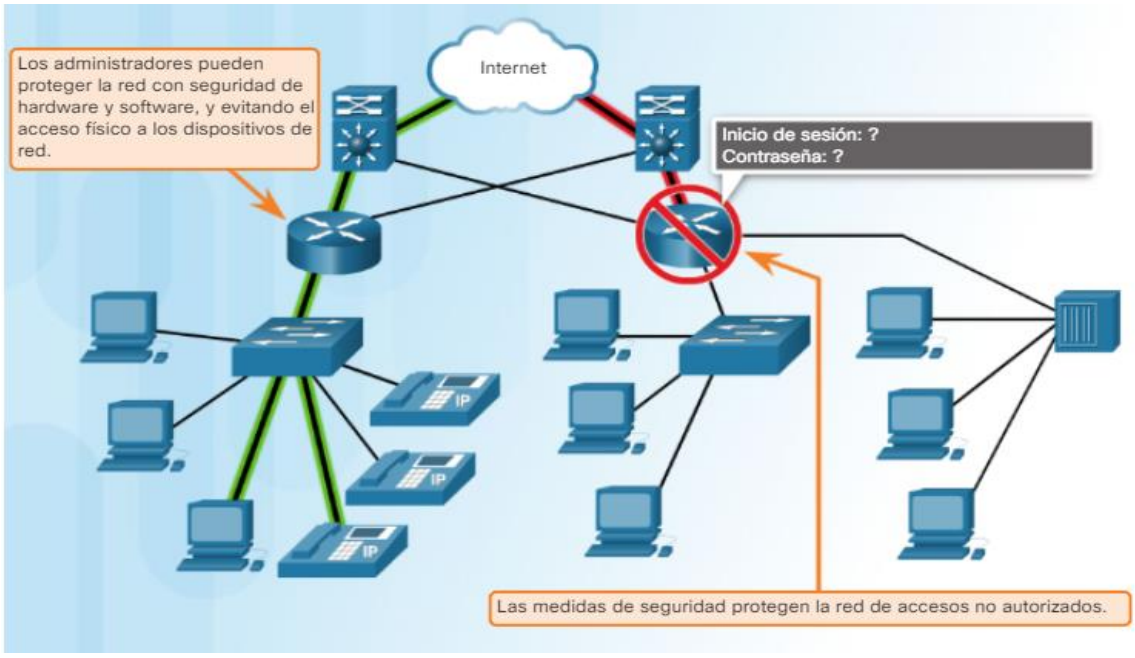
Fuente: Cisco Networking Academy*. Introducción a redes*. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.3.2.4. Consulta: 11 de diciembre de 2019.

2.1.4.4. Seguridad

La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Existen dos tipos de problemas de seguridad de red que se deben tratar: la seguridad de la infraestructura de red y la seguridad de la información.

La seguridad de la infraestructura de una red incluye el aseguramiento físico de los dispositivos que proporcionan conectividad y evitan el acceso no autorizado al software administrativo que reside en ellos, como se muestra en la figura 16.

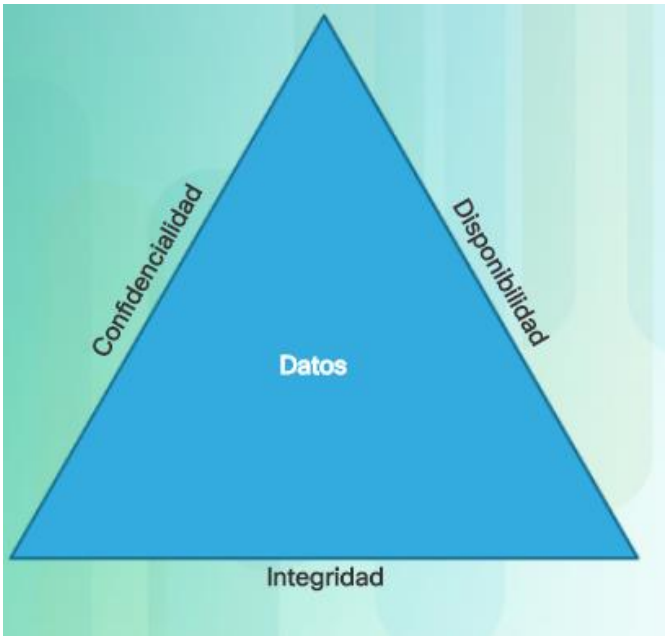
Figura 16. **Seguridad**



Fuente: Cisco Networking Academy. *Introducción a redes.* https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.3.2.5. Consulta: 11 de diciembre de 2019.

La seguridad de la información se refiere a proteger la información que contienen los paquetes que se transmiten por la red y la información almacenada los dispositivos conectados a la red. Para alcanzar los objetivos de seguridad de la red, hay tres requisitos principales, que se muestran en la figura 17:

Figura 17. **Requisitos de seguridad**



Fuente: Cisco Networking Academy*. Introducción a redes.* https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.3.2.5. Consulta: 11 de diciembre de 2019.

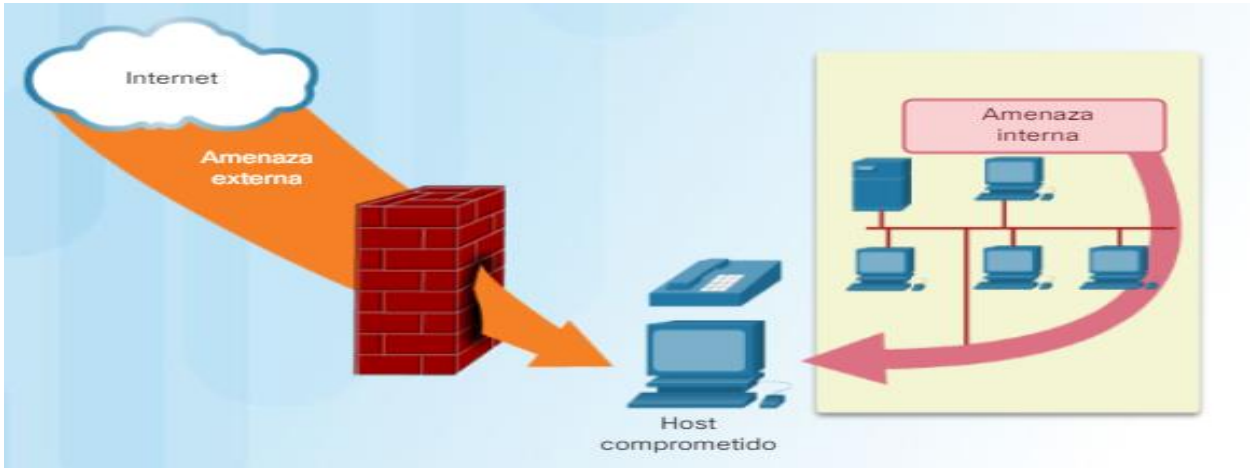
- Confidencialidad: se refiere a que solamente los destinatarios deseados y autorizados pueden acceder a los datos y leerlos.
- Integridad: significa tener la seguridad de que la información no se va a alterar en la transmisión, del origen al destino.
- Disponibilidad: significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados.

2.1.5. Amenazas de seguridad

La seguridad de la red es una parte integral de las redes de PC, independientemente de si la red está limitada a un entorno doméstico con una única conexión a Internet o si es tan extensa como una empresa con miles de usuarios. La seguridad de la red implementada debe tener en cuenta el entorno, así como las herramientas y los requisitos de la red. Debe poder proteger los datos y, al mismo tiempo, mantener la calidad de servicio que se espera de la red.

La protección de la red incluye protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar amenazas. Los vectores de amenazas pueden ser externos o internos. En la actualidad, muchas amenazas de seguridad de red externas se expanden por Internet.

Figura 18. **Amenazas de seguridad**



Fuente: Cisco Networking Academy. *Introducción a redes*. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.4.3.1. Consulta: 11 de diciembre de 2019.

Las amenazas externas más comunes a las redes incluyen las siguientes:

- Virus, gusanos y caballos de troya: se trata de software malicioso y códigos arbitrarios que se ejecutan en un dispositivo de usuario.
- *Spyware* y *adware*: software instalado en un dispositivo de usuario que recopila información sobre el usuario de forma secreta.
- Ataques de hora cero: ataque que ocurre el mismo día en que se hace pública una vulnerabilidad.
- Ataques de *hackers*: ataque de una persona experta a los dispositivos de usuario o recursos de red.
- Ataques por denegación de servicio: ataques diseñados para reducir o para bloquear aplicaciones y procesos en un dispositivo de red.
- Intercepción y robo de datos: ataque para capturar información privada en la red de una organización.
- Robo de identidad: ataque para robar las credenciales de inicio de sesión de un usuario a fin de acceder a datos privados.

También es importante tener en cuenta las amenazas internas. Se llevaron a cabo numerosos estudios que muestran que las violaciones de datos más comunes suceden a causa de los usuarios internos de la red. Esto se puede atribuir a dispositivos perdidos o robados o al mal uso accidental por parte de los empleados, y dentro del entorno comercial, incluso a empleados maliciosos.

2.1.6. Soluciones de seguridad

No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad. Si un

componente de seguridad no puede identificar ni proteger la red, hay otros que pueden hacerlo.

En general, la implementación de seguridad de las redes domésticas es muy básica. Se suele implementar en los terminales de conexión, así como en el punto de conexión a Internet e incluso puede depender de servicios contratados al ISP.

Por otra parte, la implementación de seguridad de la red en redes de las empresas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico. Lo ideal es que todos los componentes funcionen juntos, lo que minimiza la necesidad de mantenimiento y aumenta la seguridad.

Los componentes de seguridad de la red para redes domésticas o de oficinas pequeñas deben incluir, como mínimo, lo siguiente:

- Antivirus y *antispyware*: protegen los terminales de infecciones con software malicioso.
- Filtrado de *firewall*: bloquean accesos no autorizados a la red. Esto puede incluir un sistema de *firewall* ejecutado en un host que se implemente para impedir el acceso no autorizado al terminal o un servicio de filtrado básico en el enrutador doméstico para impedir el acceso no autorizado del mundo exterior a la red.

Además de lo anterior, las redes más grandes y las redes corporativas generalmente tienen otros requisitos de seguridad:

- Sistemas de *firewall* dedicados: para proporcionar funcionalidades de *firewall* más avanzadas que puedan filtrar una gran cantidad de tráfico con mayor granularidad.
- Listas de control de acceso (ACL): filtran el acceso y el reenvío de tráfico.
- Sistemas de prevención de intrusión (IPS): identifican amenazas de rápida expansión, como ataques de día cero o de hora cero.
- Redes privadas virtuales (VPN): proporcionan un acceso seguro a los trabajadores remotos.

Los requisitos de seguridad de la red deben tener en cuenta el entorno de red, así como las diversas aplicaciones y los requisitos informáticos. Tanto los entornos domésticos como las empresas deben poder proteger sus datos y, al mismo tiempo, mantener la calidad de servicio que se espera de cada tecnología. Además, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, en constante cambio.

El estudio de las amenazas de seguridad de red y de las técnicas de mitigación comienza con una comprensión clara de la infraestructura de *switching* y *routing* subyacente utilizada para organizar los servicios de red.

2.2. Microcontrolador

Un microcontrolador es una computadora pequeña en un solo chip de circuito integrado de óxido de metal semiconductor (MOS). En la terminología moderna, es similar pero menos sofisticado que un sistema en un chip (SoC); un SoC puede incluir un microcontrolador como uno de sus componentes. Un microcontrolador contiene una o más CPU junto con memoria y periféricos de entrada/salidas programables. La memoria de programa en forma de RAM, también se incluye a menudo en el chip, así como una pequeña cantidad de RAM.

Los microcontroladores están diseñados para aplicaciones integradas, en contraste con los microprocesadores utilizados en computadoras personales u otras aplicaciones de propósito general que consisten en varios chips discretos.

Los microcontroladores se utilizan en productos y dispositivos controlados automáticamente, como sistemas de control de motores de automóviles, dispositivos médicos implantables, controles remotos, máquinas de oficina, electrodomésticos, herramientas eléctricas, juguetes y otros sistemas integrados. Al reducir el tamaño y el costo en comparación con un diseño que utiliza un microprocesador, memoria y dispositivos de entrada / salida separados, los microcontroladores hacen que sea económico controlar digitalmente aún más dispositivos y procesos.

Los microcontroladores de señal mixta son comunes, integrando componentes analógicos necesarios para controlar sistemas electrónicos no digitales. En el contexto de Internet de las cosas, los microcontroladores son un medio económico y popular de recopilación de datos, detección y actuación del mundo físico como dispositivos de vanguardia.

Los microcontroladores están diseñados para reducir el costo económico y el consumo de energía de un sistema en particular. Por eso el tamaño de la unidad central de procesamiento, la cantidad de memoria y los periféricos incluidos dependerán de la aplicación. El control de un electrodoméstico sencillo como una batidora utilizará un procesador muy pequeño (4 u 8 bits) porque sustituirá a un autómata finito. En cambio, un reproductor de música y/o vídeo digital requerirá de un procesador de 32 bits o de 64 bits y de uno o más códecs de señal digital. El control de un sistema de frenos ABS se basa normalmente en un microcontrolador de 16 bits, al igual que el sistema de control electrónico del motor en un automóvil.

Los microcontroladores representan la inmensa mayoría de los chips de computadoras vendidos, sobre un 50 % son controladores simples y el restante corresponde a DSP más especializados. Mientras se pueden tener uno o dos microprocesadores de propósito general en casa, usted tiene distribuidos seguramente entre los electrodomésticos de su hogar una o dos docenas de microcontroladores. Pueden encontrarse en casi cualquier dispositivo electrónico como automóviles, lavadoras, hornos microondas, teléfonos, entre otros.

Un microcontrolador difiere de una unidad central de procesamiento normal, debido a que es más fácil convertirla en una computadora en funcionamiento, con un mínimo de circuitos integrados externos de apoyo. La idea es que el circuito integrado se coloque en el dispositivo, enganchado a la fuente de energía y de información que necesite, y eso es todo. Un microprocesador tradicional no le permitirá hacer esto, porque espera que todas estas tareas sean manejadas por otros chips. Hay que agregarle los módulos de entrada/salida (puertos) y la memoria para almacenamiento de información.

2.2.1. Arquitectura del microcontrolador

Básicamente existen dos arquitecturas de computadoras, y por supuesto, están presentes en el mundo de los microcontroladores: Von Neumann y Harvard. Ambas se diferencian en la forma de conexión de la memoria al procesador y en los buses que cada una necesita.

2.2.1.1. Arquitectura Von Neumann

La arquitectura Von Neumann utiliza el mismo dispositivo de almacenamiento tanto para las instrucciones como para los datos, siendo la que se utiliza en un ordenador personal porque permite ahorrar una buena cantidad

de líneas de entrada/salida, que son bastante costosas, sobre todo para aquellos sistemas donde el procesador se monta en algún tipo de zócalo alojado en una placa madre. También esta organización les ahorra a los diseñadores de placas madre una buena cantidad de problemas y reduce el costo de este tipo de sistemas.

En un ordenador personal, cuando se carga un programa en memoria, a este se le asigna un espacio de direcciones de la memoria que se divide en segmentos, de los cuales típicamente están: código (programa), datos y pila. Es por ello que, se puede hablar de la memoria como un todo, aunque existan distintos dispositivos físicos en el sistema (disco duro, memoria RAM, memoria flash, unidad de disco óptico).

A pesar de que en los sistemas integrados con arquitectura Von Neumann la memoria esté segregada, y existan diferencias con respecto a la definición tradicional de esta arquitectura; los buses para acceder a ambos tipos de memoria son los mismos, del procesador solamente salen el bus de datos, el de direcciones, y el de control. Como conclusión, la arquitectura no ha sido alterada, porque la forma en que se conecta la memoria al procesador sigue el mismo principio definido en la arquitectura básica.

2.2.1.2. Arquitectura Harvard

La otra variante es la arquitectura Harvard y por excelencia la utilizada en supercomputadoras, en los microcontroladores y sistemas integrados en general. En este caso, además de la memoria, el procesador tiene los buses segregados, de modo que cada tipo de memoria tiene un bus de datos, uno de direcciones y uno de control.

La ventaja fundamental de esta arquitectura es que permite adecuar el tamaño de los buses a las características de cada tipo de memoria; además, el procesador puede acceder a cada una de ellas de forma simultánea, lo que se traduce en un aumento significativo de la velocidad de procesamiento. Típicamente los sistemas con esta arquitectura pueden ser dos veces más rápidos que sistemas similares con arquitectura Von Neumann.

La desventaja está en que consume muchas líneas de entrada/salida del procesador; por lo que en sistemas donde el procesador está ubicado en su propio encapsulado, solo se utiliza en supercomputadoras. Sin embargo, en los microcontroladores y otros sistemas integrados, donde usualmente la memoria de datos y programas comparten el mismo encapsulado que el procesador, este inconveniente deja de ser un problema serio y es por ello que, la arquitectura Harvard se usa en la mayoría de los microcontroladores.

Un microcontrolador se puede configurar de diferentes maneras, siempre y cuando se respete el tamaño de memoria que este requiera para su correcto funcionamiento.

2.2.2. Procesador

El procesador tiene diferentes arquitecturas, dependiendo del momento en que se creó, así como de las posibles aplicaciones que pueda tener. Aún con esas diferencias, se pueden resumir algunos parámetros básicos para todos.

2.2.2.1. Registros

Son un espacio de memoria muy reducido pero necesario para cualquier microprocesador, de aquí se toman los datos para varias operaciones que debe

realizar el resto de los circuitos del procesador. Los registros sirven para almacenar los resultados de la ejecución de instrucciones, cargar datos desde la memoria externa o almacenarlos en ella.

Aunque la importancia de los registros parezca trivial, no lo es en absoluto. De hecho, una parte de los registros, la destinada a los datos, es la que determina uno de los parámetros más importantes de cualquier microprocesador. Cuando se dice que un procesador es de 4, 8, 16, 32 o 64 bits, se refiriere a procesadores que realizan sus operaciones con registros de datos de ese tamaño y por supuesto, esto determina muchas de las potencialidades de estas máquinas.

Mientras mayor sea el número de bits de los registros de datos del procesador, mayores serán sus prestaciones, en cuanto a poder de cómputo y velocidad de ejecución, porque este parámetro determina la potencia que se puede incorporar al resto de los componentes del sistema, por ejemplo, no tiene sentido tener una ALU de 16 bits en un procesador de 8 bits.

2.2.2.2. Unidad de control

Esta unidad es de las más importantes en el procesador, en ella recae la lógica necesaria para la decodificación y ejecución de las instrucciones, el control de los registros, la ALU, los buses y cuanta cosa más se quiera meter en el procesador.

La unidad de control es uno de los elementos fundamentales que determinan las prestaciones del procesador, porque su tipo y estructura determina parámetros como el tipo de conjunto de instrucciones, velocidad de ejecución, tiempo del ciclo de máquina, tipo de buses que puede tener el sistema,

manejo de interrupciones y un buen número de cosas más que en cualquier procesador van a parar a este bloque.

2.2.2.3. Unidad aritmeticológica

Como los procesadores son circuitos que hacen básicamente operaciones lógicas y matemáticas, se le dedica a este proceso una unidad completa, con cierta independencia. Aquí es donde se realizan las sumas, restas, y operaciones lógicas típicas del álgebra de Boole.

Actualmente este tipo de unidades ha evolucionado mucho y los procesadores más modernos tienen varias ALU, especializadas en la realización de operaciones complejas como las operaciones en punto flotante. De hecho, en muchos casos le han cambiado su nombre por el de coprocesador matemático, aunque este es un término que surgió para dar nombre a un tipo especial de procesador que se conecta directamente al procesador más tradicional.

2.2.2.4. Buses

Son el medio de comunicación que utilizan los diferentes componentes del procesador para intercambiar información entre sí, eventualmente los buses o una parte de ellos estarán reflejados en los pines del encapsulado del procesador.

En el caso de los microcontroladores, no es común que los buses estén reflejados en el encapsulado del circuito, porque estos se destinan básicamente a las entradas/salidas de propósito general y periféricos del sistema.

Existen tres tipos de buses:

- Dirección: se utiliza para seleccionar al dispositivo con el que se quiere trabajar, o en el caso de las memorias, seleccionar el dato que se desea leer o escribir.
- Datos: se utiliza para mover los datos entre los dispositivos de hardware (entrada y salida).
- Control: se utiliza para gestionar los distintos procesos de escritura lectura y controlar la operación de los dispositivos del sistema.

2.2.3. Diseño embebido

Un microcontrolador puede considerarse un sistema autónomo con procesador, memoria y periféricos y puede usarse como un sistema integrado. La mayoría de los microcontroladores en uso hoy en día están integrados en otra maquinaria, como automóviles, teléfonos, electrodomésticos y periféricos para sistemas informáticos.

Si bien algunos sistemas embebidos son muy sofisticados, muchos tienen requisitos mínimos para la memoria y la longitud del programa, sin sistema operativo y con baja complejidad de software. Los dispositivos de entrada y salida típicos incluyen interruptores, relés, solenoides, led, pantallas de cristal líquido pequeñas o personalizadas, dispositivos de radiofrecuencia y sensores para datos como temperatura, humedad, nivel de luz, entre otros. Los sistemas integrados generalmente no tienen teclado, pantalla, discos, impresoras u otros dispositivos de entrada/salidas reconocibles de una computadora personal, y pueden carecer de dispositivos de interacción humana de cualquier tipo.

2.2.3.1. Interrupciones

Los microcontroladores deben proporcionar una respuesta en tiempo real (predecible, aunque no necesariamente rápida) a los eventos en el sistema integrado que controlan. Cuando ocurren ciertos eventos, un sistema de interrupción puede indicarle al procesador que suspenda el procesamiento de la secuencia de instrucciones actual y comience una rutina de servicio de interrupción (ISR, o manejador de interrupción), que realizará cualquier procesamiento requerido basado en la fuente de la interrupción, antes volviendo a la secuencia de instrucciones original. Las posibles fuentes de interrupción dependen del dispositivo y a menudo incluyen eventos como un desbordamiento interno del temporizador, completar una conversión de analógico a digital, un cambio de nivel lógico en una entrada, como presionar un botón, y datos recibidos en un enlace de comunicación. Cuando el consumo de energía es importante como en los dispositivos de batería, las interrupciones también pueden despertar a un microcontrolador de un estado de reposo de baja potencia donde el procesador se detiene hasta que un evento periférico requiera que haga algo.

2.2.3.2. Programas

Por lo general, los programas de microcontroladores deben caber en la memoria en chip disponible, porque sería costoso proporcionar un sistema con memoria externa expandible. Los compiladores y ensambladores se utilizan para convertir códigos de lenguaje de ensamblaje y de alto nivel en un código de máquina compacto para almacenar en la memoria del microcontrolador. Dependiendo del dispositivo, la memoria del programa puede ser permanente, memoria de solo lectura que solo se puede programar en la fábrica, flash de solo lectura o memoria de solo lectura que se puede modificar en el campo.

2.3. Raspberry pi

Raspberry pi es un ordenador de placa reducida u ordenador de placa simple (SBC) de bajo coste desarrollado en el Reino Unido por la Raspberry Pi Foundation, con el objetivo de estimular la enseñanza de informática en las escuelas. El modelo original se convirtió en más popular de lo que se esperaba, hasta incluso vendiéndose afuera del mercado objetivo para usos como robótica. No incluye periféricos (como teclado y ratón) o carcasa.

Aunque no se indica expresamente si es hardware libre o con derechos de marca, en su web oficial explican que disponen de contratos de distribución y venta con dos empresas, pero al mismo tiempo cualquiera puede convertirse en revendedor o redistribuidor de las tarjetas *Raspberry Pi*, por lo que da a entender que es un producto con propiedad registrada, manteniendo el control de la plataforma, pero permitiendo su uso libre tanto a nivel educativo como particular.

En cambio, el software sí es de código abierto, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10. En todas sus versiones, incluye un procesador Broadcom, memoria RAM, GPU, puertos USB, HDMI, Ethernet (el primer modelo no lo tenía), 40 pines GPIO (desde la Raspberry Pi 2) y un conector para cámara. Ninguna de sus ediciones incluye memoria, siendo esta en su primera versión una tarjeta SD y en ediciones posteriores una tarjeta MicroSD.

La fundación da soporte para las descargas de las distribuciones para arquitectura ARM, Raspbian (derivada de Debian), RISC OS 5, Arch Linux ARM (derivado de Arch Linux) y Pidora (derivado de Fedora) y promueve

principalmente el aprendizaje del lenguaje de programación Python. Otros lenguajes también soportados son Tiny BASIC, C, Perl y Ruby.

3. MÓDULO DE UNIDAD DE CONTROL

La unidad de control es un componente de la unidad central de procesamiento de una computadora que dirige el funcionamiento del procesador. Le dice a la memoria de la computadora, la unidad aritmética y lógica y los dispositivos de entrada y salida cómo responder a las instrucciones que se han enviado al procesador.

Dirige el funcionamiento de las otras unidades proporcionando señales de temporización y control. La mayoría de los recursos informáticos son administrados por la unidad de control. Dirige el flujo de datos entre la CPU y los otros dispositivos. En los diseños modernos de computadoras, la unidad de control es típicamente una parte interna de la CPU con su función y operación general sin cambios desde su introducción.

Para coordinar la unidad de control con cada uno de los procesos que se llevarán a cabo en este proceso es necesario conocer los protocolos de comunicación que se utilizaran para llevar a cabo el proceso de comunicación.

3.1. Protocolos y comunicaciones de red

Las redes conectan cada vez más. Las personas se comunican en línea desde cualquier lugar. Las conversaciones que tienen lugar en las aulas pasan a las sesiones de chat de mensajes instantáneos, y los debates en línea continúan en el lugar de estudios. Diariamente, se desarrollan nuevos servicios para aprovechar la red.

En lugar de crear sistemas exclusivos e independientes para la prestación de cada servicio nuevo, el sector de redes en su totalidad adoptó un marco de desarrollo que permite que los diseñadores comprendan las plataformas de red actuales y las mantengan. Al mismo tiempo, este marco se utiliza para facilitar el desarrollo de nuevas tecnologías, a fin de satisfacer las necesidades de las comunicaciones y las mejoras tecnológicas futuras.

Un aspecto fundamental de este marco de desarrollo es el uso de modelos generalmente aceptados que describen reglas y funciones de red.

Una red puede ser tan compleja como los dispositivos conectados a través de Internet, o tan simple como dos PC conectadas directamente entre sí mediante un único cable, o puede tener cualquier grado de complejidad intermedia.

Las redes pueden variar en lo que respecta al tamaño, la forma y la función. Sin embargo, realizar simplemente la conexión física por cable o inalámbrica entre los terminales no es suficiente para habilitar la comunicación. Para que se produzca la comunicación, los dispositivos deben saber cómo comunicarse.

Las personas intercambian ideas mediante diversos métodos de comunicación. Sin embargo, independientemente del método elegido, todos los métodos de comunicación tienen tres elementos en común. El primero de estos elementos es el origen del mensaje, o emisor. Los orígenes de los mensajes son las personas o los dispositivos electrónicos que deben enviar un mensaje a otras personas o dispositivos. El segundo elemento de la comunicación es el destino o receptor del mensaje. El destino recibe el mensaje y lo interpreta. Un tercer elemento, llamado canal, está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.

3.1.1. Protocolos

Antes de comunicarse entre sí, las personas deben utilizar reglas o acuerdos establecidos que rijan la conversación. Estas reglas, o protocolos, deben respetarse para que el mensaje se envíe y comprenda correctamente. Los protocolos deben dar cuenta de los siguientes requisitos:

- Un emisor y un receptor identificados
- Idioma y gramática común
- Velocidad y momento de entrega
- Requisitos de confirmación o acuse de recibo

Los protocolos utilizados en las comunicaciones de red comparten muchos de estos fundamentos. Además de identificar el origen y el destino, los protocolos informáticos y de red definen los detalles sobre la forma en que los mensajes se transmiten a través de una red.

A continuación, se muestran los requisitos de los protocolos informáticos comunes. Se analizan más detalladamente cada uno de estos protocolos:

- Codificación de los mensajes
- Formato y encapsulamiento del mensaje
- Tamaño del mensaje
- Sincronización del mensaje
- Opciones de entrega del mensaje

3.1.1.1. Codificación de los mensajes

Uno de los primeros pasos para enviar un mensaje es codificarlo. La codificación es el proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación revierte este proceso para interpretar la idea.

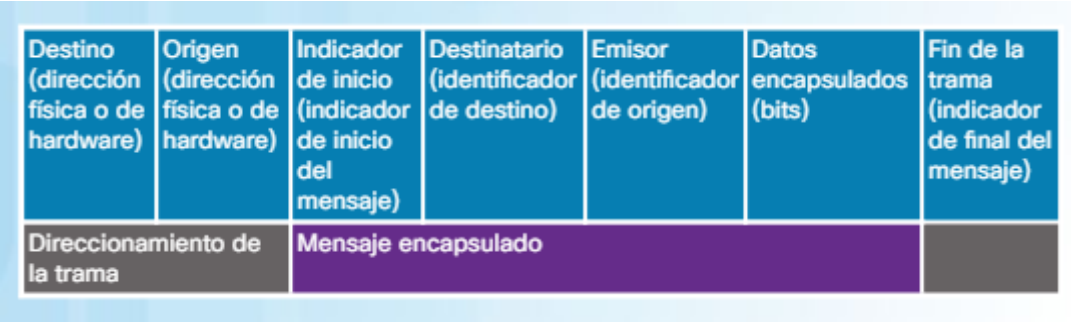
La codificación también tiene lugar en la comunicación por computadora. La codificación entre hosts debe tener el formato adecuado para el medio. El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje.

3.1.1.2. Formato y encapsulamiento del mensaje

Cuando se envía un mensaje desde el origen hacia el destino, se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje.

Un mensaje que se envía a través de una red de computadoras sigue reglas de formato específicas para que pueda ser entregado y procesado. De la misma manera en la que una carta se encapsula en un sobre para la entrega, los mensajes de las PC también se encapsulan. Cada mensaje de computadora se encapsula en un formato específico, llamado trama, antes de enviarse a través de la red. Una trama actúa como un sobre: proporciona la dirección del destino propuesto y la dirección del host de origen, como se muestra en la figura 19.

Figura 19. **Encapsulamiento del mensaje**



Fuente: *Cisco* Networking Academy*. Introducción a redes*. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.1.1.4. Consulta: 11 de diciembre de 2019.

Observe que la trama tiene un origen y un destino tanto en la parte de direccionamiento de trama como en el mensaje encapsulado.

El formato y el contenido de una trama están determinados por el tipo de mensaje que se envía y el canal que se utiliza para enviarlo. Los mensajes que no tienen el formato correcto no se pueden enviar al host de destino o no pueden ser procesados por éste.

3.1.1.3. Tamaño del mensaje

Otra regla de comunicación es el tamaño. Cuando las personas se comunican, los mensajes que envían, normalmente, están divididos en fragmentos más pequeños u oraciones. El tamaño de estas oraciones se limita a lo que la persona que recibe el mensaje puede procesar por vez. Una conversación individual puede estar compuesta por muchas oraciones más pequeñas para asegurarse de que cada parte del mensaje sea recibida y comprendida.

De manera similar, cuando se envía un mensaje largo de un host a otro a través de una red, es necesario separarlo en partes más pequeñas. Las reglas que controlan el tamaño de las partes o tramas que se comunican a través de la red, son muy estrictas. También pueden ser diferentes, de acuerdo con el canal utilizado. Las tramas que son demasiado largas o cortas no se entregan.

Las restricciones de tamaño de las tramas requieren que el host de origen divida un mensaje largo en fragmentos individuales que cumplan los requisitos de tamaño mínimo y máximo. El mensaje largo se enviará en tramas independientes, cada trama contendrá una parte del mensaje original. Cada trama también tendrá su propia información de direccionamiento. En el host receptor, las partes individuales del mensaje se vuelven a unir para reconstruir el mensaje original.

3.1.1.4. Sincronización del mensaje

Estas son las reglas de la participación para la sincronización del mensaje.

- Método de acceso: determina en qué momento alguien puede enviar un mensaje. Si dos personas hablan a la vez, se produce una colisión de información y es necesario que ambas se detengan y vuelvan a comenzar. De manera similar, las computadoras deben definir un método de acceso. Los hosts de una red necesitan un método de acceso para saber cuándo comenzar a enviar mensajes y cómo responder cuando se produce alguna colisión.
- Control de flujo: la sincronización también afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse. Si una persona habla demasiado rápido, la otra persona tendrá dificultades para escuchar y comprender el mensaje. En la comunicación de la red, los hosts

de origen y destino utilizan métodos de control de flujo para negociar la sincronización correcta a fin de que la comunicación sea exitosa.

- Tiempo de espera para la respuesta: si una persona hace una pregunta y no escucha una respuesta antes de un tiempo aceptable, la persona supone que no habrá ninguna respuesta y reacciona en consecuencia. La persona puede repetir la pregunta o puede continuar la conversación. Los hosts de las redes también tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta.

3.1.1.5. Opciones de entrega del mensaje

Un mensaje puede entregarse de distintas maneras. En algunos casos, una persona desea comunicar información a un solo individuo. Otras veces, esa persona puede necesitar enviar información a un grupo de personas simultáneamente o, incluso, a todas las personas de un área.

También puede ocurrir que el emisor de un mensaje necesite asegurarse de que el mensaje se haya entregado correctamente al destino. En estos casos, es necesario que el receptor envíe un acuse de recibo al emisor. Si no se necesita ningún acuse de recibo, se dice que el envío del mensaje es sin acuse de recibo.

Una opción de entrega de uno a uno se denomina unidifusión, que significa que el mensaje tiene solo un destinatario.

Si un host necesita enviar mensajes utilizando una opción de uno a varios, se denomina multidifusión. La multidifusión es el envío de un mismo mensaje a un grupo de hosts de destino de manera simultánea.

Si es necesario que todos los hosts de la red reciban el mensaje a la vez, se utiliza el método de difusión. La difusión representa una opción de entrega de mensaje de uno a todos. Algunos protocolos utilizan un mensaje especial de multidifusión que se envía a todos los dispositivos, lo que lo hace similar en esencia a una difusión. Asimismo, puede ser que los hosts deban emitir un acuse de recibo de algunos mensajes y no para otros.

3.1.2. Suite de protocolos

Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Los *hosts* y los dispositivos de red implementan las suites de protocolos en software, hardware o ambos.

Una de las mejores formas para visualizar el modo en que los protocolos interactúan dentro de una suite es ver la interacción como una pila. Una pila de protocolos muestra la forma en que los protocolos individuales se implementan dentro de una suite. Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores de la pila se encargan del movimiento de datos por la red y proporcionan servicios a las capas superiores, las cuales se enfocan en el contenido del mensaje que se va a enviar.

Algunas reglas de comunicación son formales y otras simplemente sobreentendidas o implícitas, basadas en los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, un nuevo conjunto de protocolos de red debe describir los requerimientos e interacciones precisos. Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Algunos de los protocolos de red más

comunes son Protocolo de transferencia de hipertexto (HTTP), el protocolo de control de transmisión (TCP), y el protocolo de Internet (IP).

La comunicación entre un servidor web y un cliente web es un ejemplo de interacción entre varios protocolos. Los protocolos más comunes son:

- HTTP: es un protocolo de aplicación que rige la forma en que interactúan un servidor web y un cliente web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor.
- TCP: es el protocolo de transporte que administra las conversaciones individuales. TCP divide los mensajes HTTP en partes más pequeñas, llamadas segmentos. Estos segmentos se envían entre los procesos del servidor y el cliente web que se ejecutan en el host de destino. También es responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.
- IP: es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignar las direcciones apropiadas y seleccionar la mejor ruta al host de destino.
- Ethernet: es un protocolo de acceso a la red que describe dos funciones principales: la comunicación a través de un enlace de datos y la transmisión física de datos en los medios de red. Los protocolos de acceso a la red son responsables de tomar los paquetes de IP y los formatean para transmitirlos por los medios.

La suite de protocolos TCP/IP es un estándar abierto, lo que significa que estos protocolos están disponibles para el público sin cargo, y cualquier proveedor puede implementar estos protocolos en su hardware o software.

Un protocolo basado en estándares es un proceso que recibió el aval del sector de redes y fue aprobado por una organización de estandarización. El uso de estándares en el desarrollo y la implementación de protocolos aseguran que productos de distintos fabricantes puedan interoperar correctamente. Si un fabricante en particular no observa un protocolo estrictamente, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes. Algunos protocolos son exclusivos, lo que significa que una empresa o proveedor controla la definición del protocolo y cómo funciona.

3.2. Organizaciones de estandarización

Los estándares se crean en los planos internacional, regional y nacional. Los Grupos de interés se reúnen junto con los organismos de normalización u organizaciones dedicadas.

La estandarización de redes no solo permite que distintas computadoras se comuniquen, sino que también incrementan el mercado para los productos que se adhieren a estos estándares.

3.2.1. Estándares abiertos

Los estándares abiertos fomentan la interoperabilidad, la competencia y la innovación. También garantizan que ningún producto de una sola empresa pueda monopolizar el mercado o tener una ventaja desleal sobre la competencia.

Las organizaciones de estandarización son importantes para mantener una Internet abierta con especificaciones y protocolos de libre acceso que pueda implementar cualquier proveedor. Las organizaciones de estandarización pueden elaborar un conjunto de reglas en forma totalmente independiente o, en otros casos, pueden seleccionar un protocolo exclusivo como base para el estándar. Si se utiliza un protocolo exclusivo, suele participar el proveedor que creó el protocolo.

Las organizaciones de estandarización generalmente son organizaciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos.

Entre estas agrupaciones se pueden encontrar las siguientes organizaciones:

- IEEE
- IETF
- IANA
- ICANN
- ITU
- TIA

3.2.2. Estándares de internet

Las organizaciones de estandarización generalmente son instituciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos. Distintas organizaciones tienen diferentes responsabilidades para promover y elaborar estándares para el protocolo TCP/IP.

- ISOC: es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo.
- IAB: es responsable de la administración y el desarrollo general de los estándares de Internet.
- IEFT: desarrolla, actualiza y mantiene las tecnologías de Internet y de TCP/IP. Esto incluye el proceso y documentación para el desarrollo de nuevos protocolos y la actualización de los protocolos existentes, conocidos como documentos de petición de comentarios.
- IRTF: está enfocado en la investigación a largo plazo en relación con los protocolos de Internet y TCO/IP, como los grupos Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) y Peer-to-Peer Research Group (P2PRG).
- ICANN: con base en los Estados Unidos, coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información utilizada por los protocolos TCP/IP.
- IANA: responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

3.3. Modelos de referencia

Modelo de referencia es un modelo normalizado que proporciona una visión integrada de alto nivel de una tecnología y sus datos; se utiliza como referencia para la construcción de modelos similares. Los modelos de referencia son útiles para proporcionar un grado de elementos de una disciplina.

3.3.1. Beneficios del uso de un modelo en capas

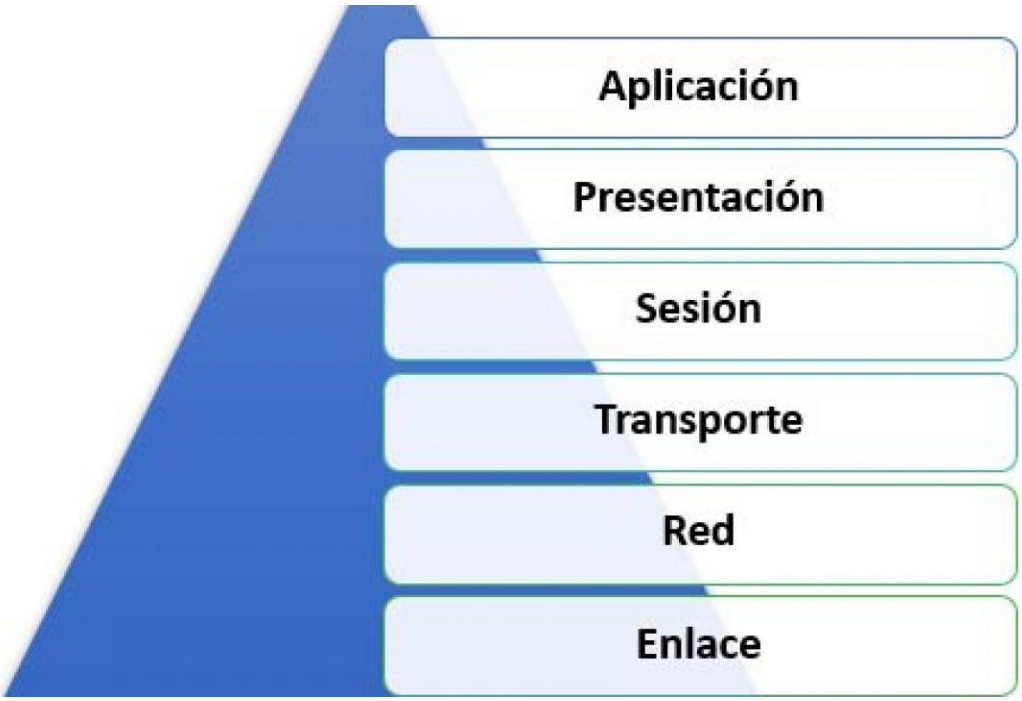
Los beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones incluyen lo siguiente:

- Ayuda en el diseño de protocolos, porque los protocolos que operan en una capa específica tienen información definida, según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
- Fomenta la competencia, porque los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las funcionalidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de red.

3.3.2. Modelo de referencia OSI

El modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.

Figura 20. **Modelo OSI**



Fuente: Profesionalreview. *Estructura del modelo OSI.* https://www.profesionalreview.com/2018/11/22/modelo-osi/. Consulta: 12 de diciembre de 2019.

Los niveles o capas de los que se compone el modelo OSI son:

- Aplicación: contiene protocolos utilizados para comunicarse proceso a proceso.
- Presentación: proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
- Sesión: proporciona servicios a la capa de presentación para organizar su dialogo y administrar el intercambio de datos.
- Transporte: define los servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales entre terminales.

- Red: proporciona servicios para intercambiar los datos individuales en la red entre terminales identificados.
- Enlace de datos: los protocolos de esta capa describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.
- Física: los protocolos de esta describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia y desde un dispositivo de red.

El modelo OSI no es la definición de una topología ni un modelo de red en sí mismo. Tampoco especifica ni define los protocolos que se utilizan en la comunicación, ya que estos están implementados de forma independiente a este modelo. Lo que realmente hace OSI es definir la funcionalidad de ellos para conseguir un estándar.

3.3.3. Modelo de protocolo TCP/IP

El conjunto de protocolos de Internet proporciona comunicación de datos de extremo a extremo que especifica cómo se deben empaquetar, direccionar, transmitir, enrutar y recibir los datos. Esta funcionalidad está organizada en cuatro capas de abstracción, que clasifican todos los protocolos relacionados de acuerdo con el alcance de las redes involucradas. De menor a mayor, las capas son:

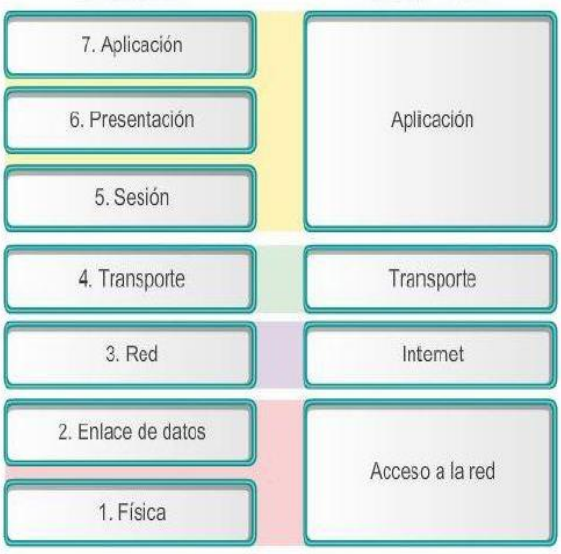
- La capa de enlace: contiene métodos de comunicación para los datos que permanecen dentro de un solo segmento de red (enlace).
- La capa de internet: proporciona interconexión entre redes independientes.
- La capa de transporte: maneja la comunicación de host a host.

- La capa de aplicación: proporciona intercambio de datos de proceso a proceso para aplicaciones.

El Equipo Técnico de Ingeniería de Internet (IETF), mantiene los estándares técnicos subyacentes al conjunto de protocolos de Internet y sus protocolos constituyentes. El conjunto de protocolos de Internet es anterior al modelo OSI, un marco de referencia más completo para sistemas de redes generales.

Las funciones de estas cuatro capas son comparables a las funciones de las siete capas del modelo OSI. La figura 21 muestra la comparación entre las capas de los dos modelos.

Figura 21. **OSI-TCP/IP**



Fuente: Ingenieria Systems. *Comparación entre modelo OSI y modelo TCP/IP.* http://www.ingenieriasystems.com/2016/10/Comparacion-entre-el-modelo-OSI-y-el-modelo-TCPIP-Comunicacion-de-mensajes-CCNA1-V5-CISCO-C3.html. Consulta: 12 de diciembre de 2019.

3.4. Transferencia de datos en la red

Transmisión de datos es la transferencia física de datos, un flujo digital de bits, por un canal de comunicación punto a punto o punto a multipunto. Los datos se representan como una señal electromagnética, una señal de tensión eléctrica, ondas radioeléctricas, microondas o infrarrojos.

Lo que se busca en la comunicación, es más información transmitida a mayor velocidad de transmisión. Por lo que la demanda de mejores características para los medios de transmisión es mayor. Esto es particularmente cierto para las redes de comunicación, en donde las condiciones requieren ser ideales debido a las posibles interferencias de máquinas eléctricas, entre otros. Por esta razón el mejor medio de transmisión depende mucho de la aplicación.

Algunos de los más habituales medios de transmisión son:

- Fibra óptica
- Cables coaxiales
- Cables trenzados

3.4.1. Encapsulamiento de datos

En teoría, una comunicación simple, como un vídeo musical o un correo electrónico puede enviarse a través de la red desde un origen hacia un destino como una transmisión de bits masiva y continua. Si en realidad los mensajes se transmitieron de esta manera, significará que ningún otro dispositivo podrá enviar o recibir mensajes en la misma red mientras esta transferencia de datos está en progreso. Estas grandes transmisiones de datos originarán retrasos importantes. Además, si falla un enlace en la infraestructura de la red interconectada durante

la transmisión, el mensaje completo se perdería y tendría que retransmitirse completamente.

Un método mejor es dividir los datos en partes más pequeñas y manejables para enviarlas por la red. La división del flujo de datos en partes más pequeñas se denomina segmentación. La segmentación de mensajes tiene dos beneficios principales:

- Primero, al enviar partes individuales más pequeñas del origen al destino, se pueden intercalar diversas conversaciones en la red, llamadas multiplexión.
- La segmentación puede aumentar la eficiencia de las comunicaciones de red. Si parte del mensaje no logra llegar al destino debido a una falla en la red o a congestión, solo se deben retransmitir las partes faltantes.

La desventaja de utilizar segmentación y multiplexión para transmitir mensajes a través de la red es el nivel de complejidad que se agrega al proceso. Suponga que tuviera que enviar una carta de 100 páginas, pero en cada sobre solo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los cien sobres requerirá mucho tiempo tanto para el remitente como para el destinatario.

En las comunicaciones de red, cada segmento del mensaje debe seguir un proceso similar para asegurar que llegue al destino correcto y que puede volverse a ensamblar en el contenido del mensaje original.

3.4.2. Acceso a los datos

Mientras los datos de la aplicación bajan a la pila del protocolo y se transmiten por los medios de la red, se agrega diversa información de protocolos en cada nivel. Esto comúnmente se conoce como proceso de encapsulamiento.

La forma que adopta una porción de datos en cualquier capa se denomina unidad de datos del protocolo (PDU). Durante el encapsulamiento, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus funciones nuevas. No existe una convención universal de nombres para las PDU.

Según la capa donde se encuentre la información que se requiere transmitir, se pueden identificar de la siguiente manera:

- Bits: unidad de datos del protocolo de capa física, que se utiliza cuando se transmiten datos físicamente por el medio.
- Tramas: unidad de datos del protocolo de capa de enlace de datos.
- Paquetes: unidad de datos del protocolo de capa de red.
- Segmentos: unidad de datos del protocolo de capa de transporte.
- Datos: termino general que se utiliza en la capa de aplicación para la unidad de datos del protocolo.

3.5. Direccionamiento lógico

En forma genérica, una dirección lógica es una dirección que enmascara o abstrae una dirección física. Las direcciones lógicas dan un nivel de abstracción por arriba de una dirección de hardware. Una dirección de hardware es aquella

utilizada por una tarjeta NIC en una red Ethernet y se encuentra grabada de fábrica en esa tarjeta.

Una dirección IP es la dirección lógica única que identifica a un ordenador en una red (local o externa). El proceso desde que los datos son incorporados al ordenador hasta que se transmiten al medio se llama encapsulación. Estos datos son formateados, segmentados, identificados con el direccionamiento lógico y físico para finalmente ser enviados al medio.

La dirección IP puede cambiar muy a menudo debido a cambios en la red, o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se le denomina también dirección IP dinámica. Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen la necesidad de una dirección IP fija. Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, porque de esta forma se permite su localización en la red.

En la actualidad se puede asignar de dos maneras diferentes una dirección lógica a cualquier dispositivo que posea una tarjeta de red, se puede utilizar direccionamiento IPv4 y direccionamiento IPv6.

3.5.1. Dirección IPv4

Las direcciones IPV4 se expresan mediante un número binario de 32 bits permitiendo un espacio de direcciones de hasta 4,294,967,296 (2^{32}), direcciones posibles.

Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

Debido a la forma en que se pueden agrupar los bits en el direccionamiento IPv4, se pueden dividir en tres clases importantes; conocidos como clase A, clase B y Clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits), para que sean asignados como direcciones disponibles, de modo que la cantidad máxima de hosts es 224-2 (no se toma en cuenta la dirección reservada para broadcast y la dirección de red), es decir, 16,777,214 direcciones disponibles.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits), para que sean asignados como direcciones disponibles, de modo que la cantidad máxima de hosts por cada red es 216-2, o 65,534 direcciones disponibles.
- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits), para que sean asignados como direcciones disponibles, de modo que la cantidad máxima de hosts por cada red es 28-2, o 254 direcciones disponibles.

3.5.2. Direcciones privadas

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT)

para conectarse a una red pública o por los hosts que no se conectan a Internet. Se reservan tres rangos no superpuestos de direcciones IPv4 para redes privadas. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión directa entre sí o que se conecten a través de un tercero que haga NAT. Las direcciones privadas son:

Figura 22. **Direcciones privadas IPv4**

Clase	Rango de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 a 10.255.255.255	10.0.0.0/8
B	172.16.0.0 a 172.31.255.255	172.16.0.0/12
C	192.168.0.0 a 192.168.255.255	192.168.0.0/16

Fuente: Cisco Networking Academy. *Clasificación de redes privadas.* https://interpolados.wordpress.com/2017/05/16/espacio-de-direcciones-ipv4-privadas/. Consulta: 3 de enero de 2020.

3.5.3. Máscara de subred

La máscara de red permite distinguir dentro de la dirección IP, los bits que identifican a la red y los bits que identifican al host. En una dirección IP versión 4, de los 32 bits que se tienen en total, se definen por defecto para una dirección clase A, que los primeros ocho bits son para la red y los restantes 24 para host, en una dirección de clase B, los primeros 16 bits son la parte de red y la de host son los siguientes 16, y para una dirección de clase C, los primeros 24 bits son la parte de red y los ocho restantes son la parte de *host*.

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando se necesita agrupar a todos los empleados pertenecientes a un departamento de una empresa. En este caso se crearía una subred que englobara las direcciones IP de estos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara.

Las redes se pueden dividir en redes más pequeñas para un mejor aprovechamiento de las direcciones IP que se tienen disponibles para los hosts, ya que estas a veces se desperdician cuando se crean subredes con una sola máscara de subred.

La división en subredes le permite al administrador de red contener los broadcasts que se generan dentro de una LAN, lo que redunda en un mejor desempeño del ancho de banda. Para comenzar la creación de subredes, se comienza pidiendo prestados bits a la parte de host de una dirección dada, dependiendo de la cantidad de subredes que se deseen crear, así como del número de hosts necesarios en cada subred.

3.5.4. Dirección IPv6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona tenga asignados varios millones de IP, ya que puede implementarse con 2^{128} (3.4×1038 hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

4. MÓDULO DE UNIDAD DE MONITOREO

En este capítulo se describirá el software y los principios de direccionamiento básico que se estarán utilizando para levantar el servidor, así como el tipo de dirección privada o pública que se utilizará, luego de analizar las diferencias entre una y otra. Además, se describirá en cierta parte que es Asterisk, esta es una de las herramientas básicas para poder desarrollar este proyecto que involucra un servicio de comunicación entre dispositivos capaces de mantener una dirección IP, utilizando el servicio de transferencia de datos mediante voz por IP, con el estándar SIP.

4.1. Asterisk

Asterisk es un marco de código abierto para crear aplicaciones de comunicaciones. Asterisk convierte una computadora ordinaria en un servidor de comunicaciones. Asterisk alimenta sistemas IP PBX, puertas de enlace VoIP, servidores de conferencia y otras soluciones personalizadas. Es utilizado por pequeñas empresas, grandes empresas, centros de llamadas, operadores y agencias gubernamentales de todo el mundo. Asterisk es gratis y de código abierto.

Hoy en día, hay más de un millón de sistemas de comunicaciones basados en Asterisk en uso, en más de 170 países. La mayoría de las veces implementada por integradores de sistemas y desarrolladores, Asterisk puede convertirse en la base de un sistema telefónico comercial completo o utilizarse para mejorar o ampliar un sistema existente o para cerrar una brecha entre sistemas.

Desde un punto de vista arquitectónico, Asterisk se compone de muchos módulos diferentes. Este módulo le brinda una flexibilidad casi ilimitada en el diseño de un sistema basado en Asterisk. Como administrador de Asterisk, da opción de elegir qué módulos cargar y la configuración de cada módulo. Cada módulo que carga proporciona capacidades diferentes al sistema. Por ejemplo, un módulo podría permitir que un sistema *Asterisk* se comunique con líneas telefónicas analógicas, mientras que otro podría agregar capacidades de informes de llamadas.

4.1.1. Arquitectura Asterisk

Asterisk tiene un núcleo que puede interactuar con muchos módulos. Los módulos llamados controladores de canal proporcionan canales que siguen el plan de marcado de Asterisk para ejecutar el comportamiento programado y facilitar la comunicación entre dispositivos o programas fuera de Asterisk. Los canales a menudo usan infraestructura de puente para interactuar con otros canales.

4.1.1.1. Núcleo

El corazón de cualquier sistema Asterisk es el núcleo. El núcleo PBX es el componente esencial que proporciona mucha infraestructura. Entre muchas funciones, lee los archivos de configuración, incluido el plan de marcado y carga todos los demás módulos, componentes distintos que proporcionan más funcionalidad.

El núcleo carga y construye el plan de marcado, que es la lógica de cualquier sistema Asterisk. El plan de marcado contiene una lista de instrucciones

que *Asterisk* debe seguir para saber cómo manejar las llamadas entrantes y salientes en el sistema.

4.1.1.2. Módulos

Además de la funcionalidad proporcionada por el núcleo de Asterisk, los módulos proporcionan todas las demás funciones. La fuente de muchos módulos se distribuye con Asterisk, aunque otros módulos pueden estar disponibles a través de miembros de la comunidad o incluso empresas que fabrican módulos comerciales. Los módulos distribuidos con Asterisk se pueden construir opcionalmente cuando se construye Asterisk.

Los módulos no solo se construyen opcionalmente, sino que puede afectar en el momento de la carga si se cargarán, el orden de carga o incluso descargarlos / cargarlos durante el tiempo de ejecución. La mayoría de los módulos son configurables independientemente y tienen sus propios archivos de configuración. Algunos módulos tienen soporte para que la configuración se lea de forma estática o dinámica (en tiempo real), desde los servidores de bases de datos.

Desde un punto de vista logístico, estos módulos son típicamente archivos con una extensión de archivo .so, que viven en el directorio de módulos de Asterisk (que generalmente es / usr / lib / asterisk / modules). Cuando se inicia Asterisk, carga estos archivos y agrega su funcionalidad al sistema.

Los módulos de asterisco que forman parte del núcleo tienen un nombre de archivo similar a pbx_xxxxx.so. Todos los tipos de módulos se analizan en la sección tipos de módulos de Asterisk.

Algunos ejemplos de módulos:

- chan_pjsip usa res_pjsip y muchos otros módulos res_pjsip para proporcionar una pila SIP para que los dispositivos SIP interactúen con Asterisk y entre ellos a través de Asterisk.
- app_voicemail proporciona funciones tradicionales de correo de voz tipo PBX.
- app_confbridge proporciona puentes de conferencia con muchas características opcionales.
- res_agi proporciona una interfaz de puerta de enlace Asterisk, una API que permite el control de llamadas desde scripts y programas externos.

4.1.1.3. Canales y llamadas

En Asterisk como navaja suiza de telefonía, el objetivo principal de Asterisk es ser un motor para construir sistemas y aplicaciones de comunicación en tiempo real.

En la mayoría de los casos, pero no en todos, esto significa que lidiará con el concepto de llamadas. Las llamadas en terminología de telefonía generalmente se refieren a un teléfono que se comunica con (llamando), otro teléfono a través de un medio, como una línea PSTN. Sin embargo, en el caso de Asterisk, una llamada generalmente hace referencia a uno o más canales existentes en Asterisk.

Algunos ejemplos de llamadas son:

- Un teléfono llamando a otro teléfono a través de Asterisk.
- Un teléfono que llama a muchos teléfonos a la vez a través de Asterisk.

- Un teléfono llama a una aplicación o sucede lo contrario. por ejemplo, app_voicemail o app_queue.
- Se crea un canal local e interactúa con una aplicación u otro canal.

Tenga en cuenta que se menciona principalmente teléfonos como ejemplo, sin embargo, puede referirse a cualquier canal o grupo de canales como una llamada. No importa si los dispositivos son teléfonos u otra cosa, como un sensor del sistema de alarma o de la puerta de garaje.

Los canales son creados por Asterisk usando los controladores de canal. Pueden utilizar otros recursos en el sistema Asterisk para facilitar varios tipos de comunicación entre uno o más dispositivos. Los canales pueden conectarse a otros canales y verse afectados por las aplicaciones y funciones. Los canales pueden hacer uso de muchos otros recursos proporcionados por otros módulos o bibliotecas externas. Por ejemplo, los canales SIP al pasar audio utilizarán el códec y los módulos de formato. Los canales pueden interactuar con muchos módulos diferentes a la vez.

Dialplan es el principal método para dirigir el comportamiento de Asterisk. Dialplan existe como archivos de texto (por ejemplo, extensiones.conf), ya sea en el lenguaje de secuencias de comandos de plan de marcado incorporado, formatos AEL o LUA. Alternativamente, dialplan podría leerse desde una base de datos, junto con otra configuración de módulo. Al escribir el plan de marcado, hará un uso intensivo de las aplicaciones y funciones para afectar los canales, la configuración y las funciones.

Dialplan también puede llamar a través de otras interfaces como AGI para recibir instrucciones de control de llamadas de scripts y programas externos.

4.1.2. Configuración principal de Asterisk

En *Asterisk* se crean diversos archivos con extensiones diferentes, sin embargo, uno de los archivos que se deben de configurar de forma primordial corresponde al archivo asterisk.conf; asterisk.conf se utiliza para configurar las ubicaciones de directorios y archivos utilizados por Asterisk, así como las opciones relevantes para el núcleo de Asterisk.

Este archivo (asterisk.conf), tiene dos contextos principales, que se muestran a continuación con algunas descripciones sobre su contenido (estos documentos los pueden observar en la sección de apéndice 1).

4.1.3. Configuración de registro

Las funciones de registro de propósito general en *Asterisk* se pueden configurar en el archivo logger.conf. Dentro de este archivo, uno puede configurar *Asterisk* para registrar mensajes en archivos y / o syslog e incluso en la consola de *Asterisk*. Tenga en cuenta que las secciones y descripciones enumeradas a continuación tienen el propósito de ser informativas y actuar como una guía al configurar el inicio de sesión en *Asterisk*. Las opciones con los valores predeterminados establecidos no tienen que establecerse explícitamente, ya que simplemente establecerán el valor predeterminado.

4.1.4. Configuración de la línea de comando

Con la excepción de la funcionalidad proporcionada por el módulo res_clialiases.so, el núcleo proporciona la interfaz de línea de comando de Asterisk. Hay algunos archivos de configuración relevantes para la CLI que verá

en una instalación predeterminada de Asterisk. Todos estos deben encontrarse en el directorio típico, entre otros, Asterisk / en una instalación predeterminada.

4.1.5. Configuración del módulo de carga

El archivo de configuración para el módulo de carga de Asterisk es modules.conf. Se lee del directorio de configuración típico de Asterisk. La configuración consta de una gran sección llamada módulos con posibles directivas configuradas dentro. Hay varias directivas que se pueden usar.

- Autoload: cuando está habilitado, Asterisk cargará automáticamente cualquier módulo que se encuentre en el directorio de módulos de Asterisk.
- Pre-load: se utiliza para especificar módulos individuales para cargar antes de que se inicialice el núcleo Asterisk. A menudo se usa para módulos en tiempo real para que los archivos de configuración se puedan enviar a un servidor antes de cargar los módulos dependientes.
- Require: establece un módulo requerido. Si un módulo requerido no se carga, Asterisk sale con el código de estado 2.
- Preload-require: una combinación de preload y require.
- Noload: no carga el módulo especificado.
- Load: carga el módulo especificado. Normalmente se usa cuando la carga automática está configurada en no.

Vea el apéndice 2 para ver la configuración de este directorio.

4.1.6. Configuración del módulo SIP

El archivo sip.conf sirve para configurar todo lo relacionado con el protocolo SIP y añadir nuevos usuarios o conectar con proveedores SIP.

El fichero sip.conf comienza con una sección [general], que contiene la configuración por defecto de todos los usuarios y peers (proveedores). Se puede sobrescribir los valores por defecto en las configuraciones de cada usuario o peer.

En general los servidores SIP escuchan en el puerto 5060 UDP. Por tanto, se configura port=5060. En algunos casos, por ejemplo, si se utiliza SER (Sip Express Router), con Asterisk se debe cambiar este puerto.

DNS es una forma de configurar una dirección lógica para que pueda ser resuelta. Esto permite que las llamadas sean enviadas a diferentes lugares sin necesidad de cambiar la dirección lógica. Usando el DNS SRV se ganan las ventajas del DNS mientras que deshabilitándolo no es posible enrutar llamadas en base a nombre de dominios. Conviene tenerlo activado, por tanto, se pone la directiva srvlookup=yes.

Cada extensión está definida por un usuario, proveedor o amigo y viene definida con un nombre entre corchetes []. El tipo (type) user se usa para autenticar llamadas entrantes peer,para llamadas salientes y friend para ambas. En este caso se ha definido una extensión pedro como friend. Puede realizar y recibir llamadas. Secret es la contraseña usada para la autenticación.

Se puede monitorizar la latencia entre el servidor Asterisk y el teléfono con qualify=yes para determinar cuando el dispositivo puede ser alcanzado En este caso Asterisk considera por defecto que un dispositivo está presente si su latencia es menor de 2000 ms (2 segundos). Se puede cambiar este valor poniendo el número de milisegundos en lugar de yes.

Si una extensión está detrás de un dispositivo que realiza NAT (*Network Address Translation*), como un *router* o *firewall* se puede configurar nat=yes para forzar a *asterisk* a ignorar el campo información de contacto y usar la dirección desde la que vienen los paquetes.

Si se pone host=dynamic quiere decir que el teléfono se podrá conectar desde cualquier dirección IP. Se puede limitar a que dicho usuario solo pueda acceder con una IP o con un nombre de dominio. Si se coloca host=static no haría falta que el usuario se registrará con la contraseña proporcionada en secret. También se ha puesto canreinvite=no. En SIP los invites se utilizan para establecer llamadas y redirigir el audio o video. Cualquier invite después de la inicial en la misma conversación se considera una reinvite.

Cuando dos usuarios han establecido la comunicación con canreinvite= yes (por defecto) los paquetes RTP de audio podrían ser enviados extremo a extremo sin pasar por el servidor asterisk. Esto, normalmente, no suele ser conveniente en casos en los que haya NAT en alguno de los clientes.

Por último, context=internal indica el contexto donde está las instrucciones para dicha extensión. Esto está relacionado con el contexto del archivo extensions.conf que marca el plan de numeración para ese contexto. Por tanto, el contexto internal debe existir en el fichero extensions.conf o de lo contrario se debería crearlo. Varias extensiones pueden tener el mismo contexto.

4.1.7. Configuración del módulo DialPlan

El archivo extensions.conf es el más importante del Asterisk y tiene como misión principal definir el dialplan o plan de numeración que seguirá la centralita para cada contexto y por tanto para cada usuario.

El fichero extensions.conf se compone de secciones o contextos entre corchetes []. Hay dos contextos especiales que están siempre presentes que son [general] y [globals].

El contexto [general] configura unas pocas opciones generales como son:

- Static: indica si se ha de hacer caso a un comando save dialplan desde la consola. Por defecto es yes. Funciona en conjunto con writeprotect.
- Writeprotect: si writeprotect=no y static=yes se permite ejecutar un comando save dialplan desde la consola. El valor por defecto es no.
- Autofallthrough: si está activado y una extensión se queda sin cosas que hacer termina la llamada con BUSY, CONGESTION o HANGUP Si no está activada se queda esperando otra extensión. Nunca debería suceder que una extensión se quede sin cosas que hacer.
- Clearglobalvars: si está activado se liberan las variables globales cuando se recargan las extensiones o se reinicia Asterisk.

En general estas opciones no son muy importantes y se pueden dejar tal y como aparecen por defecto.

En el contexto [globals], se definen las variables globales que se van a poder utilizar en el resto de los contextos.

- Console=Console/dsp; indica que cuando se hace referencia a la variable CONSOLE que se llama /Console/dsp.

Las variables suelen ponerse siempre en mayúsculas para diferenciarlas posteriormente. Para crear un contexto especifico y asignar un plan de

numeración. Todas las líneas de un determinado contexto tienen el mismo formato:

- Exten => extension, prioridad, comando(parámetros).

La extensión hace referencia al número marcado. La prioridad al orden en que se ejecutan las instrucciones. Primero se ejecuta la de prioridad 1, luego la 2 y sucesivamente.

5. DISEÑO FINAL Y PRUEBAS DEL PROTOTIPO

5.1. Descripción del prototipo, unidad de control y unidad de monitoreo

De acuerdo con el planteamiento del problema, se describen las funciones técnicas de la solución, con un dispositivo (computadora de placa reducida) con escalabilidad, compuesto por una unidad de monitoreo y una central de control, que se conectará a una computadora.

5.1.1. Unidad de monitoreo

- Es una interfaz gráfica la cual se desarrollará mediante scripts programados en el ordenador, es el encargado de registrar la cantidad de usuarios que están conectados a la red.

- Adquiere los datos de direccionamiento lógico que se les proporciona a los usuarios, así como llevar un registro de conexión de las llamadas salientes y entrantes que realiza cada usuario.

5.1.2. Unidad de control

- Permite agregar o quitar dispositivos según sea necesario en la organización, colocando un identificador a cada usuario que es agregado al servidor.
- Se conecta a la topología de una red existente de la misma organización, por lo que el montaje del dispositivo es gratuito.

- Mediante una aplicación gratuita, este servicio puede brindarse a cualquier dispositivo que cuente con una tarjeta de red (PC, computadora portátil, tablet, teléfono celular, entre otros).

En este punto, se considerará que se ha configurado de manera correcta el sistema operativo en la computadora de placa reducida (Raspberry pi), recordando que dicho sistema es otra versión de Debian 9, los comandos y la forma de instalación son similares por no decir los mismos.

Se debe tomar en cuenta que de la misma manera que en Debian, al momento de realizar el proceso de instalación se puede escoger el modo gráfico y el modo consola, en este caso se utilizará el segundo modo de operación, debido a que el modo gráfico consume más recursos de la computadora de placa reducida y no será necesario utilizar dichos recursos para lograr una buena comunicación entre los dispositivos intermedios.

5.2. Comprobación y verificación del estado de la estación de comunicación

Se describe a continuación.

Figura 23. **Modo consola**

Fuente: elaboración propia, empleando Debian9 2019.

Si se realizó de manera correcta los procedimientos de instalación de Asterisk al momento de visualizar los directorios dentro de la computadora de placa reducida, se debería ver algo similar, recordando que las versiones pueden variar dependiendo el año que se esté consultando este documento.

Figura 24. **Visualización de directorios**

Fuente: elaboración propia, empleando Debian9 2019.

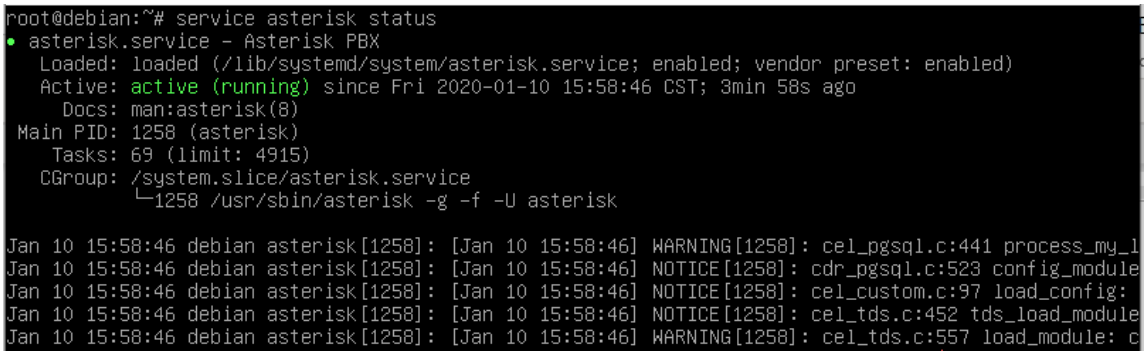
Luego debe de verificar el estado en el que se encuentra Asterisk, de estar apagado, debe de levantar el servicio para no tener problemas de comunicación con los dispositivos de prueba.

Figura 25. **Estado de Asterisk**

Fuente: elaboración propia, empleando Debian9 2019.

Como observa en la figura 25, el servicio de Asterisk se encuentra inactivo por lo que cualquier tipo de comunicación resultaría insatisfactoria, hasta que se active el servicio.

Figura 26. **Activando Asterisk**



Fuente: elaboración propia, empleando Debian9 2019.

Luego de verificar que el servidor se encuentra activo y que la computadora de placa reducida se encuentra conectada de manera correcta a una red, se puede empezar con el proceso de comunicación entre los dispositivos que se encuentran agregados en el directorio correspondiente.

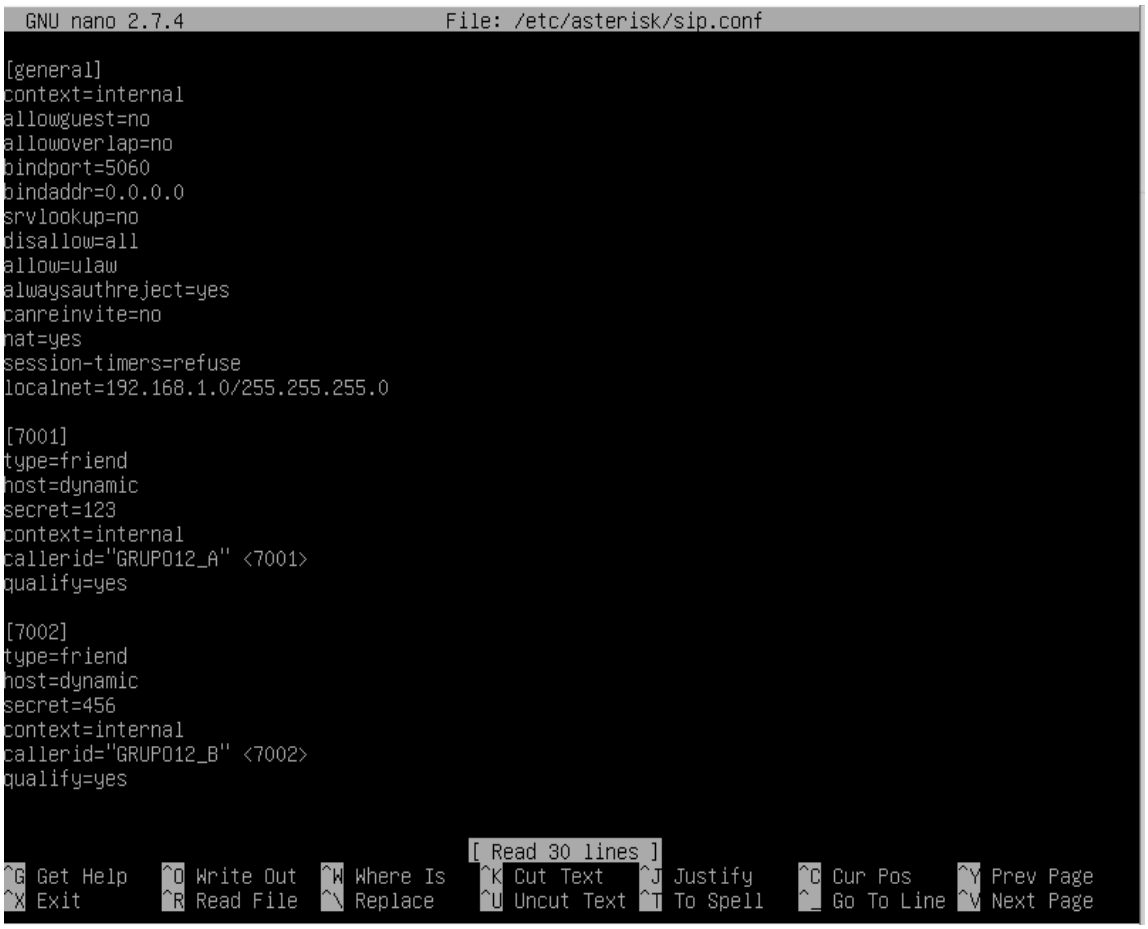
Figura 27. **Dirección IP**

Fuente: elaboración propia, empleando Debian9 2019.

5.3. Configuración de usuarios en la unidad de control

Una vez configurado de manera correcta los resultados anteriores, se debe continuar con la creación de los usuarios, en este caso se crearon dos de momento para realizar las pruebas de comunicación correspondientes.

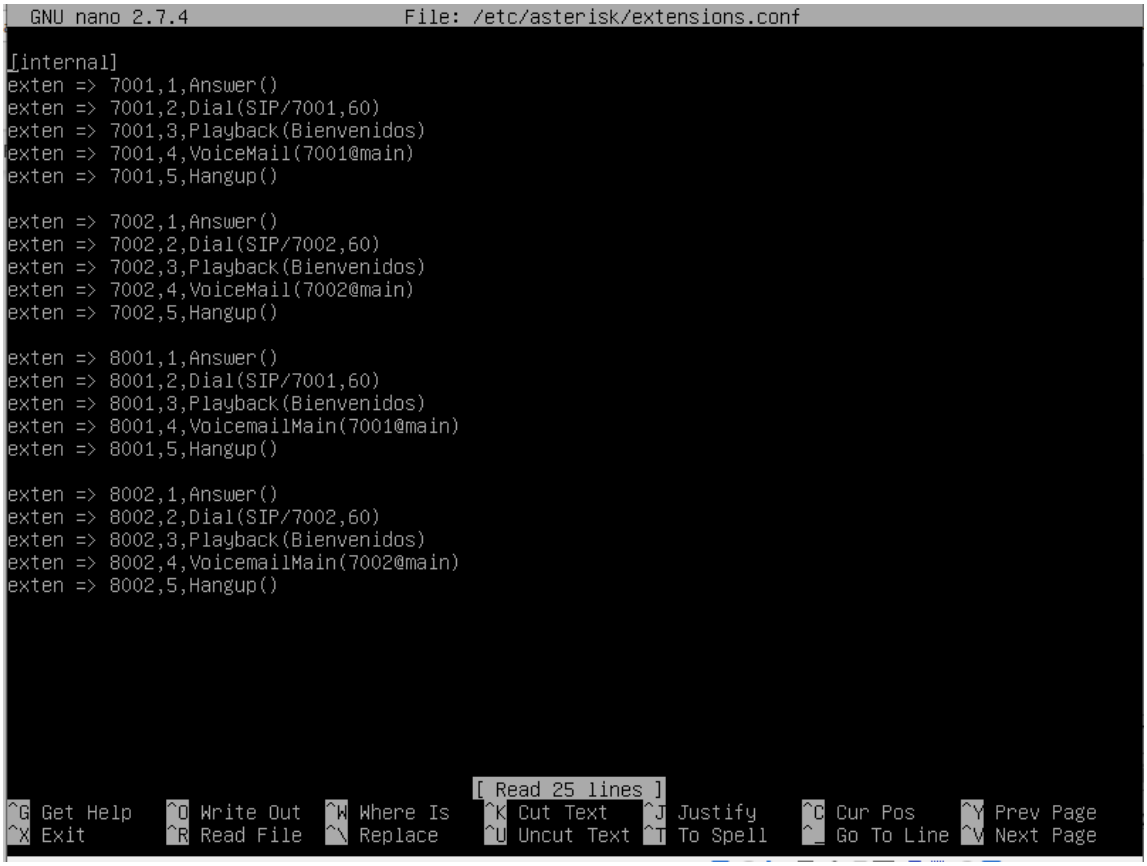
Figura 28. **Creación de usuarios**



Fuente: elaboración propia, empleando Debian9 2019.

En la figura 28 se observa los parámetros de configuración que se mencionaron en capítulos anteriores, aquí se establece la comunicación que se tendrá con la red, así como el puerto por el que estará funcionando el servicio.

Figura 29. **Habilitando servicios de comunicación**



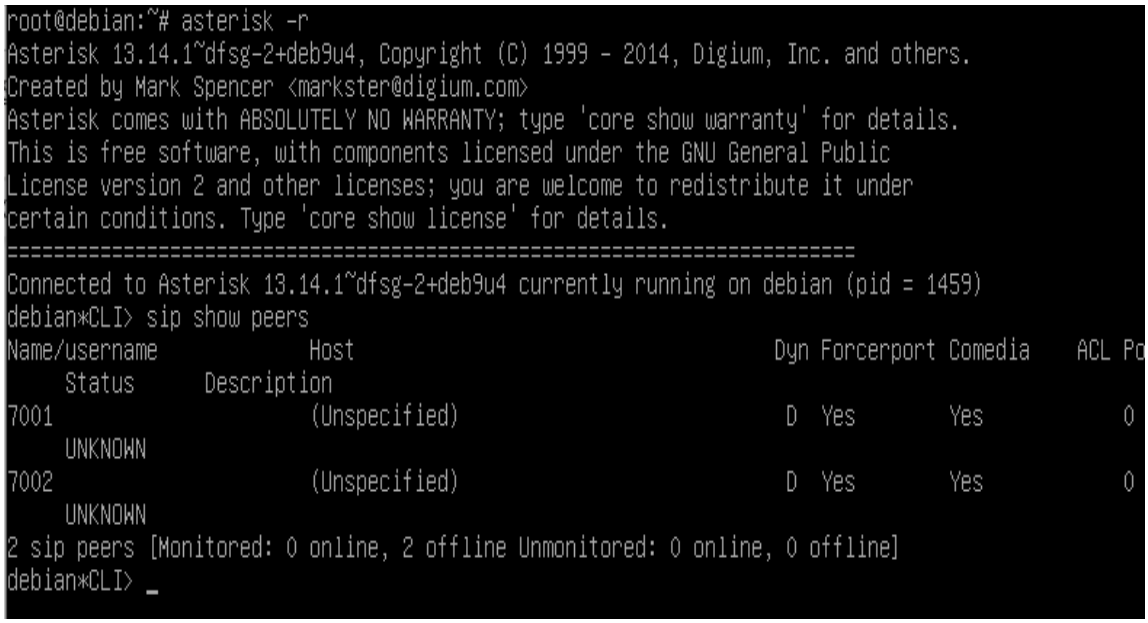
Fuente: elaboración propia, empleando Debian9 2019.

En la figura 29, se observa los servicios que le fueron habilitados a los dos usuarios que se crearon en el archivo anterior. Estos dos pasos son simples, pero si no se realizan de manera adecuada no se podrá llevar a cabo una comunicación exitosa.

5.4. Navegación dentro de la interfaz de monitoreo

En este punto ya se han creado los usuarios de manera correcta, por lo que deberán de aparecer en la interfaz de monitoreo, sin estar activos porque aún no se encuentran conectados a la red del sistema de comunicación.

Figura 30. **Modo de monitoreo**



Fuente: elaboración propia, empleando Debian9 2019.

Se puede observar los dos usuarios que se crearon anteriormente, obviamente estos usuarios se encontraran fuera de línea debido a que ninguno de los dos se encuentra conectados a la red, una vez estén conectados a dicha red, aparecerá en pantalla en el momento que se conecten.

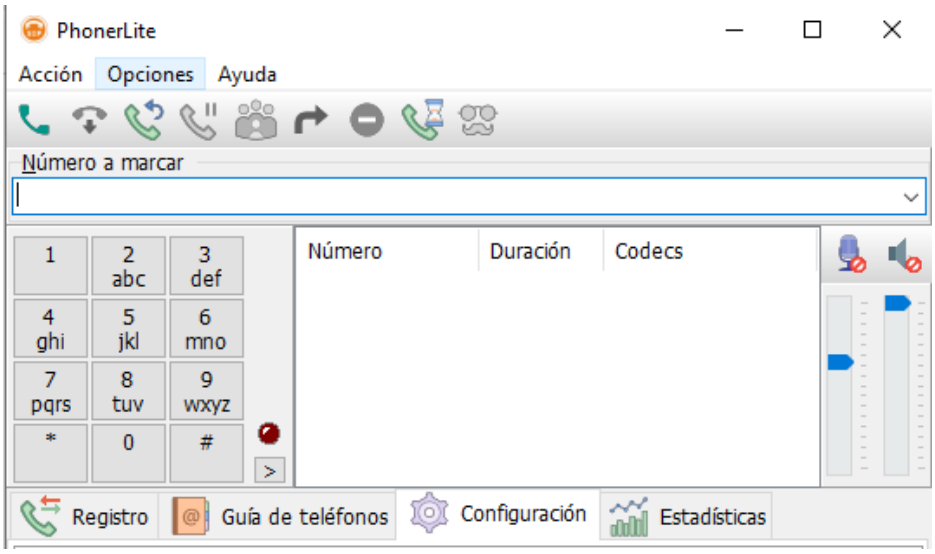
5.5. Configuración de los dispositivos finales para la comunicación mediante la utilización de VoIP

Hasta el momento se configuró el dispositivo intermedio y estará permitiendo la comunicación entre dispositivos finales, pero de igual manera que en el dispositivo intermedio se deben hacer unos ajustes dentro del dispositivo final para que se logre un intercambio de datos exitosos.

Deberá tener en cuenta que existe una diversidad de aplicaciones las cuales permitirán la configuración del servicio de voz IP, algunos son de paga y hay aplicaciones gratuitas, como las que podrá ver a continuación.

- PhonerLite: esta aplicación la puede descargar para dispositivos finales como computadoras de escritorio, Laptops, entre otros.

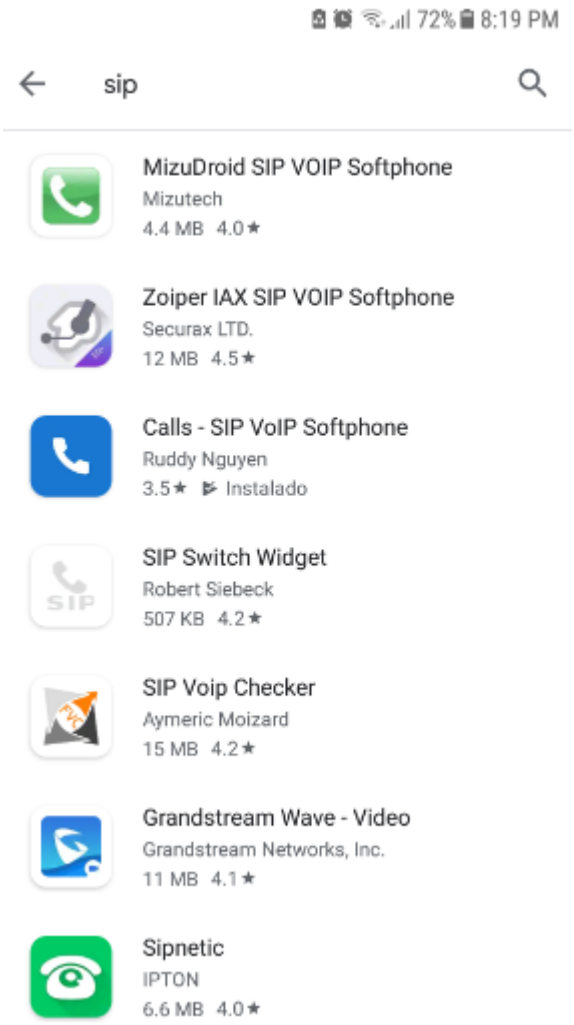
Figura 31. **PhonerLite**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

- Calls SIP VoIP Softphone: esta aplicación la puede descargar para dispositivos finales con sistema Android, celulares, tabletas, entre otros.

Figura 32. **Calls SIP VoIP Softphone**

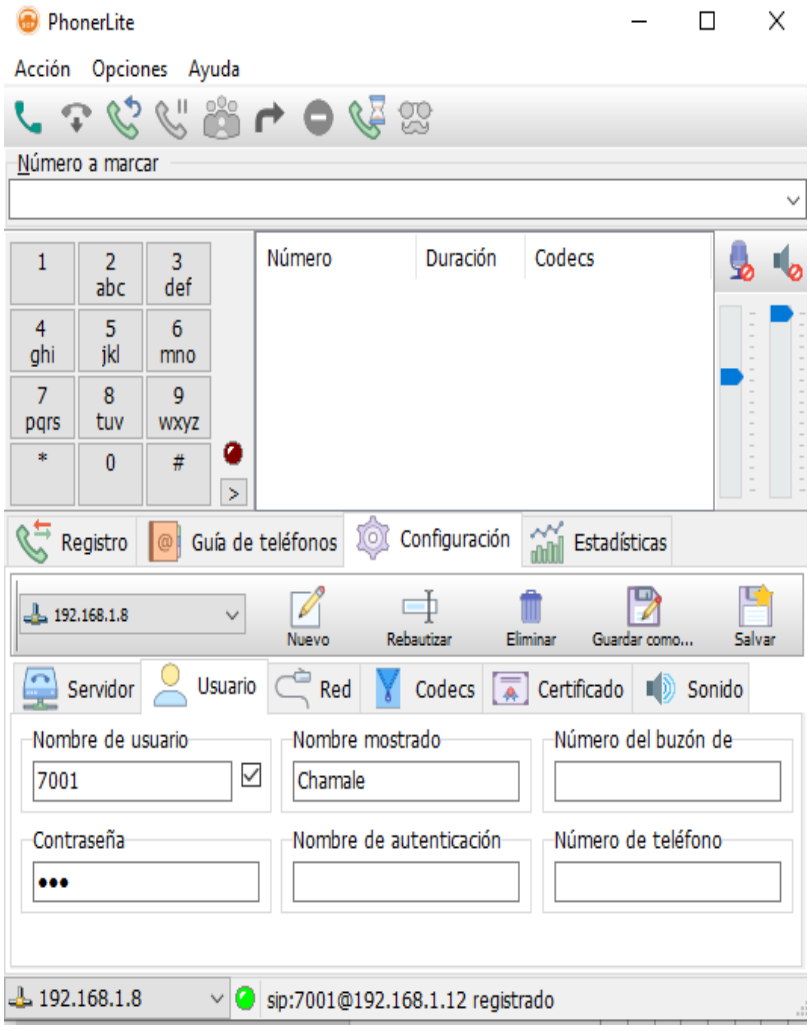


Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Recordando que estas aplicaciones son sugeridas, pero se puede utilizar cualquier aplicación que utilice el servicio de voz por IP, ahora es importante

recordar los usuarios que fueron creados en el dispositivo intermedio (computadora de placa reducida), ya que estos son los únicos usuarios de momento que se le pueden asignar a los dispositivos finales para lograr que se comuniquen entre ellos. A continuación, se muestra la configuración para cada una de las aplicaciones que se usarán para la comunicación.

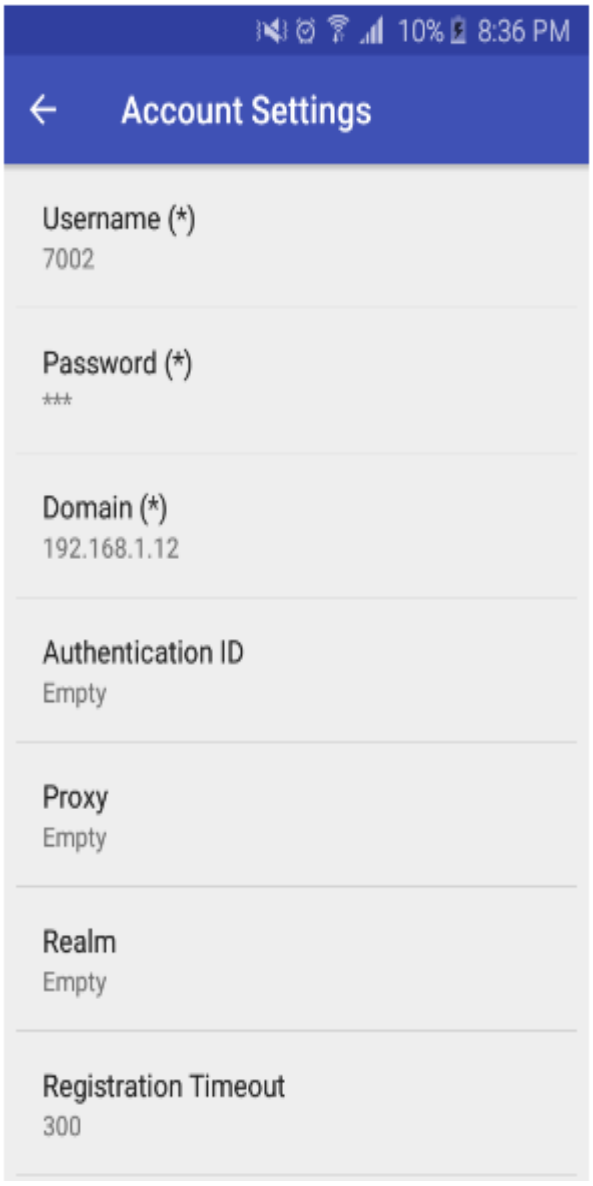
Figura 33. **Asignación de usuario y clave de acceso en PhonerLite**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

De manera similar se hacen las configuraciones para los dispositivos Android, lo único que cambia es la interfaz, pero los parámetros a configurar son los mismos.

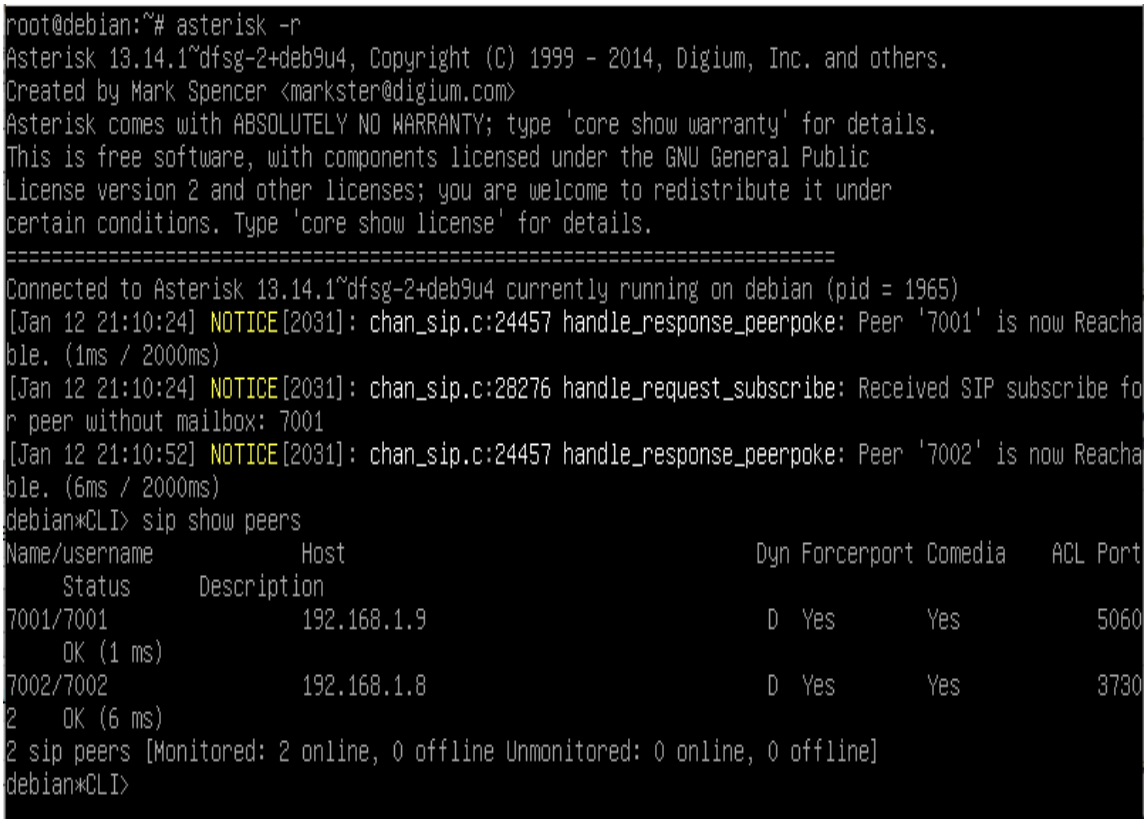
Figura 34. **Asignación de usuario y clave de acceso en Calls**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Luego de configurar de manera correcta los parámetros de los usuarios, en la etapa de monitoreo debería aparecer la conexión de los dos usuarios que se configuraron anteriormente.

Figura 35. **Visualización de dispositivos conectados en la unidad de monitoreo**



Fuente: elaboración propia, empleando Debian9 2019.

Como se puede observar en la figura 35, cuando se configura de manera correcta los parámetros de usuario, aparece una notificación diferente donde se muestra el mes, día y la hora por cada dispositivo final que se conecta en la unidad de monitoreo, además de esto aparece la dirección IPv4 y el puerto que

le fue asignado a cada uno de los dispositivos que se encuentran conectados mediante la computadora de placa reducida.

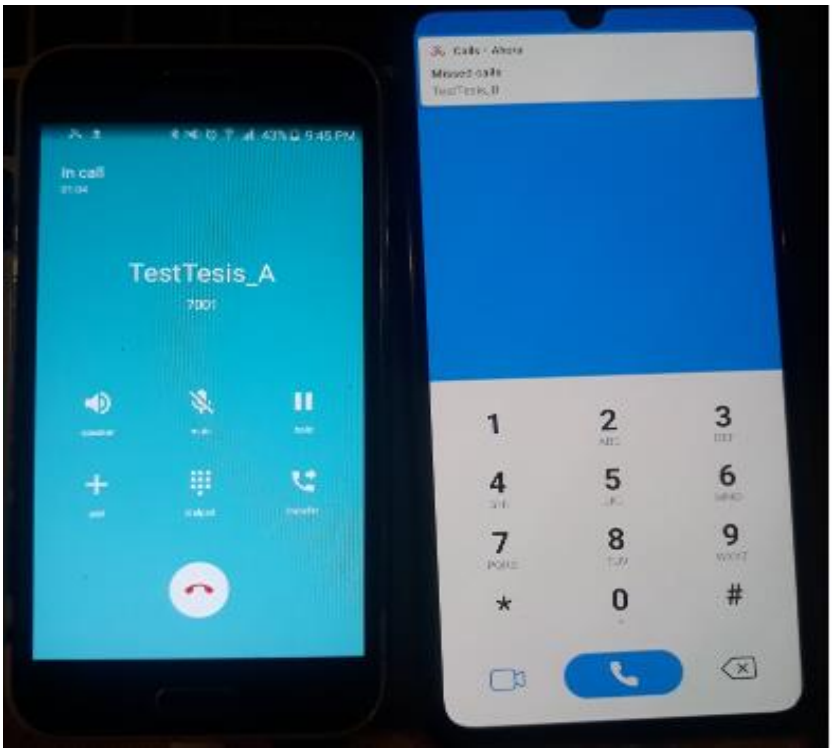
5.6. Comprobación de los servicios de comunicación entre dispositivos finales

A continuación de se describe la comprobación de los servicios de comunicación entre dispositivos.

5.6.1. Prueba de conexión entre dispositivos móviles

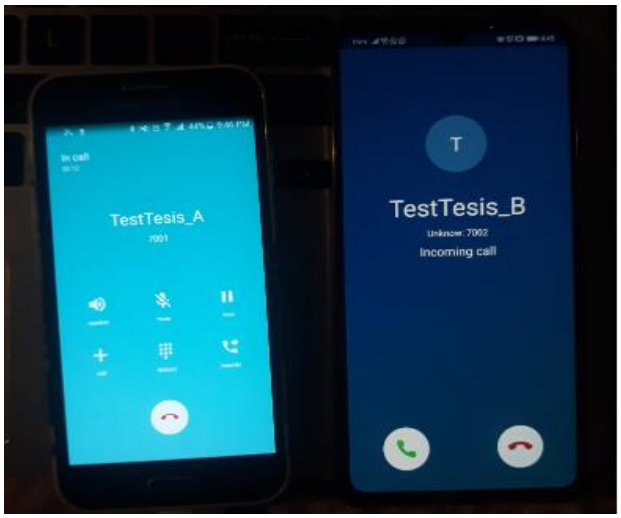
La primera prueba de comunicación se llevó a cabo entre dos dispositivos móviles, los cuales se encuentran conectados de forma inalámbrica a la computadora de placa reducida.

Figura 36. **Llamada perdida entre dispositivo móvil A y dispositivo móvil B**



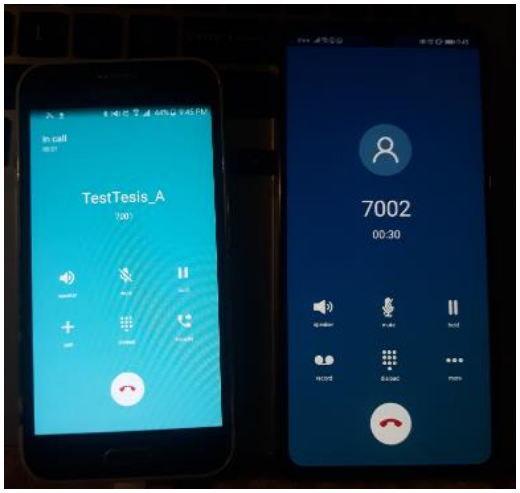
Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Figura 37. **Comunicación entre dispositivo móvil A y móvil B, modo espera**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Figura 38. **Comunicación entre dispositivo móvil A y móvil B, modo llamada**

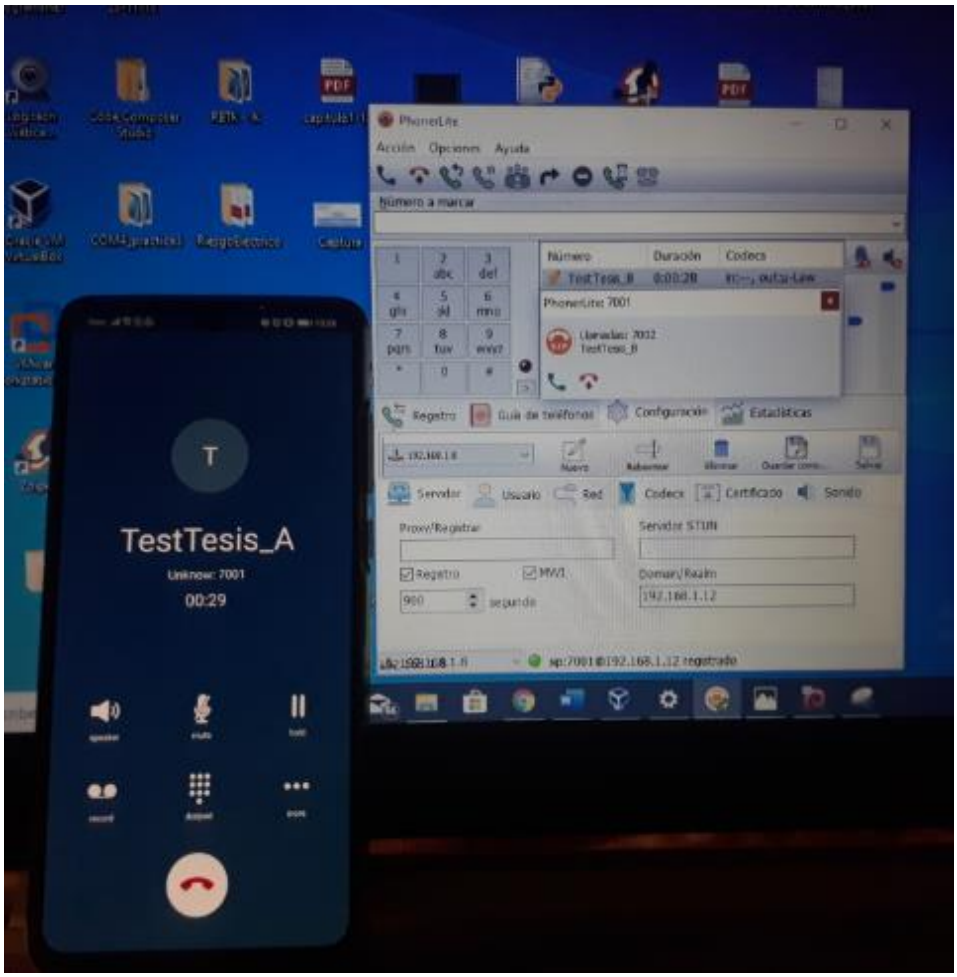


Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

5.6.2. Prueba de conexión entre dispositivo móvil y PC

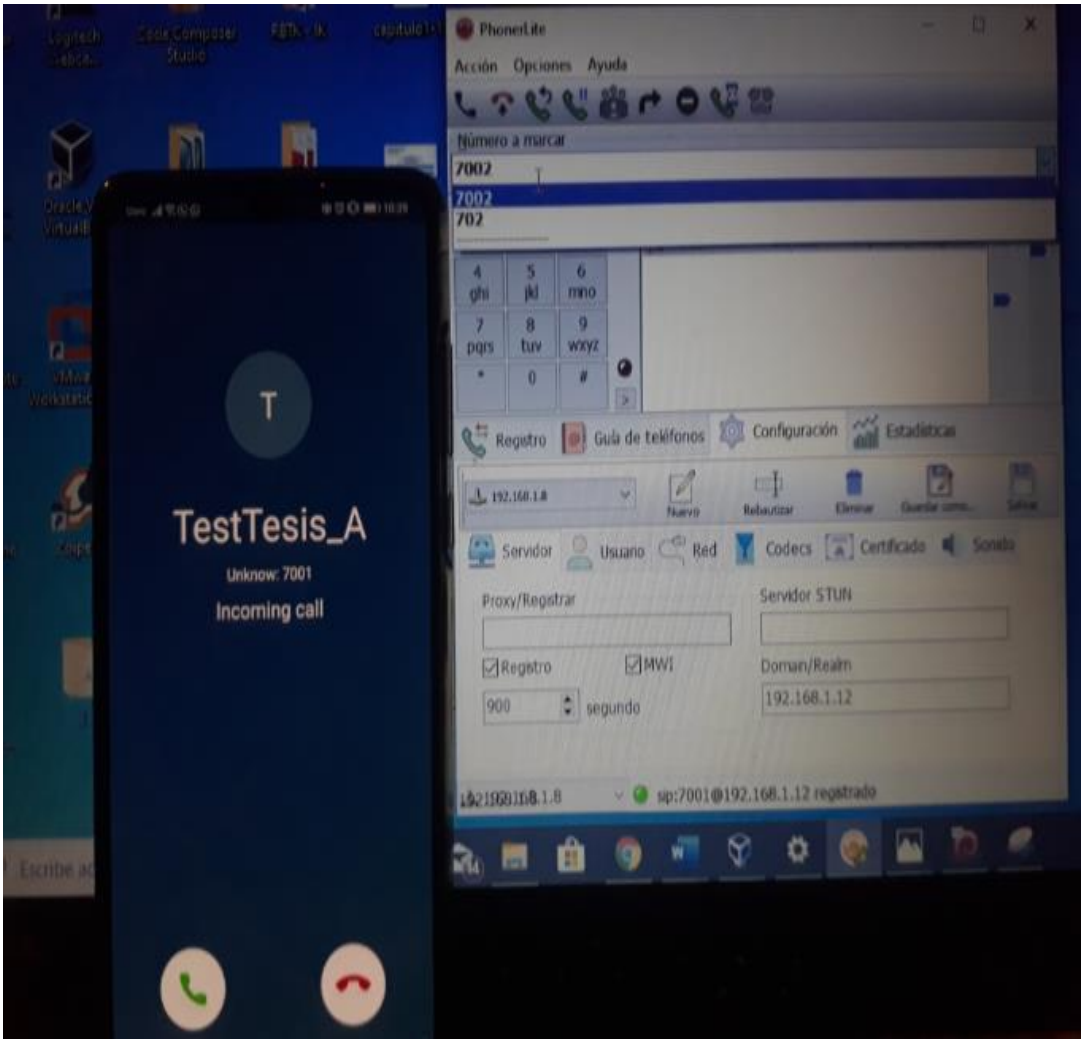
De acuerdo con la información anterior la comunicación se puede llevar a cabo entre cualquier dispositivo que posea una tarjeta de interfaz de red.

Figura 39. **Comunicación entre dispositivo móvil a Laptop, modo llamada**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Figura 40. **Comunicación entre Laptop a dispositivo móvil, modo llamada**



Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

CONCLUSIONES

1. El dispositivo posee escalabilidad, esto quiere decir que, esta estación de comunicación bidireccional puede abarcar toda la distancia que le permita la infraestructura de red, mediante la utilización de dispositivos intermedios, siempre que se respeten los estándares de red.

2. La comunicación es un factor muy relevante dentro de las organizaciones, ya que se requiere de un medio de comunicación estable y funcional para lograr un máximo rendimiento y eficiencia de las actividades que se lleven a cabo dentro de una organización.

3. Los medios y dispositivos utilizados dentro de la infraestructura de red son; fibra óptica, Wi-Fi, cobre, enrutador, interruptor y dispositivos finales.

4. Según el análisis de los parámetros de las diferentes topologías la que tiene un rendimiento óptimo y eficiente es la topología tipo anillo.

5. Las características del dispositivo permiten visualizar en tiempo real, el momento en que cualquier dispositivo se conecta a la red, así como, visualizar las acciones que los mismos realizan una vez estén conectados, logrando una comunicación bidireccional funcional.

RECOMENDACIONES

1. La escalabilidad del dispositivo dependerá del diseño de topología que se utilice, así como de los dispositivos intermedios que se utilicen para expandir el área de cobertura.

2. La versión de software que se utiliza en la computadora de placa reducida puede variar conforme el paso del tiempo, por lo que algunos comandos o archivos pueden cambiar de ubicación de directorio, por lo cual debe verificar la versión que utilice para llevar a cabo sus pruebas de comunicación.

3. La *Raspberry* pi no es la única computadora de placa reducida por lo que existen otros dispositivos en el cual se puede implementar esta estación de trabajo, pero deberá verificar que esos otros dispositivos sean compatibles con sistemas operativos Linux.

4. Para renombrar a los dispositivos que fueron asignados dentro de la unidad de control es importante que reinicie la computadora de placa reducida para que los cambios se llevan a cabo de manera satisfactoria.

BIBLIOGRAFÍA

1. Asterisk. *Channel Drivers.* [en línea]. <https://wiki.asterisk.org/wiki/display/AST/SIP/>. [Consulta: 7 de enero de 2020]

2. _____. *Documentation y configuracion de servidor VoIP.* [en línea]. <https://wiki.asterisk.org/wiki/display/AST/Configuration/> [Consulta: 6 de enero de 2020]

3. Boletín de bluesource sobre comunicación empresarial. *20 estadísticas sorprendentes sobre comunicaciones comerciales*. [en línea]. <https://www.bluesource.co.uk/knowledge-hub/20-astonishing-stats-business-communications/>. [Consulta: 15 de julio de 2019].

4. Cisco. *Direccionamiento lógico* [en línea]. <https://sites.google.com/site/redesinformaticasjh/direccionamiento-logico/>. [Consulta: 2 de octubre de 2019]

5. Cisco Certified Network Associate. *CCNA, Study Guide; Todd Lammle*. 6ª +ed. U.S.A: Willey Publishing, 2007. 67 p.

6. Cisco Networking Academy. *CCNA: Switching, Routing, Wireless Essentials.* [en línea]. <https://contenthub.netacad.com/srwe/3.1.1/>. [Consulta: 5 de septiembre de 2019].

7. _____. *Introducción a las redes.* [en línea]. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#0/>. [Consulta: 24 de julio de 2019].

8. _____. Python Institute: Open Education & Development Group. *Programming essentials in python part1.* [en línea]. <https://edube.org/learn/programming-essentials-in-python-part-1-spanish/comienza-tu-viaje-en-python>. [Consulta: 20 de septiembre de 2019].

9. CORRES, Jesús M. *El mundo de los microcontroladores, Capítulo 1*. [en línea]. <http://www.mikroe.com/chapters/view/79/capitulo-1-el-mundo-de- los-microcontroladores/>. [Consulta: 17 de julio de 2019].

10. _____. El mundo de los microcontroladores, Capítulo 2. *Programación de los microcontroladores.* [en línea]. <http://www.mikroe.com/chapters/view/80/capitulo-2-programacion-de-los-microcontroladores/>. [Consulta: 18 de julio de 2019].

11. Ingenieria Systems. *Comparacion entre modelo OSI y modelo de capa TCP/IP, comunicación de mensajes.* [en línea]. <http://www.ingenieriasystems.com/2016/10/Comparacion-entre-el-modelo-OSI-y-el-modelo-TCPIP-Comunicacion-de-mensajes-CCNA1-V5-CISCO-C3.html/>. [Consulta: 12 de diciembre de 2019].

12. Interpolados. *Direcciones IP.* [en línea]. <https://interpolados.wordpress.com/2017/05/16/espacio-de-direcciones-ipv4-privadas/>. [Consulta: 5 de octubre de 2019].

13. _____. *Representaciones de red.* [en línea]. <https://interpolados.wordpress.com/2017/02/28/representaciones-de-red/>. [Consulta: 20 de septiembre de 2019].

14. Linksys. *Resource center.* [en línea]. <https://www.linksys.com/es/r/resource-center/wifi-router/>. [Consulta: 17 de noviembre de 2019].

15. Lucidchart. *Diagrama de red.* [en línea]. <https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-red#:~:targetText=La%20topolog%C3%ADa%20de%20red%20se,como%20%22topolog%C3%ADa%20de%20se%C3%B1al%22/>. [Consulta: 9 de diciembre de 2019].

16. Profesionalreview. *Modelo OSI.* [en línea]. <https://www.profesionalreview.com/2018/11/22/modelo-osi/>. [Consulta: 12 de diciembre de 2019].

17. Raspberry. *Documentation* y configuración. [en línea]. <https://www.raspberrypi.org/documentation/configuration/config-txt/README.md/>. [Consulta: 10 de enero de 2020].

18. SEDRA, Adel; SMITH, Kenneth. *Circuitos microelectrónicos.* 4a ed. México: Oxford University Press, 1999. 1158 p.

19. SoftZone. *Linux.* [en línea]. <https://www.softzone.es/programas/linux/>. [Consulta: 10 de enero de 2020].

20. Stack overflow. *Directorios debian.* [en línea]. <https://es.stackoverflow.com/questions/52341/en-linux-se-pueden-mostrar-los-directorios-en-forma-de-%C3%A1rbol/>. [Consulta: 5 de enero de 2020].

21. Zadarma. *Configuracion de Phoner Lite.* [en línea]. <https://zadarma.com/es/support/instructions/windows/phonerlite/>. [Consulta: 12 de enero de 2020].

APÉNDICES

Apéndice 1. **Contexto de directorios**

```
[directories](!)
astetcdir => /etc/asterisk
astmoddir => /usr/lib/asterisk/modules
astvarlibdir => /var/lib/asterisk
astdbdir => /var/lib/asterisk
astkeydir => /var/lib/asterisk
astdatadir => /var/lib/asterisk
astagidir => /var/lib/asterisk/agi-bin
astspooldir => /var/spool/asterisk
astrundir => /var/run/asterisk
astlogdir => /var/log/asterisk
astsbindir => /usr/sbin
```

Fuente: elaboración propia, empleando Adobe Photoshop CS5 2010.

Apéndice 2. **Programación módulo de CLI**

```
[modules]
;autoload = yes
;preload = res_odbc.so
;preload = res_config_odbc.so
;preload-require = res_odbc.so
;require = res_pjsip.so
;noload = pbx_gtkconsole.so
;load = res_musiconhold.so
```

Fuente: elaboración propia.

Apéndice 3. **Programación modulo SIP**

```
[general]
context=default
port=5060 ; Puerto UDP en el que responderá el Asterisk
bindaddr=0.0.0.0 ; Si se quiere especificar que Asterisk esté en una IP (si un equipo tiene 3 IPs por ej.) 0.0.0.0 vale para cualquiera
srvlookup=yes ; Habilita servidor DNS SRV

[pedro]
type=friend
secret=welcome
qualify=yes ;Tiempo de latencia no superior a 2000 ms.
nat=no ; El teléfono no usa NAT
host=dynamic ; El dispositivo se registra con una IP variante
canreinvite=no ; Asterisk por defecto trata de redirigir
context=internal ; El contexto que controla todo esto
```

Fuente: elaboración propia.

Apéndice 4. **Programación módulo Exten**

Ejemplo 1: Colgar la línea

```
exten => 333,1,Hangup ; indica que cuando alguien llame al 333 saltará la prioridad 1 y el sistema colgará la llamada
```

Ejemplo 2 : Llamar a el usuario SIP 3000 y que salte el contestador si no contesta

exten => 3000,1,Dial(SIP/3000,30,Ttm) ; intenta llamar al usuario 3000 de sip que tiene que estar definido en sip.conf con ese contexto
exten => 3000,2,Hangup ; cuando acaba la llamada cuelga
exten => 3000,102,Voicemail(3000) ; La prioridad 102 significa que el usuario no estaba conectado y salta el contestador al buzon 3000
exten => 3000,103,Hangup ; se cuelga después de dejar el mensaje

Fuente: elaboración propia.

Apéndice 5. **Guía de instalación de Asterisk**

root:

```
apt-get update
apt-get upgrade

apt-get install asterisk

asterisk -r
exit

mv /etc/asterisk/sip.conf /etc/asterisk/sip.conf.orig
nano /etc/asterisk/sip.conf

[general]
context=internal
allowguest=no
allowoverlap=no
bindport=5060
bindaddr=0.0.0.0
srvlookup=no
disallow=all
allow=ulaw
alwaysauthreject=yes
canreinvite=no
nat=yes
session-timers=refuse
localnet=192.168.1.0/255.255.255.0
```

Continuación apéndice 5.

```
[7001]
type=friend
host=dynamic
secret=123
context=internal

[7002]
type=friend
host=dynamic
secret=456

mv /etc/asterisk/extensions.conf /etc/asterisk/extensions.conf.orig
nano /etc/asterisk/extensions.conf

[internal]
exten => 7001,1,Answer()
exten => 7001,2,Dial(SIP/7001,60)
exten => 7001,3,Playback(vm-nobodyavail)
exten => 7001,4,VoiceMail(7001@main)
exten => 7001,5,Hangup()

exten => 7002,1,Answer()
exten => 7002,2,Dial(SIP/7002,60)
exten => 7002,3,Playback(vm-nobodyavail)
exten => 7002,4,VoiceMail(7002@main)
exten => 7002,5,Hangup()
```

Continuación apéndice 5.

```
exten => 8001,1,VoicemailMain(7001@main)
exten => 8001,2,Hangup()
exten => 8002,1,VoicemailMain(7002@main)
exten => 8002,2,Hangup()

mv /etc/asterisk/voicemail.conf /etc/asterisk/voicemail.conf.orig
nano /etc/asterisk/voicemail.conf
```

Fuente: elaboración propia.