Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

APLICACIÓN MÓVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO *CONFIREDES*

Ferri Omar Vásquez Escobar
Asesorado por el Ing. William Estuardo Escobar Argueta

Guatemala, junio de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

APLICACIÓN MÓVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO *CONFIREDES*

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

FERRI OMAR VÁSQUEZ ESCOBAR
ASESORADO POR EL ING. WILLIAM ESTUARDO ESCOBAR ARGUETA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JUNIO DE 2021

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 Martinez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Vladimir Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing. Oscar Alejandro Paz Campos
EXAMINADOR	Ing. Luis Fernando Espino Barrios
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

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:

APLICACIÓN MÓVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO *CONFIREDES*

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha noviembre de 2020.

Ferri Omar Vásquez Escobar

Guatemala, 4 de marzo de 2021

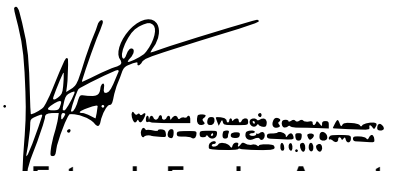
Ingeniero
Carlos Alfredo Azurdia
Coordinador de Privados y Trabajos de Tesis
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería - USAC

Respetable Ingeniero Azurdia:

Por este medio hago de su conocimiento que en mi rol de asesor del trabajo de investigación realizado por el estudiante **FERRI OMAR VÁSQUEZ ESCOBAR** con carné **201020256 y CUI 2163 52525 0115** titulado **"APLICACIÓN MOVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO CONFIREDES",** lo he revisado y luego de corroborar que el mismo se encuentra concluido y que cumple con los objetivos propuestos en el respectivo protocolo, procedo a la aprobación respectiva.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,



Ing. William Estuardo Escobar Argueta
Colegiado No. 11529

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 17 de marzo de 2021

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **FERRI OMAR VÁSQUEZ ESCOBAR** con carné **201020256** y CUI **2163 52525 0115** titulado **"APLICACIÓN MOVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO CONFIREDES"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"APLICACIÓN MÓVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO CONFIREDES",*** *realizado por el estudiante, FERRI OMAR VÁSQUEZ ESCOBAR aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Msc. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 5 de febrero de 2021

Decanato
Facultad de Ingeniería
24189101 - 24189102

DTG.243.2021

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 en Ciencias y Sistemas, al Trabajo de Graduación titulado: **APLICACIÓN MÓVIL DE APOYO PARA LA CONFIGURACIÓN DE PROTOCOLOS DE RED EN DISPOSITIVOS CISCO CONFIREDES,** presentado por el estudiante universitario: **Ferri Omar Vásquez Escobar,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, junio de 2021

AACE/asga

ACTO QUE DEDICO A:

Dios	Por brindarme sabiduría, bendiciones y perseverancia para alcanzar esta meta.
Mis padres	Rodolfo Vásquez y Rosa Escobar de Vásquez; por brindarme apoyo incondicional y la oportunidad de seguir superándome personal y académicamente, instándome a seguir adelante y nunca rendirme.
Mis hermanos	Belfri, Rosver y Damaris Vásquez; por estar a mi lado, brindándome su apoyo incondicional y ser un modelo para mí.
Mi sobrino	Joseph Hernández; por su sola existencia llena nuestras vidas de felicidad y me motiva a ser un buen ejemplo para él.
Mi familia	En especial a mi tía Vilma Jacinto de Hernández y su esposo Jairo Hernández; por su cariño y apoyo durante estos años, y a mi cuñado Hans Hernández, por los momentos y experiencias compartidas.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser mi casa de estudios durante estos años de mi vida universitaria.
Facultad de Ingeniería	En especial a la escuela de Ciencias y Sistemas, por prepararme para ser un profesional capacitado y ético.
Mis compañeros de la Facultad	Por el conocimiento compartido y experiencias vividas.
Mi asesor	Ing. William Escobar; por su amistad, asesoramiento y tiempo brindado en este proceso.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
%	Porcentaje

GLOSARIO

Broadcast

CCNA *Cisco Certified Network Associate*; es una certificación de Cisco.

Cisco Compañía estadounidense dedicada a la fabricación de dispositivos para redes locales y externas.

Gateway Es una puerta de enlace que funciona como interfaz de conexión entre dispositivos.

MAC Identificador único asignado a la tarjeta de red de cada dispositivo por parte del fabricante.

Pc Computadora personal (*personal computer*).

Pdf Formato de almacenamiento para documentos digitales (*Portable document format*).

Smartphone Dispositivo móvil el posee las funciones de un celular y un ordenador de bolsillo.

SO Sistema operativo.

Subnetting	Es el proceso de subdividir una red en varias subredes.
Tablet	Dispositivo móvil de mayores dimensiones que un *smartphone*.
USAC	Universidad de San Carlos de Guatemala.
YouTube	Sitio web utilizado para compartir videos.

RESUMEN

En el siguiente documento se presenta el análisis y desarrollo de una aplicación para dispositivos móviles, con nombre *ConfiRedes*, la cual presenta como propósito servir de apoyo para la configuración de dispositivos de red Cisco. Esta aplicación surge debido a que no existe una aplicación en la *Google Play Store* que los alumnos de Redes de computadoras 1 y Redes de computadoras 2 de la Facultad de Ingeniera, Universidad de San Carlos de Guatemala USAC, puedan utilizar como apoyo para realizar prácticas y proyectos. Las aplicaciones existentes en la *Google Play Store* se enfocan en ser herramientas de *subnetting* o de contenido didáctico, lo cual obliga a los estudiantes a hacer uso de aplicaciones con demasiado contenido (en muchos casos irrelevante) y a tener instaladas dos o más de estas.

Por tales motivos, se plantea como solución el desarrollo de una aplicación para dispositivos móviles desarrollada para dispositivos Android, por medio de la cual los usuarios cuenten con una herramienta que combine el cálculo de *subnetting* y contenido didáctico/multimedia sobre dispositivos (*switch*, *switch multilayer*, *router* y *firewall*) y protocolos (en función del dispositivo seleccionado) abarcados en los cursos Redes de computadoras 1 y Redes de computadoras 2. El apartado de *subnetting* brinda al usuario, paso a paso, una explicación de cómo se obtiene el resultado. El apartado de contenido presenta al usuario, de forma concisa, el funcionamiento y comando de configuración de los dispositivos y protocolos; esto es acompañado de contenido multimedia (mediante el simulador Packet Tracer) que muestra al usuario el correcto funcionamiento de los comandos.

OBJETIVOS

General

Desarrollar una aplicación móvil la cual sirva de apoyo para la configuración de protocolos en dispositivos Cisco, para estudiantes de los cursos Redes de computadoras 1 y Redes de computadoras 2.

Específicos

1. Crear una aplicación con interfaz intuitiva y amigable para el usuario, la cual sea empleada como herramienta educativa por los alumnos de los cursos Redes de computadoras 1 y Redes de computadoras 2, de la Universidad de San Carlos de Guatemala.

2. Facilitar la consulta de los diversos protocolos configurables en dispositivos Cisco.

3. Mostrar la forma correcta de realizar la subdivisión de una red en subredes (*subnetting*).

4. Mostrar el impacto de las aplicaciones móviles en la educación, como herramientas didácticas.

Hipótesis

La aplicación móvil *ConfiRedes* demostrará la necesidad de implementar aplicaciones móviles en el sector educativo que sirvan como herramientas de estudio y apoyo en configuraciones de dispositivos de redes, y, que esto no se limita únicamente a estudiantes de Redes de computadoras 1 y Redes de computadoras 2, de la Facultad de Ingeniería de la Universidad de San Carlos, sino que puede ser utilizado por profesionales, estudiantes de acreditaciones y todas aquellas personas que necesiten configurar un dispositivo de red Cisco, y alcanzar de esta manera un mercado mucho más extenso y amplio, como otras universidades o empresas privadas.

Hipótesis nula

Al usuario no le parece amigable ni intuitiva la interfaz de la aplicación móvil, por lo que no percibe un impacto positivo, comparado con las otras herramientas existentes.

Hipótesis alternativa

El usuario manifiesta su aceptación por la aplicación móvil, la cual le parece una herramienta útil para la configuración de dispositivos de red Cisco y observa el potencial que esta puede tener para el ámbito laboral.

INTRODUCCIÓN

Con los avances tecnológicos, las redes de computadoras han tomado mayor importancia; estas se pueden encontrar en hogares, universidades, empresas y en la mayoría de los servicios que se adquieren (que necesitan una conexión a internet). Por ello, en los cursos como Redes de computadoras 1 y Redes de computadoras 2, se enfatiza en el análisis y la configuración de las redes, a partir de conceptos básicos, modelos de referencia y dispositivos configurables que interactúan en la composición de la topología de red.

Para el análisis, diseño e implementación de las topologías de redes de computadoras, es necesario tener de forma concisa los conceptos tanto de los modelos por implementar, como de los protocolos necesarios. Además del concepto, es necesario tener a disposición los comandos para la configuración de los diversos dispositivos que interactúan en la red.

Por ello, se desarrolló una aplicación para dispositivos móviles con sistema operativo Android, aprovechando que este sistema operativo posee mayor popularidad en el mercado guatemalteco. Dicha aplicación tiene como objetivo proveer de herramientas para la configuración de dispositivos de red Cisco y su utilización no depende de una conexión a internet para el despliegue de la información. En ella, el estudiante podrá encontrar información relevante y los protocolos configurables para los dispositivos Cisco: *switch*, *router*, *switch multicapa* y *firewall*. Lo anterior, con la intención de ser una herramienta educativa de apoyo para que los estudiantes puedan realizar sus tareas, prácticas y proyectos.

1. REDES DE COMPUTADORAS

Las redes se componen, básicamente, de dispositivos configurables que interactúan entre sí; por ello, para su correcto funcionamiento es necesaria la correcta implementación de los protocolos en dichos dispositivos. En este primer capítulo se analiza el modelo de referencia OSI y el modelo TCP/IP, así como los protocolos configurables para dispositivos Cisco que se incluyen en el programa de los cursos Redes de computadoras 1 y Redes de computadoras 2, para los estudiantes de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala. Esto, con el objetivo de entender su funcionamiento y dar a conocer los comandos con los cuales son configurados dichos protocolos. Para los comandos de configuración se toman como referencia los planteados en el libro de Todd Lammle, *CCNA: Cisco Certified Network Associate Study Guide, Sixth Edition.*

A continuación, se presentan los modelos de referencia OSI y TCP/IP, dispositivos y protocolos configurables: VLAN, VTP, STP, puerto en modo *trunk*, puerto en modo *access*, InterVLAN, enrutamiento estático, enrutamientos dinámicos, ACL, NAT, GLBP, HSRP, VRPP, políticas de seguridad en un *firewall* y SSH.

1.1. Modelo de referencia OSI

El modelo OSI (modelo abierto de *internetwork*) divide una red en diferentes capas con el objetivo de que cada desarrollador trabaje en su área sin dependencias de otras. No es considerado una arquitectura debido a que este modelo no especifica un protocolo que se debe de seguir en cada capa; su

objetivo es definir las funcionalidades que cada capa debe brindar para generar un estándar.

Figura 1. **Diagrama modelo OSI**

Nº de capa	OSI
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Fuente: Di Tommaso, Leandro. *Modelos OSI y TCP/IP*. https://www.mikroways.net/2009/08/08/modelos-osi-y-tcpip/. Consulta: diciembre de 2020.

1.1.1. Capas del modelo OSI

El modelo OSI se compone de siete capas que se comunican con sus homólogos (protocolos ubicados en el otro extremo de la comunicación). Cada capa trabaja de forma independiente a las otras, lo cual genera la ventaja de que cada una puede ser modificable sin que afecte a las demás. Sin embargo, cada capa presta un servicio a la inmediata superior, por lo que la de aplicación es la única que no lo realiza debido a ser la última y su función está directamente asociada con el usuario.

1.1.1.1. Capa física

En esta capa se establecen los requisitos necesarios para la transmisión de los datos. En esta se gestionan los procedimientos a nivel físico y eléctrico para garantizar la comunicación de los paquetes desde el transmisor hasta el receptor, sin ninguna alteración. Para cumplir su objetivo, define los medios físicos por los que viaja la comunicación: tipo de cable, ondas o fibra óptica y características de los materiales: conectores, niveles de tensión, señales eléctricas, entre otros.

1.1.1.2. Capa de enlace de datos

Esta capa proporciona la comunicación entre *hosts* establecidos en la capa física. Es la encargada de transferir de manera confiable la información a través de la red. Se compone de dos subcapas: LLC (*Logical Link Control*), la cual es la encargada de identificar lógicamente los tipos de protocolos y encapsulamiento posterior de estos y la subcapa MAC (*Media Access Control*), que se encarga del acceso al medio, los direccionamientos físicos, las notificaciones de error, el control óptimo del flujo y la distribución ordenada de las tramas.

1.1.1.3. Capa de red

Esta capa se encarga del transporte del tráfico de datos entre *hosts* que no se ubiquen localmente en el mismo dominio de difusión (entre diferentes redes). Su función es permitir que las tramas puedan llegar desde el transmisor al receptor, al realizar las conmutaciones y enrutamientos pertinentes. Para cumplir con su objetivo, es necesario que esta capa conozca la topología de red en la cual está funcionando.

1.1.1.4. Capa de transporte

Se encarga de la correcta comunicación entre *hosts*; para esto, se asegura de que los segmentos distribuidos sean confirmados al remitente y coloca los segmentos en el orden correcto en el receptor. Adicionalmente, proporciona un control de flujo que regula el tráfico de datos.

Puede retransmitir los datos de forma segura o no. Mediante el protocolo TCP (*Transmision Control Protocol*) realiza la transmisión de forma segura, mediante un “saludo de tres pasos”, mientras que si se utiliza el protocolo UDP (*User Datagram Protocol*) realiza la transmisión de forma insegura, mediante un “saludo de dos pasos”.

1.1.1.5. Capa de sesión

Esta capa se encarga de la administración y conclusión de las sesiones de comunicación entabladas entre dispositivos de la capa de presentación. Establece los mecanismos de gestión y control que regulan el establecimiento de la conexión, el mantenimiento de esta y su finalización.

1.1.1.6. Capa de presentación

Esta capa se encarga de garantizar que la información enviada por la capa de aplicación pueda ser leída por la de aplicación de otro, aunque los dispositivos cuenten con diferentes representaciones internas de caracteres; por lo cual, de ser necesario, traduce de varios formatos de datos a un formato común.

1.1.1.7. Capa de aplicación

Esta capa ofrece a las aplicaciones la forma de acceder a los servicios ubicados en las otras; además, define los protocolos que utilizarán las aplicaciones en el intercambio de información.

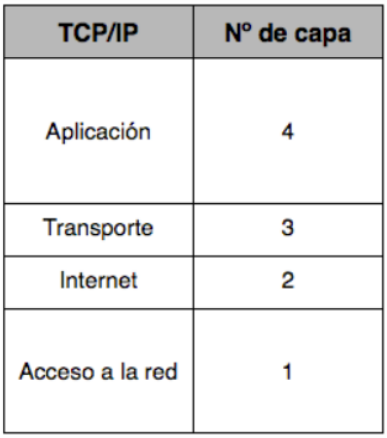
1.2. Modelo TCP/IP

Debido a la necesidad de tener una red que pudiera sobrevivir ante las diversas circunstancias, fue creado el modelo TCP/IP por parte del Departamento de Defensa de Estados Unidos (DoD). Este modelo surge como solución una para transmitir datos de forma fiable sin importar el estado de un nodo o una red en particular; por lo tanto, el modelo TCP/IP apoya en el diseño de redes para adaptarse a cualquier circunstancia. Se ha convertido en el estándar en el cual se basa el internet. Sus siglas (TCP/IP) hacen referencia a dos protocolos:

- TCP: *Transmision Control Protocol*, es un protocolo el cual permite establecer de forma segura conexiones e intercambio de datos entre dos o más *hosts*. El protocolo TCP se encarga de validar que los paquetes enviados sean entregados mediante al acuse de recibido (mensaje que es enviado por parte de la aplicación destino a la aplicación origen confirmando la recepción de los paquetes).

- IP: *Internet Protocol*, es un protocolo de comunicación el cual se encarga de determinar la ruta que deben utilizar los paquetes, con base en la dirección IP del sistema receptor. El protocolo IP se encarga de permitir un intercambio de datos fiable dentro de la topología de red, ya que define los pasos desde que se envían los paquetes hasta que son recibidos.

Figura 2. **Diagrama modelo TCP/IP**



TCP/IP	Nº de capa
Aplicación	4
Transporte	3
Internet	2
Acceso a la red	1

Fuente: DI TOMMASO, Leandro. *Modelos OSI y TCP/IP*. https://www.mikroways.net/2009/08/08/modelos-osi-y-tcpip/. Consulta: diciembre de 2020.

1.2.1. Capas del modelo TCP/IP

El modelo TCP/IP se conforma de cuatro capas; a pesar de que algunas capas del modelo TCP/IP comparten nombre con las del modelo OSI, es importante resaltar que no se deben confundir las funciones de cada, ya que se desempeñan de diferente forma en cada modelo.

1.2.1.1. Capa de acceso a la red

En esta capa se define el acceso físico de los dispositivos que se encuentran conectados a la red y, a su vez, de los protocolos que permiten la comunicación. Adicionalmente, en esta capa se suele definir la topología que tendrá la red: malla, anillo, red, árbol, punto a punto, entre otros.

Finalmente, en esta capa también se definen las características de los dispositivos de la red (*hardware*).

1.2.1.2. Capa de internet

Esta capa se ocupa de la estructura de los paquetes de datos básicos que transitan por la red y define la manera en que se envían. También cumple la función de identificar a los *hosts* mediante una dirección y enrutamiento que permitan a los paquetes llegar a su destino. En esta capa es donde trabaja el protocolo IP.

1.2.1.3. Capa de transporte

Sobre esta capa funciona el protocolo TCP y UD; una de sus principales funciones es la segmentación de paquetes, control de errores y flujo de estos.

Así también, establece los canales básicos que utilizarán las aplicaciones para el intercambio de paquetes entre dos *hosts*; esto lo realiza asociando un puerto con un tipo de aplicación y de dato.

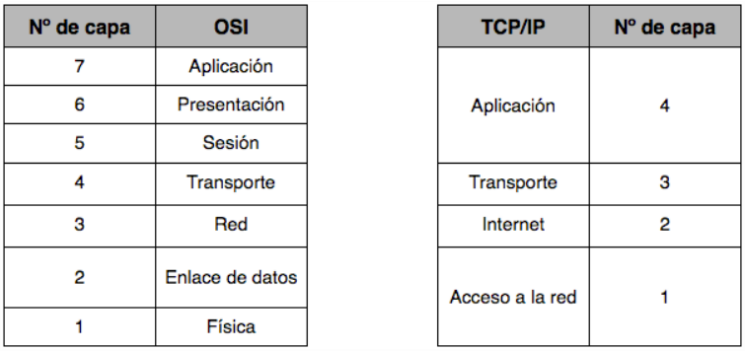
1.2.1.4. Capa de aplicación

Al igual que en el modelo OSI, esta capa, al ser la última, es la más cercana al usuario. En esta se definen los protocolos que usarán las aplicaciones que brindan un servicio al usuario. Se comunica con las tres capas inferiores y proporciona su propio encapsulamiento según el tipo de aplicación y dato con el cual se trabaja.

1.3. Comparación entre el modelo OSI y modelo TCP/IP

El protocolo TCP es utilizado para que todos los nodos conectados a internet se puedan comunicar entre sí de manera fiable. Es un protocolo orientado a la conexión que junto con el protocolo IP han servido de base para el modelo TCP/IP, dichos protocolo han sido utilizados desde antes que se estableciera el modelo OSI y por esta razón el modelo TCP/IP es comparado con el modelo OSI.

Figura 3. **Diagrama de los modelos OSI y TCP/IP**



Nº de capa	OSI
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

TCP/IP	Nº de capa
Aplicación	4
Transporte	3
Internet	2
Acceso a la red	1

Fuente: DI TOMMASO, Leandro. *Modelos OSI y TCP/IP.* https://www.mikroways.net/2009/08/08/modelos-osi-y-tcpip/. Consulta: diciembre de 2020.

En el caso del modelo OSI, este se conforma de siete capas; tres más que el modelo TCP/IP. La capa de aplicación es la más cercana al usuario y la física la más lejana de este.

Acerca de las descripciones de las capas de ambos modelos, se puede concluir que la de aplicación del modelo TCP/IP cumple con las funciones de las capas 5, 6 y 7 (sesión, presentación y aplicación) del modelo OSI. La capa de transporte del modelo TCP/IP cumple con las mismas funciones que la capa 4 (transporte) y algunas responsabilidades de la capa 6 (sesión) del modelo OSI.

La capa de acceso a la red del modelo TCP/IP abarca las capas 1 y 2 (física y enlace de datos) del modelo OSI.

El modelo OSI se suele tomar como un modelo conceptual, el cual se utiliza principalmente para describir, discutir y entender el funcionamiento de una red individual. En contraparte, el modelo TCP/IP está diseñado para resolver un conjunto específico de problemas y no para funcionar como una descripción de generación para las comunicaciones de red.

1.4. Dispositivos configurables

Los dispositivos que puede ser empleados en una red de computadoras son *hardware,* los cuales permiten la comunicación entre varios *hosts* en una red. Se cuenta con dispositivos configurables y con los que realizan ciertas acciones por defecto.

1.4.1. *Switch*

Es un dispositivo que permite conectar varios dispositivos (pc, impresora, etc.) dentro de una red. Al momento en que es enviado un paquete a través de la red, se envía un mensaje y el *switch* es el encargado de la retransmisión de este solo por la salida en que se encuentra el destino del paquete. Este dispositivo no proporciona conectividad con otras redes por sí solo (únicamente con una red local) y tampoco proporciona conectividad con internet. Para realizar estas funciones es necesario la implementación de un router. Este trabaja en la capa 2 del modelo OSI.

1.4.2. *Router*

Es un dispositivo que permite el tráfico de información a través de una ruta adecuada. Para su funcionamiento utiliza direcciones IP y así determinar por dónde tiene que enviar los paquetes. En este dispositivo las rutas deben ser indicadas por el administrador de la red. En caso de que estas rutas no sean indicadas, el dispositivo no puede enviar los paquetes a su destino. Este trabaja en la capa 3 del modelo OSI.

1.4.3. *Switch* multicapa

Es un dispositivo que integra funciones de conmutación (*switch*) y enrutamiento (*router*). Está diseñado para el manejo a alto rendimiento del tráfico de redes locales, por lo cual este puede ser ubicado en cualquier lugar dentro de la red y puede sustituir a los *switch* y *router* convencionales. Por medio de configuración, se puede indicar al dispositivo si trabajará en la capa 2 o 3 del modelo OSI.

1.4.4. *Firewall*

Es un dispositivo orientado a la seguridad de la red que tiene como función el monitoreo del tráfico de la red (paquetes que entran salen) en función de las políticas configuradas que permiten o deniegan el paso de los paquetes. Si un *firewall,* inicialmente, no posee ninguna configuración, bloqueará el paso de todo el tráfico de la red. Este trabaja en las capas 3 y 4 del modelo OSI.

1.5. Protocolos configurables

Los diversos dispositivos que interactúan en una topología de red necesitan ser configurados para permitir o denegar el trafico de paquetes. Estos protocolos trabajan sobre la capa 2, 3 y 4 de las capas del modelo OSI.

1.5.1. VLAN

Las VLANs (*Virtual LAN*) son empleadas para agrupar *hosts* que pertenecen a un mismo domino de *broadcast*, independientemente de dónde estén localizados dentro de la red física. Con ello, se provee a la red de flexibilidad, segmentación y seguridad.

Este protocolo es únicamente configurable en un *switch* o en varios de estos. Al momento de emplear varios *switches*, es necesario propagar las VLANs mediante el uso de enlaces troncales.

Cada VLAN es configurada en la topología de red corresponde a una IP, lo cual se debe tomar en cuenta al momento de implementar un esquema de direccionamiento de red jerárquico. Esto indica que los números de redes IP se deben aplicar a los segmentos de red o a las VLANs de forma ordenada.

Para la configuración de las VLANS en dispositivos Cisco, se realiza mediante los siguientes comandos:

Figura 4. **Comandos de configuración VLAN**

```
Switch# configure terminal
Switch(config)# vlan vlan-number
Switch(config-vlan)# vlan vlan-name
Switch(config-vlan)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 568 y 569.

1.5.2. VTP

El protocolo VTP (*Vlan Trucking Protocol*) mantiene la relación de las VLANs configuradas a través de un dominio de administración común y gestiona el control sobre los cambios (adición, eliminación y modificación) en las VLANS a través de la red.

Un dominio VTP se refiere a los *switches* que se encuentran interconectados compartiendo un mismo entorno de VTP. Un *switch* solamente puede albergar un único dominio VTP.

Para que un *switch* pertenezca al mismo dominio, debe:

- Estar configurado bajo el mismo dominio.
- Tener la misma contraseña del dominio.
- Tener la misma versión de VTP (por defecto los dispositivos Cisco asignan la versión 2).

El protocolo VTP puede estar configurado en tres modos:

- Servidor: Es el modo por defecto. Los dispositivos configurados en este modo pueden crear, modificar y eliminar VLANs. Estos cambios se verán reflejados en todos los dispositivos configurados bajo el mismo dominio de VTP.
- Cliente: En este modo los dispositivos no pueden crear, modificar o eliminar VLANs. Solamente pueden sincronizar la información del dispositivo configurado en modo servidor.
- Transparente: Los dispositivos configurados en este modo permiten crear, modificar y eliminar VLANs, pero los cambios efectuados solamente son a nivel local; no son trasmitidos a los demás *switches* del dominio.

La configuración de este protocolo se realiza mediante los siguientes comandos:

Figura 5. **Comandos de configuración VTP**

```
Switch# configure terminal
Switch(config)# vtp mode {client | server | transparent}
Switch(config)# vtp domain domain-name
Switch(config)# vtp password domain-password
Switch(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 581.

1.5.3. STP

Generalmente las redes se encuentran diseñadas con dispositivos y enlaces redundantes. Esto, con el objetivo de evitar que un fallo individual afecte directamente a toda la red, y esto genere la pérdida del tráfico de paquetes. Por ello, el protocolo STP (*Spanning Tree Protocol*) presenta como objetivo eliminar

los bucles infinitos que se puedan crear dentro de la topología de red. Esta función la lleva a cabo mediante el siguiente proceso:

- Elección de un switch raíz: Dentro de un dominio de difusión solamente puede existir un *switch* raíz. Los puertos de este *switch* se encuentran en estado enviando y se denominan puertos designados. Esta elección se realiza según la prioridad de los *switches*: el que tenga menor prioridad es seleccionado como raíz, y en caso de que todos los dispositivos posean la misma prioridad, se selecciona el dispositivo con mayor dirección MAC (en su valor hexadecimal).
- Puerto raíz: Corresponde a la ruta que presenta el menor costo desde el *switch* no raíz a la raíz. Esta ruta se basa en el ancho de banda.
- Puerto designado: Es el encargo de conectar los segmentos hacia el *switch* raíz; solamente puede existir uno por segmento.

Este protocolo se configura por defecto; en caso de que se quiera cambiar el *switch* raíz se realiza mediante los siguientes comandos:

Figura 6. **Comandos de configuración STP**

```
Switch# configure terminal
Switch(config)# spanning-tree vlan # {primary | secundary}
Switch(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 534.

1.5.4. Puertos

En ocasiones es necesario juntar diversos *hosts* que pertenezcan a una misma VLAN, los cuales físicamente se encuentra en diferentes partes de la red. Para permitir la comunicación entre ellos, es necesario la configuración de los puertos con los cuales van a interactuar.

Cuando las tramas salen de los *switches*, estas son etiquetadas según la VLAN a la que corresponden. Por ello, es necesario configurar la interfaz de los dispositivos para permitir el ingreso de los paquetes; por consiguiente, los puertos son configurables en los siguientes modos: *trunk* y *access*.

1.5.4.1. Puerto en modo *trunk*

Este tipo de puerto presenta como principal utilidad realizar la conexión entre varios *switches*, lo cual permite el tráfico de múltiples VLANs y, por consiguiente, poseer diversas VLANs en un *switch* y un único enlace para el transporte de todo el tráfico.

La configuración del puerto en modo *trunk*, se realiza mediante los siguientes comandos:

Figura 7. **Comandos de configuración puerto en modo *trunk***

```
Switch# configure terminal
Switch(config)# interface type-interface #/#
Switch(config)# switchport mode trunk
Switch(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 571.

1.5.4.2. Puerto en modo *access*

Este tipo de puerto presenta como principal utilidad realizar la conexión con equipos finales, lo cual permite el tráfico de paquetes correspondiente a una única VLAN.

La configuración del puerto en modo *access*, se realiza mediante los siguientes comandos:

Figura 8. **Comandos de configuración puerto en modo *access***

```
Switch# configure terminal
Switch(config)# interface type-interface #/#
Switch(config)# switchport mode access
Switch(config)# switchport access vlan #
Switch(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 571.

1.5.5. InterVLAN

Las VLANs son un dominio de broadcast único. Por lo tanto, un *host* de una VLAN no puede comunicarse con otro de una diferente. Cada vez que *hosts* de diferentes VLANS necesitan comunicarse entre sí, se debe rutear el tráfico entre ambos. Este proceso se conoce como InterVLAN. Este protocolo trabaja sobre la capa 3 del modelo OSI.

Para permitir este ruteo se deben realizar las siguientes configuraciones:

Figura 9. **Comandos de configuración InterVLAN**

```
Router# configure terminal
Router(config)# interface type-interface #/#
Router(config-if)# encapsulation dot1Q vlan-number
Router(config-if)# ip address ip-address subnet-mask
Router(config-if)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 575, 578.

1.5.6. Enrutamiento

Es un proceso que permite mover un paquete desde un *host* que se encuentra en una red hacia otro que se encuentra en una diferente. El enrutamiento se puede llevar a cabo en dispositivos enrutables (*routers*, *firewalls*, *switch* multicapa, entre otros). Para poder enviar un paquete hacia otra es necesario que los dispositivos conozcan lo siguiente:

- Dirección IP del dispositivo destino
- Dispositivos vecinos desde los cuales se puede aprender rutas de redes remotas
- Posibles rutas hacia cada red remota
- La mejor ruta hacia cada red remota
- Cómo mantener y verificar la información de enrutamiento

1.5.6.1. Enrutamiento estático

En este tipo de enrutamiento las rutas son de carácter estático y son definidas manualmente por el administrador.

Entre las ventajas de implementar un enrutamiento estático están:

- Facilita la implementación en redes pequeñas.
- Brinda mayor seguridad; no hace envío de mensajes como algunos protocolos de enrutamiento dinámico.
- La ruta hacia el destino es siempre la misma.
- No implementa algoritmos de *routing* o actualización, por lo cual no requiere de recursos adicionales.

Las desventajas que presenta el enrutamiento estático son:

- La complejidad de la configuración aumenta en función del crecimiento de la red.
- El mantenimiento de la red incrementa en función del tamaño de la red.
- Se requiere de una intervención manual para volver a enrutar el tráfico de paquetes, en caso de una falla en la ruta.

La configuración del enrutamiento estático se realiza mediante los siguientes comandos:

Figura 10. **Comandos de configuración enrutamiento estático**

```
Router# configure terminal
Router(config)# ip route destination-network mask next-hop-
address
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 364.

1.5.6.1.1. Enrutamiento estático predeterminado

Es un enrutamiento especial, el cual se implementa normalmente para el tráfico de internet, debido a que es imposible indicarle manualmente al dispositivo todas las rutas. Consiste en indicarle al dispositivo una dirección de red destino predeterminada (0.0.0.0) y una máscara, también predeterminada, para la red destino (0.0.0.0).

La configuración de este enrutamiento se realiza mediante los comandos:

Figura 11. **Comandos de configuración enrutamiento estático predeterminado**

```
Router# configure terminal
Router(config)# ip route 0.0.0.0 0.0.0.0 outside-interface
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 692.

1.5.6.2. Enrutamiento dinámico

Este tipo de enrutamiento permite a los dispositivos ajustar, en tiempo real, los caminos que se van a emplear para trasmitir paquetes. Los dispositivos reciben y procesan actualizaciones enviadas por los dispositivos vecinos, esto, con el objetivo de conocer las rutas existentes para el envío de tráfico.

Entre las ventajas de implementar un enrutamiento dinámico están:

- El trabajo de configuración (agregar o quitar redes) es menor.
- Los protocolos de enrutamiento reaccionan automáticamente a los cambios dentro de la topología de red.
- El crecimiento de la red no presenta inconvenientes en la configuración; proporciona escalabilidad a la solución.
- La configuración es menos propensa a errores.

Las desventajas que presenta el enrutamiento dinámico son:

- La cantidad de recursos en los dispositivos configurados son mayores en comparación al enrutamiento estático.
- El personal que administra los dispositivos requiere mayor conocimiento para la configuración, verificación y resolución de errores.

1.5.6.2.1. Enrutamiento RIP

El protocolo RIP (*Routing Information*), es un protocolo de enrutamiento de tipo vector distancia, por ello calcula la mejor ruta para el envío del tráfico de paquetes utilizado como métrica el número de saltos. Este protocolo soporta un máximo de quince saltos.

La configuración del protocolo RIP se realiza mediante los siguientes comandos:

Figura 12. **Comandos de configuración enrutamiento dinámico RIP**

```
Router# configure terminal
Router(config)# router rip
Router(config-router)# network network-identifier
Router(config-router)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 384.

1.5.6.2.2. Enrutamiento OSPF

El protocolo OSPF (Open Shortest Path First) utiliza el algoritmo Dijkstra para encontrar la mejor ruta para enviar el tráfico; no requiere que los dispositivos configurados bajo este protocolo intercambien tablas de enrutamiento en intervalos específicos. Se basa en el ancho de banda para el cálculo de métricas.

La configuración del protocolo OSPF se realiza mediante los siguientes comandos:

Figura 13. **Comandos de configuración enrutamiento dinámico OSPF**

```
Router# configure terminal
Router(config)# router ospf #
Router(config-router)# network network-identifier wildcard
Router(config-router)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 450.

1.5.6.2.3. Enrutamiento EIGRP

El protocolo EIGRP (*Enchaced Interior Gateway Routing Protocol*), se puede definir como híbrido, ya que es un protocolo de tipo vector distancia y estado enlace. EIGRP permite a los dispositivos involucrados en la topología sincronizarse para la actualización de la tabla de ruteo. Este protocolo tiene un número de saltos máximos de 255.

La configuración del protocolo EIGRP se realiza mediante los siguientes comandos:

Figura 14. **Comandos de configuración enrutamiento dinámico EIGRP**

```
Router# configure terminal
Router(config)# router eigrp #
Router(config-router)# network network-identifier
Router(config-router)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 426.

1.5.7. *Access-List*

Las ACL indican al dispositivo qué tipo de paquetes debe aceptar o rechazar, en función de las condiciones establecidas con las cuales se administra el tráfico de paquetes y se asegura el acceso hacia y desde una red. Las ACL son restricciones que definen cómo se procesan los paquetes que:

- Entran en las interfaces del dispositivo.
- Se reenvían a través del dispositivo.
- Salen de las interfaces del dispositivo.

1.5.7.1. *Access-List* estándar

Las ACL estándar filtran según la dirección origen de donde provienen los paquetes IP. Para la configuración, es necesario indicarle un número a la lista de restricciones o permisos; este debe estar dentro del rango de 1 a 99 y de 1,300 a 1,999. Se recomienda que las ACL estándar se configuren cerca del destino del paquete.

Para la configuración de una ACL estándar se realiza mediante los comandos:

Figura 15. **Comandos de configuración *Access-list* estándar**

```
Router# configure terminal
Router(config)# access-list # {deny | permit | remark} {host | any}
{wilcard}
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*. p. 620 y 621.

1.5.7.2. *Access-List* extendida

Las ACL extendidas filtran en función tanto de la dirección origen de donde proviene el paquete, como de la dirección destino a donde se dirige el paquete IP. Se suelen implementar con mayor frecuencia que las ACL estándar debido a que permiten filtrar los paquetes mediante protocolos, número de puerto, valor de precedencia, etc. Para la configuración, es necesario indicarle un número a la lista; este debe estar dentro del rango de 100 a 199 y de 2 000 a 2 699. Se recomienda que las ACL extendidas se coloquen y configuren cerca de la fuente u origen del paquete.

Para la configuración de una ACL extendida se realiza mediante los comandos:

Figura 16. **Comandos de configuración *Access-list* extendida**

```
Router# configure terminal
Router(config)# access-list # {deny | permit | remark | dynamic}
{protocol} {source-adress | host | any} {wilcard} {source-adress |
host | any} {wilcard} {source-adress | host | any} {wilcard}{source-
adress | host | any} {wilcard}
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 620 y 621.

1.5.7.3. Configuración de interfaces ACL

Posterior a la configuración de la ACL, se deben configurar las interfaces de los dispositivos donde se ha configurado la ACL.

Para la configuración de los puertos se realiza mediante los siguientes comandos:

Figura 17. **Comandos de configuración interfaces ACL**

```
Router# configure terminal
Router(config)# interface type-interface #/#
Router(config-if)# ip Access-group numer-ACL {in | out }
Router(config-if)# exit
```

Fuente: elaboración propia, con datos de *Listas de Control de acceso ACL.* http://atc2.aut.uah.es/~rosa/LabRC/Prac_5/Listas%20de%20Control%20de%20acceso.pdf Consulta: diciembre de 2020.

Donde:

- In: Es la interfaz por donde llega el tráfico de paquetes y luego pasa al dispositivo.
- Out: Es la interfaz por donde ya ha pasado el tráfico de paquetes y está saliendo del dispositivo.

1.5.8. NAT

Un protocolo NAT (*Network Address Translator*) permite modificar la dirección de salida de los paquetes, con lo cual, se puede enmascarar una red privada permitiéndole salir a internet con una dirección pública. El objetivo de este protocolo es brindar seguridad a los *hosts* conectados a una red privada, ya que estas no serán visibles desde el exterior, lo cual previene un posible ataque externo.

Adicionalmente, utilizar NAT proporciona un ahorro de dirección IP, debido a que permite conectar múltiples dispositivos de una red a internet utilizando una única dirección IP pública.

1.5.8.1. NAT estática

Este tipo de NAT es una asignación, de uno a uno, entre una dirección IP privada con una pública (la cual no sufre cambios; siempre será la misma). Esto permite que los *hosts* externos puedan iniciar conexiones con los internos de la red, por medio de la dirección pública asignada a este dispositivo.

Los comandos para la configurar NAT estática son:

Figura 18. **Comandos de configuración NAT estática**

```
Router# configure terminal
Router(config)# ip nat inside source static in-address out-address
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 689.

1.5.8.2. NAT dinámica

Este tipo de NAT le asigna varias direcciones de IP públicas al dispositivo, de manera que cada dirección IP privada es mapeada por medio de una de las direcciones de IP públicas asignadas al dispositivo. Así, cada vez que la dirección IP privada sale, puede utilizar cualquiera de las direcciones IP públicas disponibles y por ende, la dirección del host siempre va cambiando.

Los comandos para la configuración NAT dinámica son:

Figura 19. **Comandos de configuración NAT dinámica**

```
Router# configure terminal
Router(config)# ip nat pool name-list first-source-address last-source-address netmask network-mask
Router(config)# exit
```

Fuente: TODD LAMMLE. *CCNA: Cisco Certified Network Associate Study Guide*, Sixth Edition. p. 682.

1.5.9. Protocolos de redundancia

Los protocolos de redundancia tienen como función primordial mantener la confiabilidad de la red, mediante diversos enlaces físicos conectados entre dispositivos. Estos proporcionan rutas redundantes, con lo cual se permite a la red seguir funcionando en caso de fallo de un enlace. Proporcionan al *host* un *gateway* predeterminado (virtual) con el cual los paquetes saldrán, en caso de que falle el principal.

1.5.9.1. Protocolo GLBP

El protocolo GLBP (*Gateway Load Balance Protocol*), además de proporcionar redundancia a la red, permite el balanceo de cargas al asignar varias direcciones MAC a una misma IP virtual. Este protocolo funciona por medio de la asignación de un rol a los dispositivos; entre los roles se encuentran:

- AVG: Es el dispositivo con mayor prioridad y funciona como el encargado de responder a las peticiones, así también, indica hacia dónde se deben enviar los paquetes en el caso de balanceo.
- AVF: En este modo operan los demás dispositivos en la red. En caso de que el AVG falle, el dispositivo con mayor prioridad de los AVF asumirá el rol de AVG.

El protocolo GBLP permite configurar tres tipos de balanceos de cargas:

- *Round Robin:* En este tipo, los dispositivos configurados reciben y envían la misma cantidad de tráfico.
- *Weighted:* En este tipo de balanceo, se indica el porcentaje de tráfico que permitirá cada dispositivo.

- *Host dependent:* En este tipo, el tráfico se envía a un dispositivo en específico.

Figura 20. **Comandos de configuración, protocolo de redundancia GLBP (*router* AVG)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# glbp # ip ip-address
Router(config-if)# glbp # pritority #
Router(config-if)# glbp # preempt
Router(config)# exit
```

Fuente: SUPUTRA, Arranda. *Configure GLBP in Cisco IOS Router.* http://www.mustbegeek.com/configure-glbp-in-cisco-ios-router/. Consulta: diciembre de 2020.

Figura 21. **Comandos de configuración, protocolo de redundancia GLBP (*router* AVF)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# glbp # ip ip-address
Router(config-if)# glbp # pritority #
Router(config)# exit
```

Fuente: SUPUTRA, Arranda. *Configure GLBP in Cisco IOS Router.* http://www.mustbegeek.com/configure-glbp-in-cisco-ios-router/. Consulta: diciembre de 2020.

1.5.9.2. Protocolo HSRP

El protocolo HSRP utiliza una dirección MAC y una IP virtual donde un *gateway backup* asume el mando en caso de ocurrir un fallo en el *gateway active*.

Este protocolo funciona por medio de la asignación de un rol a los dispositivos; entre los roles se encuentran:

- *Active:* Es el dispositivo con mayor prioridad y se encarga de enrutar los paquetes mediante la IP virtual configurada.
- *Standby:* Son los dispositivos que esperan a asumir el rol de *active,* en caso de una falla. El dispositivo que se asigna como *active* (en caso de una falla) es el que posea la mayor prioridad configurada (menor a la del dispositivo active) entre los *standby*.

Figura 22. **Comandos de configuración, protocolo de redundancia HSRP (*router active*)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# standby ip ip-address
Router(config-if)# standby # pritority #
Router(config-if)# standby # preempt
Router(config)# exit
```

Fuente: Suputra Arranda. *Configure HSRP in Cisco IOS Router.* http://www.mustbegeek.com/configure-hsrp-in-cisco-ios-router/. Consulta: diciembre de 2020.

Figura 23. **Comandos de configuración, protocolo de redundancia HSRP (*router standby*)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# standby ip ip-address
Router(config-if)# standby # pritority #
Router(config)# exit
```

Fuente: SUPUTRA, Arranda. *Configure HSRP in Cisco IOS Router.* http://www.mustbegeek.com/configure-hsrp-in-cisco-ios-router/. Consulta: diciembre de 2020.

1.5.9.3. Protocolo VRRP

El protocolo VRRP (*Virtual Router Redundancy Protocol*) asigna de manera dinámica la responsabilidad para un dispositivo virtual, el cual manejará el tráfico en la red. Este protocolo no es propiedad de Cisco, pero es implementable en sus dispositivos. Este funciona por medio de la asignación de un rol a los dispositivos; entre los roles se encuentran:

- *Master:* Es el dispositivo configurado con mayor prioridad; este se encarga del manejo del tráfico de la red.
- *Slave:* Son los dispositivos que esperan a asumir el rol de *master,* en caso de una falla. El dispositivo que se asigna como *master* (en caso de una falla) es el que posea la mayor prioridad configurada (menor a la del dispositivo *master*) entre los *slave*.

La configuración del protocolo VRRP se realiza mediante los siguientes comandos:

Figura 24. **Comandos de configuración, protocolo de redundancia VRRP (*router* maestro)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# vrrp # ip ip-address
Router(config-if)# vrrp # pritority #
Router(config-if)# vrrp # preempt
Router(config-if)# exit
```

Fuente: SUPUTRA, Arranda. *Configure VRRP in Cisco IOS Router.* http://www.mustbegeek.com/configure-vrrp-in-cisco-ios-router/. Consulta: diciembre de 2020.

Figura 25. **Comandos de configuración, protocolo de redundancia VRRP (*router* esclavo)**

```
Router# config terminal
Router(config)# interface type-interface #/#
Router(config-if)# vrrp # ip ip-address
Router(config-if)# vrrp # pritority #
Router(config-if)# exit
```

Fuente: SUPUTRA, Arranda. *Configure VRRP in Cisco IOS Router.* http://www.mustbegeek.com/configure-vrrp-in-cisco-ios-router/. Consulta: diciembre de 2020.

1.5.10. *Firewall*

Este dispositivo trabaja en función de reglas de seguridad, las cuales determinan si permite o no el tráfico de paquetes en la red. Se pueden establecer reglas que analicen el tráfico de paquetes en base de direcciones IP o protocolos.

1.5.10.1. Políticas de seguridad

Las políticas de seguridad en un *firewall* son un conjunto de restricciones, con las cuales se analizan los paquetes tanto de entrada como de salida. Los paquetes son filtrados mediante protocolos; entre estos se encuentran: dns, ftp, h323, http, icmp y tftp.

En caso de que no exista alguna configuración de políticas el *firewall,* se bloquea todo el tráfico de datos.

Figura 26. **Comandos de configuración, políticas de seguridad en *firewall***

```
Firewall# config terminal
Firewall(config)# class-map name-class-map
Firewall(config-cmap)# match match-inspection-traffic
Firewall(config-cmap)# exit
Firewall(config)# policy-map name-policy
Firewall(config-pmap)# class name-class-map
Firewall(config-pmapC)# inspect protocol
Firewall(config-pmapC)# exit
Firewall(config)# service-policy name-policy global
Firewall(config)# exit
```

Fuente: MUNAGALA SRINIVASA, Sharma Dinkar. *Guía de Cisco para endurecer el Firewall de Cisco ASA.* https://www.cisco.com/c/es_mx/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html. Consulta: diciembre de 2020.

1.5.10.2. VLAN

Las VLANs (*Virtual LAN*) son empleadas para agrupar *hosts* que pertenecen a un mismo domino de *broadcast*, independientemente de dónde se encuentren

localizados dentro de la red física. Con ello, se provee a la red de flexibilidad, segmentación y seguridad.

En los *firewalls* ASA o PIX se manejan 3 VLANs:

- Vlan 1: Corresponde a la red *outside* y para su configuración y correcto funcionamiento, se le debe asignar un nivel de seguridad de 0. Esta VLAN se recomienda que sea asignada a la interfaz 0/0 del *firewall*.
- Vlan 2: Corresponde a la red DMZ y para su configuración y correcto funcionamiento, se le debe asignar un nivel de seguridad de 50. Esta VLAN se recomienda que sea asignada a la interfaz 0/1 del *firewall*.
- Vlan 3: Corresponde a la red *inside* y para su configuración y correcto funcionamiento, se le debe asignar un nivel de seguridad de 100. Esta VLAN se recomienda que sea asignada a la interfaz 0/2 del *firewall*.

La configuración del puerto en modo *trunk*, se realiza mediante los siguientes comandos:

Figura 27. **Comandos de configuración VLAN en *firewall***

```
Firewall# configure terminal
Firewall(config)# interface vlan #
Firewall(config-if)# name-if name-vlan
Firewall(config-if)# security-level #
Firewall(config-if)# ip address ip-address network-mask
Firewall(config-if)# exit
```

Fuente: elaboración propia.

1.5.10.3. SSH

El protocolo SSH (*Secure Shell*) permite realizar administración remota de los dispositivos por medio de un canal donde es cifrada la información, lo cual se garantiza mediante técnicas criptográficas. Este servicio fue creado como un reemplazo seguro del protocolo Telnet (el cual no cifraba la información).

La configuración de acceso remoto mediante SSH se realiza mediante los comandos:

Figura 28. **Comandos de configuración de SSH en *firewall***

```
Firewall# configure terminal
Firewall(config)# username name password user-password
Firewall(config)# aaa authentication ssh console LOCAL
Firewall(config)# cryto key generate rsa modulus 1024
Firewall(config)# ssh ip-address network-mask name-VLAN
Firewall(config)# exit
```

Fuente: MUNAGALA SRINIVASA, Sharma Dinkar. *Guía de Cisco para endurecer el Firewall de Cisco ASA.* https://www.cisco.com/c/es_mx/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html. Consulta: diciembre de 2020.

2. USO DE APLICACIONES MÓVILES EN EL SECTOR EDUCATIVO

En la actualidad, la mayoría de la población tiene acceso a un teléfono móvil (*smartphone*) y debido al avance tecnológico, varios sectores se han innovado para adaptarse; esto incluye al sector educativo. Lo anterior, ha provocado el surgimiento de conceptos como *e-learning* (aprendizaje electrónico) y *"Mobile Learning* (aprendizaje móvil). Estos buscan transferir el conocimiento de una manera más flexible y aprovechar las nuevas tecnologías móviles que facilitan, apoyan y mejoran el proceso de aprendizaje-enseñanza.

El uso del internet y almacenamiento en la nube ha dado la posibilidad de interactuar y obtener información en tiempo real. Las constantes innovaciones en tecnología que buscan aprovechar los dispositivos móviles obligan a los diversos sectores, incluido el educativo, a no enforcarse únicamente en plataformas web.

La implementación de las Tecnologías de la Información y Comunicación (TIC) en el sector educativo ha adquirido una creciente importancia y ha ido evolucionando con el paso del tiempo. Según la página web AppBrain[1], durante el presente año, las aplicaciones educativas que poseen los primeros lugares de descargas en la *Play store* (de Google) son Google Classroom[2], seguida de Duolingo[3].

[1] Google Play. *Most popular categories.* https://www.appbrain.com/stats/android-market-app-categories.
[2] Google. Classroom https://play.google.com/store/apps/details?id=com.google.android.apps.classroom&hl=es_GT.
[3] Google Play. *Duolingo*. https://play.google.com/store/apps/details?id=com.duolingo&hl=es_G.

2.1. ¿Qué son las aplicaciones móviles educativas?

El creciente uso de la tecnología móvil (*smartphones* y *tablets*) y el acceso al internet desde cualquier lugar, han dado paso a conceptos como *e-learning* y *Mobile Learning*. El *Mobile Learning* ofrece la posibilidad de un aprendizaje más personalizado y fomenta el aprendizaje autodirigido, además de la practicidad que ofrece utilizar el *smartphone* como medio de aprendizaje por su mayor portabilidad en comparación con otros dispositivos.

Una aplicación móvil educativa se puede definir como una plataforma que incluye diversas herramientas destinadas a fines docentes, mediante contenido didáctico (material pdf, lecturas, entre otros) o contenidos multimedia, los cuales permiten aprender o reforzar conocimientos. Estos *softwares* son diseñados para ser utilizados a través de dispositivos móviles.

Las aplicaciones móviles también buscan aprovechar la influencia positiva que ejercen los dispositivos móviles en la motivación de los estudiantes, obtenida de la gran popularidad que los dispositivos móviles poseen entre la población de todas las edades. Además de fomentar la interacción entre usuarios, pues se rompe con la clásica experiencia de aprendizaje pasivo, estos permiten un aprendizaje más eficaz, ya que el alumno también es partícipe activo durante todo el proceso.

2.1.1. Tipos de aplicaciones móviles educativas

Existen dos tipos de aplicaciones móviles educativas, estas son según el tipo de actividad a la cual están destinadas.

2.1.1.1.1. Aplicaciones móviles educativas comerciales

Se trata de aplicaciones que han sido creadas por empresas o instituciones con fines de lucro. En este caso, requieren del pago de una cuota; en contraparte, por este pago se obtiene mayor fiabilidad y asistencia al docente.

2.1.1.1.2. Aplicaciones móviles educativas de *software* libre

Se trata de aplicaciones que han sido creadas sin fines de lucro. Son aplicaciones para ser usadas con cualquier finalidad; de estas es posible distribuir copias y no es necesario realizar un pago para tener acceso.

2.2. Tecnologías de la información y comunicación (TIC) y su uso en Educación

Las Tecnologías de la información y comunicación (TIC) son los recursos y herramientas utilizables para administrar, procesar y compartir información, a través de los diversos soportes tecnológicos (*smartphones*, *tablets*, televisores, entre otros).

Las TIC juegan un papel importante en la actualidad, ya que ofrecen diversos servicios imprescindibles tales como: búsqueda de información, servicios de correo electrónico, descarga de data, entre otros.

Según el informe *Coronavirus (COVID-19): impact on the global tech goods & services industry*[4] de Statista, existe un aumento en pedidos a nivel global de *smartphones* y *tablets* para el año 2020 y de ventas para el periodo 2020-2021. Este incremento en el uso de dispositivos móviles es un reflejo del impacto que tiene la tecnología en el uso cotidiano para realizar la mayoría de las actividades diarias. Por otro lado, esto refleja la necesidad de los diversos sectores de incursionar en el tema de aplicaciones móviles.

Durante el 2020, a causa de la pandemia de COVID19, las tendencias en el sector educativo se orientaron hacia a la educación a distancia. Los artículos Aprendiendo en casa: educación a distancia para todos[5] y La brecha digital impacta en la educación[6], de Unesco y Unicef, respectivamente, resaltan las necesidades de tener plataformas virtuales de calidad orientadas a la educación. Estas ofrecen alternativas educativas en momentos críticos, en los cuales la educación tradicional no es una opción.

Esta tecnología está implícita en las herramientas educativas según las funciones antes descritas; esto, para adaptarse y mejorar la experiencia de los usuarios y lograr así, un proceso de aprendizaje más dinámico. Al combinar el uso de otros servicios (como almacenamiento en la nube) con las TIC se permite un mejor control administrativo y el acceso a la data de forma inmediata por parte de los usuarios.

[4] Coronavirus. (COVID-19). *Impact on the global tech godos & services industry*. https://statista.com/ topics/6156/coronavirus-covid-19-impact-on-tech-goods-and-services.
[5] Aprendiendo en casa. *Educación a distancia para todos*. https://es.unesco. org/news/aprendiendo-casa-educacion-distancia-todos.
[6] UNICEF. *La brecha digital impacta en la educación*. https://www.unicef.es/educa/blog/covid-19-brecha-educativa.

2.3. Sistemas operativos para dispositivos móviles utilizados en Guatemala

En Guatemala, se hace uso de diversos sistemas operativos en los teléfonos móviles y el sistema operativo Android es el que posee mayor presencia en el mercado. La aplicación de *ConfiRedes,* la cual se detalla en el siguiente capítulo, fue desarrollada para Android. Por lo anterior, este sistema operativo se explica más ampliamente a continuación, en comparación con los otros sistemas utilizados en el territorio nacional.

2.3.1. Android

Es el sistema operativo más popular a nivel mundial para dispositivos móviles. Según la página web Statcounter[7], Android cuenta con un 71,93 % de la participación del mercado a nivel global.

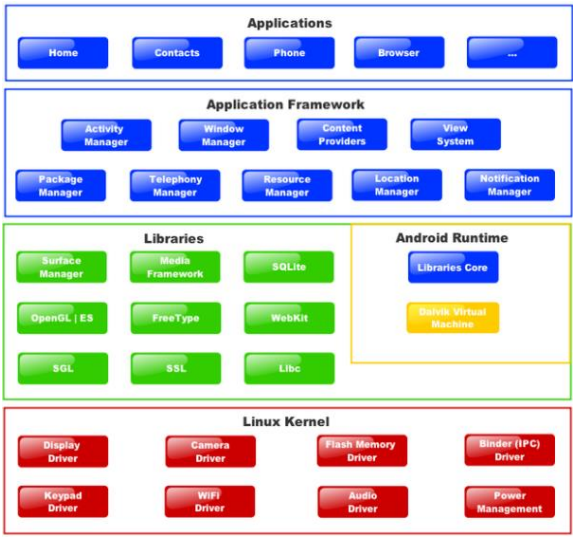
Fue desarrollado por Android Inc., y adquirido en el 2005 por Google. Se encuentra desarrollado con base en el Kernel de Linux y de otros softwares de código abierto; actualmente Android es un sistema operativo mantenido por la comunidad de Linux Open Source. La versión más reciente es Android 11, la cual fue lanzada el 8 de septiembre de 2020.

2.3.1.1. Arquitectura de Android

Android maneja una arquitectura divida en cinco capas: *Linux Kernel, android runtime, libraries, application framework* y *applications.*

[7] Statcounter GlobalStats. https://gs.statcounter.com/os-market-share/mobile/worldwide Consultado: 11 de febrero de 2021.

Figura 29. **Arquitectura de Android**



Fuente: NIETO GONZALES, Alejandro. *¿Qué es Android?* En: https://i.blogs.es/87e688/646px-diagram_android/1366_2000.png. Consulta: febrero de 2021.

A continuación, se detallan los principales componentes que conforman la arquitectura de Android.

2.3.1.1.1. Linux Kernel

Actúa como una capa de abstracción entre el *hardware* y las aplicaciones instaladas en el dispositivo. Depende de Linux para la gestión de servicios como seguridad, gestión de memoria, gestión de procesos, controladores y pila de red.

2.3.1.1.2. Android runtime

Es un conjunto de bibliotecas basadas en el lenguaje Java, las cuales proporcionan la mayor parte de funciones disponibles para el correcto

funcionamiento del SO. Posterior de la versión 5 de Android, las bibliotecas son compiladas al momento de la instalación de las aplicaciones.

2.3.1.1.3. *Libraries*

Son un conjunto de bibliotecas basadas en el lenguaje C o C++, las cuales son utilizadas por diversos componentes del sistema. Entre estas se pueden encontrar bibliotecas como System C, bibliotecas de medios, bibliotecas de gráficos, bibliotecas de SQLite, entre otros.

2.3.1.1.4. *Application framework*

La arquitectura de Android está diseñada para la reutilización de componentes, por lo cual esta capa hace referencia a los API del entorno de trabajo utilizados como aplicaciones base.

2.3.1.1.5. *Applications*

Son un conjunto de aplicaciones base que proporcionan funcionalidades básicas a otras aplicaciones. Entre estas funcionalidades básicas están: correo electrónico, SMS, calendarios, mapas, contactos, entre otros.

2.3.2. IOS

Es el segundo sistema operativo más popular a nivel mundial para dispositivos móviles; según la página web Statcounter[8] IOS cuenta con un 27,47 % de la participación del mercado a nivel global.

[8] Statcounter. *GlobalStats.* https://gs.statcounter.com/os-market-share/mobile/worldwide.

Fue desarrollado por Apple, en los lenguajes de programación: C, C++, Objective-C y Swift. Cabe mencionar que Apple no permite la utilización de IOS en *hardware* de terceros. Actualmente, su versión más reciente es IOS 14, lanzada en el mes de septiembre de 2020

2.3.3. Windows

En el mercado actual tiene una participación casi nula; según la página web Statcounter[9] Windows Mobile cuenta con un 0,02 % del total de usuarios que utilizan este sistema operativo.

Fue desarrollado por Windows en el lenguaje de programación C++. Actualmente se encuentra EOF; su última versión fue Windows 10 Mobile, lanzada el mes de julio de 2015.

2.3.4. Samsung

Este sistema operativo es mejor conocido como Tizen. En la actualidad este SO está más orientado a otro tipo de dispositivos inteligentes como: televisores, *smartwatches*, entre otros. y no tanto hacia smartphones.

En el mercado actual, tiene una participación casi nula; según la página web Statcounter[10] el sistema operativo de Samsung cuenta con un 0,28 % del total de usuarios que utilizan este sistema operativo.

[9] Statcounter. *GlobalStats*. https://gs.statcounter.com/os-market-share/mobile/worldwide.
[10] Ibíd.

Fue desarrollado por Samsung y se encuentra basado en la plataforma Linux de Samsung (Samsung Linux Platform - SLP). Actualmente su versión más reciente es la 4.0.0.4, lanzada en mayo de 2019.

2.3.5. Otros

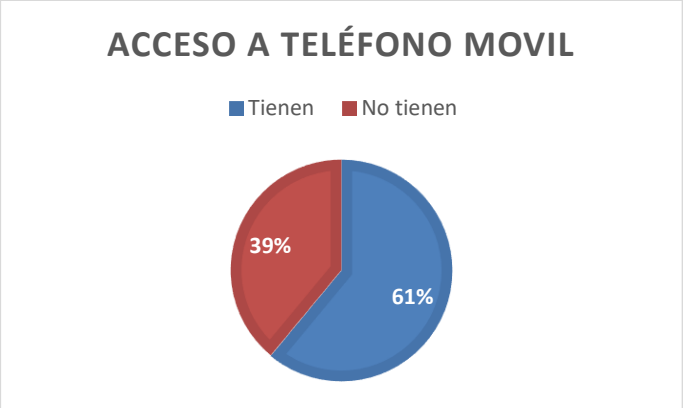
Adicional a los sistemas operativos antes mencionados, existen otros con menor participación en el mercado; según la página web Statcounter[11] estos otros sistemas operativos cuentan con un 0,30 % del total de usuarios. Entre estos se pueden mencionar: HarmonyOS, Symbian, Series 40, entre otros.

2.3.6. Uso de los sistemas operativos móviles en Guatemala

En una nota publicada en el sitio web soy502 en enero de 2020[12], se muestra un resumen sobre los datos obtenidos del último censo realizado en el territorio nacional acerca del uso de teléfonos móviles. Dicha nota menciona los siguientes resultados: un total de 7,7 millones de 12,5 millones (12 528 937) de encuestados tienen acceso a un teléfono móvil (61 % de la población).

[11] Statcounter. *GlobalStats*. https://gs.statcounter.com/os-market-share/mobile/worldwide.
[12] MEDINILLA, A. *El censo revelo que el 66 % de guatemaltecos usan celular*. https://www.soy502.com/articulo/62-guatemaltecos-encuestados-censo-usan-celular-101025.

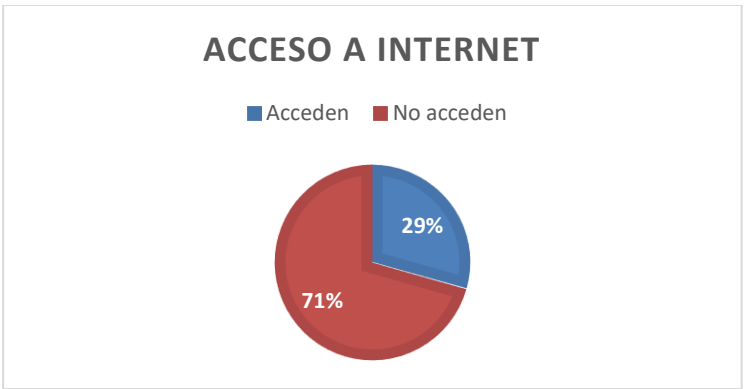
Figura 30. **Gráfica del porcentaje de población que tiene un teléfono móvil**



Fuente: elaboración propia con base en Medinilla, A. 2020.

Adicionalmente, de la nota antes mencionada cabe resaltar que solo un total de 3,6 millones (3 673 979) de usuarios acceden al internet mediante sus teléfonos móviles (29,4 % de la población).

Figura 31. **Gráfica del porcentaje de población que accede al internet mediante su teléfono móvil**



Fuente: elaboración propia con base en Medinilla, A. 2020.

De los 7,7 millones de guatemaltecos que poseen un teléfono móvil, según la página web Statcounter[13], en enero de 2021, un 87,54 % de usuarios tienen un dispositivo con sistema operativo Android (por lo que este es el principal sistema operativo utilizado en Guatemala).

A continuación, se detalla el porcentaje de usuarios que utiliza los principales sistemas operativos para teléfonos móviles en los últimos 12 meses, hasta la fecha.

Tabla I. **Comparativa de uso de los sistemas operativos (%)**

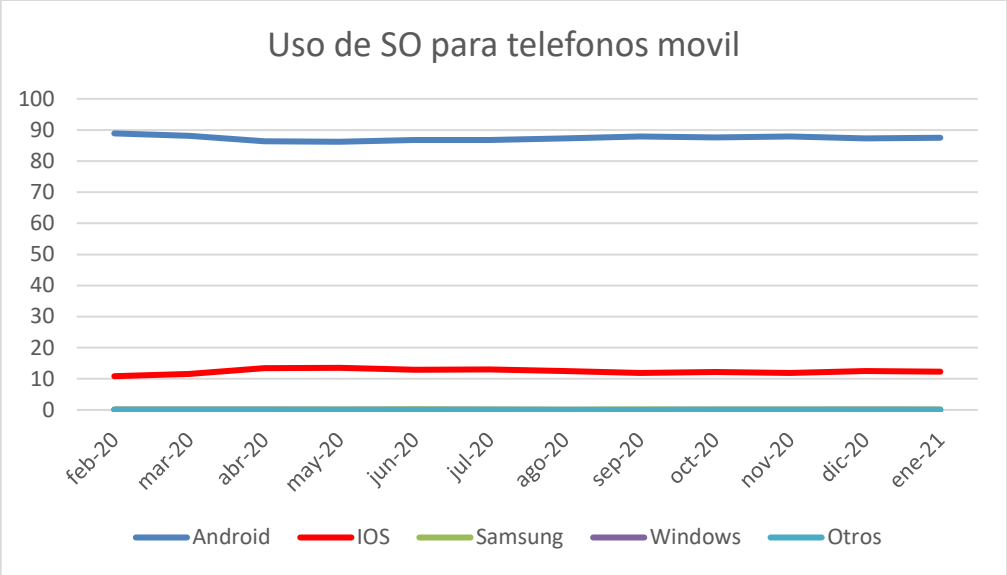
	Android	IOS	Samsung	Windows	Otros
Febrero 2020	88,9	10,85	0,13	0,05	0,07
Marzo 2020	88,12	11,63	0,17	0,05	0,02
Abril 2020	86,33	13,39	0,19	0,05	0,04
Mayo 2020	86,22	13,54	0,19	0,01	0,03
Junio 2020	86,79	12,93	0,22	0,01	0,03
Julio 2020	86,77	13,02	0,17	0,01	0,03
Agosto 2020	87,32	12,54	0,11	0,01	0,02
Septiembre 2020	87,93	11,91	0,13	0,01	0,02
Octubre 2020	87,69	12,17	0,16	0,01	0,03
Noviembre 2020	87,9	11,94	0,12	0,01	0,03
Diciembre 2020	87,35	12,46	0,15	0,02	0,02
Enero 2021	87,54	12,25	0,17	0,01	0,03

Fuente: elaboración propia, con datos obtenidos de https://gs.statcounter.com/os-market-share/mobile/guatemala. Consulta: febrero de 2021.

A continuación, se presentan, mediante un gráfico de líneas, los datos plasmados en la tabla I.

[13] Statcounter. *GlobalStats*. https://gs.statcounter.com/os-market-share/mobile/worldwide.

Figura 32. **Uso de los sistemas operativos en teléfonos móviles en Guatemala**



Fuente: elaboración propia con datos obtenidos de: https://gs.statcounter.com/os-market-share/mobile/guatemala. Consulta: febrero de 2021.

3. ANALISIS Y DISEÑO DE LA APLICACIÓN *CONFIREDES*

En el siguiente capitulo se realiza el análisis y diseño de la aplicación móvil *ConfiRedes*. Para el diseño de la aplicación se tomó como guía el modelo 4 + 1 vistas propuesto por Philippe Kruchten el cual utiliza el estándar IEEE 1471-2000 (*Recommended Practice for Software Requirementes Specification*), utilizado para describir los diferentes puntos de vista que conforman la arquitectura de un sistema de *software*.

3.1. Identificación del problema

Se identificó que no existen aplicaciones móviles en la play store de Google en las cuales se expongan, de forma concisa, conceptos y comandos para la configuración de dispositivos Cisco, y que, adicionalmente, integren herramientas para el cálculo de *subnetting*. Por lo tanto, el usuario necesita instalar dos o más aplicaciones móviles para tener acceso a esta información.

3.2. Justificación del problema

Las aplicaciones móviles en la actualidad son herramientas de fácil acceso, debido a que la mayoría de las personas cuentan con un dispositivo móvil. Lo anterior, facilita el acceso a materiales educativos; por ello, empresas como Cisco System proporcionan aplicaciones móviles para apoyar a los estudiantes, tanto desde el aspecto de conceptos (Cisco Technical Support[14], Cisco eReader[15],

[14] Cisco. *Technical Support.* https://play.google.com/store/apps/details?id=com.cisco.swtg_android&hl=es_UY.
[15] Cisco. *eReader.* https://play.google.com/store/apps/details?id=com.cisco.dkit&hl=es_MX.

entre otros), como con aplicaciones que abarcan el aspecto práctico (Cisco Packet Tracer Mobile[16]). Estas herramientas ayudan a los estudiantes universitarios y de las acreditaciones de Cisco a aprender, repasar y poner en práctica los conceptos necesarios para el correcto funcionamiento de una red de computadoras.

En la *play store* de Android existen diversas aplicaciones (Subneteo de redes[17], VLSM/ CIDR Subnet Calculator[18], Subnetting Calculator[19],entre otros), enfocadas al *subnetting* y conceptos de redes de computadoras. Sin embargo, las aplicaciones que se enfocan en el *subnetting* solamente despliegan los resultados finales; no muestran el proceso de cómo se obtienen estos resultados. Esto genera que el estudiante no tenga los conceptos básicos de cómo se obtienen intervalos de redes, máscaras de red, identificadores de red, entre otros conceptos. A su vez, las aplicaciones que muestran conceptos de redes están más enfocas en ser tutoriales o material de apoyo para repaso. Por lo tanto, el contenido suele ser extenso y genera que el estudiante pierda el concepto principal de los temas. Otra limitante de la mayoría de las aplicaciones es el uso excesivo de publicidad de otros productos, por lo cual, su uso tiende a ser tedioso.

Por estos motivos, es importante que los estudiantes de los cursos Redes de computadoras 1 y Redes de computadoras 2 tengan a su disposición herramientas que les permitan tener como referencia conceptos y comandos basados en los programas de estudio de ambos cursos para la configuración de dispositivos Cisco.

---

[16] Cisco. *Packet Tracer Mobile.* https://play.google.com/store/apps/details?id=com.netacad. PacketTracerM&hl=es_MX.
[17] Google Play. *Subneteo de redes*. https://play.google.com/store/apps/details?id=com. rsanabria.subetting& hl=es_MX.
[18] Google Play. *VLSM/ CIDR Subnet Calculator*. https://play.google.com/store/apps/details?id= uk.co.znder. subnetcalculator&hl=es_MX.
[19] Google Play. *Subnetting Calculator.* https://play.google.com/store/apps/details?id=com. oosterglue. subnetcalc &hl=es_MX.

3.3. Alcances y límites de la solución

La aplicación se dirige a los estudiantes de los cursos Redes de computadoras 1 y Redes de computadoras 2 de la Facultad de Ingeniería, USAC. Entre los dispositivos que la aplicación maneja se encuentran *switch*, *switch* multicapa, *router*, *firewall* ASA y *firewall* PIX; así también, los protocolos configurables para cada dispositivo. La aplicación será desarrollada con el objetivo de que los estudiantes de los cursos antes mencionados puedan apoyarse para obtener la información relevante y los comandos para configurar los dispositivos en topologías Cisco.

La aplicación en un futuro podrá ser utilizada por universidades privadas nacionales que implementan en su pénsum de estudio cursos de redes de computadoras (Universidad del Valle, Universidad Mariano Gálvez, Universidad Galileo, entre otras). Además, se puede expandir la aplicación al agregarle dispositivos y protocolos (no necesariamente de la propiedad de Cisco), para poder ser utilizada como herramienta de apoyo para empleados de empresas que se dediquen al área de infraestructura.

Entre las limitantes actuales de la aplicación se encuentran los pocos dispositivos y protocolos configurables; esto, debido a que la aplicación se enfoca en los cursos Redes de computadoras 1 y Redes de computadoras 2. Por lo tanto, no puede ser utilizado por otro tipo de usuarios, por ejemplo: estudiantes de certificaciones de Cisco, trabajadores de empresas del área de infraestructura, etcétera.

3.4. Propuesta de aplicación *ConfiRedes* como solución

La aplicación *ConfiRedes* consiste en un desarrollo para dispositivos móviles (SO Android) que permita apoyar a la configuración de dispositivos Cisco. Mediante contenido didáctico y multimedia, esta aplicación muestra al usuario la forma correcta de realizar las configuraciones. Además, cuenta con una calculadora de *subnetting*, la cual muestra al usuario paso a paso cómo se realiza el proceso de cálculo.

3.4.1. Dispositivos configurables contemplados en la propuesta

Los dispositivos que se pueden encontrar dentro de *ConfiRedes* se seleccionaron en función de los que se trabajan en las prácticas y proyectos de los cursos Redes de computadoras 1 y Redes de computadoras 2; estos son:

- *Switch*
- *Switch multilayer*
- *Router*
- *Firewall* ASA/PIX

Las funcionalidades de dichos dispositivos fueron enunciadas en el capítulo 1 del presente documento. Dentro de la aplicación se tiene la opción de seleccionar el dispositivo. Posterior a ello, se despliega la información relevante sobre su funcionamiento, comandos sobre las configuraciones básicas y contenido multimedia que ejemplifica la forma correcta de implementar los comandos (configuraciones básicas).

3.4.1.1. Protocolos configurables en el dispositivo *switch*

A continuación, se listan los protocolos configurables contemplados en la aplicación *ConfiRedes* para un dispositivo *switch* Cisco, el cual trabaja en la capa 2 del modelo OSI.

Tabla II. **Protocolos configurables en un *Switch***

Id	Protocolo
SN1	VLAN
SN2	VTP
SN3	STP

Fuente: elaboración propia.

En el capítulo 1 del presente documento se describen las funcionalidades y comandos de cada uno de los protocolos. Dentro de la aplicación se tiene la opción de seleccionar el protocolo (una vez seleccionado el dispositivo); posterior a ello, se despliega la información relevante sobre su funcionamiento, los comandos para configurar el protocolo y el contenido multimedia que ejemplifica la forma correcta de implementar los comandos.

3.4.1.2. Protocolos configurables en el dispositivo *switch multilayer*

A continuación, se listan los protocolos configurables contemplados en la aplicación *ConfiRedes* para un dispositivo *switch multilayer* Cisco, el cual trabaja en las capas 2 o 3 del modelo OSI.

Tabla III. **Protocolos configurables en un *switch multilayer***

Id	Protocolo
SM1	VLAN
SM2	InterVLAN
SM3	VTP
SM4	Ruteo estático
SM5	Ruteo dinámico
SM6	*Access-list*
SM7	Redundancia

Fuente: elaboración propia.

En el capítulo 1 del presente documento se describen las funcionalidades y comandos de cada uno de los protocolos. Dentro de la aplicación se tiene la opción de seleccionar el protocolo (una vez seleccionado el dispositivo); posterior a ello, se despliega la información relevante sobre su funcionamiento, los comandos para configurar el protocolo y el contenido multimedia que ejemplifica la forma correcta de implementar los comandos.

3.4.1.3. Protocolos configurables en el dispositivo *router*

A continuación, se listan los protocolos configurables contemplados en la aplicación *ConfiRedes* para un dispositivo router Cisco, el cual trabaja en la capa 3 del modelo OSI.

Tabla IV. **Protocolos configurables en un router**

Id	Protocolo
RO1	InterVLAN
RO2	Ruteo estático
RO3	Ruteo dinámico

Continuación de la tabla IV.

RO4	*Access-list*
RO5	NAT
RO6	Redundancia

Fuente: elaboración propia.

En el capítulo 1 del presente documento se describen las funcionalidades y comandos de cada uno de los protocolos. Dentro de la aplicación se tiene la opción de seleccionar el protocolo (una vez seleccionado el dispositivo); posterior a ello, se despliega la información relevante sobre su funcionamiento, los comandos para configurar el protocolo y el contenido multimedia que ejemplifica la forma correcta de implementar los comandos.

3.4.1.4. Protocolos configurables en el dispositivo *firewall* ASA/PIX

A continuación, se listan los protocolos configurables contemplados en la aplicación *ConfiRedes* para un dispositivo *firewall* ASA/PIX Cisco, el cual trabaja en la capa 3 del modelo OSI.

Tabla V. **Protocolos configurables en un firewall**

Id	Protocolo
FI1	VLAN
FI2	Políticas de seguridad
FI3	*Access-list*
FI4	SSH

Fuente: elaboración propia.

En el capítulo 1 del presente documento se describen las funcionalidades y comandos de cada uno de los protocolos. Dentro de la aplicación se tiene la opción de seleccionar el protocolo (una vez seleccionado el dispositivo); posterior a ello, se despliega la información relevante sobre su funcionamiento, los comandos para configurar el protocolo y el contenido multimedia que ejemplifica la forma correcta de implementar los comandos.

3.4.2. Contenido de la aplicación

La aplicación *ConfiRedes* está orientada a ser una herramienta educativa, por lo cual posee contenido que permite comprender dispositivos de red Cisco y protocolos configurables en los mismos. Dicho contenido se clasifica en: contenido didáctico y contenido multimedia.

3.4.2.1. Contenido didáctico

El contenido didáctico utilizado en la aplicación *ConfiRedes* para describir los diferentes dispositivos y protocolos (con sus respectivos comandos de configuración) fue obtenido del capítulo 1 del presente documento.

3.4.2.2. Contenido multimedia

El contenido multimedia se compone, en este caso, de videos de autoría propia; para la elaboración de estos, se empleó el *software* de simulación de topologías de redes Cisco Packet Tracer. Los comandos empleados en los videos fueron descritos en función de los protocolos presentados en el capítulo 1 de este documento.

El contenido multimedia fue cargado en la plataforma de videos YouTube. por otro lado, todo el contenido adicional, que no es de autoría propia, se encuentra libre de copyright.

3.4.2.2.1. Contenido multimedia del dispositivo *switch*

A continuación, se listan los videos cargados en la plataforma de YouTube y sus respectivas URL.

Tabla VI. **URL de contenido multimedia dispositivo *switch***

Video	URL
Configuraciones básicas	https://www.youtube.com/watch?v=Z0acN1AMpeU
Interfaces	https://www.youtube.com/watch?v=UcM25czuV7k
Protocolo VLAN	https://www.youtube.com/watch?v=rIN052CxnN0
Protocolo VTP	https://www.youtube.com/watch?v=7JUadOy352c
Protocolo STP	https://www.youtube.com/watch?v=Mhg8f40l2kc

Fuente: elaboración propia.

3.4.2.2.2. Contenido multimedia del dispositivo *switch multilayer*

A continuación, se listan los videos cargados en la plataforma de YouTube y sus respectivas URL.

Tabla VII. **URL de contenido multimedia dispositivo *switch multilayer***

Video	URL
Configuraciones básicas	https://www.youtube.com/watch?v=ht4KOtoMOOg
Interfaces	https://www.youtube.com/watch?v=UcM25czuV7k

Continuación de la tabla VII.

Protocolo VLAN	https://www.youtube.com/watch?v=x_uyxc5jze4
Protocolo InterVLAN	https://www.youtube.com/watch?v=cf7CobOk9x0
Protocolo VTP	https://www.youtube.com/watch?v=zv3YPiewBnY
Enrutamiento estático	https://www.youtube.com/watch?v=gkYZ2UCJdWw
Enrutamiento dinámico	https://www.youtube.com/watch?v=q-6rxIO46nc
Access-list	https://www.youtube.com/watch?v=cDqq5Cr9x24
Redundancia	https://www.youtube.com/watch?v=2XYj-aIn8JU

Fuente: elaboración propia.

3.4.2.2.3. Contenido multimedia de dispositivo *router*

A continuación, se listan los videos cargados en la plataforma de YouTube y sus respectivas URL.

Tabla VIII. **URL de contenido multimedia dispositivo router**

Video	URL
Configuraciones básicas	https://www.youtube.com/watch?v=iduPDOSItmw
Protocolo InterVLAN	https://www.youtube.com/watch?v=wIwFuD3Z59w
Enrutamiento estático	https://www.youtube.com/watch?v=JRbMaWiPTrw
Enrutamiento dinámico	https://www.youtube.com/watch?v=wxfZEB0Pk7A
Access-list	https://www.youtube.com/watch?v=kC5beyDxUF4
Protocolo NAT	https://www.youtube.com/watch?v=4Y50HHVga_Q
Redundancia	https://www.youtube.com/watch?v=1mR8PfnfonA

Fuente: elaboración propia.

3.4.2.2.4. Contenido multimedia del dispositivo *firewall*

A continuación, se listan los videos cargados en la plataforma de YouTube y sus respectivas URL.

Tabla IX. **URL de contenido multimedia dispositivo firewall**

Video	URL
Configuraciones básicas	https://www.youtube.com/watch?v=-H2MSFs9F3c
Protocolo VLAN	https://www.youtube.com/watch?v=zj6mLA4FVvw
Políticas de seguridad	https://www.youtube.com/watch?v=pfEmgYHhPHI
Access-list	https://www.youtube.com/watch?v=0qyMvb1pQac
SSH	https://www.youtube.com/watch?v=p6BUBkYJLwA

Fuente: elaboración propia.

3.4.3. Funcionalidades

Las funcionalidades de la aplicación móvil están orientadas a brindar una interfaz intuitiva y amigable al usuario, tratando de simplificar de la mejor manera posible los procesos.

A continuación, se listan las funcionalidades principales de la aplicación *ConfiRedes*.

Tabla X. **Funcionalidades de la aplicación *ConfiRedes***

ID	Funcionalidad	Descripción
FU1	Desplegar ayuda	Permite visualizar al usuario una guía básica sobre los iconos y la navegación dentro de la aplicación *ConfiRedes*.

Continuación tabla X.

FU2	Desplegar menú	Permite visualizar al usuario una lista de accesos directos hacia la pantalla de las principales opciones, en las cuales se contemplan: pantalla principal, dispositivos configurables y ayuda.
FU3	*Subnetting*	El usuario debe ingresar la dirección IP (valores menores a 255), CIDR (valor menor a 32) y número de subredes. La aplicación validará los datos y realizará el cálculo de *subnetting* desplegando en pantalla, paso a paso, el procedimiento al usuario.
FU4	Desplegar información (dispositivo / protocolo)	Según la opción seleccionada por el usuario (dispositivo o protocolo), la aplicación desplegará en pantalla la información más relevante sobre esta.
FU5	Desplegar comandos	Según la opción seleccionada por el usuario, la aplicación desplegará en pantalla los comandos para realizar las configuraciones pertinentes. En el caso de los dispositivos, los comandos son sobre las configuraciones básicas y, en los protocolos, los comandos para su configuración.
FU6	Desplegar video	Según la opción seleccionada por el usuario (dispositivo o protocolo), la aplicación mostrará el video de la configuración seleccionada. El sistema valida si el video aún está disponible en la plataforma de YouTube; en caso contrario, retornará un mensaje de error. Adicionalmente, valida si el video es restaurado; si es el caso, lo retoma desde donde lo dejó de ver el usuario.

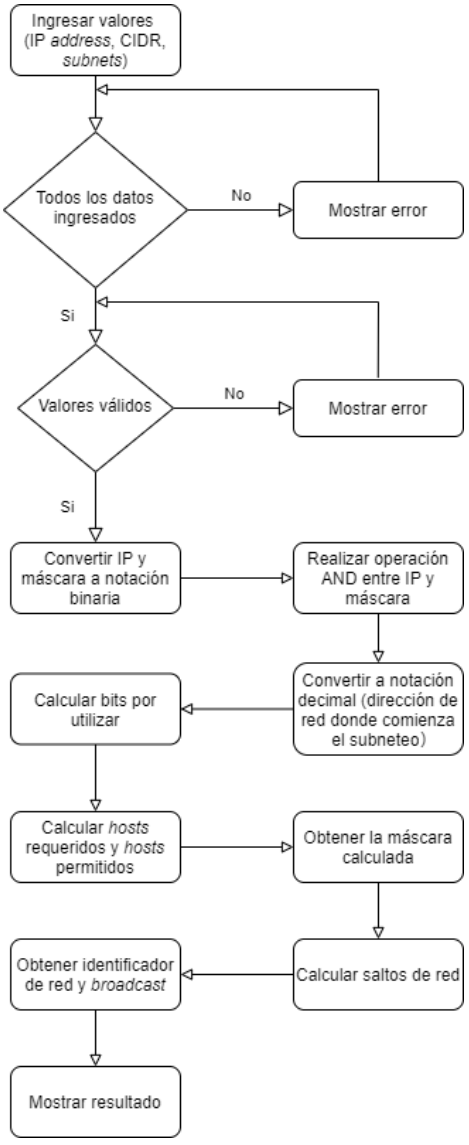
Fuente: elaboración propia.

Las funcionalidades FU4, FU5 y FU6 son aplicables a las pantallas de dispositivos y a las pantallas de protocolos. Esto, debido a que su funcionamiento es el mismo.

3.4.3.1. Fujo de la funcionalidad FU3

A continuación, se describe la funcionalidad FU3 mediante un diagrama de flujo.

Figura 33. **Diagrama de flujo de la funcionalidad *Subnetting***

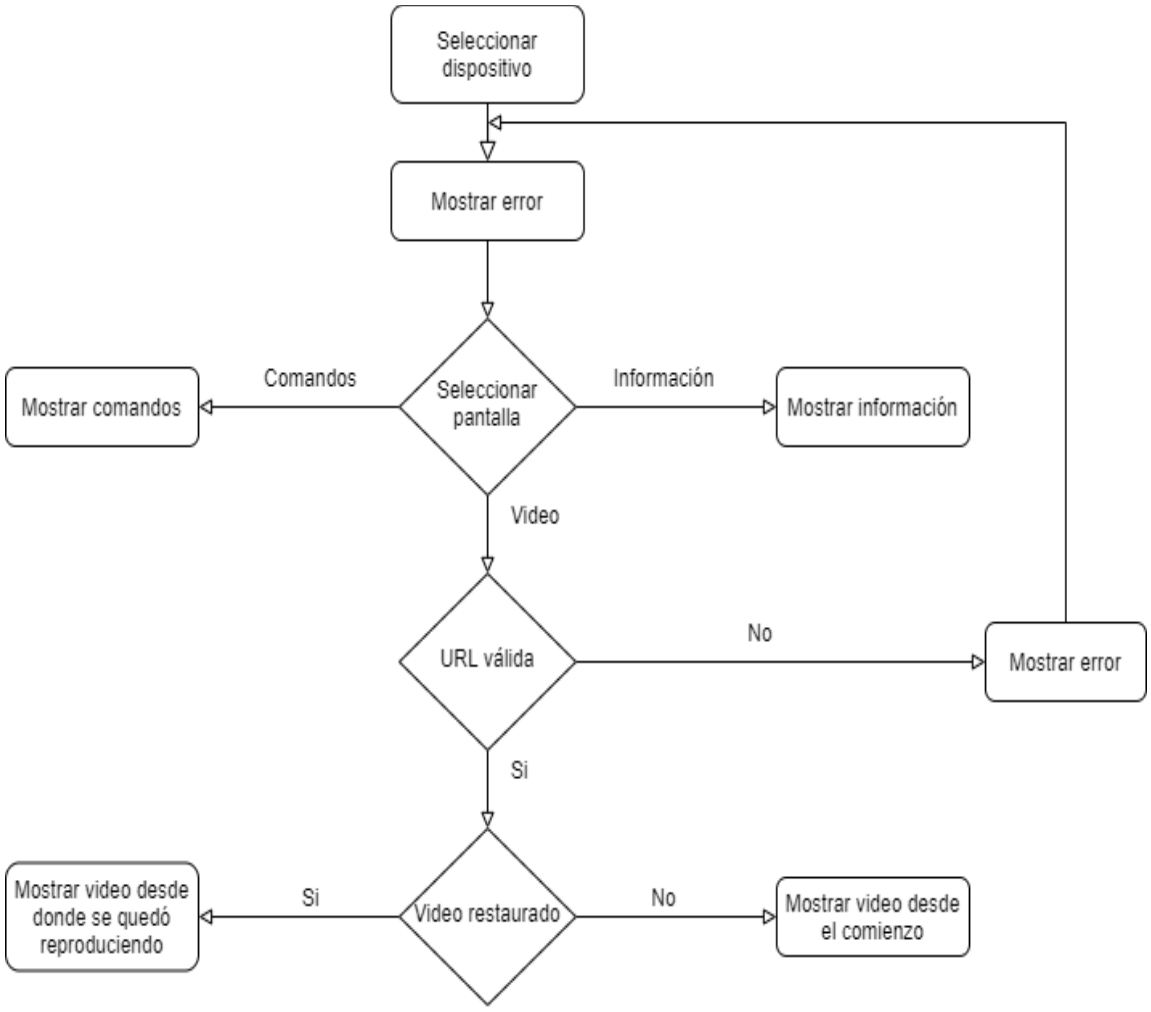


Fuente: elaboración propia, empleando software Draw.io.

3.4.3.2. Fujo de las funcionalidades FU4, FU5 y FU6

A continuación, se describen las funcionalidades FU4, FU5 y FU6 mediante un diagrama de flujo.

Figura 34. **Diagrama de flujo de las funcionalidades: Desplegar información, Desplegar comandos y Desplegar video**



Fuente: elaboración propia, empleando software Draw.io.

3.5. Diseño de la aplicación *ConfiRedes*

El diseño de la aplicación es una etapa fundamental en cualquier proyecto, ya que permite llegar a una solución que cumpla con los requerimientos del problema. Un mal diseño puede generar problemas y provocar que el proyecto caiga en constantes cambios.

Un correcto diseño permite entender y desarrollar de manera más fácil la aplicación, debido a que se conoce cómo funciona cada uno de los componentes que van a interactuar para completar los objetivos propuestos. Una vez finalizado el proyecto, se facilita la tarea de modificación o adición de funcionalidades para los desarrolladores o analistas de *software*. Por tal motivo, se puede implementar una arquitectura de *software*; es decir, un conjunto de patrones y abstracciones que proporcionan un marco definido sobre la forma en que se abarcará el proyecto.

Al tomar en cuenta las ventajas de trabajar con una arquitectura de *software*, el modelo *4 + 1 vistas* fue el utilizado para el diseño de la aplicación *ConfiRedes*; por ello, a continuación se describe el modelo utilizado y cada una de sus vistas.

3.5.1. Modelo *4 + 1 vistas*

El modelo *4 + 1 vistas* permite describir la arquitectura de un sistema de *software* que se basa en el uso de múltiples perspectivas. Fue propuesto por Philippe Kruchten en 1995 y encaja con el estándar IEEE 1471-2000 (*Recommended Practice for Software Requirementes Specification*).

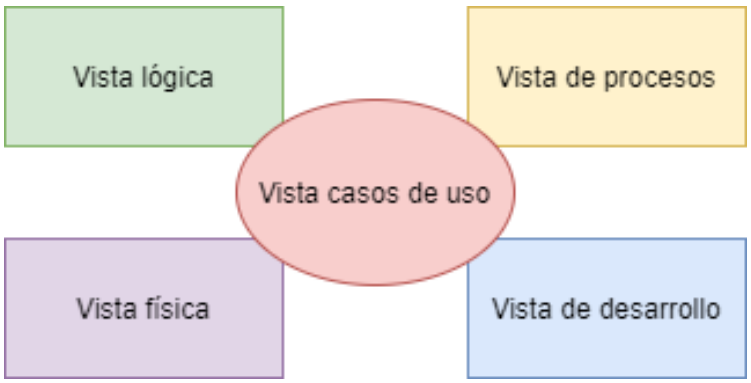
Se denomina *4 + 1 vistas* debido a que el modelo se divide en cuatro vistas diferenciadas (lógica, de desarrollo, de proceso y física) y una vista (de escenario) adicional, la cual cumple con la función de relacionar las diferenciadas entre sí.

Cada una de estas, busca modelar un punto de vista. Una vista se define como una representación de todo el sistema desde una determinada perspectiva, y, un punto de vista se define como un conjunto de normas para realizar y describir la vista.

Las vistas que conforman este modelo permiten tomar en cuenta las perspectivas de usuarios finales, desarrolladores, ingenieros de sistemas, etc. Con esto, garantiza que el sistema contará con las funcionalidades requeridas por los diversos actores que interactúan con el mismo.

A continuación, se documenta el diseño de la aplicación ConfiRedes, por medio de diferentes diagramas que modelan el sistema en función de las diferentes vistas del modelo descrito.

Figura 35. **Modelo *4 + 1 vistas***

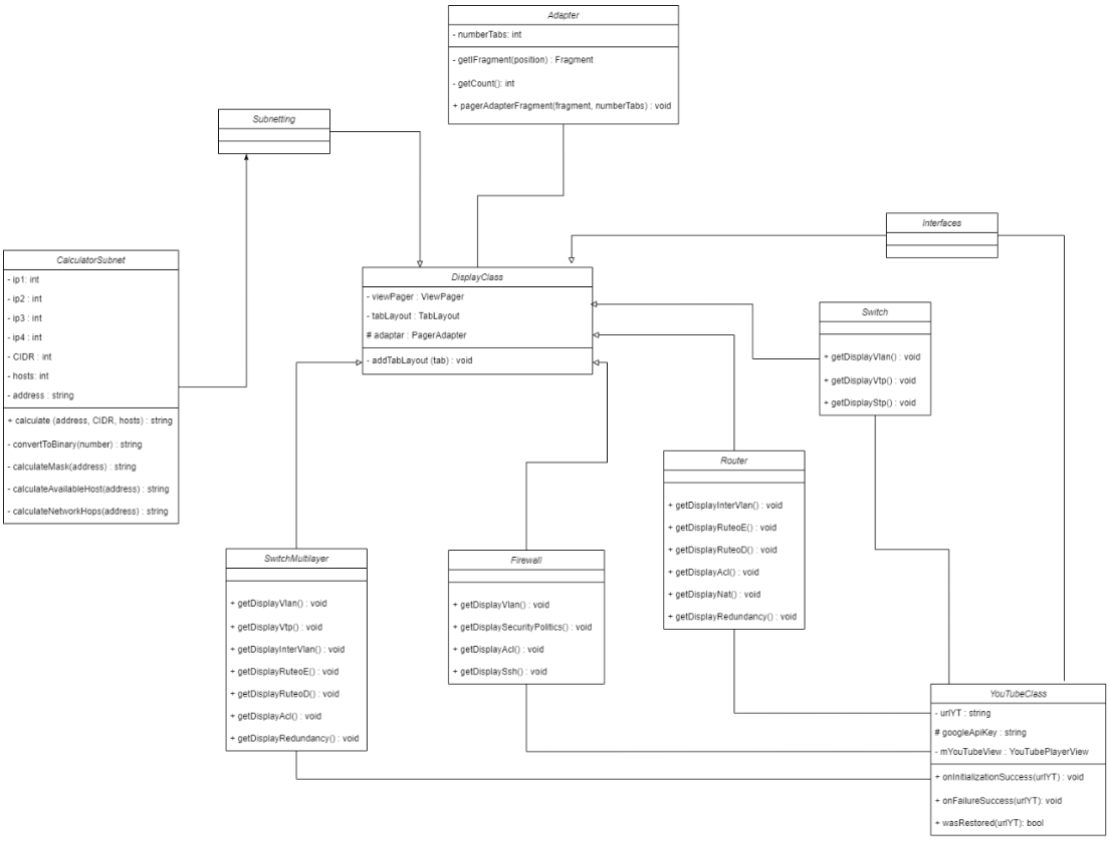


Fuente: elaboración propia, empleando software Draw.io.

3.5.1.1. Vista lógica

En esta vista se modelan las funcionalidades que se proporcionarán a los usuarios y se enfoca en describir qué es lo que el sistema debe ser capaz de realizar. En esta vista se modela a través del diagrama de clases o diagramas de comunicación.

Figura 36. **Diagrama de clases**

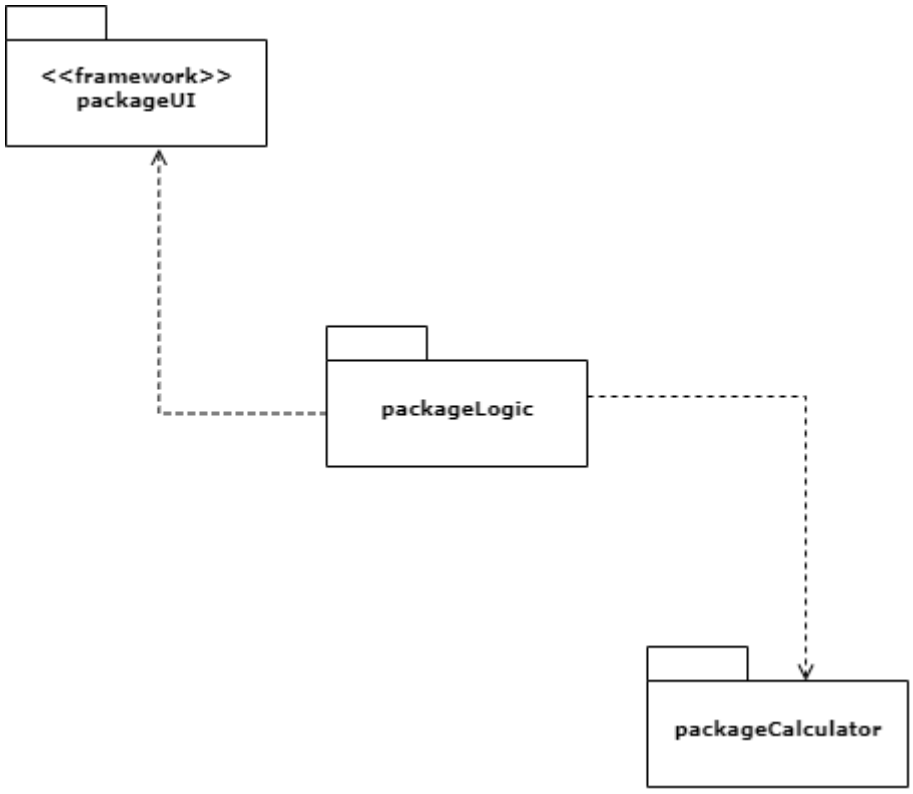


Fuente: elaboración propia, empleando software Draw.io.

3.5.1.2. Vista de desarrollo

En esta vista se modela cómo la solución se encuentra divida en componentes y la dependencia que existe entre estos. En esta vista se modela a través del diagrama de paquetes.

Figura 37. **Diagrama de paquetes**

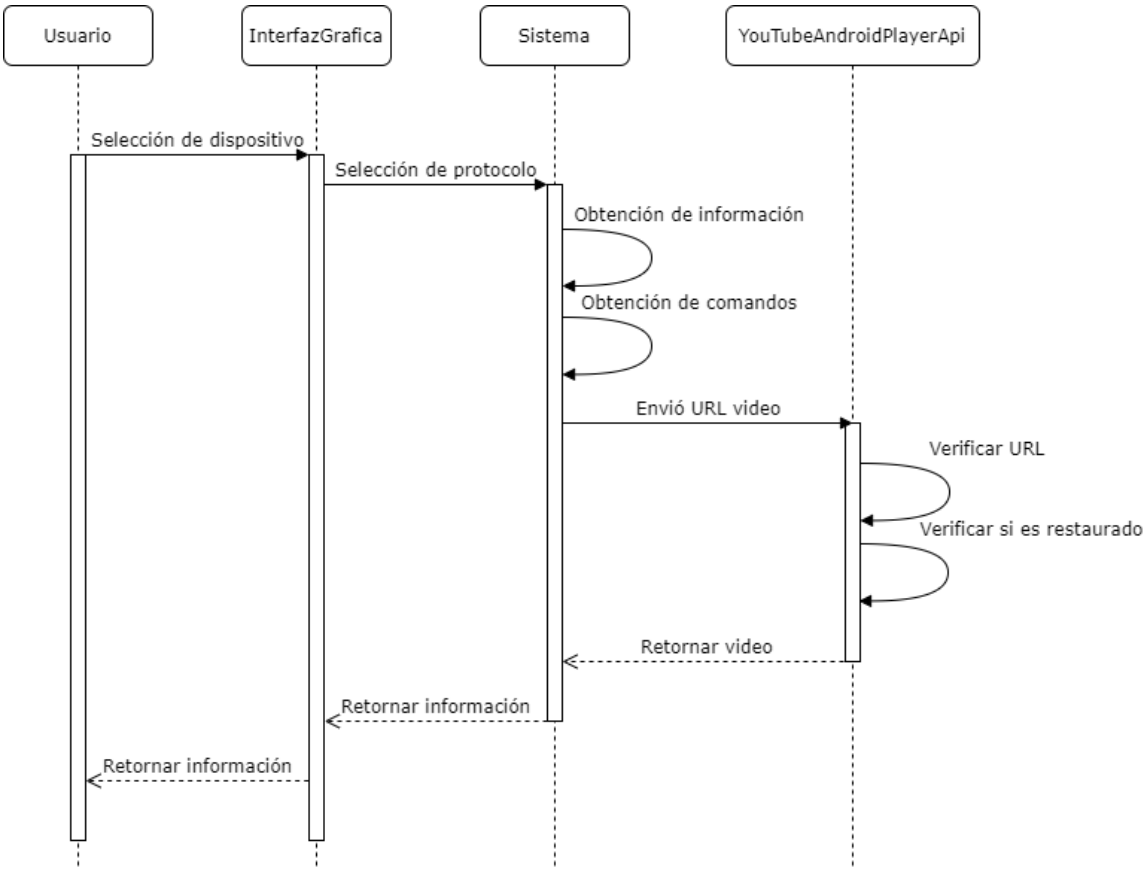


Fuente: elaboración propia.

3.5.1.3. Vista de proceso

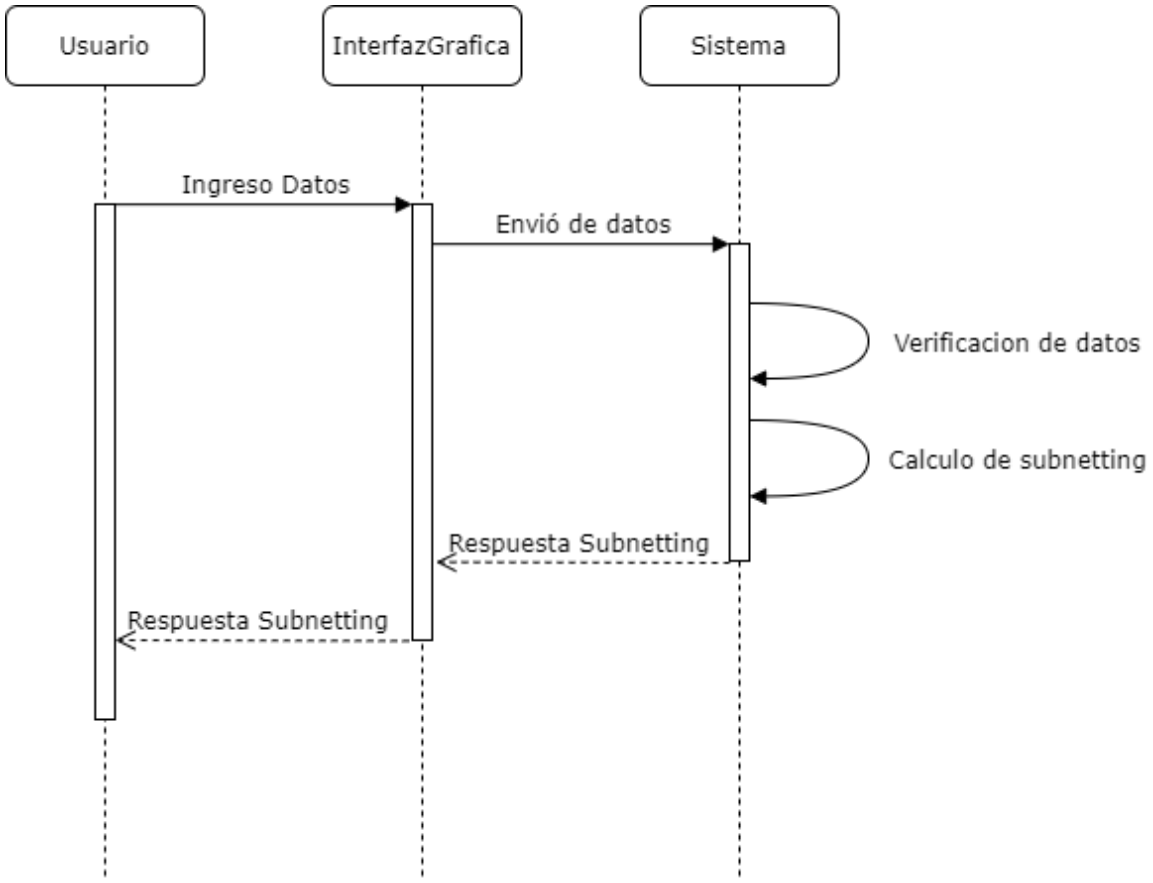
En esta vista se modelan los diferentes procesos que interactúan en la solución y la forma en que estos procesos se comunican entre sí. Su objetivo es describir el flujo de trabajo de los procesos paso a paso, considerando aspectos de concurrencia, escalabilidad, rendimiento, entre otros. En esta vista se modela a través del diagrama de secuencia.

Figura 38. **Diagrama de secuencia del sistema**



Fuente: elaboración propia, empleando software Draw.io.

Figura 39. **Diagrama de secuencias *subnetting***



Fuente: elaboración propia, empleando software Draw.io.

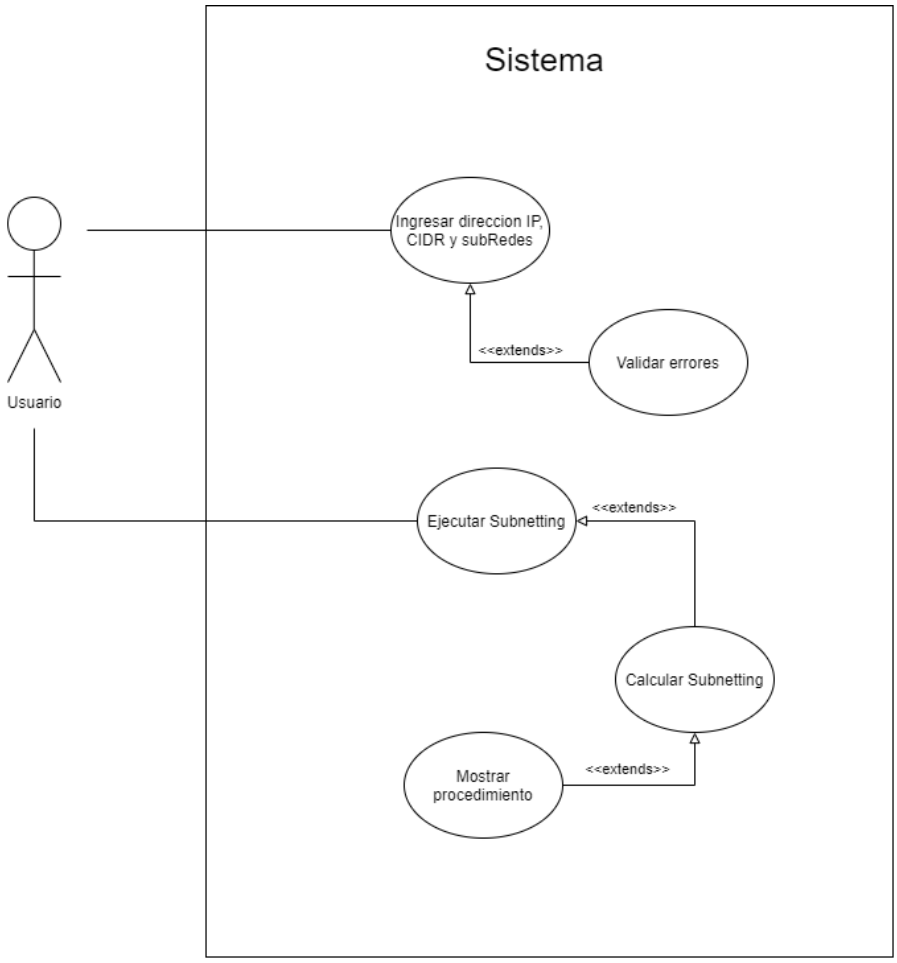
3.5.1.4. Vista de física

En la vista física se modelan cómo los diferentes componentes que conforman el sistema se encuentran distribuidos en los diferentes componentes físicos que conforman la solución. En esta vista se modela a través del diagrama de despliegue.

3.5.1.5. Vista de escenario

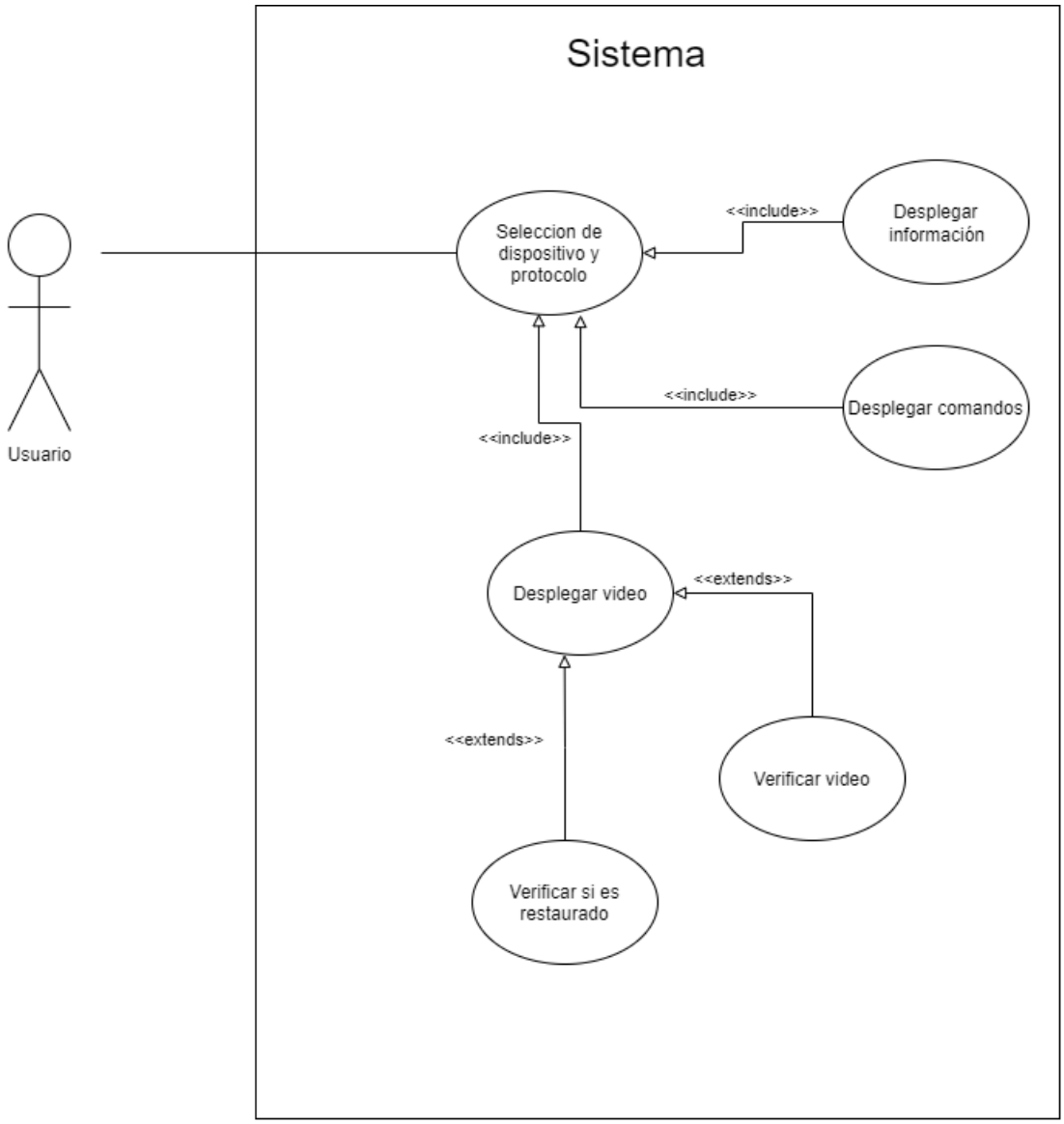
Es la vista llamada *4 +1*; en esta, se modelan las secuencias de las interacciones entre los objetos y procesos con el fin de que desde un caso de uso se pueda visualizar cómo se va integrando las vistas: lógica, de desarrollo, de procesos y física. En esta vista se modela a través del diagrama de casos de uso.

Figura 40. **Diagrama de uso de caso contenido didáctico**



Fuente: elaboración propia, empleando software Draw.io.

Figura 41. **Diagrama de caso de uso *subnetting***



Fuente: elaboración propia, empleando software Draw.io.

3.6. Herramientas de desarrollo

Para la creación de la aplicación móvil se utilizaron diversas herramientas de *software* y *hardware* que permitieran la creación de una aplicación intuitiva y amigable para el usuario. A continuación se detallan las herramientas utilizadas en la fase de desarrollo y pruebas, clasificándolas en herramientas para la creación de la aplicación móvil, contenido multimedia y dispositivos de pruebas.

3.6.1. Aplicación móvil

- Android Studio: Entorno de desarrollo integrado utilizado para el desarrollo de aplicaciones para dispositivos con sistemas operativo Android. Se utilizó para el desarrollo completo de la aplicación *ConfiRedes*.
- YouTubeAndroidPlayerApi: API para aplicaciones móviles Android que permite incorporar las funcionalidades de reproducción de videos de YouTube. Este API se implementó en la sección de Configuración de la aplicación *ConfiRedes* para la reproducción del contenido multimedia utilizado y para la correcta configuración de configuraciones básicas y protocolos.
- draw.io: Página web que permite la generación de diagramas utilizados para la documentación de proyectos. Se utilizó para la elaboración de los diagramas (de clase, de flujo, de secuencia, de paquetes y de casos de uso) utilizados para la documentación de la aplicación colocados en este capítulo.

3.6.2. Contenido multimedia

- Cisco Packet Tracer: Herramienta que permite el diseño y simulación de topologías de red utilizando dispositivos Cisco. Se utilizó para la elaboración

de los videos (configuraciones básicas y configuración de protocolos) cargados en la plataforma de YouTube y utilizados en la sección de Configuración de la aplicación *ConfiRedes*.

- Adobe Photoshop: *Software* que permite la edición de diseños gráficos. Se utilizó para la elaboración del arte utilizado en los iconos e imágenes de la aplicación móvil y pantallas de inicio-fin del contenido multimedia.
- Adobe Premiere: *Software* que permite la edición de contenido multimedia. Se utilizó para la edición del contenido multimedia cargado en la plataforma de YouTube.

3.6.3. Dispositivos de pruebas

Para garantizar el correcto funcionamiento del producto final, se realizaron pruebas de la aplicación *ConfiRedes* en tres dispositivos diferentes. Los dispositivos utilizados se detallan a continuación.

- Dispositivo 1
  - Marca: Samsung
  - Modelo: S8
  - S.O: Android, v9 Pie
  - Procesador: Exynos 8895
  - Memoria: 4GB de RAM y 64GB de ROM
  - Pantalla: 5,8”, 1440 x 2960 px

- Dispositivo 2
  - Marca: Huawei
  - Modelo: Mate 30 Pro
  - S.O: Android, v10 Android 10
  - Procesador: Kirin 990

- Memoria: 8GB de RAM y 256GB de ROM
- Pantalla: 6,53”, 1176 x 2400 px

- Dispositivo 3
  - Marca: LG
  - Modelo: G8X Thinq
  - S.O: Android, v10 Android 10
  - Procesador: Snapdragon 855
  - Memoria: 6GB de RAM y 128 GB de ROM
  - Pantalla: 6,4”, 1080x2340 px

3.7. Requerimientos mínimos de la aplicación

Para asegurar el correcto funcionamiento de la aplicación “ConfiRedes”, el usuario debe de contar con un dispositivo móvil que cumpla con las siguientes características mínimas.

- S.O: Android, 5,0 Lollipop
- Almacenamiento: 30 Mb
- CPU: 1.0 Ghz
- RAM: 512 Mb
- Permisos: No requiere permisos del S.O

3.8. *Link* de descarga

https://play.google.com/store/apps/details?id=config_redes.app.redes.confiredes.

3.9. Código QR de descarga.

CONCLUSIONES

1. Al implementar un diseño arquitectónico basado en el modelo *4 + 1 capas*, se permite la separación de los diferentes aspectos del desarrollado de la aplicación. Así también, al tomar en cuenta la perspectiva de cada uno de los involucrados en el sistema, se permite crear una interfaz con la cual el usuario final puede interactuar de una manera fácil, intuitiva y amigable. En la vista de casos de uso se contemplaron los procesos que realizará la aplicación y estos se trataron de simplificar lo más posible, para que las transiciones entre pantallas fueran fluidas (apoyado en la vista lógica, donde se estructuró una aplicación que, en su mayor parte, hereda de otras clases).

2. Las pantallas correspondientes a la principal y de menú (ver apéndices), facilitan la búsqueda mediante botones con imágenes y descripciones claras y concisas que facilitan el desplazamiento entre estas.

3. La pantalla correspondiente a la opción de *subnetting* proporciona una herramienta en la cual se validan los datos ingresados y, posterior a ser ingresados correctamente, despliega el procedimiento paso a paso. Así muestra cómo se van obteniendo cada uno de los resultados y al mismo tiempo despliega una explicación del procedimiento.

4. Aspectos como los mencionados en el capítulo 2, que enfatizan la importancia de tener plataformas alternas a la educación tradicional, las cuales puedan apoyar en circunstancias como la vivida en el año 2020 originada por la pandemia de COVID-19. Sumado a la practicidad de

utilizar el *smartphone* para cualquier actividad cotidiana, estos impulsan las aplicaciones móviles como una muy buena alternativa. En Guatemala un 66 % de la población posee un *smartphone*, lo cual abre un mercado para estas soluciones en apoyo a la educación.

RECOMENDACIONES

1. Promover el uso de la aplicación *ConfiRedes* como herramienta de apoyo para la configuración de prácticas y proyectos para los cursos Redes de computadoras 1 y Redes de computadoras 2, con la colaboración de la Escuela de Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, USAC.

2. Extender el uso de la aplicación *ConfiRedes* a otras universidades nacionales que incorporen los cursos de redes de computadoras dentro de sus pénsum de estudios, agregando dispositivos o protocolos para adaptarlos según sus necesidades.

3. Extender las funcionalidades de la aplicación *ConfiRedes*, agregando más dispositivos y protocolos de otras marcas (Huawei, Fortinet, Dell, etc.). Además, agregar módulos que permitan al usuario ingresar los comandos del protocolo que se va a configurar y este valide la sintaxis correspondiente, con el objetivo de adaptar la aplicación para ambientes laborales y no únicamente educativos.

BIBLIOGRAFÍA

1. ARIGANELLO, Ernesto. *Guía de estudio para la certificación CCNA Routing y Switching*. 4a ed. España: Ra-Ma, 2016. 572 p.

2. Aula school management. *Apps educativas ¿Cuáles son sus ventajas?* [en línea]. <https://www.aula1.com/apps-educativas/> [Consulta: enero de 2021].

3. BARROSO, Javier. *Windows phone, que es y para qué sirve*. [en línea]. <https://www.tuexperto.com/2012/05/09/windows-phone-que-es-y-para-que-sirve/>. [Consulta: enero de 2021].

4. BUNTON, Cam. *¿Qué es el sistema operativo Tizen de Samsung y en que dispositivos esta?* [en línea]. <https://www.pocket-lint.com/es-es/smartphones/noticias/samsung/127527-que-es-tizen-y-en-que-dispositivos-aparecera> [Consulta: enero de 2021].

5. Cisco, Sitio oficial. *Políticas de seguridad de la red*. [en línea]. <https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/13601-secpol.html>. [Consulta: diciembre de 2020].

6. DOHERTY, Jim; ANDERSON, Neil; DELLA, Paul. *Introducción a las redes Cisco.* 1a ed. España: Anaya multimedia, 2009. 560 p.

7. GARCIA, Roció. *¿Qué es iOS? Todo sobre el sistema operativo Apple.* [en línea]. <https://www.adslzone.net/reportajes/software/que-es-ios/>. [Consulta: enero de 2021].

8. LAMMLE, Todd. *CCNA Cisco Certified Network Associate Study Guide*. 6a ed. Estados Unidos: Sybex, 2011. 1008 p.

9. NIETO GONZALEZ, Alejandro. *¿Qué es Android?* [en línea]. <https://www.xatakandroid.com/sistema-operativo/que-es-android>. [Consulta: enero de 2021].

10. Read the Docs Template. *Diseño – Modelo 4+1 – Documento 1 (Software Architecture Document)*. [en línea]. <https://proyecto-semestral.readthedocs.io/en/latest/6%20-%20Design.html> [Consulta: enero de 2021].

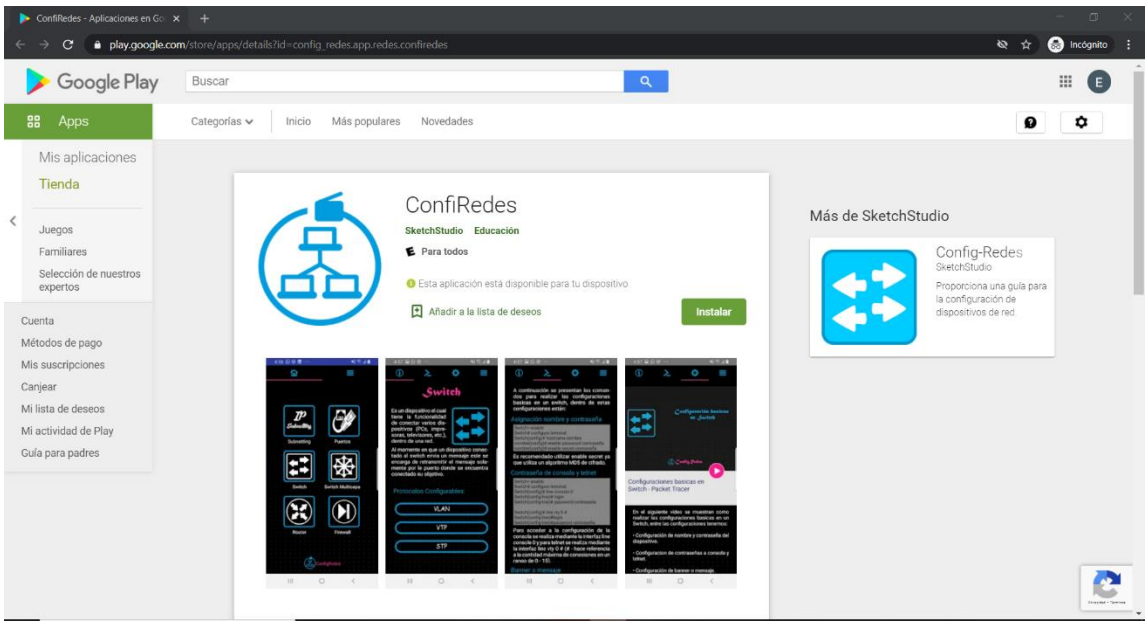
11. TANENBAUM, Andrew; WETHERALL, David. *Redes de Computadoras*. 5a ed. México: Pearson, 2012. 816p.

APÉNDICES

Apéndice 1. **Guía de usuario**

***Link* de descarga**

Lo primero es descargar la aplicación desde el siguiente link: https://play.google.com/store/apps/details?id=config_redes.app.redes.confiredes.



Fuente: elaboración propia.

Continuación apéndice 1.

Código QR

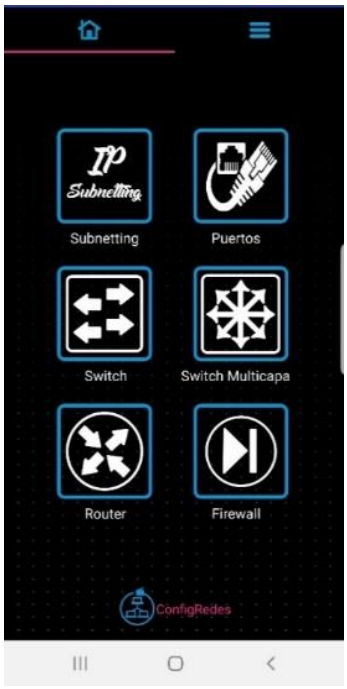
Como alternativa a descarga mediante el *link* de descarga, se puede realizar mediante el siguiente código QR:

Fuente: elaboración propia.

Pantalla principal

Esta es la primera pantalla que se visualiza al abrir la aplicación; en la parte superior se encuentra el acceso al menú. En la pantalla se pueden visualizar seis botones (*subnetting*, puertos, *switch*, *switch* multicapa, *router* y *firewall*); según la opción seleccionada, se redireccionará a la pantalla de la opción.

Continuación apéndice 1.

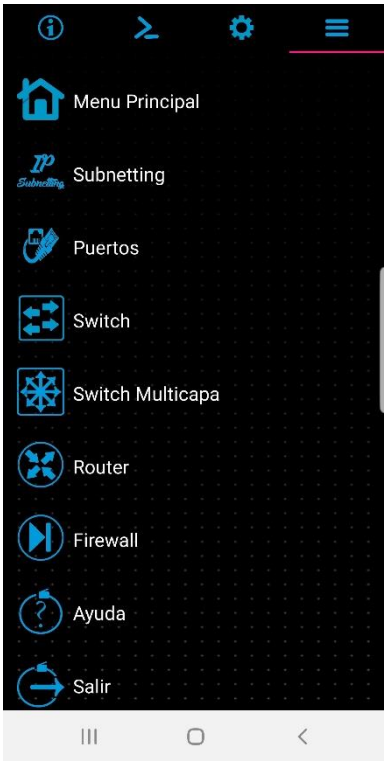


Fuente: elaboración propia.

Menú

Al acceder a la pantalla de menú se cuenta con: la opción de regresar a la pantalla principal, accesos directos hacia cada una de las opciones de la pantalla principal (*subnetting*, configuración de puertos, *switch*, *switch* multicapa, *router*, *firewall*), la opción que redirecciona hacia la pantalla de ayuda y la opción de salir de la aplicación.

Continuación apéndice 1.

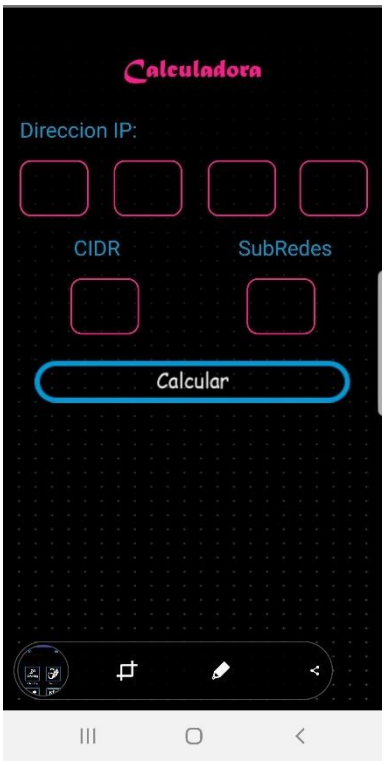


Fuente: elaboración propia.

Subnetting

Al seleccionar la opción de subnetting se despliega la pantalla correspondiente, se conforma de la dirección IP, CIDR y número de subredes para el cálculo.

Continuación apéndice 1.



Fuente: elaboración propia.

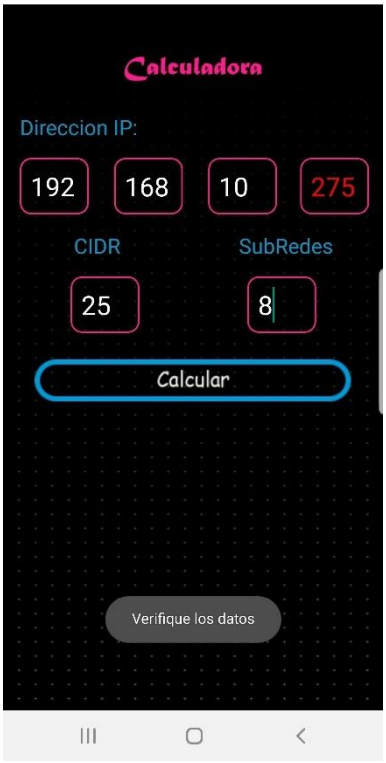
Al no ingresar un dato (octeto de la dirección IP, CIDR o de la cantidad de subredes) o ingresar un dato incorrecto (según las validaciones que se indican al finalizar este párrafo), se mostrará un mensaje de error durante un lapso de 2 segundos y se colocará en color rojo el dato erróneo (este cambiará al momento de ingresar un dato correcto y presionar el botón Calcular).

Se considera un dato incorrecto lo siguiente:

- Dirección IP: valor mayor a 255 o no ingresado.
- CIDR: valor mayor 32 o no ingresado.

Continuación apéndice 1.

- Subredes: valor no ingresado.

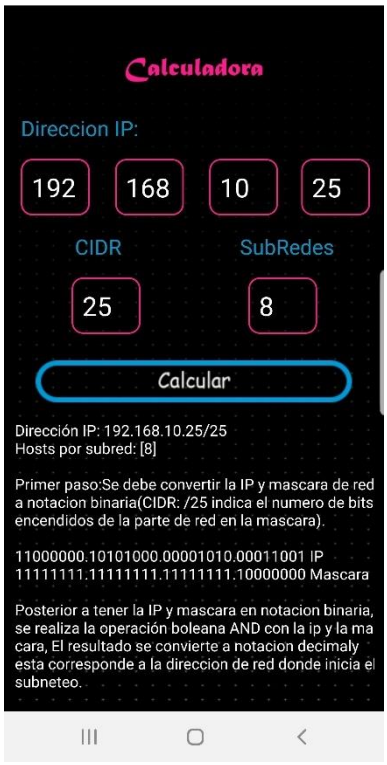


Fuente: elaboración propia.

Al ingresar los valores correctos y presionar el botón Calcular, se validará que los datos ingresados sean correctos (al ser correcto no despliega ningún mensaje de error y los datos se colocan en color blanco). Se mostrará el cálculo descrito, paso a paso, en la parte inferior.

Para visualizar completo el procedimiento se debe de realizar *scroll* vertical sobre el texto. En este caso, la funcionalidad de *subnetting* se conforma únicamente de esta pantalla.

Continuación apéndice 1.



Fuente: elaboración propia.

La última imagen corresponde a un caso donde se han ingresado correctamente los datos y se ha desplegado la información del proceso de *subnetting*.

Pantalla de dispositivo/protocolo

Al seleccionar una opción, ya sea dispositivo (desde la pantalla principal o menú) o protocolo (desde cualquier dispositivo), se despliega una pantalla compuesta por el nombre del dispositivo/protocolo, imagen del dispositivo, información relevante sobre el funcionamiento y, en el caso de los dispositivos, en la parte inferior, los protocolos configurables.

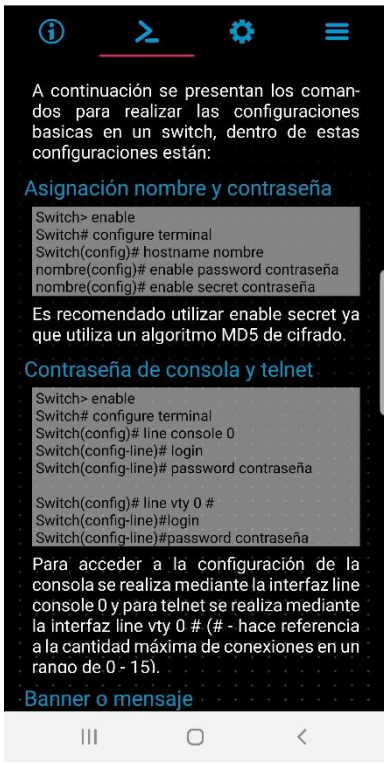
Continuación apéndice 1.

Fuente: elaboración propia.

Pantalla de comandos

En la pantalla de comandos se despliega la información o recomendaciones sobre los protocolos; esta pantalla tiene como objetivo principal mostrar los comandos con los cuales se configuran los protocolos.

Continuación apéndice 1.



Fuente: elaboración propia.

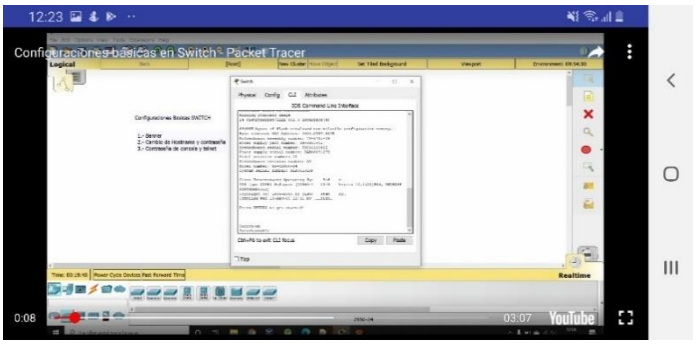
Pantalla de configuración

En esta pantalla se muestra una miniatura de la imagen del video que se va a reproducir y en la parte inferior se encuentra la información relevante sobre este. Para reproducir el video se debe presionar el botón Play.

Continuación apéndice 1.

Fuente: elaboración propia.

Al comenzar a reproducir el video automáticamente la pantalla se coloca de forma horizontal y para controlar los videos, se trabaja mediante los controles de YouTube.

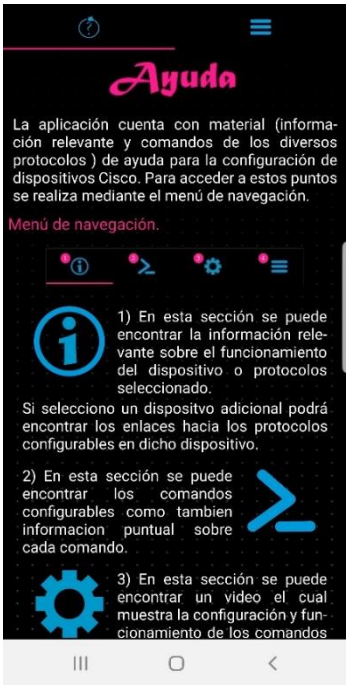


Fuente: elaboración propia.

Continuación apéndice 1.

Ayuda

En la pantalla de ayuda, la cual se encuentra en la pantalla de menú, se presenta el significado de cada uno de los botones de desplazamiento en la parte superior de las pantallas.



Fuente: elaboración propia.